



8 Things Your Next SIEM Must Do

CrowdStrike eBook

Copyright 2023 CrowdStrike, Inc.

Cybersecurity is constantly evolving in response to emerging threats, customer demands and technological breakthroughs. Nowhere is this transformation more apparent than in the domain of security logging and analytics. Since the term SIEM – or security information and event management – was first coined in 2005, the SIEM product category has adapted and reinvented itself multiple times, while subsuming a number of other technologies along the way.

Early SIEM tools laid the foundation for today's full-featured threat detection and incident response platforms that now serve as the command centers for most enterprise SOCs. But while SIEMs have matured, adding an array of capabilities to outsmart adversaries, many are still shackled by decades-old architectures that hinder search speed, scale and efficiency. And now, a new wave of industry trends is set to upend the SIEM and log management markets once again. Let's take a look at the changes forcing organizations to rethink their security logging strategies.

Log Data Is Expanding Faster than IT Budgets

Data is growing exponentially, with the global datasphere expected to reach 180 zettabytes by 2025,¹ and overall data growing at an impressive compound annual growth rate (CAGR) of 23%.² As data volumes increase, log volumes increase too.

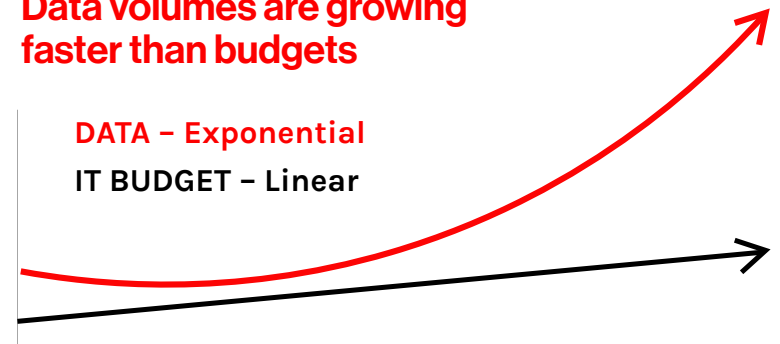
Limited financial resources are forcing teams to grapple with the task of logging and retaining their log data. And these problems are likely to worsen. In its latest monthly forecast for Worldwide IT Spending Growth, IDC forecasts overall growth in constant currency of 4.8% to \$3.27 trillion in 2023.³

SIEMs empower SecOps teams to detect, investigate and hunt for threats. But to be successful, teams need multifaceted data from countless sources. The more data SecOps teams collect, the more likely they can uncover sophisticated attacks, identify the root cause of incidents and fend off fast-moving threats. The consequences of not logging everything are blind spots and missed attacks.

As a market trend, the unmitigated growth in log data will compel many SecOps teams to opt for more scalable and cost-effective SIEM platforms that can keep up with increasing log volumes.

Data volumes are growing faster than budgets

DATA – Exponential
IT BUDGET – Linear



¹ Total Data Volume Worldwide 2010-2025 - Statista

² Ibid.

³ 2022 IDC Worldwide Semiannual Services Tracker: IT Budget

Threat Hunting and Investigations Are Slowing Down

Hunting for advanced threats can be like finding one specific needle in a needle stack. Hunters must continuously scour through mounds of data to reveal the telltale signs of an attack. To do this, they must be able to perform countless searches quickly. They also need the flexibility to construct advanced queries with regular expressions and gain additional context by enriching data.

Unfortunately, traditional SIEMs and log management systems struggle to keep up with today's performance requirements. SIEMs typically provide index-based searching, but as log volumes and the number of log sources rise, the size of the indexes grows, which bogs down search performance and makes it harder to hunt down and stop attacks before damage is done.

Traditional SIEMs also consume excessive CPU and memory resources when they index incoming data, which not only impacts search speed but also increases latency because data must be indexed before it is available for analysis, alerting and querying.

Many of today's SIEM and logging tools were not purpose-built for speed and performance. As a result, they typically lack critical features such as bloom filters and lightweight tagging. Most were architected over a decade ago and fail to take advantage of modern logging or cloud computing innovations. And if they do support cloud deployment, they struggle to ingest multiple terabytes a day.

