The 7 Essential Capabilities of a Data-Driven SIEM

Modern threats demand data-driven security and continuous monitoring

splunk>

Legacy SIEMs are stuck in the past

There's no shortage of ways to collect, store and analyze data, with plenty of on-prem, cloud and hybrid options out there. But turning all that data into actionable intelligence isn't easy. Security incident and event management (SIEM) technology is now over a decade old, and legacy SIEMs just weren't built to keep up with today's constantly evolving security challenges. With a closed environment and a limited range of data available to ingest, legacy SIEM solutions are slow at queries and investigations, and struggle to scale to meet business and mission needs.

Countless organizations that invested in a SIEM solution back in the day had to learn this the hard way. Even after investing precious company resources into ingesting and recording enterprise data, the underlying systems associated with these legacy solutions were largely static, allowing for more advanced or anomalous threats to go undetected.

Worse yet, legacy SIEMs can only provide data on security events (ignoring other types of incidents), making it difficult to correlate security events with what's happening across the rest of the organization's environment. Especially with today's rapid adoption of cloud services, which continues to expand into new threat vectors, today's organizations need to respond to more threats than ever before.

Investigating security events takes precious time most organizations simply can't afford. A legacy SIEM can't keep pace with the rapid-fire rate of security events in need of investigation. What security operations center (SOC) analysts require today is a simple way to correlate information across all security-relevant data, from all sources.

Your SOC analysts must be able to anticipate what threats might be lurking and put measures in place to limit the vulnerability of their organization in real time. For that, they need a data-centric, modern SIEM solution that gives analysts full visibility into the data being generated and works with more than just log data and simple correlation rules for data analysis.

Today's leading SIEM solutions now combine long-time storage of event logs with real-time monitoring to provide your team with a holistic understanding of the organization's security posture. Here are the SIEM essentials to look for.

The 7 essential capabilities of an analytics-driven SIEM

1. **Real-time security monitoring and analysis:** detect and respond to threats fast.

2. **Cloud security:** detect and respond to threats across hybrid, cloud and multicloud environments.

3. **Incident response:** identify incidents when they occur, and track, route and annotate events.

4. **Threat intelligence:** access curated, in-product security research on existing and emerging threats.

5. **Incident investigation and forensics:** optimize threat hunting, reduce the volume of alerts and increase true positives.

6. **Advanced and insider threat detection:** exponentially improve detection success, freeing up time and resources to zero in on complex, high-fidelity threats.

7. **Compliance:** unify the three pillars of compliance — process, technology and people — through greater visibility across systems and processes.

01

Real-time security monitoring and analysis

Organizations need to be able to detect and respond to threats in record time — no matter the nature or severity of the attack. But to do this and do it well, security monitoring is a must-have, and luckily, a modern SIEM offers robust, real-time monitoring.

How does it work? To pinpoint and identify different types of malicious and/or anomalous behavior, a SIEM retrieves and maintains contextual data around users, devices and applications (e.g., asset and identity data) from across on-prem, cloud, multicloud and hybrid environments. All relevant data is then fed into a workflow to assess potential risks.

By monitoring and ingesting machine data from a diverse set of sources across different types of deployments, security teams have a comprehensive view of potential security events — making it that much easier to detect and zero in on bad actors. A leading SIEM should provide a library of customizable, predefined correlation rules, a security event console for real-time presentation of security incidents, and dashboards to provide real-time visualizations of ongoing threat activity.

Security monitoring can also be augmented with out-of-the-box correlation searches that can be invoked in real time or scheduled regularly. These searches can be available via an intuitive user interface that doesn't require analysts or administrators to master a search language. Finally, a modern SIEM will have a local and historical search function to make easy work of searching log data, and reduce the amount of network traffic accessing search data.

02

Cloud security

As organizations sprint ahead with digital initiatives, they need to pay close attention to both general security requirements and the technical complexities of cloud migration. Inevitably, the journey to cloud nativity presents a considerable increase in risk to the enterprise — especially if the organization is not up-to-date on network controls, access management systems or cloud configuration options. Add to that an expanding attack surface and a lack of visibility, and you've got yourself a high chance of breach. So traditional monitoring just isn't enough. Security teams need the capabilities of a modern SIEM to analyze and ingest data from a wide range of sources, across all types of environments, in order to detect the where and why of security events.

How does it work? With a leading SIEM solution, you get out-of-the-box cloud security monitoring content that makes it easier to detect and respond to threats across hybrid, cloud and multicloud environments, including sophisticated detection rules for cloud attacks, and tools to help you test and improve cloud detections via attack simulation.

Especially in the age of remote work, you need to be able to capture and analyze all cloud and endpoint data — regardless of volume, variety and velocity. Ultimately, by monitoring the uptime, availability and activity across multiple cloud deployments with a modern SIEM, you'll have full visibility into cloud services (including Amazon Web Services, Azure and Google Cloud Platform) and all the actionable insights that come with it.

03

Incident response

Today's organizations also need an up-to-date incident response strategy, and a modern SIEM can help you identify incidents when they occur, and provide a means for tracking, routing and annotating events.

How does it work? A SIEM can manually or automatically aggregate events, support third-party systems and vendors (allowing for the easy ingestion of data to and from a diverse set of sources), and provide up-to-date threat intelligence and auto-response capabilities (like playbooks) that preempt or disrupt cyberattacks either right before or right after they emerge.

