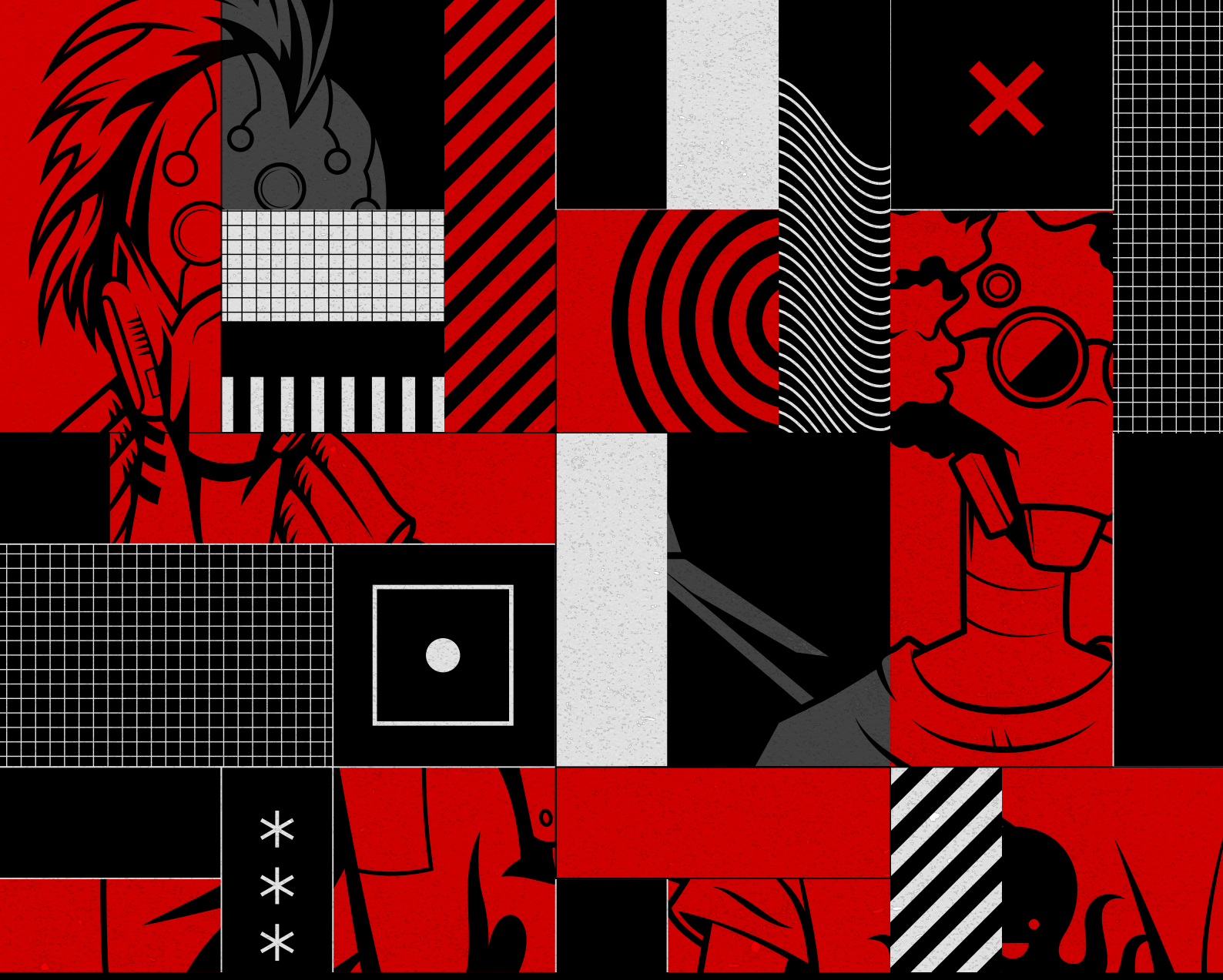


CROWDSTRIKE

Combating Cross-Domain Attacks Across Endpoint, Identity and Cloud

How speed, visibility and unified security defeat the new era of cyber threats

Today's sophisticated adversaries are targeting not just isolated systems but entire interconnected domains — spanning endpoints, identities and cloud environments. These cross-domain attacks exploit fragmented security measures, leveraging compromised credentials, valid tools and gaps between siloed systems to infiltrate, escalate and execute their objectives with unprecedented speed and precision.

The rise of cloud-native infrastructures, hybrid environments and remote work has expanded organizational attack surfaces while increasing complexity. In this eBook, CrowdStrike dissects the anatomy of cross-domain attacks, unveiling how adversaries navigate modern IT ecosystems to evade traditional defenses. From real-world case studies featuring notorious adversaries like SCATTERED SPIDER and HORDE PANDA to actionable strategies for proactive threat hunting, this eBook empowers security teams to dismantle silos, streamline operations and stay ahead of evolving threats.

Prepare to uncover how a unified platform redefines modern defense, ensuring unmatched visibility, accelerated response times and robust protection against the next wave of cyber adversaries.

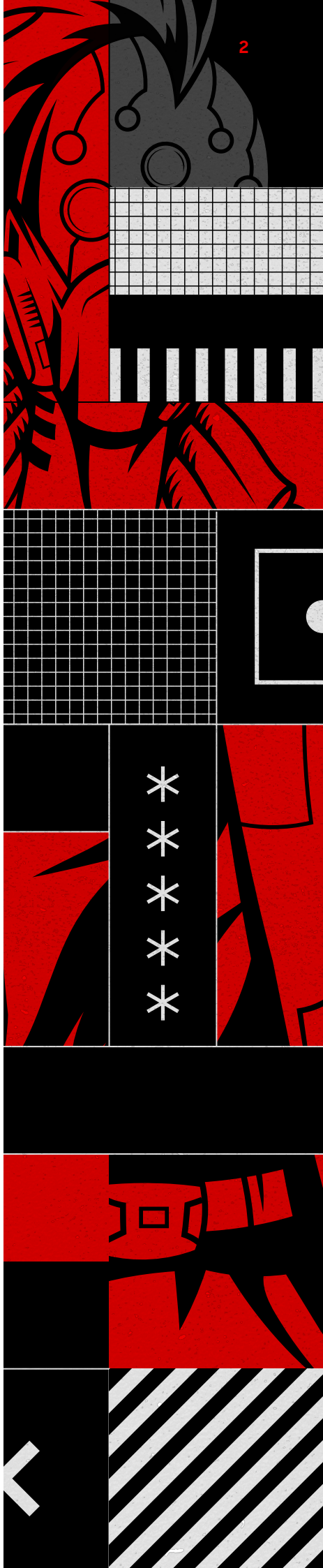


Table of Contents

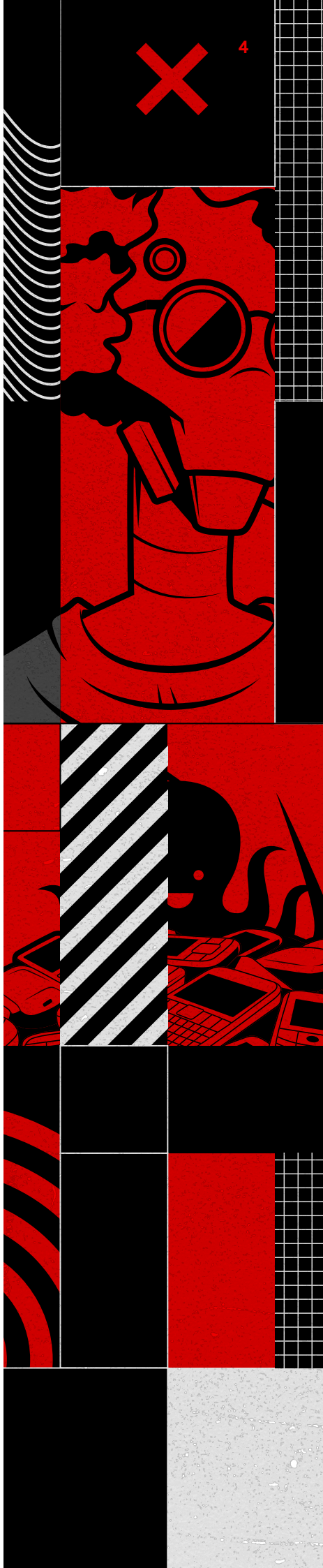
The Rise of Cross-Domain Attacks

Modern adversaries live by two principles: speed and stealth. These aren't the brute-force hackers of old. Today's attackers operate faster and quieter than ever, using legitimate tools to carry out rapid, hands-on-keyboard attacks while remaining under the radar. This calculated shift in tactics allows them to bypass defenses, exploiting trusted systems and processes with a cunning that often goes without a trace.

What's driving this shift in tactics? As security defenses strengthened and became more adept at detecting long-standing threats, cybercriminals have been compelled to adopt stealthier, more sophisticated methods. For example, traditional malware attacks have lost their edge because security systems have gotten better at detecting and neutralizing them. This evolution has pushed adversaries to explore more inventive intrusion methods. Case in point: 75% of attacks to gain initial access are now malware-free.[1]

At the same time, cybercriminals are increasingly using valid credentials to bypass defenses entirely, leveraging compromised credentials as a low-effort, high-reward approach. This trend is fueled by a booming industry of access brokers — an underground marketplace for compromised credentials. These brokers act as intermediaries, gaining access to organizations and selling valid entry points to other malicious actors on the dark web. With over 24 billion compromised credentials circulating in this cybercrime ecosystem, demand is only growing.[2]

Fueling the threat landscape even further is the blistering speed of modern cyber intrusions. In 2023, the eCrime breakout time — the window for an adversary to move laterally within a network after initial access — dropped drastically from an average of **84 minutes** to a mere **62 minutes**. The record speed? An astonishing **2 minutes and 7 seconds**, leaving no margin for delayed detection and response.[3]



1 CrowdStrike 2024 Global Threat Report

2 Digital Shadows, Account Takeovers in 2022: The 24-Billion Password Problem

3 CrowdStrike 2024 Global Threat Report

This relentless adversary drive for speed and stealth combined with growing attack sophistication has led to a new era of threats: cross-domain attacks.

Cross-domain attacks aren't just a minor shift — they mark a profound change in how adversaries can achieve their objectives. Once inside, they exploit disjointed security ecosystems, siloed security tools and the gaps between cloud, on-premises and hybrid environments, finding weaknesses to move seamlessly from one domain to the next while blending in with regular user behavior. With this approach, attackers can chart the quickest, most effective paths to high-value targets.

The prevalence of cross-domain attacks underscores the urgent need for organizations to elevate their defenses. This eBook examines the anatomy of cross-domain attacks and outlines a strategic approach for organizations to strengthen their protection and secure their path into the future.

