

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY

SKYSONG INNOVATIONS, LLC v. CROWDSTRIKE, INC. AND CROWDSTRIKE HOLDINGS, INC.,
U.S. District Court for the Western District of Texas
C.A. No. 7:25-cv-00040

Plaintiff’s Preliminary Infringement Contentions
U.S. PATENT NO. 10,313,385
CrowdStrike Falcon Platform

EXHIBIT 1

I. INTRODUCTION

The chart below demonstrates how Defendants CrowdStrike, Inc. and CrowdStrike Holdings, Inc. (collectively “CrowdStrike” or “Defendants”) as well as Defendants’ partners, customers, and end users of the products and features discussed below, directly infringe, either literally or under the Doctrine of Equivalents, at least claims 1-17 of U.S. Patent No. 10,313,385 (“385 Patent”). Defendants and Defendants’ partners, customers, and end users directly infringe the identified claims at least by making, using, selling, installing, configuring to operate, importing, testing, and/or offering to sell at least Defendants’ CrowdStrike Falcon Platform, including Falcon Prevent, Falcon Go, Falcon Pro, Falcon Enterprise, Falcon Complete, Falcon Prevent, Falcon Insight XDR, CrowdStrike Endpoint Security, Falcon Identity Protection, Falcon Shield SAAS Security, Falcon Cloud Security, Falcon Next-Gen SIEM, Falcon Intelligence, Falcon Exposure Management, Falcon Data Protection, Falcon for IT (Automation), Falcon Sensor, Threat Graph, Intel Graph, Asset Graph, CrowdStrike Cloud, Falcon Real Time Response, Falcon Sandbox, Falcon Fusion SOAR, Falcon Managed Detection and Response, Falcon Cloud Detection and Response, Falcon Adversary Intelligence, Falcon Intelligence Recon, Falcon Intelligence Recon+, Falcon Adversary OverWatch, CrowdStrike Counter Adversary Operations, and Charlotte AI (collectively, “the Accused Products”), either alone, and/or when installed and operated as designed and intended on a computer system or network, as detailed below.

Each element of each asserted claim is presently alleged to be literally present. Because discovery has not started and the Asserted Claims have not yet been construed, Skysong Innovations, LLC (“Plaintiff” or “Skysong”) reserves the right to supplement its contentions, including with respect to the Doctrine of Equivalents as appropriate. In addition, any of Defendants’ products that perform similar functions and/or incorporate or rely on the same or similar functionality (for example, without limitation, any predecessor or

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY

successor products performing the same functions in the same ways or products which use the same software, plugins, or libraries or call the functions underlying the operations identified below) as the Accused Products also infringe in the manner set out below.

Defendants directly infringe at least claims 1-17 of the '385 Patent, either literally or under the Doctrine of Equivalents, by making, using, offering to sell and selling the systems described below. Defendants’ partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claims 1-17 of the '385 Patent, literally or under the Doctrine of Equivalents, at least by using the Accused Products and corresponding systems and services, as described below. For example, Defendants publicize and market that they work with partners worldwide in connection with using their Accused Products and corresponding systems and services:



The cybersecurity platform for the AI era



Cloud-native architecture by design

Our revolutionary, cloud-native architecture isn't bound by hardware-defined network perimeters.



Single platform, console, and agent

The Falcon platform converges security and IT to protect all key areas of risk. Easily deploy through a single, lightweight agent, then manage your security from a unified console.



Open and extensible ecosystem

Add more platform modules using the same lightweight sensor from the original deployment. Integrate data from any source, try partner applications, and build with low-code tools.

See <https://www.crowdstrike.com/en-us/platform/>

Accelerate your business with a world-class partner

Build, scale, and grow with an industry leader in AI-powered cybersecurity.

Become a partner →

Login to partner portal →

Why partner with CrowdStrike?

Boost your security offerings with unmatched global protection for your customers.



Drive innovation

Deliver faster solutions and solve challenges with streamlined, collaborative selling.



Scale go-to-market

Extend your reach and drive demand with differentiated products, services, and strategies.



Optimize investments

Unlock sales tools, marketing benefits, and security specs to showcase your validated offerings.



Join an elite ecosystem



See <https://www.crowdstrike.com/en-us/partner-program/>

Defendants have actively induced and are actively inducing infringement of at least claims 1-17 of the '385 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that its acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use the Accused Products in a manner that infringes claims 1-17 of the '385 Patent at least by offering and providing the software and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to use the Accused Products in infringing ways. Defendants further encourage and induce their customers to infringe claims 1-17 of the '385 Patent: 1) by widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike Falcon Platform, and services in the United States. (See <https://www.crowdstrike.com/en-us/pricing/>) Further, as the entities that provide installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Products remain operational for each customer through ongoing technical support, on information and belief, Defendants and/or their partners affirmatively aid and abet each customer's use of the Accused Products in a manner that infringes the '385 Patent.

Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, constituting a material part of the inventions claimed,

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY

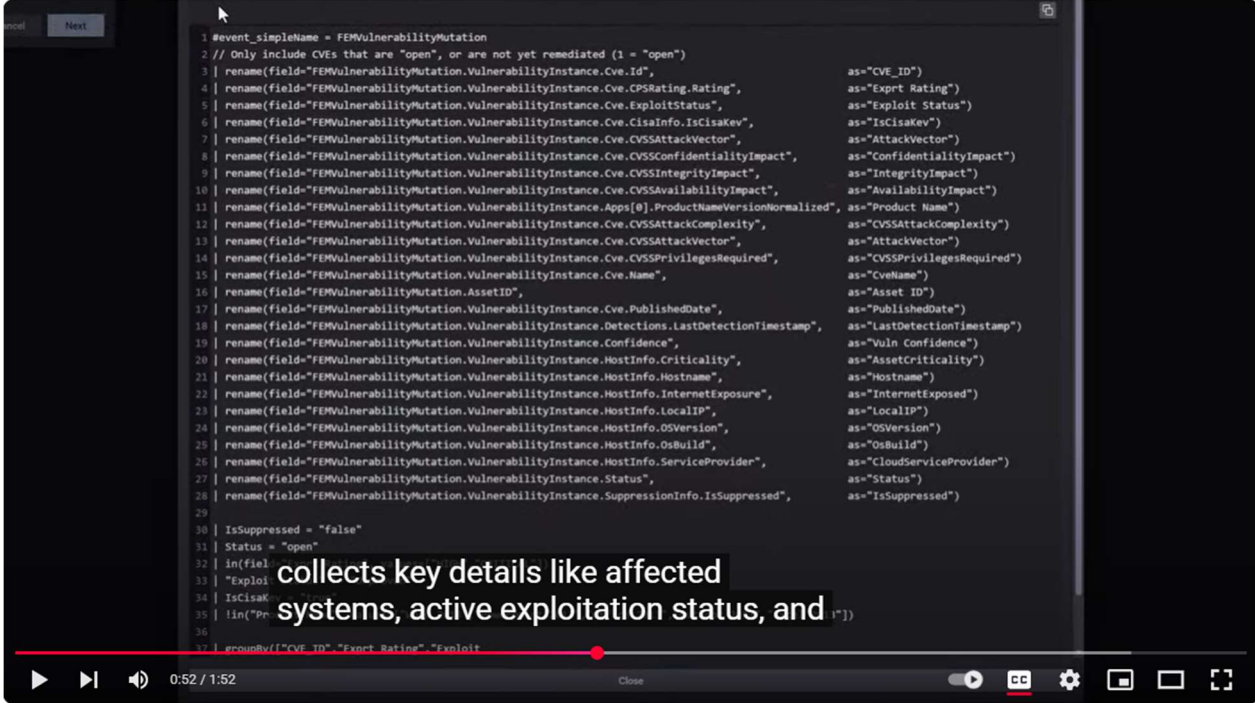
and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown below, the Accused Products have no substantial non-infringing uses because the accused functionality is an integral part of the Accused Products and must be performed for the Accused Products to perform their intended purpose. These functionalities are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without the system and components identified below that practice the '385 Patent, that functionality could not be performed. Additionally, the accused functionality itself has no substantial non-infringing uses because the components, modules and methods identified below are a necessary part of that functionality. For example, without the malware detection and endpoint protection platform and dark net threat intelligence set forth in the claims, the Accused Products could not effectively protect computer systems preemptively from malware attacks and cybersecurity threats that exploit vulnerabilities using threat intelligence collected from the dark net. These functionalities are continually running when the system is in use and cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without the system and components identified below that practice claimed in the '385 Patent, that functionality could not be performed.

Indeed, as shown below, the Accused Products have no substantial non-infringing uses because the accused functionality is an integral part of the Accused Products and must be performed for the Accused Products to perform their intended purpose. For example, at least the functionalities and corresponding modules (whether software and/or hardware) described below have no suitable non-infringing use and form a material part of the Accused Products. In other words, when each of the Accused Products operates, the functions below are performed. Moreover, when the functionality and modules specifically described below are operated, they perform the steps described below. The Accused Products (and the specific modules and functionalities described herein) are designed and intended specifically to perform the inventions claimed in the Asserted Claims, and do not have any other purpose. For example, the Accused Products and accused functionalities constitute a material part of the inventions claimed because such architecture is integral to the system as recited in the claims of the '385 Patent. None of these products are staple goods—they are sophisticated and customized malware detection, endpoint protection, and threat intelligence products, methods, and systems.

Plaintiff provides the following example claim charts based on currently available information, including through public sources. Plaintiff reserves the right to modify, amend, or supplement these claim charts should it become aware of additional information regarding the Accused Products and systems, including through discovery, or should one or more claims be construed in a manner differently than interpreted herein.

Claim Language	CrowdStrike Falcon Platform
[1E] obtaining a set of exploits from the dark net information, the set of exploits configured to penetrate the computer system;	The CrowdStrike Falcon Platform embodies a system that includes “<i>obtaining a set of exploits from the dark net information, the set of exploits configured to penetrate the computer system.</i>” As previously discussed in [1D] (e.g., <i>accessing data through the network connection, the data comprising dark net information associated with exploits of a computer system</i>), <i>supra</i>, the Falcon Platform and Falcon Adversary Intelligence monitors the dark web as part of CrowdStrike’s counter adversary operations. In addition, Falcon Adversary Intelligence and CrowdStrike’s threat hunters implement “dark web monitoring” to “develop a more comprehensive understanding of attackers and their methods” (e.g., <i>obtaining a set of exploits from the dark net information, the set of exploits configured to penetrate the computer system</i>). How Does Dark Web Monitoring Work? Dark web monitoring continuously searches the dark web and pulls in raw intelligence in near real time. Millions of sites are monitored for specific information (e.g., corporate email addresses), or general information (e.g., the company name and industry). When a threat is discovered, users can create a customized alert that notifies team members and anyone else in the organization who is relevant to the threat, such as marketing, legal, human resources or fraud teams. Features of Dark Web Monitoring → Threat intelligence. The data captured by the dark web monitoring solution can be fed into automated threat intelligence systems and used to enrich that data. → Threat hunting. Threat hunters can use dark web monitoring to speed their hunting and develop a more comprehensive understanding of attackers and their methods. → Faster incident response. Investigation and response workflows can be used to mitigate threats as rapidly as possible. → Integration into security platforms. The data collected can be sent to other systems to formulate more accurate insights from the entire security stack. https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web-monitoring/ In an example from the prior Falcon Platform Falcon Intelligence module Falcon Intelligence Recon and Falcon Intelligence Recon+ both “Monitored Criminal Forums” (e.g., <i>obtaining a set of exploits from the dark net information</i>) and implemented “Vulnerability Exploit Intelligence” (e.g., <i>the set of exploits configured to penetrate the computer system</i>).