Because of the architectural deficiencies of legacy SIEMs, SecOps teams increasingly encounter:

- Slow searches that take minutes or even hours to return results
- A limited number of queries that can be executed simultaneously
- Dropped packets at higher ingestion rates
- High latency and delayed alerts due to indexing data before analyzing it

Attackers won't stand by idly and wait for a logging platform to pinpoint attacks or reveal malicious behavior. Organizations need a better, faster way to detect, investigate and hunt for threats if they want to avoid devastating breaches. SIEMs and log management platforms must be rearchitected from the ground up to maximize performance.



79 minutes
is the average eCrime
breakout time.

**Stopping threats before
they spread requires
speed and intelligence.**

Source: CrowdStrike 2023 Threat Hunting Report

Organizations Are Consolidating Siloed Monitoring and Logging Tools

Another key trend impacting SIEM and log management, as well as cybersecurity in general, is technology consolidation. For years, the standard reaction to any new requirement or challenge was to purchase another product. But this disjointed approach has led to tool sprawl, operational headaches and runaway costs.

The growth of cloud computing has exacerbated this problem by introducing an ever-increasing array of applications and containers to monitor and protect. Organizations are not only continuously rolling out new cloud services, they are provisioning more monitoring tools to track application performance, debug issues and investigate threats. In fact, almost 40% of organizations have deployed 11 or more tools to monitor applications, network and security infrastructure, and cloud environments.⁴

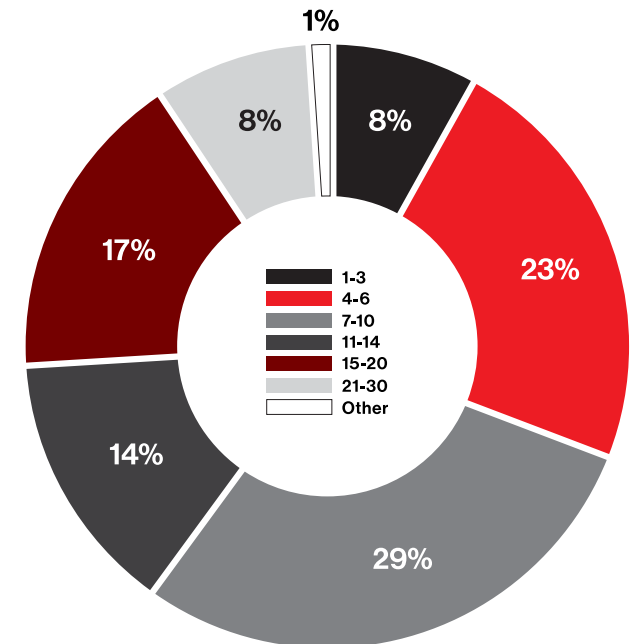
Unfortunately, tool sprawl has created data silos, which in turn has led to inefficiencies, visibility gaps and difficulty correlating data across sources. With the traditional network perimeter dissolving and the attack surface extending to remote users and cloud environments, SecOps teams must expand their visibility to all data and not just a small number of security alerts. By analyzing all data, they can unearth adversaries lurking in the farthest reaches of their network. This boundless visibility helps them identify the root cause and the scope of incidents, and eliminate “dark data” and blind spots.

With the increasing interconnectedness of systems and data, it simply doesn't make sense for SecOps, DevOps and ITOps to maintain siloed data lakes and monitoring tools. Not only is it costly and complex to store the same data in multiple locations, it inhibits teams from collaborating to solve joint problems, such as determining whether a distributed denial-of-service attack caused application downtime. By centrally storing all logs in one place, various groups — from DevOps and SecOps, to fraud analysts to business leaders — can efficiently analyze and correlate data to get the answers they need.

However, the convergence of security and observability is also reinforcing the importance of logging scale and performance. SecOps leaders should carefully evaluate whether their SIEM can collect high-volume data from web servers, cloud services, network devices, endpoints and more. They should test data ingestion rates, search performance and the number of simultaneous queries and users the logging platform can support. Only then can they realize the benefits, cost savings and productivity gains of a centralized data lake, or explore the option for SIEM augmentation.

