

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

CENTRIPETAL NETWORKS, INC.,

Plaintiff,

v.

CISCO SYSTEMS, INC.,

Defendant.

CIVIL ACTION NO.
2:18cv94

*** * CONFIDENTIAL INFORMATION REDACTED * ***

TRANSCRIPT OF VIDEOCONFERENCE BENCH TRIAL PROCEEDINGS

Norfolk, Virginia

May 21, 2020

Volume 11
Pages 1570-1751

BEFORE: THE HONORABLE HENRY COKE MORGAN, JR.
United States District Judge

APPEARANCES:

KAUFMAN & CANOLES, P.C.

By: Stephen E. Noona

- and -

KRAMER LEVIN NAFTALIS & FRANKEL LLP

By: Paul J. Andre

Lisa Kobialka

Hannah Y. Lee

Counsel for the Plaintiff

TROUTMAN SANDERS LLP

By: Dabney J. Carr, IV

- and -

DUANE MORRIS LLP

By: Matthew C. Gaudet

Louis N. Jameson

Counsel for the Defendant

Carol L. Naughton, Official Court Reporter

Patent Owner, Centripetal Networks, Inc. - Ex. 2012, p. 1

I N D E X

PLAINTIFF'S
WITNESSPAGE

JAMES MALACKOWSKI

Direct Examination By Ms. Kobialka 1572

Cross-Examination By Mr. Jameson 1613

Redirect Examination By Ms. Kobialka 1632

DEFENDANT'S
WITNESSPAGE

MICHAEL SCHECK

Direct Examination By Mr. Gaudet 1658

Cross-Examination By Ms. Lee 1734

Redirect Examination By Mr. Gaudet 1744

E X H I B I T S

PLAINTIFF'S
NO.PAGE

PTX-1600 1583

PTX-1600, Pages 9 through 12 1620

DTX-409, Pages .001, .004 and .005 1719

DEFENDANT'S
NO.PAGE

DTX-693 1703

DTX-693.1 1703

DTX-729 1712

DTX-623 1725

DTX-623.1 1725

DTX-609 1732

DTX-632 1733

DTX-632.1 1733

~~Malackowski, J. - Direct~~

1	(Proceedings commenced at 10:03 a.m.)	09:57:14
2	THE CLERK: Civil Action Number 2:18cv94, plaintiff,	10:03:48
3	Centripetal Networks, Inc. v. Cisco Systems, Inc.	10:03:55
4	For the plaintiff, Ms. Kobialka, Mr. Noona, are you	10:03:59
5	ready to proceed?	10:04:03
6	MR. NOONA: We are, Your Honor.	10:04:05
7	THE CLERK: For defendants, Mr. Jameson and	10:04:06
8	Mr. Carr, are you ready to proceed?	10:04:10
9	MR. JAMESON: Yes, we are, Your Honor.	10:04:13
10	THE COURT: All right. We'll begin this morning	10:04:15
11	with what I assume is Cisco's last witness?	10:04:18
12	MS. KOBIALKA: Your Honor, it's Centripetal's last	10:04:27
13	witness.	10:04:29
14	THE COURT: I meant Centripetal. Excuse me. I	10:04:29
15	guess hope got ahead of me.	10:04:35
16	All right. You may proceed.	10:04:40
17	MS. KOBIALKA: We're presenting Mr. James	10:04:44
18	Malackowski.	10:04:54
19	JAMES MALACKOWSKI, called by the Plaintiff, having	10:05:02
20	been first duly sworn, was examined and testified as follows:	10:05:02
21	DIRECT EXAMINATION	10:05:03
22	BY MS. KOBIALKA:	10:05:03
23	Q. Mr. Malackowski, could you please introduce yourself?	10:05:03
24	A. Good morning. My name is Jim Malackowski. I'm the	10:05:05
25	Chairman and Chief Executive of Ocean Tomo, LLC,	10:05:09

—Malackowski, J. - Direct—

1 headquartered in Chicago, which is where I live, and today
2 I'm coming to you from my home.

3 Q. If we could turn to slide 7, could you give a quick
4 overview of what your opinion is going to be in this case?

5 A. Yes. My opinion in this case is to focus on the
6 valuation of Centripetal's technology and, in particular, how
7 that valuation will be impacted into the future. There are
8 three segments of that opinion.

9 Q. All right. And are you offering a damages opinion?

10 A. I am not.

11 Q. And how is your opinion different from what we've heard
12 from Mr. Gunderson? As I understand, you've watched the
13 trial.

14 A. Mr. Gunderson's opinion was focused on a minimum measure
15 of damages, as represented by a royalty for past
16 infringement, and my focus is on the impact of the asserted
17 infringement on Centripetal going forward and the notion of
18 how their activities were thwarted as a result of the
19 infringement.

20 Q. Thank you. Let's go to slide 3.

21 Where do you currently work?

22 A. So I am the Chief Executive of Ocean Tomo, LLC, in
23 Chicago. We have offices throughout the country and in Asia.

24 Q. And can you tell us a little bit about what Ocean Tomo
25 does?

—Malackowski, J. - Direct—

1 A. Yes. Your Honor, you can think of Ocean Tomo as an 10:06:25
2 investment banking firm or a financial advisory firm solely 10:06:29
3 focused on intellectual property. 10:06:32

4 We have three business groups. The first is the 10:06:34
5 valuation group, where we will appraise or value intellectual 10:06:36
6 property for transactions, investments, disputes. 10:06:41

7 Our second group is a strategy practice, where we 10:06:44
8 work with start-ups to some of the largest companies in the 10:06:48
9 world and, frankly, even governments, on how to manage their 10:06:51
10 intellectual property assets for their stakeholders. 10:06:54

11 And our third group is the investment bank. It's a 10:06:57
12 registered broker-dealer, and there we help investors to make 10:07:00
13 decisions as to whether or not to invest or buy or sell 10:07:05
14 businesses that are driven by IP or, frankly, the IP assets 10:07:08
15 themselves. 10:07:12

16 Q. And in your position, do you oversee all of those 10:07:13
17 different lines of business? 10:07:16

18 A. Yes. As CEO I have the opportunity and do engage with 10:07:17
19 clients across all three divisions, as well as I have 10:07:22
20 administrative responsibility for the company. 10:07:27

21 Q. Now, on the slide here I see a bullet about four from the 10:07:29
22 bottom that says, "Solutionary director for 13 years." 10:07:32

23 Could you talk a little bit about that and how that 10:07:35
24 will relate today? 10:07:37

25 A. As a result of my focus on IP, I'm asked from time to 10:07:38

—Malackowski, J. - Direct—

1 time to sit on various for-profit or nonprofit boards. One 10:07:43
2 of the companies that I worked on for 13 years, initially as 10:07:47
3 one of the founding directors and as the independent director 10:07:50
4 all the way through the sale of that business more than a 10:07:53
5 decade later, was Solutionary. 10:07:57

6 We were a managed security services provider. So, 10:07:58
7 as we'll talk about, it was an earlier stage of cyber 10:08:03
8 security than what's at issue in this case. 10:08:08

9 Q. All right. Now, let's talk a little bit about your 10:08:10
10 certifications. 10:08:12

11 Could you start at the third bullet, I believe, or 10:08:13
12 maybe -- yeah, the third bullet. 10:08:16

13 A. Yes. I have three certifications of note. 10:08:18

14 The first is as a Licensing Professional. That's a 10:08:20
15 recognition of experience in training and examination in the 10:08:25
16 transfer of intellectual property from one business to 10:08:30
17 another, either through licenses or sale. And so I've been a 10:08:33
18 CLP since that certificate was originated. 10:08:38

19 Q. And how about the next two certifications? 10:08:41

20 A. The next two are accounting. 10:08:43

21 Your Honor, I'm an accountant by training. My 10:08:46
22 university degree is in accounting and philosophy, and 10:08:49
23 really, since graduation, I have been a Registered Certified 10:08:53
24 Public Accountant, but within that, I've had a specialty 10:08:57
25 focus in valuation, so I'm certified in business valuation, 10:09:01

—Malackowski, J. - Direct—

1 forensic accounting. 10:09:05

2 And then you can even go deeper, and my real 10:09:06
3 practical experience, as I talked about, is in the valuation 10:09:09
4 of patents, trademarks, and copyrights. 10:09:11

5 Q. The second bullet refers to being the past president of 10:09:14
6 the Licensing Executive Society. Could you please talk a 10:09:18
7 little bit about that? 10:09:21

8 A. The Licensing Executive Society is the largest business 10:09:21
9 professional trade association in the world for technology 10:09:25
10 transfer. I was president of the U.S.A./Canada Division and 10:09:30
11 then president of the International Group. When I ran it, I 10:09:33
12 think we had about 10,000 members in 32 countries, so it was 10:09:37
13 quite a large effort. 10:09:41

14 Q. Have you taught any courses that relate to your opinion 10:09:42
15 today, and could you describe those? 10:09:46

16 A. Yes. Putting aside the work that I do for my own firm 10:09:49
17 for newer people, most of my training is either divided to 10:09:52
18 CLE, actually training lawyers on these subjects, or academic 10:09:57
19 teaching. And so I've taught at my alma mater, the 10:10:01
20 University of Notre Dame, University of Chicago, North 10:10:04
21 Western -- so a focus in the Midwest -- but also I've taught 10:10:07
22 at Harvard and the University of California and other places. 10:10:10

23 Q. And are there certain types of courses that you've taught 10:10:12
24 at those different places? 10:10:16

25 A. Yes, they really parallel the three branches of our 10:10:17

—Malackowski, J. - Direct—

1 division. 10:10:22

2 So I've taught on intellectual property valuation, 10:10:22
3 strategy, and monetization or investments. 10:10:25

4 MS. KOBIALKA: At this time, we'd like to tender 10:10:29
5 Mr. Malackowski as an expert in business and IP valuation and 10:10:32
6 patent licensing. 10:10:35

7 THE COURT: Is there any voir dire on his expertise, 10:10:38
8 Counsel? 10:10:43

9 MR. JAMESON: No, Your Honor, and no objection to 10:10:43
10 the tender. 10:10:45

11 THE COURT: All right. You may proceed. 10:10:46

12 MS. KOBIALKA: Thank you, Your Honor. 10:10:50

13 BY MS. KOBIALKA: 10:10:51

14 Q. If we could turn to slide 4, could you just explain here 10:10:52
15 what we're looking at? 10:10:55

16 A. Yes. Your Honor, this really lays out the steps, at a 10:10:57
17 high level, that I took in order to reach my conclusion. And 10:11:01
18 it's best described as looking at the life cycle of 10:11:04
19 Centripetal's innovation and the valuation creation. 10:11:08

20 So I looked at the baseline, where were things 10:11:11
21 before Centripetal, I focused on Centripetal's innovation, I 10:11:15
22 then looked at the impact to that from the alleged 10:11:19
23 infringement that we're dealing with in this case, and then, 10:11:24
24 finally, my real focus is, well, what happens from here? 10:11:26
25 What was the impact on the value of that innovation as a 10:11:29

—Malackowski, J. - Direct—

1 result of that.

10:11:33

2 Q. Could we start with the prior technology, sort of back up
3 here, and could you explain what you considered for that
4 portion?

10:11:34

10:11:39

10:11:41

5 A. Yes. So, really, this draws upon both my experience in
6 the industry through Solutionary but, importantly, the work
7 that I did in this case reviewing the documents and other
8 materials.

10:11:43

10:11:46

10:11:49

10:11:55

9 Q. And, if you could, talk a little bit about what you saw
10 with the traditional devices and technologies in the
11 Solutionary experience.

10:11:56

10:11:59

10:12:02

12 A. So, Your Honor, when I was at Solutionary, that company
13 started in 2000 through a group of professionals that used to
14 run a call center business; those annoying phone calls that
15 you would get over dinner asking to try to sell something --

10:12:04

10:12:10

10:12:13

10:12:17

16 THE COURT: I'm very familiar with those.

10:12:20

17 THE WITNESS: And the reason they felt they could
18 move into cyber security is because at the time the next big
19 thing was to -- instead of each company monitoring the
20 security issues themselves with their own CTO, is they would
21 monitor it remotely in what we call the securities operation
22 center, and then, if they saw anything suspicious, the call
23 center went into action, and they would call the company, the
24 executives, the CEO -- outbound telemarketing, essentially,
25 but it was outbound telesecurity service -- and we started a

10:12:22

10:12:25

10:12:28

10:12:31

10:12:35

10:12:39

10:12:43

10:12:47

10:12:52

—Malackowski, J. - Direct—

1 small business to do that, and it grew to being worth several 10:12:55
2 hundred million dollars. But that was early-stage security 10:13:00
3 technology. 10:13:04

4 BY MS. KOBIALKA: 10:13:05

5 Q. All right. If we could go to the next slide, what are we 10:13:05
6 seeing happen in the marketplace? 10:13:08

7 A. Well, we sold that business in 2013. And one of the 10:13:10
8 reasons we sold it is because we saw change coming, 10:13:14
9 significant change, in that the industry needed to adapt to 10:13:18
10 the increased activity in threat. 10:13:22

11 And what this slide talks about is that, ultimately, 10:13:25
12 that was recognized in 2015 by Gartner. That's the research 10:13:28
13 firm we've heard a fair bit about over this trial. But 10:13:33
14 Gartner marked 2015 as the change point in this industry, and 10:13:38
15 the focus was that, instead of a bunch of people watching 10:13:42
16 screens and picking up the phone, you need to have increased 10:13:45
17 use of analytics and then a behavior model to operationalize 10:13:48
18 the response. And that response had to be able to scale, not 10:13:53
19 through adding more people but through adding technology. 10:13:56

20 And at this trial I've heard conversations about 10:13:59
21 moving from a reactive to a proactive view of cyber security. 10:14:03
22 That's exactly what we saw coming, that's what Gartner 10:14:08
23 documented, and, in my view, that was the value, as we'll 10:14:13
24 talk about, of the Centripetal innovation. 10:14:17

25 Q. So let's take a look at what's been marked -- this is in 10:14:20

Malackowski, J. - Direct

1	Exhibit PTX-1600.	10:14:24
2	A. Yes.	10:14:32
3	MS. KOBIALKA: And, Your Honor, this is the only	10:14:33
4	exhibit we have, I think, in the book there for you.	10:14:35
5	THE COURT: Okay.	10:14:42
6	BY MS. KOBIALKA:	10:14:42
7	Q. Mr. Malackowski, is this the Gartner report that you were	10:14:42
8	just referring to?	10:14:48
9	A. It is.	10:14:49
10	Q. And what is the date of the report?	10:14:50
11	A. It is October 2015.	10:14:53
12	Q. And just briefly, what is this about? And who is	10:14:55
13	Gartner, too, as well, if you could explain that to give some	10:15:01
14	context.	10:15:04
15	A. So Gartner is the leading market research firm across a	10:15:04
16	number of industries but especially technology and,	10:15:09
17	specifically, security.	10:15:13
18	For example, when I was at Solutionary, we would	10:15:14
19	look at the Gartner reports as they came out to see if they	10:15:16
20	talked about us, how they mentioned us, and, hopefully, they	10:15:20
21	would recognize us. So they're sort of the gold standard for	10:15:23
22	the marketplace.	10:15:26
23	Q. And it's very comon -- is it very common for companies to	10:15:27
24	rely on Gartner for part of their business records and for	10:15:31
25	their business?	10:15:35

—Malackowski, J. - Direct—

1 A. You have to, because what Gartner says customers will 10:15:35
2 respond to and, in our case, investors respond to. 10:15:42

3 So we raised capital through a number of rounds over 10:15:45
4 those 13 years, and I don't think there was a meeting when 10:15:50
5 Gartner wasn't discussed, not because we raised it -- 10:15:53
6 sometimes we did -- but because investors asked about it; 10:15:56
7 wanted to know how we fit in with the trends that they were 10:15:59
8 predicting. 10:16:02

9 Q. Okay. If we could take a look at the paragraph here that 10:16:02
10 is highlighted -- oh, sorry. If we could go back. Yeah. 10:16:06

11 Could you just explain what in this informed your 10:16:09
12 opinions? 10:16:13

13 A. Well, this really sums up that transition I was speaking 10:16:13
14 of. It talks about, "product leaders need insights into 10:16:17
15 expansion of threat intelligence," and that, "these new 10:16:21
16 emerging capabilities will be instrumental to defining the 10:16:25
17 future," in the third line. 10:16:29

18 The document goes on to describe this transition in 10:16:33
19 detail, but that really crystalizes what was happening and, 10:16:37
20 frankly, what was expected to happen. 10:16:41

21 Q. I'd like to turn to Page 3 of this document. If we could 10:16:43
22 enlarge the top half -- 10:16:49

23 THE COURT: What's the Bates number on this? 10:16:51

24 MS. KOBIALKA: It ends in 753. 10:16:55

25 BY MS. KOBIALKA: 10:17:01

—Malackowski, J. - Direct—

1 Q. Mr. Malackowski, could you explain what we're looking at 10:17:02
2 here? 10:17:03

3 A. So this is a chart that I found in the course of my work, 10:17:03
4 and it really struck me because it described both the 10:17:07
5 experience I had and then the research or information I 10:17:11
6 gathered on Centripetal and Cisco. 10:17:15

7 So, Your Honor, this chart, this pyramid, describes 10:17:17
8 cyber security in four key stages or epics. They call it 10:17:22
9 "epics," as they describe, because these are not simple 10:17:27
10 incremental transitions in the market, these are fundamental 10:17:30
11 changes in the way the industry is responding. 10:17:33

12 The second box from the bottom that talks about 10:17:36
13 intelligence awareness, that was my experience from 20 to 10:17:38
14 2013. We were watching to see what happened, and then we 10:17:42
15 shared that response with the client. 10:17:45

16 But the doc that notes, we are here -- it's sort of 10:17:48
17 the end of 2015 -- really describes uniquely where 10:17:53
18 Centripetal was when they were entering the market, and they 10:17:56
19 were moving into that next epic stage of analytics and 10:17:59
20 modeling that was really behavioral modeling era of controls, 10:18:04
21 moving already towards that machine learning and adaptive 10:18:09
22 response. 10:18:14

23 So, in some ways, Centripetal was two generations 10:18:16
24 ahead of the market when they came out in 2014. 10:18:19

25 Q. Okay. And if we could look at the bottom half of this 10:18:21

—Malackowski, J. - Direct—

1 document and starting with "intelligence awareness" all the 10:18:25
2 way down, could you talk a little bit about what you found -- 10:18:29
3 well, informed your opinion from this? 10:18:33

4 A. Yes. Let's go to the third line. 10:18:36

5 What struck me about this paragraph was just the 10:18:37
6 recognition or the acknowledgment that a human response 10:18:40
7 cannot act or cannot react fast enough, and it compounded the 10:18:43
8 fact that there just aren't enough security practitioners. 10:18:48
9 So what we were doing, for example, at Solutionary was fine 10:18:52
10 for the time, but this is exactly the problem that we saw 10:18:56
11 and, frankly, the problem that Centripetal solved and that 10:19:00
12 I'll be talking about. 10:19:02

13 MS. KOBIALKA: At this time, Your Honor, we'd like 10:19:05
14 to move PTX-1600 into evidence. 10:19:06

15 THE COURT: PTX-1600 will be admitted. 10:19:12

16 (Plaintiff's Exhibit PTX-1600 was received in 10:19:15
17 evidence.) 10:19:16

18 MS. KOBIALKA: Thank you. 10:19:17

19 BY MS. KOBIALKA: 10:19:17

20 Q. So let's go back to the demonstrative. 10:19:18

21 So let's talk a little bit about Centripetal's 10:19:20
22 innovation in light of what we've just looked at. 10:19:23

23 A. So the phrase "operationalize threat intelligence" has 10:19:27
24 been discussed at length. I won't repeat it. But simply 10:19:32
25 very briefly, it came as a result of the fact that cyber 10:19:36

—Malackowski, J. - Direct—

1 security was becoming more a complex and difficult dynamic,
2 that conventional technologies couldn't meet the challenge,
3 and, importantly, that a next generation of sort of a simple
4 improvement wasn't going to be very successful.

5 They had to have something that was really
6 revolutionary, and so Centripetal solved that problem through
7 RuleGATE, and it was able to automatically collect and
8 process data, check that box, and it was able to stop attacks
9 before they were done, check that box. That essentially
10 capitalizes or crystalizes this notion of going from reactive
11 to proactive, and that's why it was so significant for the
12 company and, ultimately, for the market.

13 Q. What was some of the foundation that you had for your
14 opinions that you're going to provide that we talked about
15 earlier today?

16 A. The foundation was the work that I did in this case
17 specifically, substantial study, and, obviously, my
18 experience as an accountant, a licensing professional, and an
19 industry director.

20 Q. Okay. So let's turn to slide 7 here. Oh, we've seen
21 this. I'm sorry. Can we go to slide 8?

22 Can you describe your fact investigation, at a high
23 level, that you did?

24 A. A very high level. It's very similar to what the other
25 experts in this case have talked about. They've had a chance

Malackowski, J. - Direct

1 to review substantial documents. I've been under the
2 protective order, so I've been able to read the depositions
3 prior to the case, I've been able to see the testimony from
4 the beginning of this trial, and I've had access to the
5 expert reports.

6 The only thing I would add that maybe is somewhat
7 unique -- I did a fair bit of my own independent research to
8 validate what I was finding in the record of the case, and
9 that's very typical of my study.

10 Q. And did you speak with anybody, as well, for your
11 opinion?

12 A. Yes, in two ways. Directly, I spoke to Jonathan Rogers
13 and was able to interview him and ask any question I wanted,
14 frankly. Indirectly -- I call it interviewing, but I
15 submitted questions to you, and you were able to ask those
16 questions in depositions of the Cisco executives. So that's
17 the process.

18 Q. Let's take a look. We'll go to the next slide. Let's
19 take a look at some of the Cisco records you reviewed.

20 So this is an exhibit that's already in evidence, so
21 we -- if you could explain here, from PTX-995, what -- how
22 did this inform your opinion?

23 MR. JAMESON: Your Honor, I've got what I think is
24 going to be a major problem with this examination.

25 He's now just identified PTX-995 as a document that

—Malackowski, J. - Direct—

1 he's apparently going to rely on for his opinions. It's not 10:22:20
2 in the exhibit binder. It has not been provided to us. And, 10:22:25
3 in fact, there's only one exhibit that's in this witness's 10:22:31
4 exhibit binder, and so we're now being blindsided by 10:22:34
5 documents that he appears to rely on through the guise of a 10:22:38
6 demonstrative, and it's going to impact my ability to 10:22:45
7 cross-examine this witness. 10:22:48

8 THE COURT: Well, are the "terms" column set forth 10:22:49
9 on this exhibit in his report? 10:23:03

10 MS. KOBIALKA: Yes, Your Honor. 10:23:06

11 THE COURT: I'm not so much interested in whether 10:23:07
12 this particular diagram is in the report, but does he say in 10:23:11
13 his report -- does he refer to "ransomware" and "industry 10:23:15
14 average time" and "cloud," et cetera? Were these all in his 10:23:20
15 report? 10:23:24

16 MS. KOBIALKA: Yes, Your Honor. This is explicitly 10:23:25
17 cited in his report at Page 15, at Note 98. 10:23:27

18 THE COURT: "This is" -- what is "this"? 10:23:30

19 MS. KOBIALKA: "This" is just this document, 10:23:32
20 PTX-995, and the analysis contained throughout. This is all 10:23:37
21 part of his opinion. We did not mark it, just for time. We 10:23:40
22 were trying to get moved through this, since this is already 10:23:45
23 in evidence. 10:23:48

24 There's nothing -- 10:23:49

25 THE COURT: What do you mean it's already in 10:23:50

—Malackowski, J. - Direct—

1	evidence?	10:23:53
2	MS. KOBIALKA: PTX-995.	10:23:54
3	THE COURT: Is that already an exhibit?	10:23:55
4	MS. KOBIALKA: Yes.	10:23:57
5	THE COURT: All right. But you didn't put it in	10:23:59
6	your exhibit book as something you were going to use.	10:24:01
7	MS. KOBIALKA: We did not. This was -- we've been	10:24:04
8	using portions of exhibits that are already admitted.	10:24:08
9	THE COURT: All right. Well, where is this in his	10:24:12
10	report?	10:24:16
11	MS. KOBIALKA: In his report -- and we gave you a	10:24:17
12	copy of his report in the binder.	10:24:19
13	THE COURT: I know. What page is --	10:24:24
14	MS. KOBIALKA: Page 15, under the heading in his	10:24:27
15	report, "The Cyber Security Industry."	10:24:36
16	THE COURT: "Cyber Security Industry." Where does	10:24:40
17	it say that on Page 15?	10:24:43
18	MS. KOBIALKA: That's the heading.	10:24:45
19	THE COURT: Oh, at the top.	10:24:46
20	MS. KOBIALKA: Yes.	10:24:48
21	THE COURT: Well, I mean, are all of those things	10:24:54
22	mentioned on this page?	10:24:58
23	MS. KOBIALKA: Yes, Your Honor. In fact, it's	10:25:00
24	verbatim. If you'd like, I can read the very first sentence.	10:25:02
25	It refers to this very figure.	10:25:06

—Malackowski, J. - Direct—

1 THE COURT: What is this? Is this the white paper 10:25:14
2 from Centripetal? 10:25:17

3 MS. KOBIALKA: This is Cisco's security analytics 10:25:17
4 estimate that they had done -- that they expected in 2020. 10:25:25
5 And if you read -- I'll read verbatim from his report. 10:25:29

6 It says, "Roughly 200 billion innovative things, 10:25:33
7 devices, will have access to the Internet." That's -- citing 10:25:39
8 this document, that is part of -- 10:25:42

9 THE COURT: It says, "according to Centripetal's 10:25:46
10 white paper." Now, you said this was a Cisco document. 10:25:48

11 MS. KOBIALKA: Correct. The citation is the 10:25:52
12 sentence before that I'm referring to. 10:25:54

13 (There was a pause in the proceedings.) 10:26:14

14 THE COURT: What is that piece of paper? 10:26:25

15 THE CLERK: This is just my exhibit list. I was 10:26:27
16 just giving you the title of that exhibit. 10:26:29

17 THE COURT: Is that an exhibit list? 10:26:30

18 THE CLERK: Yes, sir. 10:26:31

19 THE COURT: It was furnished in this case? 10:26:32

20 THE CLERK: Yes, sir. 10:26:34

21 THE COURT: The objection is overruled. You may 10:26:36
22 proceed. 10:26:38

23 MR. JAMESON: Your Honor, please indulge me on this. 10:26:39

24 We just looked -- we just looked at Page 15 of his 10:26:44
25 report, and the only thing that I see on Page 15 that is 10:26:49

Malackowski, J. - Direct

1 reflected in this slide is a reference to "200 billion." I 10:26:54
2 have not memorized his expert report, but the -- 10:27:01

3 THE COURT: Well, this is on an exhibit list that 10:27:09
4 was supplied, according to my clerk. 10:27:12

5 MR. JAMESON: Your Honor, under the pretrial order, 10:27:17
6 they were supposed to identify the exhibits that they were 10:27:19
7 going to use with this witness, and the only one that was 10:27:22
8 identified -- 10:27:25

9 THE COURT: Right, they were supposed to furnish the 10:27:26
10 exhibits they were going to use with this witness, and they 10:27:31
11 didn't furnish this exhibit with this witness, but they can 10:27:34
12 refer to what's on the page. But they'll have to use this as 10:27:41
13 a demonstrative exhibit, instead of -- that's what I would 10:27:50
14 say, except it's already been admitted in evidence. I would 10:27:53
15 have said they would be confined to that, but it's already 10:27:58
16 been admitted -- 10:28:00

17 MR. JAMESON: Your Honor -- 10:28:01

18 THE COURT: -- with another witness. 10:28:02

19 MR. JAMESON: Your Honor, my point is when I look at 10:28:04
20 slide 9 -- and they said look at Page 15. It's all there. 10:28:09

21 For example, I see no reference to "11.5 billion 10:28:13
22 global ransomware damage costs." 10:28:18

23 THE COURT: Is that in the expert report, 11.5 10:28:23
24 billion? 10:28:31

25 MR. JAMESON: I don't know where it is. That's what 10:28:31

—Malackowski, J. - Direct—

1 I'm trying to figure out. I -- 10:28:33

2 MS. KOBIALKA: Your Honor, it's cited throughout his 10:28:38
3 report. There were other places in his report this is cited. 10:28:40
4 I'll give you another example. 10:28:44

5 On Page 37 of his report, it's explicitly cited as 10:28:46
6 footnote 314. Again, we quote verbatim from this document, 10:28:52
7 and we talk about how 80 percent of all Internet traffic will 10:28:57
8 be encrypted, the second bullet point on Page 37 of his 10:29:01
9 opening report. 10:29:10

10 We could keep doing this all day, but this was 10:29:13
11 clearly a part of his opinion. It's throughout his report. 10:29:15
12 This is an exhibit that was already admitted. We're merely 10:29:20
13 showing a portion of the document to align with what has been 10:29:23
14 disclosed to the other side, and they should be quite 10:29:27
15 familiar with his report at this point. 10:29:30

16 THE COURT: Well, Mr. Jameson, I would require that 10:29:33
17 they use this exhibit only as a demonstrative, except it's 10:29:43
18 already been admitted. And if the exhibit has already been 10:29:56
19 admitted, they can certainly question the witness on it, and 10:30:02
20 it appears that what is on -- I mean, the exhibit is already 10:30:06
21 in evidence. 10:30:11

22 Your objection is overruled. 10:30:13

23 MR. JAMESON: I understand that, Your Honor. 10:30:15

24 THE COURT: That's it. The Court has ruled. 10:30:16

25 Proceed. 10:30:22

—Malackowski, J. - Direct—

1	MS. KOBIALKA: Thank you, Your Honor.	10:30:22
2	BY MS. KOBIALKA:	10:30:23
3	Q. Mr. Malackowski, can you explain how this informs your	10:30:24
4	opinion?	10:30:27
5	A. Yes. This is the Cisco Security Analytics report that	10:30:28
6	we've been talking about, and this was prepared in 2018.	10:30:35
7	MS. KOBIALKA: Your Honor, it is a retrospective of	10:30:39
8	Cisco's description of why they have launched new products in	10:30:43
9	the market, and they cite, as we've just talked about, the	10:30:47
10	internet of things and the encrypted traffic as two of the	10:30:50
11	five reasons why they're moving in the direction that they	10:30:54
12	are.	10:30:57
13	THE COURT: All right. Now, this document, how was	10:30:57
14	it created?	10:31:02
15	THE WITNESS: This is created internally at Cisco by	10:31:02
16	their analytics team --	10:31:06
17	THE COURT: This document was obtained from Cisco?	10:31:08
18	THE WITNESS: Yes, sir.	10:31:11
19	THE COURT: All right. Well --	10:31:13
20	THE WITNESS: And the reason that I brought it out	10:31:16
21	of my report and highlight it here is a confirmation of what	10:31:18
22	we've talked about to this point, but also because I think	10:31:23
23	the date is significant, the 2018 date. Because at this	10:31:26
24	point, Your Honor, Cisco was claiming that they alone were	10:31:30
25	the only ones in the market who could address these concerns,	10:31:33

—Malackowski, J. - Direct—

1 and I'm going to come back and talk to you about how I 10:31:37
2 believe that had an impact on Centripetal. 10:31:40

3 THE COURT: Where is the date on this? 10:31:42

4 THE WITNESS: It's on the first page of the actual 10:31:44
5 exhibit, in the bottom left-hand corner. 10:31:48

6 THE COURT: Exhibit PTX-995? Well, that's not in 10:31:53
7 the book. 10:31:57

8 MS. KOBIALKA: We can pull up PTX-995 and show the 10:32:01
9 date. 10:32:04

10 THE COURT: All right. Well, do that. This is a 10:32:05
11 Cisco document that was previously admitted, right? 10:32:15

12 MS. KOBIALKA: Yes, Your Honor. 10:32:24

13 THE COURT: Okay. 10:32:26

14 BY MS. KOBIALKA: 10:32:30

15 Q. Okay. If we could go back to the demonstrative, I would 10:32:31
16 like to turn to slide 10. 10:32:33

17 Did you do any independent analysis to see whether 10:32:37
18 or not what we were seeing with the cyber security demand was 10:32:42
19 consistent with the Cisco document we just saw? 10:32:46

20 A. Yes. So in my -- 10:32:49

21 THE COURT: Has this exhibit been introduced? 10:32:51

22 MS. KOBIALKA: No, Your Honor. This is a 10:32:58
23 demonstrative summarizing his analysis that he has contained 10:33:00
24 in his report. 10:33:03