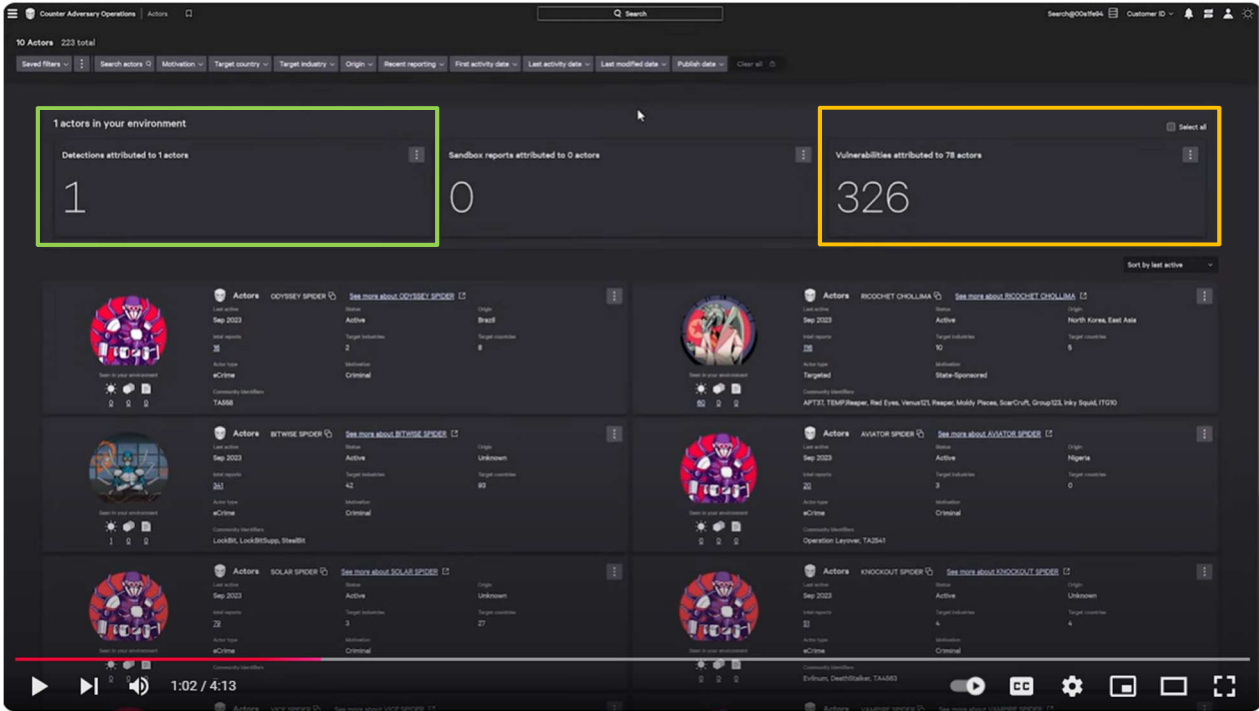
Claim Language	CrowdStrike Falcon Platform																																				
	Falcon Intelligence Recon vs. Falcon Intelligence Recon+ <table><tr><th></th><th>Falcon Intelligence Recon</th><th>Falcon Intelligence Recon +</th></tr><tr><td>Monitoring of Criminal Forums</td><td>✓</td><td>✓</td></tr><tr><td>Detection of Domain Abuse</td><td>✓</td><td>✓</td></tr><tr><td>Vulnerability Exploit Intelligence</td><td>✓</td><td>✓</td></tr><tr><td>Cybercrime Reports</td><td>✓</td><td>✓</td></tr><tr><td>Assigned CrowdStrike Expert</td><td></td><td>✓</td></tr><tr><td>Identification of Monitoring Needs</td><td></td><td>✓</td></tr><tr><td>Managed Detection Rules</td><td></td><td>✓</td></tr><tr><td>Alert Triage and Assessment</td><td></td><td>✓</td></tr><tr><td>Mitigation Recommendations</td><td></td><td>✓</td></tr><tr><td>Monthly Summary Report</td><td></td><td>✓</td></tr><tr><td>Quarterly Threat Briefings</td><td></td><td>✓</td></tr></table> https://www.crowdstrike.com/wp-content/uploads/2023/12/crowdstrike-falcon-intelligence-recon-plus.pdf (emphasis added)		Falcon Intelligence Recon	Falcon Intelligence Recon +	Monitoring of Criminal Forums	✓	✓	Detection of Domain Abuse	✓	✓	Vulnerability Exploit Intelligence	✓	✓	Cybercrime Reports	✓	✓	Assigned CrowdStrike Expert		✓	Identification of Monitoring Needs		✓	Managed Detection Rules		✓	Alert Triage and Assessment		✓	Mitigation Recommendations		✓	Monthly Summary Report		✓	Quarterly Threat Briefings		✓
	Falcon Intelligence Recon	Falcon Intelligence Recon +																																			
Monitoring of Criminal Forums	✓	✓																																			
Detection of Domain Abuse	✓	✓																																			
Vulnerability Exploit Intelligence	✓	✓																																			
Cybercrime Reports	✓	✓																																			
Assigned CrowdStrike Expert		✓																																			
Identification of Monitoring Needs		✓																																			
Managed Detection Rules		✓																																			
Alert Triage and Assessment		✓																																			
Mitigation Recommendations		✓																																			
Monthly Summary Report		✓																																			
Quarterly Threat Briefings		✓																																			
[1F] applying an exploit function which takes the set of exploits as input and returns a set of vulnerabilities;	The CrowdStrike Falcon Platform embodies a system that includes “<i>applying an exploit function which takes the set of exploits as input and returns a set of vulnerabilities.</i>” For example, as part of Falcon Adversary Intelligence, “CrowdStrike tracks over 235 nation-state e-crime and activists.” In the example shown below, 326 “Vulnerabilities” (e.g., <i>returns a set of vulnerabilities</i>) are “attributed to 78 actors” (e.g., <i>applying an exploit function which takes the set of exploits as input</i>). “Community identifiers” such as “LockBit, LockBitSupp, StealBit” (e.g., <i>applying an exploit function which takes the set of exploits as input</i>) for eCrime actor “BITWISE																																				