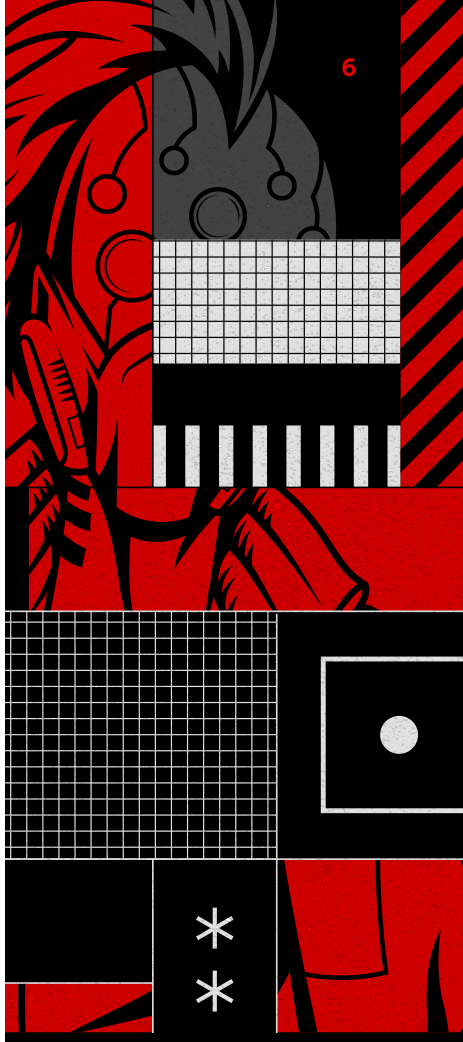
Anatomy of a Cross-Domain Attack

A cross-domain attack is a sophisticated adversary method that exploits weaknesses across multiple domains of an organization's security infrastructure — notably, endpoint, identity and cloud. Once attackers gain an initial foothold — often through credential theft or social engineering — they don't just linger in the entry point domain. Instead, they start an active search for weaknesses in other areas of the network.

This involves probing for accessible applications, accounts, misconfigurations and interdependencies between systems, such as the links between identity management systems and cloud accounts. By navigating through these entry points, they can then move laterally across different domains, each time mimicking legitimate user activity to avoid triggering alerts. Their ultimate objective is to locate and infiltrate high-value targets, such as endpoints with access to sensitive data or privileged accounts.

One of the core challenges of protecting against cross-domain attacks is that the activity often appears fragmented across various parts of the enterprise's digital estate. Individual point security solutions, operating independently within their own domains, often miss the signals of a broader attack campaign. For example, a compromised credential might appear as typical user behavior, especially if it's combined with the use of legitimate tools like remote management software that mimic routine workflows. Attackers capitalize on this disconnect by spreading their actions across domains, which generates fewer alerts and hampers detection, making it challenging for SOCs to recognize the full scope of the intrusion.

Significance of Cross-Domain Attacks



The enterprise IT landscape has evolved into a hyper-connected ecosystem where innovation and interconnectivity fuel growth, but simultaneously widen the attack surface. These advances, while enabling unprecedented operational efficiencies and innovation, have also introduced significant security challenges.

Cross-domain attacks are a direct response to this interconnectedness. They leverage the very innovations that organizations rely on to operate — such as software-as-a-service (SaaS) applications, cloud computing, hybrid environments and remote work infrastructures — which all create new avenues for threat actors to move undetected.

Economic and market forces also play a substantial role in the rise of cross-domain attacks. Businesses, driven to innovate and scale quickly, often adopt cloud-based solutions, hybrid architectures and third-party integrations to remain competitive. In fact, for integrations, companies heavily depend on APIs (application programming interfaces) — averaging 613 per organization — to ensure seamless communication between their various software solutions.[4]

As a result, these environments are highly interconnected and interdependent. Yet they are disjointed, often relying on disparate security systems that lack visibility across domains. For attackers, this infrastructure complexity provides a broad landscape to exploit, where legitimate tools and compromised credentials can be used to infiltrate systems and blend into regular processes.

The current trend toward decentralization — such as the shift to hybrid work and the integration of third-party supply chains — adds further challenges to securing interconnected systems. With critical assets spread across the digital infrastructure, and silos between security teams, processes and tools can create blind spots that adversaries exploit. These gaps in security visibility make it easier for attackers to move laterally across systems without being detected. And, as organizations expand their digital ecosystems, the stakes continue to rise.

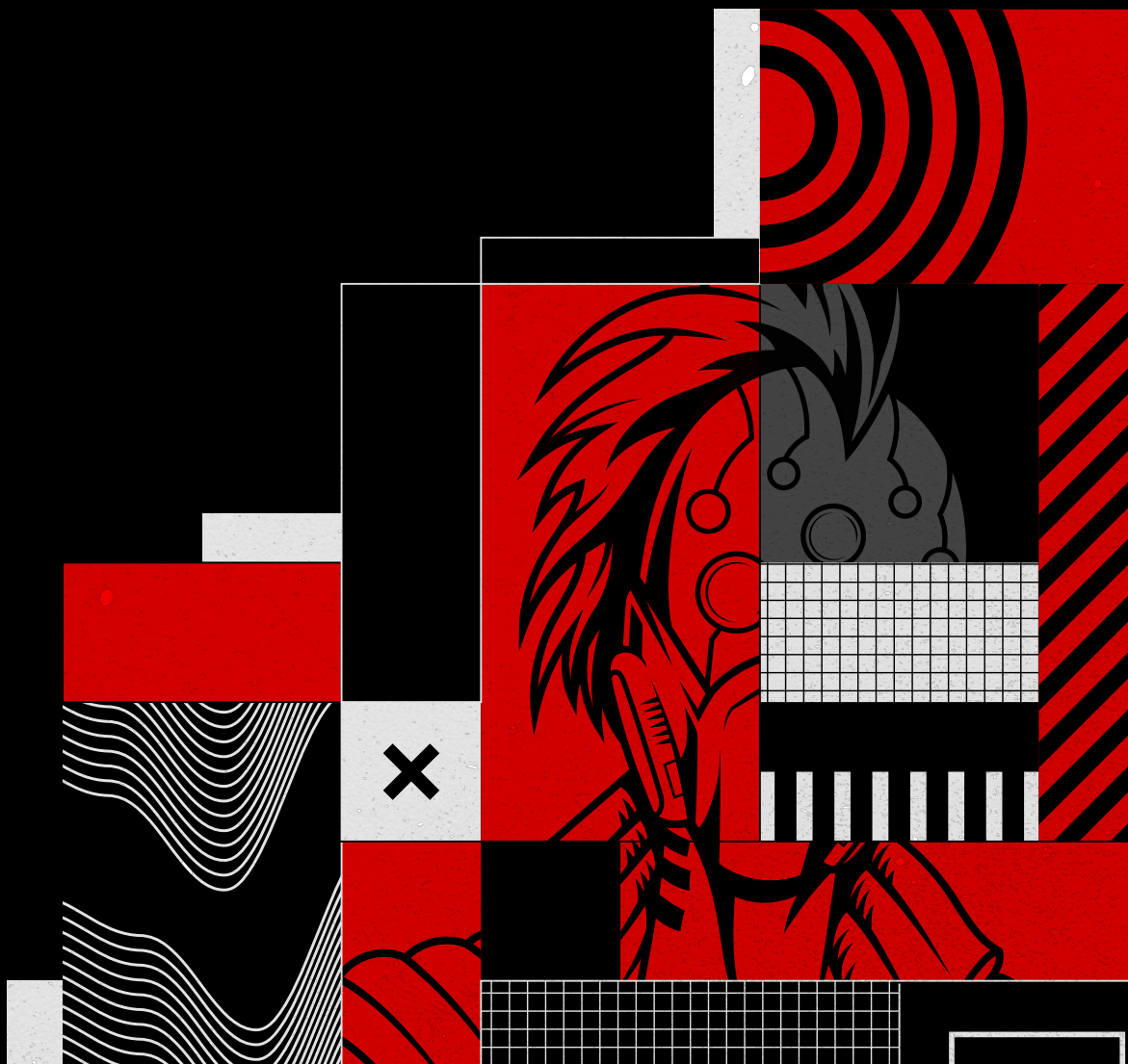
> **"The smartest adversaries will know your environment as well as you do — in many cases, they may know it a lot better than you do, and the whole idea is to slip through the cracks, to generate fewer detections, to fly under the radar."**
>
> **Mike Sentonas**
> **CrowdStrike President**

4 Imperva, The State of API Security in 2024

A Closer Look at Cross-Domain Attack Strategies

To understand how cross-domain attacks exploit interconnected IT environments, it's crucial to examine case studies that reveal the tactics, tools and strategies attackers use to achieve their objectives. While cross-domain intrusions can vary significantly in complexity, CrowdStrike commonly observes adversaries moving between the endpoint and identity planes or pivoting from the cloud to an endpoint.

In the following cases, we explore how adversaries navigate across systems and domains — bypassing defenses and blending in with legitimate activity to gain access to high-value targets. Each example highlights a unique approach.



CASE STUDY

SCATTERED SPIDER: CLOUD-CONSCIOUS ATTACK

OVERVIEW

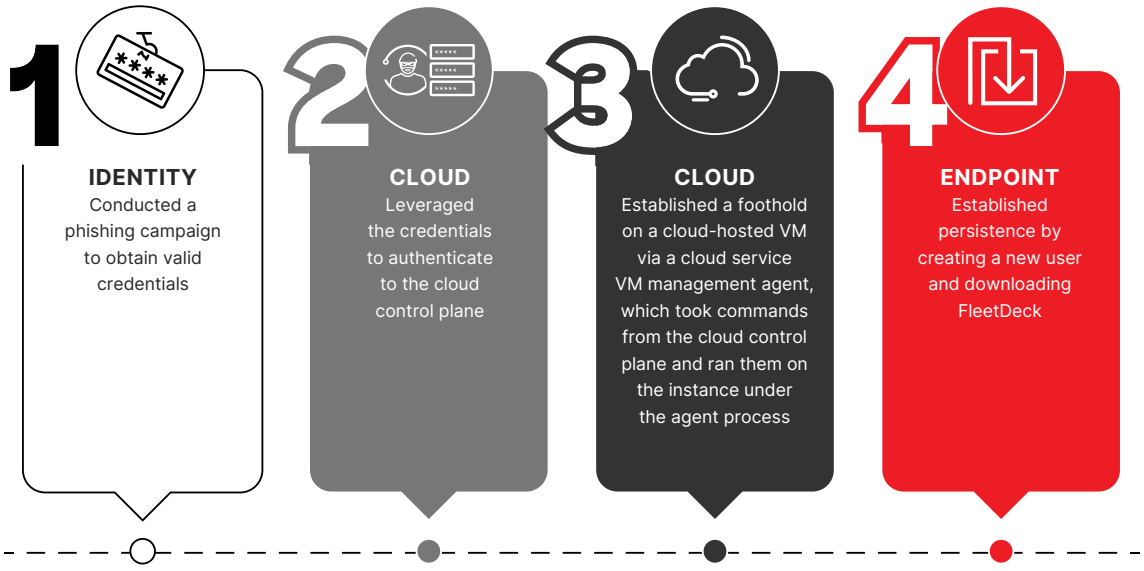
With intrusions in cloud environments surging by 75% from 2022 to 2023, the cloud remains a primary target for adversaries. Tactics have shifted, with "cloud-conscious" attacks — those specifically crafted to exploit cloud-based services — increasing by 110%.[5] Notably, SCATTERED SPIDER remains the most prominent adversary in cloud-based intrusions, conducting 29% of all associated activity observed in 2023.[6]

ATTACK METHODOLOGY

In May 2024, CrowdStrike detected SCATTERED SPIDER established a foothold on a cloud-hosted virtual machine (VM) instance via a cloud service VM management agent. To do so, the adversary compromised existing credentials to authenticate to the cloud control plane via an identified phishing campaign.

