

Planet Depos®
We Make It Happen™

Transcript of Seth James Nielson, Ph.D

Date: April 26, 2024
Case: IriusRisk, Inc. -v- Threatmodeler Software, Inc. (PTAB)

Planet Depos
Phone: 888.433.3767
Email: transcripts@planetdepos.com
www.planetdepos.com

WORLDWIDE COURT REPORTING & LITIGATION TECHNOLOGY

1

BEFORE THE PATENT TRIAL AND APPEAL BOARD

IRIUSRISK, INC.,

Petitioner,

v.

THREATMODELER SOFTWARE INC.,

Patent Owner.

IPR2023-00821

U.S. Patent No. 10,699,008

Deposition of SETH JAMES NIELSON, Ph.D.

Conducted virtually via Zoom

Friday, April 26, 2024

8:59 a.m. CST

Job No.: 533699

Pages: 1 - 75

Reported by: THERESA A. VORKAPIC,

CSR, RMR, CRR, RPR

2

Videotaped deposition of Seth James Nielson, Ph.D., conducted virtually via Zoom, pursuant to notice before Theresa A. Vorkapic, a Certified Shorthand Reporter, Registered Merit Reporter, Certified Realtime Reporter, Registered Professional Reporter and a Notary Public in and for the State of Illinois.

3

A P P E A R A N C E S

ON BEHALF OF THE PETITIONER:

MATTHEW MIDDLETON, ESQUIRE
DLA PIPER LLP
1201 North Market Street
Suite 2100
Wilmington, Delaware 19801
302-468-5675
matthew.middleton@dlapiper.com

ON BEHALF OF THE PATENT OWNER:

DONALD L. JACKSON, ESQUIRE
RIMON PC
8300 Greensboro Drive
Suite 500
McLean, Virginia 22102
571.765.7703
donald.jackson@rimonlaw.com

4

C O N T E N T S

EXAMINATION OF SETH JAMES NIELSON, Ph.D. PAGE
Examination By Mr. Middleton 5
Examination By Mr. Jackson 66

E X H I B I T S

(Attached to transcript.)

NIELSON DEPOSITION EXHIBITS PAGE
Exhibit 1001 US Patent 10,699,008 Agarwal 28
Exhibit 1004 US Patent 9,602,529 Jones 39
Exhibit 2003 Nielson Declaration 6

5

PROCEEDINGS
THE REPORTER: Would you raise your right hand, please.
(The witness was duly sworn.)
SETH JAMES NIELSON, Ph.D.,
called as a witness herein, having been first duly sworn, was examined and testified as follows:
EXAMINATION
BY MR. MIDDLETON:
Q Good morning, Dr. Nielson.
A Good morning.
Q A few preliminary questions, do you understand that you're under oath today?
A I do.
Q Is there any reason that you can't give me your best testimony today?
A No.
Q Since we're taking this deposition remotely, do you have any physical documents with you today?
A I do not have any physical documents. I do have some electronic documents open which is my

6

report, the patent, and Jones -- I have them open in PDF.
Q When you say the patent, you're referring to the '008 patent?
A Correct.
Q Do you have any notes or annotations on any of those documents?
A I do not.
Q Do you have anything else open on your computer?
A No.
Q No messaging apps or anything like that?
A No, those have all been turned off.
Q Let's take a look at your declaration which is Exhibit 2003.
(A certain document was marked Nielson Deposition Exhibit 2003 for identification, as of 04/26/2024.)
BY MR. MIDDLETON:
Q Do you have it open?
A One moment. I'm downloading it now.
Q Sure?

7

A I have it now, thank you.
Q Did you review this declaration -- sorry, backing up.
This is your declaration for the '008 patent; is that correct?
A Yes. This appears to be a complete draft of my declaration for the '008 -- I mean for this matter regarding the '008 patent.
Q Have you reviewed your declaration in preparation for your deposition today?
A I did.
Q Does this declaration represent all the opinions you currently have for this matter?
A I noticed one small oversight in the listing of the claims for Ground 2, there are Claims 1 through 20, and I apparently left off the Dependent Claim 20, but it is the same language as Claim 11 and I believe it's 1-F I think. I'd have to double check here. Mr. Hurlbut relies on similar analysis and my analysis is the same for Claim 20 as it is for Claim 11.
Q Do you have any other corrections to your

8

report sitting here today?
A Nothing else that I saw as I went through.
Q Moving on to your background, your expertise involves cybersecurity; is that right?
A Yes.
Q And you're the founder of a firm called Crimson Vista?
A Correct.
Q When was this founded?
A 2016, it would have been March 1st.
Q And Crimson Vista is a computer security research and engineering company?
A That's correct.
Q And the common consulting service you provide is source code review?
A That's one of the services that we provide. We do a lot of that.
Q Could you please describe for me your experience with threat modeling?
A Yes, I've done quite a bit of threat modeling both in terms of what I teach with my classes and then what I work on with my clients.

9

I recently was working with a client that had had a -- what did they call it? -- an analysis of -- security analysis that was done by their cybersecurity insurance company and then sent to them. They had not requested it. It was done without any explanation and sent to them, and they had no idea what any of it meant, and so a good part of what we went through as I assisted them in understanding their report was to help them understand the threat models that were being used in the analysis that had been done so they could make better decisions about whether or not these represented real threats to their organization and whether or not they wanted to also appeal their insurance classification.

So we worked through some threat models with what was going on and what the report seems to be getting at.

Also, I actually recently had another set of discussions with some potential investors in an insurance project that dealt with cybersecurity where I was providing expertise on threat models

10

and risk analysis for cybersecurity in order to better understand the start-up they were considering and the potential investments, opportunities and risks.

Those are just some of the more recent ones since we talked in my last deposition. Obviously all the expertise I listed there is still relevant.

Q Have you ever heard of IriusRisk before this case?

A No.

Q Have you ever heard of ThreatModeler before this case?

A No.

Q Have you ever heard of Stephen de Vries before this case?

A No.

Q Have you ever heard of Anurag Agarwal before this case?

A No.

Q Have you ever heard of Adam Shostack before this case?

11

A The name sounds familiar, but I'm not sure. I don't think so, but it's tickling my recognition section so I don't want to say for sure, but I don't know.

Q Have you ever heard of John Steven before this case?

A I don't think so.

Q Have you ever used IriusRisk threat modeling tool before this case?

A No.

Q Have you ever used ThreatModeler threat modeling tool before this case?

A No.

Q Have you ever used the Microsoft threat modeling tool before this case?

A No.

Q What threat modeling tools have you used before this case?

A The threat modeling that I've done has all been by hand, so that usually involves drawing my own diagrams or creating my own reports.

Q And when you would make a threat model by

12

hand, can you describe for me how you would do that?

A Well, it depends. A lot of times there's an even higher level process of just trying to understand the organization's goals or the individuals -- the goals of the system. That's necessary in order to understand what the valuable pieces are.

When you're creating security, there's different tradeoffs between locking things down, making things available, et cetera, so my starting process is actually trying to understand what it is that the organization in question is most needing to protect and what it is they're trying to accomplish.

Once I have an understanding of that, then it's a process of looking at existing models. When I say "models," I mean conceptual models for different types of threat actors and threat approaches.

So one of the highest level that you can think about is are we talking about an insider or

13

an external threat? If you're dealing with insider threats, for example, that's a whole different set of modeling. It has a whole different set of questions that need answered and issues to consider. So I'll start with a very high level of threat modeling and then I will narrow down as necessary to get into more details.

If we're getting down just to give you an example -- if we're talking about like on a network level, if we're coming down to that level of an analysis, there are also existing models that we use for networks. Again, these are conceptual models. They're kind of like templates that you then use and apply as you're trying to understand what sort of threats ands risks you're going to deal with in the network. And, for example, one of the common types of models for a network is do we have a passive listener or do we have an active adversary.

An active adversary on a network can do more than just intercept messages. They can put messages on to the network, perhaps even lock

14

messages and change them, alter, you know, some type of active interference.

So there is a certain level of threat modeling that's just attempting to understand the types of adversaries that are likely to be an issue for your system, again, with the starting point being what is it that you're most trying to protect.

Then there's a whole additional level which is you start looking at systems and components that comprise the system. If it's going to be built, then you have to have a certain amount of hypothetical -- if it's already built, you're going to need do some inventory analysis. Then there's a whole level of threat analysis that tends to be related to vulnerability analysis and adequate authentication and authorization enforcement and some of those kind of things.

So there's a range, and depending on what it is that my client is looking for, we work at these different levels to identify the threats and how to address them.

15

Q How exactly is all of this done by hand?

A Well, so as I'm saying, a lot of this for a trained cybersecurity person like myself, we're trained with some of the key theoretical models to start with like insider threats. Those are one of the most overlooked from somebody who isn't a trained professional, right.

So then the question is if we're going to do that, then the by hand analysis is what does the insider have access to and then we start that whole lower level investigation.

Like so, for example, let's say we're talking about a bank. If we're worried about insider threats, then you have to look at your access controls differently. Right? You're not just trying to keep out somebody who is external. Your internal controls that are supposed to allow things to get done have to be modeled in a way where you are also ensuring if someone goes rogue, then it's still protected.

So then you start working with threat models like are we talking about a single bad

16

actor or are we talking about a coalition? If we're dealing with a single bad actor, right, this is a model. That's what all much this is about, right? If we model our threat as one person goes rogue, then you can have litigations related to there have to be two people who access the financial information or approve it, right? But that doesn't work if you're dealing with, you know, a coalition.

So you have to work with the client to kind of understand what levels of threat they are concerned about. Some of that is based off historical data. Some of that is based off other experiences, but then you model based on these pieces of information and then you create -- you know, you then refine the model with additional levels of detail as you build out from the start.

Q Is this process of threat modeling by hand that you're describing any different from threat modeling used in a computer?

A Well, I mean, I use a computer to the extent I'm either drawing up diagrams or writing a

17

report, but I guess it wouldn't be that different if I just wrote it all out on a piece of paper.
Just so I understand your question, are you asking about computers in general or are you asking about automation tools?
Q Let's start with computers in general.
A Well, as I said, I use computers to create reports or to draw diagrams, so obviously that's using a computer for creating the work product.
Q What are automation tools?
A So automation tools are like ThreatModeler, for example, where the idea is that if you can take a significant amount of information for which there are some understood models at a particular level that the system can in an automated fashion help to construct parts of your overall threat model.
Q Are the claims of the '008 patent directed to automation tools?
MR. JACKSON: Object to the form.
BY THE WITNESS:
A Well, looking at Claim 1, Claim 1 requires

18

that there are databases that have a plurality of threat model components and there are threats that are stored there and associated with threat model components and then stored therein are compensating controls providing interfaces including a diagram interface configured to be displayed on one or more end user computing devices communicatively coupled with one or more databases and then configuring the diagram interface to display a relational diagram, one of a system, an application and a process using visual representations of one or more of the threat model components and visual representations of one or more of the compensating controls, relational diagram defining a first threat model.
And then the last requirement, configuring the diagram interface to response receiving one or more user inputs, add a component group to the first threat model and thereby redefine the first threat model by including it in a second threat model associated with the component group wherein the component group comprises a predefined

19

interrelated group of two or more of the threat model components.
So at the very least, having a user interface wherein there's an input that adds a component group that thereby redefines the threat model, that is certainly at least partially automated. Automated in the sense that the redefinition of the threat model is done by the computer drawing on information from these databases.
Q And we can talk generally about this, but how are automation tools different than what you would do by hand -- or scratch that.
Are the automation tools different than what you would do by hand?
A Well, the final threat analysis isn't any different. The automation tools are meant to make life easier and be able to speed up certain aspects of threat modeling.
Q So if I understand your earlier testimony correctly, you've been involved in actually drafting and developing threat models, right?

20

A Yes.
Q Do you recall how many threat models that you've drafted or developed?
A Well, let me see, but the challenge in answering that is just about any security analysis requires a threat model whether it's fully formally specified or whether or not you're working with a more general template. So I've worked with threat models at some level or another in every security project or at least almost every security project that I've been involved with since I've been doing security in 2005.
In terms of how many actually ended up drafted or written out to some degree or another, that's a smaller set.
Sometimes I consulted with companies where they were going to make the more detailed document, and I was providing them with the expertise necessary to do that correctly.
So, for example, in 2015, there was a medical device manufacturer where we were helping them solve their security issues because medical

21

devices are on the market for a really long time because of how regulation and whatever else works, and so all of a sudden they had devices that were never intended to be on the network that were on a network. So they had almost no experience with understanding the threats that they were facing, so we guided them through creating their threat model.

I specifically drafted parts of the model specifically connecting up certain requirements they had with the way those were potentially exploitable, what the different threats would be that they would need to identify and deal with.

I did not create the entire document, but I assisted with drafting a part of it as well as provided the overall guidance for the entire document. So figuring out a count, I would say I have contributed to... Well, I'm not sure. Since I started doing security in 2005, I'm not sure.

Q When you do build or contribute to threat models, what types of methodologies do they use?

A Well, if you even look at the claim we

22

were just talking about, right, there's going to be a database in this claim, for example, where there are collected threats associated with a component.

So a big part of what a security professional like myself is expected to know is what are the types of threats that apply to different types of components under different types of circumstances.

So with my training, for example, in network security I have a deep insight into how attackers exploit devices that are on a network, what the mitigations do, what they can and can't do and how attackers still get around them.

So when I'm contributing to a threat model, some part of my expertise is even in knowing what threats apply where, and so if somebody is relying on me then in some ways I'm kind of serving as a human database for the different threats that are common or not even common but relevant, that's the better word, relevant to a given scenario. So that's one part

23

of it.

The other part of it is understanding how to prioritize in terms of, you know, if you've got X amount of dollars that goes into a system, understanding which threats are going to have the biggest impact is another part of the analysis so that clients can make an informed decision about how they're going to invest their defensive dollars in a way that's going to have the best outcomes.

So there's a knowledge component in terms of what are the threats, there is an experience or a wisdom component maybe you could call it in terms of which ones need the higher priorities and then of course, I also have extensive background in working with developing the mitigations that can be put into place to reduce the potential risks that a threat might cause.

Q Are there any specific named methodologies that you've used before such as NIST, for example, N-I-S-T?