25 THE COURT: Well, it's marked as an exhibit, not a 10:33:04

—Malackowski, J. - Direct—

1 demonstrative. 10:33:11

2 MS. KOBIALKA: No, this is just referring to where 10:33:12
3 the information came from, but it's not intended to be an 10:33:13
4 exhibit. It was just a demonstrative. 10:33:18

5 THE COURT: Well, I mean, I can understand the 10:33:26
6 reason the Court overruled the objection. One of the reasons 10:33:33
7 the Court overruled the objection to the last exhibit was 10:33:38
8 that it was a Cisco document which had already been 10:33:45
9 introduced in evidence. This is not a Cisco document. This 10:33:49
10 is something that the witness made up, is it? 10:33:52

11 MS. KOBIALKA: Yes, this is a demonstrative of his 10:33:57
12 opinions. 10:34:00

13 THE COURT: Well, it's not an exhibit. 10:34:01

14 MS. KOBIALKA: Correct. 10:34:03

15 THE COURT: What is your agreement as to 10:34:04
16 demonstratives? Are they supposed to be exchanged? 10:34:06

17 MS. KOBIALKA: No. The parties agreed not to 10:34:09
18 exchange demonstratives. 10:34:11

19 THE COURT: Okay. Well, this is a demonstrative 10:34:13
20 exhibit, but it's not going to be an exhibit in the case. 10:34:17

21 MS. KOBIALKA: That's correct, Your Honor. 10:34:23

22 THE COURT: Because if you were going to use it for 10:34:24
23 that purpose, you have to put it in your book, which you 10:34:26
24 didn't. You didn't put the last one in, but that was a Cisco 10:34:30
25 document that had already been admitted in evidence. This is 10:34:35

—Malackowski, J. - Direct—

1 not a Cisco document, so you can use it only as a 10:34:38
2 demonstrative, for whatever it's worth. "HACK fund versus 10:34:43
3 the S&P Index" -- go ahead. 10:34:50

4 BY MS. KOBIALKA: 10:34:53

5 Q. Mr. Malackowski, can you explain what your independent 10:34:54
6 analysis showed? 10:34:56

7 A. Yes, Your Honor. And it is just meant to be a 10:34:59
8 demonstrative of the market data that I include in my report. 10:35:03

9 So I studied this period of 2017 through 2019 as the 10:35:07
10 critical period for my evaluation analysis, and I saw 10:35:12
11 documents like the one that we just reviewed, where Cisco was 10:35:15
12 very bullish on the potential for these technologies in the 10:35:20
13 market. What I wanted to do was to check that to see if 10:35:24
14 others concurred, and given our experience as an investment 10:35:28
15 banker, the way that we do that is we look to the 10:35:32
16 marketplace. 10:35:35

17 And so, specifically, I was able to compare the 10:35:37
18 expectations for the stock market overall, the S&P 500, to 10:35:39
19 the expectations for a specialized fund that I talk about in 10:35:45
20 my report, called the HACK fund, because it relates to cyber 10:35:49
21 security or the hack threat. It's a collection of 55 10:35:54
22 companies that are generally in the cyber security industry, 10:35:56
23 but it includes Cisco, and Cisco is the largest member of the 10:35:59
24 HACK fund. And what it confirmed for me is that Cisco was 10:36:05
25 not alone in their recognition of this transition in the 10:36:08

—Malackowski, J. - Direct—

1 industry, but the market was generally recognizing the 10:36:11
2 importance of cyber security today more than historically. 10:36:15

3 THE COURT: All right. 10:36:15

4 BY MS. KOBIALKA: 10:36:20

5 Q. If we could go to the next slide in your demonstrative, 10:36:20
6 could you explain, then, what else you considered for your 10:36:26
7 opinion? 10:36:30

8 A. So at this point I'm bringing that background, those 10:36:30
9 expectations, to my study of Centripetal's technology 10:36:34
10 specifically. And I looked at Centripetal's adoption, the 10:36:39
11 investment that they were making, whether or not they were 10:36:44
12 receiving recognition from the market or otherwise, and then 10:36:46
13 what options they had as a result of their intellectual 10:36:50
14 property development. 10:36:55

15 Q. If we could go to the next slide, did you consider a 10:36:55
16 timeline for framing all of your analysis? 10:36:58

17 A. I did. Consistent with most of my projects, one of the 10:37:01
18 first things I will do with my team is I'll take the 10:37:06
19 documents of note in the case, and I put them in 10:37:10
20 chronological order. And the reason I do that is to 10:37:13
21 understand generally what happened, not only when, but 10:37:17
22 relative to others in the market. 10:37:21

23 And so, Your Honor, what this chart shows is events 10:37:23
24 related to Centripetal, on the top half of the chart, and 10:37:26
25 events related to Cisco or the conversations between Cisco 10:37:31

—Malackowski, J. - Direct—

1 and Centripetal, on the bottom half of the chart. And I 10:37:35
2 won't go into great detail now, but one of the conclusions 10:37:38
3 that this led me to is a simple one; that Centripetal was 10:37:42
4 first as with respect to the technologies that are at issue, 10:37:47
5 that they were in the market with the solutions first. 10:37:52

6 Q. Okay. If we could go to the -- 10:37:55

7 THE COURT: Who was first? 10:38:00

8 THE WITNESS: Centripetal, Your Honor. 10:38:00

9 BY MS. KOBIALKA: 10:38:06

10 Q. So the next demonstrative slide, could you explain how 10:38:07
11 Centripetal's investment informed your opinion? 10:38:10

12 A. So as a valuation expert, I wanted to understand what was 10:38:11
13 it that allowed Centripetal to be first to market, and in my 10:38:16
14 interviews with Mr. Rogers, Mr. Jonathan Rogers, he talked 10:38:21
15 about the extensive investment that they had made into the 10:38:27
16 technology. 10:38:29

17 And as a CPA by training, I wanted to verify that 10:38:30
18 investment and understand what the components were and when 10:38:33
19 it occurred. And so what this chart shows, which comes out 10:38:37
20 of my report -- it's simply a reflection of the R & D 10:38:41
21 expenses and the supporting operational expenses that 10:38:46
22 Centripetal incurred through the last data that I had, which 10:38:49
23 was about a year old at this point. 10:38:54

24 And you can see that's \$45 million, but that doesn't 10:38:56
25 include all the costs. There are litigation costs, which I 10:39:00

—Malackowski, J. - Direct—

1 excluded from my analysis, which you would add to this chart. 10:39:03

2 THE COURT: What do you mean "mitigation costs"? 10:39:08

3 THE WITNESS: Litigation costs. 10:39:11

4 THE COURT: Oh, "litigation." I'm sorry. 10:39:13

5 BY MS. KOBIALKA: 10:39:16

6 Q. If we could go to the next demonstrative slide, are these 10:39:17
7 the costs that you had quantified? 10:39:21

8 A. Yes. These are the litigation costs specifically for 10:39:23
9 Keysight and the Cisco litigation, and I totaled those so 10:39:27
10 that I can reconcile the accounting numbers I found against 10:39:31
11 my interviews with Mr. Jonathan Rogers. 10:39:35

12 MR. JAMESON: Your Honor, I'm going to renew an 10:39:40
13 objection. I can't find this in his report, and I just don't 10:39:41
14 know where this is coming from. 10:39:46

15 And there's no -- I have no basis to know where he's 10:39:47
16 going, and I don't know where this is in his report, and I'm 10:39:52
17 trying to find it. I couldn't find the last demonstrative 10:39:55
18 evidence, as well. 10:39:59

19 MS. KOBIALKA: It's cited on Page 23 of his report. 10:40:01
20 It explicitly -- and I can quote directly -- 10:40:06

21 THE COURT: Well, is Counsel correct when she 10:40:12
22 reported to me that you did not agree to exchange 10:40:14
23 demonstrative exhibits? Is that correct, Mr. Jameson? 10:40:18

24 MR. JAMESON: Your Honor, we agreed to not exchange 10:40:25
25 demonstratives. My point is that the evidence that 10:40:30

—Malackowski, J. - Direct—

1 Mr. Malackowski is providing orally -- I'm trying to find 10:40:33
2 where it is in his report, and I can't find it. 10:40:37

3 THE COURT: Where did you say it was, Ms. Kobialka? 10:40:40

4 MS. KOBIALKA: So if we could go to Page 23 of his 10:40:46
5 opening report, and you read the second sentence -- I'll 10:40:54
6 quote: 10:41:02

7 "As Jonathan Rogers, Centripetal's VP of Operations, 10:41:03
8 testified, Centripetal spent approximately 60 million in 10:41:07
9 research and development since the founding of the 10:41:12
10 company..." and it continues on. He cites -- 10:41:16

11 THE COURT: I'm looking at the wrong report. I 10:41:20
12 thought I had the first one. 10:41:24

13 Where are you on -- wait a minute. I've got 10:41:27
14 Page 24. I thought I had 23. Excuse me. 10:41:36

15 Page 23. 40 million, 60 million, 40 million -- 10:41:43
16 where do you get to the litigation costs? 10:41:50

17 MS. KOBIALKA: So that is contained within the 10:41:53
18 citations at footnote 193. He did a breakdown of the 10:41:58
19 financials, in addition to relying on some of this testimony. 10:42:15
20 Those were part of the documents that he reviewed. 10:42:21

21 And if you continue on -- 10:42:24

22 THE COURT: Well, wait a minute. I don't see -- 10:42:27
23 where does it say 11.5 million on research? 10:42:30

24 MS. KOBIALKA: That's all part of it. 10:42:35

25 THE COURT: "All part of it." Where does it say it? 10:42:37

—Malackowski, J. - Direct—

1	MS. KOBIALKA: It doesn't say 11.5 million in	10:42:41
2	research.	10:42:43
3	THE COURT: Well, what does it say? It says	10:42:44
4	40 million and 50 million.	10:42:48
5	MS. KOBIALKA: And then, if you continue on, he	10:42:52
6	explains the revenues and the revenue analysis that the	10:42:54
7	company had.	10:42:59
8	THE COURT: Where are you reading from?	10:43:00
9	MS. KOBIALKA: I'm reading from Page 23.	10:43:02
10	THE COURT: Where on Page 23?	10:43:04
11	MS. KOBIALKA: So I started with what is cited for	10:43:07
12	footnote 193. There's an entire sentence here --	10:43:13
13	THE COURT: Are you reading footnote 193? Is that	10:43:17
14	what you're reading?	10:43:20
15	MS. KOBIALKA: No, the sentence that is citing to	10:43:21
16	footnote 193. It is the second sentence, and I can read the	10:43:24
17	whole sentence.	10:43:27
18	THE COURT: "Investment capital..." (reading).	10:43:29
19	I don't see anything in there. I don't see a	10:43:41
20	number, and I don't see anything about litigation costs. Can	10:43:43
21	you tell me where it says "litigation costs"?	10:43:51
22	MS. KOBIALKA: He doesn't have a number --	10:43:54
23	THE COURT: Okay. Well, then he didn't say it. Why	10:43:56
24	don't you just admit that, instead of wasting the Court's	10:43:58
25	time?	10:44:03

—Malackowski, J. - Direct—

1 MS. KOBIALKA: The objection was to both slides. 10:44:03

2 THE COURT: All right. He didn't mention it. Ditch 10:44:07

3 that slide and move on. And the next time this happens, 10:44:11

4 don't try to waste the Court's time like that. 10:44:14

5 MS. KOBIALKA: Okay. I'd like to turn to slide 15. 10:44:24

6 BY MS. KOBIALKA: 10:44:28

7 Q. So, Mr. Malackowski, can you explain -- because you 10:44:32

8 mentioned Centripetal's technology had recognized value. 10:44:38

9 Can you explain how that informed your opinion? 10:44:41

10 A. Very briefly. We have seen others testify as to the 10:44:43

11 awards that Centripetal has received. They're listed on the 10:44:47

12 screen. 10:44:51

13 Important from my perspective was, again, the 10:44:52

14 chronology that early on Centripetal was recognized through 10:44:54

15 research grants, in 2011; that as soon as they entered the 10:44:59

16 market in 2014, they were considered a company to watch; and 10:45:04

17 then, importantly, after they displayed their technology at 10:45:08

18 the Cisco Live event, for which they were also recognized, 10:45:14

19 they began to win industry response as an innovator, a "Cool 10:45:16

20 Vendor," and as a highest performance solution. 10:45:22

21 So what I really take is not just the fact that they 10:45:25

22 were recognized, but when they were recognized, relative to 10:45:28

23 their launch into the market. 10:45:32

24 Q. And if we could go to the next demonstrative slide, can 10:45:34

25 you explain here, then, what Centripetal's pre-infringement 10:45:39

Malackowski, J. - Direct

1 IP options were?

10:45:44

2 A. So at the time that Centripetal went to market with their
3 technology, they basically had all of the options that I
4 would teach in my class, which is, first, they had the option
5 to practice the technology for themselves. That was their
6 desired option at the time.

10:45:45

10:45:47

10:45:51

10:45:55

10:46:00

7 If you go down, secondly, they had the option to
8 license it to others. That creates a shared value
9 proposition, so that may or may not be desirable. It's
10 case-specific.

10:46:01

10:46:05

10:46:08

10:46:13

11 Third, back up at the top, they had the option to
12 sell the patents or the technology. That would result in a
13 discounted value, because the buyer would have to then
14 capture profits in a return.

10:46:13

10:46:18

10:46:21

10:46:24

15 And then, finally, they could use the intellectual
16 property for collateral, if they wanted to raise additional
17 investment capital.

10:46:26

10:46:28

10:46:31

18 Importantly, from my perspective, is all of these
19 options were on the table to Centripetal at the time they
20 entered the market.

10:46:33

10:46:35

10:46:37

21 Q. Now, did Cisco have the same kind of options with respect
22 to -- well, what kind of options did Cisco have with regard
23 to the technology at issue?

10:46:38

10:46:44

10:46:49

24 A. They did not have the same options. They did not have an
25 alternative identified solution to what Centripetal was

10:46:50

10:46:54

Malackowski, J. - Direct

1 doing.

10:46:57

2 Q. Okay. Did you rely on Dr. Mitzenmacher and Dr. Cole to
3 come to that conclusion for your opinion?

10:46:57

10:47:03

4 A. In part, yes, I did.

10:47:06

5 Q. If we could go to the next slide.

10:47:08

6 If you could explain, then, here how that informed
7 your opinion.

10:47:10

10:47:13

8 A. So in my opinion, based upon my work, there were no
9 alternative available to the market to solve this problem,
10 other than Centripetal. There were no available
11 technologies. Cisco did not suggest or offer any
12 alternatives or even what it would cost to come up with
13 alternatives.

10:47:13

10:47:17

10:47:21

10:47:24

10:47:28

10:47:31

14 Obviously, we're still in this litigation after a
15 number of years, and when I studied the Keysight agreement,
16 my conclusion was they, too, had no alternative.

10:47:32

10:47:34

10:47:37

17 THE COURT: When you studied the Keysight
18 agreement -- what?

10:47:41

10:47:44

19 THE WITNESS: The Keysight agreement, which we'll
20 talk about in a moment further, leads me to the conclusion
21 that Keysight did not have a ready alternative to the
22 Centripetal technology, and that was, in part, why they took
23 a future but limited-term license.

10:47:44

10:47:47

10:47:50

10:47:54

10:47:58

24 MS. KOBIALKA: May I continue?

10:48:08

25 THE COURT: You said "limited-term." I was

10:48:10

—Malackowski, J. - Direct—

1 wondering why the license -- well, Keysight expired, what, 10:48:13
2 after two-and-a-half years? The patent lasted considerably 10:48:19
3 longer than that. 10:48:26

4 THE WITNESS: It did, Your Honor. 10:48:27

5 THE COURT: The limited-term license, what effect 10:48:28
6 did that have on your valuation? 10:48:34

7 THE WITNESS: So that's something that I focused on 10:48:35
8 very specifically, and I can address it now. 10:48:37

9 I've seen thousands of license agreements in my 10:48:39
10 term; that's what I do. There are very few, a handful, that 10:48:43
11 I've seen that have that provision that the Keysight 10:48:48
12 agreement does, which is a limited-term license with minimums 10:48:51
13 and maximums. 10:48:57

14 And when we would talk about such a thing in class, 10:48:58
15 that's indicative of a need to allow the licensee -- in this 10:49:03
16 case Keysight -- to transition the technology to find another 10:49:08
17 solution without impacting customers by removing the solution 10:49:12
18 immediately, because they didn't have a ready replacement. 10:49:17
19 And so that, to me, was confirming that not only did Cisco 10:49:20
20 not have an alternative to go to, but others in the market, 10:49:24
21 Keysight being an example, did not as well. 10:49:28

22 THE COURT: Well, in what way do you believe that 10:49:31
23 that impacted the entire computation of the royalty, if you 10:49:42
24 have -- if you've expressed such an opinion? I don't know if 10:49:50
25 you've expressed any such opinion, except for the limited 10:49:53

—Malackowski, J. - Direct—

1 term. Is that the only thing in your report that you cited? 10:49:59

2 THE WITNESS: So my focus in the report is on that 10:50:02
3 term issue, because it relates to the value question. 10:50:04

4 In my deposition I was asked questions that really 10:50:07
5 relate to Mr. Gunderson's work and opinion, and so I had 10:50:10
6 views on that, obviously, but that's not the focus of my... 10:50:14

7 THE COURT: All right. Well, let's move on, then. 10:50:17

8 BY MS. KOBIALKA: 10:50:20

9 Q. Okay. If we could go to the next slide, explain now 10:50:20
10 where we are with your analysis. 10:50:25

11 A. So we're getting close to the end. So I recognized 10:50:29
12 Centripetal's innovation as being that next generation or two 10:50:34
13 of technology. They got there because they invested in it, 10:50:38
14 they were recognized for it, and because they did, 10:50:41
15 quote/unquote, the expected thing of filing patents and 10:50:44
16 disclosing that publicly, in exchange for that monopoly 10:50:48
17 right, they had a number of options. 10:50:53

18 So now I'm looking to understand what did the 10:50:55
19 alleged infringement do to Centripetal as a business, in 10:50:57
20 particular, as it ultimately relates to their value going 10:51:00
21 forward. So there I looked at Cisco's adoption, Cisco's 10:51:04
22 promotion, the profits Cisco did or didn't realize, and the 10:51:07
23 impact that they had on others in the industry. 10:51:11

24 Q. If we could go to the next slide, can you explain here 10:51:13
25 what Cisco's strategy was and how it informed your opinion? 10:51:22

—Malackowski, J. - Direct—

1 A. Cisco describes their strategy very directly in their 10:51:26
2 security filing, and, in particular, as I cite at the top of 10:51:29
3 this demonstrative, their strategy is focused on delivering 10:51:33
4 effective cyber security architecture through combinations of 10:51:37
5 technology. 10:51:41

6 And so with that guidance, Your Honor, I went and 10:51:41
7 studied the acquisitions that Cisco made, as well as the 10:51:45
8 asserted infringement in this case. On the left side of the 10:51:50
9 chart, you can see the 2013 acquisition of Sourcefire for 10:51:54
10 2.7 billion, the 2014 acquisition of ThreatGRID, the 2015 10:51:58
11 acquisition of Lancope for 435 million. These were large 10:52:02
12 existing businesses with substantial revenues and customers 10:52:08
13 that were being added to Cisco, and then, of course, we've 10:52:12
14 got the asserted misappropriation of the Centripetal 10:52:15
15 technology. 10:52:18

16 And then we can see, as we look at the patents at 10:52:19
17 issue in this case, that the Centripetal technology actually 10:52:22
18 covers the combination of many of the things that Cisco 10:52:26
19 acquired. So on a continuum from a smaller firm that 10:52:30
20 innovates by themselves in the lab and files patents to the 10:52:35
21 other continuum of a larger firm that uses its resources to 10:52:40
22 make acquisitions and put things together, you can see that 10:52:43
23 these companies had very different strategies. 10:52:47

24 Q. If you turn to the next demonstrative slide, can you put 10:52:51
25 that within your timeline here? 10:52:54

—Malackowski, J. - Direct—

1 A. So with that background, I go back to -- 10:52:55

2 THE COURT: We've seen this one before. 10:52:58

3 THE WITNESS: We have, Your Honor, and this time I'm 10:53:00
4 simply focusing on that the activity of Cisco, again, comes 10:53:03
5 relatively late in the period vis-a-vis Centripetal, as it 10:53:07
6 relates to these technologies, and I try to show where the 10:53:11
7 acquisitions are made and then how, after or concurrent with 10:53:14
8 those last acquisitions, the discussions between Cisco and 10:53:18
9 Centripetal are active, ultimately leading to the accused 10:53:22
10 infringement. 10:53:28

11 BY MS. KOBIALKA: 10:53:29

12 Q. And did you see documentation in which Cisco made use of 10:53:29
13 this technology with respect to its marketing and what it did 10:53:36
14 in the marketplace? 10:53:39

15 A. Yes, I have, and that's been talked about somewhat 10:53:40
16 extensively during this trial, including with Mr. Gunderson. 10:53:44
17 A lot of the witnesses have shown the headlines, and so I 10:53:47
18 looked at that, obviously, and I also dug into the documents 10:53:51
19 behind the headlines. 10:53:56

20 Q. Did you see anything that, in particular, came to mind 10:53:57
21 with respect to those statements? 10:54:03

22 A. Yes. The last witness, Mr. Gunderson, put up a 10:54:05
23 demonstrative where he showed four different headlines 10:54:12
24 related to press releases and other marketing materials 10:54:16
25 describing Cisco's presentation of these technologies as a 10:54:18

—Malackowski, J. - Direct—

1 new era, as revolutionary. And that's fine; we've heard
2 that.

3 But when I dug further, what I found was they were
4 also describing it as Cisco being the only one who could
5 provide these solutions, and so that struck me, because from
6 as early as, you know, 2017, through as late as 2018, the
7 document that we talked about earlier, Cisco was claiming to
8 the industry that they alone were able to provide these
9 solutions, which in my view had significant impact on
10 Centripetal's ability to defend their first-mover advantage.

11 Q. And is that first-mover advantage important for a company
12 like Centripetal?

13 A. It's critical. As an executive or as an investor, to be
14 recognized as Centripetal was early -- and I referred you to
15 those recognitions and awards a moment ago -- was critical to
16 their ability to capture customers and to capture further
17 investment so they could scale. And if when they called on
18 those accounts and those investors the market believed that
19 it wasn't Centripetal that was the innovator but Cisco was
20 the innovator, I can tell you as an investor that that's a
21 problem.

22 Q. Okay. Now, did you see evidence of how Cisco was able to
23 capitalize on being -- you know, taking the claim to being
24 the first to market? And we can turn to slide 24.

25 A. Yes. In my analysis to my report, I again put my

—Malackowski, J. - Direct—

1 accounting hat back on, and I went to understand, if the 10:56:02
2 claims that Cisco was making turned out to be true, that they 10:56:07
3 were being successful with them. 10:56:13

4 So, Your Honor, what this data shows is two sets of 10:56:16
5 information. The top two lines are revenue data for Cisco 10:56:19
6 overall, both for its security products and its total 10:56:25
7 products, and the bottom two lines relate to the products 10:56:30
8 that are accused in this case. I think some of this was 10:56:35
9 generally discussed with Mr. Gunderson, about the rate of 10:56:38
10 growth. 10:56:41

11 And what this chart clearly shows is whereas Cisco 10:56:42
12 products overall were growing by 5 to 16 percent, which is 10:56:47
13 good, the accused security products were growing much, much 10:56:52
14 quicker. And that was, in part, because these products were 10:56:56
15 being introduced at the time, so more products were coming 10:56:58
16 into market, but in the end they represented 7.5 billion out 10:57:01
17 of 36 billion. So not only were they growing rapidly, they 10:57:06
18 were a meaningful part of Cisco's result. 10:57:11

19 Q. Now, let's turn to the next demonstrative slide. You had 10:57:16
20 discussed something called "me-too followers." Can you 10:57:20
21 explain what you were referring to there? 10:57:24

22 A. When I interviewed Mr. Jonathan Rogers, one of the things 10:57:26
23 that I noted is his explanation of how the alleged 10:57:29
24 infringement in this case not only affected his business 10:57:34
25 because of Cisco's revenue, but affected his business because 10:57:37

—Malackowski, J. - Direct—

1 Cisco is the largest player in cyber security. They're 10:57:43
2 approximately 50 billion in annual revenue, number 1 in the 10:57:45
3 HACK index. 10:57:52

4 And as Cisco goes, so goes the industry, so 10:57:54
5 Mr. Rogers talked about -- first it is Keysight, but then it 10:57:58
6 is Juniper and Palo Alto, who have entered the market seeking 10:58:01
7 to compete with Cisco and emulate their messaging. And so 10:58:06
8 when he told me that, I went back to the securities reports 10:58:08
9 and was able to confirm that those are indeed competitors, 10:58:13
10 and, indeed, Cisco was having that effect on Centripetal. 10:58:14

11 Q. If we could turn to the next demonstrative slide, what is 10:58:18
12 the final element of your analysis? 10:58:21

13 A. So the final -- the most important point, frankly, is how 10:58:23
14 does all this affect Centripetal from here? And in my 10:58:27
15 opinion, it's permanent loss of value. They've been 10:58:31
16 thwarted. They've lost control. They've done licensing, but 10:58:36
17 it's been through enforcement, and they've lost value into 10:58:40
18 the future that they will not be able to reclaim. 10:58:44

19 MS. KOBIALKA: Your Honor, at this time I'd like to 10:58:46
20 briefly seal the courtroom, because we will be talking about 10:58:49
21 the Keysight agreement. 10:58:52

22 THE COURT: All right. 10:58:54

23 (Confidential testimony from Page 1609, Line 23,
24 through Page 1611, Line 17, was redacted.)

25 * * * * *

Malackowski, J. - Direct

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15 (Confidential testimony from Page 1609, Line 23,
16 through Page 1611, Line 17, was redacted.)

17 * * * * *

18 BY MS. KOBIALKA:

11:01:27

19 Q. And if you can take the slide down, we'd like to go to
20 slide 30.

11:01:27

11:01:30

21 So this is, I think, the last point on -- I have a
22 different slide 30. I'm sorry. It's the slide before.

11:01:32

11:01:42

23 Thank you. Yes.

11:01:45

24 So on the last point, you talked about the loss of
25 value. Can you explain now what your analysis was as it

11:01:46

11:01:48

Malackowski, J. - Direct

1 relates to this element?

11:01:53

2 A. Yes. And this is the penultimate chart, so we're pretty
3 much done.

11:01:54

11:02:00

4 But, basically, this summarizes my conclusion, Your
5 Honor, as to why I believe that there's been a permanent loss
6 of value. I started by looking at the options Centripetal
7 had pre-infringement, outstanding board of directors, first
8 to operationalize threat intelligence, products in the
9 market, ecosystem partners, industry recognition, and
10 exclusivity. They had exclusivity because of the bargain
11 they struck with the Patent Office.

11:02:00

11:02:04

11:02:06

11:02:09

11:02:12

11:02:16

11:02:20

11:02:23

12 But post-infringement they now are in the market
13 competing against their own technology. There are new
14 competitors who are seeking to emulate that because of
15 Cisco's scale in the market. They've lost that reputation of
16 being the first mover or, certainly, the leader. And they do
17 not have the same ability to grow their business, both in the
18 market or through investment, because they no longer have
19 that exclusive right.

11:02:25

11:02:29

11:02:32

11:02:35

11:02:39

11:02:42

11:02:45

11:02:48

20 So their capacity to lead this new epic of
21 operationalized or proactive security response has been
22 thwarted permanently.

11:02:50

11:02:55

11:03:00

23 Q. Is there any way to quantify that?

11:03:04

24 A. No, there's really no way to make a calculation to make
25 them whole for that. The Gunderson analysis does not

11:03:09

11:03:12

—Malackowski, J. - Cross—

1 consider that. It's what we would call irreparable harm. 11:03:16

2 Q. Okay. If we could turn, then, to the last slide, could 11:03:21

3 you just now summarize your opinion? 11:03:24

4 A. Yes. So the opinions I reached are, not surprisingly, 11:03:26

5 consistent with the business I run. The first opinion is a 11:03:31

6 valuation opinion, and my view was that the evidence is that 11:03:35

7 the Centripetal patents had value. 11:03:37

8 The second opinion is a strategy-focused opinion; 11:03:40

9 that at the time of pre-infringement, Centripetal had all of 11:03:43

10 its options available. The innovators' return was available 11:03:48

11 to them. 11:03:52

12 And the third is an investor opinion that that's 11:03:53

13 gone, and it's not coming back. 11:03:57

14 MS. KOBIALKA: I don't have any further questions at 11:04:00

15 this time. I pass the witness. 11:04:02

16 THE COURT: All right. Counsel, you may 11:04:08

17 cross-examine. 11:04:13

18 MR. JAMESON: Thank you, Your Honor. 11:04:15

19 CROSS-EXAMINATION 11:04:25

20 BY MR. JAMESON: 11:04:25

21 Q. Good morning, Mr. Malackowski. 11:04:25

22 THE COURT: Wait a minute. Let me get the binder. 11:04:28

23 There's only one exhibit. 11:04:31

24 MR. JAMESON: Your Honor, we should have had a 11:04:33

25 supplemental exhibit delivered to the Court this morning. 11:04:36

Malackowski, J. - Cross

1	THE CLERK: It was.	11:04:39
2	THE COURT: I have it. I said there was only one in	11:04:40
3	the direct exam.	11:04:43
4	MR. JAMESON: Thank you.	11:04:46
5	THE COURT: That's what I was referring to.	11:04:48
6	MS. KOBIALKA: And I want to make sure you sent the	11:04:52
7	e-mail to us, because we haven't received anything yet in	11:04:54
8	terms of the cross-examination.	11:04:57
9	MR. JAMESON: It has been sent.	11:04:59
10	May I proceed, Your Honor?	11:05:01
11	THE COURT: Well, if it's been sent, where is it?	11:05:06
12	Who's got it?	11:05:11
13	MR. JAMESON: It was just sent to Centripetal. I	11:05:11
14	mean, it could be that the Internet speed is not moving as	11:05:17
15	fast as we would like today, but it has been sent.	11:05:20
16	THE COURT: Did you encrypt it?	11:05:25
17	MS. KOBIALKA: It may be undecipherable by the time	11:05:31
18	we get it, right?	11:05:35
19	MR. JAMESON: Possibly.	11:05:36
20	MS. KOBIALKA: Go ahead and start. If it becomes an	11:05:42
21	issue, I'll raise it. We still haven't received it, but	11:05:44
22	that's fine.	11:05:47
23	THE COURT: All right. Well, I don't know where you	11:05:48
24	are. They said they sent it to Centripetal. I don't know if	11:05:51
25	that's where you are or not.	11:05:53

—Malackowski, J. - Cross—

1 MR. JAMESON: You know what? Why don't we start, if 11:05:58
2 we can, Your Honor, by closing the courtroom and pulling back 11:06:02
3 up slide 28 that was used by Mr. Malackowski. And I would 11:06:07
4 ask that Centripetal display that for the witness, please. 11:06:13

5 THE COURT: Slide 28. Okay. 11:06:20

6 (Confidential testimony from Page 1615, Line 6,
7 through Page 1617, Line 7, was redacted.)

8 * * * * *

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

Malackowski, J. - Cross

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

(Confidential testimony from Page 1615, Line 6,
through Page 1617, Line 7, was redacted.)

* * * * *

BY MR. JAMESON:

Q. And I believe you testified that this document by Gartner
was created in 2015, right?

A. It was published October 30, 2015, yes, sir.

Q. And everyone in the industry -- not everyone. Most
companies in the world view Gartner as the gold standard for
where the market is headed, right?

A. Certainly. I would agree with that.

Q. And so the market reads what Gartner publishes, and they
basically go in the direction that Gartner suggests.

A. Well, they certainly contemplate the direction. Often
they'll read what Gartner suggests and many of them will say,
well, that sounds great, but I can't do that; I don't know
how to do that. So they're projecting, in some cases,
10-plus years out.

