CROWDSTRIKE | Cribl

CrowdStrike and Cribl
White Paper

THE STATE OF THE SIEM MARKET

Overcoming the Data Deluge: Modernizing SIEM for Today's Threats

Security has a data problem. With log volumes skyrocketing, security teams are drowning in data, and legacy security information and event management (SIEM) solutions are buckling under the pressure. Many of these outdated solutions, designed for simpler on-premises environments, simply can't keep up, leading to ingestion bottlenecks and painfully slow searches. As security teams struggle with rising SIEM costs and expanded regulatory requirements, they must choose which data to prioritize and which to ignore, creating dangerous blind spots that adversaries are quick to exploit. According to a Cribl report, 63% of companies surveyed said their data management strategies will only be sustainable for the next three years, with one-third saying their strategies won't last beyond 12 months.[1]

Meanwhile, adversaries move with alarming speed, leveraging malware-free and identity-based attacks to blend in and avoid detection. But security teams beleaguered with legacy SIEMs spend inordinate amounts of time wrangling data across patchwork cloud and on-premises architectures and pivoting across disjointed tools. In a landscape where the average eCrime breakout time observed in 2023 was just 62 minutes, organizations need a SIEM solution capable of real-time detection and streamlined response, or they risk falling behind.[2]

3.7TB

median volume of data ingested per day[3]

83%

of organizations ingest over 1TB of data per day[1]

SIEM Market Turmoil Sets the Stage for Change

In recent years, SIEMs have evolved from basic log management solutions to next-gen platforms built in the cloud and powered by AI and automation. Moreover, organizations are increasingly seeking to consolidate their tools and break down silos across their environment.

(1) Cribl, Navigating the Data Current

(2) CrowdStrike 2024 Global Threat Report

(3) IDC, SIEM Data Ingestion: Comparing 2021 with 2024, Doc #US52617724, September 2024

In turn, vendors are pursuing mergers and acquisitions in a scramble to offer all-in-one platforms that can handle both on-premises and cloud environments. Legacy SIEM vendors, unable to keep pace with the demands of growing log volumes and the shift to cloud architecture, have struggled to maintain relevance. Faced with scalability challenges, many have turned to acquisitions as a lifeline to stay competitive in a rapidly evolving market. The result? A more concentrated market with fewer players but more scalable and comprehensive solutions.

"Gartner has seen evidence that the SIEM market itself has been disrupted by external forces that cause clients to rethink the role of a SIEM, and how to select the best technology for them."[4]

The State of SIEM

As organizations face an influx of security data from endpoint, cloud and identity systems, **data pipelines** have emerged as the backbone of modern security operations. Challenges with legacy SIEM solutions continue to burden security teams striving to keep up with the speed of modern attacks.

Modernization	Data Management	Automation and Compliance	Migration Hesitancy
According to IDC, ease of management (configuration and maintenance) was the top reason organizations recently replaced or augmented their SIEM.[5]	Legacy SIEM platforms often follow a "one-size-fits-all" storage model, which is no longer sufficient for handling the diverse types of data generated in modern environments.	Many teams lack the resources and automation needed to keep up with evolving reporting and retention requirements.	According to IDC, 35% of respondents chose to stick with their incumbent SIEM platform after evaluating other options.[3]

Recent research shows the ability to ingest, process and deliver data quickly and efficiently is essential for enabling real-time detection, automation and AI-driven insights. Read on to discover how the next generation of SIEMs — combined with data stream management excellence — is transforming SOCs today.

(4) Gartner® Magic Quadrant™ for Security and Information Event Management. Andrew Davies, Mitchell Schneider, et al., 8 May 2024 (report accessible to Gartner subscribers only). GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.

(5) IDC, Why Do Customers Keep or Replace Their SIEM? Doc #US52342924, June 2024

Platform Consolidation

Environments are more complex than ever before. According to Gartner, complexity is the enemy of security, yet the average organization works with 10 to 15 security vendors and 60-70 security tools in place.[6] Security teams are bogged down by "swivel chair syndrome," shuffling between consoles, chasing false positives and navigating slow, inefficient workflows. Beyond increased security risk, this complexity also drives up total cost of ownership when teams must spend time integrating disparate tools.

