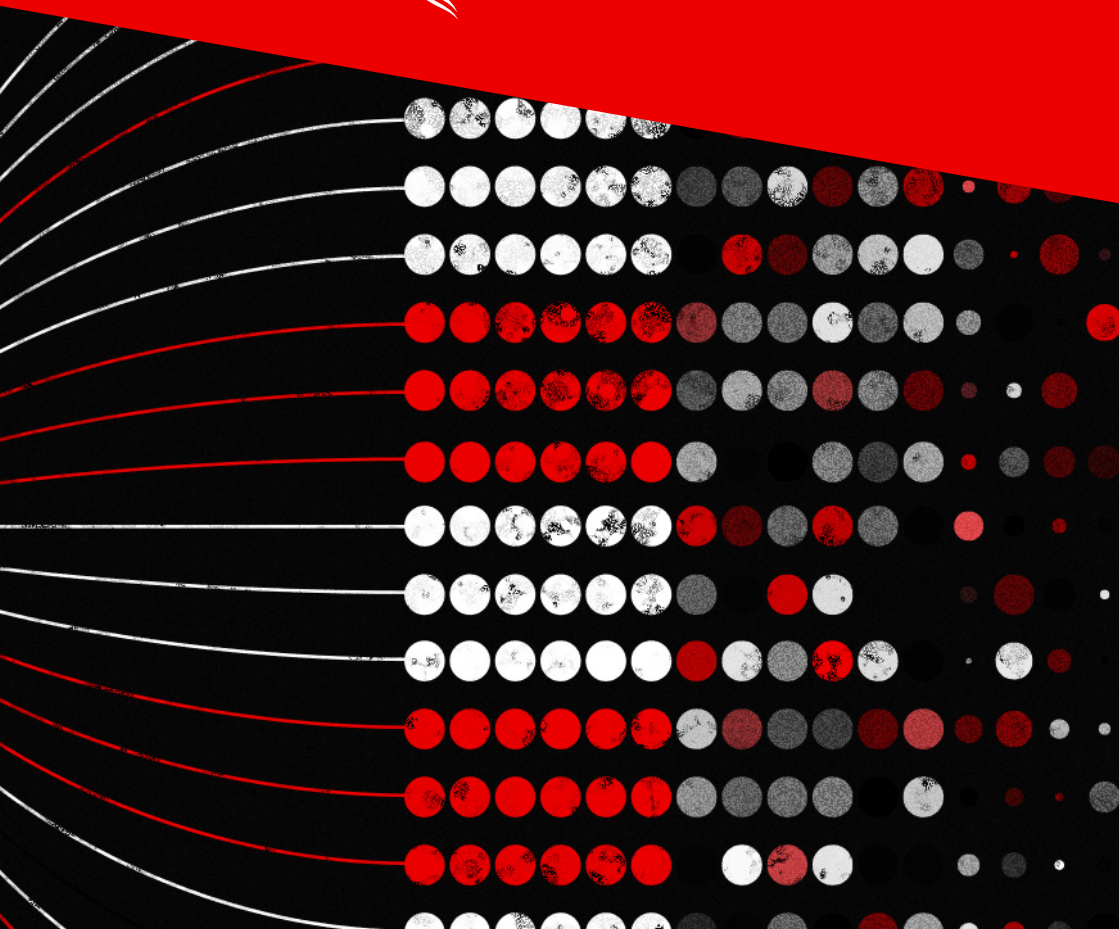
The Complete Guide to Next-Gen SIEM

CROWDSTRIKE



What You'll Learn in This Guide

The Complete Guide to Next-Gen SIEM is your essential resource for understanding security information and event management (SIEM) solutions.

Within these pages, you'll gain insights into how SIEM technologies work and their pivotal role in security operations. We'll delve into the history of SIEM, tracing the journey from legacy models to next-generation innovations. We'll also explore how SIEMs have evolved as the landscape has undergone paradigm shifts — such as cloud computing, big data and remote work models — requiring security teams to extend visibility beyond traditional perimeters.

An integral goal of this guide is to assist you in identifying how a next-gen SIEM solution can elevate the current practices and workflows of your security analysts. Equally important for readers already overseeing a SIEM within their operational setting, this guide will aid you in evaluating your existing SIEM against the capabilities of next-gen SIEM. By doing so, you can pinpoint key areas for improving the effectiveness and efficiency of your security operations, thereby enhancing your organization's overall cybersecurity posture.

Table of Contents

Chapter 1

The Threat Landscape and Rise of SIEM Solutions

Before we can discuss the details and functionalities of next-gen SIEM, it's important to first understand the threat landscape and how the need for this technology emerged.

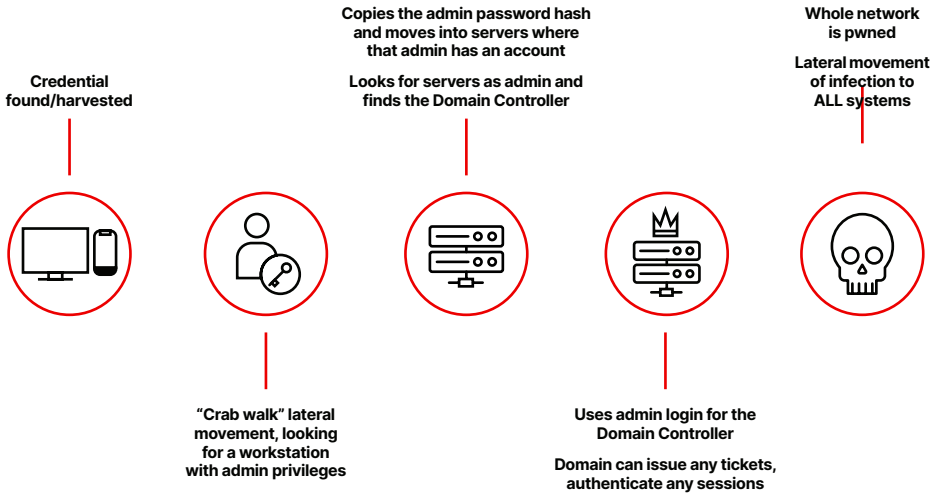
It all starts with adversaries. Across eCrime groups and state-sponsored threat actors, we've seen the rise of over 200 adversaries, with 34 added in 2023 alone.[1] These sophisticated attackers use multiple vectors to target a wide variety of assets, from endpoints and servers to internet of things (IoT) devices, mobile devices and even networking equipment. As modern systems evolved, digital assets were no longer restricted to on-premises data centers. Security needed to extend beyond the corporate network to cover multi-cloud, edge and hybrid environments along with more ephemeral DevOps instances.

34 new adversaries tracked by CrowdStrike, raising to total **232**

[1] CrowdStrike 2024 Global Threat Report

As cyber threats advanced, traditional signature- and policy-based defenses — such as firewalls, intrusion prevention systems (IPSs), intrusion detection systems (IDSs), anti-malware and email security — became less effective. Time and time again, adversaries continued to exploit their inherent advantage. They could launch an unlimited number of attacks with no consequences, and they only needed to succeed once to breach an organization. Security teams, on the other hand, needed to block every single attack. It was virtually impossible for one single security tool to stop all attacks. This challenge intensified as adversaries evolved. As a case in point, 75% of attacks observed in 2023 did not even use malware to gain initial access.[2] Today's attackers increasingly exploit employees and customers to breach organizations' cyber defenses. By compromising credentials, they can then move laterally and escalate privileges to access critical assets, often within minutes.

Lateral Movement Example: Pass-the-Hash



[2] CrowdStrike 2024 Global Threat Report

In addition to external attacks, organizations face internal threats from malicious insiders and risky behavior from negligent employees, which can lead to the loss of intellectual property and sensitive data. The never-ending headlines about corporate data breaches, often involving the theft of thousands of customer records, underscore the urgency of this issue. Each incident forces consumers and the market to confront a critical question: How do we hold organizations accountable for safeguarding our data?

Emergence of Cybersecurity Regulations

The growing concern over data security spurred the creation of new data privacy and security regulations. Compliance laws, such as HIPAA, SOX and PCI DSS, triggered a flood of requirements for organizations to monitor and track access to sensitive information while mitigating threats. This timeline highlights the pivotal regulations that have reshaped the compliance landscape.

1996

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA establishes privacy and security standards for safeguarding protected healthcare information (PHI).

1998

U.K. Data Protection Act

The U.K. Data Protection Act regulates the processing of personal data to ensure individuals' rights are protected and their data is not misused.

1999

Gramm-Leach-Bliley Act (GLBA)

GLBA requires financial institutions to explain how they share and protect customers' private information.

2002

Sarbanes-Oxley Act (SOX)

SOX mandates strict financial reporting and auditing requirements to enhance transparency and prevent corporate fraud.

2004

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS establishes information security standards for organizations that handle payment card information to prevent breaches of sensitive data and reduce the risk of fraud.

2018

General Data Protection Regulation (GDPR)

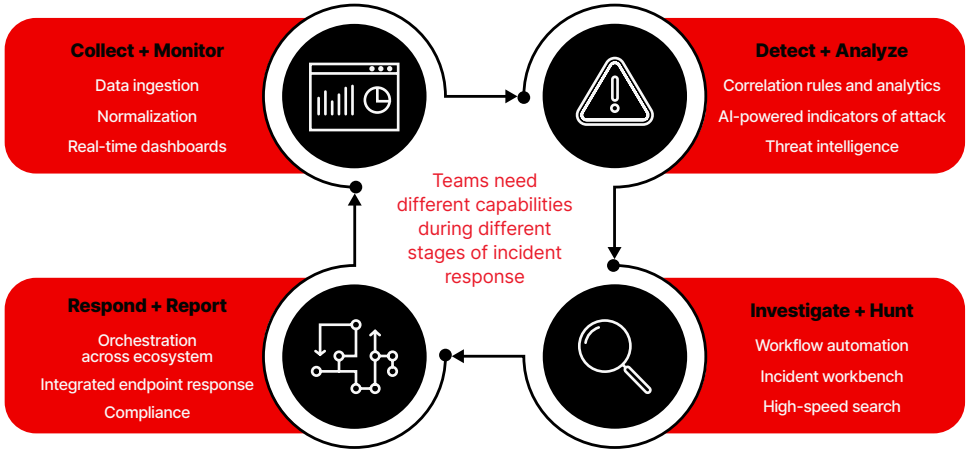
GDPR standardizes data protection laws across the European Union, enhancing individuals' control over their personal data and imposing strict requirements on how data is handled.