After authenticating to the cloud console, the adversary established persistence by executing commands on the cloud-hosted VM via the management agent. After establishing an initial connection, SCATTERED SPIDER executed the `ping` command against several domains within and outside of the target organization, likely to identify their level of access and visibility within the network. The adversary then ran several variations of the `nltest` command to identify domain controllers (DCs) of interest and the `wmic` command to identify programs currently installed on the host.

Finally, the adversary established persistence by creating a new user on the host and attempting to download FleetDeck remote access software.



5 CrowdStrike 2024 Global Threat Report

6 CrowdStrike 2024 Threat Hunting Report

SCATTERED SPIDER

PROFILE

SCATTERED SPIDER is a prolific eCrime adversary that has conducted a range of financially motivated activity since early 2022. The adversary's early campaigns predominantly targeted firms specializing in customer relationship management (CRM) and business-process outsourcing (BPO), as well as telecommunications and technology companies.

Identity abuse is central to SCATTERED SPIDER's tradecraft. The adversary often specifically targets accounts belonging to IT and information security personnel in order to gain access to security tooling, or to documentation and other resources that may assist with lateral movement and account compromise.

CASE STUDY

CHEF SPIDER: ENDPOINT ATTACK

OVERVIEW

In some cases, adversaries gain an initial foothold in an organization through social engineering tactics, tricking users into allowing access to an endpoint. Once inside, they operate under the radar by using legitimate remote monitoring and management (RMM) tools to remotely control a computer without authorization, for the purpose of commercial advantage and private financial gain. In fact, the use of RMM tools among attackers surged by 70% year-over-year, with 27% of all interactive intrusions leveraging these tools to gain unauthorized access.[7]

7 CrowdStrike 2024 Threat Hunting Report

ATTACK METHODOLOGY

CHEF SPIDER used this tactic in May 2024, leveraging RMM tools delivered via social engineering to gain initial access to a network. In this cross-domain attack example, CHEF SPIDER initiated the breach by sending the target victim a phishing email that contained a weaponized link but appeared to be for rescheduling a meeting.

Once the victim clicked on the link, ConnectWise's RMM tool, ScreenConnect, was downloaded to the victim's host, establishing contact with CHEF SPIDER's controlled infrastructure.

From there, the adversary executed a malicious `.bat` script, enabling them to manipulate power settings on the victim host. In just six minutes, they gained a foothold within the network, allowing them to explore vulnerabilities and identify pathways for lateral movement to other systems.

This rapid intrusion not only underscores the efficiency of the adversary's tactics but also highlights the significant risks posed by unchecked access and the interconnected nature of modern IT environments.

CHEF SPIDER

PROFILE

CHEF SPIDER is an eCrime adversary that has historically compromised point-of-sale (POS) systems in the food & beverage and hospitality sectors, likely to steal payment card information (PCI).

The adversary has also likely acted as an access broker for other eCrime adversaries in several 2023 intrusions.

Since discovery in March 2021, CHEF SPIDER has consistently deployed the remote monitoring and management (RMM) tool ConnectWise ScreenConnect, gaining initial access either by exploiting public-facing applications or via tailored social engineering.

CHEF SPIDER's social-engineering techniques include spoofing legitimate companies by typosquatting their domains and impersonating their executives. CHEF SPIDER poses as a potential customer to lure targets into downloading ScreenConnect installers from an alleged scheduling page.

*****

CASE STUDY

HORDE PANDA: IDENTITY ATTACK

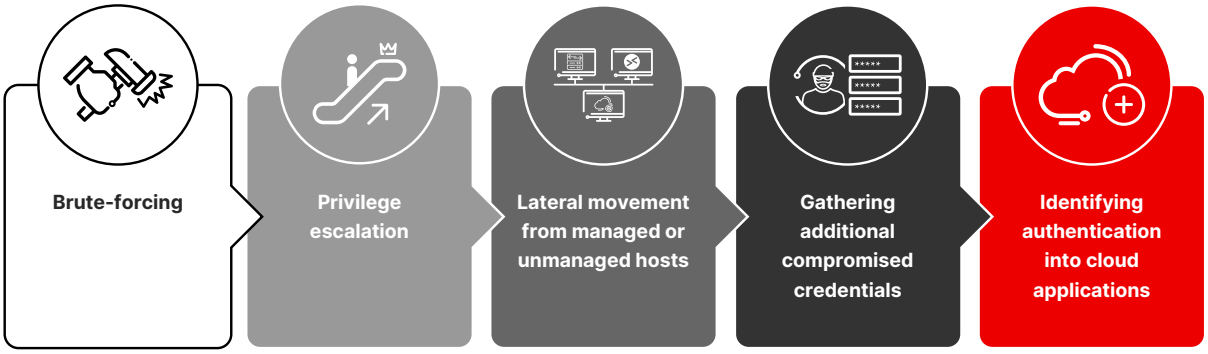
OVERVIEW

Adversaries continue to maximize the use of stolen credentials to effortlessly stroll into an organization's digital estate. Indeed, five of the top 10 MITRE ATT&CK® techniques observed from July 2023 to June 2024 were identity-based.[8] Once attackers gain entry, they can seamlessly navigate through the entire infrastructure, using what's known as hybrid lateral movement — where adversaries move between on-premises identity providers and the cloud, or vice versa.

ATTACK METHODOLOGY

Between late June 2023 and early August 2023, using identity-based indicators, CrowdStrike identified suspicious activity at a South Asian telecommunications provider. The China-nexus HORDE PANDA adversary leveraged multiple compromised identities to attempt to embed further into the network and move laterally. The adversary gained initial access via the VPN IP range.

In early July 2023, CrowdStrike Counter Adversary Operations investigated identity hunting leads for unusual activity targeting a domain controller (DC). This activity originated from unexpected sources, including the VPN IP range and a host that was not registered with a CrowdStrike Falcon® sensor for endpoint. Domain replication requests using DCSync had been attempted from five user accounts but were unsuccessful, as the requesting accounts lacked the permissions for domain replication.



8 CrowdStrike 2024 Threat Hunting Report

HORDE PANDA

PROFILE

HORDE PANDA is a China-based targeted intrusion adversary that has been active since at least mid-2023 with operations that primarily focus on entities in the telecommunications sector in South Asia.

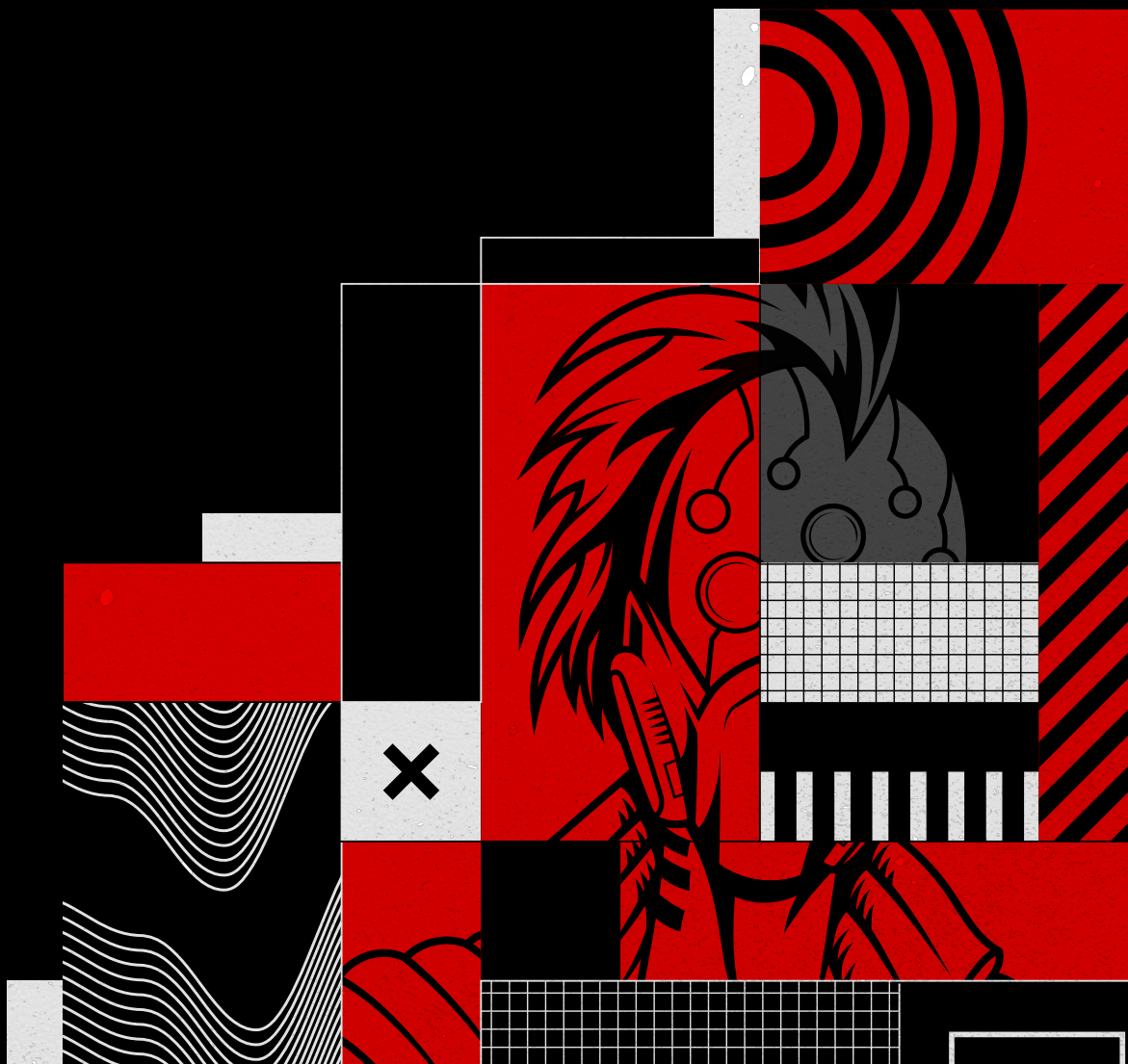
HORDE PANDA leverages several shared China-nexus malware families, including KEYPLUG, ShadowPad, Proxip and PlugX. The adversary also uses LuaPlug — a custom malware family unique to their operations.

HORDE PANDA deploys malware via DLL search-order hijacking and uses third-party executables to load implants, including an Open JDK Platform executable, Java Chromium Embedded Framework Helper executables, and the Windows debugger x64dbg. The use of these third-party executables to load implants is a rare tactic. The adversary has deployed multiple malware families on the same victim hosts to facilitate their operations.

Between June 2024 and September 2024, HORDE PANDA acquired and operationalized six new KEYPLUG command-and-control (C2) domains. The adversary continues to leverage Cloudflare's content-delivery network(CDN) to proxy C2 communications, likely in an attempt to obfuscate their operations.

Challenges with a Siloed Security Approach

To effectively tackle cross-domain attacks, it's crucial to recognize the gaps left by isolated, siloed security systems. By acknowledging these security issues, organizations can adopt more integrated and streamlined approaches, empowering SOCs to stay ahead of increasingly sophisticated adversaries.



Disjointed Security Ecosystem

SOC teams today face the challenge of navigating a sprawling average of 50 disparate tools,[9] which creates a fragmented security environment of data streams, scattered alerts and time-intensive — often manual — processes for correlating information across sources. Or, even more alarmingly, many security teams may not be fully aware of their entire cloud footprint, let alone have the tooling deployed to protect it.

