CROWDSTRIKE

SOC Survival Guide

Defeating modern adversaries with an AI-native SOC

Table of Contents

Modernize Your SOC to Outpace Adversaries

Protectors are in a never-ending race against time to find and shut down threats. Today's adversaries are faster and stealthier than ever, using legitimate tools to carry out lightning-fast, hands-on-keyboard attacks, while staying under the radar.

2'07" **fastest recorded eCrime breakout time in 2023[1]**

But security teams burdened with legacy tools struggle to match the speed of attackers. Security information and event management (SIEM) systems, once heralded as the single solution for incident response, have failed to fulfill their promise. As log volumes and sources proliferate, their poor scalability and high costs prevent teams from collecting and retaining all data in their SIEMs. Patchwork architectures of legacy SIEMs, data lakes and analytics tools have turned security analysts into data wranglers, wasting time pivoting between consoles and manually correlating data rather than attacks.

The complexities of the past impede teams' ability to secure the future. SOCs must transform so their organizations can face the threat landscape of today and tomorrow.

This transformation requires the ability for protectors to collect and analyze more data from more sources at massive scale to see the entire life cycle of an attack. And they need to fuse their data with AI to better understand and correlate data, detect threats and accelerate investigation and response.

In this eBook, we define the vision of the fully realized AI-native SOC and provide insights and strategies on how to begin modernizing so security teams can survive and thrive in today's dynamic environment.

> **As technology evolves, so do the threats. The AI-native SOC is not just about operationalizing new tech internally — it's also about defending against mutating malware, AI-driven phishing and data poisoning. Staying ahead means adapting swiftly to an ever-changing threat landscape.**
>
> **Justin Acquaro**
> CrowdStrike Chief Information Security Officer

1 CrowdStrike 2024 Global Threat Report

MEASURING SUCCESS FOR THE AI-NATIVE SOC

SOC modernization is a journey. Security leaders seeking to measure progress should anchor on tangible outcomes including:

- **Time to detect:** The time required to identify a security incident or threat after it has occurred
- **Time to triage:** How swiftly a security analyst can assess and prioritize incidents amid the sea of alerts to pinpoint the most impactful threats
- **Time to investigate:** The time it takes for a security analyst to understand the environment, get the required context to determine potential security threats before they manifest and make an informed decision to prevent a breach
- **Time to respond and recover:** How quickly threats can be neutralized and systems restored to a known good state so there's minimal disruption to normal business operations

Security leaders should also consider operational costs, including ramp-up time to develop skilled and effective analysts and time to onboard key data in their tooling. By focusing on outcomes, CISOs can steer their organizations toward a more resilient and agile security posture that's better equipped to combat the ever-evolving threat landscape.

Challenges with Legacy SIEMs

Before delving into modern SOC design, it's important to understand the challenges that SOCs face today, particularly with their legacy SIEM solutions. Let's dive into how and why the SIEM is holding teams back and creating an arduous analyst experience.

Slow detection and response times

Stopping modern attacks demands that security operations match adversaries' speed — with the average eCrime breakout dropping to 62 minutes in 2023, a decrease from 84 minutes in 2022.[2] Legacy SIEMs are slow, complex and cumbersome, with searches that take hours and gaps that leave analysts struggling to extract the insights they need for rapid threat detection and response.

Data management overload

Modern environments contain multitudes of security tools, making it costly and complex to "get data in" to a legacy SIEM. Consequently, security engineers must spend excess time and resources to manage data ingestion and maintain complicated architectures of SIEMs, data lakes and detection and response platforms.

Soaring SIEM costs that lead to blind spots

High SIEM costs compound risks by limiting data retention and analysis capabilities. For many organizations, it is cost-prohibitive to log and retain all of the relevant data needed for comprehensive threat detection and response. As a result, the SOC is left with blind spots and misses attacks.

Overburdened SOC Teams

50
security tools used by the SOC, on average[3]

67%
of daily alerts are ignored due to alert fatigue[4]

Slow investigations without context

Every day, analysts sift through hundreds of alerts from disparate sources that are often full of false positives. To get the context they need during investigations, they painstakingly enrich data and perform slow, manual searches within legacy SIEMs, consuming valuable time cycles.

Fragmented response actions

Response actions and automation lack cohesion when dispersed across several disjointed tools. This fragmentation complicates incident response, prolonging adversary dwell time. Analysts grapple with inefficiencies in coordinating response actions, resulting in delayed threat mitigation and heightened repercussions from security incidents.