Maturing Security Practices

The collapse of the network perimeter and the increasing sophistication of cyber threats and mounting regulatory requirements underscore the necessity for centralized security information and event management. Standards like NIST, ISO and FedRAMP offer guidelines to help organizations evaluate risks, refine processes and implement stronger security controls. Following these frameworks equips practitioners with enhanced visibility and early threat detection capabilities that span their entire environment.

Tackling Every Stage of Incident Response

As cybersecurity threats escalated, organizations needed a comprehensive approach to detect and stop them.



Data Collection and Threat Monitoring

The evolving threat landscape demanded continuous monitoring capabilities across all facets of the organization's digital estate, including networks, endpoints, cloud environments and applications. The first step was centrally collecting and integrating all of this data. Security analysts needed a unified view of potential threats and vulnerabilities with real-time monitoring to turn the tide against cyber adversaries.

Threat Detection and Analytics

Security teams needed to identify threats automatically. First, correlation rules emerged as a way to uncover cross-domain attacks. Over time, analytics and AI ushered in more precise threat detection capabilities, enabling SOC teams to quickly find and mitigate emerging threats and anomalies that could evade traditional security measures.

Investigation and Threat Hunting

Once analysts detected threats, they needed to identify the root cause, scope and impact of an attack. With actionable context at their fingertips, investigations could unfold at lightning speed, paving the way for faster and smarter incident response. A reduction in investigation time using automated actions meant security leaders could drastically lower mean time to respond (MTTR) to contain and neutralize active threats — a decisive win in the race against the clock.

Recognizing the limitations of traditional security approaches, organizations required proactive methods to find malicious activity. Threat hunting allowed teams to uncover latent threats lurking within the network and reveal system and application vulnerabilities. Security teams required a means to analyze and correlate threat indicators from across security tools and threat intelligence data sources to identify and neutralize sophisticated threats before they could cause harm.

Response and Reporting

Security teams needed to expedite incident response and stop threats directly by orchestrating response across their security and IT stack. Faced with stringent data protection regulations and industry standards, organizations were under increasing pressure to demonstrate compliance with established security frameworks. This made it imperative for security leaders to adopt robust security controls and mechanisms to safeguard sensitive data and ensure regulatory adherence. Comprehensive logging, auditing and reporting capabilities were essential for demonstrating compliance.

These market drivers and operational requirements culminated in the emergence of a new cybersecurity technology: security information and event management.

By consolidating and correlating security event data from disparate sources, SIEM platforms emerged to empower organizations to monitor, detect, investigate and respond to security threats. Additionally, SIEM solutions helped organizations address compliance objectives by facilitating log monitoring and retention of security data.

What We Covered

The threat landscape is constantly evolving. Adversaries, from eCrime groups to state-sponsored actors, continually adapt their tactics to exploit vulnerabilities across diverse digital environments. As organizations expand into multi-cloud, edge and hybrid setups, security must extend beyond traditional boundaries to safeguard against evolving threats.

Traditional security defenses, like firewalls and anti-malware, struggle to keep pace with the agility of modern adversaries. With the majority of attacks bypassing malware altogether and internal threats on the rise, organizations face mounting pressure to secure their digital assets. Compliance and regulatory frameworks further compound these challenges, driving the need for robust security measures to protect sensitive data and ensure compliance.

In response to these complexities, SIEM solutions have emerged as a cybersecurity cornerstone, offering organizations a centralized platform to monitor, detect and respond to security threats.

Chapter 2
Navigating Security Operations with SIEM

Cybersecurity teams are like an elite squad, bonded by a shared mission to defend the organization against cyber threats. The members of this unit often work together on highly stressful projects that impact the entire organization. They are a well-oiled machine, triaging alerts, prioritizing where to focus and resolving security risks day in and day out. As you can imagine, achieving this level of performance takes a lot of coordination.

To build a SOC that is primed for peak speed and efficiency, security leaders need to equip their teams with centralized security insights from across the organization's environment. Think of it as the nerve center for digital defense. This is where SIEM steps in, serving as the SOC's cyber backbone. SIEMs act as the central hub, pulling together and analyzing telemetry across multiple environments to give security analysts a unified view of potential threats and vulnerabilities.

Naming a Game Changer

Back in 2005, Gartner analysts Mark Nicolett and Amrit Williams coined the term "SIEM," setting the stage for a revolution in cybersecurity.

What Is a SIEM?

A SIEM platform is the bedrock of security operations, described by many as a single pane of glass. It functions as a centralized platform that ingests and aggregates security data from multiple, disjointed tools across an organization's entire digital estate, including on-premises and cloud environments. For today's digitally driven business, that's a lot of data. To manage it all, SIEMs use advanced analytics and machine learning (ML) techniques to detect suspicious activities, anomalies and potential security breaches in real time or near-real time, all while providing analysts with the right context and enabling prioritization.

At its core, the SIEM provides unparalleled visibility into an organization's security posture, delivering continuous monitoring of unauthorized access attempts, malware infections, insider threats and other malicious behaviors. A SIEM platform boasts a suite of features, including robust log management, sophisticated event correlation, swift incident response capabilities and comprehensive compliance reporting. These features are essential tools for cybersecurity teams, helping analysts expertly navigate the demanding role of investigating security incidents. By leveraging a SIEM, analysts can promptly address security risks, mitigate threats and uphold the organization's security standards.

Additionally, SIEM tools are crucial for helping companies meet compliance requirements, providing detailed audit trails and reports tailored to standards like GDPR, HIPAA and PCI DSS. They simplify the task of navigating compliance audits by offering exhaustive documentation of security events, user activities and policy adherence, promoting transparency and accountability.

Trends Driving SIEM Innovation

The SIEM journey hasn't always been easy. Before we move forward, let's address the elephant in the room: SIEM has had a bumpy history for many companies.

Computing has migrated to cloud-based systems, and game-changing tech like software-as-a-service (SaaS) applications, mobile devices, artificial intelligence and automation are racing ahead at full throttle. Originally designed for a simpler IT landscape, traditional SIEMs have struggled to keep pace with today's data volumes, lightning-fast adversaries and ever-evolving threats.

As organizations moved to the cloud and adopted SaaS applications, security teams faced the challenge of collecting logs from a complex web of cloud providers and services. Inevitably, security analysts found themselves submerged in the complexities of SIEM setup and maintenance rather than the pursuit of meaningful security insights.

In response to these market disruptions, security teams have pursued innovations that can boost their agility and maintain a competitive edge over adversaries. Key pressure points include:

Poor Scalability

Staying ahead in security necessitates a strategic reevaluation of SIEM log management capabilities and detection tactics. In today's world, critical data, essential applications and vital business processes are dispersed across a vast digital landscape. Everything from cloud hosting and SaaS providers to mobile devices and IoT gadgets contributes to a torrent of data, significantly increasing the volumes that a SIEM needs to centrally store, analyze and correlate. Yet traditional SIEMs struggle to scale and keep pace. Deployed on-premises, IT and security teams had to manage the storage capacity and scalability requirements, constantly adding more servers to keep up with the ever-growing data influx.

Manual, Slow Security Investigations

For today's valiant security analysts, the SIEM's shortcomings in handling growing log volumes has thrown a wrench into the well-oiled SOC engine. Analysts are inundated with a relentless stream of alerts from siloed and disparate security tools. Manual triage becomes the norm as they try to wade through the noise, searching for meaningful signals amongst false positives. And here's another kicker: Sluggish searches bog down their investigations and often lead to wasted time.

Additionally, response actions and automation are scattered across different tools. This can cause "swivel chair syndrome," which not only delays incident resolution but leads to process inconsistencies. This increases dwell time, hindering the team's ability to stay on top of things. These issues can be demoralizing for a team dedicated to keeping the company and its data secure, particularly when response speed is a key performance indicator for a mature SOC.

Diminished SOC Effectiveness

At the helm, SOC leaders bear the charter of safeguarding the business, making risk mitigation their prime focus. They're laser-focused on driving down risk, which translates into metrics like tracking the number of alerts analysts can effectively investigate and close, and reducing their mean time to detect (MTTD) and MTTR. Yet there's a notable disconnect between what the traditional SIEM is capable of and what leaders need it to accomplish.

The arduous process of ingesting data into the SIEM and fine-tuning its rules has been painstaking, consuming valuable time and resources. Compounding this is the relentless influx of low-fidelity alerts, which obscure the path to effective threat detection and response.

The implications of these challenges are far-reaching. With visibility blind spots and sluggish response times, the organization becomes increasingly vulnerable to data breaches. Additionally, the toll on the SOC team is significant — alert fatigue and analyst burnout increasingly plague the team — leading to increased staff turnover and diminished operational effectiveness.

Escalating SOC Costs

SIEMs serve as central repositories, promising a single pane of glass for security visibility. But when companies are billed based on ingested data volumes, they face a dilemma of choosing which data sources to collect in their SIEM to stay on budget. This cost-saving measure, though seemingly practical, creates a catch-22 dilemma. It's a high-stakes game of budget versus security. When the SOC is limited in its ability to log and retain all data, it introduces security blind spots. The risk? Increased vulnerability to data breaches. Additionally, the growing data volumes can make it hard to predict the bill and remain within your budget.