Q. But Gartner was stating in 2015 that the market is moving
in this direction of relying on automated threat
intelligence, and security is a growing market for all

11:09:28

11:09:28

11:09:28

11:09:35

11:09:39

11:09:43

11:09:50

11:09:54

11:09:56

11:09:59

11:10:04

11:10:06

11:10:11

11:10:15

11:10:18

11:10:23

11:10:24

11:10:35

11:10:40

Malackowski, J. - Cross

1 concerned, right? 11:10:44

2 A. Generally, yes, and I'll note they specifically cite 11:10:44
3 Centripetal in this report. 11:10:50

4 Q. You do not know if they cite Centripetal? 11:10:51

5 A. No, I do know. They do. 11:10:53

6 Q. And, in fact, over the last three or four years, the 11:10:55
7 market has increased their network security offerings, just 11:11:00
8 as Gartner predicted. 11:11:05

9 A. The demand has risen, just as Gartner predicted. The 11:11:06
10 technologies have evolved largely along the lines that we've 11:11:11
11 been talking about the last two weeks. 11:11:14

12 Q. And when demand rises, market leaders usually take 11:11:15
13 advantage of that demand and increase their sales, right? 11:11:22

14 A. If they have the technology. There's demand for a 11:11:26
15 million-mile electric car, but you can't go buy it, because 11:11:30
16 the technology doesn't exist. 11:11:34

17 Q. And if we would take a look at -- 11:11:35

18 MR. JAMESON: And, Your Honor, this is -- I think 11:11:40
19 the whole document was admitted into evidence. If we could 11:11:42
20 turn to Bates 759... 11:11:46

21 THE COURT: I don't believe the whole document was 11:12:04
22 admitted. 11:12:10

23 MR. JAMESON: Okay. I've got the same document in 11:12:10
24 our binder, Your Honor. It's 1600 in our binder. 11:12:13

25 THE COURT: 1600? 11:12:24

—Malackowski, J. - Cross—

1	MR. JAMESON: PTX-1600 in our binder, and I --	11:12:25
2	THE COURT: Yeah, I have it.	11:12:33
3	MR. JAMESON: I wanted to turn to Bates 759.	11:12:34
4	THE COURT: Give me a moment here.	11:12:37
5	(There was a pause in the proceedings.)	11:12:37
6	THE COURT: 759?	11:12:51
7	MR. JAMESON: Yes, Your Honor.	11:12:53
8	THE COURT: Well, these numbers all begin with 8.	11:12:58
9	MR. JAMESON: Your Honor, 8759. The last three are	11:13:07
10	759.	11:13:10
11	THE COURT: I don't have a 759 in the exhibit book.	11:13:17
12	It begins with 875.	11:13:23
13	MR. JAMESON: This is PTX-1600, Your Honor?	11:13:32
14	THE COURT: Yes, it is.	11:13:35
15	MR. JAMESON: I wonder if the last number may have	11:13:37
16	cut off in copying. Can you tell if you got a bad copy, by	11:13:40
17	any chance?	11:13:44
18	THE COURT: I guess that's possible. I can't really	11:13:48
19	tell.	11:13:57
20	MR. JAMESON: How about this, Your Honor: Do you	11:13:58
21	have Page 9 of 23?	11:14:00
22	THE COURT: I don't have a page number at all.	11:14:08
23	MR. JAMESON: Bottom right? You don't have a Page 9	11:14:12
24	of 23?	11:14:15
25	THE COURT: Yeah, I have Page 9 of 23, right.	11:14:37

Malackowski, J. - Cross

1 MR. JAMESON: Are we good? 11:14:40

2 THE COURT: All right. 11:14:42

3 MR. JAMESON: And, Your Honor, I'm going to ask 11:14:48

4 Mr. Malackowski some questions about this table, and it 11:14:50

5 extends from 9 of 23, 10 of 23, 11 of 23, to 12 of 23, so I'd 11:14:54

6 ask that those four pages be admitted. 11:15:01

7 THE COURT: Okay. 9 through 12 of 23. Okay. 11:15:08

8 (Plaintiff's Exhibit PTX-1600, Pages 9 through 12 11:15:13

9 were received in evidence.) 11:15:13

10 MR. JAMESON: And just for the record, Your Honor -- 11:15:13

11 and we will get you a better copy -- the last three Bates are 11:15:15

12 759, 760, 761, and 762. 11:15:20

13 THE COURT: I think what happened is just what you 11:15:25

14 said. I think the copying cut off the last number. 11:15:27

15 MR. JAMESON: Okay. I'm sorry about that, Your 11:15:33

16 Honor. May I proceed? 11:15:35

17 THE COURT: You may. 11:15:37

18 BY MR. JAMESON: 11:15:38

19 Q. Mr. Malackowski, this reflects table 1. It's a market 11:15:39

20 sampling of products with integrated third-party threat 11:15:45

21 intelligence. Do you see that? 11:15:49

22 A. I do. 11:15:50

23 Q. And this table is not dividing the market up into any 11:15:51

24 various specific technologies other than companies that are 11:16:01

25 offering any network security products that is integrating 11:16:07

—Malackowski, J. - Cross—

1 third-party threat intelligence, right? 11:16:12

2 A. That's fair. You would need to look specifically at the 11:16:13
3 offerings that are listed for each company to understand the 11:16:16
4 scope of their service. 11:16:20

5 THE COURT: Okay. Well, this entire document was 11:16:22
6 published in October of 2015, I assume, the entire document 11:16:27
7 was. 11:16:36

8 THE WITNESS: That's my understanding, yes, sir. 11:16:40

9 BY MR. JAMESON: 11:16:42

10 Q. And, Mr. Malackowski, I'm not going to ask you to do it 11:16:43
11 on the fly, but I have counted the number of companies that 11:16:45
12 had a product offering in October of 2015, according to 11:16:52
13 Gartner, that were relying on integrated third-party threat 11:16:58
14 intelligence, and they identify 49 different companies that 11:17:03
15 were in the marketplace as of this point in time. 11:17:07

16 Does that sound about right? 11:17:10

17 A. Yeah, but only one was proactive, as opposed to 11:17:11
18 reactive -- Centripetal. But that's right, there was a large 11:17:15
19 industry of the earlier generation of threat observation, 11:17:19
20 including Cisco. 11:17:23

21 For example, Cisco's product is limited to e-mail 11:17:27
22 security appliance; whereas, Centripetal is talking about 11:17:30
23 RuleGATE, which is the proactive solution. 11:17:34

24 Q. Mr. Malackowski, I was trying to make the simple point 11:17:36
25 that there were a lot of companies out there that were 11:17:43

Malackowski, J. - Cross

1	offering products that were relying on third-party threat	11:17:46
2	intelligence, according to the industry --	11:17:48
3	THE COURT: He's answered your question. Move on.	11:17:51
4	MR. JAMESON: Could we go to the last page?	11:17:55
5	THE COURT: You mean 12?	11:17:59
6	MR. JAMESON: 12 of 23, Your Honor.	11:18:02
7	And if you would highlight the note right underneath	11:18:05
8	the chart.	11:18:09
9	BY MR. JAMESON:	11:18:09
10	Q. And Gartner states, "This is not an exhaustive list of	11:18:15
11	providers, integrations, or partnerships. This research	11:18:19
12	serves as a sampling to illustrate some of the threat	11:18:24
13	intelligence integrations and partnerships in the security	11:18:27
14	market and to illustrate the depth of expansion being seen."	11:18:30
15	Do you see that?	11:18:33
16	A. I do. I agree with that, absolutely.	11:18:33
17	Q. Now, at the end of your testimony, you mentioned -- I	11:18:38
18	think I heard you say "irreparable harm;" is that right?	11:18:47
19	A. I believe I used the word "irreparable" in the fact that	11:18:51
20	Centripetal has been thwarted and I do not believe they will	11:18:58
21	recover, and that's typically the phrase that's used.	11:19:02
22	Q. And to the extent Centripetal has not been as successful	11:19:05
23	in the marketplace as it would have liked, are you pointing	11:19:14
24	the finger at Cisco for that?	11:19:19
25	A. To be direct, yes, in part, in substantial part.	11:19:21

—Malackowski, J. - Cross—

1 Q. And you're stating your opinion that Centripetal's lack 11:19:31
2 of success in the marketplace is a result of Cisco's 11:19:42
3 infringement of the Centripetal patents, right? 11:19:50

4 A. Well, more specifically, I'm focused on this point 11:19:52
5 looking forward, not looking back, so Centripetal's 11:19:56
6 limitations to be successful from today into the future are 11:20:00
7 due in substantial part to the infringement. 11:20:05

8 Q. You're not aware of any other reasons that Centripetal 11:20:08
9 has not been as successful in the marketplace as they would 11:20:22
10 have liked? 11:20:25

11 A. Of course I am. You're referring back historically 11:20:26
12 again, but, for example, Mr. Rogers testified as to other 11:20:30
13 challenges, like any business has. But, in my opinion, when 11:20:34
14 you look at the scale of Centripetal as a business, versus 11:20:38
15 Cisco, the extent of the infringement, and the usurpment of 11:20:42
16 the first-mover position, it was detrimental. 11:20:47

17 Q. I would like to turn to Defendant's Trial Exhibit Number 11:20:53
18 59. 11:21:09

19 MR. JAMESON: And that should be in your notebook, 11:21:13
20 Your Honor. 11:21:15

21 THE COURT: Yes, I have it. 11:21:24

22 BY MR. JAMESON: 11:21:27

23 Q. Mr. Malackowski -- 11:21:28

24 MS. KOBIALKA: Your Honor, I'm going to object to 11:21:29
25 this exhibit. This is an expert report from the Keysight 11:21:31

—Malackowski, J. - Cross—

1 case on damages. This is not -- I don't see how this is 11:21:35
2 appropriate. 11:21:41

3 MR. JAMESON: I haven't even asked my question yet, 11:21:42
4 but this expert talks about the issues that Centripetal faced 11:21:45
5 in the marketplace and who their competitors were and the 11:21:54
6 obstacles that they were dealing with as of 2018. 11:22:00

7 THE COURT: Well, the Court notified counsel prior 11:22:05
8 to this case that it had in its possession the transcript of 11:22:15
9 the Keysight trial, and Cisco objected to the Court reviewing 11:22:23
10 any portion of the transcript of the Keysight trial, so I 11:22:32
11 didn't. So I sustain the objection to this exhibit. 11:22:37

12 If I let this exhibit in, then I'd have to go back 11:22:46
13 and go through all of the exhibits to which Cisco objected as 11:22:51
14 not being relevant to this case. If the transcript isn't 11:22:57
15 relevant, then certainly a portion of the expert report 11:23:01
16 wouldn't be relevant. 11:23:03

17 MR. JAMESON: Yeah. This witness did not testify at 11:23:05
18 trial, Your Honor. 11:23:07

19 THE COURT: Well, that doesn't make any difference, 11:23:08
20 Counsel. 11:23:10

21 MR. JAMESON: Yeah. I was using it for impeachment 11:23:11
22 purposes. 11:23:14

23 THE COURT: I don't know how you can impeach one 11:23:15
24 expert with an opinion given in a different case, 11:23:18
25 particularly when you objected to the Court looking at the 11:23:21

Malackowski, J. - Cross

1 different case.

11:23:24

2 BY MR. JAMESON:

11:23:51

3 Q. You provided testimony on direct that basically the
4 industry follows the lead of Cisco; is that right?

11:23:51

11:24:00

5 A. The industry is very aware of Cisco's position, and, yes,
6 to the extent that it's possible, they migrate towards
7 competing directly with Cisco and whatever it offers.

11:24:07

11:24:12

11:24:19

8 Q. Okay. But -- and you mentioned that -- you mentioned
9 Juniper and Palo Alto Networks as two companies that did what
10 in reaction to something Cisco did in the marketplace? I
11 really did not follow that.

11:24:23

11:24:30

11:24:36

11:24:40

12 A. That those are two companies -- along with Keysight, the
13 two companies that specifically have sought to imitate the
14 Cisco solutions that are described as infringing the patents
15 in this suit. And so from Centripetal's perspective, they
16 are now competing against what is represented to be their own
17 technologies, not only with Cisco, but with others in the
18 marketplace.

11:24:41

11:24:46

11:24:49

11:24:53

11:24:57

11:25:02

11:25:06

19 Q. What specific products has Juniper offered in the
20 marketplace that imitates Cisco?

11:25:06

11:25:13

21 A. So in my report there's a description of the products for
22 each company. I don't recall by memory, in part because
23 that's not the relevant point I'm making. I'm not doing a
24 technical product comparison, I'm relaying what was striking
25 to me in my interview with Centripetal executives. And I

11:25:16

11:25:22

11:25:24

11:25:27

11:25:32

—Malackowski, J. - Cross—

1 simply wanted to confirm that those two companies are 11:25:38
2 directly competing. 11:25:41

3 I think you'll see, in the last document we had, 11:25:42
4 they show up there, as well. 11:25:45

5 Q. Juniper and Palo Alto have been competing with Cisco in 11:25:46
6 the marketplace for a long time, right? 11:25:51

7 A. True, but not in a way that Centripetal thought was 11:25:54
8 mimicking their own solution. 11:25:59

9 Q. Okay. But you can't identify any product of Juniper that 11:26:01
10 allegedly has infringing functionality in it, right? 11:26:08

11 A. I am not contending they infringe. That was asked about 11:26:12
12 in my deposition. That's a technical analysis. I'm only 11:26:16
13 relaying my interviews, my experience in the industry, and 11:26:20
14 the confirmation that those are competitors. And so from 11:26:24
15 Centripetal's business operations, they now deem those to be 11:26:29
16 offering technologies mimicking Cisco's infringement. 11:26:33

17 Q. You're aware of no evidence that Juniper is offering a 11:26:37
18 product in the marketplace that infringes, right? 11:26:42

19 A. I -- there's been no infringement accusation. 11:26:45

20 Q. Okay. And you cannot identify any product of Palo Alto 11:26:48
21 Networks that is mimicking what's been alleged as Cisco's 11:26:58
22 infringing technology, right? 11:27:08

23 A. Again, I refer you to my report where the products are 11:27:09
24 identified. None have been accused of infringement. 11:27:11

25 Q. Your opinion is that Centripetal's losing sales because 11:27:24

—Malackowski, J. - Cross—

1 of Cisco, right?

11:27:30

2 A. Well, in part, that they have lost value, and that has
3 been reflected by the competition that they are facing in the
4 market and, frankly, more their inability to compete against
5 Cisco.

11:27:31

11:27:35

11:27:39

11:27:43

6 I think Mr. Rogers talked about how when they
7 approach customers and describe their solution and the
8 customer says, well, I'm getting that from Cisco, the
9 conversation ends.

11:27:43

11:27:47

11:27:50

11:27:52

10 Q. Are you aware of any evidence of Centripetal losing a
11 specific sale because of Cisco?

11:27:53

11:28:00

12 A. Anecdotally, there are a few examples in my report, but I
13 don't have a customer-to-customer historical loss. I think
14 that's a question better for Mr. Gunderson.

11:28:02

11:28:08

11:28:13

15 Q. I, unfortunately, have lost that opportunity,
16 Mr. Malackowski.

11:28:16

11:28:20

17 A. I can tell you what he told me.

11:28:22

18 THE COURT: All right. This is a good time to take
19 our morning recess. We'll be in recess until 11:45.

11:28:31

11:28:33

20 During the recess, you should not consult anything
21 that would improve your knowledge of the subject matter of
22 your testimony. In other words, you should come back after
23 the break just as you leave.

11:28:38

11:28:41

11:28:47

11:28:49

24 THE WITNESS: Yes, sir, understood.

11:28:55

25 (There was a recess from 11:29 a.m. to 11:47 a.m.)

11:29:29

Malackowski, J. - Cross

1 THE COURT: All right, Mr. Jameson, you may proceed. 11:47:38

2 MR. JAMESON: Thank you, Your Honor. 11:47:41

3 BY MR. JAMESON: 11:47:45

4 Q. Mr. Malackowski, you mentioned that there were some other 11:47:45

5 factors impacting Centripetal's ability to compete in the 11:47:49

6 marketplace other than just Cisco's alleged infringement, and 11:47:53

7 I would just ask for your testimony as to what those other 11:47:57

8 factors, in your opinion, are. 11:48:00

9 A. I referred you specifically to my conversation and the 11:48:03

10 testimony of Mr. Rogers. I believe he talked about personnel 11:48:07

11 changes that they had, access to capital, the typical thing 11:48:11

12 that any emerging business goes through. 11:48:17

13 Q. Competition with Ixia would have been another factor. Is 11:48:19

14 that fair? 11:48:28

15 A. Absolutely. I certainly did not mean to leave that out, 11:48:28

16 Cisco, or the me-too followers, no, sir. 11:48:32

17 Q. And how about, just in general, that the network security 11:48:35

18 industry is really, really big, and there's a lot of players 11:48:40

19 in the industry? Would that be a factor in why, perhaps, 11:48:44

20 their sales aren't where they wanted them to be? 11:48:49

21 A. Uniquely, no, because in this case they would view that 11:48:51

22 large industry as an opportunity, because there was an 11:48:54

23 established space of the reactive security, and they were 11:48:57

24 offering the only unique proactive. 11:49:01

25 So they didn't have to sell people on, you needed 11:49:03

—Malackowski, J. - Cross—

1 security. That was already done. They were able to go in 11:49:06
2 and say, we're going to offer you one and two generations 11:49:08
3 ahead, and see what Gartner is predicting. 11:49:13

4 Q. Are you suggesting that was a niche product offering? 11:49:16

5 A. No, it's a generational product offering, because it was 11:49:21
6 such a large installed base of threat intelligence, threat 11:49:24
7 gathering, and they could take that base and take it to the 11:49:28
8 next level. It was actually a benefit to them, not a 11:49:32
9 hindrance. They didn't have to convince people that they had 11:49:35
10 to focus on threats to begin with. 11:49:40

11 Q. If it was a generational product offering, as you 11:49:43
12 suggest, do you have an explanation for why their sales 11:49:50
13 started declining in 2017, before Cisco started infringing? 11:49:56

14 A. So that was discussed during the trial, as well. I don't 11:50:00
15 have a lot to offer in that regard, except to reinforce what 11:50:03
16 was said; that even before Cisco's marketing materials came 11:50:06
17 out, Jonathan Rogers talked about how the fact that he was, 11:50:11
18 you know, hearing from the market that Cisco's working on 11:50:15
19 doing the same. 11:50:17

20 And that's typical. The companies will begin to 11:50:18
21 talk about, socialize with customers, their next products 11:50:22
22 before they're actually released. And that's the only thing 11:50:26
23 that I identified. 11:50:29

24 Q. Is it your opinion that Centripetal's RuleGATE product is 11:50:30
25 directly competing with Cisco's router and switch product 11:50:42

—Malackowski, J. - Cross—

1	line?	11:50:46
2	A. Not directly competing in that they're the same product	11:50:46
3	but competing in the sense that once a customer buys the	11:50:51
4	Cisco infringing solution, they no longer have a need for	11:50:55
5	Centripetal's offering.	11:50:59
6	Q. What if we turn that around and -- scenarios where there	11:50:59
7	are companies out there that have been relying on Cisco for	11:51:08
8	network infrastructure for years. Would that be a reason why	11:51:12
9	those companies would return to Cisco for the next product	11:51:20
10	line, as opposed to Centripetal?	11:51:23
11	A. Well, that's a great question. If Cisco offered the same	11:51:24
12	solution, yes, of course, they would. That was the problem.	11:51:27
13	But if they didn't, that's why Centripetal wanted to partner	11:51:31
14	with Cisco, because they can then take those legacy customers	11:51:35
15	with routers and switches and say, we're Cisco's partner with	11:51:38
16	proactive security, and the two go together like, you know,	11:51:43
17	chocolate and peanut butter. But that's not what happened.	11:51:47
18	Q. So they would have been a Reese's cup if they had a	11:51:53
19	partnership.	11:51:57
20	A. They would have been a good solution. That was the goal.	11:51:58
21	Q. You mentioned that Cisco's growth rate in the network	11:52:01
22	security space for fiscal year 2018 to 2019 was 16.6 percent;	11:52:07
23	is that correct?	11:52:15
24	A. I believe so, yes, sir.	11:52:15
25	Q. And are you attributing that to Cisco's infringement or	11:52:17

—Malackowski, J. - Cross—

1 purported infringement of Centripetal's technology? 11:52:24

2 A. I believe, in part, if you dig into that number, you'll 11:52:26

3 see that the infringing technology was the most rapidly 11:52:31

4 growing, so mathematically it has to be a contribution. 11:52:33

5 Q. Did you, by any chance, do the growth rate calculations 11:52:37

6 for Cisco's network security products in the years leading up 11:52:42

7 to the purported infringement? 11:52:49

8 A. No, those would be factored -- impacted by many other 11:52:53

9 variables that I couldn't control for. I simply wanted to 11:52:57

10 understand, during the period of infringement, were the 11:53:00

11 accused products driving the growth, and the answer was yes. 11:53:03

12 Q. Would it surprise you that Cisco's growth rate in the 11:53:06

13 network security industry for years leading up to the 11:53:12

14 purported infringement were double digit, year after year? 11:53:17

15 A. No, I would expect that. That's how they got to be the 11:53:23

16 \$50 billion leading firm. 11:53:27

17 Q. One of the reasons that this double-digit growth rate was 11:53:31

18 occurring, even before the purported infringement began, was 11:53:35

19 precisely what Gartner predicted, which is this is an 11:53:39

20 exploding industry. Fair? 11:53:44

21 A. In part, fair. 11:53:45

22 MR. JAMESON: I've got no further questions, Your 11:53:48

23 Honor. 11:53:50

24 THE COURT: All right. 11:53:50

25 MS. KOBIALKA: Your Honor, just one area of inquiry. 11:53:51

Malackowski, J. - Redirect

1	REDIRECT EXAMINATION	11:53:55
2	BY MS. KOBIALKA:	11:53:58
3	Q. If we could turn to and pull up the actual exhibit	11:53:59
4	PTX-1600 and turn to Page 12, that ends in 762. There was a	11:54:06
5	box that says, "Note: This is not an exhaustive list of	11:54:12
6	providers."	11:54:16
7	THE COURT: All right.	11:54:16
8	BY MS. KOBIALKA:	11:54:16
9	Q. Mr. Malackowski, you were asked about this note here, and	11:54:18
10	you said you agreed with that statement.	11:54:20
11	Can you explain what you meant when you said you	11:54:22
12	agreed with that statement during cross-examination?	11:54:25
13	A. Yes. One of the assets that Centripetal was building was	11:54:27
14	to partner with all of those threat-identifier firms. I	11:54:32
15	think Mr. Rogers testified that they had close to 100. 90 is	11:54:37
16	a number that comes to mind.	11:54:42
17	So this lists about half of them. There are a lot	11:54:43
18	more. And they all represent opportunity to Centripetal,	11:54:46
19	because they're the ones that are integrating that	11:54:50
20	information in an operationalized way, and that was, in part,	11:54:53
21	what made their product offering so exciting, from an	11:54:57
22	investor's perspective or from the market perspective.	11:55:01
23	Q. And by virtue of having someone like Cisco, a Fortune 100	11:55:04
24	company, coming into that market, can you just explain how	11:55:09
25	harmful that is in terms of the first-mover position, the	11:55:13

—Malackowski, J. - Redirect—

1 reputational irreparable harm that you talked about? 11:55:19

2 A. It is critical to a small or growing company. To be 11:55:23

3 recognized as the first mover and to maintain it is what 11:55:26

4 drives customer adoption. It's what drives investment 11:55:30

5 capital. It's what drives recruiting. And so if you lose 11:55:33

6 that, then not only have you lost it, but, importantly, 11:55:37

7 someone else has claimed it; in this case, Cisco. 11:55:41

8 So it's not from 1 to 0, it's from 1 to 0 to 11:55:43

9 negative 1. You're in a negative position, because now you 11:55:50

10 have to try to fight against that, and the best thing you 11:55:52

11 have to fight it with is your own technology that they're 11:55:56

12 emulating. So you can't win, you just can't. 11:56:00

13 Q. And is part of the power of having a patent to be able to 11:56:02

14 maintain the exclusivity of that market? 11:56:05

15 A. Well, it's not only the power, it's the bargain you make. 11:56:06

16 You disclose, as an inventor, your invention in sufficient 11:56:09

17 detail that others could practice it, and in exchange for 11:56:14

18 that, you are given a protected right. And the system just 11:56:16

19 breaks down if others take that right from you, because 11:56:21

20 you've already given up the explanation. It's public. 11:56:24

21 MS. KOBIALKA: I have no further questions. 11:56:29

22 THE COURT: All right. If there's nothing further 11:56:32

23 from the defense, may this witness be excused, or is he 11:56:39

24 somebody who is going to be recalled? 11:56:43

25 MR. JAMESON: Nothing further from me, Your Honor. 11:56:46

1	THE COURT: How about the plaintiff?	11:56:48
2	MS. KOBIALKA: We will not be recalling	11:56:51
3	Mr. Malackowski.	11:56:53
4	THE COURT: All right. You're excused as a witness,	11:56:54
5	with the caution that you may not discuss your testimony with	11:57:00
6	any other witness in the case until the case is concluded.	11:57:05
7	You may witness the remaining portion of the case in any way	11:57:12
8	you choose, as long as you don't discuss your testimony with	11:57:24
9	other witnesses.	11:57:27
10	THE WITNESS: May I indulge one clarifying question?	11:57:30
11	THE COURT: Yes.	11:57:33
12	THE WITNESS: A number of people know my	11:57:34
13	participation. They're just asking me what it's like to	11:57:36
14	testify on video. Can I talk about that independent of the	11:57:40
15	case facts, or should I not even do that?	11:57:44
16	THE COURT: I don't think it would be a good thing	11:57:46
17	to do at this point. It would be fine when the case is	11:57:47
18	over --	11:57:50
19	THE WITNESS: Thank you, Your Honor.	11:57:52
20	THE COURT: -- but it's hard to draw the line	11:57:53
21	between --	11:57:55
22	THE WITNESS: I understand. That's why I asked.	11:57:57
23	THE COURT: Right.	11:57:58
24	THE WITNESS: Thank you.	11:58:00
25	THE COURT: All right. You may be excused.	11:58:01

1	(Witness excused.)	11:58:03
2	MS. KOBIALKA: Thank you. At this time, Your Honor,	11:58:06
3	Centripetal rests its case in chief against Cisco.	11:58:08
4	THE COURT: All right. Are you going to begin your	11:58:12
5	case, or do you have any motions you want to make, or what?	11:58:22
6	MR. JAMESON: Your Honor, we have a motion to make,	11:58:26
7	and I'm going to turn it over to Mr. Gaudet for that, so	11:58:27
8	we're swapping out spots. If you'll give us just a second,	11:58:31
9	please.	11:58:37
10	THE COURT: All right.	11:58:37
11	MS. KOBIALKA: Your Honor, I'm going to turn it over	11:58:37
12	to Paul Andre.	11:58:40
13	THE COURT: All right.	11:58:57
14	MR. GAUDET: Your Honor, Matt Gaudet, and Cisco	11:59:07
15	hereby moves for a judgment on partial findings pursuant to	11:59:11
16	Rule 52(c).	11:59:14
17	We have a very short presentation here. I think	11:59:15
18	it's about 15 slides. We provided a paper copy of that to	11:59:19
19	you, Your Honor. There should be a binder there.	11:59:25
20	THE COURT: Is that something that was delivered	11:59:29
21	today or what?	11:59:32
22	MR. GAUDET: It should have been delivered this	11:59:33
23	morning.	11:59:35
24	THE COURT: It's on the shelf?	11:59:35
25	THE CLERK: It should be on the bottom shelf, Your	11:59:39

1	Honor.	11:59:44
2	MR. GAUDET: It has "May 21, 2020" on it.	11:59:44
3	THE COURT: Yes, I have it.	11:59:48
4	All right. You may proceed.	11:59:52
5	MR. GAUDET: Thank you, Your Honor.	11:59:53
6	And, in parallel with this, we're also filing a	11:59:54
7	paper on the online filing system with the Court. I will	11:59:57
8	move through this --	12:00:02
9	THE COURT: The "online filing system"?	12:00:03
10	MR. GAUDET: I'm sorry, PACER. We're filing the	12:00:06
11	motion officially, in addition to saying it out loud in	12:00:10
12	court. That's all that I meant, Your Honor.	12:00:14
13	THE COURT: All right.	12:00:16
14	MR. ANDRE: Mr. Gaudet, did you give us a copy of	12:00:16
15	this slide presentation? We don't seem to have one.	12:00:17
16	MR. GAUDET: The parties have not -- it's	12:00:20
17	demonstrative. The parties agreed not to exchange	12:00:22
18	demonstratives, so per that agreement, we have not done so.	12:00:26
19	MR. ANDRE: All right.	12:00:28
20	MR. GAUDET: We'd be happy to change the rules if	12:00:29
21	you-all wanted to, but that's...	12:00:34
22	Your Honor, very quickly, Rule 52(c) is what we're	12:00:36
23	moving under, and the important part of Rule 52(c) is this is	12:00:39
24	very different than a jury trial. That is to say, under	12:00:44
25	Rule 52(c), you can weigh the evidence right now. You don't	12:00:48

1 have to give inferences in favor of the plaintiff. If you
2 think you've heard enough on something, you're allowed to
3 weigh the evidence, even make credibility determinations, and
4 that's obviously very different from a jury trial.

5 The other point I want to make procedurally is that,
6 of course, we can move just on some issues. So what we're
7 doing in, hopefully, a very streamlined way, is I want to
8 give you essentially one noninfringement position -- or
9 maybe, at most, one and a related one -- on each patent, and
10 that's all that I'm going to do.

11 And so the first one we've got here is the '856
12 patent. That was JTX-5. That's what we've been referring to
13 as the encryption patent. It's the first patent that
14 Dr. Cole referred to, and it's got -- it's the one that's
15 got -- it's got the proxy system in it, that sort of thing.
16 There are just three key elements that you need to focus on,
17 and quickly their infringement theory becomes an
18 impossibility.

19 The claims require that you determine packets that
20 comprise encrypted data, you filter those determined packets,
21 and you route the filtered packets to a proxy system. Okay.
22 The problem for Centripetal is they're -- based on the
23 different components they accuse to do these things, it's
24 literally impossible.

