**United States House of Representatives**
**Committee on Homeland Security**
**Subcommittee on Cybersecurity and Infrastructure Protection**

**Testimony of Adam Meyers**
**Senior Vice President, Counter Adversary Operations**
**CrowdStrike Holdings, Inc.**

September 24, 2024

Chairmen Green and Garbarino, Ranking Members Thompson and Swalwell, Members of the Subcommittee: Good afternoon and thank you for having me here today. I am Adam Meyers, Senior Vice President for Counter Adversary Operations at CrowdStrike.

At CrowdStrike, our vision is to protect good people from bad things, and we have been very successful at doing that for more than a decade. I am proud to lead the threat intelligence side of our business. In my role, I direct a geographically dispersed team of cyber threat experts tracking criminal, state-sponsored, and cyber adversary groups across the globe. My team's goal is to produce actionable intelligence and leverage it to protect our customers from malicious cyber behavior and stop increasingly sophisticated adversaries.

Despite our strong track record in these areas, I am here today because, just over two months ago, on July 19, we let our customers down. As part of regular operations, CrowdStrike released a content configuration update for the Windows sensor that resulted in system crashes for many of our customers.

On behalf of everyone at CrowdStrike, I want to apologize. We are deeply sorry this happened and are determined to prevent it from happening again. We appreciate the incredible round-the-clock efforts of our customers and partners who, working alongside our teams, mobilized immediately to restore systems and bring many back online within hours. I can assure you that we continue to approach this with a great sense of urgency.

More broadly, I want to underscore that this was not a cyberattack from foreign threat actors. The incident was caused by a CrowdStrike rapid response content update. We have taken steps to help ensure that this issue cannot recur, and we are pleased to report that, as of July 29, approximately 99% of Windows sensors were back online.

Since this happened, we have endeavored to be transparent and committed to learning from what took place. We have undertaken a full review of our systems and begun implementing plans to bolster our content update procedures so that we emerge from this experience as a stronger company. I can assure you that we will take the lessons learned from this incident and use them to inform our work as we improve for the future.

I look forward to our discussion today about what happened, our subsequent diligent focus on restoring customer systems, and what we have done to enhance our processes since.

**CrowdStrike and The Falcon Platform**

CrowdStrike was built on the principle of applying the Observe, Orient, Decide, Act ("OODA") loop methodology, originally developed for military combat operations. This approach emphasizes the critical importance of speed in cybersecurity, where the ability to quickly observe threats, orient to the changing landscape, decide on a course of action, and execute that action faster than the adversary is paramount.[1] CrowdStrike leverages this methodology to protect 538 Fortune 1000 companies, 298 Fortune 500 firms, and 43 of 50 U.S. states from sophisticated nation-state, hacktivist, and criminal threat actors.[2]

CrowdStrike has redefined security with the world's most advanced cloud-native platform that protects and enables the people, processes, and technologies that drive modern enterprise. CrowdStrike secures the most critical areas of risk—endpoints and cloud workloads, identity, and data—to keep customers ahead of today's adversaries and stop breaches. We have done attribution on attackers hiding in the shadows; we have disrupted ransomware attacks and high-risk intrusions at thousands of companies; and we have identified and blocked nation state adversaries seeking to exfiltrate valuable intellectual property globally.

In today's rapidly evolving threat landscape, the need for dynamic security measures is critical. Adversaries continue to employ increasingly sophisticated techniques to target and infiltrate systems at various stages. We have unfortunately seen a drastic rise in the malicious technologies deployed by bad actors, and the complexity of attacks continues to increase as a reaction to defenders' postures. My particular work at CrowdStrike is focused on ensuring the smooth and speedy integration of intelligence into our entire lineup of products and services to help prevent and detect threats.

The concept of "community immunity" from the public health world applies directly to cybersecurity. As more organizations join the CrowdStrike network, the collective security of all customers improves. Each customer—even each endpoint—contributes additional context and visibility, making the system smarter and faster in detecting and mitigating threats. This network effect means that every participant, including those in especially targeted industries, enhances the security of the entire CrowdStrike community, creating a powerful defensive ecosystem that benefits all. As this network includes trillions of events per day derived from the global footprint of threats detected in technology, telecommunications, financial, government, retail, manufacturing, healthcare, services, education, media, and more, customers of all sizes benefit from sophisticated protection. Simply put, a thwarted breach for one customer provides a new line of defense for all customers.

[1] Falcon operates at global, cloud-scaled speeds to detect and contain threats before adversaries can escalate their attacks, effectively managing "breakout time."
[2] As of April 30, 2024

Powered by the CrowdStrike Security Cloud, our Falcon Platform leverages real-time indicators of attack, threat intelligence on evolving adversary tradecraft, and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities—all through a single, lightweight agent.