A Well, so NIST has a number of different

24

frameworks that I use. For example, the NIST 800-171 SP -- sorry, SP, SP is special publication, NIST Special Publication 800-171 has a common set of controls. So you can think of these as if you're sitting down to try and figure out if you have good security, this is a good starting point to go through and see how your organization is or is not implementing these various controls on a system. Now, that's not a threat model, though. That's kind of like a menu of techniques that help to reduce threats. And so you would need a good threat model in order to know which of those -- which of those elements were important and relevant to your portion.

SP-853 I think it is another one that is kind of like a general security framework. And then I don't remember the number for it, but there is a risk -- there's actually more than one, but there's a risk set of documents that talk about how you identify risks, how you prioritize and then look at different solutions for dealing with those risks.

25

So there's a certain amount of documents that are helpful to somebody creating a threat model.

But I would say that the broader approach that I use is actually based on Ross Anderson's security engineering book which is the one I've used both when I was a student all the way back in 2004 until today I use this book both in my class and with my clients, and in it there are discussions about different ways for modeling threats.

I've mentioned in a previous deposition I mentioned, for example, the threat trees where you start with the problem and then work your way back. But more importantly, Anderson has the kind of engineering perspective of kind of the big picture of which threat modeling a part, and within that framework you can use just about any approach to threat modeling as long as you have the proper engineering principles that are applied to the security problem.

Q Have you ever used the STRIDE methodology

26

before?

A I've heard of STRIDE. I don't remember -- I don't remember off the top of my head what is in it. I'd have to look at it again to see if that maps up with the approach I've taken to doing threat modelling.

Q So if I understand your answer correctly, you can't recall what STRIDE stands for?

A I don't remember as I sit here, no.

Q Have you ever heard of threat modeling connect before this case?

A I have not.

Q Have you ever heard of threat modeling community before this case?

A You mean the community of people, like, with their conferences and whatever else?

Q Yes.

A I am familiar there is a threat modelling community, yes.

Q We talked a little bit earlier about threat modelling by hand and, you know, we talked a little bit about this during your last

27

deposition as well. But I could build a threat model using a whiteboard; is that right?

A You could represent -- I mean, I don't know that using is the right term. You can create a threat model through analysis and investigation and then you could find different ways of representing what you came up with including a whiteboard.

Q So you could use a whiteboard to represent your threat model; is that right?

A You could use a whiteboard to depict I would say at least parts. I'd have to -- I guess it would depend a little bit -- well, let me say it differently.

You could use a whiteboard to depict the analysis that you did -- I don't want to say it that way either. You could use a whiteboard to depict a representation of the threat model that you created.

Q Let's say I want to build a threat model for my everyday life be and I'm using my work laptop right now and let's say I determined -- you

28

know, I always use my work laptop in coffee shops and I've determined that, you know, bluejacking is a potential threat; is that fair?

A Sure.

Q So if I wanted to represent this information on a whiteboard, I could start by, you know, drawing a circle with the word "bluejacking" in it, right?

A I mean, I would say that you would need to develop the threat model and then, you know, that process might involve a lot of different things. You could be whiteboarding as a part of your analysis, but I don't know that I would say that you are creating a threat model just because you drew a circle on it.

Q I'm going to drop Exhibit 1001 in the chat here.

(A certain document was marked Nielson Deposition Exhibit 1001 for identification, as of 04/26/2024.)

BY THE WITNESS:

A I've got it.

29

BY MR. MIDDLETON:
Q Can you please look at Claim 1 of the '008 patent?
A All right, I have it now.
Q Do you see where it says the term: Configuring a diagram interface to and response to receiving one or more user inputs add a component group to the first threat model?
A Yes.
Q So the way this claim is structured, the diagram interface is configured to perform an action in response to one or more user inputs; is that right?
A In response to receiving one or more user inputs configure the diagram interface to add a component group to the first threat model.
Q Just so I'm using your response, are you saying the user input is received first?
A I think that is one way of reading this claim. I know I discuss this in my report that one way of reading this claim is in response to receiving one or more user inputs, configure the

30

diagram interface to add a component. I believe that is one reading of that limitation.
Q And what would be another reading of the limitation?
A Well, I find the commas to be something I just -- you know, I think I could read it a different way which is that there is a configuring the diagram interface. Configuring the diagram interface to in response to receiving one or more user inputs add a component word, in other words the configuring is first and the configuring has configured the interface such that in response to receiving one or more user inputs add a component group. I think that's another potential of way of reading that.
Q Which reading do you think is correct?
A Well, I don't know that I've done that analysis. I know the question that I was dealing with in my report is different, and I don't know that which way is reads affects that analysis.
So I don't know that I've gone further into which one I think is the absolute most

31

likely. I think either one is potentially correct, and it doesn't change the analysis I was asked to do, so I haven't gone much further than that.
Q Okay. Let's assume that the second interpretation is correct, so configuring the diagram interface comes first and then a user input is received.
So under this interpretation -- under that interpretation if the user input is received, the claim system will then add a component group to the first threat model; is that right?
A Well, just to be clear what I'm saying is there is a configuring that happens. So the system is configured -- so maybe I'm thinking about this like a programmer, right, like, in other words, if I create a program to do something, in my mind I've configured this program to do something, right, just by writing the program that does the thing. So configuring the diagram interface to, you would -- you would create the system and set it up such that when a

32

response is received, a component group is added so that the system has to be configured to do that.
Q And conversely, the system is configured such that if the user input is not received, the claim system will then not add a component group to the first threat model?
MR. JACKSON: Object to the form.
BY THE WITNESS:
A In either case the system receives an input and adds a component in doing this claim.
BY MR. MIDDLETON:
Q What do you mean "in either case"?
A Well, so let me go back to the first one. In fact, for this one I want to take this back to my report just to find where I've got it here.
So this is Paragraph 92 of my report. So this is for that first interpretation which is what I addressed here, Paragraph 92: "The example limitation from the '008 patent that were identified as 'configuring the diagram interface to in response to receiving one or more user

33

inputs add a component group to the first threat model.'"

In my opinion there is no condition present in this claim language. Instead to satisfy the claim, the claim requires that the system receive one or more user inputs and in response to the one or more inputs, configure the diagram interface to add a component group to the first threat model.

To satisfy the step, both the user inputs must be received and the diagram interface must be configured to add a component group.

Q Looking back at Claim 1 of the '008 patent?

A Yes.

Q Do you see where it says "a plurality of compensating controls"?

A Yes, I do.

Q What is your definition of compensating controls as used in the '008 patent?

MR. JACKSON: Object to the form.

BY THE WITNESS:

34

A I don't believe I've provided a construction for compensating controls, so I was viewing compensating controls from the perspective of a POSITA.

BY MR. MIDDLETON:

Q And what is your understanding of what compensating controls are?

A Well, an example of a compensating control would be like a mitigation for a potential threat. That would be one type of a compensating control.

Q What are some other types of compensating controls?

A Well, I'm looking at the patent, Exhibit 1001 here, sorry if I'm turning my head. I'm looking at Figure 12 which is rotated on my screen.

Under Figure 12, they give some examples of compensating controls like a firewall, a DLP would be another example I guess would be a good one, HIPS. So HIPS by the way stands for host intrusion prevention system. So Fireye, these are all examples of compensating controls.

35

Q I'm at Claim 1 again. Claim 1 also requires a relational diagram using visual representations of compensating controls; is that correct?

A Yes, correct.

Q How are compensating controls visually represented in the '008 patent?

A Well, for example, Figure 10 shows them drawn in the relational diagram. So in Figure 10 you can see the firewall drawn as a box with arrows going in and out of it. So I guess that would be one way that they're visually represented.

Q Staying on Figure 10, you see the top left right above the word toolbox there's a tab there that says "compensating controls," correct?

A Yes.

Q Then can we go to Column 20, Line 59?

A Column 20, yes, I have that. Line 59, yes, I have it.

Q And this says referring back to Figure 10: The compensating controls selector may be selected

36

to display a popup similar to compensating control report and then in (report) 1200 of Figure 12.

Did I read that correctly?

A Yes, I see. Yes, I see that.

Q So that tab we looked at earlier in Figure 10, that says "compensating controls," that's a tab that user can select and when a user selects that tab, it displays a popup of the compensating controls?

A Well, it says it displays a report, right, like we saw in Figure 12. Just so we're talking -- making sure I understand the context we're talking in, in the patent claim, the claim requires a diagram interface to display a relational diagram of compensating controls. So the report wouldn't be a relational diagram of compensating controls.

Q So you're saying that the compensating controls must be displayed in the diagram?

A Let me read here from the claim limitation again. The limitation reads: Configuring the diagram interface to display a relational diagram

37

of one of a system, application and a process using visual representations of one or more of the threat model components and visual representations of one or more of the compensating controls, the relational diagram defining a first threat model.

So this limitation requires displaying a relational diagram using visual representations of threat model components and visual representations of one or more of the compensating controls.

Q So you're saying that the compensating controls must be displayed in the diagram per the claim?

A Well, I'm saying it says: Display a relational diagram using visual representation of threat model components and visual representations of compensating controls.

So what must be displayed for this limitation is a relational diagram that uses those visual representations of threat model components and visual representations of compensating controls.

Q And those visual representations of

38

compensating controls can be displayed in a popup based on what we just read, right?

MR. JACKSON: Object to the form.

BY THE WITNESS:

A A popup would not be part of a relational diagram of a system, an application or a process. No, I should clarify.

A popup of a report is not a relational diagram of a system, an application or a process.

BY MR. MIDDLETON:

Q But a different type of popup would be a visual representation?

MR. JACKSON: Object to the form.

BY THE WITNESS:

A I don't know for sure. I haven't considered all possible popups. I'm simply saying in answer to your question about what we looked at here with Figure 12, that's not a relational -- it's not a part of a relational diagram.

BY MR. MIDDLETON:

Q Can we look at Figure 10 again?

A Of course. All right, I have Figure 10

39

now.

Q You said firewall, you said that was a compensating controls?

A Yes.

Q Isn't that a component?

A Well, firewall is a compensating control, it's listed as a compensating control, so is the active Akamai DNS. So multiple compensating controls are visualized here in this relational diagram.

MR. MIDDLETON: I think we can take a ten-minute break.

THE WITNESS: Sure.

(A recess was had.)

MR. MIDDLETON: I'm dropping Exhibit 1004 in the chat.

(A certain document was marked Nielson Deposition Exhibit 1004 for identification, as of 04/26/2024.)

BY THE WITNESS:

A While that's coming down, I wanted to make a clarification about something I said in the

40

previous hour.

Based on a couple of the questions you asked me triggered some thoughts in my head so I went back and looked at the transcript from my first deposition with you, and I just wanted to make sure so it didn't sound inconsistent.

In talking about the NIST framework, as I said today, I use these pieces the 800171 and the risk analysis and these other documents as part of doing my threat analysis, and so that is the framework that I was talking about in my first deposition. I just wanted to make sure that didn't come across as a contradiction.

BY MR. MIDDLETON:

Q Okay. Anything else you'd like to add?

A No, that's it.

Q All right. Let me know you when have Exhibit 1004.

A Yes, I have it right now.

Q So you have Exhibit 1004 in front of you, Dr. Nielson?

A I do.

41

Q And this is the Jones reference, correct?
A Correct.
Q Did you review this reference in preparation for your deposition?
A I did.
Q Jones generally discloses the content of an information system; is that right?
A I mean, it references information system within it.
Q And what is your understanding of the information system in Jones?
A Let's see. Jones says in Column 5 starting at Line 4: "The information system may include components such as hosts, processes, data stores and/or external entities and data flows between those components."
Q Can we look at Figure 9 of Jones.
A Yes, I have Figure 9.
Q And do you see where it says "example server"?
A Yes.
Q That's an example of a component, right?

42

A A component in the language of the '008 patent.
Q Well, Jones also calls these components components, right?
A Well, that's what I was asking which patent language you were asking about.
Q So under Jones, this is a component, right?
A Yes.
Q Under the '008 patent, this is a threat model component, right?
MR. JACKSON: Object to the form.
BY THE WITNESS:
A Well, once again, the definition of threat model components is a potential relevant source for one or more threats, and I would agree that the server is a potential source for threats.
So, yes, I would agree that that is a threat model component.
BY MR. MIDDLETON:
Q And the example server in Figure 9 is represented as a large rectangle with two other

43

components inside that rectangle; is that right?
A That is how it's visually depicted, yes.
Q And those two, you know, components that are inside the example server component are the authentication module and the example web server, right?
MR. JACKSON: Object to the form.
BY THE WITNESS:
A Correct.
BY MR. MIDDLETON:
Q And Jones would describe the authentication module in the example web server as nested within the example server, right?
MR. JACKSON: Object to the form.
BY THE WITNESS:
A Jones does not specifically describe these elements in Figure 8 as nested, so I'm not sure if Jones would describe these as nested components.
BY MR. MIDDLETON:
Q You said Figure 8 there but we're looking at Figure 9, right?
A I'm sorry. I might have been looking at

44

Figure 8. Let me -- let me correct myself. One moment.
I don't believe Jones describes the elements in Figure 9 as nested, either. So I'm not sure.
Q And just for clarification, were you looking at Figure 8 when I asked my questions earlier?
A I might have been -- the figures are very similar and so now I'm -- I'm questioning myself. I'm not sure. I have Figure 9 now if you want to re-ask it.
Q So Figure 9 shows a large rectangle labeled as example server 804, right?
A It does, yes.
Q And then inside that large rectangle labeled example server there are two components, right?
MR. JACKSON: Object to the form.
BY THE WITNESS:
A Sorry. Go ahead.
MR. JACKSON: I was just objecting to

45

form. Go ahead.
BY THE WITNESS:
A There are two other rectangles labeled authentication module and example web server. They're both numbered 806.
BY MR. MIDDLETON:
Q And you would agree that the example server is a threat model component, right?
A So in the language of the '008 patent, it is a threat model component to the extent that it is identified as a potential relevant source for one or more threats.
So assuming that threats are identified to the example server, it would be a threat model component.
Q And the authentication module is a threat model component as well, right?
MR. JACKSON: Object to the form.
BY THE WITNESS:
A Again, as I said before, assuming that there are threats identified for the authentication module, it would be a threat model

46

component.
BY MR. MIDDLETON:
Q And do you see the circle above authentication module labeled 904?
A I do.
Q That's a threat, right?
A Yes, it says that 904 is a shape for cybersecurity threats to various elements.
Q So the circle labeled 904 is a threat for the authentication module?
MR. JACKSON: Object to the form.
BY MR. MIDDLETON:
Q The circle above authentication module labeled 904 is a threat for the authentication module; is that right?
A Well, Jones doesn't say that that is a threat to the authentication module so it's not clear if it is a threat to the authentication module or to the example server.
Q And then same for the example web server, that's also -- well, scratch that.
The example web server you see there's

47

three circles above it labeled 904?
A I do see that.
Q So there are three threats next to the example web server?
A There are three circles labeled 904 directly above example web server inside the box labeled example server.
Q So example web server has threats associated with it, right?
A Well, Jones does not say that.
Q Based on your understanding looking at this figure?
A No, that's not clear to me. I mean, that is one possible interpretation, but it certainly is not the only possible interpretation.
Q So this box labeled example server, you know, either the example server, the authentication module or the example web server have threats that are associated with one or more of these components?
MR. JACKSON: Object to the form.
BY THE WITNESS:

48

A It appears that the circles 904 are associated with example server or modules within it. Jones doesn't state -- sorry, go ahead.
BY MR. MIDDLETON:
Q Go ahead and finish.
A Oh. Jones doesn't say that. Jones just says in Column 19 starting on Line 10: Figure 9 illustrates the GUI including a Level N threat model DFD 902 produced from the Level N DFD 902 and further including a number of shapes for cybersecurity threats 904 to various elements of the information system modeled by the DFD.
So Jones does not make any kind of mapping. Jones describes these as kind of exemplary, so I would say that they are within the box of the example server suggesting an association, but Jones does not identify what that is.
Q So your understanding would be then one or more of the example server or the modules within it are threat model components?
A So as I gave my answer before, Jones

49

describes them as components. From the perspective of the '008 patent if they have threats associated with them, then they become threat model components. It's not clear to me which components these 904 circles apply to.