25 So Dr. Cole says that Cognitive Threat Analytics, or

1 CTA, part of Stealthwatch up in the cloud, determines the 12:02:29
2 packets that are encrypted and filters the determined 12:02:34
3 packets. He was unambiguous about that. That's where it 12:02:37
4 happens, okay? 12:02:37

5 The problem right out of the gate: Everyone agrees 12:02:40
6 Stealthwatch and Cognitive Threat Analytics do not receive 12:02:44
7 packets. They don't get them. They get, as he said, 12:02:47
8 representations in the form of NetFlow records, but they 12:02:51
9 don't get the packets, so they can't filter the packets. 12:02:54

10 The second point is, Your Honor -- and we've got the 12:02:57
11 citations to where Dr. Cole said different things. The 12:03:02
12 second point is, even if they could overcome that hurdle, 12:03:07
13 which they can't -- we simply don't filter packets, as they 12:03:13
14 allege -- is by cognitive but the thing he's saying is doing 12:03:16
15 the filtering. 12:03:20

16 The second point is you then have to route those 12:03:20
17 determined packets. In other words, after, according to him, 12:03:26
18 Stealthwatch and Cognitive Threat Analytics have made this 12:03:30
19 determination and this filtering, something then has to route 12:03:34
20 the packets to a proxy system. And what they're accusing is 12:03:37
21 that the router or switch routes those packets to something 12:03:41
22 called a Null interface, which is just a graveyard, and 12:03:45
23 that's how you drop packets, okay? 12:03:49

24 So, again, it's literally an impossibility, because 12:03:51
25 by the time Stealthwatch has even gotten information about 12:03:54

1 these packets, it's already been forwarded to the 12:03:59
2 destination. They cannot be dropped anymore; they're gone. 12:04:03
3 And everybody agreed to that. This is all undisputed 12:04:05
4 testimony. 12:04:09

5 And Centripetal has no DOE position on this. So 12:04:10
6 even if they want to use the phrase "representations" and 12:04:13
7 "it's sort of like" they didn't argue doctrine of 12:04:16
8 equivalents, and this is everything you need to know in order 12:04:20
9 to enter judgment, Your Honor. 12:04:24

10 That's all I have on the first patent, and now I'm 12:04:26
11 going to turn to the next patent, with the Court's 12:04:28
12 permission. 12:04:30

13 THE COURT: Well, let's take them one at a time. 12:04:31

14 MR. GAUDET: Okay. 12:04:31

15 THE COURT: What's the plaintiff's response to that? 12:04:33

16 MR. ANDRE: Your Honor, with respect to the 12:04:41
17 testimony from Dr. Cole and the evidence that was put in for 12:04:44
18 the determined, just if you look at the slide right here, 12:04:50
19 they're cherry-picking portions of the trial testimony, and 12:04:54
20 they're mischaracterizing the trial testimony. 12:04:58

21 Dr. Cole testified, at trial testimony 935 through 12:05:01
22 936 and using PTX-578, that this element is met -- the 12:05:06
23 determined element is met when -- determined based on the 12:05:14
24 portion of the unencrypted data corresponding to one or more 12:05:18
25 network threat indicators, the plurality of network threat 12:05:22

1 indicators, packets comprising encrypted data that correspond 12:05:25
2 to one or more network threat indicators, they're 12:05:28
3 mischaracterizing the claim language and reading it in a way 12:05:32
4 that is incomprehensible. 12:05:34

5 Dr. Cole provided ample evidence to show that the 12:05:36
6 system that we accused in this case meets that element 12:05:41
7 literally. Dr. Cole did testify, and in great detail, using 12:05:44
8 Exhibit PTX-989, showing that the initial data packet and the 12:05:49
9 sequence of packet length time intervals, and the time and 12:05:55
10 the global risk map, are all part of this system, and that is 12:05:59
11 incorporated through the switches, it goes through the 12:06:04
12 routers, it goes up to the Stealthwatch, which is part -- it 12:06:07
13 has part of that in the CTA and the ETA, the Cognitive Threat 12:06:13
14 Analytics and the Encrypted Traffic Analytics, and also is 12:06:17
15 implicated by the ISE, the Identity Services Engine. So 12:06:21
16 there's multiple pieces of evidence that shows that this is a 12:06:26
17 single system and not separate components. 12:06:32

18 What the cross-examination of Dr. Cole showed was 12:06:34
19 that not only were the defendants trying to read the claims 12:06:38
20 in isolation, claim elements independently, as if their own 12:06:44
21 separate invention, they also tried to do the same thing with 12:06:49
22 the system. They never once looked at the system as a whole, 12:06:53
23 because the reason that Dr. Cole used the switches and 12:06:56
24 routers, the Stealthwatch, and the Identity Service Engine as 12:07:00
25 a single system was each of those contribute to different 12:07:04

1 aspects of the infringement. 12:07:08

2 So we have provided an abundance of evidence to show 12:07:10
3 that the determine element was met. 12:07:15

4 When we get to the filter element, the same thing. 12:07:18
5 Dr. Cole said filtering began both at the routers and 12:07:20
6 switches and continues up into the Stealthwatch, and there's 12:07:24
7 no evidence to show otherwise. In fact, I don't think 12:07:26
8 it will even be contested by their expert if it was. These 12:07:29
9 are packet-filtering systems, and this system filters packets 12:07:34
10 as they go through. 12:07:38

11 Now, they're trying to say that -- 12:07:39

12 THE COURT: I understand your position. 12:07:43

13 MR. ANDRE: Okay. All right. 12:07:45

14 And, Your Honor, with respect to the doctrine of 12:07:47
15 equivalents, as I told you during Dr. Cole's testimony, 12:07:50
16 Dr. Cole did not give an opinion on doctrine of equivalents 12:07:55
17 in these elements. He did not, but we did provide factual 12:07:56
18 evidence, and it is in our pretrial order that doctrine of 12:08:00
19 equivalents is in this case. 12:08:05

20 The Court -- as Counsel just pointed out, this is 12:08:06
21 not a jury trial. The Court can look at the facts asserted 12:08:08
22 and, based on the conclusions of law and the statements of 12:08:11
23 fact, can find doctrine of equivalents based on the evidence 12:08:15
24 supported -- provided to the Court, and that's in the 12:08:19
25 pretrial order. Dr. Cole did not give opinion testimony as 12:08:22

1 to doctrine of equivalents, but that doesn't preclude the 12:08:25
2 Court from finding that that's the case. 12:08:28

3 Also, with respect to the routing issue, Counsel 12:08:30
4 submits that they routed to a Null interface. Now -- 12:08:39

5 THE COURT: I don't think you need to say any more. 12:08:42

6 MR. ANDRE: Okay. Thank you, Your Honor. 12:08:42

7 THE COURT: The Court is going to deny the motion. 12:08:45

8 It was obvious during the examination that the 12:08:49
9 defendant was trying to draw a distinction between how 12:08:54
10 different elements of the packets moved through the system. 12:09:08
11 It looked to me as if it was an effort -- the inference the 12:09:15
12 Court draws is that they made an effort to design around the 12:09:22
13 patent and failed. 12:09:26

14 There's certainly ample evidence to support the fact 12:09:31
15 that the accused products do infringe, and I think Counsel is 12:09:33
16 exactly right. That's why I kept asking about equivalents, 12:09:40
17 because the Court doesn't need an expert to say that it falls 12:09:49
18 under the doctrine of equivalents if the evidence establishes 12:09:57
19 that it does. And the Court believes that it does establish 12:10:00
20 it, without the necessity of an opinion, that if it's not 12:10:07
21 direct infringement it would be infringement under the 12:10:11
22 doctrine of equivalents. 12:10:14

23 Let's move on to the next patent. 12:10:16

24 MR. GAUDET: Thank you, Your Honor. 12:10:17

25 With respect to the next patent, it's the '176 12:10:19

1 patent, Your Honor, and the '176 patent is the other patent 12:10:23
2 that Dr. Cole addressed. This is the correlation patent, and 12:10:29
3 this is the one that has the word "obfuscation" in it. It's 12:10:35
4 the patent that has packets that come into a network device 12:10:40
5 and then packets that go out of the network device and use 12:10:43
6 the logs to correlate those two to be sure you still know 12:10:47
7 that it's the same packet. 12:10:51

8 What they're accusing, Your Honor, are the ingress 12:10:53
9 and egress NetFlow records. They're saying there's NetFlow 12:10:57
10 records when the packet comes into the device, the router and 12:11:02
11 switch, and NetFlow records when it goes the other way. So 12:11:05
12 what the claim requires that you correlate those two things. 12:11:11
13 You correlate the two -- under their theory, you have to 12:11:14
14 correlate those two NetFlow records with each other. You're 12:11:19
15 correlating packets transmitted with packets received. 12:11:23

16 And the point here is very simple; it's that 12:11:27
17 Dr. Cole never showed any evidence that one NetFlow record or 12:11:31
18 log is correlated with another one and that there be -- 12:11:38
19 that's not how the system works. Instead, the evidence he 12:11:42
20 showed is that NetFlow information gets sent to the cloud, so 12:11:46
21 to speak, and it's correlated with other things; that, in the 12:11:52
22 first example -- and this was PTX-1065 -- it was that it 12:11:55
23 correlates threat behavior seen in the enterprise -- that 12:12:00
24 would be the stuff from NetFlow -- with those seen globally. 12:12:03
25 That's not correlating things inside of the enterprise 12:12:07

1 together, that's correlating inside of the enterprise with 12:12:10
2 something else entirely. 12:12:14

3 And the other example was similar. It was -- 12:12:17

4 THE COURT: Well, they couldn't correlate until it 12:12:22
5 got inside the network. They just had different sources of 12:12:27
6 something getting inside the network. 12:12:31

7 MR. GAUDET: Your Honor, our point is that these two 12:12:36
8 NetFlow records, the ingress and the egress, those two are 12:12:38
9 not -- there's no evidence that those two are correlated with 12:12:42
10 each other at all. In other words, you don't correlate them 12:12:47
11 and then go correlate them with something else. That's not 12:12:49
12 how the -- that's not what the system is doing. 12:12:52

13 And the evidence -- the evidence never suggests that 12:12:55
14 you would correlate the NetFlow record entering a device with 12:12:59
15 the NetFlow record exiting the device. That's not -- that's 12:13:03
16 not what the evidence shows. NetFlow is used for a different 12:13:08
17 purpose, Your Honor. And what they're showing on correlation 12:13:12
18 is that you would flow -- you would correlate some NetFlow 12:13:15
19 information with other things entirely. 12:13:19

20 That's our point, Your Honor. 12:13:21

21 THE COURT: All right. What does the plaintiff have 12:13:24
22 to say? 12:13:26

23 MR. ANDRE: Should I address that, Your Honor? 12:13:26

24 THE COURT: Please. 12:13:27

25 MR. ANDRE: Your Honor, Dr. Cole provided testimony, 12:13:28

1 starting at trial transcript 993 and going through 999, and 12:13:32
2 even PTX-1065 and PTX-591 and others, to show that, in fact, 12:13:37
3 there was a correlation based on plurality of log entries 12:13:44
4 corresponding to the plurality of packets received. 12:13:48

5 He actually showed, through his own experimentation 12:13:50
6 and testing of the products, how the -- when packets are 12:13:54
7 coming through, logs of those packets were sent up to 12:13:57
8 Stealthwatch and those -- Stealthwatch -- in Stealthwatch, 12:14:00
9 they were correlated. And he actually used the words, "they 12:14:04
10 were correlated." They correlated all the log entries that 12:14:07
11 went up. They also -- what they're talking about with global 12:14:10
12 log entries is other system log entries, syslog and other 12:14:13
13 logging entries. They correlate all the log entries, and 12:14:17
14 Dr. Cole talked about that in great detail. 12:14:20

15 In fact -- 12:14:23

16 THE COURT: That's the way I recall it. He said 12:14:24
17 they were all correlated. 12:14:26

18 MR. ANDRE: Thank you, Your Honor. 12:14:26

19 THE COURT: I deny the motion as to the '176 patent. 12:14:28
20 Let's move on. 12:14:33

21 MR. GAUDET: Okay. Thank you, Your Honor. 12:14:35

22 The next patent, Your Honor, is the '205 patent. 12:14:39
23 The '205 patent -- this is the last one that Dr. Mitzenmacher 12:14:43
24 did. 12:14:51

25 This is the patent that -- it's really about a 12:14:51

1 specific rule. This is the one that's got the phrase Session
2 Initiation Protocol, SIP, Uniform Resource Identifier, URI.
3 And the issue here, Your Honor, is about the Court's claims
4 instruction on "configured to," that the claims
5 require that -- you know, in 63 it's the packet network that
6 is configured to. In 63 and 67, it's the network device
7 configured to copy information. And there was a big dispute
8 about this. What does "configured to" mean? Is it the mere
9 capability; in other words, the fact that maybe theoretically
10 somebody could write a rule.

11 THE COURT: Yeah. I think I -- I'm not sure I got
12 that one right, where I said it had to be actually
13 configured. I think if it is capable of being configured,
14 that that would be sufficient.

15 MR. GAUDET: And, Your Honor --

16 THE COURT: I think that -- I was worried about
17 that, my finding of "actually configured." If the system is
18 configured so that it can do it, I don't think it has to
19 actually do it in order to infringe. I think -- because it's
20 very easy just to infringe on a patent and make the
21 distinction that -- or put some function in it that allows
22 you to disable the "configured to." So I think I got that
23 one wrong.

24 So I think if it's capable of configuring to it, it
25 doesn't have to actually be configured to it. I think I got

1 that wrong. 12:16:45

2 MR. GAUDET: And, Your Honor, I very much appreciate 12:16:46
3 that clarification, and let me take this just one step 12:16:48
4 further to give you a little more context. Because I still 12:16:52
5 think what they're doing is so far from the type of 12:16:55
6 capability that we think that would be, it still wouldn't 12:16:58
7 infringe, and this is why: 12:17:03

8 The patent requires a rule that identifies something 12:17:05
9 called the Session Initiation Protocol, SIP, URI, and that it 12:17:09
10 then causes this encapsulation. Now, I'll completely agree 12:17:16
11 that if they showed us that that rule was there, that such a 12:17:22
12 rule existed -- here's the rule, here's the example of the 12:17:25
13 rule, okay -- but nobody is using it, that would be one 12:17:28
14 thing. That, I think, goes to your point. That's not what 12:17:32
15 they showed us. 12:17:34

16 They can't show us an example of that rule existing 12:17:35
17 anywhere. No one has that rule. It's not a rule that we 12:17:39
18 would release, it's not a rule we're aware of anybody ever 12:17:42
19 writing. And so I kept asking him. Do you have an example 12:17:46
20 of this rule? Again, we're not saying, show us that somebody 12:17:50
21 used that rule, we're saying, just show us that you at least 12:17:54
22 have to have the rule for this thing to be capable. And he 12:17:58
23 could never even point to the existence of a specific rule 12:18:01
24 that would be capable of doing this. 12:18:06

25 That's our point on this one, Your Honor. 12:18:08

1 THE COURT: All right. 12:18:10

2 MR. ANDRE: Your Honor, we showed white papers, data 12:18:12
3 sheets, and the source code. All of them have the SIP, the 12:18:16
4 URI, and the products had compatibility. 12:18:21

5 We actually showed the rule written in the source 12:18:26
6 code, as Dr. Mitzenmacher has, perhaps a little too 12:18:29
7 thoroughly, demonstrated to the Court with numerous exhibits 12:18:33
8 and a considerable amount of time showing this very specific 12:18:36
9 element. There is ample evidence to show that this element 12:18:41
10 is met regarding the Session Initiation Protocol, Uniform -- 12:18:45

11 THE COURT: Well, look at what he said on this -- 12:18:50
12 what they quote him as saying. You have not shown us any 12:18:55
13 examples of where someone actually set up a rule to do this. 12:18:58
14 He says, "I don't recall specifically showing that." And 12:19:02
15 then he said again, "I don't recall identifying a rule that 12:19:05
16 has that condition." 12:19:08

17 Did he say something contrary to that, or he's just 12:19:12
18 saying that that doesn't answer the issue? 12:19:17

19 MR. ANDRE: Your Honor, this is when they were 12:19:20
20 trying to show that there was actual -- not only "configured 12:19:22
21 to" language, that somebody had actually had done it. 12:19:27

22 Their premise was you had to actually have done the 12:19:32
23 thing in the rule, but what he showed was the rule in the 12:19:36
24 code. He actually showed the source code that had the rule. 12:19:39
25 What he was not able to show was someone actually took that 12:19:43

1 rule and used it, essentially, but that was something that 12:19:46
2 was not in his -- was not in his assignment, because we had 12:19:49
3 CRM claims, computer-readable media claims. So if we showed 12:19:56
4 it in the code, therefore, it met that claim element. It 12:20:01
5 didn't have to be used, as per se. 12:20:04

6 And this is what he said, actually, on Page 863: 12:20:09

7 And the question was: "And your point is the system 12:20:13
8 doesn't have to actually configure with the rule? Is that 12:20:16
9 your point?" 12:20:19

10 He goes, "No. My point is like the system is 12:20:19
11 configured to do all these actions. You know, someone may 12:20:22
12 have to set up a rule to do it, but the system has the code 12:20:25
13 to do all this. It's configured to do this." 12:20:28

14 So they were focusing on the Court's interpretation 12:20:30
15 of "configured to," and this was their whole -- that you 12:20:39
16 actually had to -- it hadn't been done, actually configured 12:20:42
17 to do the function. 12:20:49

18 And what he's saying is, yes, the code itself, the 12:20:50
19 CRM language -- that's what we actually used, Your Honor, in 12:20:53
20 every one of our claims. We had a system claim, and we had a 12:20:57
21 CRM claim that was identical, and the reason we did that was 12:21:00
22 a very specific reason. Because a lot of times you get these 12:21:03
23 defendants who say, well, the system maybe can do it, but it 12:21:07
24 doesn't do it. So we put the CRM claims in based on a 12:21:10
25 Federal Circuit case that I actually argued a few years back 12:21:14

1 that says, if it's in the code, that's good enough. 12:21:16

2 So here Dr. Mitzenmacher said it was in the code, 12:21:18
3 and he gave examples of that, and he gave cites to that. 12:21:21

4 THE COURT: Well -- 12:21:25

5 MR. GAUDET: Could I respond to that? 12:21:28

6 THE COURT: -- I think that answers the issue, 12:21:32
7 because I was concerned about -- I mean, as you say, this was 12:21:35
8 a very contentious issue at the *Markman* hearing, and, as I 12:21:37
9 say, I just think I got it wrong when I said it had to 12:21:41
10 actually do that. Maybe if we stuck with that *Markman* 12:21:45
11 ruling, I would see more merit to the defendant's position, 12:21:54
12 but I just think I got the *Markman* ruling wrong. I wish I'd 12:22:00
13 have had the tutorial before I made that ruling. 12:22:06

14 So I think that if it's in the code and it's capable 12:22:13
15 of doing it, that that meets the claim language, so I'm going 12:22:16
16 to deny the motion as to the '205 patent. 12:22:21

17 MR. GAUDET: Thank you. And, Your Honor, just as a 12:22:26
18 quick preview, we very much disagree with Mr. Andre's 12:22:27
19 characterization of the record, but we totally understand. 12:22:33
20 Our turn is coming up. We're going to put on our side of the 12:22:35
21 story so you can see the other half. 12:22:39

22 THE COURT: All right. 12:22:39

23 MR. GAUDET: The '806 patent -- this is the 12:22:41
24 second-to-the-last one. We're almost there. 12:22:43

25 The '806 patent -- I'm going to click on through 12:22:44

1 here. 12:22:48

2 THE COURT: Well, the next one I have is the '205. 12:22:49

3 MR. GAUDET: Your Honor, we just spoke about the 12:22:53
4 '205. 12:22:55

5 THE COURT: Oh, we just spoke about that. 12:22:55

6 MR. GAUDET: I hope it's okay. I'm skipping some 12:22:58
7 slides. I'm trying to get us through. 12:23:01

8 THE COURT: That's always okay. 12:23:03

9 MR. GAUDET: Your Honor -- 12:23:06

10 THE COURT: This is the rule-swapping patent? 12:23:07

11 MR. GAUDET: The rule-swapping patent. It should be 12:23:09
12 slide number 9, Your Honor. 12:23:12

13 THE COURT: Right, I have it. 12:23:15

14 MR. GAUDET: Okay. And, Your Honor, this was, I 12:23:16
15 believe, the second patent that Mr. Mitzenmacher testified 12:23:19
16 about. 12:23:22

17 And the issue we've got for Your Honor is purely a 12:23:22
18 claim construction issue. It's something -- a dispute that 12:23:25
19 has become clear as the case progressed, and I know we've 12:23:29
20 briefed this in summary judgment, as well. It's that the 12:23:32
21 claim requires that you start processing the packet, you stop 12:23:35
22 processing the packet that has already begun processing -- 12:23:40

23 THE COURT: Okay. Don't go anywhere with this one. 12:23:44
24 You have to stop processing it. You can't simultaneously do 12:23:47
25 it, based on the evidence that I've heard. The stop may be, 12:23:51

1 and is, I suspect, a fraction of a second, but you can't be 12:24:02
2 processing packets at the same time as you change rules. 12:24:06

3 The only thing you people said was that you got the 12:24:10
4 rules finally changed. Well, you can't be changing the rules 12:24:14
5 absolutely simultaneously with processing, so let's move on 12:24:23
6 from that one. 12:24:28

7 MR. GAUDET: Your Honor, again, just asking for just 12:24:29
8 a little bit of leeway on this. That's not the argument I 12:24:32
9 was going to make. That's not it. And we will have -- we 12:24:34
10 will put on evidence, but that's not this issue. 12:24:38

11 THE COURT: Well, that's what this slide says. 12:24:40

12 MR. GAUDET: The issue is that, according to the 12:24:43
13 patent, you have to start processing a packet with one set of 12:24:46
14 rules, you stop processing that same packet, and then you, in 12:24:50
15 effect, restart with a different set of rules. So you've now 12:24:56
16 processed the same packet -- regardless of how much time is 12:25:00
17 in between, you start processing the packet, you stop 12:25:02
18 processing that packet, then you change the rules, however 12:25:06
19 much time is in between there, then you cache it, and you 12:25:10
20 process that same packet with the next set of rules. 12:25:15

21 That's our argument, and if you don't want to hear 12:25:18
22 any more about it, I'm going to move on. 12:25:21

23 THE COURT: Move on. 12:25:23

24 MR. GAUDET: Fair enough. Thank you for your 12:25:24
25 guidance, Your Honor. 12:25:26

1 Last one, and then we're done. Your Honor, this 12:25:27
2 is -- I'm moving through a lot of stuff now -- the '193 12:25:29
3 patent. This is the last one. 12:25:33

4 The '193 patent was the exfiltration patent that 12:25:35
5 Dr. Mitzenmacher -- the first one, so this is now going back 12:25:40
6 to, I believe, Monday of last week, when Dr. Mitzenmacher 12:25:43
7 presented, and this is, again, a patent on a specific kind of 12:25:46
8 a rule. 12:25:51

9 And it's that one or more packet-filtering rules 12:25:51
10 configured to prevent a particular type of data transfer. 12:25:55
11 And this one becomes a mouthful pretty quickly, but I just 12:25:59
12 wanted to show you two quick points that we think are 12:26:03
13 dispositive and that were agreed to. 12:26:07

14 All right. It's these two pieces of 12:26:09
15 Dr. Mitzenmacher's theory that cannot work. We're looking 12:26:12
16 for a packet-filtering rule configured to prevent a 12:26:17
17 particular type of data transfer. He said the 12:26:21
18 packet-filtering rule is the quarantine. And you fairly 12:26:23
19 asked a question, is that really it? And he confirmed, yeah, 12:26:26
20 that was my only example, is the quarantine. 12:26:29

21 He also said the particular type of data transfer -- 12:26:32
22 so the thing you are looking for with this packet-filtering 12:26:36
23 rule -- is, again, a mouthful, an HTTP POST command or an 12:26:39
24 HTTP GET command. 12:26:45

25 So they're saying their theory is that this 12:26:49

1 quarantine rule is configured to prevent the HTTP POST or
2 HTTP GET. That's what it says that this rule has to do, but
3 he admitted that's impossible. A quarantine can't even look
4 where those kinds of things would be. Those kinds of things
5 are always in the payload, and he admitted, as he said, that
6 the quarantine does not look specifically for the POST or the
7 GET. It just breaks down.

8 The rule that he -- the type of rule he identified,
9 he admitted literally a quarantine cannot do. It cannot
10 identify a POST or a GET. That's the position on that one,
11 Your Honor.

12 THE COURT: All right.

13 MR. ANDRE: Your Honor, needless to say, they're
14 mischaracterizing what Dr. Mitzenmacher stated. He showed
15 that you can block data transfer based on the header. He
16 very specifically said that. I can point you to the cite in
17 a few minutes as we pull it up. He also said that the
18 quarantine code, the actual code for the quarantine, is in
19 the switch and routers.

20 So their convoluted theory here just doesn't sync
21 up. It says the quarantine looks specifically at the POST
22 and GET, but that's not the point. The point is you can look
23 at the header and block transfer based on the header, and
24 there was ample evidence of that. So they're trying to
25 mischaracterize the one example he gave of the POST and GET

1 and trying to limit the claim to a single example. He only 12:28:23
2 gave the one example, because that's all he needed. He used 12:28:26
3 that as an exemplar of how it works. He also talked about, 12:28:29
4 in the source code, about how this system blocks or forwards 12:28:33
5 the packets. 12:28:40

6 And so they're trying to use a specific example and 12:28:43
7 limit his entire testimony to that one example, but he also 12:28:47
8 gave other evidence to show that, in fact, their system does 12:28:50
9 operate exactly as the claims require. And this is found at 12:28:55
10 trial transcripts 489 through 521, PTX-1849 at Pages 9, 21, 12:29:02
11 and 228, showing the source code that shows rules for 12:29:10
12 quarantine are created using information of a particular type 12:29:13
13 of data transfer. 12:29:16

14 The public -- 12:29:18

15 THE COURT: The particular type being the header? 12:29:20

16 MR. ANDRE: Yes, Your Honor. 12:29:22

17 THE COURT: Is that the only particular type? 12:29:24

18 MR. ANDRE: It's one of the types. He actually 12:29:26
19 talks about different types of headers, as well. 12:29:29

20 THE COURT: Different types of headers? 12:29:31

21 MR. ANDRE: Yeah. He mentioned two different types 12:29:34
22 of headers that you can look at, and both of them would be 12:29:36
23 responsive to blocking the data transfer based on those 12:29:40
24 headers. 12:29:45

25 When he's talking about the GET and POST, the HTTP 12:29:46

1 POST and GET, and the payload, he was using that as an 12:29:50
2 example that was demonstrated in Cisco's documents, because 12:29:53
3 that's what they use as an exemplar, so so did he. But in no 12:29:58
4 way did he say that that was the sole substance of his 12:30:03
5 testimony, because he gave considerable testimony on this 12:30:07
6 very element. 12:30:09

7 Once again, Your Honor, when we get a chance -- we 12:30:11
8 don't have the brief yet. We're seeing this for the first 12:30:13
9 time. On all of these issues we can give substantive 12:30:16
10 evidence to show that their theory is just taking the claim 12:30:21
11 language and mischaracterizing it and then taking snippets of 12:30:25
12 testimony out of context to try to make this argument. 12:30:29

13 THE COURT: The motion is overruled as to '193. 12:30:34

14 MR. GAUDET: Your Honor, thank you. We realize that 12:30:41
15 when we do these things mid-trial, we are at a serious uphill 12:30:43
16 battle, and we are looking forward to presenting our side of 12:30:48
17 the case now with our first witness. 12:30:52

18 THE COURT: All right. Well, why don't we -- I 12:30:53
19 think it would be better to go ahead and take our recess at 12:31:03
20 this time, instead of waiting. I don't know what your first 12:31:07
21 presentation is going to be, but is it going to take more 12:31:15
22 than a half an hour? 12:31:17

23 MR. GAUDET: Your Honor, I believe it will. I 12:31:19
24 expect -- well, I don't want to set up to disappoint with my 12:31:21
25 very first witness, but it will be more than 30 minutes. 12:31:27

1 THE COURT: Who is your witness? 12:31:30

2 MR. GAUDET: Mike Scheck. He's a fact witness, and 12:31:32
3 he's going to speak about Stealthwatch and some of those 12:31:35
4 other products. 12:31:38

5 THE COURT: Yes, he's one of the ones we saw a slide 12:31:38
6 on, right, one of the engineers that the plaintiff showed a 12:31:45
7 slide on? I believe I remember that name. 12:31:50

8 MR. GAUDET: Your Honor, I don't believe they have. 12:31:54
9 I cannot guarantee it, but I'm looking at the people that I 12:31:56
10 can see, and at least they don't recall it. 12:32:00

11 THE COURT: I thought I had seen that name before. 12:32:03

12 Okay. Let's go ahead and take our recess. We'll 12:32:06
13 resume at 1:35. 12:32:11

14 (Luncheon recess from 12:32 p.m. to 1:35 p.m.) 12:43:33

15 THE COURT: All right. Is the defendant ready with 01:35:46
16 its evidence? 01:35:52

17 MR. GAUDET: We are, Your Honor, we're ready to 01:35:53
18 proceed. 01:35:55

19 THE COURT: Okay. And your first witness is 01:35:56
20 Mr. Scheck? 01:36:12

21 MR. GAUDET: Mr. Scheck. 01:36:14

22 THE COURT: Scheck. 01:36:16

23 MR. GAUDET: And you should have a Michael Scheck 01:36:23
24 direct examination book. 01:36:26

25 THE COURT: I do. You may proceed. 01:36:27

—Scheck, M. - Direct—

1	MR. GAUDET: Thank you, Your Honor.	01:36:35
2	(The witness was sworn.)	01:36:45
3	MICHAEL SCHECK, called by the Defendant, having been	01:36:45
4	first duly sworn, was examined and testified as follows:	01:36:45
5	DIRECT EXAMINATION	01:36:45
6	BY MR. GAUDET:	01:36:45
7	Q. Good afternoon, Mr. Scheck.	01:36:55
8	A. Good afternoon.	01:36:57
9	Q. Could you state your name for the record?	01:36:58
10	A. It's Michael Scheck.	01:37:00
11	Q. By whom are you employed?	01:37:03
12	A. Cisco Systems.	01:37:04
13	Q. How long have you been employed by Cisco?	01:37:05
14	A. About 20 years. The first four were as a contractor, and	01:37:07
15	the last 15 have been as a full-time employee.	01:37:12
16	Q. And, Mr. Scheck, where do you live?	01:37:15
17	A. I live in Raleigh, North Carolina.	01:37:19
18	Q. So you're almost halfway between where I am, in Atlanta,	01:37:21
19	and where the Court is, in Norfolk, Virginia, I think.	01:37:24
20	A. At least we're on the right coast.	01:37:27
21	Q. Mr. Scheck, is that where you are currently?	01:37:30
22	A. It is.	01:37:32
23	Q. And what is your current position with Cisco?	01:37:33
24	A. I'm the Senior Director of Incident Command.	01:37:36
25	Q. And we'll build that out a little bit, but are you	01:37:40

—Scheck, M. - Direct—

1	familiar with the Computer Security Incident Response Team at	01:37:43
2	Cisco?	01:37:49
3	A. I am. That's one of the organizations that's part of	01:37:49
4	Incident Command.	01:37:53
5	Q. Talk generally about what Incident Command is.	01:37:54
6	A. Sure. So CSIRT and Incident Command, the role of that --	01:37:58
7	Q. Actually, let me jump in for just one moment.	01:38:03
8	Are you abbreviating Computer Security Incident	01:38:06
9	Response Team as CSIRT?	01:38:10
10	A. Yes. Thank you.	01:38:12
11	Q. Okay.	01:38:14
12	THE COURT: As what?	01:38:14
13	MR. GAUDET: CSIRT, C-S-I-R-T, Your Honor. It's	01:38:16
14	the --	01:38:20
15	THE COURT: What does that stand for?	01:38:21
16	BY MR. GAUDET:	01:38:24
17	Q. Mr. Scheck, do you want to...	01:38:25
18	A. It's the Computer Security Incident Response Team, Your	01:38:26
19	Honor.	01:38:31
20	THE COURT: Security what, now?	01:38:37
21	THE WITNESS: Incident Response Team.	01:38:39
22	THE COURT: Computer Security Incident Response	01:38:46
23	Team. Okay.	01:38:50
24	BY MR. GAUDET:	01:38:51
25	Q. What does Cisco's Computer Security Incident Response	01:38:51

—Scheck, M. - Direct—

1 Team do? 01:38:55

2 A. The role of the organization is essentially to deploy 01:38:56
3 equipment on Cisco's network, to look for security events 01:39:01
4 that may be security incidents, to investigate, and respond 01:39:07
5 to those. 01:39:12

6 Q. And a couple follow-up questions: 01:39:12

7 Is this with respect to Cisco's own corporate 01:39:15
8 network? 01:39:19

9 A. That is correct. 01:39:19

10 Q. And you referenced a security event and a security 01:39:20
11 incident. If you could, elaborate a little bit about what 01:39:25
12 those are and what the differences are. 01:39:30

13 A. So as we're deploying all these different tools to look 01:39:31
14 for interesting behavior, potentially malicious actions, 01:39:34
15 those types of things, they generate a lot of alerts. A lot 01:39:39
16 of data comes out of those systems, and our job is to look at 01:39:44
17 that data and find out if something bad has actually 01:39:47
18 happened. 01:39:51

19 And the data itself, as it's coming out, is what we 01:39:52
20 would call a security event. It's a log. It shows something 01:39:56
21 happened. When things happen in the right order, and when 01:39:59
22 something malicious has happened and we can investigate it, 01:40:04
23 that's a security incident. We know there's been an issue at 01:40:09
24 that point. 01:40:12

25 Q. And is your team responsible for investigating security 01:40:12

—Scheck, M. - Direct—

1	incidents?	01:40:15
2	A. That's correct.	01:40:16
3	Q. Are you also responsible for the tools used to	01:40:17
4	investigate security incidents?	01:40:20
5	A. That's correct.	01:40:22
6	Q. Okay. Now, in connection with that role, have you used	01:40:23
7	Stealthwatch?	01:40:28
8	A. I have.	01:40:28
9	Q. And are you familiar with how Stealthwatch operates?	01:40:29
10	A. Yes, I am.	01:40:33
11	Q. And what about NetFlow?	01:40:34
12	A. I am familiar.	01:40:36
13	Q. Encrypted Traffic Analytics?	01:40:37
14	A. Yes, familiar with that, as well.	01:40:41
15	Q. And what about Cognitive Threat Analytics?	01:40:43
16	A. Yes.	01:40:46
17	Q. And do you use other tools in investigating security	01:40:46
18	events, besides just those?	01:40:51
19	A. Yeah, we use quite a few tools. When you take a step	01:40:52
20	back and look, there's about 75-ish different tools that we	01:40:58
21	use to secure Cisco; you know, IPS, host-based monitoring,	01:41:03
22	e-mail monitoring, Stealthwatch, NetFlow analysis, et cetera.	01:41:08
23	Q. In addition to your work with Cisco's network, do you	01:41:11
24	also have interactions with customers?	01:41:16
25	A. I do.	01:41:18

—Scheck, M. - Direct—

1 Q. And describe those.

01:41:18

2 A. Often, because we're one of the first to deploy a new
3 Cisco technology, customers will come to us and ask us what
4 worked well for us, what issues we ran into, and they want to
5 have an honest conversation. You know, I'm not on a sales
6 team, so they want to come to me and figure out what is the
7 best way to secure their network using Cisco's tools.

01:41:22

01:41:27

01:41:33

01:41:36

01:41:39

01:41:42

8 Q. And do you also provide internal product feedback to
9 Cisco's teams that are designing products?

01:41:46

01:41:50

10 A. I do. Just like any other customer, you give feedback to
11 the person selling you something about things that you'd like
12 improved. It's just I'm in a unique situation where we're at
13 the same company, and I get to have more conversations with
14 those folks.