"Nearly half of organizations are looking to consolidate threat intelligence; security orchestration, automation, and response (SOAR); NDR; and XDR in some way."[7] — IDC

Many organizations are consolidating their security tools onto a single platform to overcome complexity, reduce risk and total cost of ownership, and achieve superior security outcomes like faster mean time to respond (MTTR). In fact, over half of organizations surveyed already have consolidation plans underway, with an additional 35% saying they will begin to consolidate by 2025.[5]

Benefits from Tool Consolidation[8]

16%
savings on total tool costs

20%
savings in analyst time

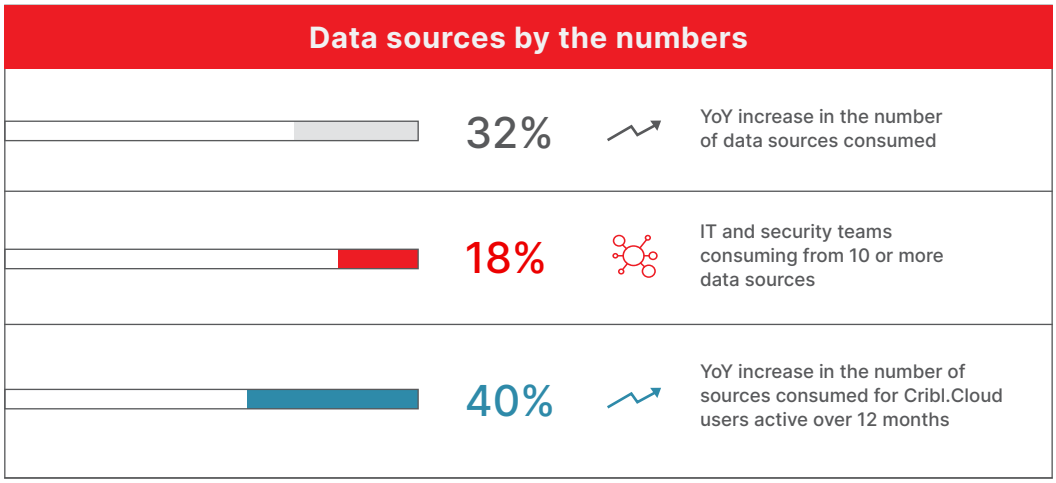
(6) Gartner, Simplify Cybersecurity With a Platform Consolidation Framework, G00781423. Dionisio Zumerle, John Watts, 26 March 2024 (report accessible to Gartner subscribers only). GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

(7) IDC, North American Security Tools and Vendors Consolidation Study: NDR, SOAR, TI, and XDR, Doc #US52303824, June 2024

(8) IDC, North American Tools/Vendors Consolidation Survey, Doc# US52023024, April 2024

Streamlined Data Onboarding

As the volume and diversity of security data grow, IT and security teams are increasingly facing challenges related to data onboarding. In 2024, the number of data sources ingested by organizations has grown by 32% year-over-year, with nearly one-fifth of companies pulling in data from 10 or more sources, including cloud, endpoint and identity systems.[9] This complexity brings significant onboarding challenges, as security teams struggle to integrate and manage these diverse streams efficiently. With each additional data source comes the need for costly configurations and time-consuming integrations, placing a significant burden on teams already stretched thin.



Source: Cribl, Navigating the Data Current

However, the trend toward **SIEM platforms that natively house critical data sources** — like endpoints, cloud telemetry and threat intelligence — aims to address these challenges. The vast majority of data sent to SIEMs comes from the endpoint, so many customers are seeing value from native integration.