---

2 CrowdStrike 2024 Global Threat Report

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

4 Vectra, 2023 State of Threat Detection

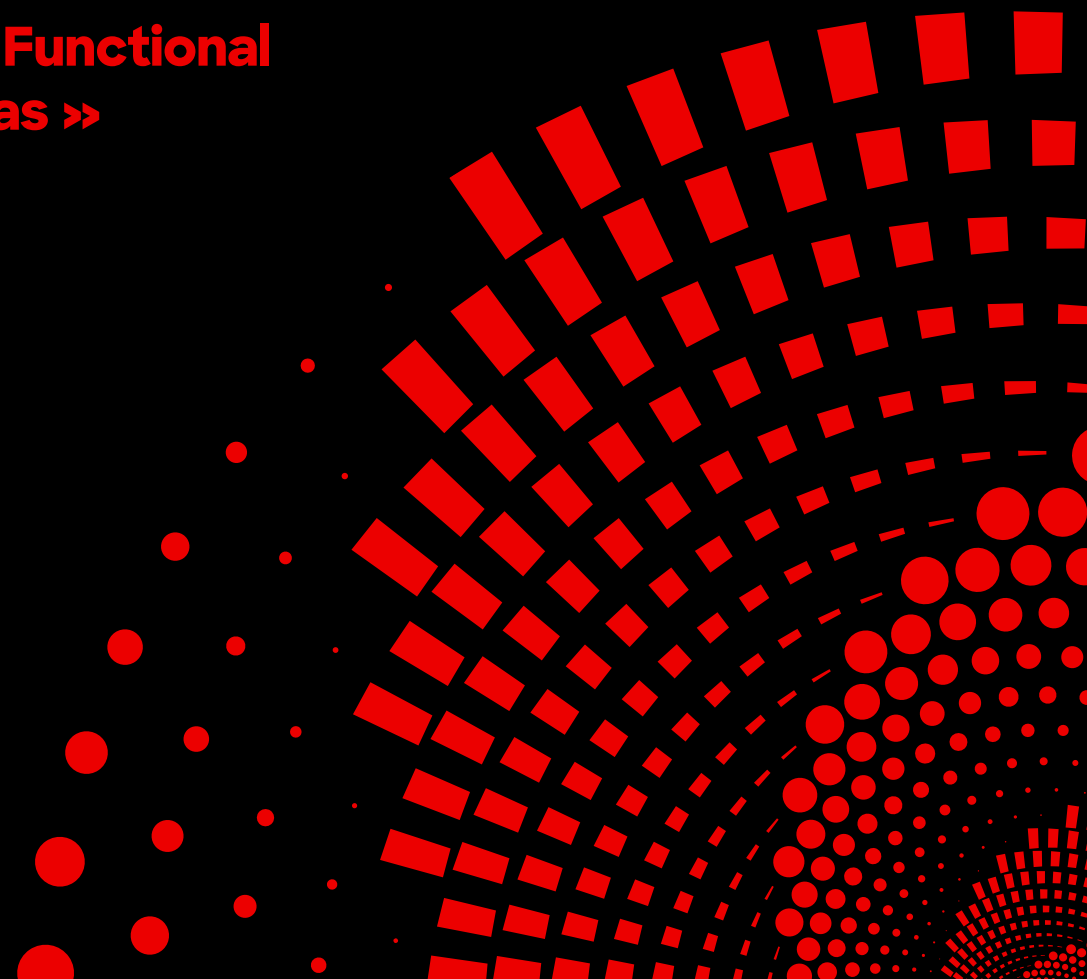
Transform Security Operations with an AI-Native SOC

With the challenges of legacy SIEMs driving the SOC to modernize, where should security leaders direct their strategic focus? The answer lies in the AI-native SOC.

AI-native cybersecurity empowers organizations to use the strengths of modern cloud-native data platforms — along with cutting-edge AI and automation — to analyze vast datasets, detect emerging threats and expedite response. Modernizing security operations with an AI-native platform improves accuracy, efficiency and speed across the threat detection, investigation and response (TDIR) life cycle.

Let's delve into how to transform five key functional areas of security operations.

5 Key Functional Areas »



1 FRICTIONLESS DATA ONBOARDING AND SETUP

Legacy SOC

Data is at the heart of nearly every aspect of security operations, and legacy approaches to data collection fail to effectively scale. Ingesting and centralizing data is a complex process that requires extensive manual work and creates high costs. Due to exploding data volumes, SOCs are pressed to make budget-conscious choices on the data they analyze and develop convoluted architectures with "franken-SIEMs" with multiple data stores and replicators. Unable to analyze all of their data, SOCs are left with security blind spots.

Furthermore, SOC teams must gain context from the data to drive meaningful investigations. Data alone is just raw input. It must be enriched with human intelligence and context from incident response, managed detection and response (MDR) and threat intelligence to make it useful, valuable and high-fidelity enough to be trusted for detections and investigations. Without enriched data with insights from these sources, the SOC will continue to face low-fidelity alerts and false positives that squander analyst time.

AI-Native SOC

The SOC of the future makes deployment effortless with flexible, simple data onboarding options.

Accelerate time-to-value and cut costs with key data already built in

The AI-native SOC collects essential data — endpoint, identity, cloud workload and more — with a unified agent and embeds it natively into one AI-native platform. This data is instantly actionable for modeling, detection, investigation and response — without any additional configuration or deployment. By consolidating on one platform for detection, response, and information and event management, teams can drastically simplify operations while saving on ingestion and retention costs.