01:41:52

01:41:57

01:42:00

01:42:03

01:42:06

15 Q. And then do you give presentations to third parties about
16 the various Cisco security products?

01:42:06

01:42:09

17 A. I do.

01:42:12

18 Q. About how often do you give presentations to third
19 parties?

01:42:12

01:42:16

20 A. Honestly, I have conversations with customers and give a
21 presentation on probably a weekly basis. There's also larger
22 events, like Cisco Live and some of the big security
23 conferences, where there might be hundreds or thousands of
24 people that are attending each talk, and I do those a few
25 times a year, as well.

01:42:16

01:42:24

01:42:28

01:42:32

01:42:35

01:42:38

—Scheck, M. - Direct—

1	Q. Let's pull up Defense Trial Exhibit DTX-693.	01:42:39
2	MR. GAUDET: Your Honor, this should be a tab in	01:42:47
3	your notebook.	01:42:49
4	THE COURT: 693?	01:43:02
5	MR. GAUDET: DTX-693. It should be the	01:43:06
6	third-to-last tab in your notebook.	01:43:09
7	THE COURT: There's 693, and then a 693.1. Okay.	01:43:13
8	MR. GAUDET: That's right. We're going to talk	01:43:18
9	about them both, and we'll explain why there's a .1 there.	01:43:19
10	THE COURT: All right.	01:43:24
11	BY MR. GAUDET:	01:43:29
12	Q. Let's start with 693.	01:43:24
13	Mr. Scheck, is that your name at the top?	01:43:30
14	A. It is.	01:43:33
15	Q. And what is this document?	01:43:33
16	A. This is a presentation that I delivered to NATO in	01:43:35
17	December of 2015, I believe.	01:43:41
18	Q. And, to be clear, this is a nontechnical acronym. That's	01:43:43
19	the North Atlantic Treaty Organization?	01:43:48
20	A. That's correct.	01:43:51
21	Q. Okay. Did NATO ask you to make this presentation?	01:43:53
22	A. They did.	01:43:55
23	Q. And why did they ask you to make this presentation?	01:43:56
24	A. The head of the Cyber Security Division at NATO was	01:44:00
25	looking to invest in securing their network and had heard of	01:44:07

—Scheck, M. - Direct—

1 me and my position at Cisco and wanted to have conversations 01:44:12
2 around ways that they could do that more successfully. 01:44:15

3 Q. And let's just talk briefly about how we know the date of 01:44:18
4 this document. 01:44:22

5 Do you see at the bottom left there there's some 01:44:23
6 indications of dates? Do you see that? 01:44:27

7 A. I do. 01:44:29

8 Q. And is this, in effect, what's called the speaker view of 01:44:34
9 a PowerPoint? 01:44:40

10 A. That's correct. 01:44:41

11 Q. What does that mean? 01:44:42

12 A. The top half of the screen would be displayed to whoever 01:44:43
13 you're presenting to, the bottom half of the screen would 01:44:49
14 not, and it's there so that you can review it while you're 01:44:51
15 presenting and you have some notes that you may reference. 01:44:56

16 Q. So the 4/15/2020 date, is that an indication of when this 01:44:58
17 document was actually printed for purposes of this 01:45:05
18 litigation? 01:45:07

19 A. Yes, I believe that is correct. 01:45:07

20 Q. And you see there's a "Cisco Live 2014" reference 01:45:08
21 underneath that. What is that about? 01:45:12

22 A. So when the gentleman from NATO reached out to me and 01:45:14
23 asked to have the conversation, I went back through all the 01:45:21
24 previous presentations I had done, and there was one a few 01:45:25
25 months prior at Cisco Live, or a year prior at Cisco Live, 01:45:29

—Scheck, M. - Direct—

1 and I really liked the format of it. I liked the pictures
2 and all those sorts of things, so I took that Cisco Live
3 presentation and just erased all the content and created a
4 new one with that template.

5 Q. Let's now go and pull up 693.1.

6 THE COURT: Does that mean that you presented it in
7 2014 or not? When did you present it?

8 THE WITNESS: Yeah. This original template and
9 original presentation -- which some of the material that I
10 presented in 2015 was in there, but the original Cisco Live
11 presentation was in 2014.

12 THE COURT: Well, some of the material?

13 THE WITNESS: That's correct.

14 THE COURT: When was the presentation to NATO?

15 THE WITNESS: If I recall correctly, it was
16 mid-December of 2015.

17 THE COURT: That date doesn't appear on here,
18 though, does it?

19 MR. GAUDET: Your Honor --

20 THE COURT: December of '15. Okay.

21 MR. GAUDET: Your Honor, we're going to clear that
22 up with the next exhibit, and we'll do this probably for a
23 few presentations.

24 THE COURT: Okay.

25 BY MR. GAUDET:

—Scheck, M. - Direct—

1 Q. If we can pull up 693.1, Mr. Scheck, what is 693.1? 01:46:56

2 A. This is the metadata from that slide, that shows that it 01:47:01
3 was originally -- the original slide deck was created in 01:47:09
4 2013, and it had been modified several times, the last of 01:47:15
5 which was for the presentation to NATO in December 9th of 01:47:20
6 2015. 01:47:28

7 Q. The metadata is sort of embedded -- travels with the 01:47:29
8 document, sort of like the acid test of what really happened 01:47:34
9 with the document? 01:47:38

10 A. That's correct. 01:47:39

11 MS. LEE: Your Honor, I just have an objection to 01:47:40
12 this slide here that's being presented. 01:47:42

13 It does not appear to be the accurate metadata, 01:47:44
14 because it shows the last print date of May 19, 2014, when 01:47:47
15 the document, the witness just testified to, has a last print 01:47:52
16 date of April 15, 2020. 01:47:56

17 THE COURT: I don't see a last print date on the 01:48:19
18 preceding document. 01:48:26

19 MS. LEE: Your Honor, the witness had testified that 01:48:27
20 the April 15, 2020, date was the date that this document was 01:48:28
21 last printed. 01:48:31

22 MR. GAUDET: Your Honor, I will represent to the 01:48:39
23 Court this is the metadata of the document we produced in 01:48:41
24 this litigation. That's exactly as it appears. 01:48:45

25 MS. LEE: If it was the right metadata, it would 01:48:53

—Scheck, M. - Direct—

1	show up as the April 15th date.	01:48:56
2	MR. GAUDET: Your Honor, that's not right, actually.	01:48:58
3	THE COURT: Well, it could have been reprinted in	01:49:01
4	'20.	01:49:03
5	MR. GAUDET: Exactly. Exactly.	01:49:04
6	MS. LEE: But it says "last printed" --	01:49:07
7	THE COURT: Yeah, it says last printed in '20. That	01:49:10
8	doesn't mean that it wasn't printed before then.	01:49:13
9	MS. LEE: It says "last printed" on the slide that's	01:49:17
10	being shown on the screen.	01:49:20
11	THE COURT: Well, I don't think there's anything to	01:49:25
12	object to.	01:49:27
13	You may proceed.	01:49:28
14	MR. GAUDET: Thank you.	01:49:29
15	BY MR. GAUDET:	01:49:30
16	Q. Mr. Scheck, consistent with your recollection, did you	01:49:30
17	prepare this for the NATO presentation and last modify it on	01:49:33
18	December 9, 2015, in connection with that presentation?	01:49:40
19	A. Yes, that's correct. And I'm not only relying on the	01:49:42
20	metadata, I have the calendar dates, as well, so I know I	01:49:45
21	delivered this presentation in December of 2015.	01:49:48
22	Q. Thank you. Let's go back to Defense Exhibit 693, and	01:49:51
23	we'll go to the second page. We can blow that up, the actual	01:49:57
24	image there.	01:50:04
25	MR. GAUDET: Your Honor, this is Bates .002.	01:50:05

—Scheck, M. - Direct—

1 BY MR. GAUDET:

01:50:05

2 Q. And, Mr. Scheck, was this the second slide in this
3 presentation?

01:50:08

01:50:11

4 A. It was.

01:50:12

5 Q. And what is this?

01:50:12

6 A. When I talk to customers, a lot of times I'm talking to
7 them about how to secure their network to protect it from bad
8 things happening so that they can protect intellectual
9 property and those types of things, and with the gentleman
10 from NATO, I wanted to start off right away and say that I
11 understood and appreciated the fact that he's actually trying
12 to protect people's lives, and so I put in a medal that I had
13 received when I was an infantry member of the Marines
14 assigned to NATO.

01:50:14

01:50:19

01:50:24

01:50:27

01:50:30

01:50:34

01:50:37

01:50:41

01:50:45

15 Q. If we could now go to the Bates .004...

01:50:46

16 MR. GAUDET: Your Honor, this should be the next
17 page in your binder.

01:50:54

01:50:56

18 THE COURT: Yes, it is.

01:50:58

19 BY MR. GAUDET:

01:50:58

20 Q. And we'll blow up the actual image.

01:51:01

21 Mr. Scheck, what is this slide showing?

01:51:04

22 A. This slide is a representation of all of the events that
23 we see at Cisco on a daily basis.

01:51:06

01:51:12

24 Q. And, for example -- and this is a snapshot as of 2015; is
25 that right?

01:51:15

01:51:22

—Scheck, M. - Direct—

1	A. That's correct.	01:51:22
2	Q. And, for example, the upper left says, "16 billion	01:51:22
3	NetFlows." Do you see that?	01:51:27
4	A. I do.	01:51:28
5	Q. And how does that number compare, for example, with	01:51:29
6	today?	01:51:32
7	A. Today, it's closer to double that. It's in the high 20s	01:51:33
8	or low 30s, so, you know, 29, 30 billion NetFlow records a	01:51:38
9	day.	01:51:44
10	Q. Do you see there's a reference to "120,000 Windows host"	01:51:44
11	in the middle of the far right? Do you see that?	01:51:50
12	A. I do.	01:51:53
13	Q. What is that referring to?	01:51:53
14	A. A Windows host is just another name for a Windows PC. So	01:51:54
15	we have PC or server, so we have 120,000 Windows PCs or	01:51:59
16	servers deployed.	01:52:07
17	Q. And when you say "PC," is that just a computer that a	01:52:07
18	user can use?	01:52:10
19	A. That's correct.	01:52:10
20	Q. Okay. And then underneath that it says, "40,000	01:52:11
21	routers." Do you see that?	01:52:13
22	A. I do.	01:52:14
23	Q. And what's that referring to?	01:52:14
24	A. The 40,000 routers deployed on Cisco's network to move	01:52:15
25	traffic around our internal internet.	01:52:20

—Scheck, M. - Direct—

1 Q. Okay. And then you and your team were responsible for 01:52:23
2 investigating security events that bubble up from this stuff. 01:52:28
3 Is that fair? 01:52:34

4 A. That's correct. 01:52:35

5 Q. What are -- how many different tools do you use for that? 01:52:35

6 A. About 75 different types of tools are generating events 01:52:38
7 for our team. 01:52:43

8 Q. And I want to focus on one of those, in particular. Are 01:52:44
9 you familiar with Stealthwatch? 01:52:49

10 A. I am. 01:52:50

11 Q. Okay. Let's bring up the Stealthwatch demonstrative 01:52:51
12 slide 1. 01:52:59

13 MR. GAUDET: Your Honor, this should be in your 01:53:00
14 notebook under, I believe, the second tab. It should say, 01:53:02
15 "Stealthwatch demonstrative." 01:53:05

16 THE COURT: Okay. 01:53:22

17 BY MR. GAUDET: 01:53:23

18 Q. Mr. Scheck, does this appear to be just a fair sort of 01:53:23
19 generic representation, in the grayed box, of a local 01:53:26
20 network? 01:53:30

21 A. It is. 01:53:31

22 THE COURT: Well, you've used this diagram before. 01:53:33

23 MR. GAUDET: This is exactly the same one we've used 01:53:36
24 before, Your Honor, but Mr. Scheck was not part of the trial. 01:53:39

25 BY MR. GAUDET: 01:53:43

—Scheck, M. - Direct—

1	Q. And you understand that the Internet is off of the cloud	01:53:44
2	off to the left, Mr. Scheck?	01:53:48
3	A. I do.	01:53:50
4	Q. Okay. Now, as packets traverse this network, would they	01:53:50
5	hit the various routers and switches on their way to a given	01:54:03
6	user?	01:54:06
7	A. They would.	01:54:07
8	Q. And can a router or switch block traffic, block packets,	01:54:08
9	based on rules?	01:54:13
10	A. Yes, they can.	01:54:14
11	Q. How long has that been the case?	01:54:15
12	A. For as long as there have been routers and switches.	01:54:17
13	That's one of their core functions.	01:54:23
14	Q. Now, you see there's a dotted line or a series of dotted	01:54:25
15	lines that say "NetFlow" that run off to the right to	01:54:30
16	something called Stealthwatch. Do you see that?	01:54:34
17	A. I do. I do.	01:54:35
18	Q. Hold on just one second. I'm...	01:54:41
19	Are you familiar with NetFlow?	01:54:48
20	A. I am.	01:54:50
21	Q. How long have you worked with NetFlow?	01:54:51
22	A. Since about 2004.	01:54:54
23	Q. And do you give presentations to customers and other	01:54:58
24	third parties relating to NetFlow?	01:55:01
25	A. I do.	01:55:02

—Scheck, M. - Direct—

1 Q. Okay. If you could, explain your understanding of what 01:55:03
2 NetFlow is. 01:55:08

3 A. So, in its simplest form, any time -- if you look at this 01:55:09
4 picture, any time a system on this picture talks to any other 01:55:14
5 system and it passes through a router or switch and you have 01:55:18
6 NetFlow turned on, NetFlow records a record of that 01:55:22
7 conversation. 01:55:26

8 And so we talk a lot of times about NetFlow being 01:55:28
9 very much like a phone bill; you see who talked to who for 01:55:30
10 how long, but you don't see any of the details in the 01:55:35
11 transaction. You don't see all the packets that move over; 01:55:39
12 you just see the record of the conversation happening. 01:55:41

13 Q. Is there even a specific entry for a given packet? 01:55:44

14 A. No. You could have hundreds or thousands or hundreds of 01:55:49
15 thousands of packets move through a device and have one 01:55:54
16 NetFlow record for that transaction. It's really all about 01:55:57
17 how long the transaction took that the NetFlow record 01:56:00
18 records. 01:56:06

19 Q. In terms of timing, how often would any of these devices 01:56:06
20 send a NetFlow record to some other device? 01:56:11

21 A. It is a configurable option, but generally it's between 01:56:15
22 30 seconds and five minutes for those systems. 01:56:21

23 Q. How long does it take for a packet to reach its 01:56:25
24 destination? 01:56:29

25 A. Much less than one second; milliseconds. 01:56:29

—Scheck, M. - Direct—

1	Q. By the time a NetFlow record is received by something	01:56:34
2	else, where would the packet that is summarized along with	01:56:37
3	other packets -- where would those packets be?	01:56:42
4	A. It would have been delivered, you know, at least 30	01:56:44
5	seconds prior, up to five minutes before, generally.	01:56:47
6	Q. What kinds of devices can send NetFlow information?	01:56:51
7	A. Routers and switches can be set up to export NetFlow.	01:56:59
8	There's also appliances and software that you can deploy on	01:57:06
9	other parts of the network that can generate NetFlow, as	01:57:11
10	well.	01:57:14
11	Q. All right. Do routers or switches receive NetFlow?	01:57:14
12	A. They do not.	01:57:17
13	Q. Is it a one-way street?	01:57:19
14	A. That's correct.	01:57:22
15	Q. Are you familiar with something called syslog,	01:57:23
16	s-y-s-l-o-g?	01:57:27
17	A. I am.	01:57:27
18	Q. What is syslog?	01:57:28
19	A. Syslog is a way to send events off of a system when a	01:57:30
20	particular type of transaction occurs. So if someone logs	01:57:37
21	into a system and runs a command, it will generate a syslog	01:57:40
22	message for that transaction.	01:57:44
23	Q. Are NetFlow and syslog different kinds of logging tools?	01:57:45
24	A. They are different. Syslog, as I mentioned -- you have	01:57:50
25	preconfigured events that send a syslog message. NetFlow is	01:57:55

—Scheck, M. - Direct—

1	sending a record for every single transaction that occurs, so	01:58:00
2	you can't have a conversation or a connection on the network	01:58:04
3	without a NetFlow record.	01:58:06
4	Q. Do you see off to the right there something that says	01:58:07
5	"Stealthwatch"?	01:58:14
6	A. I do.	01:58:15
7	Q. And does Stealthwatch receive NetFlow?	01:58:15
8	A. It does.	01:58:18
9	Q. This syslog you just talked about, does that have	01:58:19
10	anything to do with Stealthwatch?	01:58:23
11	A. It does not.	01:58:24
12	Q. What is Stealthwatch?	01:58:24
13	A. Stealthwatch is a NetFlow collector and NetFlow analysis	01:58:25
14	system. So when you send all of those NetFlow log entries to	01:58:30
15	Stealthwatch, it takes them and it stores them in a format	01:58:34
16	that someone on my team that is doing, say, an investigation	01:58:38
17	or network forensics can go run some inquiries and actually	01:58:42
18	see what systems have talked to other systems as part of that	01:58:48
19	investigation.	01:58:52
20	Q. So who uses Stealthwatch?	01:58:52
21	A. Primarily, information security investigators and	01:58:54
22	information security analysts on my team.	01:59:00
23	Q. Is Stealthwatch used to investigate incidents that	01:59:04
24	already happened?	01:59:06
25	A. It is.	01:59:07

—Scheck, M. - Direct—

1	Q. At Cisco, for example, does any other team at Cisco use	01:59:07
2	Stealthwatch in connection with securing a Cisco network	01:59:11
3	besides you?	01:59:16
4	A. No, it's just the incident response team.	01:59:17
5	Q. Are you familiar with the term "proactive" when it comes	01:59:19
6	to network security?	01:59:22
7	A. Yes.	01:59:23
8	Q. What does that term mean to you?	01:59:23
9	A. To me, "proactive" means that you have a device on your	01:59:25
10	network, and you have created some set of rules or specific	01:59:32
11	event types that that device blocks when that transaction	01:59:41
12	occurs.	01:59:45
13	Q. Is Stealthwatch a proactive tool?	01:59:45
14	A. It cannot be, because it does not live inline with the	01:59:51
15	network. All the packets are sent to it for analysis after	01:59:56
16	the packets have already gone through the devices.	01:59:59
17	Q. And what do you mean when you say it doesn't live inline?	02:00:02
18	A. Meaning it's not -- when the packet flows across this	02:00:05
19	diagram, at no point does it pass through Stealthwatch. It	02:00:12
20	passes through routers and switches that are generating	02:00:15
21	transactions that are sent to Stealthwatch, so Stealthwatch	02:00:19
22	has no way to interact with those packets themselves.	02:00:21
23	Q. Can Stealthwatch filter packets?	02:00:25
24	A. It cannot.	02:00:27
25	Q. Can Stealthwatch block packets as they arrive into the	02:00:28

—Scheck, M. - Direct—

1	network?	02:00:32
2	A. They cannot.	02:00:32
3	Q. Do you have a general understanding of -- let me back up	02:00:33
4	a little bit.	02:00:38
5	You've interacted with various Cisco customers over	02:00:39
6	the last 15 or 20 years, right?	02:00:42
7	A. I have.	02:00:45
8	Q. Do you have a general understanding as to whether or not	02:00:45
9	most Cisco customers who buy routers or switches also buy	02:00:49
10	Stealthwatch?	02:00:54
11	A. I have a pretty good understanding.	02:00:54
12	Q. And what is that understanding?	02:00:58
13	A. The number of people that buy Stealthwatch compared to	02:01:00
14	the number of people that buy Cisco routers and switches is	02:01:04
15	fairly small.	02:01:08
16	If you consider that nearly everyone that has an	02:01:09
17	internet connection -- it's going through a piece of Cisco	02:01:14
18	gear at some point. It's a pretty broad deployment, and	02:01:16
19	Stealthwatch is a much, much smaller number of customers that	02:01:23
20	are really trying to do NetFlow security on large enterprise	02:01:26
21	networks.	02:01:30
22	Q. Are you familiar with the term "forensics" in the context	02:01:30
23	of network security?	02:01:33
24	A. I am.	02:01:35
25	Q. And would you describe Stealthwatch as a -- well,	02:01:35

—Scheck, M. - Direct—

1 actually, let me back up.

02:01:45

2 What does "forensics" mean?

02:01:47

3 A. Forensics, to me, is a way that you can go back and look
4 at historical transactions to determine what actually
5 happened in any given scope.

02:01:48

02:01:51

02:01:55

6 Q. Would you consider Stealthwatch to be a forensic tool?

02:01:57

7 A. I would. Just as you can do disc forensics to determine
8 artifacts off of a system, NetFlow and Stealthwatch is
9 looking at network artifacts to determine what happened on
10 the network.

02:02:00

02:02:07

02:02:11

02:02:14

11 Q. Now, are you familiar with the term "threat
12 intelligence"?

02:02:18

02:02:20

13 A. I am.

02:02:20

14 Q. And, just at a general level, what is threat
15 intelligence?

02:02:21

02:02:24

16 A. The simplest way to explain it is realistically there are
17 bad actors on the internet trying to do bad things. They're
18 trying to break in, steal your stuff, install ransomware,
19 charge you money. Threat intelligence is just a way of
20 describing who those bad people are and what tools they're
21 using, where they're coming from, those types of things.

02:02:25

02:02:30

02:02:34

02:02:38

02:02:41

02:02:45

22 Q. Are you familiar with the idea of a threat intelligence
23 feed?

02:02:48

02:02:50

24 A. Yes.

02:02:50

25 Q. What is a threat intelligence feed?

02:02:51

—Scheck, M. - Direct—

1	A. A threat intelligence feed is a way to transfer that	02:02:53
2	information on an ongoing basis. Here are the malicious	02:02:58
3	actors, here are the tools they're using, here's where	02:03:01
4	they're coming from, et cetera. So all of that is set up in	02:03:04
5	a feed, a stream of information that can be consumed.	02:03:07
6	Q. And what sorts of uses can threat intelligence feeds be	02:03:09
7	put to?	02:03:14
8	A. You can use it for historical forensics. You can look	02:03:14
9	and see, here's the list of everything I know was malicious.	02:03:19
10	Have I had any of that on my network? You can actually	02:03:23
11	deploy it and put it inline and say, I want to block all	02:03:25
12	connections coming from these malicious external sites,	02:03:30
13	et cetera. So it can be preventive, reactive, investigative,	02:03:33
14	et cetera.	02:03:37
15	Q. And how long have threat intelligence feeds been	02:03:37
16	available?	02:03:41
17	A. Well, I started in the incident response team in 2004,	02:03:41
18	and we were using a couple of them in 2004.	02:03:48
19	Q. Can Stealthwatch use threat intelligence feeds as part of	02:03:51
20	its forensic investigation on things that happened before?	02:03:56
21	A. It absolutely can.	02:03:58
22	Q. And we'll get into this in more detail later, but how	02:04:02
23	long has that been the case, that Stealthwatch could use that	02:04:06
24	as part of its forensic investigation?	02:04:09
25	A. When we first purchased Stealthwatch, it was around 2010,	02:04:10

—Scheck, M. - Direct—

1 and we integrated our threat intelligence feeds into the tool 02:04:15
2 itself in 2010. It wasn't part of what it was selling at the 02:04:20
3 time, but in 2013 they actually started including some 02:04:25
4 commercial threat intelligence feeds in the product. 02:04:30

5 So as far back as 2010 and built into the product as 02:04:33
6 an add-on in 2013. 02:04:37

7 Q. And is there any use for threat intelligence feeds in 02:04:39
8 Stealthwatch other than as part of a forensic investigation 02:04:44
9 about a security incident that already happened? 02:04:48

10 A. No. 02:04:51

11 Q. Let's get back again to some other parts of Stealthwatch. 02:04:52

12 What does Stealthwatch do when it receives NetFlow 02:05:00
13 records? 02:05:03

14 A. The first thing it does is it actually pulls all of the 02:05:03
15 information out of the NetFlow record and stores it in a 02:05:10
16 database so that it's available for longer periods of time 02:05:13
17 and you can query it. And then, once it's stored in that 02:05:17
18 database, it will also run analytics on it to look for 02:05:21
19 interesting behavior; you know, is one host talking to too 02:05:24
20 many hosts or sending too much data, those types of things. 02:05:28

21 Q. Let's go to the next NetFlow demonstrative -- 02:05:31

22 MR. GAUDET: Which, Your Honor, should be slide 2 in 02:05:35
23 your book. 02:05:38

24 THE COURT: All right. What is the difference 02:05:50
25 between the two? 02:05:53

—Scheck, M. - Direct—

1	MR. GAUDET: There's an exclamation point added, a	02:05:55
2	yellow exclamation point added above "Stealthwatch."	02:05:59
3	THE COURT: I was going to say, it looks like the	02:06:02
4	same one.	02:06:04
5	MR. GAUDET: It almost is.	02:06:05
6	BY MR. GAUDET:	02:06:07
7	Q. The question is what does Stealthwatch do if it detects a	02:06:06
8	possible security event?	02:06:11
9	A. It creates an alarm that is in -- one of two things	02:06:13
10	occur. It either creates an alarm and displays it on a	02:06:21
11	dashboard within Stealthwatch, or, in our case, it creates an	02:06:25
12	alarm and sends it to another tool, where it can be	02:06:28
13	correlated with additional data.	02:06:31
14	MR. GAUDET: And, Your Honor, the exclamation point	02:06:34
15	was our effort to represent the presence of an alarm.	02:06:38
16	BY MR. GAUDET:	02:06:43
17	Q. Mr. Scheck, when an alarm goes off, does anything happen	02:06:43
18	without a human responding?	02:06:47
19	A. No, nothing happens.	02:06:48
20	Q. So what can a human do when the human sees that	02:06:50
21	Stealthwatch has set off an alarm?	02:06:55
22	A. They can essentially correlate the data from the alarm,	02:06:57
23	data from other systems, or they can log in to Stealthwatch	02:07:05
24	and view more information around the NetFlow record itself.	02:07:08
25	Q. Are these all part -- go ahead.	02:07:08

—Scheck, M. - Direct—

1 A. That's all part of an investigation that's going to occur 02:07:18
2 to determine is this really a legitimate alarm, or is it 02:07:21
3 something that I can ignore? 02:07:24

4 Q. And how often, for example, does Cisco check to see if 02:07:26
5 Stealthwatch has produced alarms? 02:07:39

6 A. Generally, the way it works in our configuration is an 02:07:41
7 alarm is sent from Stealthwatch to our central system that 02:07:46
8 stores data from the -- 02:07:50

9 MS. LEE: Your Honor, I'm sorry to interrupt, but 02:07:53
10 this witness has testified at deposition that he has no 02:07:55
11 knowledge of the development of the products and engineering. 02:07:58
12 He's not on the engineering side, and they're trying to sneak 02:08:01
13 in and backdoor technical testimony with this witness who has 02:08:03
14 no foundation to provide this kind of information. 02:08:08

15 THE COURT: That's a matter to handle on 02:08:14
16 cross-examination. 02:08:17

17 MS. LEE: Okay. Thank you, Your Honor. 02:08:17

18 BY MR. GAUDET: 02:08:20

19 Q. Mr. Scheck, do you have a basis to know how Stealthwatch 02:08:21
20 works? 02:08:24

21 A. Well, before Cisco acquired them, I was on the technical 02:08:24
22 advisory board helping them develop -- helping them receive 02:08:30
23 input on what we wanted as a customer. 02:08:34

24 I would say that as a member of the Incident 02:08:37
25 Response Team, it is our responsibility to understand in 02:08:40

—Scheck, M. - Direct—

1 depth how every single tool works. I may not write the code,
2 but if I don't understand how the alarms work and where they
3 go and when they fire, I'm not able to use the tool
4 effectively.

5 Q. Thank you, sir.

6 To come back to the question -- I think you may have
7 been interrupted -- how often does the Cisco team actually
8 look to see if Stealthwatch has fired some alarms?

9 A. Generally, our analysts will, once an hour, look through
10 all of the reports that come out of a tool like Stealthwatch,
11 aggregate them, look at them in bulk, and perform
12 investigative functions on those; so on an hourly basis.

13 Q. Now, about what percentage of the alarms that
14 Stealthwatch sends to your team actually turn out to be a
15 security event that is worthy of some sort of remedial
16 action?

17 A. It's about 1 out of 100, in our situation, and that's
18 because we've taken a lot of time to only turn on the alarms
19 that are relevant and do a great deal of tuning.

20 If you were to install it and, you know, not go
21 through those recommended actions, it would probably be more
22 on the realm of 1 in 1,000 or 1 in 10,000.

23 Q. Based on your interactions with Cisco's customers that
24 you deal with, do you expect that Cisco's customers handle
25 Stealthwatch alarms in a similar fashion as you just

—Scheck, M. - Direct—

1 described? 02:10:21

2 A. Yes, very much so. They've found that that's the only 02:10:21
3 way that they can really get the right signal-to-noise ratio 02:10:23
4 from it. 02:10:29

5 Q. Now, let's talk about -- the alarm comes in, an 02:10:30
6 investigation is done, the team decides that we need to do 02:10:34
7 something about it, okay? What are the tools available to 02:10:37
8 your team to actually take action based on a Stealthwatch 02:10:40
9 alarm? 02:10:45

10 A. The most common thing that an analyst will do is actually 02:10:45
11 submit a host for reimaging, meaning it looks like this 02:10:50
12 person's laptop is infected. Let's open up a case with the 02:10:55
13 help desk. The help desk will send someone to their desk and 02:11:00
14 work with them to get their system reimaged and cleaned. 02:11:04

15 They can also do things like -- 02:11:09

16 Q. Let me just stop you there. 02:11:12

17 Do you mean literally specifically take their 02:11:14
18 computer and like wipe off and recreate the system with brand 02:11:16
19 new software that's not been infected? 02:11:19

20 A. That's correct. 02:11:21

21 MS. LEE: Objection, Your Honor. That was leading. 02:11:23

22 THE COURT: Yes, it certainly was leading. 02:11:26

23 MR. GAUDET: I apologize. 02:11:29

24 BY MR. GAUDET: 02:11:30

25 Q. Let me just ask, what do you mean by "reimage"? 02:11:31

—Scheck, M. - Direct—

1 A. Yeah, reimaging is a process where generally what happens 02:11:34
2 is the user performs a full backup of their system. The help 02:11:38
3 desk technician will come to their desk after that backup is 02:11:44
4 completed, they will wipe the laptop or the desktop system, 02:11:48
5 install a fresh set of software from either Microsoft or 02:11:53
6 Apple, whoever the vendor is for that computer, and then 02:11:59
7 they'll go restore the backup. 02:12:02

8 So to the user it takes several hours, but it's as 02:12:04
9 little interruption as possible to their flow of work. They 02:12:09
10 have their files back after that's done. 02:12:13

11 Q. What are some of the other tools that are available if 02:12:14
12 the human analyst decides that the alarm is worthy of 02:12:17
13 remedial action? 02:12:21

14 A. They can also -- if it looks more severe, they can issue 02:12:22
15 what is called a BGP, a Border Gateway Protocol, Black Hole, 02:12:29
16 which is a nice way of saying we're going to push a config to 02:12:36
17 all the routers that doesn't let you talk to anyone else on 02:12:39
18 the network. So you can isolate them as a result of an 02:12:43
19 alarm, as well. 02:12:47

20 Q. And what are some other options? 02:12:47

21 A. You can pick up a phone call and talk to the user. That 02:12:49
22 also happens. 02:12:53

23 The most common one is certainly the reimaging their 02:12:55
24 system. Although it has a little bit of impact to the 02:13:01
25 end-user, it's the best way to be certain that the threat is 02:13:05

—Scheck, M. - Direct—

1 removed.

02:13:10

2 Q. Can you quarantine a user?

02:13:10

3 A. We don't really quarantine today.

02:13:11

4 Q. And why is that?

02:13:14

5 A. It's -- I suppose the simplest way to state it is doing a

02:13:15

6 quarantine can be very complicated from an ACL management

02:13:22

7 point of view, from an Access Control List management point

02:13:28

8 of view. It's overly complicated. It's much simpler to do

02:13:31

9 something like push the BGP route and not let them talk to

02:13:36

10 anyone, versus trying to figure out who they can and can't

02:13:42

11 talk to and try to enforce all that.