[3] Vectra, 2023 State of Threat Detection
[4] Vectra, 2023 State of Threat Detection
[5] IDC, How Many Security Tools Do Organizations Have, and What Are Their Consolidation Plans?, US51973524, Mar 2024
[6] ISC2 Cybersecurity Workforce Study 2023, "How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce"

Overburdened SOC Teams

4,484 alerts per day[3]

67% of alerts are ignored[4]

50 average SOC tools, with some using over 140[5]

4 million professionals — cybersecurity workforce shortage[6]

Heeding the Call for Innovation

As the business and threat landscapes have transformed, the need for innovation in SIEM solutions has heightened. Think of it as the propulsion engine getting a turbo boost for the SOC spacecraft. Over time, SIEM platforms have adapted and evolved, becoming the rocket fuel that propels cybersecurity efforts forward amidst the ever-changing market dynamics.

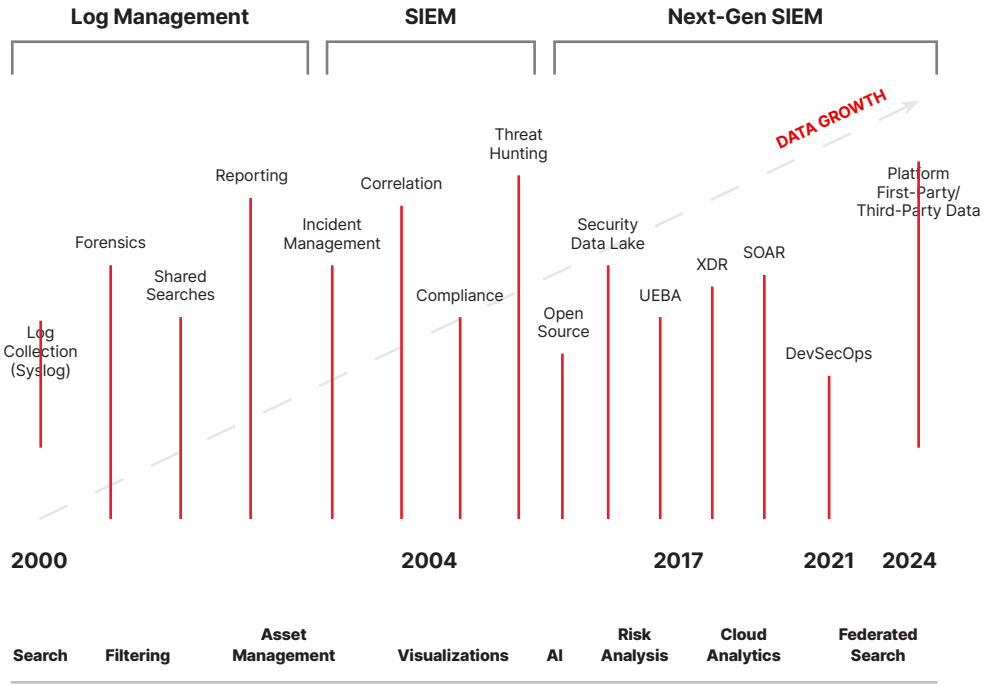
Here are the three major phases of innovation that have shaped today's modern SIEM:

Phase 1: Traditional SIEM

Early SIEM platforms combined security event and security information management. Traditional SIEM solutions primarily focused on collecting and indexing log outputs from various applications and systems within an organization's network. They enabled security analysts to search and retrieve specific log details, facilitating tasks such as auditing compliance event reporting or conducting forensic deep dives.

However, despite their capabilities, the first generation of SIEM solutions faced significant challenges. Vertical scalability limitations quickly emerged as a major hurdle, hindering their ability to support growing data volumes. It's like trying to fit more and more servers into a clown car — eventually, something's got to give. Managing the flow of data in and out also posed significant challenges, and dashboards, reports and alerts remained rudimentary in nature. They also lacked advanced correlation and enrichment features. Early SIEMs were a good effort, but there was definitely room for improvement.

History and Evolution of SIEM



Phase 2: Early Next-Gen SIEM

The advent of next-generation SIEM solutions marked a significant leap forward. These platforms embraced cloud deployment models, integrating capabilities such as user and entity behavior analytics (UEBA); security orchestration, automation and response (SOAR); and threat intelligence feeds. This phase saw SIEMs evolving from mere data repositories to proactive, intelligence-driven security platforms.

Phase 3: Evolved Next-Gen SIEM

Today, we find ourselves in the era of evolved next-generation SIEMs. These cutting-edge cloud-native solutions offer petabyte scalability, sub-second latency and ultra-high search performance. Powered by artificial intelligence, they boast advanced features such as incident grouping and prioritization, generative AI (GenAI), and comprehensive threat detection, investigation and response (TDIR) capabilities — including endpoint detection and response (EDR) and identity protection — all within a unified SOC platform.

A key advantage of next-gen SIEM is its ability to ingest diverse streaming telemetry, providing security teams a holistic and real-time view of potential risks and vulnerabilities. This adaptability, enhanced with integrated threat intelligence, empowers organizations to proactively identify and address security threats. By meeting the demands of modern environments, the latest evolution in SIEM solutions greatly improves their ability to detect, prevent and resolve a broad spectrum of potential threats.

Next-Gen SIEM Poised to Meet Market Dynamics

Having traced the evolution of SIEM technology, let's dive into why the latest iteration — next-gen SIEM — is such a big deal. Think of next-gen SIEM as the cool new tech on the block, like going from clunky cassette players to streaming crystal-clear tunes on your smartphone. It's packed with advanced features designed to tackle the unique challenges modern SOCs face, making it a game changer for cybersecurity.

With next-gen SIEM, we now have a platform that can propel us into the future of cybersecurity. Let's delve into three key areas where next-gen SIEM solutions empower security teams to fulfill their mission with unprecedented effectiveness.

1. Scaling to Support Growing Data Volumes

As we've discussed, organizations' data volumes have and will continue to skyrocket. In short, data growth is the new normal. In the face of an exponential increase in data volumes generated by a myriad of sources, next-gen SIEM platforms offer cloud-native scalability that rightsizes the legacy bottleneck challenges. And let's not forget the sigh of relief from security analysts as they're freed from the shackles of managing an on-premises solution, equipped with tools that streamline their efforts and enhance their effectiveness.

Next-gen SIEM is designed to effortlessly handle the deluge of data stemming from an expanding array of applications and IoT devices. With the ability to process up to 1 petabyte of data a day, these platforms ensure comprehensive coverage and visibility across even the most complex environments.

2. Outpacing Sophisticated Adversaries

With businesses moving to the cloud, threat actors have wasted no time in targeting them in their newfound "home." According to the **CrowdStrike 2024 Global Threat Report**, intrusions in cloud environments surged by an alarming 75% in 2023. And identities? Sophisticated threat actors are homing in on user credentials, executing 583% more Kerberoasting attacks in 2023 than the previous year. And they're lightning-fast — in 2023, the average time it took for an eCrime adversary to pivot from one compromised host to another within an organization was a mere 62 minutes.[7] If you're feeling a bit short of breath, you're not alone. But rest assured, we don't share this data to scare you — these numbers are simply benchmarks for what the next-gen solutions tackle head-on.

Next-gen SIEM platforms play a crucial role in defending against sophisticated attack techniques by integrating high-fidelity threat intelligence from a variety of sources, including identity technologies, EDR and cloud infrastructure. By leveraging advanced analytics and AI, these platforms enable SOC teams to detect and respond to threats with unprecedented speed and accuracy. With next-gen SIEM solutions at their disposal, organizations can effectively thwart even the most advanced cyberattacks and protect their sensitive data from unauthorized access.

[7] CrowdStrike 2024 Global Threat Report

3. Supporting the Cloud Revolution

With over 92% of businesses hitching a ride on the cloud train for their operations, embracing cloud-native solutions is nonnegotiable in today's digital jungle.[8] This has driven the increasing demand for cloud-native security solutions.

Next-gen SIEM platforms are uniquely positioned to address this need, offering seamless integration with cloud environments and leveraging the benefits of cloud-native computing. By embracing cloud-native architectures and supporting an organization's cloud security via the shared responsibility model, these platforms enable organizations to harness the full potential of the cloud while ensuring the security of their data and assets. And with research showing that 94% of businesses see security improvement after switching to the cloud, it's clear that next-gen SIEM is an important MVP in this security game.[9]

[8] Directive, Over 90% of Businesses Use Cloud Computing, and for Good Reason, 2023
[9] Salesforce, 12 Benefits of Cloud Computing

Quick Tip: Shared Responsibility

The shared responsibility model is vital for cloud security. While providers secure infrastructure, organizations are accountable for securing their data, apps, identities and settings within the cloud environment. Clear delineation is crucial for proper security measures and risk mitigation.

What We Covered

In our exploration of cybersecurity operations, we've uncovered the pivotal role of SIEM as the central nerve center in the defense against cyber threats. SIEM has become the cornerstone of modern security operations thanks to its ability to detect cross-domain threats, deliver crucial, investigative insights and foster collaboration among cybersecurity teams.

However, traditional SIEM solutions have faced challenges in keeping pace with the rapidly evolving threat landscape, including scalability limitations and manual security investigations. The emergence of next-gen SIEM represents a significant leap forward, offering cloud-native scalability, tool consolidation and detection that outpaces sophisticated threat actors. With next-gen SIEM innovations, organizations are better equipped to navigate the complexities of modern cybersecurity operations.

Chapter 3

The Need for Security Consolidation

Adversaries thrive in dark places, like the blind spots between security tools — security teams can't protect what they can't see. And there are a lot of blind spots — SOC teams juggle an average of 50 siloed security tools, which is a troublesome scenario that not only hinders detections but leads to delays in response times.[10]

To improve security efficiency and efficacy, organizations need to consolidate products, agents and consoles. In this chapter, we delve into the drivers behind why organizations need to unify their SOC on a single platform. We'll also explore how the evolved next-gen SIEM's innovation positions it to serve as the cornerstone of streamlined and comprehensive cybersecurity operations.