Claim Language	CrowdStrike Falcon Platform
	 https://www.youtube.com/watch?v=YPSTBgXkKi0&t
[1G] creating a constraint set of the computer system from the set of vulnerabilities, the constraint set comprising a minimum set of dependencies to operate the computer system;	The CrowdStrike Falcon Platform embodies a system that includes “<i>creating a constraint set of the computer system from the set of vulnerabilities, the constraint set comprising a minimum set of dependencies to operate the computer system.</i>” For instance, CrowdStrike Falcon Sandbox “create[s] a controlled and isolated environment” (e.g., <i>the constraint set comprising a minimum set of dependencies to operate the computer system</i>) which “establishes a space where potentially harmful code can be safely executed” (e.g., <i>creating a constraint set of the computer system from the set of vulnerabilities</i>) in which “investigators can ensure the rest of the system remains unaffected, thereby minimizing the risk of a security breach.” For example, “[a]pplication-level sandboxes restrict an application's access to certain system

Claim Language	CrowdStrike Falcon Platform
	resources. These provide enough resources for testing malicious code while still preventing that code from causing wider damage.” CrowdStrike Falcon Sandbox monitors the harmful code’s behavior, the monitoring may include the following activities: “Tracking its interaction with the file system,” “System calls,” and “Network activities.” CrowdStrike Falcon Sandbox employ various analysis methods including: “Dynamic/runtime analysis” which means “observes the code in real time as it executes within the sandbox environment.” This “aids in the detection of malicious activity that only occurs during execution.” Introducing CrowdStrike Falcon Sandbox CrowdStrike Falcon® Sandbox is a module built on the integrated, cloud-native CrowdStrike Falcon® platform. By coupling its analysis results with threat intelligence, Falcon Sandbox delivers actionable indicators of compromise (IOCs) to your security team. Its cutting-edge analysis technology enables the detection of advanced threats, and it can integrate seamlessly via rich APIs. Cybersecurity sandboxing is a powerful tool for identifying and analyzing potential threats in a controlled environment. By isolating suspicious code, security teams can study malware behaviors without triggering a system-wide compromise and gain crucial insights for developing stronger defenses. With tools like CrowdStrike Falcon Sandbox, your organization will be better equipped to navigate the challenges of modern cybersecurity threats. When you’re ready to get started, try CrowdStrike Adversary Intelligence

