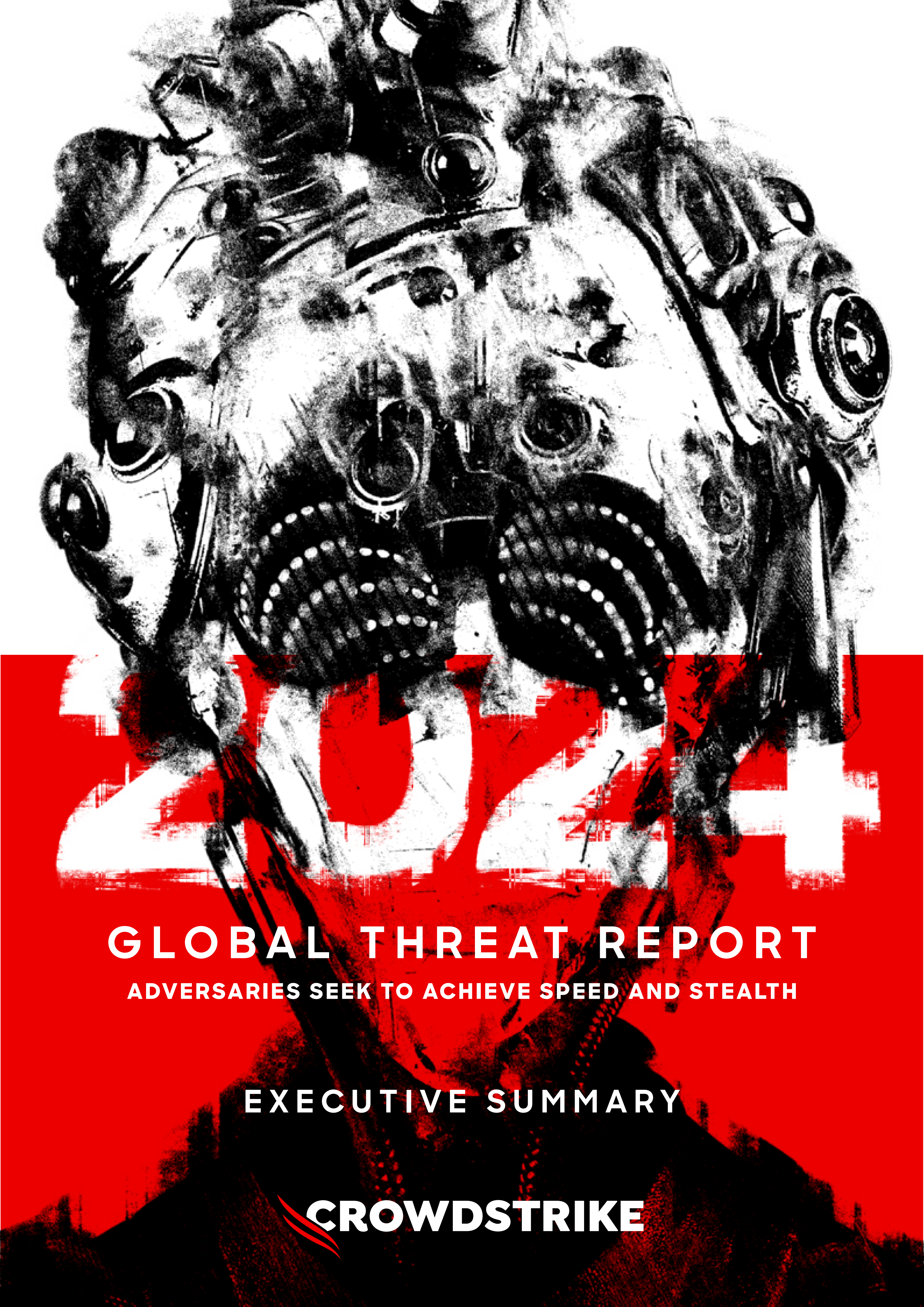
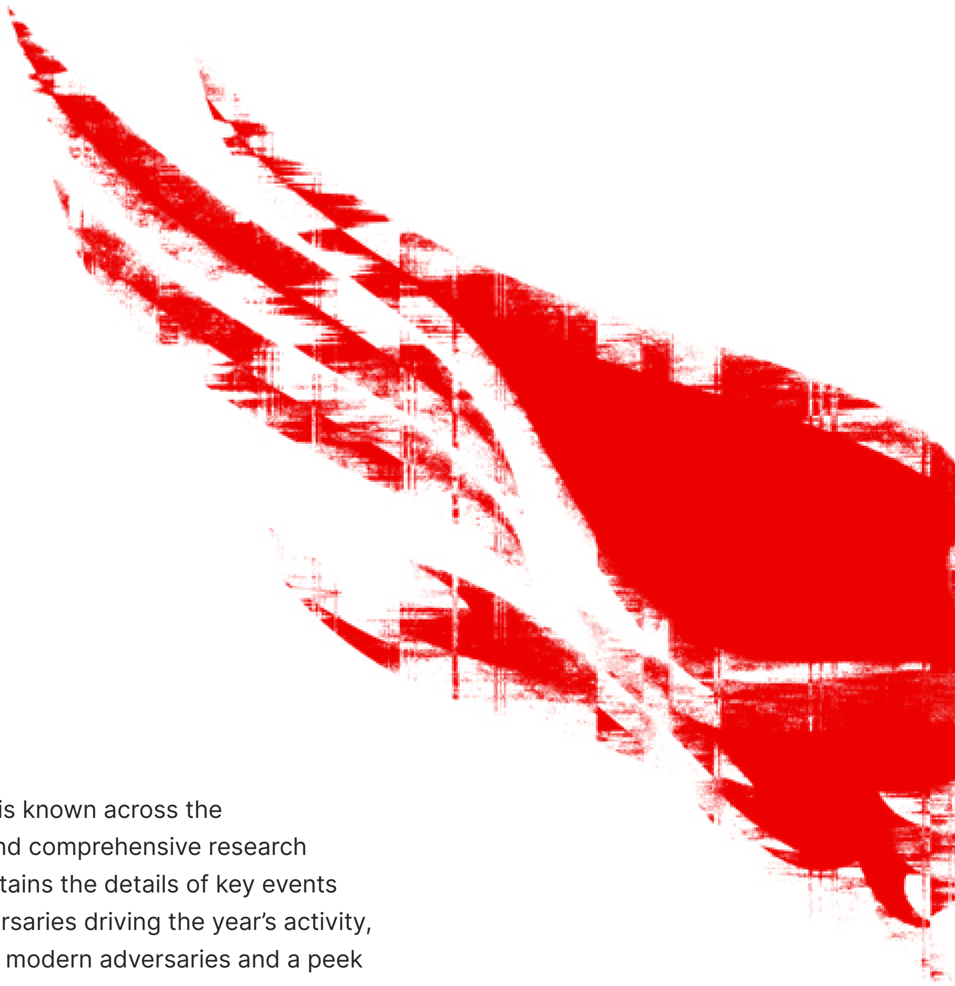