At least within the example server, if they apply to any of the internal components, that's not clear. There appears to be an association with the example server in that they are inside of it.

Q So the authentication module and the example web server are associated with the example server?

A Correct.

Q And the way these components are visually depicted, they're grouped together?

A I mean they're drawn within the example server box.

Q How are these components added to Jones's system?

MR. JACKSON: Object to the form.

BY THE WITNESS:

50

A Well, I don't know that Jones specifically describes how this box was added to the system.

BY MR. MIDDLETON:

Q How are components in general, so not just talking about the example web server, but how are components in general added to Jones's diagram?

MR. JACKSON: Object to the form.

BY MR. MIDDLETON:

Q Does Jones's system make them up? Does a user add them?

A Well, so I'm looking specifically what Jones says about Figure 9, Jones says there is a GUI so there is a user interface.

It says that cybersecurity threats or rather their shapes are placed in the workspace. It does not say how those are placed, but it says: Attributes and even further attributes of the cybersecurity threats may be entered per their shape which sounds like a user would enter those attributes.

Q Do you see on the left side of Figure 9 where it says: Threat model drop quick shapes here?

It's labeled 704.

A Yes, I see that.

Q And what is this column where it's labeled 704?

A It appears to be a place where you can drag or otherwise select shapes for including on the diagram.

Q And these shapes are components according to Jones?

MR. JACKSON: Object to the form.

BY THE WITNESS:

A I mean, it's more than just components because it also includes threats and data flows.

BY MR. MIDDLETON:

Q Yeah, if you want to read directly from Jones, I mean, we can look at Column 18, Line 47.

A 47, yes. You want me to read that?

Q You don't have to. Just let me know if this comports with your understanding, this paragraph.

A Yes, it basically says what I just said.

52

It almost literally says what I just said. It says that there are components and data flows and threats, so that seems like a pretty good list.

Q So looking at that stencil 704, you were saying earlier that a user can, you know, select one of those components, data flows or threats and then drop them into the diagram; is that right?

A Drop or some other kind of entry. I don't know if Jones specifically says drop, but something -- some user interface mechanism like that.

Q If we look at Jones Column 5, Line 45.

A Yes, I have it.

Q So this says: The DFD creator 106 may be configured to identify elements of the information system and compose a DFD for the information system from those elements.

Did I read that right?

A You did.

Q So this is saying that the DFD creator can identify elements from the information system and then from those elements create a DFD?

53

A I mean, it says what it says, it says a DFD creator -- I mean, you read it, but I'll just say it again: A DFD creator may be configured to identify elements of the information system and compose a DFD for the information system from those elements.

Q So this DFD creator can create a new DFD creator from the elements, right, one that didn't exist before?

A This line, these lines here appears to be discussing the creation of a new DFD.

Q So moving to the next paragraph, first sentence, this reads: The DFD creator may also provide structured information including attributes of the components, correct?

A Yes.

Q What is your understanding of attributes?

A Well, it goes on to kind of explain a little bit about this, so it says that there may be some metadata schema associated with elements in the DFD and it gives examples. This structured information may include hardware, software, and

54

communication attributes of at least some of the components and data flows, and then some examples the structured information may include any authentication, authorization or security controls to which the components and data flows are subject.

Q Moving to the next paragraph, first sentence here says: The threat indicator 108 may be configured to identify a cybersecurity threat to a particular element of the elements of the information system and add a secondary node representing the cybersecurity threat to the DFD to thereby produce a threat model DFD to the information system; is that right?

A You read that correctly, yes.

Q So if I understand what Jones is doing correctly, so the previous step was the DFD creator creates a DFD with components and then the threat indicator adds secondary nodes representing threats to the DFD and once those threats are added, those components that are associated with those threats become threat model components and

55

that makes the threat model DFD?

A I'm sorry. I didn't hear the question. Was there a question at the end of the statement?

Q Sure. The question was just if I'm understanding Jones correctly.

A Jones describes a threat indicator that adds a secondary node representing the cybersecurity threat to the DFD and that produces a threat model DFD.

Q So the previous step was for the DFD creator to create a DFD with elements of the information system and that can include components, right?

A Yes.

Q And then this step is the threat indicator adding threats to those components making them threat model components, right?

MR. JACKSON: Object to the form.

BY THE WITNESS:

A Well, so what we read about here in this part about the threat indicator is it says it adds a secondary node representing the cybersecurity

56

threat to the DFD to create a threat model DFD, so that line doesn't in particular tell us about the creation of threat model components, but to the extent that any of these threats -- let me back up.

The threat model component has to be a -- let me just read this again. Has to be a potential relevant source for one or more threats.

So a threat model component could be a threat model component even before you identified the threat, so I guess to the extent that these threats were added because they were identified as being related to a component, that would make the component a threat model component.

Q And this passage's use of the term "secondary node," it doesn't say this explicitly but those would be labeled 904 on Figure 9, right?

A Jones doesn't say that explicitly I don't think. I'm not aware of a place that makes that connection. What it does describe here is having this system, this DFD and then threat indicator system that can add secondary nodes representing

57

the cybersecurity threats.
So Jones describes a system that can add secondary nodes representing the cybersecurity threat DFD. I'm not aware of a place where Jones says that the ones in 904 were created from that.
Q All right. We can move on to the next paragraph and this paragraph reads: In some examples it may be desirable to look deeper into one or more components of the information system such as to provide a more thorough analysis of those components or their cybersecurity threats, and these examples, the decomposer 110 may be configured to decompose one or more components of the information system modeled by the DFD into its nested components and data flows there between.
The decomposer may then provide feedback of its decomposition to the DFD creator 106 which may modify the threat model DFD for the decomposed components to include their nested components and data flows and appropriate metadata thereby producing a Level n+1 threat model DFD?
Is that right?

58

A You read that correctly, yes.
Q So what do you understand decompose to mean here?
A Well, I mean, I think Jones explains what the decomposing is. You read it already but I'll just read this part again: In these examples the decomposer 110 may be configured to decompose one or more components of the information system modeled by the DFD into its nested components and data flows there between.
Q So this is saying the decomposer decomposes a component into a group of related nested components; is that fair?
A Related to what just so I understand how you're using the word?
Q Related to the decomposed component.
A Yes, insofar as -- yes, it is -- like it says, it's a deeper level of the components of the decomposed component.
Q And in your declaration you say that this group of decomposed components was already present in the information system, right?

59

A Correct.
Q So the group of decomposed components already exist in the information system before the decomposition begins?
A Yes.
Q So the group of decomposed components exist in the information system but they're not yet modeled in the threat model DFD?
A Correct.
Q So then the decomposer provides feedback of that decomposition to the DFD creator?
A Yes.
Q And that essentially means that the decomposer -- sorry, scratch all that.
By provide feedback that really just means, you know, sending information, right?
A I think so if I understand what you're asking. I did talk about this and that feedback component. This is -- let me just pull this up here. Just one second.
Yes, so this is in my Paragraph 102 starting about halfway down: "On the other hand,

60

Jones describes the decomposer as doing unless when decomposing existing elements. As discussed above, Jones discloses decomposing components based on their existing hierarchy, however, it chooses to decompose (which elements get included in the n+1 decomposition) is up to the decomposer indicating that there is no 'predefined' component group."
Q So once the decomposer provides feedback of that decomposition to the DFD creator, the DFD creator can then modify the threat model DFD for the decomposed components to include their nested components; is that right?
A The way Jones says it, the decomposer may then provide feedback of its decomposition to the DFD creator 106 which may modify the threat model DFD for the decomposed components to include their nested components and data flows and appropriate metadata thereby producing a Level n+1 threat model DFD.
Q And what do you understand "modified" to mean here?

61

A Well, it's modified because there's now decomposed components.
Q So it's modified because decomposed components are now in the threat model DFD?
A There are now components being modeled that were not previously modeled.
Q Continuing to your declaration to 2003?
A Yes, which paragraph?
Q 81.
A Yes, I have Paragraph 81.
Q Here you define the term redefine the first threat model by including it -- by including in it a second threat model with the component group; is that right?
A I provide a construction for that phrase.
Q And what is your construction?
A As it says here also in Paragraph 81: "...change the first threat model by adding a predefined interrelated component group and its associated second threat model to the first threat model where the added component group was not a part of the first threat model before being

62

added."
Q So your construction changes the word "redefine" to the word "change"; is that right?
MR. JACKSON: Object to the form.
BY THE WITNESS:
A I don't think I would reduce it that simply, no.
BY MR. MIDDLETON:
Q So what is your understanding of the term "redefine" specifically?
MR. JACKSON: Object to the form.
BY THE WITNESS:
A Well, as I explain here in my declaration, the word "redefine" is given within the context of claim language. The Claim 1 -- the Claim 1 language explains that redefine has a meaning. It has a thereby word, thereby redefine indicating what the redefine is supposed to mean.
So I'm simply taking what the claim requires of redefine and putting it in as the definition.
Q Can we turn to Appendix A, the listing of

63

claims in your declaration?
A Yes, I have that.
Q So just taking a look at Claim 1, you don't dispute that Jones discloses providing one or more databases, correct?
MR. JACKSON: Object to the form.
BY THE WITNESS:
A I have not done an analysis as to whether or not Jones has databases with all of the requirements for Claim 1.
BY MR. MIDDLETON:
Q You don't dispute that Jones discloses that one or more databases comprise a plurality of threat model components stored therein, right?
A I don't have an analysis related to that.
Q And you don't dispute that Jones discloses that each threat -- sorry, scratch that.
You don't dispute that Jones discloses the one or more databases comprise a plurality of threats stored therein, correct?
A I do not have any analysis about this in my report.

64

Q And you don't dispute that Jones discloses that each threat is associated with at least one of the threat model components through the one or more databases, correct?
A I do not have any analysis about that in my report, either.
Q You don't dispute that Jones discloses that one or more databases comprise compensating controls stored therein, right?
A Hold on. I do not have any analysis about whether or not there is a database with compensating controls in Jones.
Q And you don't dispute that Jones discloses that the compensating controls are associated with at least one of the threats through the one or more databases, right?
A I don't have any analysis about that, either, in my report.
Q You don't dispute that Jones provides one or more interfaces including a diagram interface configured to be displayed on one or more end user computing devices communicatively coupled with the

65

one or more databases, correct?
A I do not have any analysis related to that element in my report.
Q And you don't dispute that Jones discloses configuring the diagram interface to display a relational diagram of one of a system and application and a process using visual representations of one or more of the threat model components, correct?
A I have provided my analysis that there's no configuring the diagram interface to display a relational diagram of one of a system, an application and a process using visual representations, one or more of the threat model components and visual representations of one or more of the compensating controls, and the analysis that I've given in that section is related to the compensating controls.
Q So the analysis in those sections isn't related to the other portions of this claim limitation, just the compensating controls?
A My report does not include any analysis

66

about there being or not being visual representations of one or more threat model components.
MR. MIDDLETON: I have no further questions.
MR. JACKSON: Can we take about a ten-minute break so I can take a look at my notes?
MR. MIDDLETON: Yes, no problem.
(A recess was had.)
EXAMINATION
BY MR. JACKSON:
Q Dr. Nielson, if I could direct you to your declaration, Page 39, this is the section that begins with Paragraph 96.
A Yes, I have it.
Q Okay. And do you recall earlier you were asked about whether Jones discloses aspects of this paragraph, this claim paragraph that you have here in your Paragraph 96?
MR. MIDDLETON: Object to form.
BY THE WITNESS:
A Yes.

67

BY MR. JACKSON:
Q I'm not sure what the objection is but let me just try to clean that up a little bit since I wasn't exactly clear.
So in Paragraph 96 you reproduce one of the paragraphs from Claim 1, correct?
A Yes.
Q And in the petition that paragraph was labeled Element 1-F; is that right?
A I believe that's correct. Let me just double-check real fast. Yes, that's correct.
Q Okay. And earlier today were you asked whether Jones discloses aspects of this Element 1-F?
MR. MIDDLETON: Object to form.
BY THE WITNESS:
A I was asked about aspects of this.
BY MR. JACKSON:
Q Okay. And just to clarify, are there any aspects of Element 1-F that are not disclosed in Jones?
MR. MIDDLETON: Object to form.