Overall, industry trends such as the explosive growth in data, the increasing need for speed when hunting and investigating threats, and the consolidation of siloed monitoring tools are changing what organizations should look for when evaluating SIEM and log management platforms.

Number of Monitoring Tools in Use



Source: Tool Sprawl Is Real, Leading to Wasted Money and Lost Opportunity, 451 Research

⁴ 451 Research, Tool Sprawl Is Real, Leading to Wasted Money and Lost Opportunity

8 Things Your Next SIEM Must Do

To stay ahead of evolving security and logging requirements, look for a SIEM that can achieve the following eight objectives.



Reduce incident response time with high-speed search at real-world scale

When responding to an incident, connecting all of the dots and identifying the root cause and scope often require countless queries and in-depth analysis. If each query takes an inordinate amount of time to yield answers — or worse, returns incomplete results or times out altogether — then investigations can stretch on for weeks or months, wasting resources and potentially increasing the financial impact of an attack.

To accelerate investigations, select a SIEM that can quickly scour through your log data and return accurate results. Prior to purchase, your team should perform in-depth testing to assess how long real-world queries take to yield findings. Execute hundreds or even thousands of queries at once to understand which SIEMs crumble under stress. Side-by-side performance tests of SIEMs and security logging tools can help you confidently choose the platform that can keep up with your demanding requirements today and in the future.



Empower your threat hunters to cut through the noise with flexible, advanced queries

Your threat hunters must be able to sift through mounds of data nimbly to find what they are looking for, and this typically means constructing complex queries that filter out irrelevant data. To do this, your SIEM should not only scale to collect large volumes of data, it should also include a mature query language with rich syntax and support for aggregation, statistical functions, data manipulation and joining datasets. It should support regular expressions for advanced filtering and efficient pattern matching. Your SIEM should also provide free text search to let analysts of all experience levels quickly scan through your data for a specific value. In addition to letting your team build, schedule and save queries, your SIEM should offer a broad set of pre-defined queries through a marketplace.

Modern attacks involve multiple steps spanning multiple systems. To get a complete picture of an attack, your team must be able to search across diverse datasets and log formats swiftly. This makes a mature query language a must-have for any SIEM platform. When considering solutions, don't just evaluate query speed — review the breadth of query functions and the flexibility of the query language.



Detect threats instantly with real-time alerting

Every second counts when responding to an attack. To stop breaches or limit their impact, security teams are advised to follow the 1-10-60 rule: Detect threats within one minute, understand them within 10 minutes and respond within 60 minutes. Unfortunately, many teams cannot meet the 1-10-60 rule because their SIEM does not generate alerts in real time.

Older SIEMs often index incoming data, which requires extra processing before making data available for alerting and search. In fact, indexing can delay alerting for 60 seconds or more, making it impossible for SecOps teams to meet the 1-10-60 rule and minimize the risk of a breach.

Some SIEM vendors add real-time alerting as an afterthought by allocating computing resources for a limited number of alerts instead of architecting a SIEM for real-time alerting. However, advanced SecOps teams often need to be able to detect hundreds or even thousands of threats in real time, and this becomes prohibitively expensive to implement with legacy SIEM products.

To cut detection and response times, seek out a SIEM that offers real-time alerting. If it provides near-instant access to streaming data, you'll be able to detect attacks, spot problems and react before damage is done. High-performance, index-free logging platforms also allow you to search and visualize streaming data with sub-second latency. This means you can monitor performance in real time with live charts and hunt for malicious behavior without frustrating delays. With a SIEM platform that supports streaming data and real-time alerts, you can stop attacks faster and bolster your security posture.

1-10-60 Rule

- Detect within **1 minute**
- Investigate within **10 minutes**
- Respond within **60 minutes**

4

Scale to collect large volumes of data without ingestion bottlenecks

With the ever-increasing growth in data, organizations must plan ahead to ensure their SIEM not only meets current scalability requirements but can also handle future requirements with ease. Some SIEMs are simply incapable of ingesting a high volume of log data, resulting in performance headaches or dropped packets when data surpasses a few terabytes a day. Other SIEMs are inefficient, and their escalating software and infrastructure costs prevent SecOps teams from collecting all of the logs they need for security, creating visibility blind spots and increasing the risk of attacks.