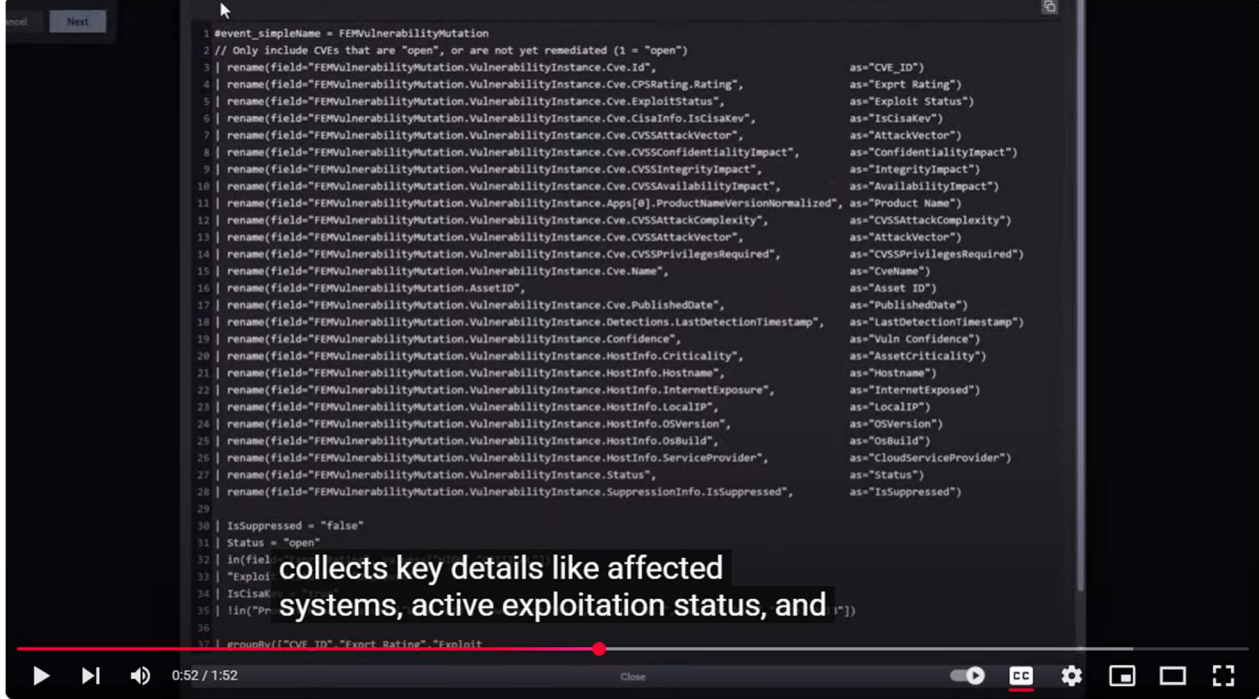
Claim Language	CrowdStrike Falcon Platform
	I Core concepts Although cybersecurity sandboxing may initially seem complex, we can break it down into several simple core concepts. The first of these is sandboxing itself, or the isolation of suspicious code. Isolation of suspicious code Sandboxing involves creating a controlled and isolated environment. Although it’s commonly used in software development, sandboxing in cybersecurity establishes a space where potentially harmful code can be safely executed. By isolating execution, investigators can ensure the rest of the system remains unaffected, thereby minimizing the risk of a security breach. Monitoring and analyzing behavior Once the suspicious code is isolated, cybersecurity researchers can monitor its behavior closely. This monitoring may include the following activities: → Tracking its interaction with the file system → System calls → Network activities

Claim Language	CrowdStrike Falcon Platform
	→ Application-level sandboxes restrict an application's access to certain system resources. These provide enough resources for testing malicious code while still preventing that code from causing wider damage. Each component contributes significantly to the safe execution and thorough analysis of suspicious code. Methods of analysis Cybersecurity professionals employ various analysis methods to investigate suspicious code from various angles: → Static analysis examines suspicious code — without executing it — to look for known malicious patterns. This offers a quick way to find potential threats without running the code. → Dynamic/runtime analysis observes the code in real time as it executes within the sandbox environment. This aids in the detection of malicious activity that only occurs during execution. → Memory dump analysis involves inspecting the memory image from the sandbox to detect malicious code residing in memory. This practice is crucial for identifying threats that reside solely in memory and leave few other traces. https://www.crowdstrike.com/en-au/cybersecurity-101/threat-intelligence/cybersecurity-sandboxing/ As another example, Falcon Adversary Intelligence is demonstrated below having detected 326 “<i>Vulnerabilities</i> attributed to 78 actors” (e.g., <i>creating a constraint set of the computer system from the set of vulnerabilities</i>) based on a customer’s computer “<i>environment</i>” (e.g., <i>the constraint set comprising a minimum set of dependencies to operate the computer system</i>).

Claim Language	CrowdStrike Falcon Platform
	 The screenshot displays the CrowdStrike Falcon Platform interface. At the top, there's a header with 'Counter Adversary Operations' and 'Actors'. Below this, a search bar and various filters are visible. The main content area shows a summary of actors and vulnerabilities. Three specific metrics are highlighted with colored boxes: '1 actors in your environment' (green box), 'Sandbox reports attributed to 0 actors' (grey box), and 'Vulnerabilities attributed to 78 actors' (yellow box). Below these, a grid of actor profiles is shown, each with a circular icon, a name (e.g., ODYSSEY SPIDER, BICOCHET OCHOLIMA), and various attributes like status, target industries, and motivation. At the bottom, there's a video player interface with a play button, volume icon, and a timestamp of 1:02 / 4:13. https://www.youtube.com/watch?v=RrKQN8x2Ldc (emphasis added) In addition, the Falcon Exposure Management dashboard is demonstrated below managing “1.6K” assets with 7 “Internet-exposed <i>assets</i>” (e.g., <i>the constraint set comprising a minimum set of dependencies to operate the computer system</i>) and “<i>Vulnerability</i> IDs” based on “prevalent actors” such as “FANCY BEAR” (20) and “CARBON SPIDER” (10) (e.g., <i>creating a constraint set of the computer system from the set of vulnerabilities</i>).