The Importance of Security Consolidation

As we discussed in Chapter 1, sophisticated threat actors continue to develop new attack tactics to evade detection for longer periods of time. And their speed continues to accelerate at an alarming rate.

[10] IDC, How Many Security Tools Do Organizations Have, and What Are Their Consolidation Plans?, US51973524, Mar 2024
[11] CrowdStrike 2024 Global Threat Report

Quick Tip: Breakout Time

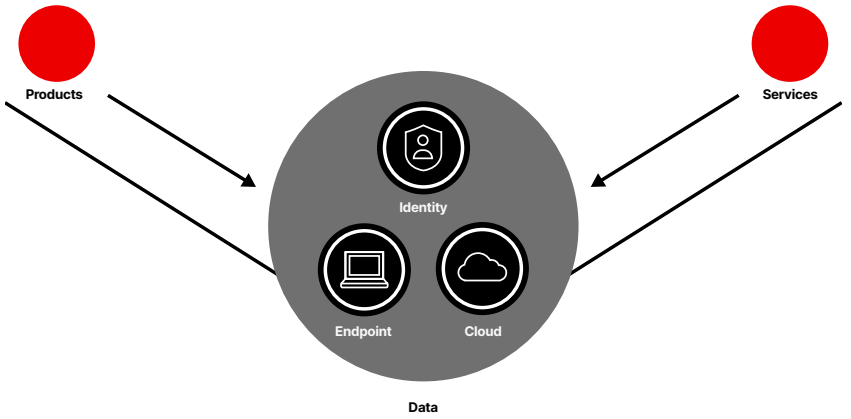
After gaining initial access, adversaries seek to "break out" to other systems in the network to gather information, establish control and pinpoint their targets. The time it takes to move laterally into the network from the initial intrusion is the "breakout time."

The average breakout time for interactive eCrime intrusion activity decreased from **84 minutes** in 2022 to **62 minutes** in 2023.[11]

Security teams must tackle herculean tasks: They need to swiftly detect threats, investigate their root cause and contain them within the narrow breakout time window (just 62 minutes). And all of this must be accomplished while navigating through a maze of siloed security tools, adding another layer of complexity to their already monumental mission. As anticipated, overcoming these obstacles proves daunting: 70% of critical issues still require more than 12 hours to resolve, underscoring the significant challenge security teams face.[12]

The Role of Data Gravity

When discussing the proliferation of tools and data, we can't overlook the concept of data gravity. It's like the unseen force shaping the flow of security data. Imagine a scenario where data behaves like a planet, exerting a gravitational pull. This is the essence of data gravity — a term that encapsulates how vast volumes of data attract applications, services and even more data. As the data pool expands, so does the strength of its pull, significantly influencing the accumulation and interaction of subsequent data.



[12] CrowdStrike 2024 State of Application Security Report

So how does this apply to cybersecurity?

Well, each security control you have in your environment generates its own high volumes of data. Take endpoint data, for example. Endpoints — the laptops, servers and other devices in your environment — generate a significant volume of data, including logs, events and performance metrics. Sending all of your security data to a centralized location for analysis gives you insights for comprehensive threat detection, but it also creates challenges. Let's dub this the "anti-gravity" paradigm.

The traditional SIEM serves as the central hub for analysis. However, it can sometimes compete with other IT and security tools — like your EDR solution — as the center of your SOC universe. Plus, you need to forward all of your logs from your various tools to your SIEM, and duplicating and sending all that telemetry can quickly become cost-prohibitive. It creates that broken anti-gravity paradigm, where security teams sometimes opt to only send a subset of the essential data for correlation in their SIEM to mitigate costs. However, this approach poses the risk of potentially overlooking threats.

So what's the solution?

Instead of fighting gravity, it makes more sense to bring services and applications to your data so that gravity works for you and not against you. This is at the heart of data gravity, and next-gen SIEM solutions do just that. They leverage data gravity to their advantage — and the most significant gravitational force comes from your EDR data.

With a unified SOC platform that natively embeds both next-gen SIEM and EDR, security teams get the best of both worlds with telemetry data at the source. This alleviates the need to store duplicate copies of your security data, driving downstream improvements in security costs and performance efficiency. This evolved approach equips security teams with full visibility to uncover vital insights for threat detection and incident response.

Ultimately, data gravity naturally guides organizations toward adopting next-gen SIEM, where SOC teams can amass a wealth of information. It's akin to conducting a rock concert, where every instrument — each data stream — blends harmoniously to create an electrifying performance. With next-gen SIEM, SOC teams can rock the stage of cybersecurity with confidence.

What About Extended Detection and Response (XDR)?

At this juncture, you might find yourself wondering, "What about XDR as a contender for consolidating threat detection, investigation and response?" If you're pondering this question, you're certainly not alone. Despite the considerable buzz surrounding XDR, it may come as a surprise that nearly one in three security professionals (29%) are only somewhat to not at all familiar with XDR.[13] Or perhaps that doesn't come as a surprise at all, given the ongoing lack of a common XDR definition.

XDR, often seen as the evolution of EDR, extends traditional endpoint visibility by integrating native or first-party data like identity, cloud and IT data to support detection and response. This focus on native data can create security gaps, particularly due to the absence of third-party data. Additionally, various use cases — like audits, compliance and forensic investigations — require robust log management that fall outside the scope of XDR. This underscores the importance of augmenting XDR with next-gen SIEM.

The Benefits of Consolidating Tools and Data

This takes us back to the central topic: the need to consolidate on a single platform. Organizations require the powerhouse capabilities provided by next-gen SIEM. After all, in the cybersecurity game, next-gen SIEM is the undisputed MVP, lighting the path for security teams to lead their organizations to victory against ever-evolving threats.

Bringing together scattered operations under a unified security platform speeds up response times and tips the scales back in favor of the SOC team. By consolidating disjointed operations with a single security platform, organizations can strategically unify disparate security tools and systems into a cohesive whole. Instead of wrestling with a patchwork quilt of tools — each with its own interface, rules and reports — the SOC gains an integrated approach.

[13] CSO, XDR: Still confusing after all these years

Consolidation creates an actionable, holistic view of your attack surface in less time with less effort, delivering essential advantages:

Better Security Outcomes

When security analysts get more in-depth context around security risks in their environment, they can connect the dots between events and activity across various security domains. By swiftly deciphering adversary attack paths and even deducing their sneaky motives, they're equipped to tackle advanced threats head-on. That's the power of a unified platform approach — it delivers the deep visibility that turns the tide against cyber adversaries.

Swift Triage and Incident Response

Consolidating input from multiple sources fuels higher-fidelity detections, minimizing those pesky false positives. Teams can say goodbye to analyst burnout — with actionable context at their fingertips, investigations and triage unfold at lightning speed, paving the way for faster and smarter incident response. Less time spent sifting through alerts means a quicker turnaround in neutralizing active threats — a major victory in the race against the clock.

And just how significant is this win? Up to 75% reduction in investigation time, resulting in the reduction of MTTD and MTTR by up to 70%.

75%

reduction in investigation time

promotes

70%

reduction in mean time to respond/detect[14]

[14]These numbers are projected estimates of average benefits based on recorded metrics provided by customers during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on individual customer's module deployment and environment.

A Future-ready Security Strategy

As the global risk landscape changes, consolidation helps shield your digital estate, warding off emerging threats and preventing costly reactive tool purchases. Instead of scrambling to acquire and stitch together specialized point solutions whenever new threats surface, a unified, scalable platform gives you a speedy and seamless way to integrate new defenses into your environment.

Picture this: leveraging already-deployed agents across your installed base or seamlessly incorporating new telemetry streams into the existing console that analysts can navigate with ease in their day-to-day operations. It's like adding new security gadgets to your utility belt without missing a beat.

What We Covered

In this chapter, we highlighted the importance of security consolidation. Adversaries exploit the blind spots between siloed security tools, slowing detection and response efforts. To counter this, organizations must consolidate their security infrastructure onto a unified platform, streamlining operations and empowering SOC teams to respond swiftly and decisively. Consolidation alleviates the complexity faced by security teams and provides a holistic view of the attack surface, enabling better security outcomes.

Because of its high value and massive scale, endpoint data exerts a strong gravitational pull that attracts other data sources. When combined with endpoint detection and response, next-gen SIEM allows SOC teams to consolidate tools and rock the stage of cybersecurity with unwavering confidence.

Chapter 4

Exploring Next-Gen SIEM Capabilities

In this chapter, we'll establish the critical capabilities for next-gen SIEM that enable unparalleled speed, simplicity and cost-effectiveness. We'll walk through how to address one of the most formidable challenges encountered by legacy SIEMs — data ingestion and storage — by harnessing a platform that inherently embeds EDR and other key security data. We'll also review the entire threat life cycle across detection, investigation and response, including threat hunting. Lastly, we'll cover considerations for deployment.

Simplified Data Ingestion

Next-gen SIEM takes a fundamentally different approach to data ingestion by having the data you need to combat adversaries already built in from the start. There's no need to spend countless cycles with data onboarding — get started right away with endpoint, identity and cloud workload data and more, consolidated into one platform solution. Teams can also easily extend the platform and ingest third-party data with out-of-the-box connectors, flexible parsers, log collector agents and integrated data pipelines. Next-gen SIEM effortlessly normalizes, transforms and standardizes data to keep your security operations running smoothly.

This approach also drastically simplifies ongoing "care and feeding" for data management, reducing total cost of ownership (TCO). Changing log formats can wreak havoc on your SIEM's data pipelines. But with key data sources already built in with next-gen SIEM, you can trust in the reliability of your data flow. Pipeline checks are seamlessly integrated, and alerts continue to fire uninterrupted by any changes or upgrades in your platform, ensuring smooth continuity in all of your security operations.