68

BY THE WITNESS:
A Well, yes, my report or my declaration lays out the parts that are not addressed. So as I say in Paragraph 98: "Jones does not satisfy these claim requirements." And the claim requirements are listed in Paragraph 97.
So reading from Paragraph 97 of my declaration: "This portion of Claim 1 requires that the component group that is added to the first threat model must comprise 'a predefined interrelated group of two or more of the threat model components,' thus the component group must be defined before it is added to the first threat model. The claim language also requires that the component group is added to the first threat model. This means that the component group could not have been part of the first threat model prior to being added. The claim language also explains that the addition of the component group to the first threat model thereby redefines the first threat model by including it in a second threat model associated with the component group, thus

69

the component group must have had its own second threat model before it was added to the first threat model. The addition of the component group also requires that the threat model of the component group is added to the first threat model."

Those pieces are what I say are not in the -- in Jones. Sorry. There is actually a little bit more later on. I don't know if you want to ask about any of these first or if I should just add the other piece.

Q Really I'm just asking, you know, what aspects of this Claim Element 1-F are not, in your opinion, disclosed by Jones. So if there are other aspects, please share those with me.

MR. MIDDLETON: Object to form.

BY THE WITNESS:

A Oh, sorry.

MR. MIDDLETON: Go ahead.

BY THE WITNESS:

A Yes, so the other piece is I talk about this in Paragraph 101, "Element 1-F requires that

70

a predefined interrelated component group of the threat model components must be added to the first threat model. Adding a component group does not occur in Jones because all components and subcomponents in the information system be examined are already present in the information system. Jones decomposer 110 breaking the Level n components into its Level n+1 subcomponents, but those subcomponents were already present. No component or component group was added to a first threat model in Jones' system.

And then, I'm sorry, there is one more, in Paragraph 102: "Element 1-F also requires that the component group that is added to the first threat model must be a predefined interrelated group of threat model components. Petitioner's expert, Mr. Hurlbut, argued that Jones discloses a predefined group of threat model components because the underlying information systems predefine."

And I'm going to skip ahead to a part I read earlier today: "As discussed above, Jones

71

discloses decomposing components based on their existing hierarchy, however, how it chooses to decompose which elements get included in the n+1 decomposition is up to the decomposer indicating that there is no predefined component group."

Q So the elements that are exposed in the decomposing process -- I'm sorry. Let me strike. Let me start over.

The components or the subcomponents that were exposed in the decomposing process, are you saying that those subcomponents were already part of the information system before the decomposition?

A Yes, that's what I say in my report. I just read that.

Q Okay. And those subcomponents that are exposed by the decomposition process, prior to them being exposed, do they have their own threat model?

A No. I also discuss that here that there was no threat model. That's what I was explaining earlier that these components don't get analyzed

72

for their threat model until after they're exposed.

Q And do you recall where in Jones that's discussed, if at all?

A Well, yes. So it's actually in the same paragraph that I was asked about earlier today, so I think we only got through about half of the paragraph. This is in Jones Column 6. Starting on about line -- what is that? -- 23: And, again, the threat indicator 108 may be applied to identify any cybersecurity threats to elements, nested components and data flows of the decomposed components and add appropriate secondary nodes and appropriate metadata representing those threats.

And then it goes on and actually almost throughout the rest of Jones it's talking about different ways that you do analysis on things, all of which would be done after the -- after this decomposition.

Q Bear with me just a minute.

Looking at the discussion about Figure 4, which starts on Column 14 of Jones, it says:

73

Figure 4 illustrates a threat analyzer 400," and then it goes on from there?
MR. MIDDLETON: Object to form. I don't think he testified about this on cross [sic].
MR. JACKSON: I understand, thanks, Matt.
BY MR. JACKSON:
Q This discussion of the threat analyzer with respect to Figure 4, does this provide any insight to you as to whether the subcomponents that are exposed by the decomposition process have a threat model associated with them prior to the decomposition process?
MR. MIDDLETON: Object to form.
BY THE WITNESS:
A So this is -- this process here is what I was just talking about, the threat analyzer in these other pieces are used in analyzing nodes that are to be modeled, and so this would be after the decomposition.
BY MR. JACKSON:
Q Is there anything else based on your testimony earlier today that you'd like to clarify

74

or elaborate on?
A Not that I'm aware of.
MR. JACKSON: That's all the questions I have, Matt. Pass the witness.
MR. MIDDLETON: No questions from me.
MR. JACKSON: Thank you, Dr. Nielson.
(Deposition concluded at 11:29 a.m. CST.)

75

CERTIFICATE OF COURT REPORTER - NOTARY PUBLIC
I, Theresa A. Vorkapic, Certified Shorthand Reporter No. 084-2589, CSR, RMR, CRR, RPR, and a Notary Public in and for the County of Kane, State of Illinois, the officer before whom the foregoing deposition was taken, do hereby certify that the foregoing transcript is a true and correct record of the testimony given; that said testimony was taken by me and thereafter reduced to typewriting under my direction; that reading and signing was not requested; and that I am neither counsel for, related to, nor employed by any of the parties to this case and have no interest, financial or otherwise, in its outcome.
IN WITNESS WHEREOF, I have hereunto set my hand and affixed my notarial seal this 30th day of April, 2024.
My commission expires November 6, 2027.

Theresa A Vorkapic

THERESA A. VORKAPIC
NOTARY PUBLIC IN AND FOR ILLINOIS

A
able
19:18
about
9:12, 12:22, 13:9, 15:13, 15:22, 16:1, 16:3, 16:12, 17:4, 17:5, 19:11, 20:5, 22:1, 23:7, 24:19, 25:10, 25:18, 26:20, 26:22, 31:16, 38:17, 39:22, 40:7, 40:11, 42:6, 50:5, 50:12, 53:19, 55:20, 55:21, 56:2, 59:18, 59:22, 63:21, 64:5, 64:10, 64:17, 66:1, 66:6, 66:17, 67:17, 69:10, 69:21, 72:6, 72:7, 72:9, 72:16, 72:21, 73:4, 73:16
above
35:15, 46:3, 46:13, 47:1, 47:6, 60:3, 70:22
absolute
30:22
access
15:10, 15:15, 16:6
accomplish
12:15
according
51:9
across
40:13
action
29:12
active
13:19, 13:20, 14:2, 39:8
actor
16:1, 16:2
actors
12:19
actually
9:19, 12:12, 19:21, 20:13, 24:18, 25:5, 69:8, 72:5, 72:15
adam
10:21
add
18:18, 29:7, 29:15, 30:1, 30:10, 30:13, 31:11, 32:6, 33:1, 33:8, 33:12, 40:15, 50:10, 54:11, 56:22, 57:2, 69:11, 72:13
added
32:1, 49:19, 50:2, 50:6, 54:21, 56:12, 61:21, 62:1, 68:9, 68:13, 68:15, 68:18, 69:2, 69:5, 70:2, 70:10, 70:14
adding
55:16, 61:18, 70:3
addition
68:19, 69:3
additional
14:9, 16:16
address
14:22
addressed
32:19, 68:3
adds
19:4, 32:11, 54:19, 55:7, 55:21
adequate
14:17
adversaries
14:5
adversary
13:19, 13:20
affects
30:20
affixed
75:16
after
72:1, 72:18, 73:18
again
13:12, 14:6, 26:4, 35:1, 36:21, 38:21, 42:14, 45:20, 53:3, 56:7, 58:6, 72:9
agarwal
4:11, 10:18
agree
42:16, 42:18, 45:7
ahead
44:21, 45:1, 48:3, 48:5, 69:19, 70:21
akamai
39:8
all
6:13, 7:12, 10:7, 11:19, 15:1, 16:3, 17:2, 21:3, 25:7, 29:4, 34:22, 38:16, 38:22, 40:17, 57:6, 59:14, 63:9, 70:4, 72:4, 72:17, 74:3
allow
15:17
almost
20:10, 21:5, 52:1, 72:15
already
14:13, 58:5, 58:21, 59:3, 70:6, 70:9, 71:11
also
9:14, 9:19, 13:11, 15:19, 23:15, 35:1, 42:3, 46:21, 51:14, 53:13, 61:17, 68:14, 68:18, 69:4, 70:13, 71:20
alter
14:1
always
28:1
amount
14:13, 17:13, 23:4, 25:1
analysis
7:20, 9:2, 9:3, 9:11, 10:1, 13:11, 14:14, 14:15, 14:16, 15:9, 19:16, 20:5, 23:6, 27:5, 27:16, 28:13, 30:18, 30:20, 31:2, 40:9, 40:10, 57:10, 63:8, 63:15, 63:21, 64:5, 64:10, 64:17, 65:2, 65:10, 65:17, 65:19, 65:22, 72:17
analyzed
71:22
analyzer
73:1, 73:7, 73:16
analyzing
73:17
anderson
25:15

anderson's
25:5
ands
13:15
annotations
6:6
another
9:19, 20:9, 20:14, 23:6, 24:15, 30:3, 30:14, 34:19
answer
26:7, 38:17, 48:22
answered
13:4
answering
20:5
anurag
10:18
any
5:15, 5:19, 5:21, 6:6, 6:7, 7:22, 9:6, 9:7, 16:19, 19:16, 20:5, 23:19, 25:18, 48:13, 49:7, 54:3, 56:4, 63:21, 64:5, 64:10, 64:17, 65:2, 65:22, 67:19, 69:10, 72:11, 73:8, 75:13
anything
6:9, 6:12, 40:15, 73:21
apparently
7:16
appeal
1:1, 9:14
appears
7:6, 48:1, 49:8, 51:6, 53:10
appendix
62:22
application
18:11, 37:1, 38:6, 38:9, 65:7, 65:13
applied
25:20, 72:10
apply
13:14, 22:7, 22:17, 49:5, 49:7
approach
25:4, 25:19, 26:5
approaches
12:20
appropriate
57:20, 60:18, 72:13, 72:14
approve
16:7
apps
6:12
april
1:15, 75:17
argued
70:17
around
22:14
arrows
35:11
asked
31:3, 40:3, 44:7, 66:17, 67:12, 67:17, 72:6
asking
17:4, 17:5, 42:5, 42:6, 59:18, 69:12
aspects
19:19, 66:17, 67:13, 67:17, 67:20, 69:13, 69:15
assisted
9:8, 21:15
associated
18:3, 18:21, 22:3, 47:9, 47:19, 48:2, 49:3, 49:12, 53:20, 54:21, 61:20, 64:2, 64:14, 68:22, 73:11
association
48:17, 49:9
assume
31:5
assuming
45:13, 45:20
attached
4:7
attackers
22:12, 22:14
attempting
14:4
attributes
50:17, 50:20, 53:15, 53:17, 54:1
authentication
14:17, 43:5, 43:12, 45:4, 45:16, 45:22, 46:4, 46:10, 46:13, 46:14, 46:17, 46:18, 47:18, 49:11, 54:4
authorization
14:17, 54:4
automated
17:16, 19:7
automation
17:5, 17:10, 17:11, 17:19, 19:12, 19:14, 19:17
available
12:11
aware
56:19, 57:4, 74:2

B

back
25:7, 25:15, 32:14, 32:15, 33:13, 35:21, 40:4, 56:4
background
8:3, 23:15
backing
7:3
bad
15:22, 16:2
bank
15:13
based
16:12, 16:13, 16:14, 25:5, 38:2, 40:2, 47:11, 60:4, 71:1, 73:21
basically
51:22
bear
72:20
because
20:22, 21:2, 28:14, 51:14, 56:12, 61:1, 61:3, 70:4, 70:19
become
49:3, 54:22
been
5:6, 6:13, 8:10, 9:11, 11:20, 19:21, 20:11, 20:12, 43:22, 44:9, 68:17
before
1:1, 2:5, 10:9, 10:13, 10:16, 10:19, 10:22, 11:5, 11:9, 11:12, 11:15, 11:18, 23:20, 26:1, 26:11, 26:14, 45:20, 48:22, 53:9, 56:10, 59:3, 61:22, 68:13,

69:2, 71:12, 75:5
begins 59:4, 66:14
behalf 3:2, 3:11
being 9:10, 14:7, 56:13, 61:5, 61:22, 66:1, 68:18, 71:18
believe 7:18, 30:1, 34:1, 44:3, 67:10
best 5:16, 23:9
better 9:12, 10:2, 22:21
between 12:10, 41:16, 57:15, 58:10
big 22:5, 25:16
biggest 23:6
bit 8:20, 26:20, 26:22, 27:13, 53:19, 67:3, 69:9
bluejacking 28:2, 28:7
board 1:1
book 25:6, 25:8
both 8:21, 25:7, 25:8, 33:10, 45:5
box 35:10, 47:6, 47:16, 48:16, 49:18, 50:2
break 39:12, 66:7
breaking 70:7
broader 25:4
build 16:17, 21:20, 27:1, 27:20
built 14:12, 14:13

C

call 9:2, 23:13
called 5:6, 8:6
calls 42:3
came 27:7
can't 5:15, 22:13, 26:8
case 10:10, 10:13, 10:16, 10:19, 10:22, 11:6, 11:9, 11:12, 11:15, 11:18, 26:11, 26:14, 32:10, 32:13, 75:13
cause 23:18
certain 6:16, 14:3, 14:12, 19:18, 21:10, 25:1, 28:18, 39:17
certainly 19:6, 47:14
certificate 75:1
certified 2:6, 2:7, 75:2
certify 75:7
cetera 12:11
challenge 20:4
change 14:1, 31:2, 61:18
change" 62:3
changes 62:2
chat 28:16, 39:16
check 7:19
chooses 60:5, 71:2
circle 28:7, 28:15, 46:3, 46:9, 46:13
circles 47:1, 47:5, 48:1, 49:5
circumstances 22:9
claim 7:17, 7:18, 7:21, 17:22, 21:22, 22:2, 29:2, 29:10, 29:20, 29:21, 31:11, 32:6, 32:11, 33:4, 33:5, 33:13, 35:1, 36:13, 36:20, 37:12, 62:15, 62:19, 63:3, 63:10, 65:20, 66:18, 67:6, 68:5, 68:8, 68:14, 68:18, 69:13
claims 7:15, 7:16, 17:18, 63:1
clarification 39:22, 44:6
clarify 38:7, 67:19, 73:22
class 25:8
classes 8:22
classification 9:15
clean 67:3
clear 31:13, 46:18, 47:13, 49:4, 49:8, 67:4
client 9:1, 14:20, 16:10
clients 8:22, 23:7, 25:9
coalition 16:1, 16:9
code 8:15
coffee 28:1
collected 22:3
column 35:18, 35:19, 41:12, 48:7, 51:4, 51:17, 52:12, 72:8, 72:22
com 3:9, 3:18
come 40:13
comes 31:7
coming 13:10, 39:21
commas 30:5
commission 75:18
common 8:14, 13:17, 22:20, 22:21,