**The July 19 Incident: What Happened?**

CrowdStrike's Falcon platform is a cloud-native, AI-powered platform that protects customers with a combination of cloud (the CrowdStrike Security Cloud) and on-device security (the Falcon sensor). The CrowdStrike Security Cloud regularly communicates with Falcon sensors installed on customers' endpoints, such as laptops, desktops, and servers. The Falcon sensor leverages AI, detection and prevention engines. The detection engine includes the ability to collect threat-related data by following a predefined set of configurations. New configurations are regularly sent to the sensor's detection engine to help protect customers against emerging threats, such as malicious code, ransomware, and data breaches. These threat detection configurations are validated before being sent to the Falcon sensor. Upon receiving new configurations, the Falcon sensor follows a predefined set of rules to enhance detections.

On July 19, 2024, new threat detection configurations were validated through regular validation procedures and sent to sensors running on Microsoft Windows devices. However, the configurations were not understood by the Falcon sensor's rules engine, leading affected sensors to malfunction until the problematic configurations were replaced.

**Why Did it Happen?**

CrowdStrike maintains rigorous testing and validation throughout its entire software development and configuration information creation processes. As part of these testing and validation processes, CrowdStrike's software code is certified by Microsoft through the Windows Hardware Quality Labs ("WHQL") program and tested through a quality assurance process. Configurations read by the code are validated to conform with the expected input specification. While code is updated less frequently, new configurations are sent with rapid occurrence to protect against threats as they evolve.

On July 19, 2024, using a longstanding, routine process, we updated threat detection configuration information leveraged by the sensor, without needing to update the sensor's code. As we describe in detail in our Technical Root Cause Analysis, the July 19 incident stemmed from a confluence of factors that ultimately resulted in the Falcon sensor attempting to follow a threat detection configuration for which there was no corresponding definition of what to do.

1. **Validation**. Our validation and testing processes in use for the past decade did not catch this unexpected discrepancy. These validation checks missed this specific scenario, which had not occurred before: a mismatch between input parameters and predefined rules.

2. **Testing**. During the development and testing phases, the scenarios tested did not include cases where the final input parameter contained a new configuration that needed a corresponding rule.

3. **Input**. The Falcon sensor's rules engine was designed to receive a specific number of inputs and take corresponding actions based upon configurations. Each input would lead to a specific threat detection action defined by the rules. One of the configurations sent on July 19, 2024, contained an extra input for which there was no defined action. This mismatch led the software to follow a configuration without knowing which rules to follow, triggering a malfunction.

**Our Support for Customers in the Wake of the Incident**

CrowdStrike began working with customers and partners to bring systems online as quickly as possible, initially through manual remediation. These efforts enabled the systems to come back online within hours following the initial incident.

On July 22, 2024, CrowdStrike introduced automated techniques to accelerate remediation.

To further help customers bring systems online as quickly as possible, CrowdStrike deployed personnel and engaged with strategic partner services teams to assist customers with recovery efforts. We also worked to provide continuous and transparent updates to customers throughout our response. As of July 29, virtually all of our customers' systems were back up and running.

**Enhancements to Help Ensure This Won't Happen Again**

We have successfully deployed critical detection and preventions over the past decade, validated and tested by our processes, to protect organizations against millions of threats from sophisticated adversaries without such an incident. Since July 19, 2024, we have implemented multiple enhancements to our deployment processes to make them more robust and help prevent recurrence of such an incident—without compromising our ability to protect customers against rapidly-evolving cyber threats.

1. **Validation**. We have introduced new validation checks to help ensure that the number of inputs expected by the sensor and its predefined rules match the same number of threat detection configurations provided. This is designed to prevent similar mismatches from occurring in the future.

2. **Testing**. We have enhanced existing testing procedures to cover a broader array of scenarios. This includes testing all input fields under various conditions to detect potential flaws before rapidly-released threat detection configuration information is sent to the sensor.

3. **Customer Control**. We have provided customers with additional controls over the deployment of configuration updates to their systems.

4. **Rollouts.** Our threat detection configuration information, known as Rapid Response Content, is now released gradually across increasing rings of deployment (*See* Appendix). This allows us to monitor for issues in a controlled environment and proactively roll back changes if problems are detected before affecting a wider population.

5. **Safeguards**. We have added additional runtime checks to the system, designed to ensure that the data provided matches the system's expectations before any processing occurs. We are also working to further enhance our safeguards for validation and quality assurance, including by implementing more granular controls.