Bring in data from any source with prebuilt data connectors

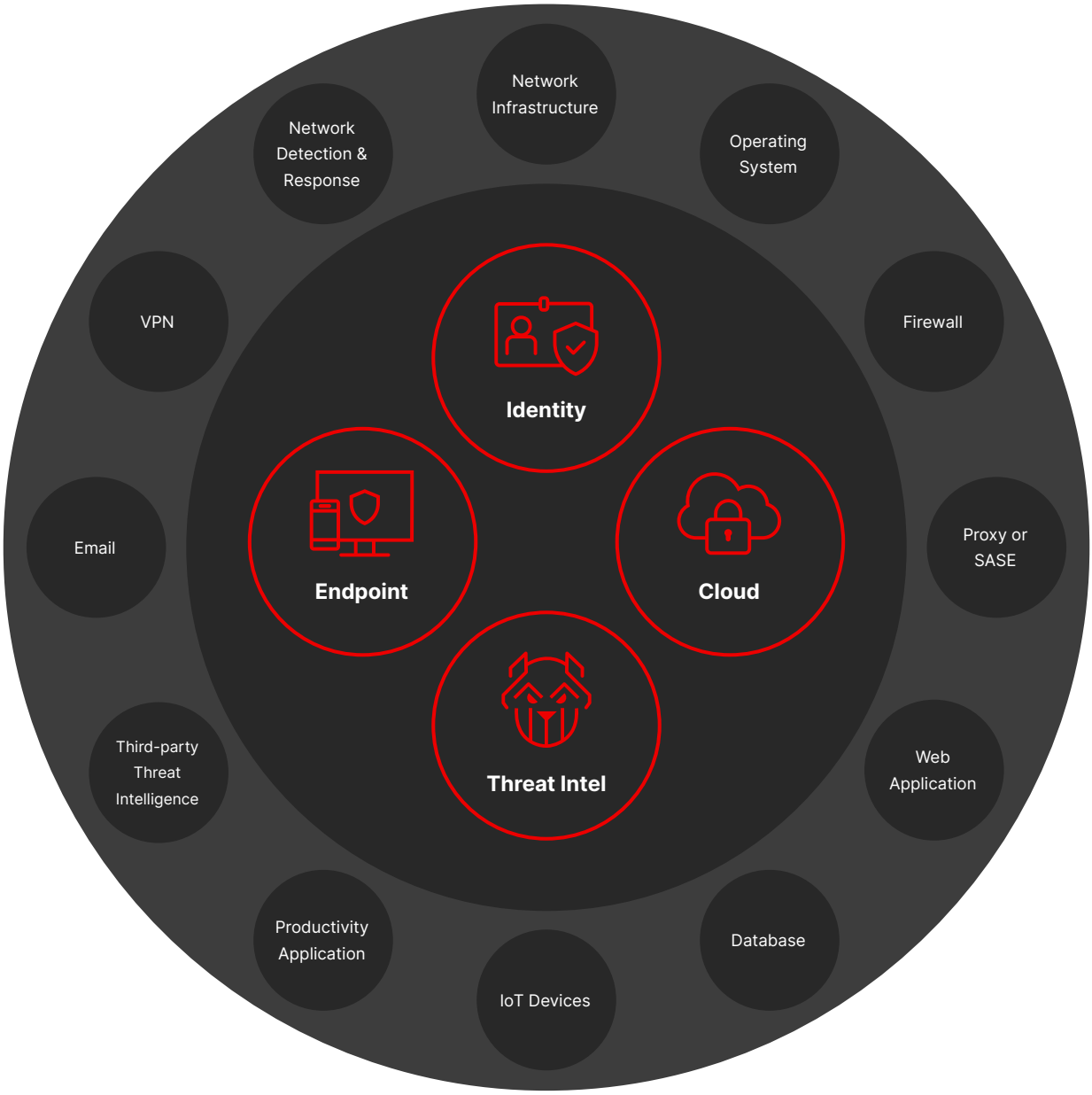
Beyond native data, the modern SOC should prioritize onboarding key data sources, including web, firewall, email security and network traffic. To simplify ingestion, the AI-native SOC uses large language models (LLMs) to effortlessly generate parsers with minimal manual input. This approach extends visibility to diverse data sources by automating key aspects of data processing.

This contemporary data management approach offers simplicity, elegance and efficiency. And by consolidating data origin, use and storage within a scalable platform, it offers significant cost savings.

The AI-native SOC collects essential, unified data that is instantly actionable for modeling, detection, investigation and response.

Strategic Data Onboarding

To ensure success with operationalizing your SIEM, start with key data sources such as endpoint, cloud, identity and threat intelligence. Further extend visibility by onboarding additional data sources from across your environment.



2 ACCURATE AI-POWERED THREAT PREVENTION AND DETECTION

Legacy SOC

Legacy SOCs are inundated with a barrage of alerts. Traditional SIEMs typically offer generic detection rules nonspecific to different data sources and vendors. As a result, they typically generate low-fidelity alerts, forcing detection engineers to update and test rules with painstaking care or craft custom rules tailored to their environment. It's a never-ending cycle of tuning to minimize noisy false positives.

Despite these tuning efforts, security analysts are overwhelmed by the sheer volume of daily alerts — an average of 4,484 alerts per day.[5] Because these alerts are generated by siloed tools, analysts often struggle to see separate indicators as part of the same attack. Effectively detecting threats and triaging this high volume of alerts is simply unfeasible. So despite their best efforts, teams leave up to 67% of alerts unaddressed.[5]

4,484
average alerts per day for security analysts[5]

67%
of alerts go unaddressed by traditional SOCs[5]

AI-Native SOC

The AI-native SOC is built on a cutting-edge architecture that incorporates modern AI models and automation to deliver superior threat prevention, precise detections, faster alert triage and a transformed analyst experience. The AI-native SOC empowers organizations to:

Automatically prevent known and zero-day attacks

The AI-native SOC includes ironclad security controls that block the 99%+ of attacks that can be stopped without human intervention, dramatically reducing the risk of a breach. By combining behavioral protection, threat intelligence, AI models, exploit protection and more, the AI-native SOC accurately blocks attacks targeting critical assets such as endpoints, cloud workloads and identity services, drastically reducing the number of threats to detect and investigate.

Detect threats with laser precision

The AI-native SOC leverages cloud-native machine learning models to build AI-powered detection rules. These models are trained using massive volumes of curated data to predict and protect against emerging classes of threats. Modern security teams further fortify their detections with human expertise from dedicated services teams for incident response, managed detection and response, threat hunting, threat intelligence and more. The AI-native SOC combines AI, the latest adversary intelligence and human expertise to automatically detect new attack techniques and enhance the quality of existing detections, ensuring security teams stay one step ahead of evolving threats.

Group and prioritize alerts for faster triage

Using AI and machine learning models that analyze multiple attributes of an alert, the AI-native SOC seamlessly aggregates events from multiple domains and enriches them with contextual information to intelligently process and prioritize high-fidelity incidents for analysts. AI models can be trained on large volumes of alerts, threat intelligence, and analysis of how past alerts were handled. Intelligent alert grouping into incidents reduces analyst backlog, reducing the risk of missed attacks.

---

5 Vectra, 2023 State of Threat Detection

3 FASTER INVESTIGATIONS FUELED BY A MODERN ANALYST EXPERIENCE

Legacy SOC

Security analysts need efficient tools to swiftly investigate and contain threats. However, in the legacy SOC, accomplishing this involves manually navigating through a maze of siloed security tools. Adding to this inefficient workflow, legacy SOC technologies rely on outdated index-based architectures — think painfully slow searches across individual tools to piece together the context of an attack — adding more complexity for incident investigations.