24:4
communication
54:1
communicatively
18:8, 64:22
community
26:14, 26:15, 26:19
companies
20:16
company
8:12, 9:4
compensating
18:5, 18:14, 33:17, 33:19, 34:2, 34:3, 34:7, 34:8, 34:10, 34:11, 34:18, 34:22, 35:3, 35:6, 35:16, 35:22, 36:1, 36:6, 36:9, 36:15, 36:17, 36:18, 37:4, 37:9, 37:10, 37:16, 37:20, 38:1, 39:3, 39:6, 39:7, 39:8, 64:8, 64:12, 64:14, 65:16, 65:18, 65:21
complete
7:6
component
18:18, 18:21, 18:22, 19:5, 22:4, 23:11, 23:13, 29:7, 29:16, 30:1, 30:10, 30:13, 31:11, 32:1, 32:6, 32:11, 33:1, 33:8, 33:12, 39:5, 41:22, 42:1, 42:7, 42:11, 42:19, 43:4, 45:8, 45:10, 45:15, 45:17, 46:1, 56:6, 56:9, 56:10, 56:13, 56:14, 58:12, 58:16, 58:19, 59:19, 60:7, 61:13, 61:19, 61:21, 68:9, 68:12, 68:15, 68:16, 68:19, 68:22, 69:1, 69:3, 69:5, 70:1, 70:3, 70:10, 70:14, 71:5
components
14:11, 18:2, 18:4, 18:13, 19:2, 22:8, 37:3, 37:8, 37:15, 37:19, 41:14, 41:16, 42:3, 42:4, 42:15, 43:1, 43:3, 43:18, 44:17, 47:20, 48:21, 49:1, 49:4, 49:5, 49:7, 49:15, 49:19, 50:4, 50:6, 51:9, 51:13, 52:2, 52:6, 53:15, 54:2, 54:5, 54:18, 54:21, 54:22, 55:13, 55:16, 55:17, 56:3, 57:9, 57:11, 57:13, 57:15, 57:19, 58:8, 58:9, 58:13, 58:18, 58:21, 59:2, 59:6, 60:3, 60:12, 60:13, 60:17, 60:18, 61:2, 61:4, 61:5, 63:14, 64:3, 65:9, 65:15, 66:3, 68:12, 70:2, 70:4, 70:8, 70:16, 70:18, 71:1, 71:9, 71:22, 72:12, 72:13
comports
51:20
compose
52:16, 53:5
comprise
14:11, 63:13, 63:19, 64:8, 68:10
comprises
18:22
computer
6:10, 8:11, 16:20, 16:21, 17:9, 19:9
computers
17:4, 17:6, 17:7
computing
18:7, 64:22
conceptual
12:18, 13:13
concerned
16:12
concluded
74:7
condition
33:3
conducted
1:14, 2:4
conferences
26:16
configure
29:15, 29:22, 33:7
configured
18:6, 29:11, 30:12, 31:15, 31:18, 32:2, 32:4, 33:12, 52:15, 53:3, 54:9, 57:13, 58:7, 64:21
configuring
18:9, 18:16, 29:6, 30:7, 30:8, 30:11, 31:6, 31:14, 31:20, 32:21, 36:21, 65:5, 65:11
connect
26:11
connecting
21:10
connection
56:20
consider
13:5
considered
38:16
considering
10:3
construct
17:16
construction
34:2, 61:15, 61:16, 62:2
consulted
20:16
consulting
8:14
content
41:6
context
36:12, 62:14
continuing
61:7
contradiction
40:13
contribute
21:20
contributed
21:18
contributing
22:15
control
34:8, 34:10,

36:1, 39:6, 39:7
controls
15:15, 15:17, 18:5, 18:14, 24:4, 24:9, 33:17, 33:20, 34:2, 34:3, 34:7, 34:12, 34:18, 34:22, 35:3, 35:6, 35:16, 35:22, 36:6, 36:9, 36:15, 36:17, 36:19, 37:4, 37:9, 37:11, 37:16, 37:21, 38:1, 39:3, 39:9, 54:4, 64:9, 64:12, 64:14, 65:16, 65:18, 65:21
conversely
32:4
correct
6:5, 7:5, 8:8, 8:13, 30:16, 31:2, 31:6, 35:4, 35:5, 35:16, 41:1, 41:2, 43:9, 44:1, 49:14, 53:15, 59:1, 59:9, 63:5, 63:20, 64:4, 65:1, 65:9, 67:6, 67:10, 67:11, 75:8
corrections
7:22
correctly
19:21, 20:19, 26:7, 36:3, 54:15, 54:17, 55:5, 58:1
could
8:18, 9:11, 23:13, 27:1, 27:3, 27:6, 27:9, 27:11, 27:15, 27:17, 28:6, 28:12, 30:6, 56:9, 66:12, 68:16
counsel
75:12
count
21:17
county
75:4
couple
40:2
coupled
18:8, 64:22
course
23:15, 38:22
court
75:1
create
16:15, 17:7, 21:14, 27:4, 31:17, 31:22, 52:22, 53:7, 55:11, 56:1
created
27:19, 57:5
creates
54:18
creating
11:21, 12:9, 17:9, 21:7, 25:2, 28:14
creation
53:11, 56:3
creator
52:14, 52:20, 53:2, 53:3, 53:7, 53:8, 53:13, 54:18, 55:11, 57:17, 59:11, 60:10, 60:11, 60:16
crimson
8:7, 8:11
cross
73:4
crr
1:21, 75:3
csr
1:21, 75:3
cst
1:16, 74:7
currently
7:13
cybersecurity
8:4, 9:4, 9:21, 10:1, 15:3, 46:8, 48:11, 50:14, 50:18, 54:9, 54:12, 55:8, 55:22, 57:1, 57:3, 57:11, 72:11

D

data
16:13, 41:14, 41:15, 51:14, 52:2, 52:6, 54:2, 54:5, 57:15, 57:20, 58:10, 60:18, 72:12
database
22:2, 22:19, 64:11
databases
18:1, 18:9, 19:10, 63:5, 63:9, 63:13, 63:19, 64:4, 64:8, 64:16, 65:1
day
75:16
de
10:15
deal
13:16, 21:13
dealing
13:1, 16:2, 16:8, 24:21, 30:18
dealt
9:21
decision
23:7
decisions
9:12
declaration
4:13, 6:14, 7:2, 7:4, 7:7, 7:9, 7:12, 58:20, 61:7, 62:13, 63:1, 66:13, 68:2, 68:8
decompose
57:13, 58:2, 58:7, 60:5, 71:3
decomposed
57:18, 58:16, 58:19, 58:21, 59:2, 59:6, 60:12, 60:17, 61:2, 61:3, 72:12
decomposer
57:12, 57:16, 58:7, 58:11, 59:10, 59:14, 60:1, 60:6, 60:9, 60:14, 70:7, 71:4
decomposes
58:12
decomposing
58:5, 60:2, 60:3, 71:1, 71:7, 71:10
decomposition
57:17, 59:4, 59:11, 60:6, 60:10, 60:15, 71:4, 71:13, 71:17, 72:19, 73:10, 73:12, 73:19
deep
22:11
deeper
57:8, 58:18
defensive
23:8
define
61:11

defined
68:13
defining
18:15, 37:5
definition
33:19, 42:14, 62:21
degree
20:14
delaware
3:7
depend
27:13
dependent
7:17
depending
14:19
depends
12:3
depict
27:11, 27:15, 27:18
depicted
43:2, 49:16
deposition
1:13, 2:3, 4:9, 5:18, 6:17, 7:10, 10:6, 25:12, 27:1, 28:19, 39:18, 40:5, 40:12, 41:4, 74:7, 75:6
describe
8:18, 12:1, 43:11, 43:16, 43:18, 56:20
describes
44:3, 48:14, 49:1, 50:2, 55:6, 57:2, 60:1
describing
16:19
desirable
57:8
detail
16:17
detailed
20:17
details
13:7
determined
27:22, 28:2
develop
28:10
developed
20:3
developing
19:22, 23:16
device
20:21
devices
18:8, 21:1, 21:3, 22:12, 64:22
dfd
48:9, 48:12, 52:14, 52:16, 52:20, 52:22, 53:2, 53:3, 53:5, 53:7, 53:11, 53:13, 53:21, 54:12, 54:13, 54:17, 54:18, 54:20, 55:1, 55:8, 55:9, 55:10, 55:11, 56:1, 56:21, 57:4, 57:14, 57:17, 57:18, 57:21, 58:9, 59:8, 59:11, 60:10, 60:11, 60:16, 60:17, 60:20, 61:4
diagram
18:6, 18:9, 18:10, 18:15, 18:17, 29:6, 29:11, 29:15, 30:1, 30:8, 31:7, 31:21, 32:21, 33:8, 33:11, 35:2, 35:9, 36:14, 36:15, 36:16, 36:19, 36:22, 37:5, 37:7, 37:11, 37:14, 37:18, 38:6, 38:9, 38:19, 39:10, 50:6, 51:8, 52:7, 64:20, 65:5, 65:6, 65:11, 65:12
diagrams
11:21, 16:22, 17:8
different
12:10, 12:19, 13:3, 13:4, 14:21, 16:19, 17:1, 19:12, 19:14, 19:17, 21:12, 22:8, 22:20, 23:22, 24:21, 25:10, 27:6, 28:11, 30:7, 30:19, 38:11, 72:17
differently
15:15, 27:14
direct
66:12
directed
17:18
direction
75:10
directly
47:6, 51:16
disclosed
67:20, 69:14
discloses
41:6, 60:3, 63:4, 63:12, 63:16, 63:18, 64:1, 64:7, 64:13, 65:4, 66:17, 67:13, 70:17, 71:1
discuss
29:20, 71:20
discussed
60:2, 70:22, 72:4
discussing
53:11
discussion
72:21, 73:7
discussions
9:20, 25:10
display
18:10, 36:1, 36:14, 36:22, 37:13, 65:5, 65:11
displayed
18:7, 36:19, 37:11, 37:17, 38:1, 64:21
displaying
37:6
displays
36:8, 36:10
dispute
63:4, 63:12, 63:16, 63:18, 64:1, 64:7, 64:13, 64:19, 65:4
dla
3:4
dlp
34:18
dns
39:8
document
6:16, 20:18, 21:14, 21:17, 28:18, 39:17
documents
5:19, 5:21, 5:22, 6:7, 24:19, 25:1, 40:9
doing
20:12, 21:19, 26:5, 32:11, 40:10, 54:16, 60:1
dollars
23:4, 23:9

donald
3:12, 3:18
done
8:20, 9:3, 9:5, 9:11, 11:19, 15:1, 15:18, 19:8, 30:17, 63:8, 72:18
double
7:19
double-check
67:11
down
12:10, 13:7, 13:8, 13:10, 24:5, 39:21, 59:22
downloading
6:21
dr
5:10, 40:21, 66:12, 74:6
draft
7:6
drafted
20:3, 20:14, 21:9
drafting
19:22, 21:15
drag
51:7
draw
17:8
drawing
11:20, 16:22, 19:9, 28:7
drawn
35:9, 35:10, 49:17
drew
28:15
drive
3:14
drop
28:16, 50:22, 52:7, 52:8, 52:9
dropping
39:15
duly
5:4, 5:6
during
26:22

E

each
63:17, 64:2
earlier
19:20, 26:20, 36:5, 44:8, 52:5, 66:16, 67:12, 70:22, 71:22, 72:6, 73:22
easier
19:18
either
16:22, 27:17, 31:1, 32:10, 32:13, 44:4, 47:17, 64:6, 64:18
elaborate
74:1
electronic
5:22
element
54:10, 65:3, 67:9, 67:13, 67:20, 69:13, 69:22, 70:13
elements
24:13, 43:17, 44:4, 46:8, 48:11, 52:15, 52:17, 52:21, 52:22, 53:4, 53:6, 53:8, 53:20, 54:10, 55:11, 60:2, 60:5, 71:3, 71:6, 72:11
else
6:9, 8:2, 21:2, 26:16, 40:15, 73:21
employed
75:12
end
18:7, 55:3, 64:21
ended
20:13
enforcement
14:18
engineering
8:12, 25:6, 25:16, 25:20
ensuring
15:19
enter
50:19
entered
50:18
entire
21:14, 21:16
entities
41:15
entry
52:8
esquire
3:3, 3:12
essentially
59:13
et
12:11
even
12:4, 13:22, 21:22, 22:16, 22:20, 50:17, 56:10
ever
10:9, 10:12, 10:15, 10:18, 10:21, 11:5, 11:8, 11:11, 11:14, 25:22, 26:10, 26:13
every
20:10
everyday
27:21
exactly
15:1, 67:4
examination
4:2, 4:3, 4:4, 5:8, 66:10
examined
5:7, 70:6
example
13:2, 13:9, 13:17, 15:12, 17:12, 20:20, 22:2, 22:10, 23:20, 24:1, 25:13, 32:19, 34:8, 34:19, 35:8, 41:19, 41:22, 42:21, 43:4, 43:5, 43:12, 43:13, 44:14, 44:17, 45:4, 45:7, 45:14, 46:19, 46:20, 46:22, 47:4, 47:6, 47:7, 47:8, 47:16, 47:17, 47:18, 48:2, 48:16, 48:20, 49:6, 49:9, 49:12, 49:17, 50:5
examples
34:17, 34:22, 53:21, 54:2, 57:8, 57:12, 58:6
exemplary
48:15
exhibit
4:11, 4:12, 4:13, 6:15, 6:17, 28:16, 28:19, 34:14, 39:15, 39:18, 40:18, 40:20
exhibits
4:9
exist
53:9, 59:3, 59:7
existing
12:17, 13:11,