02:13:46

12 MR. GAUDET: Your Honor, did you have a question?

02:13:49

13 THE COURT: No.

02:13:50

14 MR. GAUDET: Okay. I apologize.

02:13:51

15 BY MR. GAUDET:

02:13:52

16 Q. Mr. Scheck, do you have a sense from your interactions

02:13:53

17 with Cisco's customers as to whether Cisco's customers have

02:13:55

18 the same experience in terms of not typically quarantining in

02:14:00

19 response to a Stealthwatch alarm that is worthy of

02:14:04

20 remediation?

02:14:08

21 A. Certainly, the conversations I've had with the customers

02:14:09

22 have been very in line with my experience here at Cisco, as

02:14:13

23 well.

02:14:19

24 Q. Okay. Now, let's talk about timing.

02:14:19

25 From the time that Stealthwatch receives an alarm to

02:14:21

—Scheck, M. - Direct—

1 the time that you take any of these various remedial steps, 02:14:25
2 what is kind of the average amount of time that has passed? 02:14:29

3 A. Well, if you go through the whole flow, a transaction 02:14:33
4 occurs, and you have between 30 seconds and five minutes for 02:14:39
5 a NetFlow record to be generated. So that goes into 02:14:43
6 Stealthwatch. Stealthwatch runs some analytics. It may take 02:14:46
7 a few seconds, 10 seconds. So now you're 40 seconds or a 02:14:51
8 little over five minutes. And then it goes to an analyst, 02:14:55
9 and that means that an hour later an analyst runs a report 02:14:59
10 that includes that alert. 02:15:03

11 They have to spend some time actually performing 02:15:05
12 analysis of it, looking to see does this really look like 02:15:07
13 something crazy happened, and that can take up to another 02:15:10
14 hour. So you're talking about, you know, two hours and ten 02:15:14
15 minutes from the point in time something happened, you're 02:15:16
16 opening a help desk ticket, or -- which, again, is the most 02:15:19
17 common, so we'll stick with it. 02:15:24

18 You're opening a help desk ticket. It can take 02:15:26
19 another day for the help desk technician to set up an 02:15:29
20 appointment, to get the backup done, go wipe the system, 02:15:32
21 restore all the files, and have the person up and running. 02:15:35
22 So it can easily be 24 to 36 hours from the time the event 02:15:38
23 actually occurred until the time it's remediated. 02:15:45

24 Q. We're going to shift gears just a little bit. Let's go 02:15:47
25 to slide 3 of the Stealthwatch demonstrative. 02:15:50

—Scheck, M. - Direct—

1	MR. GAUDET: Your Honor, this should be a little	02:15:54
2	more added to it.	02:15:56
3	BY MR. GAUDET:	02:15:58
4	Q. Mr. Scheck, do you see there's something called Cognitive	02:15:58
5	Threat Analytics added to this slide?	02:16:02
6	A. Yes, I see that.	02:16:03
7	Q. When did Cisco start using Cognitive Threat Analytics as	02:16:04
8	a standalone product?	02:16:07
9	A. In 2013.	02:16:08
10	Q. Where did that product come from?	02:16:10
11	A. Cisco acquired a company that was simply referred to as	02:16:13
12	Cognitive, in Prague, the Czech Republic, and it was a bunch	02:16:18
13	of university students and professors who left to do a	02:16:27
14	startup based on machine learning and artificial	02:16:30
15	intelligence.	02:16:33
16	Q. Is Cognitive Threat Analytics based on NetFlow?	02:16:34
17	A. It is.	02:16:39
18	Q. And is it another tool that Stealthwatch can use?	02:16:40
19	A. It is.	02:16:44
20	Q. Okay. What does Cognitive Threat Analytics add to sort	02:16:46
21	of the Stealthwatch investigative arsenal, if you will?	02:16:51
22	A. Sure. So when I talked about Stealthwatch being able to	02:16:54
23	run some analytics on the behavior that's happened on	02:17:00
24	network, the Cognitive Threat Analytics engine does more of	02:17:05
25	that, but it does it with larger sets of data and more	02:17:10

—Scheck, M. - Direct—

1 intelligence, I suppose is the best way to put it. So it's
2 adding the machine learning and AI piece to the analysis
3 function, versus more basic algorithms built into
4 Stealthwatch.

5 Q. You used the acronym AI. What do you mean by that?

6 A. Artificial intelligence.

7 Q. And, if you would, just describe your understanding of
8 the words "machine learning" and "artificial intelligence" so
9 we're all on the same page.

10 A. Yeah. It's not crazy science fiction stuff. At its most
11 basic level, there are differential algorithms to organize
12 and classify data and look for things that don't fall into
13 those buckets that machine learning and AI have created and
14 allow decisions to be made based on whether or not something
15 falls into one of those categories or not.

16 Q. Timing-wise, if Cognitive Threat Analytics is part of the
17 equation, what does that do to the amount of time before an
18 alert gets sent?

19 A. Generally, it takes a period of time, around 10 minutes
20 for the Stealthwatch system, to actually send the alert to
21 Cognitive, and then Cognitive, going through all of those
22 AI/machine learning algorithms, takes another two to four
23 hours, in general. So I've certainly seen cases that took
24 over 24 hours for an alert to come after it was received from
25 Cognitive.

—Scheck, M. - Direct—

1 Q. Does Cisco ever take an action based only on a Cognitive 02:18:43
2 Threat Analytics alarm? 02:18:48

3 A. No. We treat it just like every other Stealthwatch 02:18:48
4 alarm, and it follows the same process for analysis. 02:18:51

5 Q. And based on your experience and interaction with Cisco's 02:18:55
6 customers, do you have an understanding of whether Cisco's 02:18:58
7 customers would take an action, normally, based only on a 02:19:01
8 Cognitive Threat Analytics alarm? 02:19:05

9 A. No, I think the customers I've spoke to are very much 02:19:07
10 aligned with our process, as well. 02:19:11

11 Q. And then, just generally speaking, over the course of the 02:19:12
12 last three years, about how many alarms has Stealthwatch 02:19:16
13 alerted Cisco about where it turned out it was actually a 02:19:22
14 meaningful security incident that needed to be remediated? 02:19:27

15 A. Alarms from Cognitive specifically? 02:19:32

16 Q. Stealthwatch overall. 02:19:36

17 A. From Stealthwatch overall, there's been thousands of 02:19:39
18 alarms that have come in and have -- that led to an 02:19:44
19 investigation that was, in fact, a true positive, is what we 02:19:48
20 would call it when there's an incident. 02:19:53

21 Q. And then in about that same period of time, how many 02:19:55
22 times has Cognitive Threat Analytics dispersed a uniquely 02:19:59
23 identified threat that turned out to need remediation? 02:20:06

24 A. Yeah. I think when I went back and looked for three 02:20:09
25 years, there were 792 alarms from Cognitive through 02:20:11

—Scheck, M. - Direct—

1	Stealthwatch, and only three of those were true positives.	02:20:15
2	Q. Let's now turn to Encrypted Traffic Analytics. And this	02:20:20
3	will be slide 4.	02:20:29
4	Are you familiar...	02:20:29
5	A. Am I familiar with ETA? Yes, I am.	02:21:00
6	Q. No, Mr. Scheck, I'm -- given that it's a Zoom trial,	02:21:02
7	we're all trying to be sure that everybody can do what they	02:21:06
8	need to do, and I wanted to be sure the Judge had the	02:21:09
9	opportunity to...	02:21:09
10	MR. GAUDET: Your Honor, may I proceed?	02:21:13
11	THE COURT: Yes.	02:21:14
12	MR. GAUDET: Thank you.	02:21:15
13	BY MR. GAUDET:	02:21:15
14	Q. Mr. Scheck, are you familiar with Encrypted Traffic	02:21:16
15	Analytics?	02:21:20
16	A. I am.	02:21:20
17	Q. Okay. And does the figure 4 demonstrative here show a	02:21:21
18	NetFlow that includes information called for by Encrypted	02:21:27
19	Traffic Analytics?	02:21:33
20	A. It does.	02:21:33
21	Q. Okay. Now, is Encrypted Traffic Analytics based on	02:21:34
22	NetFlow?	02:21:40
23	A. It is.	02:21:40
24	Q. And what does -- let's start from the perspective of the	02:21:42
25	gateway or router, okay?	02:21:47

—Scheck, M. - Direct—

1 What does Encrypted Traffic Analytics add to NetFlow 02:21:50
2 that wasn't there already? 02:21:55

3 A. There are a few additional fields that ETA will actually 02:21:56
4 add to the NetFlow record, around timing and packet size and 02:22:04
5 a couple of other features that are not part of that 02:22:07
6 normal -- this system talked to this system for this long. 02:22:13
7 So it just injects a little bit more session information. 02:22:16

8 Q. Other than adding those two fields -- or few fields of 02:22:20
9 information to the NetFlow record, does the gateway or router 02:22:25
10 do anything else relating to -- 02:22:28

11 MS. LEE: Objection, Your Honor. This is leading. 02:22:31

12 THE COURT: I don't think that was leading. 02:22:36

13 You can answer the question. 02:22:39

14 BY MR. GAUDET: 02:22:44

15 Q. Mr. Scheck, you can answer the question or let me know if 02:22:45
16 you need me to repeat it. 02:22:47

17 A. No, there's nothing else the routers and switches are 02:22:48
18 doing from a NetFlow point of view or from an ETA point of 02:22:51
19 view. 02:22:55

20 Q. And, again, even if it's sending ETA information, is this 02:22:55
21 just a one-way street from the gateway or router to 02:22:59
22 Stealthwatch? 02:23:03

23 A. That's correct, the transport is exactly the same; it's 02:23:03
24 over NetFlow to Stealthwatch. 02:23:07

25 Q. Can Stealthwatch send anything about ETA back to the 02:23:09

—Scheck, M. - Direct—

1 gateway or router?

02:23:12

2 A. They cannot.

02:23:14

3 Q. Now, what does Encrypted Traffic Analytics do with that
4 information up in Stealthwatch?

02:23:14

02:23:23

5 A. So, essentially, it performs all of the same analytics on
6 the NetFlow that it normally does. It also sends some of the
7 data off to the Cognitive cloud that we talked about for
8 additional machine learning and AI analytics.

02:23:24

02:23:31

02:23:35

02:23:40

9 But, on top of that, there is some additional sets
10 of algorithms, again based on machine learning and AI, that
11 are looking for interesting and notable cryptographic detail
12 in the flows.

02:23:43

02:23:48

02:23:52

02:24:01

13 Q. Now is Encrypted Traffic Analytics just a component of
14 Stealthwatch?

02:24:05

02:24:08

15 A. Encrypted Traffic Analytics lives outside of Stealthwatch
16 on the analytics side.

02:24:08

02:24:17

17 Q. Okay. And in order to access that analytics, does the
18 user have to have Stealthwatch?

02:24:18

02:24:23

19 A. They do.

02:24:25

20 Q. Okay. Does the user who has Stealthwatch also have to
21 specially enable Encrypted Traffic Analytics?

02:24:26

02:24:34

22 A. They do.

02:24:37

23 Q. Now, if a user doesn't have Stealthwatch, can they get
24 any benefit whatsoever out of Encrypted Traffic Analytics?

02:24:38

02:24:42

25 A. They cannot.

02:24:45

—Scheck, M. - Direct—

1 Q. And if a user -- let's talk about enabling. 02:24:46

2 What does it mean to enable Encrypted Traffic 02:24:51

3 Analytics? 02:24:54

4 A. Essentially, you have to have a router or switch with a 02:24:54

5 version of software that supports turning on Encrypted 02:24:59

6 Traffic Analytics, and then you have to make some config 02:25:03

7 changes and send your NetFlow data, once it's been configured 02:25:06

8 correctly, to the Stealthwatch from the device. 02:25:12

9 Q. Continue, Mr. Scheck. 02:25:15

10 A. You also have to make sure that on the Stealthwatch side 02:25:16

11 you have the connection to Cognitive, CTA, set up and that's 02:25:19

12 working correctly, as well, for that to work. 02:25:23

13 Q. So let's go to the next slide. 02:25:25

14 And this now adds Cognitive Threat Analytics back 02:25:28

15 into the picture. Do you see that? 02:25:32

16 A. I do. 02:25:34

17 Q. Does Cognitive Threat Analytics have a role with 02:25:35

18 Encrypted Traffic Analytics? 02:25:39

19 A. It does. 02:25:40

20 Q. If you would, explain that. 02:25:40

21 A. Cognitive Threat Analytics, the cloud that all of the 02:25:46

22 machine learning and AI processing takes place in for all of 02:25:48

23 the NetFlow traffic that Stealthwatch sends to CTA, it's the 02:25:53

24 same cloud that does the analytics for Encrypted Traffic 02:25:56

25 Analytics. 02:26:02

—Scheck, M. - Direct—

1 Q. Because of that, can Cisco determine how many of its 02:26:02
2 customers are actually using Encrypted Traffic Analytics? 02:26:08

3 A. Yes, absolutely. You could look in the CTA cloud and 02:26:14
4 you'd be able to see who was actually submitting NetFlow for 02:26:20
5 analysis to CTA. 02:26:24

6 Q. Okay. Now, with respect to sort of the proprietary part 02:26:26
7 of Encrypted Traffic Analytics, sort of the things that Cisco 02:26:32
8 considers to be its intellectual property that it protects, 02:26:35
9 where is that? Where would that be? 02:26:39

10 A. It lives in the Cognitive cloud. 02:26:41

11 Q. Okay. What about that software back on the gateway or 02:26:45
12 router that allows you to add two more fields to the NetFlow 02:26:49
13 in the one-way street to Stealthwatch? Is that something 02:26:53
14 that Cisco shares publicly? 02:26:57

15 A. It is. There's actually an open-source project called 02:26:59
16 Joy, where the author of ETA has released the software that 02:27:05
17 generates the extra fields publicly. 02:27:10

18 Q. And that means -- I'm sorry. Could someone, for example, 02:27:14
19 just anyone on the internet, then -- would they be able to 02:27:18
20 literally get the software relating to ETA that's on the 02:27:21
21 gateways and routers? 02:27:25

22 A. That's correct. It's open to everyone, and there's no 02:27:27
23 charge. It's meant to be shared. 02:27:30

24 Q. And why does Cisco do that? 02:27:32

25 A. Cisco does it with quite a bit of software. I think the 02:27:40

—Scheck, M. - Direct—

1	idea there is there's things that add value to Cisco	02:27:44
2	products, and there's things that build trust and build	02:27:51
3	relationships with our customers and the general public, and,	02:27:58
4	you know, a lot of our products are actually open-source	02:28:01
5	products.	02:28:07
6	Q. Okay. And with respect to the really core part of	02:28:07
7	Encrypted Traffic Analytics that Cisco protects and is proud	02:28:17
8	of, is that the machine learning part?	02:28:22
9	A. It is. It's the machine learning, the AI, the	02:28:25
10	algorithms, that take all of the data and are able to process	02:28:29
11	it in a way to say something interesting has happened.	02:28:33
12	Q. And where is that located?	02:28:37
13	A. That's located in the cloud, in the Cognitive cloud,	02:28:38
14	specifically.	02:28:44
15	Q. And physically where is -- I know we talk about the	02:28:45
16	cloud, but obviously somewhere there's a physical device.	02:28:49
17	Where is that physical device that does this?	02:28:52
18	A. It actually lives in AWS's cloud now. I think -- you	02:28:55
19	know, rewinding to when we first acquired Cognitive, they had	02:29:01
20	their own data center that it lived in, and they've been	02:29:04
21	slowly shifting that to AWS.	02:29:08
22	Q. What is AWS?	02:29:12
23	A. Amazon Web Services.	02:29:13
24	Q. And what kind of service does Amazon Web Services	02:29:15
25	provide?	02:29:18

—Scheck, M. - Direct—

1 A. They give you a way to basically store data and run 02:29:19
2 servers in an elastic infrastructure. So as there's more or 02:29:23
3 less power required, you can expand and shrink your cloud 02:29:30
4 footprint very easily. 02:29:35

5 THE COURT: Wait a minute, here. AWS, that's Amazon 02:29:37
6 Web Services? Is that what you said? 02:29:43

7 THE WITNESS: Yes, Your Honor. 02:29:49

8 THE COURT: So Amazon Web Services was the cloud 02:29:51
9 where you stored Cognitive Threat Analytics when you first 02:29:56
10 got it, but you now store it in your own network? Is that 02:30:04
11 what you're saying? 02:30:09

12 THE WITNESS: It's the opposite, Your Honor. When 02:30:10
13 we first acquired them, we had a data center on our own 02:30:12
14 network. And it's more cost efficient to store that in AWS's 02:30:16
15 cloud now, so it's been migrating from what we call an 02:30:22
16 on-prem data center, one that we physically control, to a 02:30:26
17 virtual data center in the cloud. 02:30:31

18 THE COURT: All right. So it's out of your system 02:30:38
19 and into the Amazon cloud? 02:30:39

20 THE WITNESS: Yes, Your Honor. 02:30:41

21 BY MR. GAUDET: 02:30:46

22 Q. Now -- 02:30:47

23 THE COURT: Wait a minute. 02:30:48

24 MR. GAUDET: Sorry. 02:30:48

25 (There was a pause in the proceedings.) 02:30:48

—Scheck, M. - Direct—

1 THE COURT: Okay. 02:31:01

2 MR. GAUDET: Thank you, Your Honor. 02:31:03

3 BY MR. GAUDET: 02:31:04

4 Q. Mr. Scheck, do you recall we talked about the notion of a 02:31:04

5 proactive tool versus a forensic tool and we only had 02:31:09

6 Stealthwatch up on the screen? 02:31:12

7 A. Yes. 02:31:13

8 Q. Okay. Now, Stealthwatch, whether it includes Encrypted 02:31:14

9 Traffic Analytics or Cognitive Threat Analytics, or both, any 02:31:20

10 of those things, can any one of those things be proactive? 02:31:24

11 A. They cannot be proactive. The packets have been 02:31:28

12 delivered long before any analysis takes place. And that's 02:31:32

13 just not the definition of "proactive," that's the definition 02:31:35

14 of "reactive" or "investigative." 02:31:38

15 Q. Let's go to a final demonstrative slide. This is 02:31:42

16 slide 6. I'll wait just one minute. 02:31:52

17 THE COURT: Where are we now? This is another 02:32:04

18 slide? 02:32:09

19 MR. GAUDET: This is the last demonstrative slide. 02:32:10

20 It's number 6. It should be in the same tab in your binder, 02:32:13

21 Your Honor. 02:32:18

22 THE COURT: All right. 02:32:20

23 BY MR. GAUDET: 02:32:21

24 Q. Now, Mr. Scheck, do you see that there's something called 02:32:21

25 Identity Services Engine that's been added up in the top of 02:32:25

—Scheck, M. - Direct—

1	the "Management Devices" section?	02:32:28
2	A. I do.	02:32:31
3	Q. Does your team -- let me ask.	02:32:31
4	Are you familiar with the Identity Services Engine?	02:32:33
5	A. I am.	02:32:36
6	Q. And does your team use the Identity Services Engine?	02:32:36
7	A. We do.	02:32:39
8	Q. What are the core functions of the Identity Services	02:32:40
9	Engine?	02:32:46
10	A. The core function for Identity Services is essentially to	02:32:46
11	deliver what we call network access control. It decides who	02:32:53
12	can access the network and who cannot, and it also ties an	02:32:59
13	identity to a system and to a network address. So it is a	02:33:04
14	useful tool for our team, from that point of view.	02:33:11
15	Q. Does it also control wireless access?	02:33:14
16	A. It does.	02:33:17
17	Q. And what about something called network segmentation?	02:33:18
18	A. There is network segmentation that it delivers, as well.	02:33:23
19	Q. Okay. Any of the things that you've mentioned so far,	02:33:28
20	are any of those the same as quarantining?	02:33:32
21	A. No. The definition for "quarantine" differs.	02:33:34
22	Q. Does Cisco use the Identity Services Engine to quarantine	02:33:41
23	people?	02:33:46
24	A. We do not.	02:33:46
25	Q. Is the function of quarantining the core function of the	02:33:48

—Scheck, M. - Direct—

1	Identity Services Engine?	02:33:53
2	A. It's not.	02:33:54
3	Q. What does Cisco use to quarantine people when it chooses	02:33:56
4	to do so?	02:34:01
5	A. Generally, we use the protocol that I spoke of earlier,	02:34:02
6	the Border Gateway Protocol, BGP, which we refer to as a	02:34:10
7	Black Hole. It's a routing protocol that it just keeps	02:34:15
8	people from connecting to anyone. Quarantine is much more	02:34:19
9	complicated to deploy.	02:34:24
10	Q. Are you familiar, based on your interactions with	02:34:28
11	customers, with how Cisco's customers who have bought the	02:34:31
12	Identity Services Engine -- what they use it for?	02:34:36
13	A. Again, generally speaking, the customers I speak to are	02:34:39
14	using it the same way that we are and often are coming to us	02:34:45
15	for advice on how they should deploy it, and the advice that	02:34:50
16	they receive is very much the architecture that I spoke of.	02:34:53
17	Q. And that does not include quarantining, correct?	02:34:57
18	A. That is correct.	02:35:01
19	Q. Let me ask you, based on your interactions with	02:35:01
20	customers, are there customers out there who buy Cisco	02:35:07
21	routers and switches who do not buy the Identity Services	02:35:10
22	Engine?	02:35:13
23	A. Absolutely.	02:35:13
24	Q. And do you have a sense of, just generally speaking, if	02:35:15
25	the majority of Cisco customers who buy routers and switches,	02:35:24

—Scheck, M. - Direct—

1 if they have Identity Services Engines? 02:35:28

2 A. Again, because so many people buy routers and switches 02:35:30
3 for so many different purposes -- ISE is really built to 02:35:34
4 provide network access for large enterprises, so things like, 02:35:39
5 you know, Fortune 500 companies, so a lot of people that are 02:35:43
6 outside of those spaces, in the smaller businesses and even 02:35:46
7 medium businesses, they have no need for ISE. 02:35:52

8 Q. Does ISE, Identity Services Engine, does it work with 02:35:55
9 non-Cisco products? 02:35:59

10 A. It does. 02:36:00

11 Q. If you buy Stealthwatch, do you have to also buy the 02:36:01
12 Identity Services Engine to get value out of Stealthwatch? 02:36:08

13 A. Absolutely not. 02:36:10

14 Q. Why is that? 02:36:11

15 A. Because there's nothing about NetFlow that requires 02:36:12
16 Identity Services Engine for the analytics. There are some 02:36:20
17 things that ISE can do that makes -- make the analysis a bit 02:36:22
18 easier when you tie a user to an IP address, but we ran 02:36:29
19 NetFlow for -- we ran Stealthwatch for well over five or six 02:36:33
20 years -- actually, I should say we ran NetFlow for many, many 02:36:39
21 years without using ISE, and we ran Stealthwatch for several 02:36:42
22 years without having ISE deployed and got a tremendous amount 02:36:45
23 of value out of Stealthwatch. 02:36:49

24 Q. Now I'm going to ask the question the other way around. 02:36:51

25 Can you buy the Identity Services Engine, or ISE, 02:36:54

—Scheck, M. - Direct—

1 not buy Stealthwatch, and still get value out of the Identity
2 Services Engine? 02:36:57 02:37:02

3 A. Yeah. I think the most customers that I talk to that 02:37:02
4 have ISE deployed -- many customers I talk to have ISE 02:37:05
5 deployed -- the Identity Services Engine, I should say, don't 02:37:10
6 have Stealthwatch, so certainly that's true. 02:37:13

7 Q. Okay. Now, we're going to go back in time. We're now 02:37:16
8 going to switch to the history a little bit. 02:37:21

9 Now, do you recall testifying that Stealthwatch 02:37:24
10 acquired a company called Lancope? 02:37:30

11 Actually, let me -- are you familiar with a company 02:37:33
12 called Lancope? 02:37:36

13 A. I am. 02:37:38

14 Q. What is Lancope? 02:37:38

15 A. Lancope is the company that originally developed 02:37:39
16 Stealthwatch before it was acquired by Cisco. 02:37:43

17 Q. And when did -- 02:37:45

18 THE COURT: Say that again. 02:37:49

19 THE WITNESS: Yeah. Your Honor, Lancope is the 02:37:51
20 company that built Stealthwatch as a tool, and then Cisco 02:37:55
21 ended up buying that company in 2015. 02:37:59

22 THE COURT: Well, what did they do, buy Stealthwatch 02:38:04
23 from them previously just as a function, and then -- 02:38:08

24 THE WITNESS: Yes, Your Honor. 02:38:12

25 THE COURT: And then they later bought the whole 02:38:13

—Scheck, M. - Direct—

1 company? 02:38:15

2 THE WITNESS: Yes, Your Honor, that's exactly right. 02:38:16

3 THE COURT: Okay. Well, we're going to take a 02:38:18
4 recess for 15 minutes, and we'll just add 15 minutes onto the 02:38:20
5 end of the day. 02:38:25

6 During the break, you should not do anything to 02:38:28
7 improve your knowledge of your testimony. You should return 02:38:34
8 to testify with exactly the same level of knowledge as you 02:38:40
9 have at this point. 02:38:44

10 (Recess from 2:39 p.m. to 2:53 p.m.) 02:39:30

11 THE COURT: All right. You may resume, Mr. Gaudet. 02:53:26

12 MR. GAUDET: Thank you, Your Honor. 02:53:29

13 And before we resume with the questioning, I just 02:53:30
14 wanted to move into evidence DTX-693, Bates pages 1, 2, and 02:53:32
15 4. 02:53:40

16 THE COURT: You went through the whole thing, didn't 02:53:41
17 you, I think? 02:53:43

18 MR. GAUDET: I went through every page that was in 02:53:44
19 your binder, but it's a bigger presentation, and we didn't 02:53:46
20 want to overwhelm you with paper. But it's all three of the 02:53:49
21 ones that were in your binder, Your Honor. 02:53:52

22 THE COURT: Well, for the record, 693 -- there 02:53:54
23 aren't any numbers on it, so how do we identify it for the 02:54:14
24 record? You've got six charts in there? 02:54:30

25 MR. GAUDET: Your Honor, I apologize. This is not 02:54:48

—Scheck, M. - Direct—

1 the demonstrative, this is DTX-693, which was Mr. Scheck's
2 presentation to NATO. I just hadn't moved that into
3 evidence.

4 THE COURT: Right, 693.

5 MR. GAUDET: Yes, Your Honor. 693 should be the
6 three pages that we went through, 1, 2, 4.

7 THE COURT: All right. 693 will be admitted.

8 (Defense Exhibit DTX-693 was received in evidence.)

9 MR. GAUDET: And then we also want to move in 693.1,
10 which is the metadata.

11 THE COURT: That will be admitted, as well.

12 (Defense Exhibit DTX-693.1 was received in
13 evidence.)

14 MR. GAUDET: Thank you, Your Honor.

15 BY MR. GAUDET:

16 Q. Mr. Scheck, when did you first start using Stealthwatch?

17 A. 2010.

18 Q. And in 2010 how were you using Stealthwatch?

19 A. We were essentially testing it out as a NetFlow analysis
20 solution for Cisco.

21 Q. What do you mean by "NetFlow analysis solution"?

22 A. Meaning we had NetFlow deployed throughout Cisco and were
23 storing it and running queries against it to look for
24 activity. But it wasn't the most efficient tool, and it was
25 taking a lot of work to support it, so we were looking for a

—Scheck, M. - Direct—

1 commercial tool to do that work for us. 02:56:46

2 Q. Okay. And then did Lancope have a -- actually, let me 02:56:48
3 back up. 02:56:58

4 At that time in 2010, as part of the forensic 02:56:59
5 investigation that Cisco would perform with Stealthwatch, did 02:57:05
6 Cisco have threat intelligence feeds fed into Stealthwatch? 02:57:11

7 A. We did. 02:57:16

8 Q. And, if you could, explain how that was the case. 02:57:18

9 A. We had several threat intelligence feeds from different 02:57:22
10 third parties and some Cisco threat intelligence feeds that 02:57:26
11 we would essentially use an API, a way to programmatically 02:57:31
12 load that information into Stealthwatch. 02:57:38

13 Q. I'm going to slow you down for one second. 02:57:40

14 If you could, tell the Court what an API is. 02:57:42

15 A. Yeah. An API is a way to programmatically access 02:57:46
16 something. So, in simple terms, you write a -- you write a 02:57:52
17 program to use features on another program with a set of 02:57:59
18 variables. It's a language that these computers can speak to 02:58:09
19 transfer different information. 02:58:14

20 Q. And -- 02:58:15

21 THE COURT: API is not on my list of definitions. 02:58:16
22 What do those three letters stand for? 02:58:20

23 THE WITNESS: It's Application Programmatic 02:58:22
24 Interface, if I remember correctly. 02:58:30

25 THE COURT: Application Programmatic -- what? 02:58:32

—Scheck, M. - Direct—

1 THE WITNESS: Interface. It's probably been, you 02:58:41
2 know, 15 years since I've thought about what "API" stood for, 02:58:45
3 so I may be wrong, but I believe that's it. 02:58:49

4 THE COURT: All right. I understand why it's not on 02:58:51
5 my list. 02:58:55

6 BY MR. GAUDET: 02:58:59

7 Q. Mr. Scheck, if you could, explain. In 2010, what was the 02:59:01
8 use that Cisco made of threat intelligence feeds in 02:59:07
9 Stealthwatch as part of its forensic investigation into 02:59:13
10 security events? 02:59:17

11 A. Yeah. Essentially, it was one of the simplest forms of 02:59:18
12 threat intelligence, which are IP addresses. We were taking 02:59:24
13 IP addresses that we were receiving from several different 02:59:29
14 threat intelligence feeds, loading them into Stealthwatch, 02:59:32
15 and then anytime we received a flow from somewhere in the 02:59:35
16 network that matched one of the IP addresses on the feeds 02:59:39
17 that we received, it would create an alarm, which would be 02:59:42
18 analyzed by the method I described earlier. 02:59:45

19 Q. And from the very beginning, with Stealthwatch in 2010, 02:59:49
20 was Stealthwatch ever a proactive tool? 02:59:54

21 A. It was not. 02:59:57

22 Q. Why not? 02:59:59

23 A. Because the architecture has been the same since 2010. 02:59:59
24 It has always been a NetFlow consumption tool, and it has 03:00:04
25 never been inline in a way to actually be preventative. 03:00:09

—Scheck, M. - Direct—

1 Q. Has it ever received packets? 03:00:13

2 A. It has not. 03:00:16

3 Q. Did there come a time when Lancope actually integrated a 03:00:17
4 threat intelligence feed into its commercial Stealthwatch 03:00:27
5 product? 03:00:30

6 A. It did. 03:00:30

7 Q. And when was that? 03:00:32

8 A. It was 2013. We were still a customer. It was before 03:00:33
9 Cisco had acquired Lancope, and they integrated a feed called 03:00:38
10 SLIC, S-L-I-C, which was -- I actually don't remember what it 03:00:44
11 stood for, but it was Stealthwatch Labs -- was the first part 03:00:52
12 of it -- and that was essentially exactly what we were doing 03:00:55
13 in 2010. But they built it into their product and sold it to 03:01:00
14 all of their customers so you didn't have to do any of your 03:01:05
15 own programming. 03:01:09

16 Q. Was there a particular version number that was associated 03:01:10
17 with that change? 03:01:12

18 A. I do remember it was 6.3. 03:01:14

19 THE COURT: It was what? 03:01:18

20 THE WITNESS: Version 6.3, Your Honor. 03:01:19

21 THE COURT: When did you leave Lancope and come with 03:01:31
22 Cisco? 03:01:36

23 THE WITNESS: So, Your Honor, I was at Cisco the 03:01:37
24 whole time, but we were buying the equipment from Lancope. 03:01:40

25 THE COURT: Oh, you bought the equipment in 2010, 03:01:46

—Scheck, M. - Direct—

1 and you bought Lancope in 2013? 03:01:48

2 THE WITNESS: In 2015, Your Honor. 03:01:50

3 THE COURT: 2015? 03:01:53

4 THE WITNESS: Yes, Your Honor. 03:01:55

5 So there were multiple purchases from Lancope. The 03:02:00

6 first one was in 2010. The second one was in 2013, and those 03:02:03

7 were us buying the product to protect Cisco. And then in 03:02:09

8 2015, Cisco, as a company, bought Lancope, as a company, 03:02:13

9 which made it cheaper for me to get the product. 03:02:19

10 THE COURT: Well, you never did work for Lancope. I 03:02:26

11 guess I got that confused. 03:02:31

12 THE WITNESS: No, Your Honor. I've worked for Cisco 03:02:33

13 for the last 20 years but have been using the product from 03:02:35

14 Lancope as part of that. 03:02:39

15 THE COURT: All right. 03:02:41

16 BY MR. GAUDET: 03:02:41

17 Q. Mr. Scheck, even before Cisco bought the company Lancope, 03:02:44

18 was Cisco reselling the Stealthwatch product to Cisco's 03:02:48

19 customers? 03:02:51

20 A. For two years before Cisco acquired Lancope, they worked 03:02:52

21 out a partnership, and Cisco was reselling the equipment. 03:02:58

22 The reason for that was very simple. If you were buying 03:03:05

23 Stealthwatch equipment, it meant that you had to turn on more 03:03:11

24 NetFlow, which meant, hopefully, you were using Cisco routers 03:03:17

25 and switches for that. So it was a good relationship for us. 03:03:21

—Scheck, M. - Direct—

1 Q. If we could, pull up DTX-729. 03:03:25

2 MR. GAUDET: Your Honor, this should be in your 03:03:39
3 booklet. 03:03:40

4 THE COURT: That's the last one? 03:03:45

5 MR. GAUDET: That's the last one, Your Honor. 03:03:47

6 THE COURT: That's a good sign. 03:03:49

7 MS. LEE: Your Honor, I would just like to note -- I 03:03:51
8 may not have an objection to this, but the exhibit that was 03:03:54
9 actually DTX-729 is not what's being shown. There are some 03:03:58
10 columns that are missing, and it appears to be some rows that 03:04:03
11 are missing. So I just wanted to note that for the record. 03:04:06

12 MR. GAUDET: And, Your Honor, I can speak to that. 03:04:11

13 DTX-729 is actually an electronic document. It's a 03:04:14
14 native form spreadsheet. If we tried to print the whole 03:04:19
15 thing and put it in your binder, it would be a mountain. And 03:04:24
16 so what we did -- and we disclosed this to the plaintiff 03:04:29
17 already -- we created excerpts, for purposes of this 03:04:32
18 presentation, in paper copy of the relevant parts we want to 03:04:34
19 talk about. Obviously, the plaintiff has the whole thing, 03:04:37
20 and if they think I've left something out, I'm sure I'll hear 03:04:40
21 about it. 03:04:44

22 MS. LEE: The copy we received is only three pages, 03:04:44
23 so unless there was documents or pages that were missing from 03:04:47
24 the version we have, I don't believe it's a mountain. But 03:04:52
25 I'll just reserve my objection and see how the foundation is 03:04:57

—Scheck, M. - Direct—

1 laid for this.