GLOBAL THREAT REPORT

ADVERSARIES SEEK TO ACHIEVE SPEED AND STEALTH

EXECUTIVE SUMMARY

CROWDSTRIKE



The CrowdStrike Global Threat Report is known across the cybersecurity industry for its trusted and comprehensive research on the modern threat landscape. It contains the details of key events and trends that shaped 2023, the adversaries driving the year's activity, key guidance for organizations fighting modern adversaries and a peek at the events we're anticipating in the year ahead.

To defeat today's adversaries, you must first know what you're up against. Cybersecurity is constantly changing as technological innovations disrupt industries and adversaries shift their techniques to become faster, stealthier and more effective. The CrowdStrike 2024 Global Threat Report takes a look back at 2023 so organizations can prepare for the year to come. Learning the details of past events can inform a stronger understanding of what adversaries are after, who they're targeting and how they work.

In 2023, CrowdStrike Falcon® Intelligence and CrowdStrike® Falcon OverWatch® merged to become CrowdStrike Counter Adversary Operations (CAO), combining the power of threat intelligence with the speed of dedicated hunting teams and trillions of telemetry events from the AI-native CrowdStrike Falcon® platform. This year's Global Threat Report was developed based on the firsthand observations of this elite team.

This summary is an overview of the report's key findings, which detail important information on what security teams need to know — and do — in an increasingly complex threat landscape.

THREAT LANDSCAPE OVERVIEW

- **Adversaries are gaining speed:** The average eCrime breakout time in 2023 was 62 minutes, and the fastest recorded breakout time was 2 minutes and 7 seconds. In a typical attack observed by CrowdStrike, more than 88% of attack time was dedicated to gaining initial access — and adversaries are working to cut down on this. Once inside, it took only 31 seconds for a threat actor to drop an initial discovery tool.

- **Interactive intrusions are accelerating:** Hands-on-keyboard activity increased by 60% in 2023 compared to 2022. In the second half of 2023, the increase rose to 73% compared to the same time period one year earlier. Three-quarters of attacks to gain initial access were malware-free, up from 71% in 2022, underscoring adversaries' shift to faster and more effective techniques.

- **Cloud is an evolving battleground:** As organizations move their operations to the cloud, adversaries continue to develop cloud expertise. Cloud intrusions increased by 75% in 2023, and cloud-conscious cases spiked by 110%.