Claim Language	CrowdStrike Falcon Platform
	Falcon Exposure Management unified main dashboard https://www.crowdstrike.com/wp-content/uploads/2024/09/falcon-exposure-management-data-sheet.pdf (emphasis added)

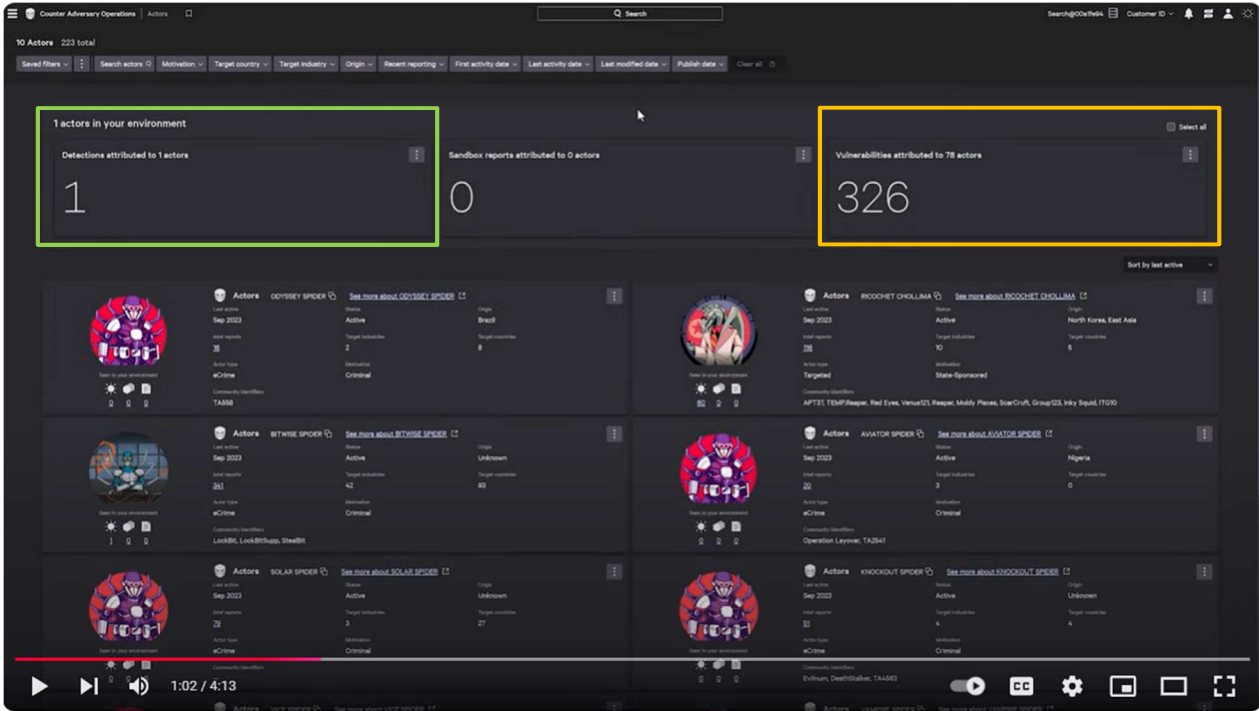
HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY

Claim Language	CrowdStrike Falcon Platform
	 collects key details like affected systems, active exploitation status, and https://www.youtube.com/watch?v=YPOSTBgXkKi0&t
[8D] creating a constraint set of vulnerabilities of the computer system from the set of vulnerabilities comprising a minimum set of dependencies to operate the computer system, wherein application of the set of exploits on the computer system comprises determining the effect of the set of exploits on the	The CrowdStrike Falcon Platform performs a method that includes “<i>creating a constraint set of vulnerabilities of the computer system from the set of vulnerabilities comprising a minimum set of dependencies to operate the computer system, wherein application of the set of exploits on the computer system comprises determining the effect of the set of exploits on the constraint set of vulnerabilities of the computer system;</i>” For instance, CrowdStrike Falcon Sandbox “create[s] a controlled and isolated environment” (e.g., <i>a minimum set of dependencies to operate the computer system</i>) which “establishes a space where potentially harmful code can be safely executed” (e.g., <i>creating a constraint set of vulnerabilities of the computer system from the set of vulnerabilities</i>) in which “investigators can ensure the rest