AI-Powered Detections

If data is the heart of your SIEM, detection content is the brain. And next-gen SIEM is smarter than the same old out-of-the-box correlation rules or dashboards you get with legacy SIEMs. Why does that matter?

Consider this scenario:

Sarah, an employee in the finance department, suddenly starts logging in remotely and accessing sensitive company files at odd hours. Though this behavior may seem innocuous at first glance, it becomes concerning when combined with other factors. For instance, Sarah's login attempts originate from an unfamiliar device located in a foreign country — a clear departure from her usual routine. Though each incident on its own may seem harmless, next-gen SIEM is adept at connecting the dots pointing to adversary compromise.

Why? Imagine a platform that collects vast swaths of data and adversary activity across your environment and from thousands of other security teams. With graph databases, this data can be automatically enriched, making it possible to correlate trillions of security events with indicators of attack (IOAs), threat intelligence and telemetry across millions of endpoints, workloads, identities and more. This makes it possible to not only better understand a single alert but put it into the context of the latest adversary attack patterns seen around the globe.

When your data is put in a risk and security context, you'll get higher-fidelity, more actionable alerts instead of endless false positives. Together with identity protection, next-gen SIEM brings these insights to the forefront with laser-precise detections designed for each native data source, giving you battle-tested, higher-quality content than ever before. In the example above, you would get an alert about Sarah's activity instantly when the platform analyzes native identity data and correlates it with her endpoint. Compared to legacy solutions that use generic behavior analytics and potentially suffer from delays, or otherwise generate noisy alerts, next-gen SIEM uses the power of the platform — including integrated endpoint, identity and cloud security — to find malicious activity straight away.

Ensure you have a good understanding of the types of attacks your organization faces and leverage frameworks like MITRE ATT&CK® to evaluate detection coverage for your SIEM.

Automated Triage and Investigations

Once SOC teams get an alert that they need to take action on, they need to know what happened as fast as possible so they can figure out what to do next. What adversary are they dealing with, how did they gain access and what did they do once inside?

Now think of how the analyst experience would change if you could instantly give them the answers they need.

Next-gen SIEM radically simplifies alert triage and investigation. By analyzing all relevant data, it automatically reconstructs an entire attack path for every incident — something not possible for humans to do alone. It presents an elegant visual graph for analysts to explore process executions, impacted assets and entities, and more, with full context and data across all of their domains.

Quick Tip:
MITRE ATT&CK

A curated knowledge base that tracks cyber adversary tactics and techniques, serving as a valuable tool for building next-gen SIEM policies that strengthen your organization's security posture

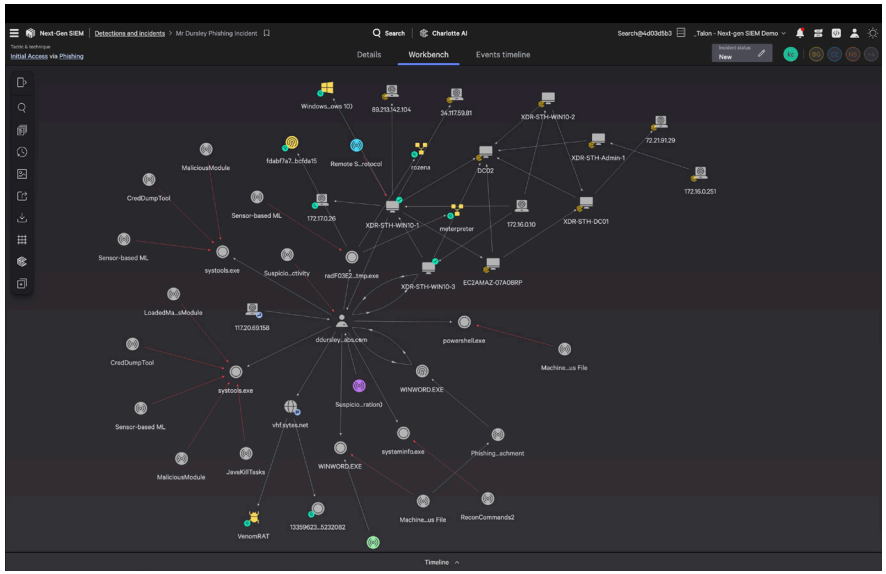


Figure 1. Next-gen SIEM solutions show the relationship between users, entities and indicators of attack in a visual graph.

Generative AI takes this to the next level by making it easier than ever to ask questions and get answers in plain language during an investigation. Next-gen SIEM can immediately tell you the answer to questions like, "Has my data been exfiltrated? From where? By whom? How much data did they take? Which credentials did they use? What other techniques did they use? How did they fly under the radar and slip past our defenses?" It also uses AI to provide digestible incident summaries, making documentation a breeze.

Supercharged Threat Hunting

Beyond investigating a single incident, there are times when teams may want to explore or hunt for similar or other related activity and potentially turn that into a detection. They might also read a threat intelligence report and want to query their SIEM directly based on newly identified adversary activity.

Next-gen SIEMs provide strong support for simple and intuitive queries. Paired with generative AI, SIEMs help threat hunters easily and quickly build searches without needing to know a specialized, complex language. They can also seamlessly pivot from threat intelligence to advanced event searches, traversing across domains and data stores with ease.

Underlying seamless search is next-gen SIEM's revolutionary approach to storing and retrieving data. Compared to legacy solutions built on indices, next-gen SIEM uses a completely different architecture with multiple levels of compression, lightweight tags and bloom filters. Say goodbye to bloated indices and patchwork architectures with cold storage — with next-gen SIEM, all data is easily searchable in seconds.

Response at Machine Speed

No incident can be complete until an analyst takes the appropriate steps for remediation. With embedded SOAR capabilities, next-gen SIEM makes it possible to respond at machine speed across all of your tools while saving your team from manual, repetitive tasks and burdensome automation engineering.

How does it do this? Remember that next-gen SIEM is natively integrated with endpoint protection. This means that straight out the gate, teams can take advantage of a range of flexible endpoint response options, such as real-time response, system recovery, network isolation and more. These capabilities empower security teams to take immediate action against threats, rapidly containing and neutralizing them before they can escalate.

Instead of writing Python or coding, analysts can use graphical interfaces and low-code tools to string together workflows and capture tribal knowledge within their security team, making response consistent and automated every time. Next-gen SIEM tools also offer easily customizable playbook templates to enhance usability and time-to-value.

Quick Tip: What is SOAR?

Security orchestration, automation and response (SOAR) triages more complex threats and automates routine responses, minimizing the need for human intervention.

Rapid Deployment

Are you raring to get started? Fear not, for next-gen SIEM is born in the cloud and sits on the same platform as other key pillars of your security stack. This means you can stand it up in an instant without worrying about administration and maintenance overhead.

Its cloud-native architecture gives next-gen SIEM the seamless scalability needed to handle massive data volumes — think terabytes and petabytes of data — while maintaining rapid performance to uncover emerging threats. With elasticity baked in, next-gen SIEM effortlessly scales to meet fluctuating demands, ensuring it's always equipped to process and analyze whatever comes its way. Built with security and resilience in mind, next-gen SIEM boasts built-in backup and disaster recovery across multiple locations.

Managed Detection and Response

Facing resource constraints and a need to show faster time-to-value, many organizations outsource security operations tasks to managed service providers. If your organization's security efforts are hindered by limited team resources or a shortage of skilled talent, you're not alone. With a global cybersecurity workforce facing a staggering shortfall of 4 million skilled workers, finding the right talent can be challenging.[15]

If this resonates, it's helpful to consider a next-gen SIEM vendor that also provides managed services that cover:

> **24/7 monitoring of your organization's environment for threats**

> **Threat detection, alerting and response from highly experienced security analysts**

> **Service-level agreements (SLAs) for time to respond with full remediation**

> **Proactive threat hunting based on current and past IOAs**

With managed services, you gain instant access to security experts who augment your organization's security efforts. When you work with a services team powered by next-gen SIEM, you can access virtually all of the capabilities outlined herein — all while allowing your internal team to shift their focus from reactive firefighting to strategic initiatives, fostering a proactive and resilient security stance.

[15] ISC2 2023 Cybersecurity Workforce Study

What We Covered

In our journey through next-gen SIEM capabilities, we've illuminated the path to unparalleled security outcomes for your team and organization. These platforms offer a comprehensive solution for handling data ingestion, natively embedding security controls — including EDR, identity security, cloud workload protection and data protection — and end-to-end detection and response across third-party data in one platform to provide full visibility and protection for your entire digital estate. With advanced analytics and automation, next-gen SIEMs transform your SOC into a proactive powerhouse, swiftly detecting, neutralizing and remediating threats. Cloud-native architecture underpins unprecedented scale and ease of deployment. And with managed services offered by the vendor, you can harness the expertise of seasoned security professionals to navigate the cyber realm with confidence and resilience.

Chapter 5

Elevating the Entire SOC Team

Next-gen SIEM not only represents a technology leap forward but serves as a catalyst for enhancing the robustness of SOC processes. Understanding how SOC members collaborate and execute their critical tasks is fundamental to maximizing the effectiveness of next-gen SIEM.

In this chapter, we'll explore the critical relationship between technology and teamwork within a SOC, highlighting the process advancements you'll experience with a next-gen SIEM.

If you work in a SOC, you understand firsthand that it safeguards your organization against the relentless tide of cyber threats. This specialized team operates with a shared mission: to secure critical systems, protect sensitive data and stop breaches that could compromise the organization's integrity and operations.

Within the SOC, each member plays a critical role in maintaining the organization's cyber resilience:

SECURITY ANALYSTS

continuously monitor the digital estate, analyze alerts and investigate potential security incidents.

SECURITY ENGINEERS AND ARCHITECTS

design and implement robust defense strategies, ensuring that systems are fortified against evolving threats.