- **Data-theft extortion aids monetization:** CrowdStrike observed a 76% increase in the number of victims named on big game hunting (BGH) dedicated leak sites, demonstrating the status of BGH as the most significant eCrime threat to organizations spanning regions and industries.

KEY THEMES

Identity-Based and Social Engineering Attacks

Adversaries spanning multiple regions and motivations continue to use phishing techniques spoofing legitimate users to target valid accounts, along with other authentication and identifying data, to conduct their attacks.

- In addition to stealing account credentials, CrowdStrike CAO observed adversaries targeting API keys and secrets, session cookies and tokens, one-time passwords and Kerberos tickets throughout 2023.

- These attacks are common among nation-state adversaries and eCrime actors alike. On the nation-state front, FANCY BEAR conducted regular credential collection campaigns throughout 2023. In credential phishing campaigns, they developed a custom toolkit to capture credentials from Yahoo! Mail and ukr.net webmail users. COZY BEAR conducted credential phishing campaigns using Microsoft Teams messages to solicit multifactor authentication (MFA) tokens for Microsoft 365 accounts.
- Identity-based techniques are also core to SCATTERED SPIDER's tradecraft: Throughout 2023, the adversary conducted sophisticated social engineering attacks to access victim accounts.

Adversaries Continue to Develop Cloud-Consciousness

As predicted, the cloud continued to prove an evolving battleground for adversary activity in 2023. CrowdStrike CAO observed a 110% increase in cloud-conscious cases — in which adversaries are aware they have breached a cloud environment and use this access to abuse the cloud service — and a 60% increase in cloud-agnostic cases. Threat actors involved in cloud-agnostic cases are not aware they compromised a cloud environment or did not take advantage of cloud-specific features.

- SCATTERED SPIDER predominantly drove the increases in cloud-conscious activity throughout 2023, accounting for 29% of total cases. The adversary demonstrated progressive and sophisticated tradecraft within targeted cloud environments to maintain persistence, obtain credentials, move laterally and exfiltrate data.
- eCrime adversaries were especially active in targeting cloud environments: 84% of cloud-conscious intrusions attributed to adversaries were conducted by likely eCrime actors.
- Adversaries' preference for identity-based techniques is evident in their cloud-focused attacks. They often use valid credentials to achieve initial access to cloud environments, achieve persistence at the identity level and escalate privileges by obtaining access to additional identities.

Third-Party Relationship Exploitation

Targeted intrusion actors consistently attempted to exploit trusted relationships to gain initial access to organizations throughout 2023. This type of attack takes advantage of vendor-client relationships to deploy malicious tools using two key techniques: One involves compromising the software supply chain using trusted software to distribute malicious tooling; the other involves leveraging access to vendors supplying IT services.

- Adversaries targeting third-party relationships are motivated by the potential return on investment: One compromised organization can lead to hundreds or thousands of follow-on targets.
- In 2023, China-nexus adversaries increasingly targeted third-party relationships to deploy malicious implants and gain initial access. JACKPOT PANDA and CASCADE PANDA consistently exploited trusted relationships via supply chain compromises and actor-on-the-side or actor-in-the-middle attacks.
- North Korea also demonstrated a growing interest in exploiting trusted relationships in 2023: LABYRINTH CHOLLIMA in particular abused a trusted relationship between a technology vendor and client in three cases last year.

Vulnerability Landscape: “Under the Radar” Exploitation

Adversaries have adapted to the improved visibility of traditional endpoint detection and response (EDR) sensors by altering their exploitation tactics for initial access and lateral movement. Now, they are targeting the network periphery, where defender visibility is reduced by the possibility that endpoints may lack EDR sensors or can’t support sensor deployment.

- Unmanaged network appliances, particularly edge gateway devices, remained the most routinely observed initial access vector for exploitation in 2023.
- Threat actors are developing exploits for end-of-life products that cannot be patched and often don’t allow for modern sensor deployment. Unsupported operating system servers and legacy gateway appliances offer easy access — even to older malware families — leading to lingering infections.

2023 Israel-Hamas Conflict: Cyber Operations Focus on Disruption and Influence

CrowdStrike CAO has tracked ongoing cyber operations from targeted intrusion and hacktivist actors since the start of the 2023 Israel-Hamas conflict. Activity and claims from both types of threat actors primarily focus on targeting operational technology or other critical systems — likely to psychologically influence target populations — and deploying destructive wipers against Israeli or Israel-linked entities.

- CrowdStrike CAO tracks multiple adversaries associated with the Hamas militant group; however, activity attributed to these adversaries has not been observed in connection with the Israel-Hamas conflict to date. This is likely due to unavailable resources or the degradation of internet and electricity-distribution infrastructure in the conflict zone.