(9) Cribl, Navigating the Data Current

Rapid Real-Time Detection

Organizations must ensure that their SIEM solutions can handle the scale and complexity of the data they collect as well as rapidly analyze and detect attacks in progress to stop the breach. When the clock is ticking, security teams are spending far too much time wrangling data, fixing broken data pipelines and chasing false positives — investigating false positives alone can sometimes take security teams up to two hours per day.[10] Cyber threats are evolving quickly, with adversaries increasingly using hands-on intrusion techniques to actively target systems. In 2023, CrowdStrike saw a 60% year-over-year increase in these interactive intrusion campaigns.[12]

Here's what today's security teams are up against:[11]

2 min, 7 sec

fastest recorded eCrime breakout time in 2023

75%

of attacks to gain access were malware-free in 2023

75%

year-over-year increase in cloud intrusions in 2023

From initial access to impact, adversaries deploy a vast range of tactics to outmaneuver defenses. The following heat map shines a spotlight on the leading MITRE ATT&CK® techniques CrowdStrike Falcon® Adversary OverWatch™ observed adversaries employ in each tactic area, July 2023 to June 2024.

(10) Vectra AI, Do SOC Professionals Know They're Spending Almost Two Hours a Day Investigating False Positives?

(11) CrowdStrike 2024 Global Threat Report

(12) CrowdStrike 2024 Global Threat Report

Initial Access	Execution	Persistence	Privilege Escalation
Exploit Public-Facing Application	Command and Scripting Interpreter	Scheduled Task/Job	Process Injection
Valid Accounts	Windows Management Instrumentation	Valid Accounts	Scheduled Task/Job
	Shared Modules	Create Account	Abuse Elevation Control Mechanism
	Exploitation for Client Execution		

Defense Evasion	Credential Access	Discovery	Lateral Movement
Masquerading	OS Credential Dumping	Account Discovery	Remote Desktop Protocol
Disable or Modify Tools	Unsecured Credentials	System Owner/User Discovery	Remote Services
Modify Registry	Brute Force	System Network Configuration Discovery	SMB/Windows Admin Shares
Process Injection	Credentials In Files	System Information Discovery	
Obfuscated Files or Information		Remote System Discovery	
Indicator Removal		Permission Groups Discovery	
Indirect Command Execution		Network Service Discovery	
Valid Accounts		Security Software Discovery	
Rundll32		Network Share Discovery	
Timestomp		Domain Groups	
File and Directory Permissions Modification		File and Directory Discovery	
Deobfuscate/Decode Files or Information			
Abuse Elevation Control Mechanism			

Collection	Command and Control	Exfiltration	Impact
Archive Collected Data	Ingress Tool Transfer		Data Encrypted for Impact
	Remote Access Software		Inhibit System Recovery
	Web Service		
	Application Layer Protocol		
	Proxy		

Source: CrowdStrike 2024 Threat Hunting Report

To detect adversaries early in the cyber kill chain, organizations are adopting unified platforms that bring together endpoint, identity and cloud data for **real-time protection**. With all data residing in the same place, security teams can avoid delays caused by routing data to external SIEMs, ensuring threats are detected and addressed faster.

Organizations also prefer SIEM solutions that offer native integration with threat intelligence to stay one step ahead of adversaries. On top of providing dedicated threat research, leading vendors further refine detections with insights from across their user base, their front-line responders and their managed services. The highest-fidelity detections move beyond mere indicators of compromise to indicators of attack, which use behavioral analysis and rich context to distinguish legitimate from malicious activity.

Independent third-party assessments like the **MITRE Engenuity ATT&CK evaluations** play a critical role in helping organizations evaluate their detection capabilities. In these **closed-book tests**, which simulate real-world attack scenarios without giving prior knowledge of the threat, top-performing vendors set benchmarks for rapid detection speeds. These evaluations showcase the need for organizations to choose solutions with fast, high-fidelity detections to protect their environments.

Security Orchestration, Automation and Response

Once a threat has been detected, security teams need to investigate threats at lightning speed, and analysts desperately need automation to help them sift the signal from the noise. This is where tightly integrated security orchestration, automation and response (SOAR) capabilities shine by automating investigation and response processes to give analysts time back to focus on the threats that matter most.

According to Forrester, 74% of decision-makers report their organizations are turning to SOAR capabilities to streamline manual processes. However, implementing these solutions often proves challenging. Legacy SOAR platforms typically require advanced skills to build playbooks, resulting in low implementation rates of only five to 10 working playbooks used in an organization.[13] Moreover, the use of disjointed IT tools can further complicate the process, making orchestration complex and developing playbooks harder.