03:05:01

2 THE COURT: Well, it doesn't sound like the entire
3 document was furnished, but what the Court instructed,
4 counsel was to submit the entire document in discovery and
5 then at the trial to only submit that portion of it that they
6 were using, so that the opposing party can add any additional
7 documentation to it.

03:05:09

03:05:13

03:05:21

03:05:28

03:05:34

03:05:45

8 So that's the way the Court instructed it to be
9 handled. That said, let's proceed.

03:05:51

03:05:54

10 MR. GAUDET: Thank you, Your Honor.

03:05:57

11 We did produce the entire document. I think my
12 characterization -- I'm being told by my team it's bigger
13 than this, and it will be messy, but it's not a mountain.
14 It's exactly the document Ms. Lee has.

03:05:58

03:06:01

03:06:05

03:06:10

15 THE COURT: All right.

03:06:13

16 BY MR. GAUDET:

03:06:14

17 Q. Mr. Scheck, have you seen this document, Exhibit DTX-729,
18 before?

03:06:14

03:06:18

19 A. I have.

03:06:18

20 Q. And is this a spreadsheet reflecting sales made by
21 Lancope?

03:06:19

03:06:27

22 A. It is.

03:06:30

23 MS. LEE: Objection, Your Honor. There's no
24 foundation. The witness testified that he never worked at
25 Lancope, so...

03:06:31

03:06:33

03:06:35

~~Scheck, M. - Direct~~

1	MR. GAUDET: I can lay a little more foundation,	03:06:41
2	Your Honor.	03:06:43
3	THE COURT: Well, how do you know this is sales by	03:06:45
4	Lancope?	03:06:51
5	THE WITNESS: From my side, Your Honor, I know that	03:06:52
6	these are sales by Lancope because I have the corresponding	03:06:57
7	records from the Cisco side showing the dates and product	03:07:01
8	versions. And I think all the sales on this spreadsheet --	03:07:04
9	THE COURT: Are these sales from Lancope to Cisco?	03:07:11
10	THE WITNESS: Yes, Your Honor, specifically to my	03:07:13
11	team.	03:07:18
12	THE COURT: So this is what you bought from Lancope?	03:07:19
13	THE WITNESS: Yes, Your Honor.	03:07:21
14	THE COURT: Well, I think that that's sufficient.	03:07:23
15	MR. GAUDET: Thank you.	03:07:28
16	BY MR. GAUDET:	03:07:29
17	Q. Let's highlight rows 17 and 18 in this.	03:07:29
18	MR. GAUDET: And, Your Honor, we can blow these up,	03:07:38
19	as well. I know that the font is kind of small. Just let us	03:07:40
20	know if that would be better.	03:07:43
21	THE COURT: I can read the original document here.	03:07:46
22	MR. GAUDET: Okay, terrific.	03:07:50
23	BY MR. GAUDET:	03:07:53
24	Q. And, Mr. Scheck, what is reflected here in rows 17 and	03:07:54
25	18?	03:07:58

—Scheck, M. - Direct—

1 A. Rows 17 and 18 reflect two of the components required to
2 run Stealthwatch; a flow collector and a management console.

3 Q. And when does the document reflect that Cisco purchased
4 those from Lancope?

5 A. In November of 2010.

6 Q. Is that consistent with your own personal recollection?

7 A. It is.

8 Q. Okay. And then if we now highlight the entire column
9 with the ship date -- and include the top of it there.

10 Mr. Scheck, does this date range correspond with
11 your recollection of sales -- sorry -- purchases that Cisco
12 made from Lancope with respect to Stealthwatch?

13 A. It does.

14 Q. Did this provide you with all of the equipment and
15 software and whatnot that you needed in order to make the use
16 of Stealthwatch that you made with respect to the things that
17 you got from Lancope?

18 A. At that particular point in time, that's correct. We
19 continued to invest and purchase more as we grew, but at that
20 point in time, that was our deployment.

21 Q. Let's go to the second page of this document, and on this
22 one I want to highlight lines 73 to 76.

23 And, sir, what were the dates of these purchases?

24 A. It was April of 2013.

25 Q. And can you identify what the version of the Stealthwatch

—Scheck, M. - Direct—

1	software was that you purchased in 2013?	03:09:53
2	A. It was 6.3.	03:09:56
3	Q. And what does that 6.3 signify?	03:09:59
4	A. It was the third release of version 6. It's significant	03:10:01
5	because 6.3 was the first release that had the Stealthwatch	03:10:09
6	Labs intelligence feed.	03:10:13
7	Q. And was that -- that was the threat intelligence feed	03:10:15
8	that we discussed a moment ago?	03:10:21
9	A. That's correct.	03:10:24
10	MR. GAUDET: Your Honor, we move DTX-729 into	03:10:28
11	evidence.	03:10:32
12	THE COURT: That will be admitted.	03:10:34
13	(Defense Exhibit DTX-729 was received in evidence.)	03:10:35
14	THE COURT: I note it's two pages.	03:10:42
15	MR. GAUDET: That is correct.	03:10:46
16	BY MR. GAUDET:	03:10:48
17	Q. Let's pull up DTX-409.	03:10:48
18	MR. GAUDET: Your Honor, this should be in your --	03:10:52
19	I'm disappointing you by going backwards, but I think we have	03:10:54
20	this one and just a couple more documents, and then we'll	03:11:00
21	shut it down.	03:11:03
22	THE COURT: 409? Yes, I've got 409.	03:11:04
23	MR. GAUDET: Thank you, Your Honor.	03:11:07
24	BY MR. GAUDET:	03:11:09
25	Q. Mr. Scheck, what is Defendant's Trial Exhibit 409?	03:11:10

—Scheck, M. - Direct—

1 A. This is a publicly facing Web page, or blog, that Cisco
2 had written in February of 2014 about our use of Lancope
3 Stealthwatch at Cisco.

4 Q. And, if we could, just blow up sort of the top fifth or
5 so of the document so we can see the February 2014 date.

6 And do you see the document has a February 2014 date
7 on the top?

8 A. I do.

9 Q. And is that consistent with your recollection of when
10 this was made available on Cisco's website?

11 A. Yes.

12 Q. Okay. Now, it says, "Using Lancope Stealthwatch for
13 information security monitoring." Do you see that?

14 A. I do.

15 Q. And, generally speaking, what sorts of things were you
16 describing in this paper about the use of Stealthwatch for
17 information security monitoring?

18 A. We were talking about the size of our deployment, where
19 we had the systems deployed, the benefits of Stealthwatch, as
20 far as being able to look back in time for a longer period
21 than we had been able to with our prior NetFlow analysis
22 tools, and we talked a little bit about using ISE to actually
23 help us identify users on the Cisco network.

24 Q. If you would, turn to -- let's bring up Exhibit -- I'm
25 sorry. Same exhibit, Bates Page 5.

—Scheck, M. - Direct—

1	MR. GAUDET: Your Honor, this should be the third	03:12:56
2	page in your book, ending in .005.	03:12:58
3	BY MR. GAUDET:	03:12:58
4	Q. And I'd like to just blow up the paragraph beginning, "In	03:13:08
5	2010..."	03:13:13
6	A. Okay. I've got Page 005 here.	03:13:21
7	MR. GAUDET: Your Honor, this paragraph begins about	03:13:25
8	two-thirds of the way down.	03:13:27
9	THE COURT: Yes, I see it.	03:13:30
10	BY MR. GAUDET:	03:13:31
11	Q. Mr. Scheck, do you see the first sentence reads, "In	03:13:32
12	2010, CSIRT deployed Stealthwatch with the intention of	03:13:36
13	aiding investigations by retaining at least 90 days' worth of	03:13:40
14	NetFlow data." Do you see that?	03:13:46
15	A. I do.	03:13:49
16	Q. And is that consistent with your recollection?	03:13:49
17	A. It is.	03:13:51
18	Q. Okay. What do you mean by "at least 90 days worth of	03:13:51
19	NetFlow data"?	03:13:55
20	A. What I mean is for every transaction that occurs on	03:13:58
21	Cisco's network, there's a NetFlow record that's generated	03:14:01
22	that's sent to Stealthwatch that's stored in the Stealthwatch	03:14:05
23	database for at least 90 days. So I can go back and say, I	03:14:11
24	want to know what happened five or six weeks ago, and be able	03:14:19
25	to get an answer out of the Stealthwatch tool.	03:14:23

—Scheck, M. - Direct—

1	Q. That phrase "NetFlow data," do you see that?	03:14:26
2	A. I do.	03:14:31
3	Q. To be clear, are those packets?	03:14:31
4	A. They're not packets, they are transaction data, again	03:14:33
5	similar to the phone bill conversation.	03:14:39
6	Q. Okay. And would that summary even have a specific entry	03:14:41
7	relating to a specific packet?	03:14:45
8	A. It would not.	03:14:47
9	Q. What is it instead?	03:14:48
10	A. Well, you would know the number of packets that moved	03:14:50
11	through. That would be the piece that it would keep track of	03:14:53
12	from a packet point of view. But it would tell you the	03:14:55
13	source and destination IP address, the time of the	03:14:58
14	conversation, what services were being used on both sides, or	03:15:01
15	what port numbers, to be technical, and the number of	03:15:06
16	packets. Those are the types of things that that would	03:15:09
17	include.	03:15:12
18	Q. In a single NetFlow record or single NetFlow summary,	03:15:12
19	about how many different packets could be reflected?	03:15:16
20	A. It could be one, or it could be a billion. It doesn't	03:15:21
21	matter to NetFlow. It just -- it logs the actual	03:15:26
22	transaction.	03:15:31
23	Q. And whether it's -- even if it's a billion in that time	03:15:33
24	frame, it's a single record?	03:15:38
25	A. That's correct.	03:15:39

—Scheck, M. - Direct—

1 Q. Okay. Let's now turn back to Page 4 of this document, 03:15:40
2 and let's just blow up that image in the middle of the page. 03:15:44

3 THE COURT: That's Bates 002? 03:15:52

4 MR. GAUDET: 004, Your Honor. Again, we took out a 03:15:55
5 couple of pages just to try to get to the point. 03:16:00

6 THE COURT: I don't have a 004, unless it's out of 03:16:04
7 order. 03:16:07

8 MR. GAUDET: Your binder should have had 001, and 03:16:11
9 the next page should have been 004, and if that's not the 03:16:14
10 case, then that is our fault. 03:16:18

11 THE COURT: No. 001 says "Page 1 of 1," 002 says 03:16:22
12 "Page 2 of 7," and then we skip to "Page 5 of 7." 03:16:27

13 MR. GAUDET: And, Your Honor, this is DTX-409? 03:16:37

14 THE COURT: Yes, it is. 03:16:49

15 MR. GAUDET: Your Honor, I apologize. I know that 03:16:50
16 our crew in Norfolk is working very hard to try to get this 03:16:52
17 straight, and it appears we've made a mistake. If we can, 03:16:55
18 I'll put the image up on the screen. 03:16:59

19 THE COURT: Does the plaintiff have this page? 03:17:03

20 MS. LEE: Yes, Your Honor, I do. 03:17:07

21 THE COURT: Okay. Well, go ahead. 03:17:10

22 MR. GAUDET: We will supplement the Court's document 03:17:15
23 so you have it in paper copy. 03:17:17

24 THE COURT: All right. 03:17:19

25 MR. GAUDET: And let's go back so that you can see 03:17:21

—Scheck, M. - Direct—

1 the entire page first, Your Honor. 03:17:24

2 BY MR. GAUDET: 03:17:24

3 Q. Mr. Scheck, do you see the image in the middle of this 03:17:26
4 page? 03:17:28

5 A. I do. 03:17:29

6 Q. Okay. Let's blow up that image. 03:17:29

7 Mr. Scheck, what is this showing? 03:17:33

8 A. It's showing a very simple investigation with NetFlow 03:17:34
9 where there's a single host that is infected, and it is 03:17:42
10 reaching out to the internet for instructions from the 03:17:47
11 malicious bad guys -- redundant, malicious threat actors, is 03:17:52
12 what we would call them -- to figure out what it needs to do. 03:17:59
13 And we can detect that conversation with NetFlow, and then we 03:18:02
14 can take a step back, and we can look for every other host on 03:18:05
15 the network that's trying to have the same conversation on 03:18:08
16 the internet. That's what's being diagrammed here. 03:18:11

17 Q. You said that you would reach out to the malicious actors 03:18:16
18 on the internet. Are you referring to a threat feed, or are 03:18:22
19 you referring to the actual bad guys? 03:18:24

20 A. Referring to the bad guys. The way that we find the bad 03:18:26
21 guys is because of the threat feed being populated. 03:18:30

22 In this document, I know that we talk specifically 03:18:38
23 about using SLIC, the Stealthwatch Labs feed of threat 03:18:41
24 intelligence. So what this is really diagramming is you find 03:18:48
25 a single host that is connecting to a host that Stealthwatch 03:18:51

—Scheck, M. - Direct—

1 is saying is malicious because of its threat feed. You then
2 just take a step back, and you say, run a query to look for
3 every other host on your network that's talking to the same
4 malicious host very quickly.

5 The reason that can be useful -- again, when you
6 talk about having a hundred days' worth of data, you may get
7 a threat feed that says, this host is a malicious host, and
8 you see one host connect to it, but if you can't go back
9 historically and look back 90 or 100 days, you could have a
10 whole bunch of other hosts that have been having that
11 connection that aren't doing it at that very moment, and you
12 won't see them.

13 Q. If we come out of this blow-up, the last thing I want to
14 do with this document, let's just blow up that next paragraph
15 there.

16 Do you see the second sentence says, "Investigators
17 receive automatic updates from intelligence feeds, such as
18 Lancop's Stealthwatch Labs Intelligence Center, SLIC, and
19 also manually create and modify host groups."

20 Do you see that?

21 A. I do.

22 Q. Okay. And what is that referring to?

23 A. It's essentially the same process I just described,
24 completely automated without anyone ever having to run
25 anything.

—Scheck, M. - Direct—

1 Q. And who are the investigators? 03:20:14

2 A. The investigators are the people on my team that are 03:20:15
3 looking at the alerts in that process that I mentioned. 03:20:20

4 Q. Now, we're going to move away from Stealthwatch, and 03:20:23
5 we've just got to -- sorry. 03:20:29

6 MR. GAUDET: Let me, actually, Your Honor, move to 03:20:31
7 admit DTX-409, the cover page, .004, and .005. 03:20:34

8 THE COURT: The cover page? 03:20:54

9 MR. GAUDET: That's .001. 03:20:55

10 THE COURT: And then .004 and .005. I've got 5. 03:20:59
11 It's 4 I don't have. 03:21:12

12 Okay. Those will be admitted. 03:21:14

13 MR. GAUDET: Thank you, Your Honor. 03:21:16

14 (Defense Exhibit DTX-409, Pages .001, .004 and .005, 03:21:16
15 were received in evidence.) 03:21:17

16 BY MR. GAUDET: 03:21:17

17 Q. Mr. Scheck, just a few more topics, and then we'll be 03:21:18
18 done. 03:21:20

19 Let's just talk generally about Cisco's use of 03:21:20
20 threat intelligence over the years. How long has Cisco been 03:21:24
21 using threat intelligence feeds in its products? 03:21:29

22 A. I can only speak of what I know of, but I know of several 03:21:32
23 different feeds from Cisco IntelliShield and Cisco Botnet 03:21:42
24 Filter in 2007 and 2009, and there were certainly things that 03:21:49
25 we were doing, from a threat intel point of view, loading 03:21:55

—Scheck, M. - Direct—

1	feeds into our products in 2004, when I started in the	03:21:59
2	response team.	03:22:02
3	Q. Let's pull up DTX-623.	03:22:03
4	THE COURT: 623?	03:22:26
5	MR. GAUDET: 623.	03:22:28
6	THE COURT: Okay, I have that.	03:22:33
7	BY MR. GAUDET:	03:22:35
8	Q. Mr. Scheck, what is Defendant's Exhibit 623?	03:22:38
9	A. This is a presentation around threat intelligence tools.	03:22:43
10	Q. And what was the purpose of this presentation?	03:22:48
11	A. Again, this is one of those conversations that we would	03:22:50
12	have with customers, generally speaking, about what we're	03:22:55
13	doing to secure our network and sharing that information with	03:22:59
14	them.	03:23:03
15	Q. And did you give this presentation?	03:23:03
16	A. I did.	03:23:05
17	Q. Let's now pull up Defendant's Exhibit 623.1. And what is	03:23:06
18	623 --	03:23:15
19	MR. GAUDET: Your Honor, this would just be the next	03:23:17
20	tab.	03:23:20
21	THE WITNESS: This is, again, the metadata for that	03:23:23
22	presentation, showing it was created in 2010 and last	03:23:25
23	modified in December of 2011.	03:23:30
24	BY MR. GAUDET:	03:23:34
25	Q. And is that consistent with your recollection, that you	03:23:34

—Scheck, M. - Direct—

1	gave this presentation in 2011?	03:23:36
2	A. It is.	03:23:38
3	Q. Now, the --	03:23:40
4	THE COURT: The first one was 2010, 623? I don't	03:23:45
5	see a date on it. That's why I'm asking.	03:23:53
6	MR. GAUDET: Your Honor, so Exhibit 623.1 --	03:23:55
7	THE COURT: I'm not talking about .1, I'm talking	03:24:01
8	about 623. There's no date on 623.	03:24:08
9	MR. GAUDET: That's correct.	03:24:12
10	THE COURT: All right. So what you're saying is	03:24:12
11	that 623.1 furnishes the date it was originated?	03:24:15
12	MR. GAUDET: That's correct, Your Honor.	03:24:19
13	THE COURT: Okay. You want that admitted?	03:24:20
14	MR. GAUDET: We do, Your Honor. I was going to sort	03:24:28
15	of tie them together, but can we admit DTX-623 and 623.1?	03:24:30
16	THE COURT: I see the dates on them. Is there a	03:24:42
17	question pending?	03:24:59
18	MR. GAUDET: I'm sorry, Your Honor. I apologize.	03:25:03
19	BY MR. GAUDET:	03:25:03
20	Q. Mr. Scheck, 623.1, is this the metadata that would have	03:25:04
21	established the date of Exhibit 623?	03:25:08
22	A. It is.	03:25:11
23	Q. Okay. And, based on this, when was this date -- when was	03:25:12
24	this document last modified?	03:25:17
25	A. December of 2011.	03:25:19

—Scheck, M. - Direct—

1 Q. And is that consistent with your recollection, that you
2 gave this presentation in 2011?

3 A. It is.

4 Q. Okay. Let's now go back to Exhibit 623 and turn to Bates
5 Page 2.

6 MR. GAUDET: There should be a Page 2 in your
7 binder, Your Honor.

8 THE COURT: Okay.

9 BY MR. GAUDET:

10 Q. Mr. Scheck, what is this showing?

11 A. It's essentially showing, if we look across, the tools
12 that we had deployed in 2011. When we talk about threat
13 intelligence and when we talk about malicious actors, there's
14 different tools that detect different techniques and
15 different what we call indicators, so what are the pieces of
16 information that tell us that something really is a bad
17 actor, and it's looking across our web proxy and all of the
18 other tools for specific malicious behavior, malicious
19 content, et cetera.

20 Q. Does this relate to the concept of threat intelligence?

21 A. It is.

22 Q. How so?

23 A. Again, threat intelligence, to me, is simply saying who
24 is the malicious actor, what tools and techniques are they
25 using, and how do you talk about them and share that

—Scheck, M. - Direct—

1 information? And that's what this is demonstrating; that 03:26:49
2 these different tools are looking for things like suspicious 03:26:53
3 behavior and suspicious content and malicious sites, which 03:26:58
4 are all parts of threat intelligence. 03:27:01

5 Q. If we go to the next page of this document -- this should 03:27:03
6 be Bates .003 -- and blow this one up. 03:27:06

7 And, just generally speaking, Mr. Scheck, what is 03:27:13
8 this one showing? 03:27:15

9 A. This one is a very primitive slide. It's basically 03:27:15
10 showing that we have different intelligence feeds that are 03:27:20
11 being fed into our tools and used for detection. 03:27:24

12 Q. And, sir, this was part of your presentation in 2011? 03:27:27

13 A. It is, that's correct. 03:27:33

14 Q. Do you see in the upper right corner it says "Operational 03:27:35
15 Use of Intel"? Do you see that? 03:27:39

16 A. I do. 03:27:41

17 Q. And what did you mean by that in 2011? 03:27:41

18 A. In 2011 there were a lot of people that would take threat 03:27:45
19 intelligence and basically have it as a reference point. So 03:27:50
20 when something bad happened, they would go back to their list 03:27:54
21 of threat intelligence and say, you know, hey, this computer 03:27:57
22 was compromised by someone on the internet, let's look at all 03:28:01
23 the stuff on the computer, do forensics on it, and compare 03:28:06
24 that information to what we have in our list of the known bad 03:28:11
25 people and see if they match up. 03:28:14

—Scheck, M. - Direct—

1 What we're really saying here is we want to 03:28:16
2 operationalize that, take those intelligence feeds, and 03:28:19
3 instead of referencing them afterwards, push them into our 03:28:21
4 products for detection and prevention in real time. 03:28:25

5 Q. So let's talk about the different kinds of products. 03:28:29

6 We just talked about Stealthwatch for quite a while. 03:28:31
7 Do you remember that? 03:28:34

8 A. I do. 03:28:34

9 Q. Okay. Now, can Stealthwatch operate things -- identify 03:28:35
10 things in real time using operationalized threat 03:28:38
11 intelligence? 03:28:44

12 A. Not in real time, near real time. Again, it's 30 03:28:44
13 seconds, five minutes later. 03:28:48

14 Q. And, in contrast, what kinds of tools can make 03:28:50
15 operational use of threat intelligence? 03:28:54

16 A. The ones you see on the screen here that say "prevent," 03:28:57
17 like a firewall -- a firewall can make a decision on whether 03:29:03
18 or not to deliver traffic based on threat intelligence. A 03:29:06
19 web proxy that is in between a system and the internet, 03:29:11
20 allowing them to either access particular web pages or not, 03:29:16
21 that can make a decision on whether or not that's allowed, 03:29:20
22 based on threat intelligence. 03:29:23

23 Q. And what is the difference between a firewall and a 03:29:24
24 product like Stealthwatch? 03:29:27

25 A. A firewall is in between the connections and can actually 03:29:28

—Scheck, M. - Direct—

1	decide whether or not a connection occurs.	03:29:35
2	Q. Let's -- the second-to-the-last document, I think. Let's	03:29:38
3	go to DTX-609.	03:29:47
4	MR. GAUDET: Oh, I'm sorry, Your Honor. I move to	03:29:49
5	admitted 623 and 623.1.	03:29:50
6	THE COURT: They will be admitted.	03:29:53
7	(Defense Exhibit DTX-623 was received in evidence.)	03:29:56
8	(Defense Exhibit DTX-623.1 was received in	03:29:56
9	evidence.)	03:29:58
10	BY MR. GAUDET:	03:29:58
11	Q. Let's go to DTX-609.	03:29:58
12	MR. GAUDET: And, Your Honor, this should be --	03:30:03
13	THE COURT: I have it.	03:30:07
14	MR. GAUDET: Okay, terrific. You will see we only	03:30:09
15	gave you a few pages, because the only thing is this book	03:30:22
16	right here.	03:30:25
17	THE COURT: I appreciate that.	03:30:29
18	MR. GAUDET: Absolutely. I figure it was a good way	03:30:30
19	to lead into the holiday weekend.	03:30:33
20	BY MR. GAUDET:	03:30:33
21	Q. Mr. Scheck, what is the front page of DTX-609?	03:30:37
22	A. It's the Cisco ASA Security Press Book, Omar and Jazib.	03:30:41
23	Q. What is the Cisco ASA?	03:30:56
24	A. The Cisco ASA is the Cisco firewall.	03:30:57
25	Q. And do you see there's a reference in the bottom left to	03:30:58

—Scheck, M. - Direct—

1	ciscopress.com?	03:31:06
2	A. I do.	03:31:09
3	Q. What is that?	03:31:09
4	A. Cisco Press is a publishing company that releases books	03:31:10
5	for commercial sale around mostly Cisco products and	03:31:17
6	solutions.	03:31:23
7	Q. Let's go to the second page of the exhibit.	03:31:25
8	And, Mr. Scheck, does this appear to be a copy of	03:31:29
9	the back page of this book?	03:31:35
10	A. It does look like it, yes.	03:31:37
11	Q. Okay.	03:31:42
12	THE COURT: Is this Bates 002?	03:31:43
13	MR. GAUDET: It is 002, Your Honor.	03:31:47
14	THE COURT: Okay.	03:31:56
15	BY MR. GAUDET:	03:31:57
16	Q. And do you see -- let's blow up the two paragraphs	03:31:58
17	beginning with Jazib Frahim and Omar Santos. Do you see	03:32:02
18	that?	03:32:12
19	A. I do.	03:32:12
20	Q. Are they the authors of this book?	03:32:12
21	A. Yes.	03:32:14
22	Q. And do you know Mr. Frahim and Mr. Santos?	03:32:15
23	A. I do. I know them both pretty well.	03:32:19
24	Q. How so?	03:32:23
25	A. Well, Omar Santos, in particular, has been at Cisco just	03:32:24

—Scheck, M. - Direct—

1 about -- probably longer than me and works on the product 03:32:28
2 security side, and we've collaborated many times on security 03:32:32
3 at different events. 03:32:36

4 And Jazib has also collaborated with my team quite a 03:32:37
5 bit, building up security architecture for services offered 03:32:43
6 to customers. 03:32:45

7 Q. And, Mr. Scheck, did you work with Mr. Santos when he was 03:32:46
8 writing this book in 2010? 03:32:54

9 A. When he was writing the book, he came and spoke to 03:32:55
10 several members of the Incident Response Team, including 03:33:00
11 myself, about what we were doing, to get sort of a real 03:33:04
12 operational hands-on feedback for what he was writing. 03:33:07

13 Q. Let's now go to the next page of the exhibit. 03:33:17

14 MR. GAUDET: This should be -- 03:33:19

15 THE COURT: 004? 03:33:21

16 MR. GAUDET: Yes, let's go to 004. 03:33:22

17 BY MR. GAUDET: 03:33:22

18 Q. And I just want to highlight the copyright notice. Just 03:33:26
19 highlight it. 03:33:32

20 Mr. Scheck, do you see the 2010 copyright notice? 03:33:34

21 A. I do. 03:33:38

22 Q. Now, I know we've talked about how sometimes copyright 03:33:38
23 notices in PowerPoints can be recycled. What about copyright 03:33:43
24 notices in books that Cisco publishes? 03:33:51

25 A. Yeah. I mean, Cisco Press is a publishing company, and, 03:33:54

—Scheck, M. - Direct—

1	as such, they use the copyright to protect their intellectual	03:33:56
2	assets that they're releasing, so they pay a lot more	03:34:03
3	attention to a copyright than internal people, like myself,	03:34:05
4	who are sharing these kinds of presentations with customers.	03:34:08
5	Q. And is it consistent with your recollection that, in	03:34:12
6	fact, this book was published in 2010?	03:34:16
7	A. It was.	03:34:18
8	Q. And if we go down about halfway, there's a reference to	03:34:18
9	second printing in May 2010. Do you see that?	03:34:22
10	A. I do.	03:34:24
11	Q. And is that further consistent with your recollection?	03:34:25
12	A. It is.	03:34:27
13	Q. Okay.	03:34:29
14	THE COURT: What is that? Second printing?	03:34:31
15	Okay. Yes, I see what you mean. All right.	03:34:36
16	BY MR. GAUDET:	03:34:39
17	Q. Let's turn to Bates Page .700.	03:34:40
18	MR. GAUDET: Which, hopefully, Your Honor, is the	03:34:45
19	next page in your notebook.	03:34:46
20	THE COURT: It is.	03:34:49
21	MR. GAUDET: If the intervening 696 were in there,	03:34:51
22	I'd have trouble.	03:34:54
23	BY MR. GAUDET:	03:34:54
24	Q. That paragraph -- I want to blow up the paragraph,	03:34:58
25	"Dynamic and Administrator Black List Data." Do you see	03:35:02

—Scheck, M. - Direct—

1 that? 03:35:06

2 A. I do. 03:35:06

3 Q. There's a reference to "Cisco ASA Botnet Traffic Filter." 03:35:06

4 Do you see that? 03:35:12

5 A. I do. 03:35:12

6 Q. What is that? 03:35:13

7 A. Essentially, Cisco maintained a list of IP addresses and 03:35:14

8 domain names, like www.badguy.com, that tracked all of the 03:35:21

9 threat intelligence that they were aware of, and when you 03:35:30

10 were deploying an ASA, you could actually turn on a traffic 03:35:33

11 filter to reach out to Cisco to fetch that list and apply it 03:35:38

12 to your access control for that device and block all 03:35:42

13 traffic -- 03:35:49

14 MS. LEE: Your Honor, I would just make an objection 03:35:50

15 for the record. 03:35:52

16 Mr. Scheck just referred to www.badguy.com, and I 03:35:53

17 have an objection to that. It appears he listened to 03:35:59

18 portions of the trial, and he was supposed to be sequestered. 03:36:02

19 BY MR. GAUDET: 03:36:08

20 Q. Mr. Scheck, did you listen -- 03:36:09

21 A. I'd love to respond to that, yeah. 03:36:10

22 We use www.badguys.com in lingo all the time. I've 03:36:13

23 used it for ten years to describe a bad site on the Internet. 03:36:19

24 And I certainly have never heard any part of the trial before 03:36:22

25 today. 03:36:26

~~Scheck, M. - Direct~~

1 You can Google www.badguys.com, and you'll see -- 03:36:27

2 THE COURT: I don't think there's anything to 03:36:30

3 suggest a link between his use of the term and any 03:36:33

4 misconduct, so I'll overrule the objection. 03:36:38

5 MR. GAUDET: Thank you, Your Honor. 03:36:43

6 BY MR. GAUDET: 03:36:45

7 Q. Mr. Scheck, why don't you -- I know, maybe sort of take 03:36:46

8 that one from the top, because you probably lost your train 03:36:50

9 of thought. 03:36:54

10 You were describing the Cisco ASA Botnet Traffic 03:36:54

11 Filter? 03:36:58

12 A. Sure. The short of it is Cisco IronPort, which was a 03:36:59

13 company that we acquired that was building security products 03:37:03

14 specifically -- they maintain a list of IP addresses and the 03:37:07

15 domain names -- like www.badguys.com was the example -- and 03:37:12

16 you can pull them into your firewall, and any traffic that 03:37:14

17 tries to go through your firewall that matches either the IP 03:37:18

18 address or the domain name is blocked. 03:37:23

19 Q. How does that relate to the use of threat intelligence? 03:37:25

20 A. That is, essentially, a textbook definition of "threat 03:37:32

21 intelligence." 03:37:36

22 Q. And is this consistent with your recollection of how the 03:37:36

23 Cisco products, in fact, operated in 2010? 03:37:46

24 A. Yes, absolutely. 03:37:48

25 Q. Now, ASA is a firewall; is that correct? 03:37:53

—Scheck, M. - Direct—

1	A. That is correct.	03:37:55
2	Q. So again, just to be sure we're oriented, that's	03:37:56
3	something different than that Stealthwatch product we talked	03:38:01
4	about, correct?	03:38:03
5	A. Correct.	03:38:03
6	Q. Okay. Now, the ASA in 2010, could it receive	03:38:04
7	rules and -- operate and have rules?	03:38:08
8	A. Yes, it could.	03:38:11
9	Q. And would it filter incoming traffic using rules?	03:38:13
10	A. Yes. That was its primary function.	03:38:19
11	Q. Let's jump forward to today. Is that still true today?	03:38:21
12	A. It is.	03:38:25
13	Q. About how many rules do the ASAs that Cisco uses in its	03:38:25
14	networks -- how many rules do they have?	03:38:32
15	A. There's a lot of different firewalls on Cisco's network.	03:38:34
16	Some of them may only have five or ten rules. Some of the	03:38:40
17	busiest may have 10- or 20,000 rules, you know, but that is	03:38:46
18	something that we are trying to reduce.	03:38:53
19	Q. Why would you want to reduce the number of rules?	03:38:56
20	A. Complexity, difficulty in maintaining configurations.	03:38:58
21	There's a lot of features in the ASA to do things like create	03:39:05
22	groups of systems, and you reference the group instead of	03:39:11
23	having a separate rule, and it can greatly reduce the amount	03:39:16
24	of lines.	03:39:18
25	Q. What would your reaction be if I suggested to you using	03:39:20

—Scheck, M. - Direct—

1 5 million rules on Cisco's ASAs?