60:2, 60:4, 71:2
expected
22:6
experience
8:19, 21:5, 23:12
experiences
16:14
expert
70:17
expertise
8:4, 9:22, 10:7, 20:19, 22:16
expires
75:18
explain
53:18, 62:13
explaining
71:21
explains
58:4, 62:16, 68:18
explanation
9:6
explicitly
56:16, 56:18
exploit
22:12
exploitable
21:12
exposed
71:6, 71:10, 71:17, 71:18, 72:2, 73:10
extensive
23:15
extent
16:22, 45:10, 56:4, 56:11
external
13:1, 15:16, 41:15

F

facing
21:6
fact
32:15
fair
28:3, 58:13
familiar
11:1, 26:18
fashion
17:16
fast
67:11
feedback
57:16, 59:10, 59:15, 59:18, 60:9, 60:15
few
5:12
figure
24:5, 34:15, 34:17, 35:8, 35:9, 35:14, 35:21, 36:2, 36:6, 36:11, 38:18, 38:21, 38:22, 41:17, 41:18, 42:21, 43:17, 43:20, 43:21, 44:1, 44:4, 44:7, 44:11, 44:13, 47:12, 48:7, 50:12, 50:21, 56:17, 72:21, 73:1, 73:8
figures
44:9
figuring
21:17
final
19:16
financial
16:7, 75:14
find
27:6, 30:5, 32:16
finish
48:5
firewall
34:18, 35:10, 39:2, 39:6
fireye
34:21
firm
8:6
first
5:6, 18:15, 18:19, 29:8, 29:16, 29:18, 30:11, 31:7, 31:12, 32:7, 32:14, 32:18, 33:1, 33:9, 37:5, 40:5, 40:11, 53:12, 54:7, 61:12, 61:18, 61:20, 61:22, 68:10, 68:13, 68:15, 68:17, 68:20, 69:2, 69:5, 69:10, 70:2, 70:10, 70:14
flows
41:15, 51:14, 52:2, 52:6, 54:2, 54:5, 57:15, 57:20, 58:10, 60:18, 72:12
follows
5:7
foregoing
75:6, 75:7
form
17:20, 32:8, 33:21, 38:3, 38:13, 42:12, 43:7, 43:14, 44:19, 45:1, 45:18, 46:11, 47:21, 49:21, 50:7, 51:11, 55:18, 62:4, 62:11, 63:6, 66:20, 67:15, 67:22, 69:16, 73:3, 73:13
formally
20:7
founded
8:9
founder
8:6
framework
24:16, 25:18, 40:7, 40:11
frameworks
24:1
friday
1:15
front
40:20
fully
20:6
further
30:21, 31:3, 48:10, 50:17, 66:4

G

gave
48:22
general
17:4, 17:6, 20:8, 24:16, 50:4, 50:6
generally
19:11, 41:6
getting
9:18, 13:8
give
5:15, 13:8, 34:17
given
22:22, 62:14, 65:17, 75:8
gives
53:21
go
24:7, 32:14, 35:18, 44:21, 45:1, 48:3, 48:5, 69:19
goals
12:5, 12:6
goes
15:19, 16:4, 23:4, 53:18, 72:15, 73:2

going
9:17, 13:16, 14:12, 14:14, 15:8, 20:17, 22:1, 23:5, 23:8, 23:9, 28:16, 35:11, 70:21
gone
30:21, 31:3
good
5:10, 5:11, 9:7, 24:6, 24:12, 34:19, 52:3
greensboro
3:14
ground
7:15
group
18:18, 18:21, 18:22, 19:1, 19:5, 29:8, 29:16, 30:14, 31:11, 32:1, 32:6, 33:1, 33:8, 33:12, 58:12, 58:21, 59:2, 59:6, 60:8, 61:14, 61:19, 61:21, 68:9, 68:11, 68:12, 68:15, 68:16, 68:19, 68:22, 69:1, 69:3, 69:5, 70:1, 70:3, 70:10, 70:14, 70:16, 70:18, 71:5
grouped
49:16
guess
17:1, 27:12, 34:19, 35:11, 56:11
gui
48:8, 50:13
guidance
21:16
guided
21:7

H

half
72:7
halfway
59:22
hand
5:3, 11:20, 12:1, 15:1, 15:9, 16:18, 19:13, 19:15, 26:21, 59:22, 75:16
happens
31:14
hardware
53:22
head
26:3, 34:14, 40:3
hear
55:2
heard
10:9, 10:12, 10:15, 10:18, 10:21, 11:5, 26:2, 26:10, 26:13
help
9:9, 17:16, 24:11
helpful
25:2
helping
20:21
here
7:19, 8:1, 26:9, 28:17, 32:16, 32:19, 34:14, 36:20, 38:18, 39:9, 51:1, 53:10, 54:8, 55:20, 56:20, 58:3, 59:20, 60:22, 61:11, 61:17, 62:13, 66:19, 71:20, 73:15
hereby
75:6
herein
5:6
hereunto
75:15
hierarchy
60:4, 71:2
high
13:6
higher
12:4, 23:14
highest
12:21
hips
34:20
historical
16:13
hold
64:10
host
34:20
hosts
41:14
hour
40:1
however
60:4, 71:2
human
22:19
hurlbut
7:19, 70:17
hypothetical
14:13

I

idea
9:7, 17:12
identification
6:18, 28:20, 39:19
identified
32:21, 45:11, 45:13, 45:21, 56:10, 56:12
identify
14:21, 21:13, 24:20, 48:17, 52:15, 52:21, 53:4, 54:9, 72:11
illinois
2:9, 75:5, 75:22
illustrates
48:8, 73:1
impact
23:6
implementing
24:8
important
24:14
importantly
25:15
inc
1:3, 1:6
include
41:14, 53:22, 54:3, 55:12, 57:19, 60:12, 60:17, 65:22
included
60:5, 71:3
includes
51:14
including
18:6, 18:20, 27:7, 48:8, 48:10, 51:7, 53:14, 61:12, 64:20, 68:21
inconsistent
40:6
indicating
60:7, 62:17, 71:4
indicator
54:8, 54:19, 55:6, 55:15, 55:21, 56:21, 72:10
individuals
12:6

information
16:7, 16:15, 17:14, 19:9, 28:6, 41:7, 41:8, 41:11, 41:13, 48:12, 52:15, 52:16, 52:21, 53:4, 53:5, 53:14, 53:22, 54:3, 54:11, 54:14, 55:12, 57:9, 57:14, 58:8, 58:22, 59:3, 59:7, 59:16, 70:5, 70:6, 70:19, 71:12
informed
23:7
input
19:4, 29:18, 31:8, 31:10, 32:5, 32:11
inputs
18:18, 29:7, 29:12, 29:15, 29:22, 30:10, 30:13, 33:1, 33:6, 33:7, 33:10
inside
43:1, 43:4, 44:16, 47:6, 49:10
insider
12:22, 13:2, 15:5, 15:10, 15:14
insight
22:11, 73:9
insofar
58:17
instead
33:4
insurance
9:4, 9:15, 9:21
intended
21:4
intercept
13:21
interest
75:14
interface
18:6, 18:10, 18:17, 19:4, 29:6, 29:11, 29:15, 30:1, 30:8, 30:9, 30:12, 31:7, 31:21, 32:21, 33:8, 33:11, 36:14, 36:22, 50:13, 52:10, 64:20, 65:5, 65:11
interfaces
18:5, 64:20
interference
14:2
internal
15:17, 49:7
interpretation
31:6, 31:9, 31:10, 32:18, 47:14, 47:15
interrelated
19:1, 61:19, 68:11, 70:1, 70:15
intrusion
34:21
inventory
14:14
invest
23:8
investigation
15:11, 27:5
investments
10:3
investors
9:20
involve
28:11
involved
19:21, 20:11
involves
8:4, 11:20
ipr
1:9
iriusrisk
1:3, 10:9, 11:8
issue
14:6
issues
13:5, 20:22

J

jackson
3:12, 4:4, 17:20, 32:8, 33:21, 38:3, 38:13, 42:12, 43:7, 43:14, 44:19, 44:22, 45:18, 46:11, 47:21, 49:21, 50:7, 51:11, 55:18, 62:4, 62:11, 63:6, 66:6, 66:11, 67:1, 67:18, 73:5, 73:6, 73:20, 74:3, 74:6
jackson@rimonlaw
3:18
james
1:13, 2:3, 4:2, 5:5
job
1:18
john
11:5
jones
4:12, 6:1, 41:1, 41:6, 41:11, 41:12, 41:17, 42:3, 42:7, 43:11, 43:16, 43:18, 44:3, 46:16, 47:10, 48:3, 48:6, 48:13, 48:14, 48:17, 48:22, 50:1, 50:12, 51:10, 51:17, 52:9, 52:12, 54:16, 55:5, 55:6, 56:18, 57:2, 57:4, 58:4, 60:1, 60:3, 60:14, 63:4, 63:9, 63:12, 63:16, 63:18, 64:1, 64:7, 64:12, 64:13, 64:19, 65:4, 66:17, 67:13, 67:21, 68:4, 69:8, 69:14, 70:4, 70:7, 70:11, 70:17, 70:22, 72:3, 72:8, 72:16, 72:22
jones's
49:19, 50:6, 50:9

K

kane
75:5
keep
15:16
key
15:4
kind
13:13, 14:18, 16:11, 22:19, 24:10, 24:16, 25:15, 25:16, 48:13, 48:14, 52:8, 53:18
know
11:4, 14:1, 16:9, 16:16, 22:6, 23:3, 24:13, 26:21, 27:4, 28:1, 28:2, 28:7, 28:10, 28:13, 29:20, 30:6,

30:17, 30:18, 30:19, 30:21, 38:15, 40:17, 43:3, 47:17, 50:1, 51:19, 52:5, 52:9, 59:16, 69:9, 69:12
knowing 22:17
knowledge 23:11

L

labeled 44:14, 44:17, 45:3, 46:4, 46:9, 46:14, 47:1, 47:5, 47:7, 47:16, 51:2, 51:4, 56:17, 67:9
language 7:17, 33:4, 42:1, 42:6, 45:9, 62:15, 62:16, 68:14, 68:18
laptop 27:22, 28:1
large 42:22, 44:13, 44:16
last 10:6, 18:16, 26:22
later 69:9
lays 68:3
least 19:3, 19:6, 20:10, 27:12, 49:6, 54:1, 64:2, 64:15
left 7:16, 35:14, 50:21
let's 6:14, 15:12, 17:6, 27:20, 27:22, 31:5, 41:12
level 12:4, 12:21, 13:6, 13:10, 14:3, 14:9, 14:15, 15:11, 17:15, 20:9, 48:8, 48:9, 57:21, 58:18, 60:19, 70:7, 70:8
levels 14:21, 16:11, 16:17
life 19:18, 27:21
likely 14:5, 31:1
limitation 30:2, 30:4, 32:20, 36:20, 36:21, 37:6, 37:18, 65:21
line 35:18, 35:19, 41:13, 48:7, 51:17, 52:12, 53:10, 56:2, 72:9
lines 53:10
list 52:3
listed 10:7, 39:7, 68:6
listener 13:18
listing 7:15, 62:22
literally 52:1
litigations 16:5
little 26:20, 26:22, 27:13, 53:19, 67:3, 69:9
llp 3:4
lock 13:22
locking 12:10
long 21:1, 25:19
look 6:14, 15:14, 21:22, 24:21, 26:4, 29:2, 38:21, 41:17, 51:17, 52:12, 57:8, 63:3, 66:7
looked 36:5, 38:17, 40:4
looking 12:17, 14:10, 14:20, 17:22, 33:13, 34:13, 34:15, 43:20, 43:22, 44:7, 47:11, 50:11, 52:4, 72:21
lot 8:17, 12:3, 15:2, 28:11
lower 15:11

M

make 9:12, 11:22, 19:17, 20:17, 23:7, 39:21, 40:6, 40:12, 48:13, 50:9, 56:13
makes 55:1, 56:19
making 12:11, 36:12, 55:16
manufacturer 20:21
many 20:2, 20:13
mapping 48:14
maps 26:5
march 8:10
marked 6:16, 28:18, 39:17
market 3:5, 21:1
matt 73:5, 74:4
matter 7:8, 7:13
matthew 3:3, 3:9
maybe 23:13, 31:15
mclean 3:16
mean 7:7, 12:18, 16:21, 26:15, 27:3, 28:9, 32:13, 41:8, 47:13, 49:17, 51:13, 51:17, 53:1, 53:2, 58:3, 58:4, 60:22, 62:18
meaning 62:16
means 59:13, 59:16, 68:16
meant 9:7, 19:17
mechanism 52:10
medical 20:21, 20:22
mentioned 25:12, 25:13

menu
24:10
merit
2:6
messages
13:21, 13:22, 14:1
messaging
6:12
metadata
53:20, 57:20, 60:19, 72:14
methodologies
21:21, 23:19
methodology
25:22
microsoft
11:14
middleton
3:3, 4:3, 5:9, 6:19, 29:1, 32:12, 34:5, 38:10, 38:20, 39:11, 39:15, 40:14, 42:20, 43:10, 43:19, 45:6, 46:2, 46:12, 48:4, 50:3, 50:8, 51:15, 62:8, 63:11, 66:4, 66:8, 66:20, 67:15, 67:22, 69:16, 69:19, 73:3, 73:13, 74:5
middleton@dlapiper
3:9
might
23:18, 28:11, 43:22, 44:9
mind
31:18
minute
72:20
mitigation
34:9
mitigations
22:13, 23:16
modeled
15:18, 48:12, 57:14, 58:9, 59:8, 61:5, 61:6, 73:18
modeling
8:19, 8:21, 11:9, 11:12, 11:15, 11:17, 11:19, 13:3, 13:6, 14:4, 16:18, 16:20, 19:19, 25:10, 25:17, 25:19, 26:10, 26:13
modelling
26:6, 26:18, 26:21
models
9:10, 9:16, 9:22, 12:17, 12:18, 13:11, 13:13, 13:17, 15:4, 15:22, 17:15, 19:22, 20:2, 20:9, 21:21
modified
60:21, 61:1, 61:3
modify
57:18, 60:11, 60:16
module
43:5, 43:12, 45:4, 45:16, 45:22, 46:4, 46:10, 46:13, 46:15, 46:17, 46:19, 47:18, 49:11
modules
48:2, 48:20
moment
6:21, 44:2
more
10:5, 13:7, 13:21, 18:7, 18:8, 18:12, 18:14, 18:18, 19:1, 20:8, 20:17, 24:18, 25:15, 29:7, 29:12, 29:14, 29:22, 30:9, 30:13, 32:22, 33:6, 33:7, 37:2, 37:4, 37:9, 42:16, 45:12, 47:19, 48:20, 51:13, 56:8, 57:9, 57:10, 57:13, 58:8, 63:5, 63:13, 63:19, 64:4, 64:8, 64:16, 64:20, 64:21, 65:1, 65:8, 65:14, 65:16, 66:2, 68:11, 69:9, 70:12
morning
5:10, 5:11
most
12:13, 14:7, 15:6, 30:22
move
57:6
moving
8:3, 53:12, 54:7
much
16:3, 31:3
multiple
39:8
must
33:11, 36:19, 37:11, 37:17, 68:10, 68:12, 69:1, 70:2, 70:15
myself
15:3, 22:6, 44:1, 44:10