As data volumes surge, manual investigations become impractical, straining the SOC analyst's most precious resource: time. As a result, investigations lag — 70% of critical issues require more than 12 hours to resolve.[6]

» **70%**

of critical issues require more than 12 hours to resolve.[6]

AI-Native SOC

The AI-native SOC speeds up incident analysis by delivering a modern analyst experience. It unifies investigations on one platform, providing a complete, graphical picture of attacks, facilitating real-time collaboration, and offering prescriptive guidance. AI and automation represent a paradigm shift that empowers the modern SOC to perform investigations in minutes instead of hours.

Reimagine investigations by visualizing incidents in an elegant graph

The AI-native SOC serves as a force multiplier for teams and slashes investigation time. By rapidly processing telemetry data at scale, it can automatically show attack activity, asset relationships and threat context in a clear visual graph for all incidents. This graphical representation helps analysts understand the scope and impact of an attack as well as adversaries' techniques and motivations. A timeline view displays the sequence of events across data sources so analysts can make rapid, informed decisions. Analysts can pivot to event searches and adversary dossiers, execute workflows, enrich entities and download incident reports in one or two clicks. By bringing together everything that's needed for incident analysis in one place, and avoiding the need to manually construct the adversary's attack path and timeline, the AI-native SOC helps teams expedite response and ultimately stop the breach.

» **AI and automation empower the modern SOC to perform investigations in minutes instead of hours.**

6 CrowdStrike 2024 State of Application Security Report

Drive faster response with real-time collaboration

Security analysts can share critical information, coordinate tasks and assess findings with real-time collaboration. Instant notifications inform team members of new updates. Analysts can bring unique perspectives and expertise, enhancing decision-making and reducing the risk that crucial details are overlooked. Discussions are automatically saved with the incident, aiding post-incident reviews and audits.

Transform every user into a power user with GenAI

The AI-native SOC accelerates security operations and reclaims the edge against adversaries with generative AI (GenAI). New security analysts can ramp up quickly because GenAI reduces the technical bar to complete complex tasks. GenAI eliminates the need for deep knowledge of query syntax, enabling analysts to ask questions in plain language and receive accurate query translations. It also shows analysts the complete scope of an incident by looking across all platform data to suggest additional related indicators to append to the case, such as additional hosts. By producing incident summaries, it not only streamlines documentation processes but saves hours of time for every investigation.

> **The evolution to an AI-powered SOC isn't just about deploying advanced technology, it's about revolutionizing the analyst experience. By harnessing AI to streamline data ingestion, incident correlation and investigation, the AI-native SOC isn't just transforming security operations but redefining how analysts interact with data to thwart threats.**

Elia Zaitsev
CrowdStrike Chief Technology Officer

4 EFFORTLESS AUTOMATION FOR EVERYONE

Legacy SOC

Today's SOC teams are bogged down by slow, manual processes, delaying incident response and increasing the risk of a devastating breach. Although automation has long promised to speed up response, security teams must invest inordinate time and resources to build security orchestration, automation and response (SOAR) playbooks. Developing playbooks demands not only programming skills but a thorough understanding of security operations and threat scenarios.

Moreover, the need to coordinate actions across various tools leads to "swivel chair syndrome." This issue not only delays incident resolution but causes inconsistencies, further slowing down the team's ability to proactively monitor threats. This prolonged dwell time can be demoralizing for security operations teams, where swift response times are crucial indicators of a SOC's effectiveness.

AI-Native SOC

Speed up incident response with workflow automation

The AI-native SOC delivers on its promise to speed up incident response by automating cumbersome and manual remediation workflows. Using GenAI, security engineers can create playbooks in seconds by describing workflows in plain language instead of spending weeks on development. A modern user interface and drag-and-drop experience lets security engineers review and adjust playbooks with ease. Extensive libraries of prebuilt playbooks, integrations and actions can automate any security or IT use case.

The AI-native SOC delivers on its promise to speed up incident response with automation.

No-code workflow automation streamlines tedious tasks and frees up analyst time for high-value work and high-risk threats. It can codify investigation and response processes to standardize best practices, increase analyst confidence, and achieve accurate and consistent outcomes. Prebuilt workflows can fast-track investigations by enriching, correlating and managing alerts and incidents and expedite threat hunting by querying data and visualizing results. Instead of deploying a few playbooks, the AI-native SOC empowers teams to build numerous workflows to automate everything, boosting SOC efficiency.

Stop threats decisively with closed-loop response

An AI-native SOC can drive any response action through tight integration with endpoint, identity and cloud controls. Built-in automation in an AI-native SOC platform allows analysts to quickly implement wide-reaching actions across third-party tools in real time, going beyond reacting to incidents and proactively protecting the whole network. Additionally, the seamless integration of identity management makes security workflows more efficient, enabling automatic, risk-based access controls.

By adapting to ever-changing threats, the AI-native SOC learns from past incidents and recommends specific, tailored remediation actions. This ongoing evolution prepares the security team to skillfully navigate new demands for automation and response that arise over time.

5 INTELLIGENCE-LED THREAT HUNTING

Legacy SOC

Given the manual and resource-intensive processes required for investigations, threat hunting in today's SOC often takes a backseat to reactive measures. Limited time, skills and resources constrain teams from conducting critical tasks like in-depth threat research, developing queries and managing lists of indicators of compromise (IOCs). Even for teams that have the bandwidth for proactive threat hunting, many rely on static listings from threat intelligence feeds that quickly become outdated.

AI-Native SOC

An AI-native SOC empowers security teams to regain control of proactive threat hunting. By harnessing the power of artificial intelligence, threat hunting libraries and optimized workflows, these platforms provide crucial assistance to overwhelmed teams.