- RENEGADE JACKAL was the most active Hamas-nexus adversary throughout 2023. CrowdStrike CAO-assessed, likely Gaza-based adversaries EXTREME JACKAL and RENEGADE JACKAL show support for strategic Hamas interests.

- Hacktivist activity will almost certainly continue apace with fluctuations in related geopolitical developments. This assessment is made with high confidence based on the activity patterns exhibited to date.

2024 OUTLOOK

As organizations plan for potential threats emerging in 2024, two potential disruption drivers are top of mind: generative AI and 2024 global government elections.

Generative AI Use in the Threat Landscape

Generative AI has massively democratized computing to improve adversary operations. It can also potentially lower the entry barrier to the threat landscape for less sophisticated threat actors.

Two primary generative AI opportunity areas within the threat landscape include:

- Developing and/or executing malicious computer network operations (CNO), including tool and resource development such as scripts or code that could be functionally malicious if used correctly

- Supporting the efficiency and effectiveness of social engineering and information operations (IO) campaigns

CrowdStrike CAO assesses that generative AI will likely be used for cyber activities in 2024 as it continues to gain popularity. The team will track how threat actors use this technology, and how this use differs from mainstream applications, throughout 2024.

2024 Elections

Individuals from 55 countries representing more than 42% of the global population will participate in presidential, parliamentary and/or general elections. This includes seven of the 10 most populous countries in the world. National-level elections will also occur in countries or groups involved in, or proximal to, major geopolitical conflicts.

The most common malicious activities targeting elections have historically involved information operations likely conducted by state-nexus entities against citizens of countries that hold specific geopolitical interest to the threat actor and simple, short-lived hacktivism — including distributed denial-of-service (DDoS) attacks and website defacements — against state and local government entities. This trend is highly likely to continue in 2024. Countries of interest involved in election cycles will likely be at risk of significant, lengthy IO campaigns from major global powers.

2024's potential to transform geopolitics around the globe for the near future will likely give adversaries numerous opportunities, and a considerable strategic impetus, to target entities involved in electoral processes throughout the coming year.

RECOMMENDATIONS

CrowdStrike offers the following recommendations to help organizations protect their assets and defend against an ever-evolving adversary ecosystem:

Make Identity Protection a Must-Have

Identity-based and social engineering attacks shaped the threat landscape in 2023. To counter these threats, it is essential to implement multifactor authentication and extend it to legacy systems and protocols, educate teams on social engineering and implement technology that can detect and correlate threats across identity, endpoint and cloud environments. Cross-domain visibility and enforcement enables security teams to detect lateral movement, gain full attack path visibility and hunt for malicious use of legitimate tools. Addressing sophisticated access methods such as SIM swapping, MFA bypass and the theft of API keys, session cookies and Kerberos tickets requires continuous hunting for malicious behavior.

Prioritize Cloud-Native Application Protection Platforms (CNAPPs)

Businesses need full cloud visibility to eliminate misconfigurations, vulnerabilities and other threats. Cloud security tools shouldn't exist in isolation, and CNAPPs provide a unified platform that simplifies monitoring, detecting and acting on potential cloud threats and vulnerabilities. Select a CNAPP that includes pre-runtime protection, runtime protection and agentless technology to help you discover and map your applications and APIs running in production, showing you all attack surfaces, threats and critical business risks.

Gain Visibility into the Most Critical Areas of Enterprise Risk

As enterprise environments expand, organizations must understand the relationships between identity, cloud, endpoint and data protection telemetry to identify and block modern attacks. By consolidating point products into a unified security platform, organizations can gain complete visibility in a single view and easily control their operations, improving their ability to discover, identify and stop breaches.

Drive Efficiency

Adversaries are getting faster. Can you keep up? Legacy security information and event management (SIEM) solutions are often too slow, complex and costly, and many were designed for an age when data volumes and adversary sophistication were a fraction of what they are today. Modern businesses need a modern SIEM solution that is faster, easier to deploy and more cost-effective than legacy SIEM tools. Investigate approaches that unify threat detection, investigation and response in a single cloud-delivered, AI-native platform.

Build a Cybersecurity Culture

The end user remains a crucial link in the chain to stop breaches. User awareness programs should be initiated to combat the continued threat of phishing and related social engineering techniques. For security teams, practice makes perfect. Encourage an environment that routinely performs tabletop exercises and red/blue teaming to identify gaps and eliminate weaknesses in your cybersecurity practices and response.

DOWNLOAD THE FULL REPORT

The CrowdStrike 2024 Global Threat Report presents deep analysis that highlights the most significant events and trends in cyber threat activity in 2023. Download a free copy of the report at https://www.crowdstrike.com/global-threat-report/.

Learn more: www.crowdstrike.com

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

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