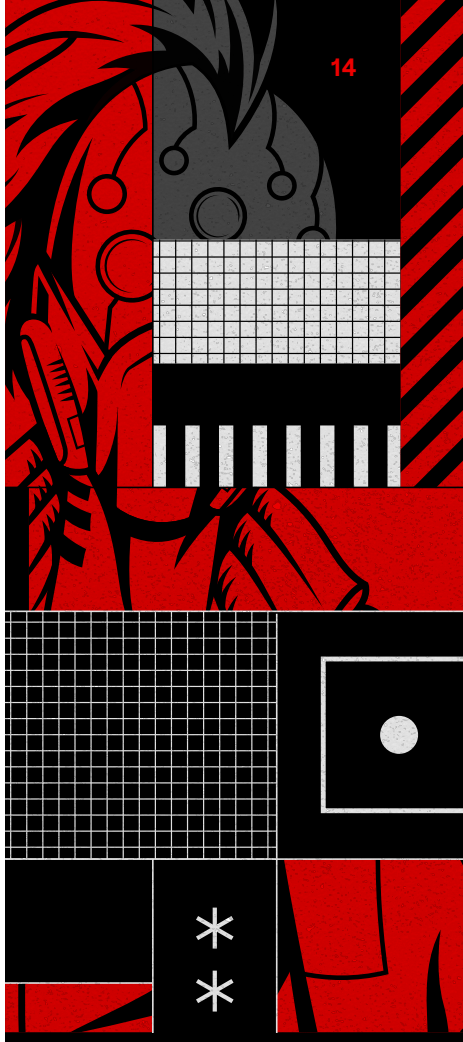
The result is a disjointed security ecosystem, which slows response times and heightens the risk of missing critical indicators. This siloed approach can't keep up with the speed and complexity of modern threats, which take advantage of even brief blind spots to infiltrate and move across endpoint, identity and cloud domains.

Complexity of Fragmented Tools and Costs

The sheer cost and complexity of managing a fragmented security ecosystem impacts both budgets and operational agility. Each additional tool brings its own licensing fees and maintenance requirements and often demands specialized training — driving up costs across the board.

Beyond the budget impact, SOCs are often organized into silos based on domain expertise, which introduces operational inefficiencies. This structure often features teams focused on specialized areas such as cloud security, identity security or IT infrastructure. However, this division leads to fragmented processes that rely heavily on IT service management (ITSM) ticketing systems as the central point for cross-team communication. Through these systems, tickets often lack any context for associated data not explicitly included in the ticket itself, removing critical information pertaining to the threat from internal communications. As a result, disjointed workflows become the norm, creating friction and delays in addressing complex, cross-domain threats as teams struggle to quickly coordinate a unified response.

Stopping or eliminating an adversary one time isn't enough — adversaries persistently adapt and attempt new methods. Consistency is critical to staying ahead, but achieving this consistency becomes nearly impossible when SOCs are forced to manually stitch together fragmented data from siloed tools.



"Speed defines the success of both the attacker and the defender."

Mike Sentonas
CrowdStrike President

9 IDC, How Many Security Tools Do Organizations Have, and What Are Their Consolidation Plans?

Expansion of SaaS Adoption

Adoption of software as a service (SaaS) continues to rapidly increase and remains the largest segment of the cloud market in end-user spending. This SaaS proliferation has created a new attack surface for adversaries, and when it comes to SaaS, IaaS and PaaS applications, there is a shared responsibility model between the vendor and the customer. Cloud providers are responsible for providing robust security controls, while organizations are responsible for ensuring that their environments are properly configured. Organizations can use tens to hundreds of applications to run their business, and each of these apps — SaaS, IaaS, and PaaS alike — requires the management of both global and identity-based configurations in an ever-evolving space. These attack surfaces create more exposure for adversaries to exploit.

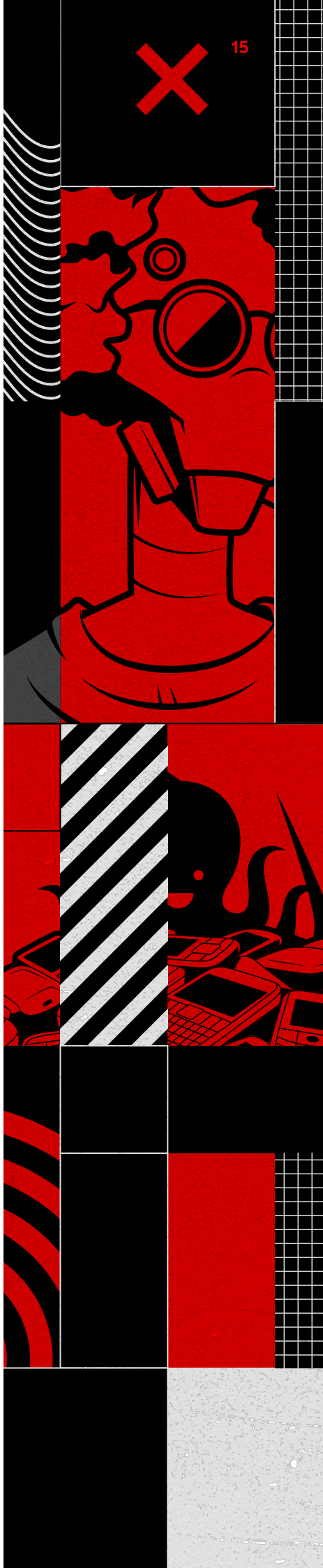
Slow Detection and Response Times

In a fragmented security setup, disjointed detection processes mean that time-consuming manual analysis often becomes a necessity. Remember, these adversaries are moving at lightning speed with a breakout time that can be as short as 2 minutes and 7 seconds. This reality means SOC teams are not just on alert — they're in a relentless race against the clock, requiring them to detect and neutralize threats with precision and agility before attackers can strike.

Each minute of delay risks giving attackers the time they need to dig deeper into systems and expand their reach across the network. But with siloed systems, response efforts are often slowed by time-intensive processes. As a result, investigations often drag on, with 70% of critical issues taking over 12 hours to resolve.[10]

Impact and Consequences for Businesses

The downstream risks of a siloed security approach are profound — from increased threat exposure and ballooning response costs to potential legal and regulatory ramifications. Every missed threat indicator or lengthy investigation represents an opportunity for attackers to exploit weaknesses and move across domains. This not only heightens financial and operational risk but also underscores the urgency of unifying security operations. Proactive, strategic alignment across security functions is key to eliminating these silo-induced weaknesses and establishing an effective, forward-thinking security posture.

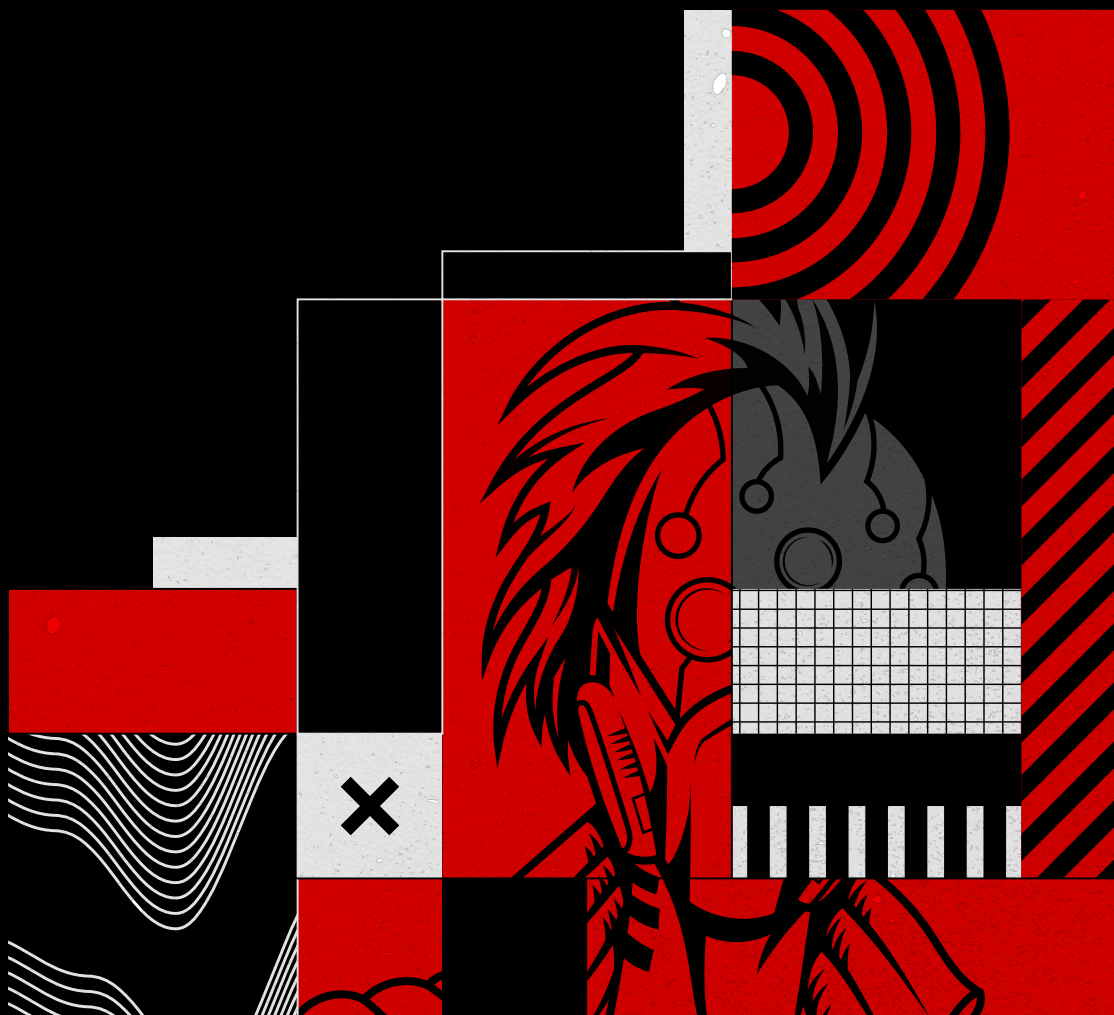


10 CrowdStrike 2024 State of Application Security Report

Speed of Response: The Role of Unified Visibility

In the relentless battle against cross-domain attacks, time is not just a factor, it's the battlefield itself. A robust security strategy to confront these sophisticated adversaries hinges on overcoming today's fragmented tool, team and process silos. By breaking down these barriers, security teams gain the unified visibility they need to detect and neutralize threats before they escalate into full-blown breaches.

To combat the escalating threat of cross-domain attacks, organizations must embrace a new approach — one that demolishes existing silos and emphasizes the critical importance of unified visibility. By integrating insights from diverse security domains, environments and applications, the SOC can create a cohesive defense strategy that empowers the organization to outpace adversaries, streamline incident response and bolster overall operational agility.