An AI-native SOC solution empowers security teams to regain control of proactive threat hunting.

Gain the upper hand against threats with adversary intelligence

The AI-native SOC leverages rich adversary intelligence built on proprietary datasets and underground sources to hunt down advanced adversaries. Curated libraries of threat hunting queries empower analysts to automatically uncover hidden and emerging threats based on the latest adversary tactics. Integrated workflows allow SOC users to operationalize threat hunts in seconds, immediately elevating the productivity of the entire SOC team while accelerating its ability to continuously adjust security controls as threats evolve. Teams can swiftly identify and neutralize potential risks without expending precious time and resources on upfront threat research or query development.

Find threats swiftly with high-speed search

Threat hunters must scour through mounds of data quickly to unearth threats. The AI-native SOC delivers the speed, scale and querying flexibility required to proactively search for and find indicators of attack. Threat hunters can optimize their searches and quickly pinpoint threats with a flexible query language that supports regular expressions and a variety of functions. Plus, they can easily query any field with free-text search.

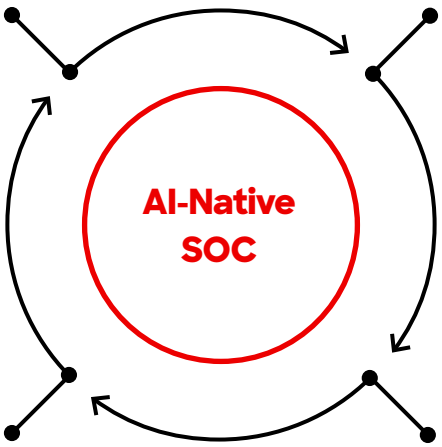
Augment with threat hunting services

In the absence of in-house resources, organizations can augment their internal capabilities by tapping into external services offered by cybersecurity experts. These experts can perform proactive threat hunting activities that deliver invaluable insights and adversary intelligence from real-world attacks. This allows SOC teams to focus their efforts on strategic initiatives and better strengthen their security posture.

The AI-Native SOC Powers World-Class Services

By bringing together all data, AI, workflow automation and threat intelligence in one unified platform, the AI-native SOC offers a robust foundation for services. Security teams achieve full visibility across their entire environment, and, using automation and generative AI, they can operate much more efficiently. The AI-native SOC allows teams to shift from "survival mode," where they struggle to keep up with a constant onslaught of attacks, to a strategic approach, where they can prepare for threats, fortify their cybersecurity posture and respond swiftly to attacks.

An AI-native SOC seamlessly leverages collaborative partners and value-added services like red team exercises, risk assessments, MDR, incident response (IR) and more.



Prepare
Equip and train your organization to defend against adversaries with real-life simulation exercises, red team evaluations and penetration tests.

Fortify
Enhance your cybersecurity controls and practices with risk assessments and actionable recommendations.

Respond
Let incident response experts help you stop breaches, investigate incidents and recover from attacks with speed and precision.

Manage
Get round-the-clock expertise and active, hands-on remediation tailored to your environment, so you can rest easy knowing you're protected.

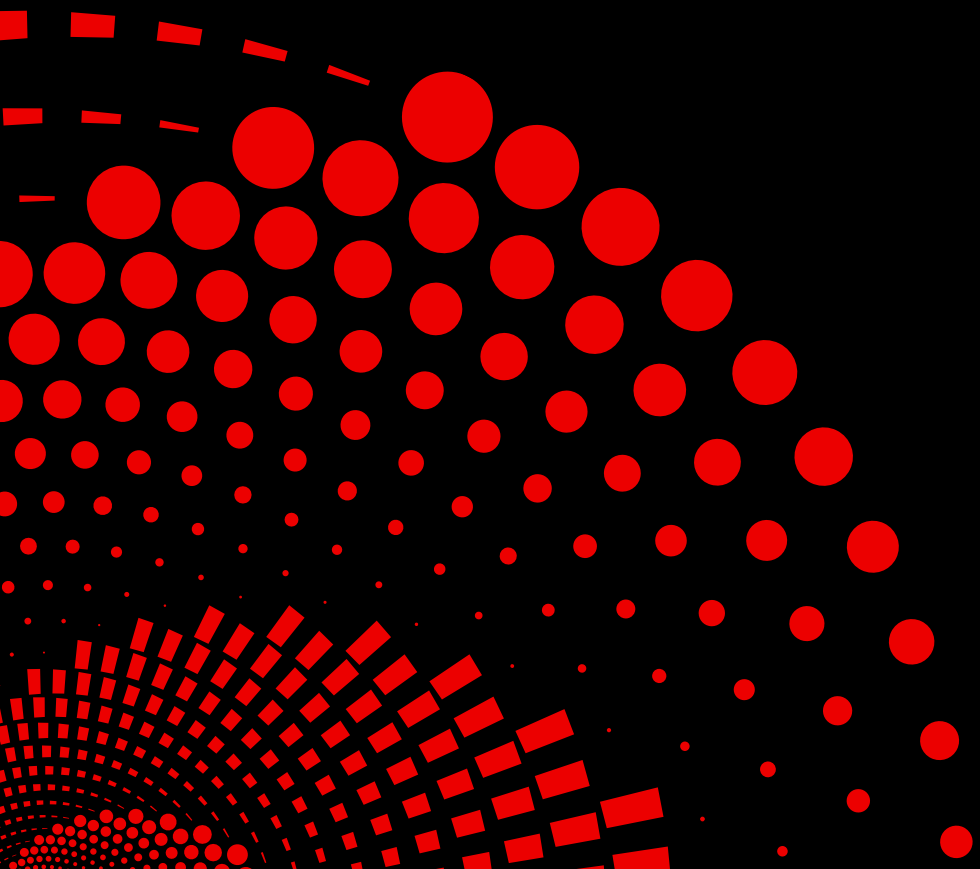
The AI-native SOC maximizes the efficiency and effectiveness of services partners by:

- Collecting rich telemetry from any source at scale
- Supporting real-time monitoring and collaboration with internal teams and consultants
- Offering robust remediation capabilities, empowering IR teams to respond at machine speed

Driving Meaningful Impact for SOC Team Members

The AI-native SOC extends beyond advanced technology and modern processes to the people powering security operations. Forward-leaning organizations cut complexity, manage manual overhead, uplevel analysts and ultimately drive down the time it takes to stop breaches. An AI-native SOC platform enables security teams to focus on strategic tasks, maximizing efficiency and effectiveness.