N

n+1
57:21, 60:6, 60:19, 70:8, 71:3
n-i-s-t
23:21
name
11:1
named
23:19
narrow
13:7
necessary
12:7, 13:7, 20:19
need
13:4, 14:14, 21:13, 23:14, 24:12, 28:9
needing
12:14
neither
75:12
nested
43:13, 43:17, 43:18, 44:4, 57:15, 57:19, 58:9, 58:13, 60:12, 60:18, 72:12
network
13:10, 13:16, 13:18, 13:20, 13:22, 21:4, 21:5, 22:11, 22:12
networks
13:12
never
21:4
new
53:7, 53:11
next
47:3, 53:12, 54:7, 57:6
nielson
1:13, 2:4, 4:2,

4:9, 4:13, 5:5, 5:10, 6:16, 28:18, 39:17, 40:21, 66:12, 74:6
nist 23:20, 23:22, 24:1, 24:3, 40:7
node 54:11, 55:7, 55:22, 56:16
nodes 54:19, 56:22, 57:3, 72:13, 73:17
north 3:5
notarial 75:16
notary 2:8, 75:1, 75:4, 75:22
notes 6:6, 66:7
nothing 8:2
notice 2:5
noticed 7:14
november 75:18
number 23:22, 24:17, 48:10
numbered 45:5

O

oath 5:13
object 17:20, 32:8, 33:21, 38:3, 38:13, 42:12, 43:7, 43:14, 44:19, 45:18, 46:11, 47:21, 49:21, 50:7, 51:11, 55:18, 62:4, 62:11, 63:6, 66:20, 67:15, 67:22, 69:16, 73:3, 73:13
objecting 44:22
objection 67:2
obviously 10:7, 17:8
occur 70:4
officer 75:5
oh 48:6, 69:18
okay 31:5, 40:15, 66:16, 67:12, 67:19, 71:16
once 12:16, 42:14, 54:20, 60:9
one 6:21, 7:14, 8:16, 12:21, 13:17, 15:5, 16:4, 18:7, 18:8, 18:10, 18:12, 18:14, 18:17, 22:22, 24:15, 24:18, 25:6, 29:7, 29:12, 29:14, 29:19, 29:21, 29:22, 30:2, 30:9, 30:13, 30:22, 31:1, 32:14, 32:15, 32:22, 33:6, 33:7, 34:10, 34:20, 35:12, 37:1, 37:2, 37:4, 37:9, 42:16, 44:1, 45:12, 47:14, 47:19, 48:19, 52:6, 53:8, 56:8, 57:9, 57:13, 58:7, 59:20, 63:4, 63:13, 63:19, 64:2, 64:3, 64:8, 64:15, 64:19, 64:21, 65:1, 65:6, 65:8, 65:12, 65:14, 65:15, 66:2, 67:5, 70:12
ones 10:6, 23:14, 57:5
only 47:15, 72:7
open 5:22, 6:1, 6:9, 6:20
opinion 33:3, 69:14
opinions 7:13
opportunities 10:4
order 10:1, 12:7, 24:12
organization 9:13, 12:13, 24:8
organization's 12:5
other 7:22, 16:13, 23:2, 30:10, 31:17, 34:11, 40:9, 42:22, 45:3, 52:8, 59:22, 65:20, 69:11, 69:15, 69:21, 73:17
otherwise 51:7, 75:14
out 15:16, 16:17, 17:2, 20:14, 21:17, 24:6, 35:11, 68:3
outcome 75:14
outcomes 23:10
over 71:8
overall 17:17, 21:16
overlooked 15:6
oversight 7:14
own 11:21, 69:1, 71:18
owner 1:7, 3:11

P

page 4:2, 4:9, 66:13
pages 1:19
paper 17:2
paragraph 32:17, 32:19, 51:21, 53:12, 54:7, 57:7, 59:21, 61:8, 61:10, 61:17, 66:14, 66:18, 66:19, 67:5, 67:8, 68:4, 68:6, 68:7, 69:22, 70:13, 72:6, 72:8
paragraphs 67:6
part 9:8, 21:15, 22:5, 22:16, 22:22, 23:2,

23:6, 25:17, 28:12, 38:5, 38:19, 40:9, 55:21, 58:6, 61:22, 68:17, 70:21, 71:11
partially 19:6
particular 17:15, 54:10, 56:2
parties 75:13
parts 17:16, 21:9, 27:12, 68:3
pass 74:4
passage's 56:15
passive 13:18
patent 1:1, 1:7, 1:10, 3:11, 4:11, 4:12, 6:1, 6:3, 6:4, 7:5, 7:8, 17:18, 29:3, 32:20, 33:14, 33:20, 34:13, 35:7, 36:13, 42:2, 42:6, 42:10, 45:9, 49:2
pc 3:13
pdf 6:2
people 16:6, 26:15
perform 29:11
perhaps 13:22
person 15:3, 16:4
perspective 25:16, 34:3, 49:2
petition 67:8
petitioner 1:4, 3:2
petitioner's 70:16
ph 1:13, 2:4, 4:2, 5:5
phrase 61:15
physical 5:19, 5:21
picture 25:17
piece 17:2, 69:11, 69:21
pieces 12:8, 16:15, 40:8, 69:7, 73:17
piper 3:4
place 23:17, 51:6, 56:19, 57:4
placed 50:15, 50:16
please 5:3, 8:18, 29:2, 69:15
plurality 18:1, 33:16, 63:13, 63:19
point 14:7, 24:7
popup 36:1, 36:8, 38:1, 38:5, 38:8, 38:11
popups 38:16
portion 24:14, 68:8
portions 65:20
posita 34:4
possible 38:16, 47:14, 47:15
potential 9:20, 10:3, 23:17, 28:3, 30:14, 34:9, 42:15, 42:17, 45:11, 56:8
potentially 21:11, 31:1
predefine 70:20
predefined 18:22, 60:7, 61:19, 68:10, 70:1, 70:15, 70:18, 71:5
preliminary 5:12
preparation 7:10, 41:4
present 33:4, 58:21, 70:6, 70:9
pretty 52:3
prevention 34:21
previous 25:12, 40:1, 54:17, 55:10
previously 61:6
principles 25:20
prior 68:17, 71:17, 73:11
priorities 23:14
prioritize 23:3, 24:20
problem 25:14, 25:21, 66:8
process 12:4, 12:12, 12:17, 16:18, 18:11, 28:11, 37:1, 38:6, 38:9, 65:7, 65:13, 71:7, 71:10, 71:17, 73:10, 73:12, 73:15
processes 41:14
produce 54:13
produced 48:9
produces 55:8
producing 57:21, 60:19
product 17:9
professional 2:8, 15:7, 22:6
program 31:17, 31:18, 31:20
programmer 31:16
project 9:21, 20:10, 20:11
proper 25:20
protect 12:14, 14:8
protected 15:20
provide 8:15, 8:17, 53:14, 57:10, 57:16, 59:15, 60:15, 61:15, 73:8
provided 21:16, 34:1, 65:10
provides 59:10, 60:9,

64:19
providing
9:22, 18:5, 20:18, 63:4
public
2:8, 75:1, 75:4, 75:22
publication
24:3
pull
59:19
pursuant
2:5
put
13:21, 23:17
putting
62:20

Q

question
12:13, 15:8, 17:3, 30:18, 38:17, 55:2, 55:3, 55:4
questioning
44:10
questions
5:12, 13:4, 40:2, 44:7, 66:5, 74:3, 74:5
quick
50:22
quite
8:20

R

raise
5:2
range
14:19
rather
50:15
re-ask
44:12
read
30:6, 36:3, 36:20, 38:2, 51:16, 51:18, 52:18, 53:2, 54:15, 55:20, 56:7, 58:1, 58:5, 58:6, 70:22, 71:15
reading
29:19, 29:21, 30:2, 30:3, 30:15, 30:16, 68:7, 75:11
reads
30:20, 36:21, 53:13, 57:7
real
9:13, 67:11
really
21:1, 59:15, 69:12
realtime
2:7
reason
5:15
recall
20:2, 26:8, 66:16, 72:3
receive
33:6
received
29:18, 31:8, 31:10, 32:1, 32:5, 33:11
receives
32:10
receiving
18:17, 29:7, 29:14, 29:22, 30:9, 30:13, 32:22
recent
10:5
recently
9:1, 9:19
recess
39:14, 66:9
recognition
11:3
record
75:8
rectangle
42:22, 43:1, 44:13, 44:16
rectangles
45:3
redefine
18:19, 61:11, 62:3, 62:10, 62:14, 62:16, 62:17, 62:18, 62:20
redefines
19:5, 68:20
redefinition
19:8
reduce
23:17, 24:11, 62:6
reduced
75:10
reference
41:1, 41:3
references
41:8
referring
6:3, 35:21
refine
16:16
regarding
7:8
registered
2:6, 2:7
regulation
21:2
related
14:16, 16:5, 56:13, 58:12, 58:14, 58:16, 63:15, 65:2, 65:18, 65:20, 75:12
relational
18:10, 18:15, 35:2, 35:9, 36:15, 36:16, 36:22, 37:5, 37:7, 37:14, 37:18, 38:5, 38:8, 38:18, 38:19, 39:9, 65:6, 65:12
relevant
10:8, 22:21, 22:22, 24:14, 42:15, 45:11, 56:8
relies
7:19
relying
22:18
remember
24:17, 26:2, 26:3, 26:9
remotely
5:19
report
6:1, 8:1, 9:9, 9:17, 17:1, 29:20, 30:19, 32:16, 32:17, 36:2, 36:10, 36:16, 38:8, 63:22, 64:6, 64:18, 65:3, 65:22, 68:2, 71:14
reported
1:20
reporter
2:6, 2:7, 2:8, 5:2, 75:1, 75:3
reports
11:21, 17:8
represent
7:12, 27:3, 27:9, 28:5
representation
27:18, 37:14, 38:12
representations
18:12, 18:13, 35:3, 37:2, 37:3, 37:7, 37:8, 37:15, 37:19, 37:20, 37:22, 65:8,

65:14, 65:15, 66:2
represented 9:13, 35:7, 35:13, 42:22
representing 27:7, 54:12, 54:19, 55:7, 55:22, 56:22, 57:3, 72:14
reproduce 67:5
requested 9:5, 75:11
requirement 18:16
requirements 21:10, 63:10, 68:5, 68:6
requires 17:22, 20:6, 33:5, 35:2, 36:14, 37:6, 62:20, 68:8, 68:14, 69:4, 69:22, 70:13
research 8:12
respect 73:8
response 18:17, 29:6, 29:12, 29:14, 29:17, 29:21, 30:9, 30:12, 32:1, 32:22, 33:7
rest 72:16
review 7:2, 8:15, 41:3
reviewed 7:9
right 5:2, 8:4, 15:7, 15:15, 16:2, 16:4, 16:7, 19:22, 22:1, 27:2, 27:4, 27:10, 27:22, 28:8, 29:4, 29:13, 31:12, 31:16, 31:19, 35:15, 36:10, 38:2, 38:22, 40:17, 40:19, 41:7, 41:22, 42:4, 42:8, 42:11, 43:1, 43:6, 43:13, 43:21, 44:14, 44:18, 45:8, 45:17, 46:6, 46:15, 47:9, 52:7, 52:18, 53:8, 54:14, 55:13, 55:17, 56:17, 57:6, 57:22, 58:22, 59:16, 60:13, 61:14, 62:3, 63:14, 64:9, 64:16, 67:9
rimon 3:13
risk 10:1, 24:18, 24:19, 40:9
risks 10:4, 13:15, 23:18, 24:20, 24:22
rmr 1:21, 75:3
rogue 15:19, 16:5
ross 25:5
rotated 34:15
rpr 1:21, 75:4

S

said 17:7, 39:2, 39:22, 40:8, 43:20, 45:20, 51:22, 52:1, 75:9
same 7:17, 7:20, 46:20, 72:5
satisfy 33:5, 33:10, 68:4
saw 8:2, 36:11
say 6:3, 11:3, 12:18, 15:12, 21:17, 25:4, 27:12, 27:13, 27:16, 27:20, 27:22, 28:9, 28:13, 46:16, 47:10, 48:6, 48:15, 50:16, 53:3, 56:16, 56:18, 58:20, 68:4, 69:7, 71:14
saying 15:2, 29:18, 31:13, 36:18, 37:10, 37:13, 38:16, 52:5, 52:20, 58:11, 71:11
says 29:5, 33:16, 35:16, 35:21, 36:6, 36:10, 37:13, 41:12, 41:19, 46:7, 48:7, 50:12, 50:14, 50:16, 50:22, 51:22, 52:1, 52:2, 52:9, 52:14, 53:1, 53:19, 54:8, 55:21, 57:5, 58:18, 60:14, 61:17, 72:22
scenario 22:22
schema 53:20
scratch 19:13, 46:21, 59:14, 63:17
screen 34:16
seal 75:16
second 18:20, 31:5, 59:20, 61:13, 61:20, 68:21, 69:1
secondary 54:11, 54:19, 55:7, 55:22, 56:16, 56:22, 57:3, 72:13
section 11:3, 65:17, 66:13
sections 65:19
security 8:11, 9:3, 12:9, 20:5, 20:10, 20:11, 20:12, 20:22, 21:19, 22:5, 22:11, 24:6, 24:16, 25:6, 25:21, 54:4
see 20:4, 24:7, 26:4, 29:5, 33:16, 35:10, 35:14, 36:4, 41:12, 41:19, 46:3, 46:22, 47:2, 50:21, 51:3
seems 9:17, 52:3
select 36:7, 51:7,