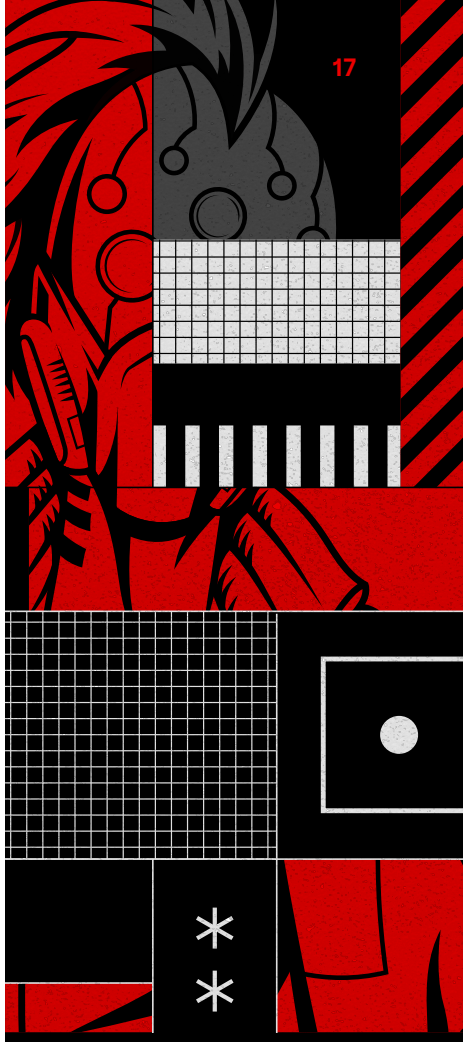
Importance of Consolidating Siloed Tools into a Unified Platform

We have entered a pivotal moment in cybersecurity: the era of cross-domain attacks. These threats are no longer confined to isolated environments — instead, they deftly traverse multiple domains, compromising endpoints, escalating privileges through identity systems and infiltrating cloud services with alarming ease.

To effectively detect and respond to these dynamic threats, security leaders must equip their SOC with centralized visibility and insights from across the organization's environment — particularly from the three key domains of endpoint, identity and cloud. Here, a unified platform serves as the SOC's cyber backbone, pulling together and analyzing telemetry from across various environments. By correlating telemetry and alerts from endpoints, identity systems and cloud services, the platform can effectively identify individual IOCs while synthesizing them into a comprehensive view of suspicious intrusion activity.

The power of a unified platform approach is in its ability to accurately detect and prioritize threats across domains. A security control might flag a potential threat as a low- or medium-priority alert, but when correlated with telemetry and alerts from the other security controls, the threat can escalate to a high priority.

This process tackles the SOC's constant challenge of tuning security policies to strike the right balance between false positives and silent failures. When security controls are too strict, they generate false alarms that disrupt business operations and waste valuable time. On the other hand, if controls are too loose, attacks slip through undetected. By analyzing detections from endpoints, identity systems and cloud services, SOCs gain a modern, adaptive security framework to identify and neutralize cross-domain attacks early in the attack cycle.



"Today's interconnected enterprises need a security approach that can keep up with their increasing complexity. A unified security platform addresses these challenges by bridging the visibility gap between domains that adversaries seek to exploit. Providing an integrated view is essential for detecting cross-domain threats early — before they can traverse the wider ecosystem."

Elia Zaitsev
Chief Technology Officer, CrowdStrike

Outpacing the Cross-Domain Adversary

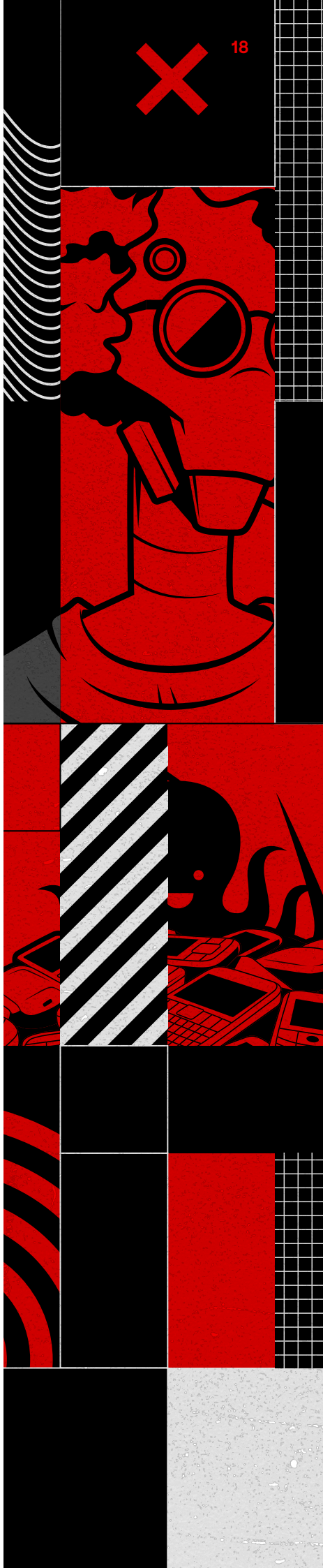
The stakes are high: Each minute lost in detection can give attackers the critical time they need to entrench themselves deeper within the enterprise's digital estate. This is why faster detection and response times are essential — they are the key to drastically reducing mean time to respond (MTTR) and thwarting adversaries before they can fully execute their malicious agendas.

Stopping one attack won't cut it when adversaries constantly adapt and find new ways to infiltrate. Consistent, automated defenses are critical to maintaining the upper hand, but siloed tools make it nearly impossible to achieve this level of continuity. By unifying tools and processes, organizations can eliminate gaps and respond faster to evolving threats.

A unified platform is essential to achieving the speed and precision needed to counter today's advanced, multi-domain threats. By seamlessly integrating high-fidelity telemetry from endpoint, identity and cloud environments along with third-party data and SaaS application activity, a unified platform leverages a modern, cutting-edge architecture built to support AI-driven threat prevention, precise detections and accelerated triage. This advanced architecture allows for real-time data correlation and streamlined alert handling, delivering actionable insights that empower SOC teams to detect and respond to threats with unparalleled speed and accuracy.

This strategy brings SOCs into a new era of agility and operational depth. With AI models fine-tuned for threat detection, the platform uncovers subtle attack indicators across interconnected environments and reduces noise. The result? Faster triage, quicker time-to-detection and a transformed response framework that minimizes the opportunities for adversaries to expand their foothold.

A unified approach further enhances operational efficiency. SOC teams gain comprehensive monitoring capabilities that shatter tool complexity and break down silos, fostering collaboration across teams and processes. Instead of drowning in a sea of alerts from disparate point solutions, analysts can zero in on critical incidents that demand immediate attention. This lays the foundation for streamlined security processes and strengthened team synergy, ultimately fortifying the organization's resilience against cross-domain attacks.

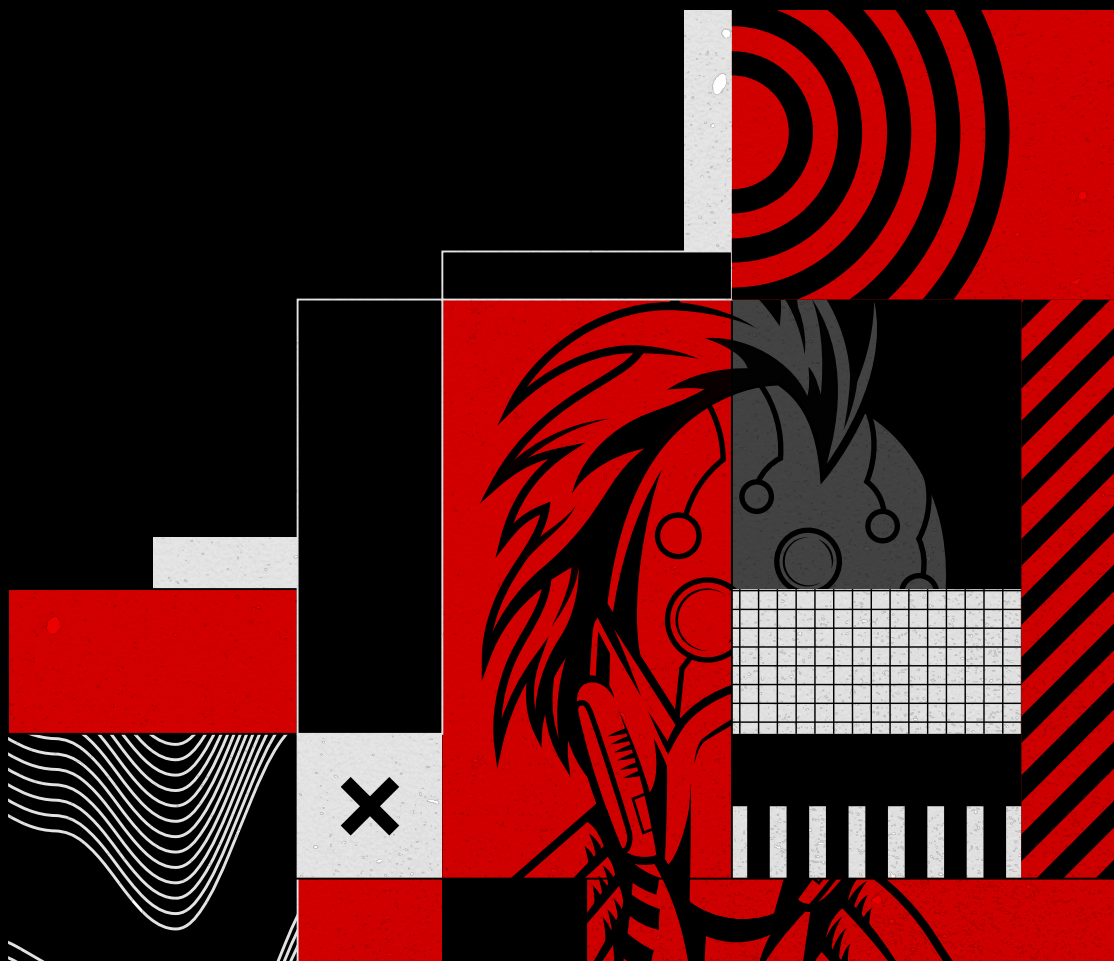


Role of Intelligence-led Threat Hunting

Proactive threat hunting is all about using real-time analysis and intelligence to uncover new attack patterns before they're officially recognized. It's fast, smart and relentless — catching those hidden threats before they even have a chance to make a move.

Rather than focusing solely on known indicators of compromise (IOCs), intelligence-led threat hunting emphasizes understanding adversary behavior — such as the stealthy tactics, techniques and procedures (TTPs) used by cross-domain adversaries.

Using TTPs and behavioral markers, threat hunters can expertly identify patterns and behaviors to proactively detect and intercept adversaries in ways that static defenses simply cannot. By staying alert to how attackers operate across domains, they can identify new threat signals and proactively stop adversaries in their tracks.



Hunting Never-Seen-Before Attacks

In today's SOC environment, proactive threat hunting is essential yet often overshadowed by reactive measures due to the disjointed nature of siloed security tools. Building an in-house threat hunting team demands a rare mix of advanced skills, cross-domain expertise, 24/7 coverage and easy access to cross-domain data, making it both costly and complex to establish. Even with dedicated teams, many SOCs depend on static threat feeds that can quickly become outdated, hindering true proactive detection. To truly stay ahead of evolving threats, SOCs need a unified, intelligence-driven approach that integrates tools, provides real-time visibility across domains and enables proactive threat detection.