As security and observability technologies converge, SecOps, DevOps and ITOps teams can easily collaborate while lowering OpEx and CapEx. But to do so, they must choose a logging platform with the power and capacity to collect all data, not a costly SIEM that can only ingest security alerts and a handful of high-value data sources. Instead, teams should opt for a scalable log management platform that can unify all data, including high-volume telemetry, to provide flexible data correlation, 360-degree visibility and reduced operational complexity.

5

Integrate with a best-in-class security ecosystem for threat detection and response

Over the past two decades, SIEMs have evolved dramatically. What began as basic, on-premises logging solutions that collected and aggregated events and alerts have transformed into powerful, full-featured threat detection and response platforms. They now offer long-term data retention for compliance as well as a range of service offerings that deliver managed detection, response and threat hunting.

While most SIEMs are still log management platforms at heart, SecOps team should consider integrated or complementary capabilities such as user behavior analytics, detection and response, and threat intelligence. However, rather than simply choosing the product that checks the most boxes in terms of features, organizations should carefully evaluate the merits of each of these add-on products or services individually.

When assessing threat intelligence services, opt for intel sources that regularly correlate trillions of events each day. When considering user behavior analytics, test whether the solution offers accurate detection with integrated response options, like stepped-up authentication, or if it just generates low-fidelity alerts. And when looking at integrated features like endpoint detection and response, choose industry-leading solutions and not inferior SIEM add-ons. Choosing exceptional products and services from a trusted leader in cybersecurity will give your team the defenses needed to outwit adversaries.



Support flexible cloud and self-hosted deployment options

IT and security teams everywhere are embracing the cloud, prioritizing cloud-based platforms above on-premises solutions to cut costs, improve uptime and performance, and reduce overhead. This cloud-first philosophy extends to SIEM and log management.

However, due to a complex web of compliance and data residency mandates, not all organizations — such as those in far-flung corners of the globe or with unique operating requirements — can adopt cloud-delivered SIEMs. Therefore, when evaluating logging platforms, look for ones that offer versatile deployment options, including cloud and self-hosted deployment.



“By 2023, 90% of SIEM solutions will offer capabilities delivered exclusively in the cloud — log storage, analytics and incident management, to name a few — up from 20% in 2020.”

- Gartner®



Enable you to log everything affordably

One of the most important criteria when selecting a SIEM is the price. All too often, high costs force security teams to limit the types of log data they collect or periodically age out log data. As a result, blind spots can multiply, making it easier for advanced adversaries to penetrate IT systems, traverse networks and avoid detection. If organizations aren't able to log everything, launching investigations can resemble a quest for the proverbial elusive needle, without knowing if the needle even exists.

When evaluating SIEM platforms, compare the subscription price as well as the overall total cost of ownership (TCO), including infrastructure, deployment and operating costs, to determine which solutions meet your budget and data retention requirements.



Eliminate hidden costs with transparent, predictable licensing plans

Procurement considerations don't end with your initial quote. In addition to evaluating upfront costs, carefully consider licensing plans, as well as additional services you may need to purchase in the future. Does the vendor offer straightforward and predictable licensing plans, or will you get surprised later with unanticipated fees? Will you need to pay separately for API or query consumption? Will you be goaded into purchasing expensive enterprise security add-ons?

You must also factor in future logging needs. SIEMs and logging products that initially look affordable may balloon in cost as data volumes increase, especially if you opt for self-hosted solutions with hefty hardware and storage costs. Better yet, find vendors that offer unlimited ingest plans, giving you a realistic way to log all of your data.

To avoid future unforeseen expenses, choose a product that offers predictable licensing and imposes minimal maintenance costs.

Replace Your SIEM with CrowdStrike Falcon LogScale

If your current SIEM is falling short in terms of addressing key security and logging requirements, then it's time to consider alternative solutions.