52:5
selected
35:22
selector
35:22
selects
36:8
sending
59:16
sense
19:7
sent
9:4, 9:6
sentence
53:13, 54:8
server
41:20, 42:17, 42:21, 43:4, 43:5, 43:12, 43:13, 44:14, 44:17, 45:4, 45:8, 45:14, 46:19, 46:20, 46:22, 47:4, 47:6, 47:7, 47:8, 47:16, 47:17, 47:18, 48:2, 48:16, 48:20, 49:6, 49:9, 49:12, 49:13, 49:18, 50:5
service
8:14
services
8:16
serving
22:19
set
9:19, 13:3, 13:4, 20:15, 24:4, 24:19, 31:22, 75:15
seth
1:13, 2:3, 4:2, 5:5
shape
46:7, 50:19
shapes
48:10, 50:15, 50:22, 51:7, 51:9
share
69:15
shops
28:1
shorthand
2:6, 75:3
shostack
10:21
should
38:7, 69:11
shows
35:8, 44:13
sic
73:4
side
50:21
signature-p1kal
75:19
significant
17:13
signing
75:11
similar
7:20, 36:1, 44:10
simply
38:16, 62:7, 62:19
since
5:18, 10:6, 20:12, 21:18, 67:3
single
15:22, 16:2
sit
26:9
sitting
8:1, 24:5
skip
70:21
small
7:14
smaller
20:15
software
1:6, 53:22
solutions
24:21
solve
20:22
some
5:22, 9:16, 9:20, 10:5, 14:1, 14:14, 14:18, 15:4, 16:12, 16:13, 17:14, 20:9, 20:14, 22:16, 22:18, 34:11, 34:17, 40:3, 52:8, 52:10, 53:20, 54:1, 54:2, 57:7
somebody
15:6, 15:16, 22:18, 25:2
someone
15:19
something
30:5, 31:18, 31:19, 39:22, 52:10
sometimes
20:16
sorry
7:2, 24:2, 34:14, 43:22, 44:21, 48:3, 55:2, 59:14, 63:17, 69:8, 69:18, 70:12, 71:7
sort
13:15
sound
40:6
sounds
11:1, 50:19
source
8:15, 42:15, 42:17, 45:11, 56:8
sp
24:2, 24:15
special
24:2, 24:3
specific
23:19
specifically
21:9, 21:10, 43:16, 50:1, 50:11, 52:9, 62:10
specified
20:7
speed
19:18
stands
26:8, 34:20
start
13:5, 14:10, 15:5, 15:10, 15:21, 16:17, 17:6, 25:14, 28:6, 71:8
start-up
10:2
started
21:19
starting
12:11, 14:6, 24:7, 41:13, 48:7, 59:22, 72:8
starts
72:22
state
2:9, 48:3, 75:5
statement
55:3
staying
35:14
stencil
52:4
step
33:10, 54:17, 55:10, 55:15
stephen
10:15
steven
11:5

still
10:8, 15:20, 22:14
stored
18:3, 18:4, 63:14, 63:20, 64:9
stores
41:15
street
3:5
stride
25:22, 26:2, 26:8
strike
71:7
structured
29:10, 53:14, 53:21, 54:3
student
25:7
subcomponents
70:5, 70:8, 70:9, 71:9, 71:11, 71:16, 73:9
subject
54:6
sudden
21:3
suggesting
48:16
suite
3:6, 3:15
supposed
15:17, 62:18
sure
6:22, 11:2, 11:4, 21:18, 21:19, 28:4, 36:12, 38:15, 39:13, 40:6, 40:12, 43:17, 44:5, 44:11, 55:4, 67:2
sworn
5:4, 5:7
system
12:6, 14:6, 14:11, 17:15, 18:11, 23:4, 24:9, 31:11, 31:15, 31:22, 32:2, 32:4, 32:6, 32:10, 33:6, 34:21, 37:1, 38:6, 38:9, 41:7, 41:8, 41:11, 41:13, 48:12, 49:20, 50:2, 50:9, 52:16, 52:17, 52:21, 53:4, 53:5, 54:11, 54:14, 55:12, 56:21, 56:22, 57:2, 57:9, 57:14, 58:8, 58:22, 59:3, 59:7, 65:6, 65:12, 70:5, 70:7, 70:11, 71:12
systems
14:10, 70:19

T

tab
35:15, 36:5, 36:7, 36:8
take
6:14, 17:13, 32:15, 39:11, 66:6, 66:7
taken
26:5, 75:6, 75:9
taking
5:18, 62:19, 63:3
talk
19:11, 24:19, 59:18, 69:21
talked
10:6, 26:20, 26:21
talking
12:22, 13:9, 15:13, 15:22, 16:1, 22:1, 36:12, 36:13, 40:7, 40:11, 50:5, 72:16, 73:16
teach
8:21
techniques
24:11
tell
56:2
template
20:8
templates
13:13
ten-minute
39:12, 66:7
tends
14:16
term
27:4, 29:5, 56:15, 61:11, 62:9
terms
8:21, 20:13, 23:3, 23:11, 23:14
testified
5:7, 73:4
testimony
5:16, 19:20, 73:22, 75:8, 75:9
th
75:16
thank
7:1, 74:6
thanks
73:5
theoretical
15:4
thereafter
75:9
thereby
18:19, 19:5, 54:13, 57:20, 60:19, 62:17, 68:20
therein
18:4, 63:14, 63:20, 64:9
theresa
1:20, 2:5, 75:2, 75:21
thing
31:20
things
12:10, 12:11, 14:18, 15:18, 28:11, 72:17
think
7:18, 11:2, 11:7, 12:22, 24:4, 24:15, 29:19, 30:6, 30:14, 30:16, 30:22, 31:1, 39:11, 56:19, 58:4, 59:17, 62:6, 72:7, 73:4
thinking
31:15
thorough
57:10
thoughts
40:3
threatmodeler
1:6, 10:12, 11:11, 17:12
threats
9:13, 13:2, 13:15, 14:21, 15:5, 15:14, 18:2, 21:6, 21:12, 22:3, 22:7, 22:17, 22:20, 23:5, 23:12, 24:11, 25:11, 42:16, 42:17, 45:12, 45:13, 45:21, 46:8, 47:3, 47:8, 47:19, 48:11, 49:3, 50:14, 50:18,

51:14, 52:3, 52:6, 54:20, 54:22, 55:16, 56:4, 56:8, 56:12, 57:1, 57:11, 63:20, 64:15, 72:11, 72:14
three 47:1, 47:3, 47:5
through 7:16, 8:2, 9:8, 9:16, 21:7, 24:7, 27:5, 64:3, 64:15, 72:7
throughout 72:16
tickling 11:2
time 21:1
times 12:3
today 5:13, 5:16, 5:20, 7:10, 8:1, 25:8, 40:8, 67:12, 70:22, 72:6, 73:22
together 49:16
tool 11:9, 11:12, 11:15
toolbox 35:15
tools 11:17, 17:5, 17:10, 17:11, 17:19, 19:12, 19:14, 19:17
top 26:3, 35:14
tradeoffs 12:10
trained 15:3, 15:4, 15:7
training 22:10
transcript 4:7, 40:4, 75:7
trees 25:13
trial 1:1
triggered 40:3
true 75:7
try 24:5, 67:3
trying 12:4, 12:12, 12:14, 13:14, 14:7, 15:16
turn 62:22
turned 6:13
turning 34:14
two 16:6, 19:1, 42:22, 43:3, 44:17, 45:3, 68:11
type 14:2, 34:10, 38:11
types 12:19, 13:17, 14:5, 21:21, 22:7, 22:8, 22:9, 34:11
typewriting 75:10

U

under 5:13, 22:8, 31:9, 34:17, 42:7, 42:10, 75:10
underlying 70:19
understand 5:13, 9:10, 10:2, 12:5, 12:7, 12:12, 13:15, 14:4, 16:11, 17:3, 19:20, 26:7, 36:12, 54:16, 58:2, 58:14, 59:17, 60:21, 73:5
understanding 9:9, 12:16, 21:6, 23:2, 23:5, 34:6, 41:10, 47:11, 48:19, 51:20, 53:17, 55:5, 62:9
understood 17:14
unless 60:1
until 25:8, 72:1
use 13:12, 13:14, 16:21, 17:7, 21:21, 24:1, 25:5, 25:8, 25:18, 27:9, 27:11, 27:15, 27:17, 28:1, 40:8, 56:15
user 18:7, 18:18, 19:3, 29:7, 29:12, 29:14, 29:18, 29:22, 30:10, 30:13, 31:7, 31:10, 32:5, 32:22, 33:6, 33:10, 36:7, 50:10, 50:13, 50:19, 52:5, 52:10, 64:21
uses 37:18
using 17:9, 18:11, 27:2, 27:4, 27:21, 29:17, 35:2, 37:2, 37:7, 37:14, 58:15, 65:7, 65:13
usually 11:20

V

valuable 12:7
various 24:9, 46:8, 48:11
via 1:14, 2:4
videotaped 2:3
viewing 34:3
virginia 3:16
virtually 1:14, 2:4
vista 8:7, 8:11
visual 18:12, 18:13, 35:2, 37:2, 37:3, 37:7, 37:8, 37:14, 37:15, 37:19, 37:20, 37:22, 38:12, 65:7, 65:13, 65:15, 66:1
visualized 39:9
visually 35:6, 35:12, 43:2, 49:15
vorkapic 1:20, 2:5, 75:2, 75:21
vries 10:15

vulnerability
14:16

W

want
11:3, 27:16, 27:20, 32:15, 44:11, 51:16, 51:18, 69:10
wanted
9:14, 28:5, 39:21, 40:5, 40:12
way
15:18, 21:11, 23:9, 25:7, 25:14, 27:17, 29:10, 29:19, 29:21, 30:7, 30:14, 30:20, 34:20, 35:12, 49:15, 60:14
ways
22:18, 25:10, 27:6, 72:17
we're
5:18, 13:8, 13:9, 13:10, 15:3, 15:8, 15:12, 15:13, 16:2, 36:11, 36:13, 43:20
web
43:5, 43:12, 45:4, 46:20, 46:22, 47:4, 47:6, 47:8, 47:18, 49:12, 50:5
went
8:2, 9:8, 40:4
whatever
21:2, 26:16
wherein
18:21, 19:4
whereof
75:15
whether
9:12, 9:14, 20:6, 20:7, 63:8, 64:11, 66:17, 67:13, 73:9
whiteboard
27:2, 27:8, 27:9, 27:11, 27:15, 27:17, 28:6
whiteboarding
28:12
whole
13:2, 13:3, 14:9, 14:15, 15:11
wilmington
3:7
wisdom
23:13
within
25:18, 41:9, 43:13, 48:2, 48:15, 48:20, 49:6, 49:17, 62:14
without
9:6
witness
5:4, 5:6, 17:21, 28:21, 32:9, 33:22, 38:4, 38:14, 39:13, 39:20, 42:13, 43:8, 43:15, 44:20, 45:2, 45:19, 47:22, 49:22, 51:12, 55:19, 62:5, 62:12, 63:7, 66:21, 67:16, 68:1, 69:17, 69:20, 73:14, 74:4, 75:15
word
22:21, 28:7, 30:10, 35:15, 58:15, 62:2, 62:3, 62:14, 62:17
words
30:10, 31:17
work
8:22, 14:20, 16:8, 16:10, 17:9, 25:14, 27:21, 28:1
worked
9:16, 20:9
working
9:1, 15:21, 20:8, 23:16
works
21:2
workspace
50:15
worried
15:13
wouldn't
17:1, 36:16
writing
16:22, 31:19
written
20:14
wrote
17:2

Y

yeah
51:16

Z

zoom
1:14, 2:4

.

.7703
3:17

0

008
6:4, 7:4, 7:7, 7:8, 17:18, 29:2, 32:20, 33:13, 33:20, 35:7, 42:1, 42:10, 45:9, 49:2
00821
1:9
04
6:18, 28:20, 39:19
084
75:3

1

1-f
7:18, 67:9, 67:14, 67:20, 69:13, 69:22, 70:13
10
35:8, 35:9, 35:14, 35:21, 36:6, 38:21, 38:22, 48:7
10,699,008
1:10, 4:11
1001
4:11, 28:16, 28:19, 34:14
1004
4:12, 39:15, 39:18, 40:18, 40:20
101
69:22
102
59:21, 70:13
106
52:14, 57:17, 60:16
108
54:8, 72:10
11
7:18, 7:21, 74:7
110
57:12, 58:7, 70:7
12
34:15, 34:17, 36:2, 36:11,

38:18
1200
36:2
1201
3:5
14
72:22
171
24:2, 24:3
18
51:17
19
48:7
19801
3:7
1st
8:10

2

20
7:16, 7:17, 7:21, 35:18, 35:19
2003
4:13, 6:15, 6:17, 61:7
2004
25:8
2005
20:12, 21:19
2015
20:20
2016
8:10
2023
1:9
2024
1:15, 6:18, 28:20, 39:19, 75:17
2027
75:18
2100
3:6
22102
3:16
23
72:9
2589
75:3
26
1:15, 6:18, 28:20, 39:19
28
4:11
29
74:7

3

30
75:16
302
3:8
39
4:12, 66:13

4

4
41:13
400
73:1
45
52:12
468
3:8
47
51:17, 51:18

5

500
3:15
533699
1:18
5675
3:8
571.765
3:17
59
1:16, 35:18, 35:19

6

66
4:4

7

704
51:2, 51:5, 52:4
75
1:19

8

8
1:16
800
24:2, 24:3
800171
40:8
804
44:14
806
45:5
81
61:9, 61:10, 61:17
8300
3:14
853
24:15

9

9,602,529
4:12
902
48:9
904
46:4, 46:7, 46:9, 46:14, 47:1, 47:5, 48:1, 48:11, 49:5, 56:17, 57:5
92
32:17, 32:19
96
66:14, 66:19, 67:5
97
68:6, 68:7
98
68:4