Importance of Intelligence in Threat Hunting

Proactive threat hunting is all about using real-time analysis and intelligence to uncover new attack patterns before they're officially recognized. It's fast, smart and relentless — catching those hidden threats before they even have a chance to make a move.

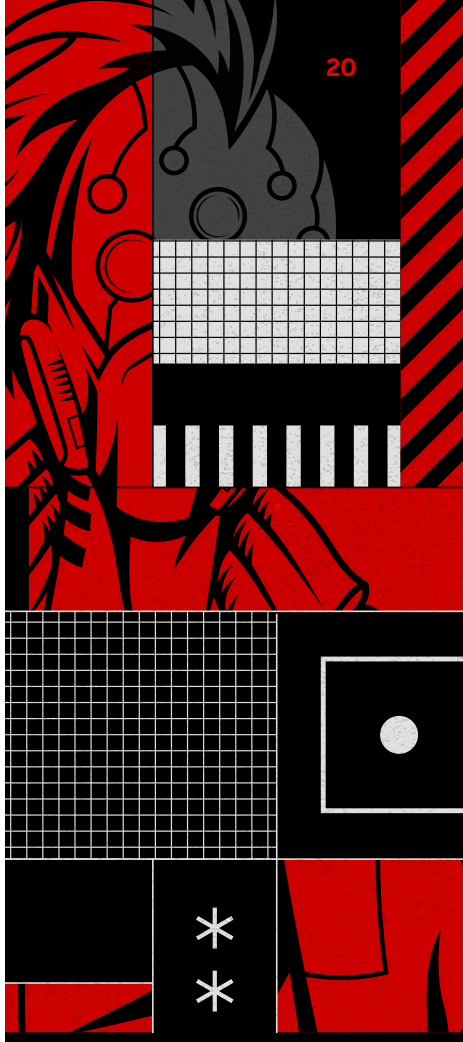
Rather than focusing solely on known indicators of compromise (IOCs), intelligence-led threat hunting emphasizes understanding adversary behavior — such as the stealthy tactics, techniques and procedures (TTPs) used by cross-domain adversaries.

Using TTPs and behavioral markers, threat hunters can expertly identify patterns and behaviors to proactively detect and intercept adversaries in ways that static defenses simply cannot. By staying alert to how attackers operate across domains, they can identify new threat signals and proactively stop adversaries in their tracks.

Always-On Threat Hunting with 24/7 Monitoring

Implementing round-the-clock threat hunting, powered by artificial intelligence, strengthens an organization's ability to detect and disrupt sophisticated attacks, including stealthy cross-domain attacks. Constant monitoring ensures emerging threats are identified early, enabling proactive defenses that minimize the risk of breaches.

With a dedicated team monitoring threats 24/7, they can proactively identify emerging attack patterns and leverage AI-driven analytics to discern not only known threats but also novel attack strategies. This relentless vigilance ensures defenses remain one step ahead of adversaries.



"Cross-domain threat hunting is essential, proactively piecing together identity, cloud, and endpoint telemetry to uncover adversaries who might otherwise remain hidden for months, moving laterally and escalating privileges to achieve their objectives."

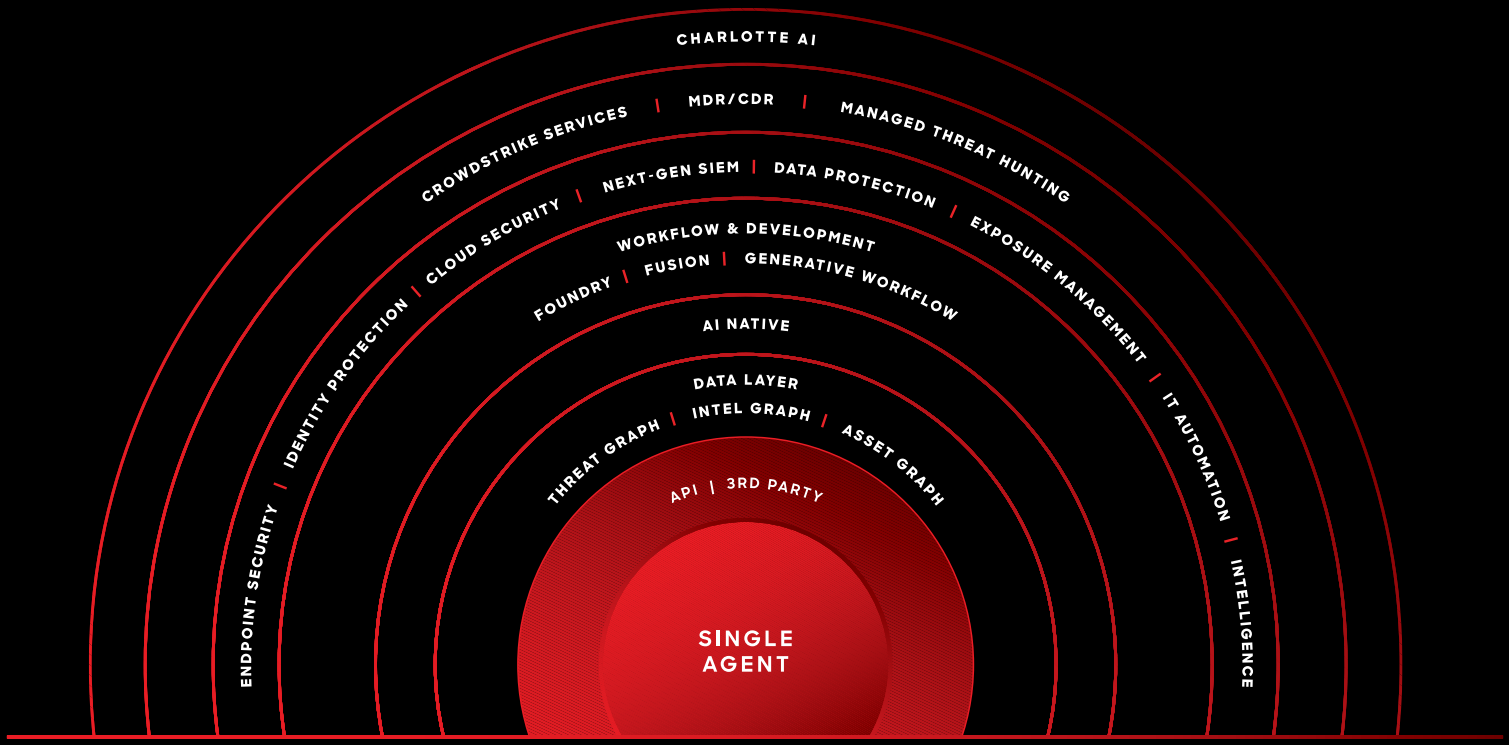
Adam Meyers

SVP of Counter Adversary Operations, CrowdStrike

How CrowdStrike Powers a Unified Defense Against Cross-Domain Attacks

CrowdStrike reimagines security operations with an AI-powered, cloud-native platform that delivers cutting-edge protection against cross-domain attacks. The CrowdStrike Falcon® platform unifies endpoint security, identity protection and cloud security, which is further enriched with world-class threat intelligence and 24/7 managed threat hunting to stop adversaries in their tracks. This ensures customers are protected with unified, proactive defenses that adapt to even the most sophisticated adversaries.

The powerful Falcon platform not only enhances your organization's defense but also delivers substantial benefits that simplify your security operations by unifying CrowdStrike's industry-leading solutions in one place — ensuring proactive, cross-domain threat protection without added complexity.



Essential Capabilities of the Falcon Platform

Endpoint

CrowdStrike Falcon® endpoint security delivers comprehensive, AI-powered protection, detection and response with a single, lightweight agent, offering ull visibility, control and intelligence-driven insights to secure diverse endpoint environments.

Identity

CrowdStrike Falcon® Identity Protection detects and intercepts identity-based threats in real time across hybrid environments, unifying threat detection into a single platform to strengthen security and simplify operations with seamless identity security posture management (ISPM) integration.

Cloud

CrowdStrike Falcon® Cloud Security delivers unified visibility and blocks threats across cloud infrastructure, applications, data and AI models, delivering unmatched contextual visibility and breach prevention from code to cloud.

Next-Gen SIEM

CrowdStrike Falcon® Next-Gen SIEM integrates third-party data to provide broad visibility across siloed environments, consolidating telemetry from email, web, network logs and more. This unified view enables SOCs to track and address threats across multiple entry points for comprehensive security.

SaaS Security

Adaptive Shield, a CrowdStrike company, provides continuous monitoring and automated remediation to ensure SaaS applications are securely configured and compliant, protecting organizations from misconfigurations and security gaps.

Threat Hunting and Intelligence

CrowdStrike Falcon® Adversary OverWatch™ is a managed threat hunting service that combines 24/7 coverage, industry-leading threat intelligence and unrivaled human expertise to proactively detect and disrupt sophisticated cyber threats across domains.

Bringing industry-leading security solutions together for a supercharged defense against cross-domain attacks

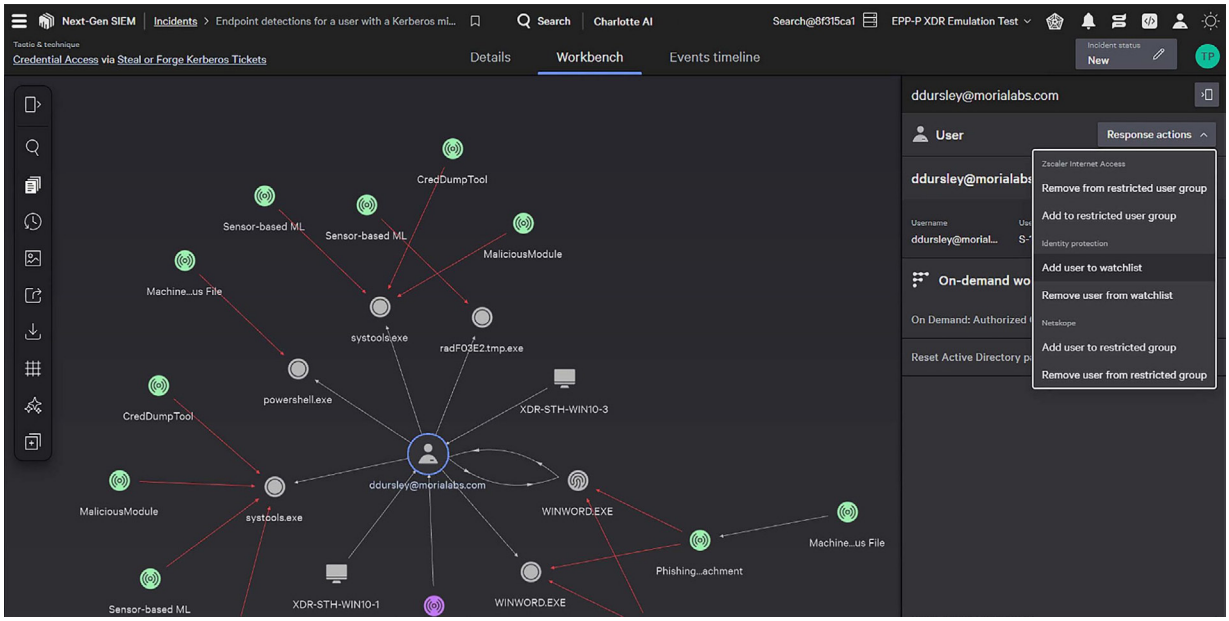


Figure 1.
The Incident Workbench view accelerates investigation and response times with a real-time user experience that maps out the full scope of cross-domain incidents for quick inspection and easy collaboration. Add and remove hosts and files to a shared incident graph, create annotations and overlay first- or third-party data.