THREAT HUNTERS

proactively seek out signs of compromise to uncover adversaries early, before they trip alarms.

CHIEF INFORMATION SECURITY OFFICERS (CISOs)

orchestrate comprehensive security measures and guide the team's strategic initiatives to mitigate risks.

Though each SOC member has their specific function, they share the same daily charter: to detect, investigate and respond swiftly to any threats or suspicious activities that could undermine the organization's security posture. This mission requires exceptional coordination, sharp analytical skills and a deep understanding of emerging threats and attack vectors**. A next-gen SIEM is central to supporting this mission.**

Let's dive into how next-gen SIEM supercharges the daily activities of each SOC team member, empowering them to excel in their roles like cybersecurity superheroes.

Security Analyst

Security analysts navigate a constant flood of alerts while making critical decisions under pressure. They pivot constantly between dozens of tools to interpret alerts, gather additional context and take response actions. Next-gen SIEM is poised to transform their experience by directly addressing these time and efficiency issues head-on, empowering them to excel in their role like never before.

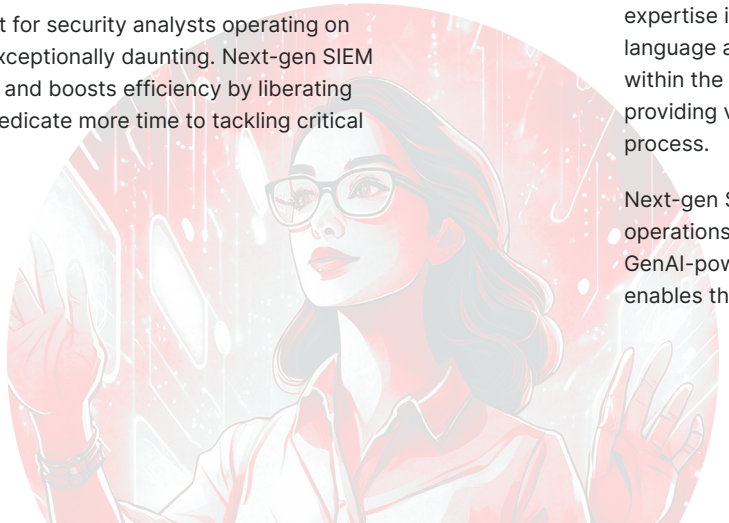
Amplify Efficiency with a Unified Console

Next-gen SIEM significantly enhances the security analyst experience, enabling them to see alerts from all of their tools in one place. This streamlines alert management and empowers analysts to make rapid, well-informed decisions. With next-gen SIEM, SOC analysts have all of the security data consolidated into a single, unified platform, eliminating the need to juggle multiple tools and interfaces.

This streamlined approach eliminates "swivel chair syndrome," saving valuable time and reducing the frustration of manual processes. Now, analysts can focus on analyzing threats, identifying root causes and taking decisive actions with clarity and speed, leveraging real-time dashboards generated by next-gen SIEM's graph technology to visualize incident connections.

Empowering Higher-order Investigations

Time is precious for every SOC team member, but for security analysts operating on the front line, the demand for time efficiency is exceptionally daunting. Next-gen SIEM fundamentally reimagines the analyst experience and boosts efficiency by liberating analysts from mundane tasks, allowing them to dedicate more time to tackling critical threats and conducting advanced investigations.



Next-gen SIEM empowers security analysts to reimagine alert triage and investigation. Alerts are no longer treated in isolation — they are automatically prioritized based on risk, grouped into incidents, and enriched with threat intelligence and additional context like associated adversary activity.

This evolution means investigations are not just faster but more holistic. Analysts can view the entire scope of an incident — including impacted hosts and assets — with a reconstructed attack path. This is a far cry from the days of manual investigation, when analysts would painstakingly piece together clues by copying and pasting them in a notepad like a gumshoe detective pinning pictures and tips on an evidence board.

Imagine a world where the burden of manual investigation is lifted. The automation and AI capabilities of next-gen SIEM revolutionize daily security analyst operations, eliminating the need for technical coding expertise. By automating routine tasks with just a few clicks, analysts can reclaim valuable hours to dive deep into priority threats and fine-tune the SIEM platform for peak performance. This shift empowers analysts to channel their inner detective, investigating the most pressing leads and staying one step ahead of cyber adversaries.

Augmenting Analyst Capabilities with GenAI

Another significant benefit of next-gen SIEM is GenAI, which is designed to enhance analysts' capabilities regardless of their experience level, particularly in handling language-related tasks. With GenAI, for example, analysts no longer require deep expertise in query language syntax. GenAI empowers analysts to ask questions in plain language and translates them into the correct query within the console. Embedded within the platform, GenAI assists security practitioners in their investigations by providing valuable insights and recommendations, streamlining the decision-making process.

Next-gen SIEM harnesses GenAI workflows that significantly accelerate cybersecurity operations, allowing analysts to work faster and more effectively. By integrating GenAI-powered capabilities into the SOC, next-gen SIEM democratizes operations and enables the entire team to perform with greater speed, proficiency and intelligence.

Security Engineers and Architects

Security engineers and architects encounter the daily challenge of designing and managing their organizations' intricate cybersecurity infrastructure. In their role supporting the SIEM, they juggle a lot of responsibilities — from onboarding data and creating parsers to writing detections, tuning alerts, building automated playbooks and more — all while overseeing the ecosystem and integrations to ensure everything operates properly. Next-gen SIEM is poised to transform their experience by simplifying these complex responsibilities, empowering them to excel in architecting and implementing robust security solutions with unprecedented efficiency and effectiveness.

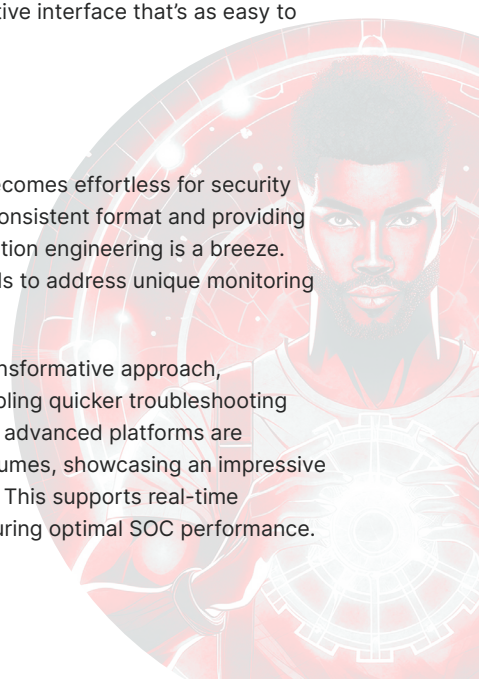
Easier Onboarding and Management

Next-gen SIEM transforms data onboarding by natively embedding EDR, identity security, cloud workload protection, exposure management and data protection into the platform. With out-of-the-box integrations, engineers can seamlessly extend data ingestion to additional third-party tools like web proxies or firewalls, simplifying setup. Next-gen SIEM makes data parsing a breeze so security engineers and architects can forgo the manual effort of mapping event fields when formats change or new data sources are added. They can apply ready-to-use connectors and also unleash their creativity with custom connectors, all through an intuitive interface that's as easy to navigate as their favorite app.

Faster Time-to-Value

Let's dive into a world where higher-fidelity alerting becomes effortless for security architects using next-gen SIEM. By parsing data in a consistent format and providing out-of-the-box detections and correlation rules, detection engineering is a breeze. Plus, next-gen SIEM provides customizable dashboards to address unique monitoring and compliance requirements.

Next-gen SIEM's cloud-native architecture offers a transformative approach, significantly reducing management overhead and enabling quicker troubleshooting that saves valuable time for security architects. These advanced platforms are purpose-built to effortlessly manage massive data volumes, showcasing an impressive capability to process up to 1 petabyte of data per day. This supports real-time monitoring of data volumes and telemetry health, ensuring optimal SOC performance.



Of course, in real life, things are bound to have hiccups. That's why architects receive alerts for any data onboarding issues, ensuring smooth operations and proactive management of potential challenges. This streamlined approach not only enhances efficiency but contributes to a substantial reduction in TCO, making next-gen SIEM a game changer for modern security operations.

Threat Hunters

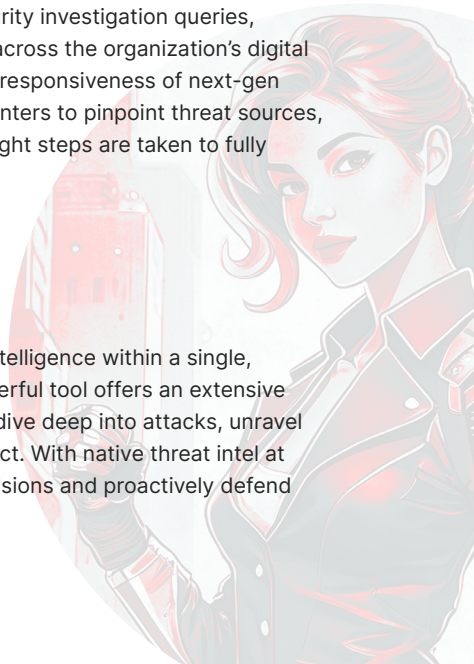
Threat hunters hold a crucial role within the SOC — their driving mission is to uncover and mitigate advanced cybersecurity threats that may be lurking undetected within the environment. Navigating complex digital landscapes and uncovering malicious activities requires skill and speed. It's essential for threat hunters to have the right tools that support their expertise and enable them to act swiftly. Next-gen SIEM equips them with advanced analysis, AI-driven insights and automation specifically designed to enhance their capabilities and adopt a proactive approach in fortifying their organization's security posture.

Finding Advanced Threats Faster and More Easily

Next-gen SIEM 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, empowering them to expertly root out hidden threats across the organization's digital estate. With powerful and fast search capabilities, the responsiveness of next-gen SIEM eliminates latency and delays, enabling threat hunters to pinpoint threat sources, identify the root cause of an incident and ensure the right steps are taken to fully remediate it.