An AI-native SOC platform enables security teams to focus on strategic tasks, maximizing efficiency and effectiveness.



SECURITY ANALYSTS

Gain speed, efficiency and automated workflows without configuration

The current SOC framework falls short in providing the support security analysts need for operating with pertinent insights, speed and efficiency. AI-native SOC platforms alleviate this burden and amplify efficiency by unifying security operations on a single platform, eliminating the need to pivot across multiple data sources, tools and consoles.

With workflow automation built in, analysts can streamline their processes, accelerate threat analysis and efficiently respond to incidents. By simplifying every stage of incident response, the AI-native SOC platform empowers security analysts to focus on high-priority tasks without being bogged down by manual processes.

Another significant enabler for empowering higher-order analyst performance is GenAI-supported investigations. With GenAI, analysts no longer need deep expertise in query language syntax. GenAI allows analysts to ask questions in plain language and translates them into the correct query within the console. This removes barriers so analysts can readily obtain valuable insights and recommendations, streamlining decision-making.

Analysts can streamline their processes, accelerate threat analysis and efficiently respond to incidents.

SECURITY ENGINEERS

Eliminate overhead with instant deployment and hassle-free management

Security engineers and architects encounter the daily challenge of managing legacy SIEM solutions with deployment complexity and ongoing maintenance. The AI-native SOC platform revolutionizes their experience by simplifying these responsibilities.

Instead of lengthy data migration projects and complex, fragmented architectures, the AI-native SOC platform transforms data onboarding and setup by natively embedding endpoint detection and response (EDR), identity security, cloud workload protection, exposure management and data protection into the platform.

The platform's cloud-native architecture offers a transformative approach, significantly reducing management overhead for security engineers and enabling quicker troubleshooting that saves valuable time. These advanced platforms are purpose-built to effortlessly manage massive data volumes, performing at petabyte scale. This supports real-time monitoring of data volumes and telemetry health, ensuring optimal SOC performance.

Instead of lengthy data migration projects and complex, fragmented architectures, the AI-native SOC platform transforms data onboarding and setup.

THREAT HUNTERS

Unlock faster search with faster outcomes

Threat hunters and incident responders require speed and agility to stay ahead of increasingly sophisticated adversaries. AI-native SOC platforms deliver orders-of-magnitude faster search performance compared to legacy SIEMs, enabling threat hunters to swiftly uncover threats and take decisive actions.

The platform not only streamlines the hunt for advanced threats but adds an important element of rich context to the process, making it both efficient and streamlined. It equips threat hunters with prebuilt security investigation queries and threat hunting workflows, empowering them to expertly root out hidden threats across the organization's digital estate. With fast, GenAI-supported search queries, threat hunters can pinpoint threat sources, identify root cause and ensure the right steps are taken to fully remediate the incident.

An AI-native SOC platform streamlines the hunt for advanced threats and adds rich context to the process.

CISOs

Realize superior outcomes at a fraction of the cost

Managing the complexity of the modern SOC is no easy feat. Siloed tools and data stores and runaway costs mean security leaders need a new way to navigate the current landscape. In addition, they also have to manage limited resources and headcount.

By consolidating multiple tools with a single platform, CISOs can cut down complexity and administrative overhead so they can redirect their focus toward strategic initiatives, ultimately enhancing the organization's security stance.

Today's CISOs have responsibilities far beyond implementing traditional security controls — they must also facilitate risk management and enable transformation. With a comprehensive view of threats and vulnerabilities, CISOs can effectively communicate their security posture to fellow executives to support board-level discussions and strategic planning. This ensures security strategies are tightly aligned with business objectives and priorities.

» With a comprehensive view of threats and vulnerabilities, CISOs can effectively communicate their security posture to fellow executives and the board.

> **Transitioning from firefighters to fire marshals, the evolution to an AI-native SOC is centered on empowering teams to work smarter, not harder. Through the reduction of manual tasks and thoughtful integration of AI and automation to upskill analysts, the AI-native SOC cultivates a culture of proactive threat protection. This transformation not only fortifies the SOC but also positions it as a catalyst for business innovation.**

Justin Acquaro
CrowdStrike Chief Information Security Officer

How CrowdStrike Powers the AI-Native SOC

To stop the breach, it's time to transform the SOC. The CrowdStrike Falcon® platform is the industry's answer to achieve the AI-native SOC of the future, bringing together all key SOC capabilities, including next-gen SIEM, endpoint, identity and cloud security, and threat intelligence, on one massively scalable platform. With AI and workflow automation built natively in the platform, and a generative AI assistant helping teams move faster than they ever thought possible, the Falcon platform future-proofs enterprise SOCs against tomorrow's threats and the deluge of data that will inevitably paralyze legacy SIEMs.

Machine learning and AI power Falcon's defenses. The Falcon platform integrates with the CrowdStrike® Security Cloud to continuously crowdsource data from tens of thousands of customers, across trillions of events weekly, and analyze this data with machine learning models to find new threats and hone existing detections. Generative, cloud and sensor-based AI models work together with behavioral analytics and threat intelligence to maximize coverage and reduce the risk of a single point of failure in its defenses.