Get comprehensive, real-time insight with unified threat visibility across multiple domains

- **Unified view of threats**
  The The CrowdStrike Falcon® platform provides provides a comprehensive, unified view of stealthy threats across multiple domains such as endpoint, identity and cloud, enabling organizations to detect and stop sophisticated adversaries across their entire attack surface.

- **Unified hybrid identity and cloud security**

  - The powerful combination of Adaptive Shield — CrowdStrike's recent acquisition — and CrowdStrike Falcon® Identity Protection will provide comprehensive identity protection across SaaS, on-premises Active Directory and cloud-based environments (e.g., Okta and Microsoft Entra ID).

  - CrowdStrike Falcon® Cloud Security customers will also gain unified visibility and protection across the entire modern cloud estate — infrastructure, custom applications, data, AI models and SaaS applications — all from the same unified console and workflow.

- **Cross-domain threat hunting**
  CrowdStrike's expert threat hunters detect even the most elusive cross-domain threats with speed and precision, delivering real-time, context-rich alerts with actionable recommendations.

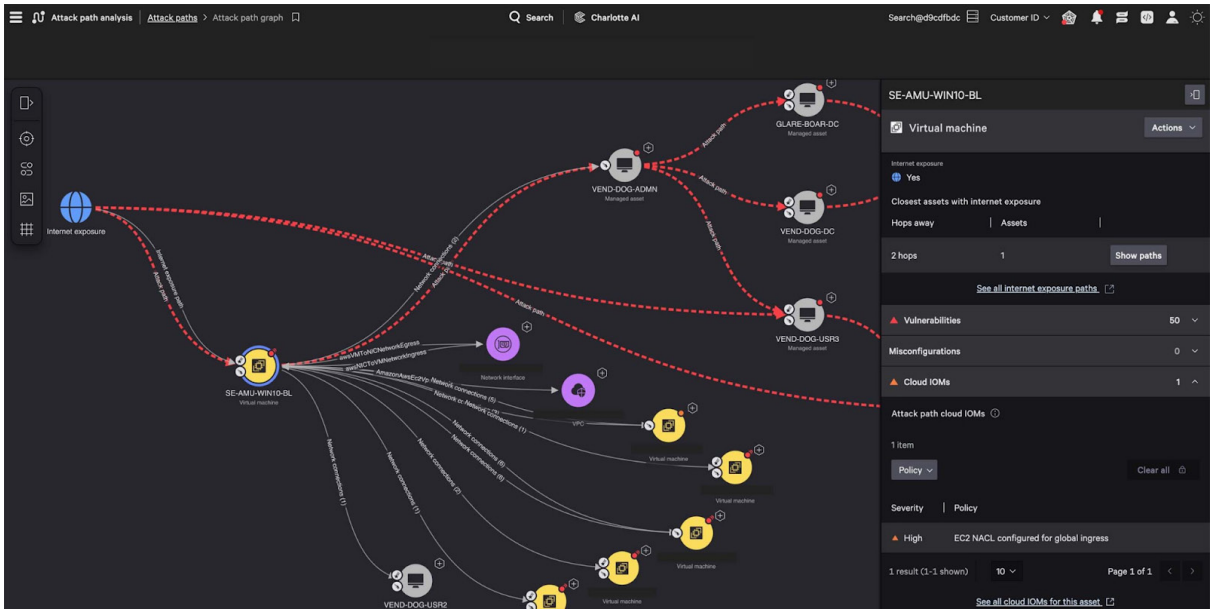


Figure 2.
Gain complete visibility into potential attack paths across on-premises and cloud environments. This comprehensive view helps teams identify and remediate exposures to critical assets, enabling a precise and confident proactive response.

Proactively detect threats and accelerate response times to move faster than the adversary

- **Real-time, context-aware insights for better, faster decision-making**
  Comprehensive attack path visibility and adversary context with integrated, industry-leading threat intelligence and MITRE ATT&CK mappings empower analysts to quickly understand threats and take decisive action.

- **Real-time, automated response**
  Leverage pre-built actions and scripts, as well as CrowdStrike Falcon® Fusion SOAR to quickly automate remediation and response at scale with easy-to-use no-code workflows.

- **Quick insights with CrowdStrike® Charlotte AI, CrowdStrike's generative AI assistant**
  Analysts can instantly access clear incident summaries, expand investigations across domains and decode attacker commands, enabling faster, more informed decision-making and action.

- **Managed threat hunting to rapidly detect previously unseen cross-domain tactics and threats**
  CrowdStrike® Falcon Adversary OverWatch™ threat hunters deliver real-time alerts into advanced and never-seen-before threats. This enables security teams to effectively respond to incidents across domains. These new detections are automatically fed back into the Falcon platform, making it smarter and enabling it to block known threats for all CrowdStrike customers.

Reduce operational complexity by breaking down security silos

- **Streamlined workflows that enhance operational efficiency**
  The Falcon platform provides a real-time, interactive view of incidents and attack paths across domains, enabling security teams to quickly triage, track and analyze incidents within a single console for more effective incident management.

- **Fast and flexible data access**
  The Falcon platform empowers teams with the ability to query comprehensive data across domains — including endpoint, identity and cloud — from a single interface using a shared query language. Unlike traditional SIEMs reliant on third-party data collection, this near-real-time access ensures faster, more consistent insights for timely and accurate threat response.

- **Enhanced collaboration**
  The Falcon platform enables seamless, real-time collaboration for globally distributed security teams, allowing analysts to take notes, assign incidents and control version history — all within the platform — to respond rapidly and collaboratively to threats.

- **Simplified deployment and reduced tool dependency**
  By consolidating various tools into a single platform with one unified agent, the Falcon platform minimizes the maintenance overhead, troubleshooting and complexity associated with managing multiple security tools and agents across systems.

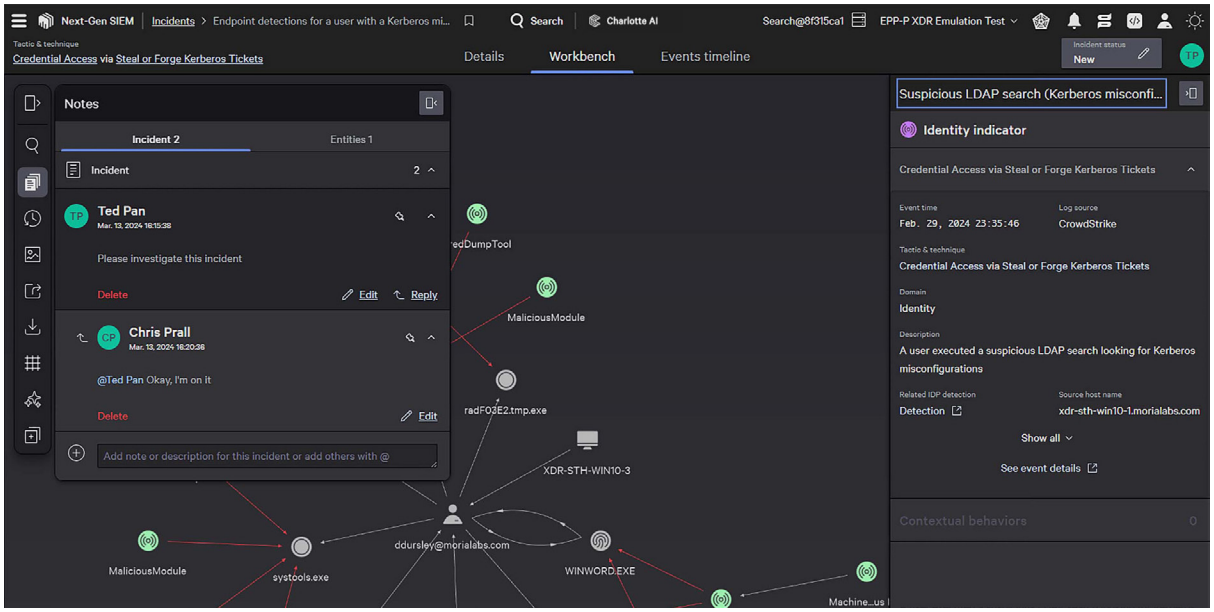


Figure 3.
Security analysts from different locations can view the same incident, share insights and coordinate next steps effectively within the Falcon platform, ensuring a unified and rapid response to threats.

Lower total cost of ownership

- **Maximized security investment with a customized, flexible licensing agreement**
  CrowdStrike Falcon® Flex offers a flexible, usage-based licensing model that allows businesses to scale resources according to their needs, avoiding the expense of over-provisioning or paying for unused licenses.

- **24/7 managed cross-domain threat hunting to reduce personnel costs**
  Get round-the-clock monitoring and expert-led threat hunting without needing to hire, train and retain in-house staff for continuous coverage.

- **Reduction in cybersecurity insurance premiums**
  Meet and exceed stringent security requirements set by insurers. The Falcon platform enables a robust security posture, making it easier to secure favorable coverage terms.

Cross-Domain Threat Hunting

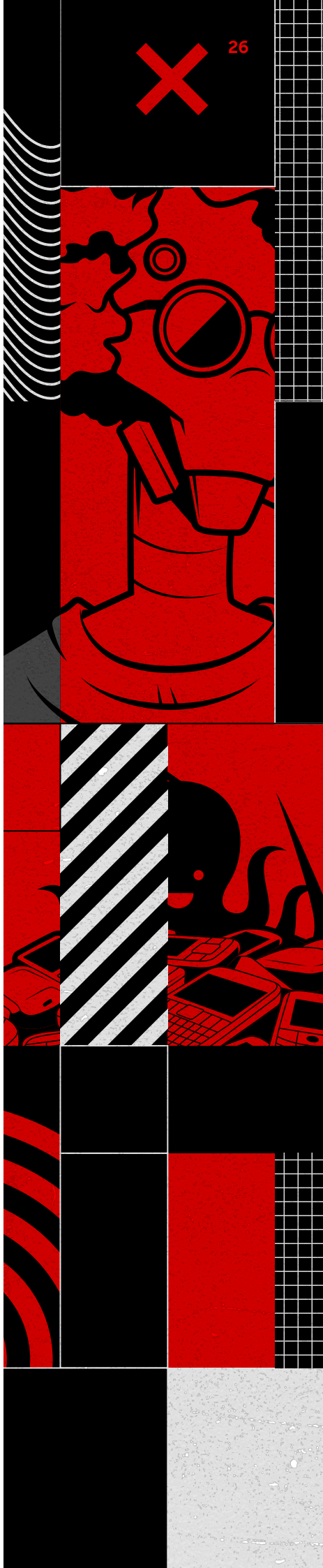
Falcon Adversary OverWatch delivers the world's most complete threat hunting capability to rapidly detect advanced cross-domain threats.

By leveraging industry-first unified visibility across cloud environments, identities and endpoints, CrowdStrike experts operate 24/7 to effectively hunt threats across domains, monitoring for compromised users in cloud attacks and tracking lateral movement between cloud and endpoint.