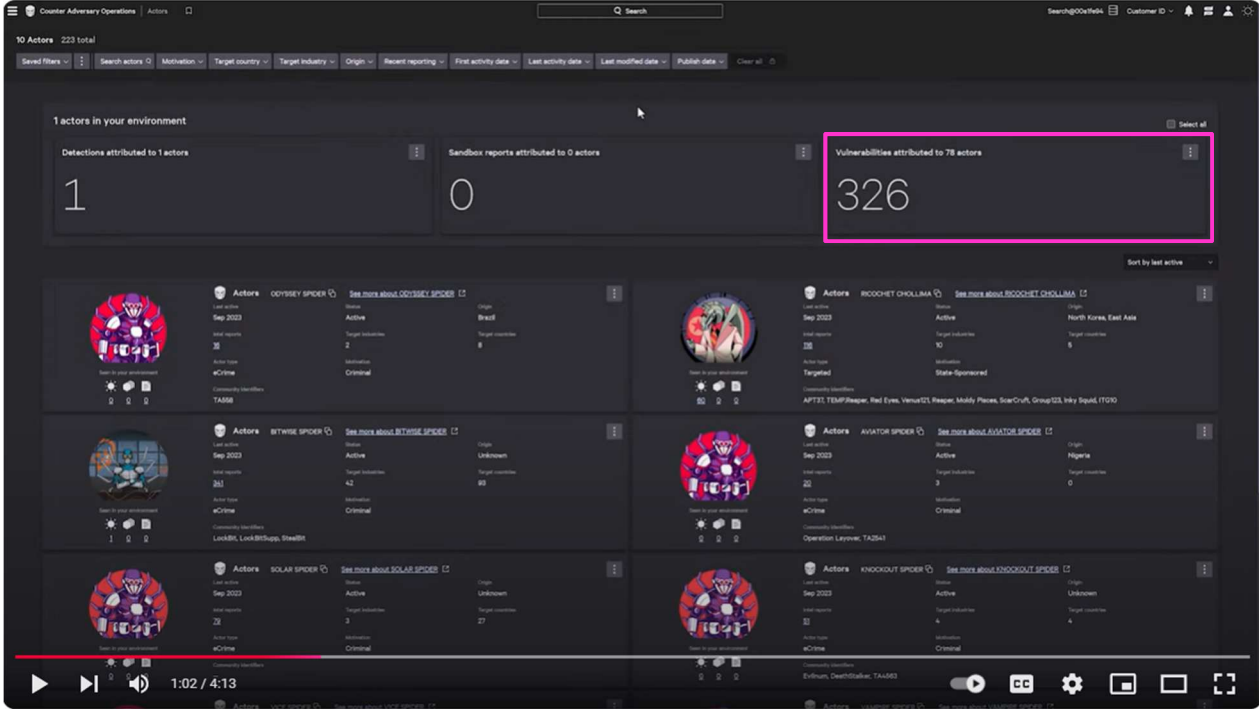
Claim Language	CrowdStrike Falcon Platform
constraint set of vulnerabilities of the computer system;	of the system remains unaffected, thereby minimizing the risk of a security breach.” For example, “[a]pplication-level sandboxes restrict an application's access to certain system resources. These provide enough resources for testing malicious code while still preventing that code from causing wider damage.” CrowdStrike Falcon Sandbox monitors the harmful code’s behavior, the monitoring may include the following activities: “Tracking its interaction with the file system,” “System calls,” and “Network activities.” CrowdStrike Falcon Sandbox employ various analysis methods including: “Dynamic/runtime analysis” which means “observes the code in real time as it executes within the sandbox environment.” This “aids in the detection of malicious activity that only occurs during execution.” (e.g., <i>application of the set of exploits on the computer system comprises determining the effect of the set of exploits on the constraint set of vulnerabilities of the computer system</i>) Introducing CrowdStrike Falcon Sandbox CrowdStrike Falcon® Sandbox is a module built on the integrated, cloud-native CrowdStrike Falcon® platform. By coupling its analysis results with threat intelligence, Falcon Sandbox delivers actionable indicators of compromise (IOCs) to your security team. Its cutting-edge analysis technology enables the detection of advanced threats, and it can integrate seamlessly via rich APIs. Cybersecurity sandboxing is a powerful tool for identifying and analyzing potential threats in a controlled environment. By isolating suspicious code, security teams can study malware behaviors without triggering a system-wide compromise and gain crucial insights for developing stronger defenses. With tools like CrowdStrike Falcon Sandbox, your organization will be better equipped to navigate the challenges of modern cybersecurity threats. When you’re ready to get started, try CrowdStrike Adversary Intelligence

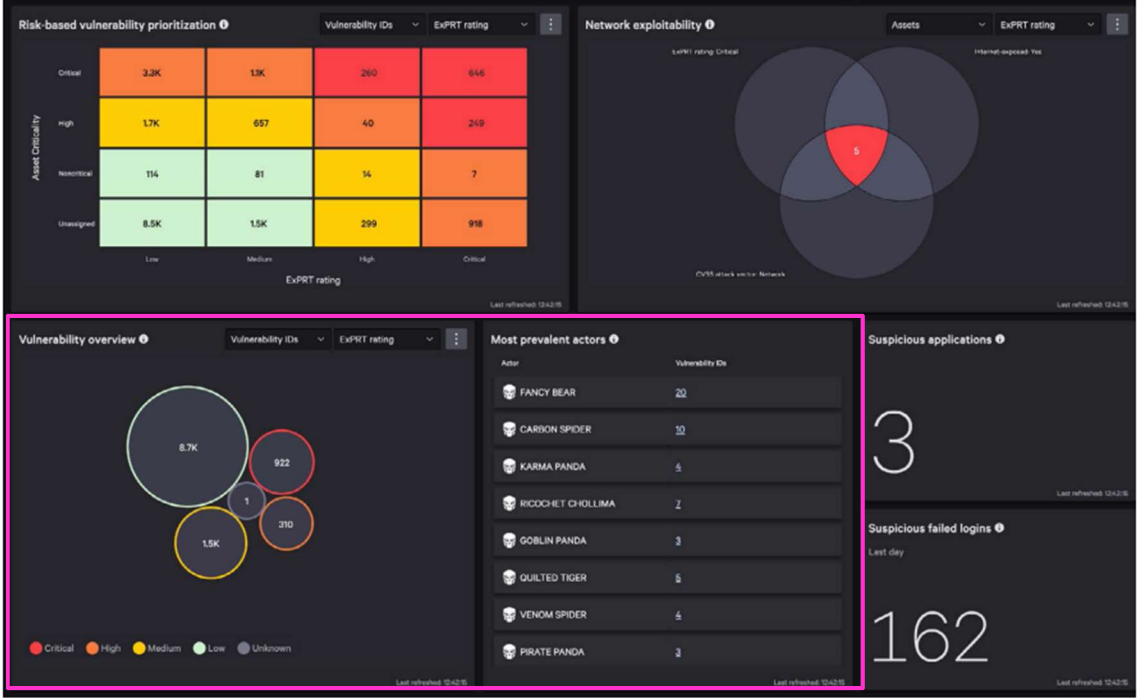
Claim Language	CrowdStrike Falcon Platform
	I Core concepts Although cybersecurity sandboxing may initially seem complex, we can break it down into several simple core concepts. The first of these is sandboxing itself, or the isolation of suspicious code. Isolation of suspicious code Sandboxing involves creating a controlled and isolated environment. Although it’s commonly used in software development, sandboxing in cybersecurity establishes a space where potentially harmful code can be safely executed. By isolating execution, investigators can ensure the rest of the system remains unaffected, thereby minimizing the risk of a security breach. Monitoring and analyzing behavior Once the suspicious code is isolated, cybersecurity researchers can monitor its behavior closely. This monitoring may include the following activities: → Tracking its interaction with the file system → System calls → Network activities