Join leading organizations around the world and choose [CrowdStrike® Falcon LogScale™](#), a modern log management platform purpose-built for unbeatable scalability, performance and exceptionally low latency. Falcon LogScale makes data onboarding a snap with the integrated [CrowdStream](#) observability pipeline, the Falcon LogScale Collector agent, and out-of-the-box content packs available in the [Falcon LogScale Marketplace](#). Its blazing-fast search, real-time alerting and customizable dashboards allow you to retain data as long as you need for compliance, threat hunting and historical investigations — at a fraction of the cost of traditional SIEM products.



“Falcon LogScale allows us to see what’s happening in our systems faster than before. At any given point, we have around 2,500 searches happening, and most complete in seconds.”

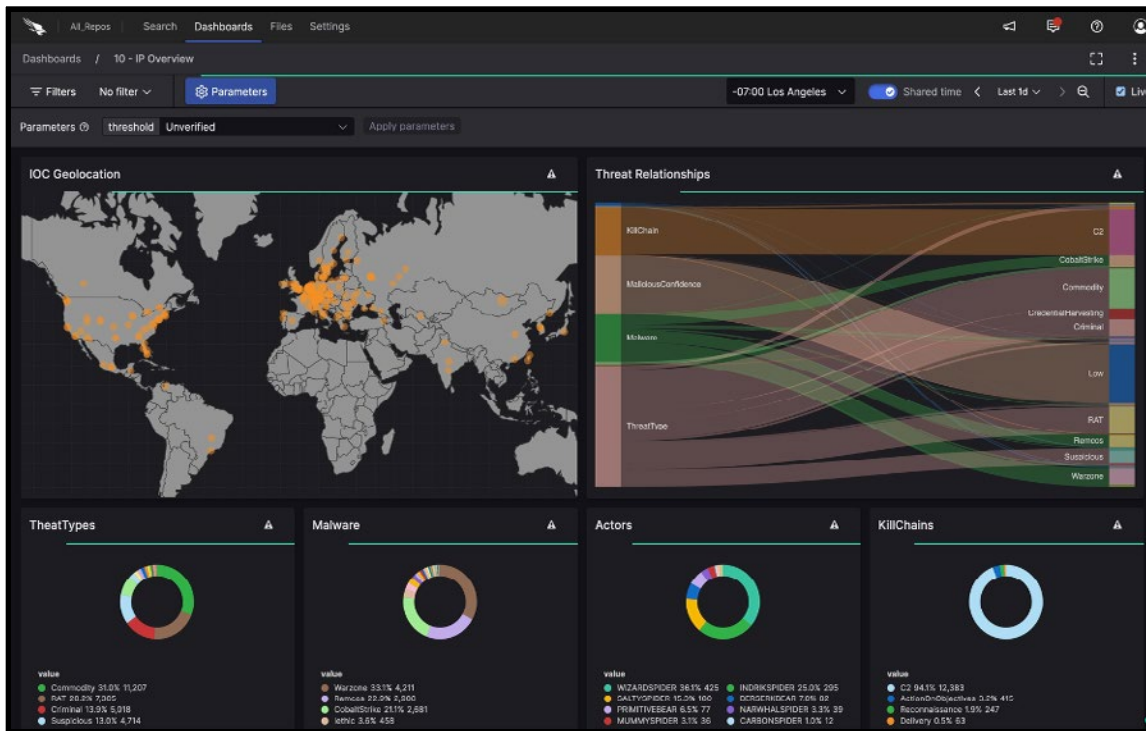
[Stian Brattlie](#), Systems Engineer, SpareBank 1



Maximize Security and Visibility by Logging Data at Petabyte Scale

With its unique index-free architecture and advanced compression technology, Falcon LogScale minimizes the computing and storage resources required to ingest and manage data, while delivering the power and speed your team needs to stop threats.

With Falcon LogScale, you can log everything to answer anything, while cutting costs by [up to 80%](#)⁵ compared to alternative SIEM and log management solutions. Its vast scale and affordable price let you avoid making tough tradeoffs between cost, how much data you can collect and how long you can store it — because with Falcon LogScale, you can retain petabytes of data for months or years.