(13) Forrester, Best Practices For Automating Security Operations Workflows, August 2023

Here's what today's security teams are up against:[10]

5 to 10

working playbooks for most organizations

41%

of organizations lack the requisite technical skills to manage a SOAR platform

These challenges are not deterring security teams from adopting SOAR capabilities. According to a recent SANS survey, one of the most popular improvements in incident response that organizations are looking to make over the next 12 months is automating response and remediation workflows (41%).[14] Imagine how much higher this number would be if teams could build workflows effortlessly, without complex coding.

The key to effective SOAR adoption and reducing attacker dwell time is intuitive, built-in **workflow automation within the SIEM**. No-code workflow builders make automation easy for analysts without advanced skills, and high-quality, out-of-the-box playbooks and pre-built integrations speed up development. A **unified SIEM and SOAR** experience boosts detection and response with shared visibility, better collaboration through visualizations and a single platform that eliminates the need to switch between multiple tools.

Every SOC is unique, varying in size, industry and specific use cases. Some teams need the flexibility to create third-party integrations or build custom apps for advanced automation. A **purpose-built low-code platform** equips security teams with modern low-code and no-code tools to build custom apps and deploy automation tailored to their needs.

Harnessing GenAI to Elevate Security Operations

To boost efficiency and stop breaches, today's teams need to do much more, much faster than ever before. Generative AI (GenAI) holds the promise of doing exactly that: It can help security teams direct workflows, rapidly triage detections, get answers to pressing questions, add context to investigations and automatically build incident reports.

As security teams evaluate the potential of GenAI to assist in detection, investigation and response, they are focused on achieving measurable **security, operational and economic outcomes**.

(14) SANS 2023 Incident Response Survey

Here's how security professionals are reporting GenAI impacts their priorities:[15]

63%

believe in AI's potential to enhance security measures, especially in improving threat detection and response capabilities

55%

of organizations are planning to implement generative AI solutions this year

Top 3

use cases include rule creation, attack simulation and compliance violation detection

Security leaders are interested in using GenAI to **better detect and respond to advanced attacks** and **improve MTTR and detection fidelity**, and in leveraging assistants to accelerate tasks and uplevel analysts as organizations continue to face a **cybersecurity skills shortage**. However, the true value of GenAI tools depends on their **integration with existing security tools**. Many security teams look for GenAI solutions with seamless integration, as GenAI solutions are only as effective as the tools and data they can access.

Security teams are turning to GenAI to enable users of all skill levels to surface insights from their SIEM and take action with plain-language queries. GenAI empowers analysts with limited knowledge of SIEM query languages to hunt for threats and get instant adversary intelligence, transforming hours of work into mere minutes or seconds.

How CrowdStrike and Cribl Reshape the SIEM Journey

Organizations are modernizing their stacks to achieve faster mean time to detect (MTTD) and MTTR in increasingly complex environments while managing their data needs. Cribl research shows CrowdStrike Falcon® Next-Gen SIEM has become one of the fastest-growing destinations for sending data, with 260% year-over-year growth in 2024 and more organizations sending their data to CrowdStrike's platform.[16] As organizations explore options, integrations between vendors — like Cribl's recent integration with Falcon Next-Gen SIEM — offer a compelling solution for modern security operations.

(15) Cloud Security Alliance, The State of AI and Security Survey Report

(16) Cribl, Navigating the Data Current

Cribl Stream's integration with Falcon Next-Gen SIEM brings a transformative approach to managing security data at scale. By enabling seamless ingestion and flexible routing of data from any source to any destination, Cribl Stream enhances the power of Falcon Next-Gen SIEM, empowering security teams to achieve faster threat detection and response. This integration with Cribl Stream simplifies telemetry management and optimizes data flows, ensuring that high-value data reaches Falcon Next-Gen SIEM for increased operational efficiency and better security outcomes. As organizations adapt to evolving security challenges, the combined capabilities of Cribl Stream and Falcon Next-Gen SIEM provide a scalable, resilient solution that adapts to meet both current and future data needs.

CrowdStream, powered by Cribl, is a separate native platform capability of Falcon Next-Gen SIEM that lets you easily collect and route data from any source using Cribl Stream, the industry's leading observability pipeline. This powerful capability provides an efficient, streamlined approach to integrating data into Falcon Next-Gen SIEM, greatly accelerating time-to-value. It is available at no additional cost for the first 10GB of daily streaming data for Falcon Next-Gen SIEM customers.