Seamless Access to Native Threat Intelligence

Threat hunters can seamlessly pivot to native threat intelligence within a single, intuitive console provided by next-gen SIEM. This powerful tool offers an extensive library of data insights, empowering threat hunters to dive deep into attacks, unravel their methods, grasp their scope and gauge their impact. With native threat intel at their fingertips, threat hunters can make informed decisions and proactively defend against evolving threats.



CISOs

CISOs play a central role in shaping and safeguarding their organizations' cybersecurity strategies amidst ever-evolving threats. Beyond technical expertise, they need the right insights, visibility and data to drive executive-level risk management and guide board-level decision-making. Leveraging next-gen SIEM capabilities will equip CISOs with cutting-edge SOC capabilities, propelling their security posture forward and elevating their role to that of an executive risk manager.

Security Consolidation

Next-gen SIEM modernizes the SOC and elevates an organization's security profile by consolidating security tools and transforming operations from manual to automation-first, AI-driven processes. By centralizing security operations on a unified platform, next-gen SIEM reduces complexity and administrative overhead, enabling CISOs to focus on strategic initiatives and enhance overall cybersecurity posture. This AI-native SOC platform with converged solutions replaces disparate point products — like legacy SIEM, SOAR, EDR, identity protection and more — significantly enhancing threat detection and response capabilities and ensuring proactive defense against evolving cyber threats.

Moreover, next-gen SIEM lowers TCO and enhances operational efficiency by streamlining operations and reducing complexity. CISOs can optimize resource allocation and improve return on investment (ROI) for security investments, maximizing the value of cybersecurity initiatives within the organization. This improved efficiency allows CISOs to focus on strategic initiatives and align cybersecurity efforts with business objectives, ultimately strengthening the organization's overall security posture and resilience against cyber threats.

Empowering Informed Risk Management

Next-gen SIEM provides CISOs with invaluable insights into their organization's security posture, empowering them to make informed risk management decisions. By offering a comprehensive view of threats and vulnerabilities, next-gen SIEM enables CISOs to effectively communicate security performance to fellow executives. This enhanced understanding of security posture facilitates board-level discussions and strategic planning, ensuring that risk management decisions align with business objectives and priorities.

Future-proofed Security and Reduced Risk

Next-gen SIEM is designed to handle growing log volumes and tomorrow's threats. With advanced detection and proactive security measures built in, next-gen SIEM significantly reduces the risk of a breach, enhancing overall cyber resilience and safeguarding critical assets and data.

What We Covered

In our exploration of modern security operations within a SOC, we've highlighted the critical roles of security practitioners, architects, threat hunters and CISOs. Each member plays a pivotal part in defending against cyber threats, from monitoring alerts and designing robust defense strategies to proactively hunting for advanced threats and guiding executive-level risk management.

Next-gen SIEM emerges as a transformative solution, empowering SOC members to excel in their roles. For security practitioners, it simplifies alert management and automation, freeing up time for high-priority investigations. Security architects benefit from streamlined data onboarding and management, optimizing resource allocation and reducing operational overhead. Threat hunters can leverage powerful search capabilities and native threat intelligence to swiftly root out hidden threats. And CISOs gain invaluable insights into security posture, enabling informed risk management decisions and strategic planning to strengthen the organization's cybersecurity posture.

Through next-gen SIEM, modern security operations become more efficient, proactive and aligned with business objectives, ensuring robust protection against evolving cyber threats.

Chapter 6

Considerations for Selecting Your Next-Gen SIEM

While businesses are tied to scheduled cycles for financial reporting and performance reviews, cybercriminals are like sprinters in a perpetual race, always on and launching new cyberattacks. It's a relentless scenario where the SOC — as a central function within the business — needs to evolve just as swiftly as the adversaries it defends against.

Cyber threats do not wait for scheduled upgrades or budget cycles — they require immediate attention and proactive defense measures. By prioritizing the adoption of a next-gen SIEM, you can empower your SOC to stay ahead of threats and capitalize on the transformative benefits of a highly efficient and effective security team.

But security and risk management leaders have many competing priorities, and deciding when to invest in new tools can be a challenge. Ultimately, the key is to assess the specific outcomes your security operations will achieve by implementing next-gen SIEM. This involves identifying exactly how and where a next-generation SIEM will make a significant impact and move the needle in your organization. Understanding the potential benefits will provide the motivation needed to prioritize and drive the project forward.

Ready to get motivated? Let's dive into the important factors to consider when choosing a next-gen SIEM and assessing its contribution to your SOC's mission. We'll take a close look at desired outcomes and key requirements. Spoiler alert: Next-gen SIEM will give your SOC a high-tech upgrade that even James Bond would envy.

Focus on an Outcomes-Driven Approach

To ensure success with your next-gen SIEM, ensure you focus on desired outcomes instead of getting hung up on speeds and feeds. Consider some of the following outcomes as you navigate the selection of a next-gen SIEM.

Security Outcomes

When adopting a next-gen SIEM, the aim is to fortify your organization's security posture with enhanced visibility, more accurate detection, and faster investigation and response. **You should look for:**

- **Stronger posture for your organization**
- **Enhanced visibility with a unified platform**
- **Faster MTTD and MTTR**
- **More accurate threat detections and lower false positives**
- **Enhanced analyst time efficiency, productivity and skill development**

Business Outcomes

Let's talk dollars and sense — adopting a next-gen SIEM not only strengthens cybersecurity but has far-reaching benefits across the business, including benefits for functions like IT, risk and compliance. **You should look to achieve:**

- **Enhanced collaboration between security and IT functions, fostering improved communication for streamlined workflows and effective incident response**
- **Support for proactive risk management strategies to stay ahead of emerging threats and regulatory requirements**
- **Improved TCO from factors like cloud-native architecture, reducing deployment and operational overhead, and data retention cost considerations**
- **Fast time-to-value with simplified deployment, prebuilt quality detection policies and fast onboarding**

Define Your Requirements

Selecting the right next-gen SIEM is critical for optimizing value for your SOC. There are a lot of capabilities in these robust platforms, and your process should start by defining your organization's prioritized requirements that meet your specific TDIR needs.

By clearly defining and prioritizing these requirements, you can make a well-informed decision that aligns with your organization's objectives and growth trajectory. Consider evaluating the SIEM in the following key areas:

Part of a Unified Platform

A next-gen SIEM cannot live in isolation. Choose a solution that is part of a unified platform that consolidates key components of your security stack, such as endpoint, identity and cloud workload protection. Ideally, this platform should also leverage a single agent and be architected using a common schema to power uniform data flows and analysis without requiring extra collectors or processing. This is a surefire way to achieve your desired security and business outcomes without having to worry about cumbersome implementation processes.

Broad Integrations Ecosystem Across Categories and Your Relevant Vendors

A next-gen SIEM solution excels in providing comprehensive visibility by ensuring accessibility to every critical data source for in-depth analysis and correlation across diverse environments. It seamlessly ingests data from various sources — such as security solutions, applications, endpoints and network packet information — to provide a holistic view of the environment.

A next-gen SIEM must offer seamless integration with public and private cloud platforms such as AWS, Microsoft Azure and Google Cloud. This capability extends its reach for efficient data gathering and advanced threat analytics across multiple clouds.

By integrating with a broad range of categories and vendors relevant to your organization, a next-gen SIEM enables enhanced visibility and threat detection capabilities across the entire ecosystem. This comprehensive approach ensures a streamlined and robust defense against emerging threats, supporting proactive security measures and rapid incident response.

AI-powered Analytics and Out-of-the-Box Content

Step into the future with a next-gen SIEM that's fueled by cutting-edge AI, ML and behavioral analytics. These capabilities decode the language of security threats with unmatched precision, illuminating the path to enhanced accuracy and deeper insights into security entities.

Imagine a central command center for your SOC where advanced analytics deliver actionable intelligence, allowing security teams to stay one step ahead of cyber adversaries.

Next-gen SIEM doesn't stop there — the ideal solution comes equipped with a treasure trove of out-of-the-box content and detection policies. These policies are like ready-made tools, ensuring high-quality threat detections right out of the gate. And if your security landscape is as unique as your fingerprint, fear not — the platform should let you customize and fine-tune these policies to fit your needs, enhancing your defense strategy with tailored precision.

Performance and Scalability

The SIEM is the source of truth for the SOC, so scalability is paramount. The next-gen SIEM solution must scale effortlessly to ingest numerous data sources and support big data analytics without hesitation or strain. Look for a cutting-edge cloud-native solution that offers petabyte scalability, sub-second latency and ultra-high search performance.

The SIEM solution plays a pivotal role and should be highly responsive to support security analysts with triaging and investigating while continuously monitoring and analyzing large data volumes. It should also perform a search query across multiple datasets simultaneously. This capability, known as federated search, empowers real-time retrieval of information from various siloed data sources through a single search, significantly enhancing the efficiency and agility of cybersecurity operations.

Retention and Storage

Next-gen SIEM continues to play a key role in forensics, audits and compliance. To ensure you can access your data for these scenarios — potentially going back multiple years — look for a SIEM that offers economical storage at scale without requiring you to adopt additional infrastructure or architecture requirements.

Cloud Deployment

The evolved next-gen SIEM has a cloud-native architecture. This not only reduces deployment complexities but delivers cost savings in operations and management overhead, marking a significant leap forward in cybersecurity efficiency. With this approach, you'll benefit from not having to handle the setup or management of the SIEM software.

By adopting a cloud-native SIEM solution, you can reduce the time and expertise required for deployment and ongoing maintenance. This significantly lowers implementation costs and operational overhead, allowing your team to focus on harnessing the SIEM's advanced capabilities for enhanced security and threat detection.