03:39:24

2 A. It would be very tough as an administrator, because when
3 you have 5 million rules, a human cannot look at 5 million
4 lines and tell you what that firewall is doing. It's going
5 to be really difficult to troubleshoot, and it's going to be
6 impossible to say what is and isn't being allowed into your
7 network.

03:39:27

03:39:34

03:39:39

03:39:42

03:39:46

03:39:51

8 MR. GAUDET: Your Honor, we move to admit 609.

03:39:52

9 THE COURT: That will be admitted.

03:39:59

10 (Defense Exhibit DTX-609 was received in evidence.)

03:40:01

11 MR. GAUDET: Thank you, Your Honor.

03:40:01

12 BY MR. GAUDET:

03:40:02

13 Q. Let's pull up DTX-632. Mr. Scheck, what is Exhibit 632?

03:40:03

14 A. This is another one of the presentations that I've given
15 around threat indicators and threat intelligence.

03:40:12

03:40:18

16 Q. And if we could pull up 632.1, what is 632.1?

03:40:20

17 A. This is, again, the metadata for that presentation,
18 stating that it was created in 2011 and last modified in
19 December of 2013.

03:40:41

03:40:45

03:40:51

20 Q. When was the first time that you recall using -- making
21 presentations with this cover of "Operationalizing Threat
22 Indicators"?

03:40:52

03:40:56

03:41:04

23 A. Probably in the very beginning of that, around the
24 2010-2011 time frame.

03:41:04

03:41:08

25 Q. Two more topics. Changing gears briefly.

03:41:12

~~Scheck, M. - Direct~~

1 MR. GAUDET: Sorry. Your Honor, could we move to 03:41:18
2 admit DTX-632 and 632.1. 03:41:20

3 THE COURT: They will be admitted. 03:41:24

4 (Defense Exhibit DTX-632 was received in evidence.) 03:41:27

5 (Defense Exhibit DTX-632.1 was received in 03:41:27
6 evidence.) 03:41:28

7 MR. GAUDET: Thank you, Your Honor. 03:41:28

8 BY MR. GAUDET: 03:41:29

9 Q. Sir, do you have a general familiarity with the number of 03:41:31
10 times that a competitor of Cisco's would access Cisco's 03:41:34
11 website on a given monthly basis or something like that? 03:41:43

12 MS. LEE: Objection, Your Honor. I don't believe 03:41:47
13 the witness has any foundation to testify on behalf of the 03:41:49
14 entire company of Cisco. 03:41:52

15 THE COURT: This seems a little far-fetched, 03:41:54
16 counsel. 03:41:59

17 MR. GAUDET: Your Honor, the truth is it's a minor 03:41:59
18 point. We'll move past it. He did have a foundation, but 03:42:01
19 there's no reason to do this. 03:42:04

20 Three last questions. 03:42:06

21 BY MR. GAUDET: 03:42:07

22 Q. Are you aware that Cisco has been sued by a company 03:42:07
23 called Centripetal? 03:42:10

24 A. I am. 03:42:11

25 Q. Have you ever had any interactions of any sort with 03:42:11

~~Scheck, M. - Cross~~

1	Centripetal?	03:42:15
2	A. No, I have not.	03:42:15
3	Q. Had you ever heard of Centripetal before you learned that	03:42:18
4	they sued Cisco in this lawsuit?	03:42:21
5	A. I had not.	03:42:23
6	MR. GAUDET: Thank you. No further questions.	03:42:25
7	MS. LEE: Your Honor, I have a few questions on	03:42:33
8	cross-examination. May I proceed?	03:42:35
9	THE COURT: You may.	03:42:37
10	CROSS-EXAMINATION	03:42:37
11	BY MS. LEE:	03:42:37
12	Q. Mr. Scheck, my name is Hannah Lee. I represent	03:42:41
13	Centripetal. It's nice to meet you.	03:42:43
14	A. You, too.	03:42:45
15	Q. There have been numerous changes to Stealthwatch over the	03:42:46
16	years, right?	03:42:49
17	A. There have.	03:42:49
18	Q. And as part of your job at Cisco, you aren't responsible	03:42:50
19	for designing Cisco's products, right?	03:42:54
20	A. That is correct.	03:42:57
21	Q. And you don't work on the engineering side of things,	03:42:59
22	right?	03:43:02
23	A. There are times that I will work with Engineering to	03:43:03
24	provide feedback as a customer and as part of what we call	03:43:07
25	Customer Zero, meaning we are often deploying Alpha code	03:43:11

—Scheck, M. - Cross—

1 before it's publicly available, but I'm not involved in their 03:43:16
2 design process; that's correct. 03:43:19

3 Q. And you don't write source code? 03:43:21

4 A. I do not. 03:43:23

5 Q. You do not work on any engineering aspects of 03:43:23
6 Stealthwatch, correct? 03:43:27

7 A. That is correct. 03:43:27

8 Q. And you did not contribute to the design of Cisco's ETA, 03:43:28
9 correct? 03:43:34

10 A. That is correct. 03:43:34

11 Q. You haven't written any code for the use of NetFlow, 03:43:37
12 right? 03:43:42

13 A. That's not correct. I would say I have not written any 03:43:42
14 code for the use of Stealthwatch. 03:43:47

15 Q. Okay. And you've not written any code for the use of 03:43:48
16 Cisco's threat intelligence? 03:43:53

17 A. Again, I would say I have not written code for threat 03:43:55
18 intelligence products. I've written a great deal of code for 03:44:01
19 how we use it internally. 03:44:05

20 Q. Okay. Your testimony at your deposition was that you did 03:44:07
21 not write code for any of Cisco's products, correct? 03:44:10

22 A. That is correct. 03:44:14

23 THE COURT: Counsel, the Court's rule is that if 03:44:15
24 you're going to question anybody on their deposition, you 03:44:23
25 don't paraphrase the question and his answer. He's already 03:44:26

~~Scheck, M. - Cross~~

1 answered it, and it was a similar question, but if you're 03:44:33
2 going to use deposition testimony to attempt to impeach a 03:44:41
3 witness, you must read the question and the answer verbatim 03:44:44
4 from the deposition record. 03:44:48

5 MS. LEE: Understood, Your Honor. 03:44:51

6 THE COURT: In the future. We'll pass this one, 03:44:53
7 because I thought it was pretty obvious what his answer was. 03:44:55
8 He admitted it, so that's it. 03:45:00

9 BY MS. LEE: 03:45:06

10 Q. And during your testimony, your direct examination, you 03:45:07
11 did not discuss any particular release notes of Cisco's 03:45:10
12 products, right? 03:45:13

13 A. I'm sorry. Could you repeat the question? 03:45:14

14 Q. Yes. During your direct examination, you did not show 03:45:17
15 any release notes for Cisco's products, right? 03:45:21

16 A. Are you referring to the direct examination that just 03:45:24
17 occurred? 03:45:28

18 Q. Yes. 03:45:29

19 A. Not that I recall. 03:45:31

20 Q. And I just wanted to clear up one thing you mentioned 03:45:32
21 earlier about Amazon Web Services. 03:45:38

22 Do you recall your testimony on that? 03:45:41

23 A. I do. 03:45:43

24 Q. Cisco leases space on those Amazon Web servers, right? 03:45:44

25 A. Space and compute hour and those types of things, 03:45:49

~~Scheck, M. - Cross~~

1 correct.

03:45:53

2 Q. And those servers store Cisco software for Cisco, right?

03:45:55

3 A. I think that's a very complicated answer, to be honest.

03:45:59

4 I don't want to get philosophical, but they run the

03:46:10

5 infrastructure that those products use, and in many cases

03:46:15

6 there may not actually be software on them, it may be part of

03:46:19

7 what's -- the overall product. So if we get very specific, I

03:46:23

8 can answer, but sometimes, yes, sometimes no.

03:46:29

9 Q. So Cisco owns the software, right, and it's just renting

03:46:31

10 the space to use the Amazon infrastructure. Is that fair?

03:46:35

11 A. That's fair.

03:46:41

12 Q. Now, if we can pull up DTX-409, I believe this was

03:46:42

13 mentioned during your direct examination.

03:46:49

14 And this is a Lanclope Stealthwatch document from

03:46:55

15 2013, if we blow up the lower left-hand corner on the first

03:47:01

16 page.

03:47:06

17 Does this 2013 document mention anything about

03:47:07

18 detecting threats in encrypted traffic without decryption?

03:47:09

19 A. It does not.

03:47:13

20 Q. And Cisco --

03:47:13

21 A. Actually -- yeah, I don't believe so.

03:47:18

22 Q. Cisco, in 2018 and 2019, has marketed Stealthwatch as

03:47:22

23 working with Encrypted Traffic Analytics to detect threats in

03:47:31

24 encrypted traffic without decryption, correct?

03:47:37

25 A. That's correct.

03:47:41

~~Scheck, M. - Cross~~

1	Q. Let me pull up PTX-276.	03:47:44
2	THE COURT: This is PTX? Did you say "PTX"?	03:47:50
3	MS. LEE: PTX, yes, Your Honor.	03:48:00
4	THE COURT: So are we now switching to your	03:48:01
5	cross-examination book?	03:48:04
6	MS. LEE: Yes, Your Honor, and this has already been	03:48:06
7	admitted.	03:48:08
8	THE COURT: Give me the number again.	03:48:09
9	MS. LEE: 276.	03:48:11
10	THE COURT: All right. Has this been admitted?	03:48:16
11	MS. LEE: Yes, it has.	03:48:19
12	THE COURT: 276. This is a PTX. Okay, I have it.	03:48:22
13	BY MS. LEE:	03:48:30
14	Q. The title of this Cisco public document from 2019 is	03:48:31
15	"Encrypted Traffic Analytics With the New Cisco Network and	03:48:38
16	Stealthwatch," right?	03:48:41
17	A. Yes, that is the title.	03:48:41
18	Q. And if we could go to the second page of the document,	03:48:44
19	under "Encrypted Traffic Analytics," "Cisco, with its	03:48:49
20	expertise in the network infrastructure market, conducted	03:48:54
21	extensive research and is introducing innovative and	03:48:58
22	revolutionary technology, Encrypted Traffic Analytics."	03:49:02
23	This is what Cisco was marketing last year, in 2019,	03:49:04
24	right?	03:49:08
25	A. Yes.	03:49:08

—Scheck, M. - Cross—

1 Q. And if we go to the next page of the document, at the 03:49:10
2 top, if we could blow up the figure there, this is showing 03:49:15
3 Cisco's Stealthwatch Enterprise as part of its Cisco system 03:49:21
4 using routers and switches to find malicious activity in 03:49:26
5 encrypted traffic, right? 03:49:32

6 A. That's correct. 03:49:33

7 Q. And if we could go to the bottom of the document, the 03:49:33
8 last sentence there says, "Using the collective enhanced 03:49:39
9 telemetry, Stealthwatch Enterprise provides the ability to 03:49:44
10 view and search on parameters, such as encryption key 03:49:47
11 exchange, encryption algorithm, key length, TLS/SSL version, 03:49:51
12 etc., to help ensure cryptographic compliance." 03:49:58

13 Do you see that? 03:50:04

14 A. I do. 03:50:04

15 Q. This is what Cisco was marketing about Stealthwatch in 03:50:05
16 2019, right? 03:50:07

17 A. Yes. 03:50:08

18 Q. Now, let's go to DTX-609. 03:50:12

19 THE COURT: We're back to the other binder? 03:50:18

20 MS. LEE: Yes, Your Honor, we're back to one of the 03:50:21
21 exhibits that was raised on direct examination. This page 03:50:24
22 I'm about to reference will not be in your book, because it 03:50:31
23 was something that the defendants opened the door to, so I'll 03:50:34
24 be discussing another page of this book. 03:50:38

25 THE COURT: Where would I find that? 03:50:42

~~Scheck, M. - Cross~~

1	MS. LEE: We'll put it on the screen so that it can	03:50:47
2	be seen.	03:50:50
3	THE COURT: It's not in your book?	03:50:51
4	MS. LEE: It is not, Your Honor. We did not	03:50:53
5	anticipate the witness addressing this.	03:50:54
6	THE COURT: All right.	03:51:00
7	MS. LEE: Can we go to Page 73?	03:51:02
8	THE COURT: And you're representing this as being	03:51:09
9	one of the pages from DTX-609?	03:51:11
10	MS. LEE: It is, Your Honor, yes.	03:51:15
11	BY MS. LEE:	03:51:22
12	Q. Mr. Scheck, do you recall testifying in your direct	03:51:24
13	examination about the ASA firewall --	03:51:26
14	THE COURT: No, don't do that again. I just warned	03:51:29
15	you about that.	03:51:31
16	MS. LEE: Your Honor, I'm not talking about the	03:51:34
17	deposition, I'm talking about the exhibit, the book.	03:51:36
18	THE COURT: Well, don't ask him if he testified to	03:51:38
19	something in his deposition without reading the question and	03:51:41
20	the answer. I just finished going over that.	03:51:44
21	MS. LEE: Your Honor, I'm not raising the deposition	03:51:48
22	at all. This is -- during his direct examination, he	03:51:49
23	discussed this book, and that was my question. And I can	03:51:54
24	rephrase, Your Honor, if it came out wrong. That was not my	03:51:57
25	intention, to raise the deposition.	03:52:01

~~Scheck, M. - Cross~~

1 THE COURT: Well, you asked him if he said something 03:52:05
2 in his deposition. Don't ask him if he said something in his 03:52:08
3 deposition unless you're going to read the question and the 03:52:13
4 answer. 03:52:15

5 MS. LEE: If I did, Your Honor, I apologize. I 03:52:17
6 absolutely meant to ask him about his direct examination. 03:52:21

7 THE COURT: All right. What's the question? 03:52:27

8 BY MS. LEE: 03:52:30

9 Q. Mr. Scheck, do you recall during your direct examination 03:52:31
10 referring to this ASA firewall book? 03:52:35

11 A. I do. 03:52:38

12 Q. Okay. Now, in the screen in front of you -- and we can 03:52:40
13 blow it up. I'm referring to Page 73. I'd like to highlight 03:52:45
14 the note at the bottom. 03:52:48

15 THE COURT: Page 73? 03:52:49

16 MS. LEE: Yes, Your Honor. 03:52:53

17 THE COURT: Is that Bates -- 03:52:55

18 MS. LEE: It's Bates number 73. 03:52:56

19 THE COURT: All right. Nobody has that. We're just 03:53:06
20 looking at it on the screen? 03:53:12

21 MS. LEE: Yes. 03:53:13

22 BY MS. LEE: 03:53:15

23 Q. Here the note says, "The Cisco ASA CSC-SSM cannot scan 03:53:17
24 traffic using the HTTPS protocol because this traffic is 03:53:23
25 encrypted." 03:53:28

~~Scheck, M. - Cross~~

1 At this time, as we're discussing this book, the 03:53:29
2 Cisco ASA product could not depict threats in encrypted 03:53:33
3 traffic. Is that fair? 03:53:39

4 A. It's a complicated answer. I would say that if all of 03:53:41
5 the details around the threat are contained in an encrypted 03:53:51
6 session, that's correct. 03:53:54

7 When we talk about things like the botnet filter, 03:53:57
8 that still applies, even if the session is encrypted, because 03:54:01
9 those are obviously parts of the conversation that happened 03:54:06
10 outside of encryption. 03:54:08

11 BY MS. LEE: 03:54:13

12 Q. At this time the Cisco ASA could not detect threats in 03:54:13
13 encrypted traffic without decryption, right? 03:54:17

14 A. Again, I will stick to the it's more complicated than a 03:54:22
15 "yes" or "no" answer and say you cannot decrypt a session and 03:54:27
16 find malicious content within a decrypted session, but even 03:54:32
17 though the session is encrypted, I can still detect threats 03:54:37
18 in that session, even in 2010. 03:54:40

19 Q. Is it your testimony, Mr. Scheck, that the ASA product 03:54:43
20 that's being sold today with FirePOWER services has the exact 03:54:46
21 same technology as the ASA in this book? 03:54:49

22 A. I wouldn't make that claim. 03:54:52

23 Q. Now, let's bring up -- actually, let me ask you this: 03:54:56

24 You testified during your direct examination that 03:55:06
25 Stealthwatch cannot block or quarantine, correct? 03:55:09

~~Scheck, M. - Cross~~

1 A. I don't think that was -- I recall the question being 03:55:12
2 around automatic quarantine and automatic blocking. 03:55:22

3 Q. Okay. And is it your testimony -- are you correcting 03:55:26
4 your testimony to say that Stealthwatch can block and 03:55:30
5 quarantine? 03:55:33

6 MR. GAUDET: Objection. I don't think there's any 03:55:35
7 need for a correction. 03:55:37

8 THE COURT: What was the original question? 03:55:42

9 MS. LEE: The original question was, "Mr. Scheck, 03:55:45
10 did you testify that Stealthwatch cannot block or 03:55:49
11 quarantine?" 03:55:53

12 THE COURT: Did you say that? 03:55:58

13 THE WITNESS: No, I did not, Your Honor. 03:55:59

14 BY MS. LEE: 03:56:01

15 Q. Is it your testimony that Stealthwatch can block or 03:56:03
16 quarantine? 03:56:06

17 MR. GAUDET: I'm going to object that that's 03:56:07
18 compound. Those are two very different things. 03:56:09

19 But, with that... 03:56:12

20 THE COURT: Overruled. 03:56:13

21 MS. LEE: Your Honor -- 03:56:13

22 THE COURT: Overruled. 03:56:13

23 You can answer the question. 03:56:16

24 THE WITNESS: It cannot block. It can be used to 03:56:24
25 initiate a quarantine with human intervention. 03:56:32

~~Scheck, M. - Redirect~~

1 MS. LEE: Can we pull up -- and, Your Honor, this is 03:56:42
2 again not in your book because we did not anticipate the 03:56:44
3 witness would go here, but we can show it on the screen. 03:56:46

4 THE COURT: All right. 03:56:46

5 MS. LEE: It is already in evidence. 03:56:52

6 Could we bring up PTX-312 -- oh, excuse me, 584. 03:56:55
7 And this is already admitted into evidence. 03:57:02

8 BY MS. LEE: 03:57:02

9 Q. If we can go to the Bates number ending in 403 and blow 03:57:06
10 up the bottom of the page, the last sentence. 03:57:22

11 Now, Mr. Scheck, this is a Cisco white paper about 03:57:28
12 ETA. It says, "Upon discovery, a malicious encrypted flow 03:57:31
13 can be blocked or quarantined by Stealthwatch." 03:57:37

14 Do you agree with that? 03:57:42

15 A. Yes, I suppose it's a true statement. 03:57:43

16 Q. Okay. 03:57:52

17 MS. LEE: No further questions, Your Honor. 03:57:54

18 THE COURT: Any redirect? 03:57:58

19 MR. GAUDET: Briefly. 03:58:00

20 REDIRECT EXAMINATION 03:58:00

21 BY MR. GAUDET: 03:58:00

22 Q. Let's pull that same document up, the same blow-up, if 03:58:06
23 Centripetal's team would do that for us. 03:58:11

24 What is the next sentence of this statement, 03:58:18

25 Mr. Scheck? 03:58:21

—Scheck, M. - Redirect—

1 A. I'm sorry. Some of the video is actually in the way, and 03:58:21
2 it makes it difficult for me to read it: 03:58:25

3 "Policy-driven remediation actions via pxGrid using 03:58:28
4 Cisco Identity Services Engine, or ISE, with Cisco Trustex 03:58:36
5 and Software Defined Access, SDX, simplify and accelerate 03:58:41
6 network security operations." 03:58:43

7 Q. What does that mean? What is that talking about, about 03:58:47
8 how Stealthwatch can be used? 03:58:50

9 A. So -- yeah, it is one of those very complicated answers. 03:58:53
10 And, you know, again, it's probably a fair statement to say 03:59:01
11 "upon discovery," and that's the real piece of that that's 03:59:05
12 interesting. 03:59:09

13 Again, discovery can be minutes or hours from the 03:59:11
14 time a flow occurs, but when that happens, you can actually 03:59:15
15 push policy through pxGrid and ISE from Stealthwatch. Again, 03:59:20
16 it's not an automatic thing. It takes some user interaction. 03:59:28
17 It also takes a lot of configuration of very specific 03:59:33
18 software-defined policy rules being deployed on your devices 03:59:39
19 to consume that information. 03:59:43

20 So, you know, basically, if I were to try to explain 03:59:45
21 it in layman's terms -- 03:59:48

22 THE COURT: On a high level. 03:59:53

23 THE WITNESS: -- you can take a whole bunch of 03:59:57
24 different stuff and kind of get it glued together to issue a 03:59:59
25 policy change when something is discovered with Stealthwatch, 04:00:03

—Scheck, M. - Redirect—

1	which it is a fair statement, but that's not the sort of	04:00:07
2	thing that's happening automatically or in real time or	04:00:10
3	anything like that.	04:00:14
4	BY MR. GAUDET:	04:00:15
5	Q. Would this be after a human investigation?	04:00:16
6	A. Generally, that would be, out of the box, very true. I	04:00:18
7	think, again, because you're talking about a lot of very	04:00:27
8	complex things, you could build orchestration and automation	04:00:30
9	in to handle some of this, you know, without having someone	04:00:35
10	as a human there, but you're getting to the point where	04:00:39
11	you're talking about -- you know, you can get computers to do	04:00:42
12	all sorts of crazy stuff if you spend enough time in	04:00:46
13	automation and engineering, right? And that's a little bit	04:00:52
14	of what it takes here.	04:00:53
15	Q. Are you aware of any Cisco customer who has ever done	04:00:54
16	that?	04:00:58
17	A. Not that I have talked to.	04:00:58
18	MR. GAUDET: Sorry, Your Honor?	04:01:03
19	THE COURT: Never mind.	04:01:06
20	THE WITNESS: No, I've not spoken to any Cisco	04:01:08
21	customer that's done this.	04:01:11
22	BY MR. GAUDET:	04:01:13
23	Q. And what is the status of the packets about which the	04:01:13
24	NetFlow records that set all this off -- where are they by	04:01:18
25	the time any of this happens?	04:01:22

—Scheck, M. - Redirect—

1	A. Well, they would have been delivered hours ago, which is	04:01:24
2	why in my original answer on, you know, can it block, can it	04:01:29
3	quarantine, I said "no" to block. Because, to me, block	04:01:32
4	implies that you're talking about that connection, and it	04:01:37
5	would potentially be two to four hours later that you	04:01:40
6	actually are trying to block, so that's not very realistic.	04:01:44
7	However, if a computer was, say, infected, you could push a	04:01:47
8	quarantine to try to keep that computer from talking to other	04:01:51
9	computers through something like this. That's really what	04:01:55
10	we're talking about here.	04:01:59
11	Q. Let's go to -- I want to pull back up Defendant's	04:02:00
12	Exhibit 0409.	04:02:07
13	THE COURT: 409?	04:02:16
14	MR. GAUDET: It's 409, yes, Your Honor, it should be	04:02:19
15	in your --	04:02:21
16	THE COURT: It says "0409" in one place and "409" in	04:02:22
17	another, but I know the one you're talking about.	04:02:27
18	BY MR. GAUDET:	04:02:29
19	Q. Do you recall, Mr. Scheck, that, on the	04:02:33
20	cross-examination, counsel asked you if this said anything	04:02:35
21	about encryption anywhere, and off the top of your head you	04:02:37
22	couldn't recall?	04:02:44
23	A. That's correct.	04:02:45
24	Q. Let's go to .004.	04:02:45
25	THE COURT: That's the one I'm missing.	04:02:49

—Scheck, M. - Redirect—

1	MR. GAUDET: That's the one you're missing, Your	04:02:51
2	Honor, unfortunately.	04:02:53
3	BY MR. GAUDET:	04:02:53
4	Q. I want to blow up the last full paragraph, and let's	04:02:53
5	highlight the sentence, the second sentence, "Because	04:03:01
6	Stealthwatch was developed to function without relying on the	04:03:06
7	data portion of the packets, all of the alarms and algorithms	04:03:10
8	that work with traditional network traffic are not affected	04:03:14
9	by encryption."	04:03:17
10	Do you see that?	04:03:20
11	A. I do.	04:03:21
12	Q. What does this mean?	04:03:23
13	A. It means that the reason that Stealthwatch and NetFlow,	04:03:24
14	in general, is effective without going into the encrypted	04:03:27
15	stream of a packet, it's -- the same reason that I was a	04:03:32
16	little hesitant on the 2010 answer.	04:03:37
17	There are lots of pieces of data in a connection	04:03:39
18	that occur that have nothing to do with the encrypted content	04:03:42
19	of the packet, and so there's a great deal of analytics and	04:03:45
20	blocking that you can do at, say, the firewall level and	04:03:49
21	detection you can do at a Stealthwatch level, without ever	04:03:54
22	having to look at the content of the data.	04:03:57
23	Q. Does that mean that you were filtering encrypted threats	04:03:59
24	without decrypting the e-mail?	04:04:03
25	A. Without decrypting the content, absolutely.	04:04:05

—Scheck, M. - Redirect—

1 Q. And how long has that been going on, as you just 04:04:07
2 described it? 04:04:11

3 A. I mean, realistically, as long as there's been firewalls. 04:04:12
4 Because you're looking at portions of the connection that 04:04:16
5 you're making decisions on whether allowing or dropping that 04:04:20
6 traffic that have nothing to do with the encrypted content of 04:04:23
7 that traffic. 04:04:27

8 Q. And do you recall a document where Cisco described 04:04:27
9 Encrypted Traffic Analytics as revolutionary and innovative? 04:04:32
10 Do you remember that? 04:04:36

11 A. I do. 04:04:36

12 Q. Was the revolutionary and innovative part the idea of, 04:04:37
13 hey, we can filter traffic that's encrypted -- 04:04:41

14 MS. LEE: Objection, Your Honor. This is leading. 04:04:45

15 THE COURT: Well, it sure is. 04:04:47

16 MR. GAUDET: Okay. 04:04:49

17 BY MR. GAUDET: 04:04:49

18 Q. What is the revolutionary and innovative part of 04:04:50
19 encrypted analytics? 04:04:55

20 A. Yeah. David McGrew and Blake Anderson are the two 04:04:57
21 primary authors for ETA, and they are -- David is a 04:05:01
22 cryptography person, and Blake is a machine learning and AI 04:05:06
23 expert. And really what they managed to do was figure out a 04:05:11
24 way to look for -- if you recall the document that was shared 04:05:14
25 that had the announcement around ETA and the fields that they 04:05:18

~~Scheck, M. - Redirect~~

1 were actually examining, all of those fields are unencrypted 04:05:23
2 fields in the packet. And so you take -- 04:05:27

3 THE COURT: What exhibit is this? 409? 04:05:31

4 MR. GAUDET: This is 409, Your Honor. 04:05:40

5 THE COURT: Page 004? 04:05:42

6 MR. GAUDET: Your Honor, the witness has started 04:05:46
7 referencing a document that the plaintiff showed him, and if 04:05:49
8 it's helpful, we can bring up that document, as well. 04:05:53

9 THE COURT: I don't have any problem. I just wanted 04:05:56
10 to know where this came from. 04:06:01

11 MR. GAUDET: Fair enough. And let's bring this one 04:06:02
12 down. 04:06:02

13 BY MR. GAUDET: 04:06:02

14 Q. But just to kind of fully set the context, Mr. Simons, if 04:06:05
15 you would, put up Plaintiff's Exhibit 276, and let's go to 04:06:11
16 Page 002. 04:06:21

17 Was this what you were referring to, Mr. Scheck? 04:06:28

18 A. It is. When you look at the four main data entries that 04:06:29
19 this document talks about, the sequence packet length and 04:06:33
20 times, the Initial Data Packet, byte distribution, 04:06:36
21 TLS-specific features -- like all that stuff, none of that is 04:06:42
22 encrypted. All of that is required to set up the encryption, 04:06:46
23 and so what ETA does is it's not actually looking at the 04:06:52
24 contents that are encrypted, it's sending off some of the 04:06:56
25 items required to enable that encryption. And, in doing 04:07:00

1 that, it's running the machine learning and AI against that 04:07:06
2 content. 04:07:11

3 And that's where the magic, if you will, of ETA is, 04:07:11
4 is figuring out what's interesting or different about the way 04:07:14
5 this encryption is being established from the pieces that are 04:07:19
6 unencrypted. 04:07:24

7 MR. GAUDET: No further questions. 04:07:29

8 THE COURT: Any recross? 04:07:30

9 MS. LEE: No further questions for this witness, 04:07:32
10 Your Honor. 04:07:34

11 (Witness excused.) 04:07:37

12 THE COURT: All right. Well, we will be adjourned 04:07:37
13 until 10:00 Tuesday morning, since Monday is a holiday. 04:07:50

14 So who's going to testify on Tuesday? 04:08:06

15 MR. GAUDET: Your Honor, our next witness is going 04:08:14
16 to be David McGrew. In fact, he's the witness that 04:08:16
17 Mr. Scheck just referenced. He was the developer of 04:08:20
18 Encrypted Traffic Analytics. 04:08:23

19 And the witness after that will be our first expert, 04:08:23
20 who will be Dr. Schmidt. 04:08:26

21 THE COURT: On what subject? 04:08:29

22 MR. GAUDET: On the '856 patent, Your Honor. He 04:08:31
23 will cover both infringement and invalidity. 04:08:34

24 THE COURT: All right. We'll be adjourned. 04:08:40

25 MR. GAUDET: Happy Memorial Day, Your Honor. 04:08:46

1 THE COURT: Well, I hope everyone enjoys the 04:08:50
 2 weekend. I guess we're in different parts of the country. I 04:08:53
 3 just heard that we're allowed -- in Virginia, we can actually 04:08:56
 4 go inside a restaurant as of today. I don't know if that's 04:09:01
 5 true for all the rest of you, but it's my baby brother's 04:09:06
 6 birthday, so I'm going into a restaurant. 04:09:13

7 MR. GAUDET: Well, happy birthday. We look 04:09:17
 8 forward -- 04:09:19

9 THE COURT: Well, it's not my birthday, it's my baby 04:09:21
 10 brother's. 04:09:23

11 Anyway, I hope everyone enjoys the weekend, and I'll 04:09:25
 12 see you Tuesday at 10:00. 04:09:28

13 MR. GAUDET: Thank you, Your Honor. 04:09:30

14 MS. LEE: Thank you, Your Honor. 04:09:32

15 (The proceedings recessed at 4:10 p.m.) 04:13:47

16 CERTIFICATION

17
 18 I certify that the foregoing is a correct transcript
 19 from the record of proceedings in the above-entitled matter.

20

21

22 _____/s/_____

23 Carol L. Naughton

24 May 21, 2020

25