With Cribl and Falcon Next-Gen SIEM, organizations can:

- Easily connect and route data from any source into Falcon Next-Gen SIEM while minimizing the complexity and cost of connecting data sources.
- Enhance threat hunting with blazing-fast search and enrichment across all of your data.
- Take advantage of log management at petabyte scale by seamlessly migrating from legacy logging platforms to Falcon Next-Gen SIEM.
- Improve security and compliance postures with features such as data masking, enrichment and selective filtering.
- Select the integration option that best fits their needs, whether that's CrowdStream's native capability or Cribl Stream's enhanced integration with Falcon Next-Gen SIEM.

Achieving Superior Security Outcomes with CrowdStrike and Cribl

4 Min

CrowdStrike delivers rapid MTTD in the MITRE Engenuity ATT&CK Evaluations: Managed Services, Round 2

150x

Faster search performance compared to legacy solutions

Source: Performance measured against two leading security logging platforms evaluating the speed to query DNS requests to top abused domains.

13M+

Detections resolved annually by CrowdStrike Falcon® Complete Next-Gen MDR

Source: Results collected from Falcon Complete customers from the period July 2023-July 2024

75

Hours saved per month from autonomously resolving false positive alerts

Source: Results from a healthcare organization. Individual results may vary by customer.

$500K

Savings achieved through data optimization, reducing 6TB of on-premises legacy SIEM data

Source: Results from a large global enterprise company. Individual results may vary by customer.

95K+

Customer-defined workflows that orchestrate across CrowdStrike modules and third-party tools

Source: Results are based on an aggregate assessment of CrowdStrike Falcon® Insight XDR customers.

20

Net-new log sources onboarded in just a few weeks using Cribl Stream for a global healthcare organization

Source: Results from a global healthcare organization. Individual results may vary by customer.

1 Month

Rapid migration to Falcon Next-Gen SIEM enabled by Cribl Stream, delivering near-instant time-to-value and saving up to six months in deployment time

Source: Results from a large global enterprise company. Individual results may vary by customer.

15K+

Detections in the CrowdStrike Falcon® platform mapped to the MITRE ATT&CK framework

Forging Ahead: The Future of SIEM

As organizations face a surge in data volumes and increasingly sophisticated adversaries, modernizing SIEM platforms is no longer a choice — it's a necessity. The next generation of SIEM tools must provide real-time detection, integrated automation and AI-powered insights to empower security teams to respond swiftly and accurately.

With platform consolidation reducing complexity and blind spots — and GenAI tools offering enhanced threat detection and operational efficiency — security teams can stay one step ahead of attackers. However, success depends on selecting solutions that are deeply integrated with existing tools, reduce manual effort through automation and are backed by specialized cybersecurity expertise.

By embracing these innovations, organizations can build a resilient, future-ready security posture, ensuring they can mitigate threats in real time and optimize their operations for the long term.

See CrowdStrike Falcon Next-Gen SIEM in action in a demo or request a free virtual test drive

Get started with a free Cribl.Cloud trial and process up to 1TB/day into CrowdStrike Falcon Next-Gen SIEM at no cost or schedule a custom demo.

About Cribl

Cribl is the Data Engine for IT and Security, empowering organizations to transform their data strategy. Customers use Cribl's vendor-agnostic solutions to analyze, collect, process, and route all IT and security data from any source or in any destination, delivering the choice, control, and flexibility required to adapt to their ever-changing needs. Cribl's product suite, which is used by Fortune 1000 companies globally, is purpose-built for IT and Security, including Cribl Stream, the industry's leading observability pipeline, Cribl Edge, an intelligent vendor-neutral agent, Cribl Search, the industry's first search-in-place solution, and Cribl Lake, a turnkey data lake. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Cribl: The Data Engine for IT and Security.

Learn more: www.cribl.io

Try now: Cribl sandboxes

Join us: Slack community

Follow us: LinkedIn | Twitter

About CrowdStrike

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

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

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

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/

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

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