CrowdStrike Falcon® Next-Gen SIEM extends the industry-leading security and performance of the Falcon platform to all data for complete visibility and protection. A single, unified console eliminates "swivel chair syndrome," simplifying every aspect of detection, investigation and response. Falcon Next-Gen SIEM's modern analyst experience amplifies the speed and efficiency of incident response, so teams can swiftly root out threats while slashing SOC costs.

> **In the journey to the modern SOC, the emphasis extends beyond AI implementation to delivering a seamless, collaborative analyst experience. With capabilities like incident workbenches and graphical exploration, CrowdStrike is empowering analysts to navigate complex threat landscapes with unprecedented efficiency and clarity, forging the path toward proactive defense strategies.**
>
> **Elia Zaitsev**
> CrowdStrike Chief Technology Officer

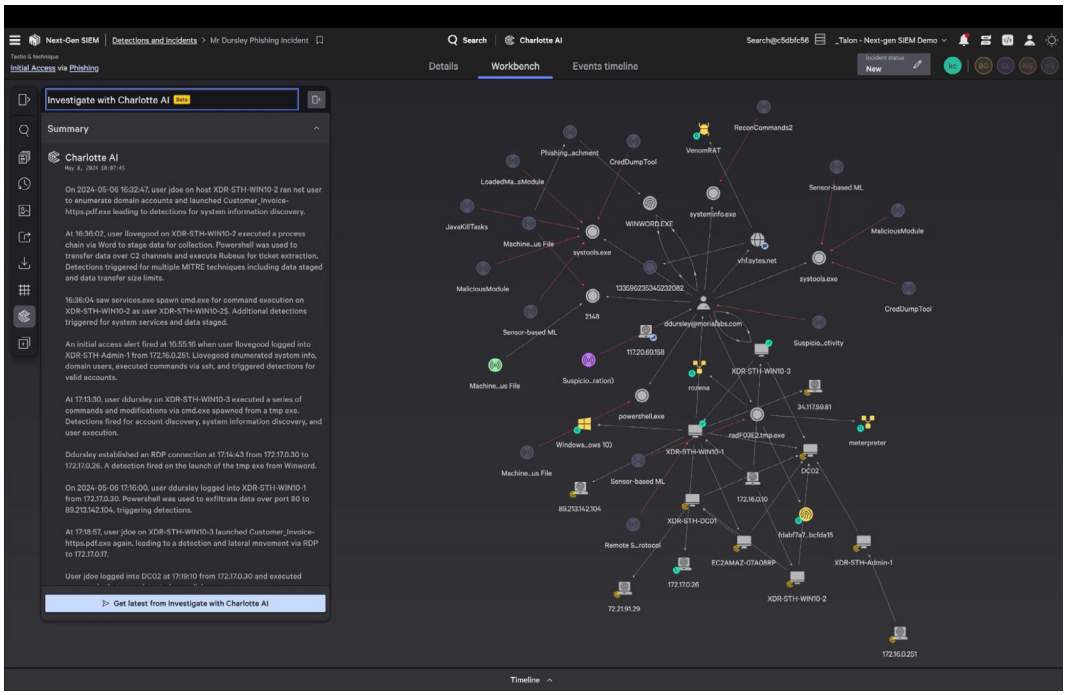


Figure 1. Falcon Next-Gen SIEM reimagines the analyst experience with Charlotte AI and Incident Workbench to drive down investigation and response times from hours to minutes.

Consolidate point solutions and experience a fast ramp-up with:

- **A unified platform with key data built in:**
  All critical data — endpoint, identity and cloud controls — and threat intelligence are natively built into the Falcon platform
- **Frictionless onboarding for third-party data sources:**
  Falcon Next-Gen SIEM makes it easy to ingest third-party data sources with custom connectors — all through an intuitive interface that's as easy to navigate as your favorite app
- **Long-term IT and security data storage:**
  Falcon Next-Gen SIEM offers long-term data storage at a cost up to 80% lower than that of legacy SIEMs,[7] with a revolutionary, index-free architecture that scales to more than one petabyte per day

Detect threats in real time and investigate in seconds with:

- **Incident visualization that reveals the full path of an attack:**
  Instantly understand the scope of an attack in an elegant visual graph that correlates users, entities and threat context so you can rapidly orient and respond
- **Faster search and real-time collaboration:**
  Dramatically speed up investigations with search performance that's up to 150x faster than legacy SIEMs[7] and collaborate instantly to quickly take action

7 Results are from a customer. Individual results may vary.

- **Generative AI, the ultimate force multiplier:**
  Elevate the skill level of your entire team by harnessing the power of GenAI to prioritize incidents, enrich them with threat intelligence and summarize them in plain language, turning hours of work into minutes or seconds

- **Expert resources that augment your team:**
  Disrupt adversaries across all attack surfaces with 24/7 AI-powered managed threat hunting, detection and response