6. **Third-Party Reviews.** We have engaged two independent third-party software security vendors to conduct further Falcon sensor code and end-to-end quality control and release processes reviews.

**Emerging Threats to Resiliency Posed by Adversaries**

As we have enhanced our own resiliency, we remain steadfast in our commitment to continuing to protect our customers against disruptive cyberattacks as we have for a decade. In doing so, we must remain vigilant against cyber threats on the horizon.

Advancements in threat detection, prevention, and response capabilities have aided defenders in recent years, but adversaries have responded by increasingly adopting and relying on techniques to evade detection. This includes supply chain attacks, insider threats, and identity-based attacks. Threat actors' speed also continues to accelerate as adversaries compress the time between initial entry, lateral movement, and "actions of objective" (like data exfiltration or attack). At the same time, the rise of generative AI has the potential to lower the barrier of entry for low-skilled adversaries, making it easier to launch attacks that are more sophisticated and state of the art.

These threats include nation-state adversaries, issue-motivated "hacktivists," and sophisticated eCrime actors motivated by profit. China-nexus adversaries, for instance, have continued to operate at an unmatched pace across the global landscape, leveraging stealth and scale to collect targeted group surveillance data, strategic intelligence and intellectual property. In other areas of the world, conflict has continued to drive nation-state and hacktivist adversary activity. In 2023, as the Russia-Ukraine war entered its second year, Russia-nexus adversaries and activity clusters maintained high, sustained levels of activity in support of Russian Intelligence Service ("RIS") intelligence collection, disruptive activity, and information operations (IO) targeting Ukraine and NATO countries. Iran-nexus adversaries and Middle East hacktivist adversaries were also observed pivoting cyber operations in the latter half of last year in alignment with kinetic operations stemming from the 2023 Israel-Hamas conflict. And North

Korean adversaries maintained a consistently high tempo throughout 2023. Their activity continued to focus on financial gain via cryptocurrency theft and intelligence collection from South Korean and Western organizations, specifically in the academic, aerospace, defense, government, manufacturing, media and technology sectors. In the eCrime sphere, ransomware remains a chronic problem targeting victim organizations across the globe.

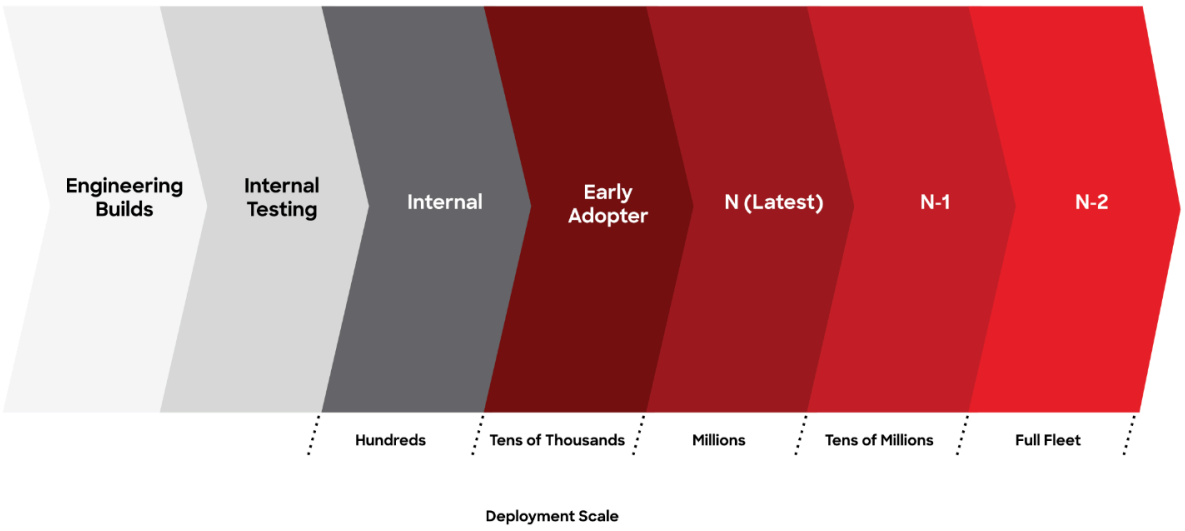
**Our Ongoing Commitment to Our Partners and Customers**

Nothing is more important to CrowdStrike than the trust and confidence that our customers and partners have put into our company and its products as we continue our mission to stop breaches. We have long focused on protecting the resiliency of critical organizations and infrastructure against sophisticated adversaries. Going forward, we will build upon our longstanding contributions to cybersecurity by continuing to share our lessons learned on ecosystem resiliency.

Thank you, and I look forward to your questions.

CROWDSTRIKE

## Sensor Software Updates




## Rapid Response Content