Falcon LogScale provides customizable dashboards with drill-down capabilities that allow users to view underlying data with a single click.



“With Falcon LogScale, our logs appear instantly. It's not a visible delay where we're waiting minutes, like with before. Now we can search three billion events in under a second.”

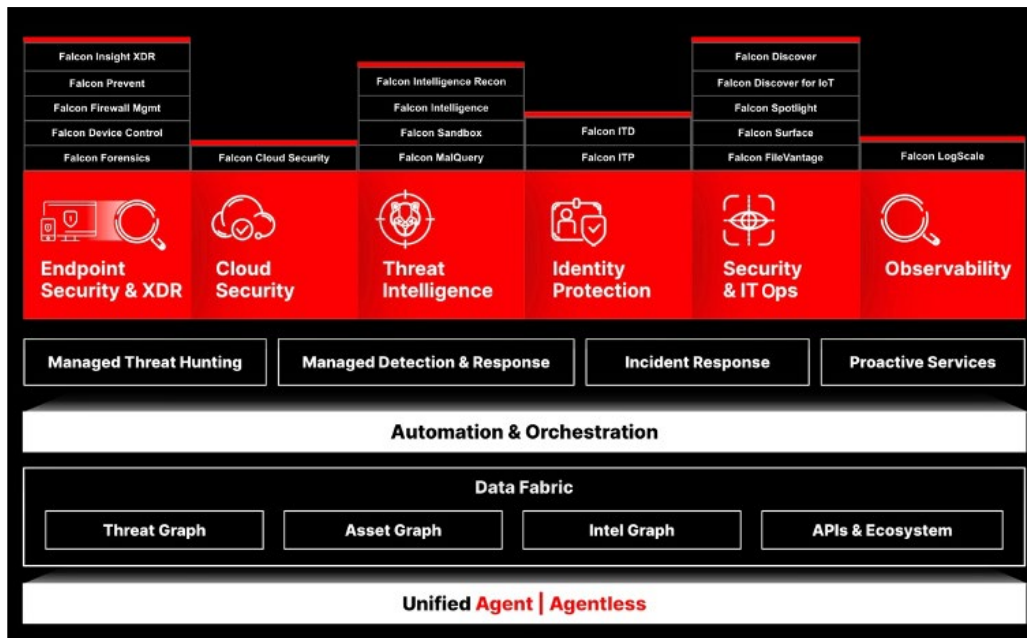
Sumit Bhargava, [Divisional Assistant VP,](#)
Great American Insurance Group

⁵ Cost savings estimate determined by product and infrastructure cost analysis performed by CrowdStrike and validated by CrowdStrike customers. See the [Falcon LogScale online savings calculator](#) for more information.

One platform. Complete protection.





Falcon LogScale is a key part of the CrowdStrike Falcon® platform. Powered by cloud-scale AI, the Falcon platform delivers superior protection and performance, reduced complexity and immediate time-to-value through a range of threat detection, threat intelligence, endpoint security and orchestration products. Combined with CrowdStrike Falcon® Identity Threat Protection, you receive adversary-focused user behavior analytics with integrated response.

In addition, you can augment your team with continuous, hands-on log management expertise from [CrowdStrike Falcon® Complete LogScale](#). By accelerating time-to-value with custom dashboards, workflows and guidance on operationalizing your log data, Falcon Complete gives your team insights to proactively identify threats and keep your organization secure.



The Total Economic Impact

Through five customer interviews and data aggregation, Forrester concluded that Falcon LogScale has the following three-year financial impact.⁶

-  ROI **210%**
-  Benefits Present Value **\$9.9M**
-  Net Present Value **\$6.7M**
-  Payback **< 6 Months**

Ready to learn more about Falcon LogScale?

Attend a [Falcon Encounter Threat Hunting Lab](#) to take your threat hunting and investigation skills to the next level, and get hands-on with Falcon LogScale and Falcon Long Term Repository.

⁶ Forrester Consulting, The Total Economic Impact™ of CrowdStrike Falcon LogScale, 2022



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.**

Follow us: [Blog](#) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

© 2023 CrowdStrike, Inc. All rights reserved.