These threat hunters have access to unprecedented telemetry from not only your environment but from every CrowdStrike customer worldwide. This global visibility gives CrowdStrike the ability to identify patterns and threats that even the most advanced in-house teams cannot replicate. Customers that rely solely on in-house threat hunting lack the breadth and scale of this collective insight, which is crucial for staying ahead of today's sophisticated adversaries.

Falcon Adversary OverWatch breaks down silos to hunt adversaries everywhere, significantly reducing the SOC cost and complexity of in-house threat hunting and accelerating response times. Also, when the threat hunting team identifies a threat, they inform not only the affected customer but other customers who might be at risk, providing detailed data and remediation guidance.

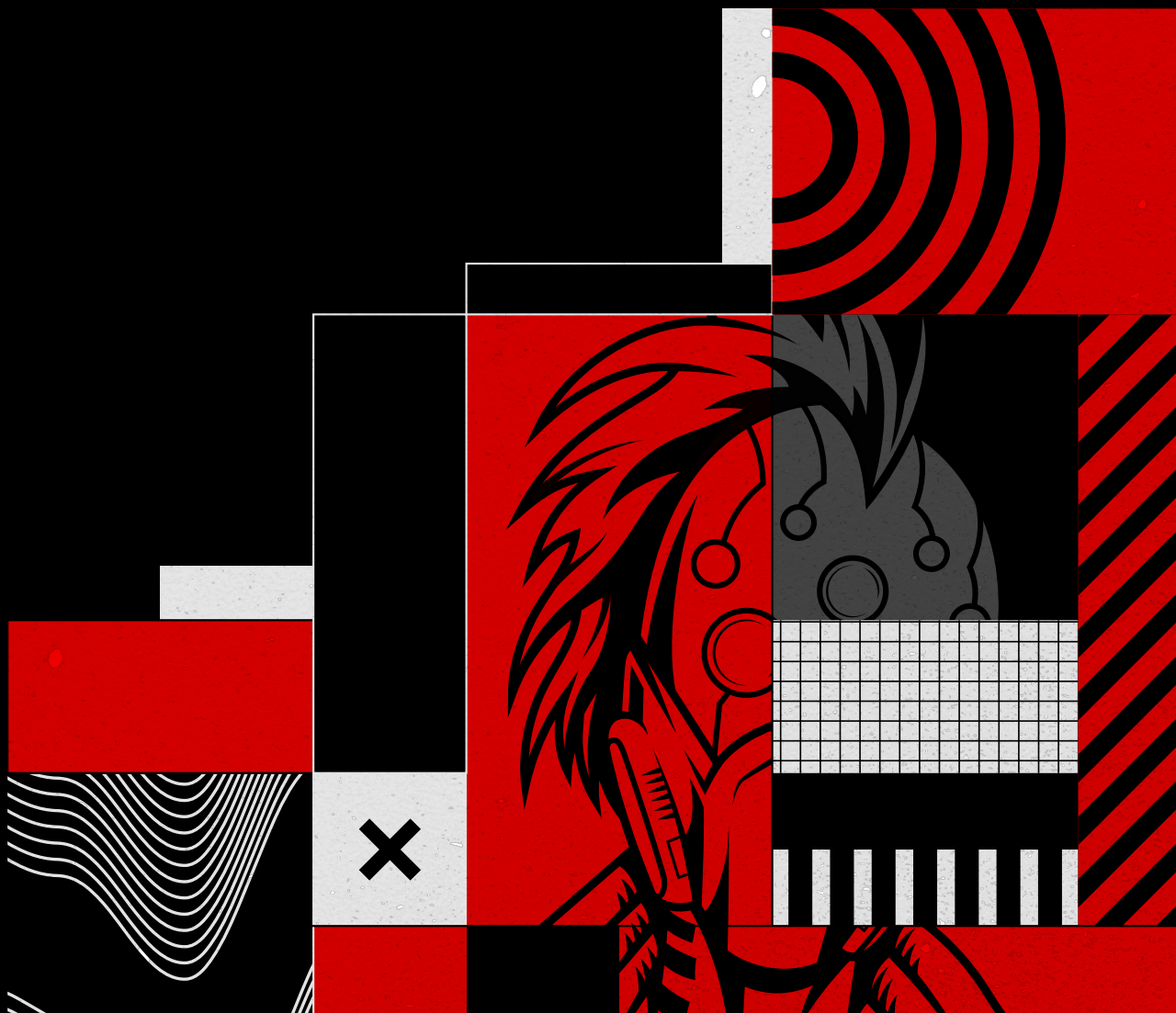
Their diligent work not only bolsters your security posture but also feeds back into the Falcon platform, transforming new threats into known ones. This continuous cycle enhances overall effectiveness, delivering a security framework that's constantly adapting to emerging threats, optimizing threat detection capabilities and ensuring your defenses evolve in tandem with adversary tactics. By integrating real-time insights from these elite threat hunters, SOC teams can adopt a proactive stance, elevating their ability to respond to the ever-innovating cyber threat landscape.



CrowdStrike in Action

For most organizations, today's average breakout time of just 62 minutes presents a razor-thin opportunity to disrupt a cross-domain attack before the adversary digs in. This is precisely where Falcon Adversary OverWatch's state-of-the-art threat hunting team flips the script, closing the gap and turning the tide in the SOC's favor.

To highlight the importance of speed, accuracy and human ingenuity when hunting and countering the adversary at every turn, the following interactive intrusion case study examines an attack by one of the most prevalent and fast-moving eCrime adversaries: PUNK SPIDER. This is a great example of how automatic detections and human-led hunting work together to defeat adversaries at speed and scale.



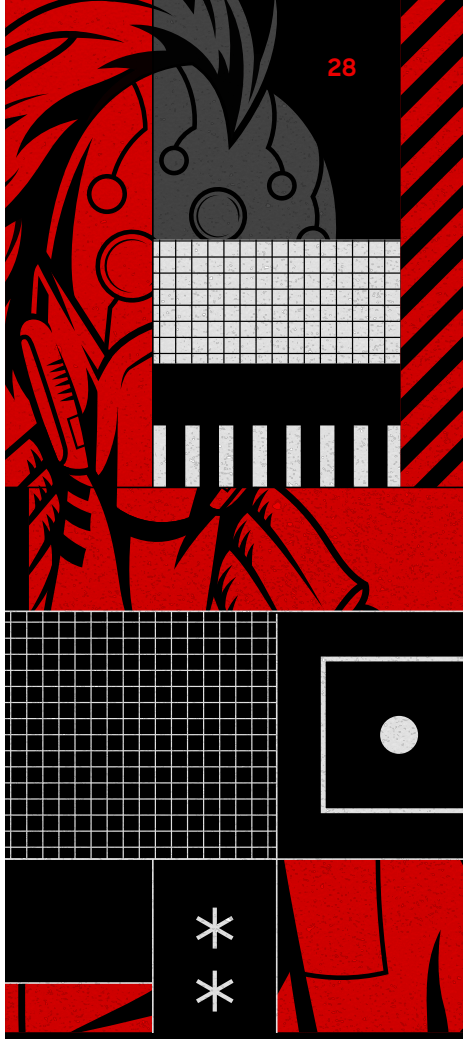
HUNTING PUNK SPIDER

In April 2024, CrowdStrike Counter Adversary Operations identified suspected PUNK SPIDER activity at a North American technology company. Together — supplemented with information from the victim — CrowdStrike identified that PUNK SPIDER had accessed the victim's network environment through an unmanaged[11] Palo Alto Networks GlobalProtect VPN appliance vulnerable to CVE-2024-3400 exploitation. The first evidence of adversary activity was when PUNK SPIDER used a service account to log on to another network host via Remote Desktop Protocol (RDP), causing the Falcon sensor to immediately alert CrowdStrike to potential malicious activity. PUNK SPIDER then attempted to dump credentials and deploy legitimate proxy-tunneling and remote access tools to establish persistence.

The adversary attempted to elevate their privileges by adding compromised and adversary-created user accounts to local administrator groups and the ESX Admins group. PUNK SPIDER commonly uses this technique to gain privileged access to ESXi devices, as members of the ESX Admins group automatically have administrative access to all ESXi devices in the same Active Directory domain. However, the Falcon sensor blocked these privilege escalation attempts. In communication with the victim, CrowdStrike's managed detection and response service, CrowdStrike Falcon® Complete Next-Gen MDR, began containing compromised accounts and devices to prevent PUNK SPIDER from adversely affecting the victim's operations.

PUNK SPIDER attempted to use the open-source reconnaissance tool SharpShares to enumerate network shares — this adversary regularly identifies network shares before exfiltrating data and deploying their proprietary Akira ransomware. When the Falcon sensor prevented this execution, the adversary attempted to use an Antimalware Scan Interface (AMSI) bypass to execute Invoke-ShareFinder.ps1, another network share reconnaissance tool — and the Falcon sensor also prevented this execution. PUNK SPIDER attempted to execute Akira ransomware on compromised devices, and the Falcon sensor prevented the Akira ransomware from encrypting any files.

Running out of time, PUNK SPIDER used WinRAR to collect and archive data and attempted to use FileZilla to exfiltrate the file archives. When countering a known adversary such as PUNK SPIDER, the Falcon Complete Next-Gen MDR team leverages tactical custom IOAs and applies them to the customer environment, which prevented PUNK SPIDER from using FileZilla to exfiltrate data. This case study on defeating PUNK SPIDER highlights how CrowdStrike's automated and human-led threat detections create a powerful framework that enables rapid, scalable defense against adversaries.



Adversaries continue to operate with speed and stealth.

CrowdStrike's powerful combination of the AI-powered Falcon platform and intelligence-led threat hunting helps organizations detect elusive threats and outpace the adversary.

11 An unmanaged device is a device without an installed Falcon sensor.

Conclusion:
Winning the Speed Race Against Adversaries

As businesses embrace innovations like cloud infrastructure, hybrid work environments and interconnected supply chains, they benefit from new efficiencies and expanded capabilities. However, these advancements also bring a level of complexity that creates new openings for cybercriminals.

Adversaries exploit visibility gaps between siloed security tools to orchestrate sophisticated cross-domain attacks, moving laterally across identity, endpoint and cloud domains without detection. These intrusions aren't just opportunistic — they're precise maneuvers designed to bypass the limitations of isolated tools and traditional defenses.

Countering today's sophisticated threats requires a decisive shift: dismantling the silos that isolate security domains. CrowdStrike provides a comprehensive solution that unifies identity, endpoint and cloud security into a cohesive platform. This unified approach fuses real-time threat intelligence with round-the-clock managed threat hunting, providing cross-domain visibility that transcends fragmented security measures. This isn't about simply adding more tools — it's about creating a seamless, adaptive defense architecture where every security layer works in unison.

In an age where adversaries operate with unprecedented speed and stealth, organizations need a security strategy that's as agile and proactive as the threats they face. The CrowdStrike Falcon platform provides that advantage, transforming the way security teams detect and dismantle cross-domain attacks. This unified approach is a decisive move toward staying ahead and thriving in a landscape where agility and foresight are paramount.

Ready to turn the tide against cross-domain attacks?

Get in touch with us to discover how to better protect your business against today's sophisticated threats with our unified platform.

Learn More

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, 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.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: www.crowdstrike.com

Follow us: Blog | X | LinkedIn | Facebook | Instagram

Start a free trial today: www.crowdstrike.com/free-trial-guide