Claim Language	CrowdStrike Falcon Platform
	→ Application-level sandboxes restrict an application's access to certain system resources. These provide enough resources for testing malicious code while still preventing that code from causing wider damage. Each component contributes significantly to the safe execution and thorough analysis of suspicious code. Methods of analysis Cybersecurity professionals employ various analysis methods to investigate suspicious code from various angles: → Static analysis examines suspicious code — without executing it — to look for known malicious patterns. This offers a quick way to find potential threats without running the code. → Dynamic/runtime analysis observes the code in real time as it executes within the sandbox environment. This aids in the detection of malicious activity that only occurs during execution. → Memory dump analysis involves inspecting the memory image from the sandbox to detect malicious code residing in memory. This practice is crucial for identifying threats that reside solely in memory and leave few other traces. https://www.crowdstrike.com/en-au/cybersecurity-101/threat-intelligence/cybersecurity-sandboxing/ For instance, Falcon Adversary Intelligence is demonstrated below having detected 326 “<i>Vulnerabilities</i> attributed to 78 actors” (e.g., <i>creating a constraint set of the computer system from the set of vulnerabilities</i>) based on a customer’s computer “<i>environment</i>” (e.g., <i>the constraint set comprising a minimum set of dependencies to operate the computer system</i>).

Claim Language	CrowdStrike Falcon Platform
	 The screenshot displays the CrowdStrike Falcon Platform interface. At the top, it shows '10 Actors' and '223 total'. Below this, there are three summary boxes: '1 actors in your environment' (highlighted with a green border), 'Sandbox reports attributed to 0 actors' (highlighted with a yellow border), and 'Vulnerabilities attributed to 78 actors' (highlighted with a yellow border). The main area lists several actors, including ODYSSEY SPIDER, BICOCHET OCHOLIMA, INTRINSIC SPIDER, AVATAR SPIDER, SOLAR SPIDER, and KNOCKOUT SPIDER, each with associated statistics and a 'See more about' link. A video player at the bottom shows a video titled 'CrowdStrike Falcon Platform' with a duration of 1:02 / 4:13. https://www.youtube.com/watch?v=RrKQN8x2Ldc (emphasis added) In addition, the Falcon Exposure Management dashboard is demonstrated below managing “1.6K” assets with 7 “Internet-exposed <i>assets</i>” (e.g., <i>the constraint set comprising a minimum set of dependencies to operate the computer system</i>) and “<i>Vulnerability</i> IDs” based on “prevalent actors” such as “FANCY BEAR” (20) and “CARBON SPIDER” (10) (e.g., <i>creating a constraint set of the computer system from the set of vulnerabilities</i>).

Claim Language	CrowdStrike Falcon Platform
	Falcon Exposure Management unified main dashboard https://www.crowdstrike.com/wp-content/uploads/2024/09/falcon-exposure-management-data-sheet.pdf (emphasis added)

Claim Language	CrowdStrike Falcon Platform
	As previously discussed, Falcon Adversary Intelligence is demonstrated below having 326 “Vulnerabilities attributed to 78 actors” based on a customer’s computer “environment” (e.g., <i>application of the set of exploits on the computer system comprises determining the effect of the set of exploits on the constraint set of vulnerabilities of the computer system</i>).  https://www.youtube.com/watch?v=RrKQN8x2Ldc (emphasis added) In addition, the Falcon Exposure Management dashboard is demonstrated displaying “Vulnerability IDs” based on “prevalent actors” such as “FANCY BEAR” (20) and “CARBON SPIDER” (10) as well as 922 “Critical” “Vulnerability IDs” based on “ExPRT rating” (e.g., <i>application of the set of exploits on the computer system comprises determining the effect of the set of exploits on the constraint set of vulnerabilities of the computer system</i>).

Claim Language	CrowdStrike Falcon Platform
	 Falcon Exposure Management unified main dashboard https://www.crowdstrike.com/wp-content/uploads/2024/09/falcon-exposure-management-data-sheet.pdf (emphasis added)
[8E] analyzing an application associated with the set of exploits on the computer system to detect a particular vulnerability of the constraint set of vulnerabilities of the computer system; and	The CrowdStrike Falcon Platform performs a method that includes “<i>analyzing the application of the set of exploits on the computer system to detect a particular vulnerability of the computer system.</i>” For example, as previously discussed, the Falcon Sandbox, by isolating suspicious code, “can help analyze the impact of suspicious code” by “monitor[ing] code behavior within a controlled environment.” (e.g., <i>analyzing an application associated with the set of exploits on the computer system</i>) “The data collected through sandbox investigations can be used for proactive threat