Supported Migration and Deployment Process

Transitioning to a next-gen SIEM involves a critical migration process that must be supported by the chosen solution. Look for a SIEM vendor that offers comprehensive migration assistance, ensuring a smooth and efficient transfer of existing data and configurations.

A deployment process should include:

> **Data onboarding** that helps bring log data into the SIEM, parse it and process it, enabling detection, monitoring and search

> **Out-of-the-box security content**, including threat intelligence, correlation rules, detections across all data sources — including endpoint, identity and cloud data — prebuilt dashboards and more

> **Training and enablement** sessions for your security team that help them ramp up in the platform and familiarize themselves with the next-gen SIEM functionalities and workflows

> **Ongoing support** and guidance throughout the migration process to address any challenges or issues that arise

Market Recognition

Selecting a vendor with a strong track record instills confidence in the reliability, effectiveness and long-term viability of the next-gen SIEM solution. Look for a vendor with a rock solid reputation in the industry — you want one with the badges of honor, backed by industry validation, awards and rave reviews from happy customers. It's like choosing your own cybersecurity Avenger — you want the best of the best to defend your digital universe.

Start by researching the vendor's reputation within the cybersecurity community. Seek feedback from industry peers and analysts to assess their standing and reliability. Additionally, consider vendors with proven defenses validated by third-party tests — such as MITRE Engenuity ATT&CK evaluations — and industry certifications like SOC 2 Type II and ISO 27001. This demonstrates their commitment to security best practices. Awards and recognition are also indicative of vendor excellence and innovation. Check if the vendor has received accolades for their SIEM solution, highlighting their ability to deliver cutting-edge technology and customer satisfaction.

Lastly, request customer references to gain insights into real-world experiences with the vendor's SIEM solution. Understanding how other organizations have benefited from the vendor's offerings can provide valuable insights for your decision-making process.

What We Covered

The urgency to evolve your SOC and adopt a next-gen SIEM solution cannot be overstated. Cyber adversaries are constantly innovating, launching new attacks and exploiting vulnerabilities. It's essential for SOCs to operate with agility and resilience so they can defend against emerging threats in real time.

By identifying use cases, prioritizing outcomes and defining requirements, your SOC is poised for a high-tech upgrade that will fortify security, enhance collaboration and elevate your organization's resilience against cyber threats. With a strategic focus on outcomes, you'll harness the full potential of next-gen SIEM and usher in a new era of cybersecurity excellence for your SOC and beyond.

Chapter 7

Transforming Your SOC with CrowdStrike Falcon Next-Gen SIEM

Working in the fast-paced world of security can be intense, and having a next-gen SIEM in your organization's toolkit can be a game changer. If your SOC currently operates without a SIEM or is struggling with the constraints of a legacy system, prioritizing a transition to an evolved next-gen SIEM is essential.

The security market evolves rapidly, so it's important to partner with a next-gen SIEM vendor that's at the forefront of innovations to adapt and stay ahead of emerging threats. For that reason, leading organizations around the world choose CrowdStrike.

Powering the Converged, AI-Native SOC

CrowdStrike Falcon® Next-Gen SIEM unifies data, threat intelligence, AI and workflow automation to stop breaches. It delivers more capabilities and up to 150x faster search performance than legacy SIEMs at up to an 80% lower total cost of ownership. Built from the ground up around a modern security analyst experience, Falcon Next-Gen SIEM consolidates AI-powered detections, investigation workflows and recommended response actions across all data on one platform managed through a single console.

Your team can detect and respond faster than you ever thought possible with real-time alerts, live dashboards and world-class intelligence. Your threat hunters can scour petabytes of data at blazing-fast speed with index-free search. AI features transform your entire SOC team into experts by correlating threats with adversary behavior to reveal the timeline and impact of an attack and automating manual investigation steps. What took hours or days now takes minutes — and years of human expertise will help power every decision your team makes.

Unify Your SOC Operations on One Platform

With Falcon Next-Gen SIEM, you can safeguard your business with industry-leading, comprehensive security from the company that understands adversaries better than anyone. You can rest easy knowing experts from the world's top managed detection and response provider are working around the clock for you.

And for the first time ever, your team can leverage one unified data platform to hunt down and eliminate threats and address the compliance obligations and security challenges you face.

Falcon Next-Gen SIEM empowers your organization to:

> **Achieve instant time-to-value** with critical data already in the CrowdStrike Falcon® platform and easily extend data collection to third-party data sources

> **Reduce mean time to respond** and say goodbye to tedious tasks with workflow automation

> **Coordinate response** across your infrastructure and drive any endpoint remediation action through tight integration with the Falcon agent

> **Slash SOC costs** by consolidating tools and streamlining operations on a single-agent, single-platform architecture

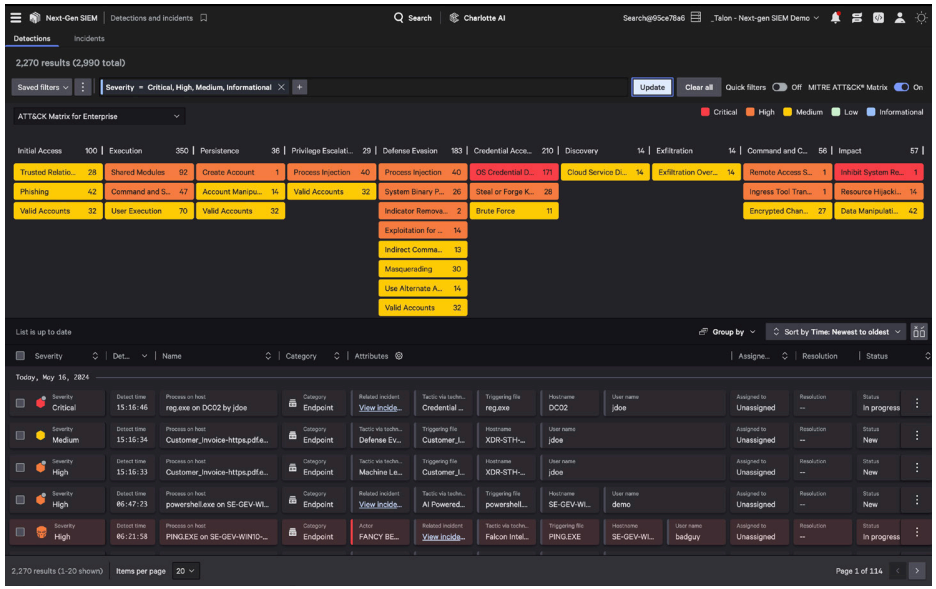


Figure 2. Falcon Next-Gen SIEM helps pinpoint threats with 360° visibility and high-fidelity detections

Leading Capabilities that Simplify and Advance Your SOC

Falcon Next-Gen SIEM reimagines security operations by delivering a cloud-native, petabyte-scale platform that gives you unprecedented visibility across your entire digital estate. The lightweight Falcon agent simplifies data collection across endpoints and workloads, and an expanding set of data connectors harnesses the potential of all of your security tools and data.

Falcon Next-Gen SIEM lets you 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 and collaborate instantly to quickly take action.

> **Generative AI, the ultimate force multiplier:** Elevate the skill level of your entire team by harnessing the power of generative AI to prioritize, enrich and summarize incidents in plain language.

You can 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 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.

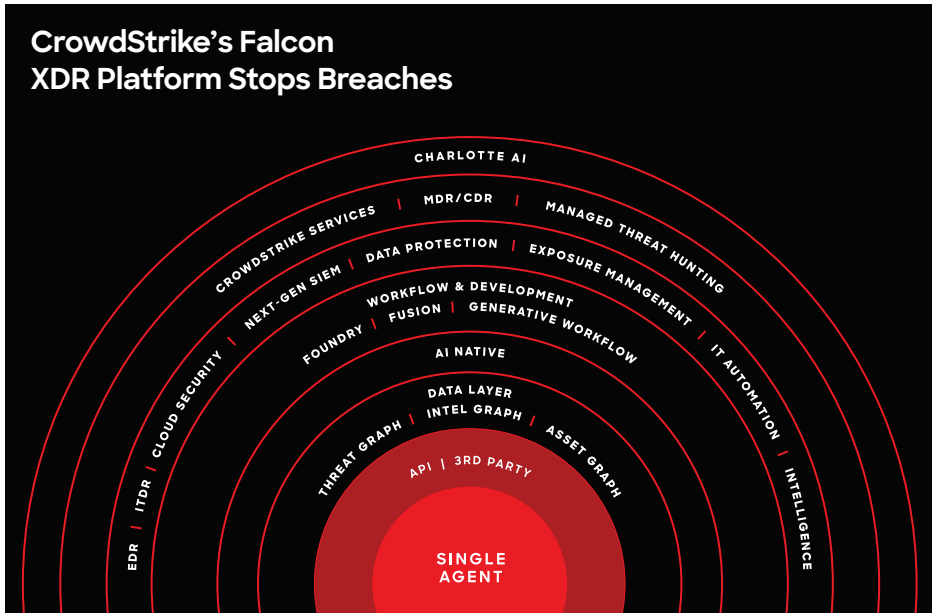
[16] Performance measured against two leading security logging platforms evaluating the speed to query DNS requests to top abused domains.
[17] Based on a benchmark report conducted by GigaOm
[18] Sub-second latency measured across all Falcon LogScale customers.
[19] IDC White paper: Why Customers Choose CrowdStrike for Cybersecurity Consolidation

Up to
150x
faster search to accelerate investigations[16]

1PB/ day
data ingestion at massive scale[17]

<1 sec
latency, the time required to process incoming data[18]

Up to
80%
savings per year versus legacy SIEM solutions[19]



Falcon Next-Gen SIEM drives the convergence of security, data, automation and AI to cut complexity and stop breaches.

CrowdStrike Falcon Next-Gen SIEM enables:

Visit the Falcon Next-Gen SIEM page or request a free virtual test drive.

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.