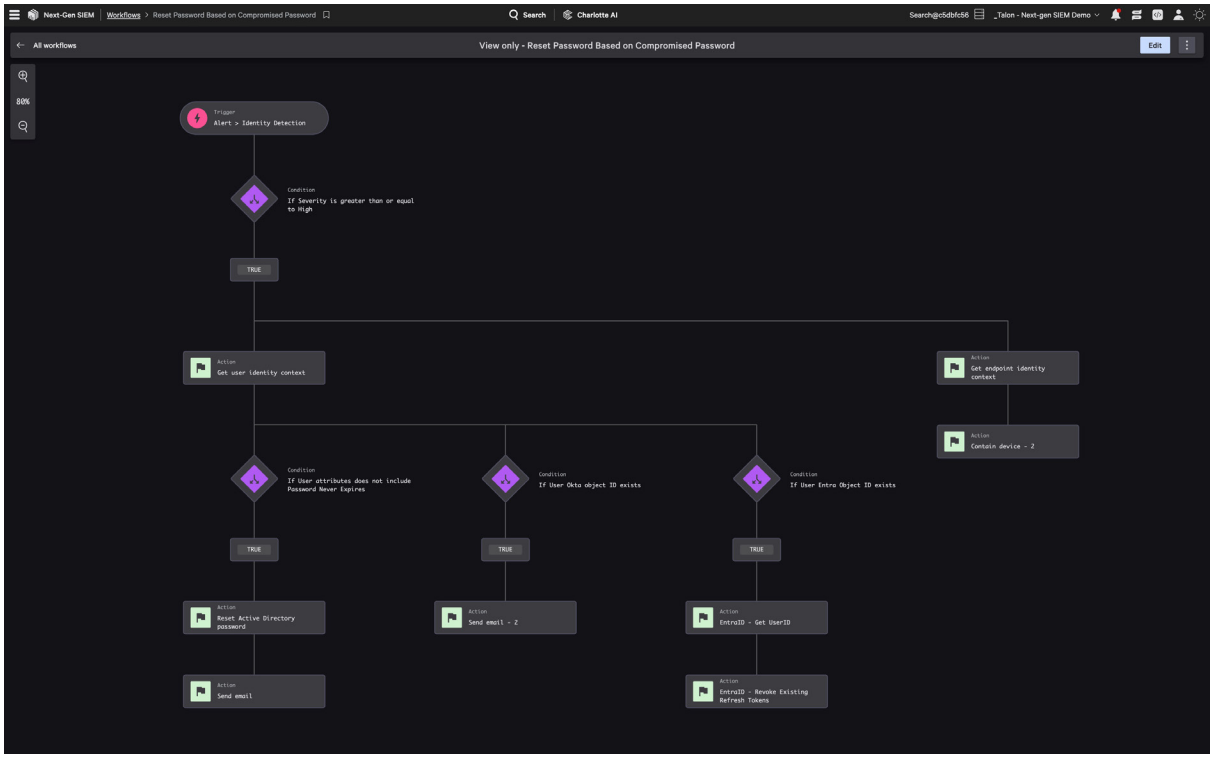


Figure 2. A flexible visual editor lets your team build advanced workflows in minutes.

Stop the breach with:

- **Automated response with intuitive built-in workflows and actions:**
  Coordinate response across your security and IT stack with native workflow automation powered by CrowdStrike Falcon® Fusion SOAR — more than 125 workflow actions let you fully eradicate threats and free up your team to focus on higher-order operations

- **Smarter decisions and swifter resolution with adversary intelligence:**
  Speed up incident response with world-class threat intelligence and workflow automation on your side — get direct context on adversaries and their tradecraft from CrowdStrike's industry-leading threat intelligence

- **Tight integration with the Falcon agent to drive any endpoint action:**
  Contain fast-moving attacks, limit lateral movement and stop breaches through native integration with the Falcon agent for rapid response and optimal recovery

CrowdStrike's Own SOC Transformation with Next-Gen SIEM

Falcon Next-Gen SIEM not only helps leading organizations around the world modernize their security operations, it also transformed CrowdStrike's own SOC. Facing scalability limitations and hefty SIEM costs with data volumes growing at 30% per year, CrowdStrike CISO Justin Acquaro knew he needed to bring the SOC into the future and give analysts a radically improved experience to drastically cut down onboarding time.

Embracing innovation: The path to modernization

Recognizing the imperative for modernization, Justin embarked on a journey to revolutionize the SOC's capabilities, with the foundation of that evolution built on Falcon Next-Gen SIEM. The rollout was seamless, characterized by careful planning and smooth data migration to the Falcon platform. Routing Falcon platform endpoint, identity and cloud security logs was a breeze. The team also leveraged the CrowdStrike® CrowdStream data pipeline to onboard third-party data sources quickly.

Today, CrowdStrike's SOC boasts unparalleled visibility, ingesting 50% more data than before and achieving search speeds 150 times faster. Automation and AI in the platform instantly enrich alerts and reconstruct attack paths for every incident. This means analysts automatically have context and insights at every step of their workflow for drastically faster response — all without investing in additional resources. All of this has helped the SOC team consistently stay ahead when it comes to detection and response metrics. As CrowdStrike Senior Director of Information Security Tim Briggs noted, “With Falcon Next-Gen SIEM, we have successfully built a response time that is less than a few minutes.”

Falcon Next-Gen SIEM provides a blueprint for the SOC of the future. It allows CrowdStrike to collect and store all security data in one place while avoiding the hassle of siloed data lakes and cold storage. And the team can now unify all security operations on one platform.

“The days of using point products and building massive teams to manage these tools are over,” said Justin. “Instead of building an army of people to stitch tools together, you can allocate people to actively defending your company.”

Conclusion

The success of the AI-native SOC hinges on the seamless integration of people, processes and technology. As detailed in this survival guide, leveraging advanced AI and automation capabilities in an AI-native SOC platform is crucial for effectively combating modern cyber threats.

CrowdStrike provides a comprehensive solution that addresses all three pillars of people, processes and technology that converges data, security and IT, with AI and workflow automation built natively within. Additionally, CrowdStrike works with an ecosystem of leading partners to design, deploy and operationalize services for the AI-native SOC.

By harnessing the power of AI and automation, organizations can elevate their threat detection and response capabilities, streamline security operations and effectively mitigate risks. CrowdStrike's innovative approach empowers the SOC to modernize and stay ahead of evolving threats. With a commitment to collaboration and innovation, CrowdStrike delivers unparalleled expertise to help organizations navigate the complexities of the cybersecurity landscape — now and in the future.

The success of the AI-native SOC hinges on the seamless integration of people, processes and technology.

READY TO MODERNIZE WITH AN AI-NATIVE SOC?

Request a test-drive of Falcon Next-Gen SIEM to experience the power of the platform in your environment.

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