In order to do all of this, a SIEM solution should be the hub around which an incident response workflow is customized and crafted. Since security events have different levels of urgency attached to them, potential threats can be identified, categorized and triaged via dashboards, then assigned to analysts for review. By identifying, triaging and auditing notable events based on the fidelity of the threat, a modern SIEM makes the start of the remediation process more reliable, equipping your teams with the contextual awareness they need to determine next steps.

To expand or reduce the scope of their analysis (which can be vast), your SOC analysts can use a SIEM to apply filters to the sea of log data, then place events, actions and annotations into a timeline to see everything that's going on. They can then review and codify these timelines as a repeatable kill chain methodology to deal with specific event types.

04

Threat intelligence

Threat intelligence is another must-have strategy. But threat intelligence is often too noisy, with your security analysts having to manually curate data to make use of it. With manual input, context gets lost during the investigation process or the data becomes too disparate, while enrichment in playbooks is too clunky. Making it even harder for your analysts, the most valuable security data is often locked inside silos in and across companies. With more integrations coming online that are generating more data needing to be secured and stored, this problem isn't going away.

Fortunately, thanks to the rapidly growing intelligence marketplace, modern SIEM solutions can integrate threat intelligence into every stage of the incident response flow, as well as across an ecosystem of teams, tools, peers and partners.

How does it work? Threat intelligence transforms internal and external sources of security intelligence for informed, actionable automation across ecosystems of teams and tools and helps with intelligence sharing with internal and external stakeholders. Your team can preempt attacks and create complex pipelines without ever having to write or maintain scripts in the backend. Threat intelligence comes integrated into most modern SIEM solutions or as cloud-native SaaS that integrates seamlessly with a modern SIEM platform.

The intelligence provided usually includes indicators of compromise (IOCs), adversary tactics, techniques and procedures, alongside additional context for various types of incidents and activities. This makes it much easier to recognize abnormal activities, as your analysts have all the information they need to assess the risks, impact and objectives of an attack — no matter how cunning — and respond appropriately.

Threat intelligence data can be integrated with machine data to create watchlists, correlation rules and queries for better detection and response to attacks. This information can be automatically correlated with event data and added to dashboard views and reports, or forwarded to devices that can then remediate the vulnerability in question.

05

Incident investigation and forensics

Chances are, your security team spends too much time investigating low-value alerts with too little context. Incidents based on narrowly defined detections can lead to a high volume of false positives and a lot of extra noise, quickly overwhelming and overburdening anyone on the front lines. That's why you need a strong incident investigation and forensics strategy powered by a modern SIEM.

How does it work? A modern SIEM visualizes and correlates data by mapping categorized events against a kill chain, or creating heat maps to better support incident investigations by providing important insight into which tactics have been used by an adversary that map to a particular industry framework.

Risk attribution can also help optimize threat hunting and reduce the volume of alerts — thereby increasing true positives — while surfacing more sophisticated threats, like low and slow attacks that most correlation searches traditionally miss. This frees up time and resources to home in on actual (often complex) threats, aligning operations to industry-standard cybersecurity frameworks.

Bottom line: freeing up your analysts to focus on high-value tasks means they're better positioned to respond quickly and efficiently in the event of a security breach — and who wouldn't want that?

Plus, your team can make better informed decisions and gather forensics evidence with the comprehensive collaboration and reporting capabilities integral to a modern SIEM investigative workflow.

06

Advanced and insider threat detection

Security threats continue to evolve, mutate and find ways to evade standard security procedures — and the more sophisticated the attack, the harder it is for your team to detect and remediate it. Between the changing threat landscape and the crafty nature of new and emerging threats, advanced and insider threat detection strategy has never been more important.

Most traditional security tools can't meet the challenge. They rely on existing rulesets and signatures, and can only detect straightforward, well-known threats, so they fail to address the complexity of advanced security threats, like insider threats, zero-day attacks, laterally moving malware and compromised accounts.

How does it work? Fortunately, a modern SIEM can adapt to these threats by stitching together anomalies and correlating them as part of the incident response workflow, as well as implementing capabilities like endpoint detection and behavioral analytics.

By establishing multi-dimensional behavior baselines and dynamic peer group analysis — ideally in tandem with unsupervised machine learning — compromised or misused accounts can be detected.

The goal is to not only detect hidden threats, but also determine the scope of the attack and how best to contain it. For this, your team requires real-time views and reporting capabilities that can be extended to include any number of third-party applications and services.

This type of analytics and behavior profiling in a SIEM can exponentially improve detection success, freeing up your team's time and resources to focus on complex, high-fidelity threats, before it's too late.

07

Compliance

Whether it's for cybersecurity, forensic analysis, privacy, fraud or risk management, different teams require different views and processes around data in order to guarantee compliance. A modern SIEM can help unify the three pillars of compliance — process, technology and people — by providing you with greater visibility across the board.

How does it work? A modern SIEM solution takes a holistic, foundational approach to compliance that not only connects compliance teams, silos and technology fiefdoms, but also streamlines the overall efficiency of compliance-related operations. This means the tedious, time-consuming chore of legally-mandated log review can finally be put to bed. Your analysts can be more productive and maintain the buttoned-up, documented approach to risk management that's expected of them.

With a modern SIEM, organizations can see across the entire security stack for assessments, rankings, investigations and audits, and are no longer dependent on a single department or functional unit for insights. Your analysts can search, alert and report on machine data from an array of sources, meet compliance requirements from audit trail collection and reporting, and generate sector-specific compliance reports in seconds.

A SIEM powered by data

Organizations today need their SIEM solutions to do more than simply collect security events. To see that data in context and turn it into actionable intelligence, enterprise security teams need a modern, data-centric approach to their security operations fueled by machine learning and advanced analytics.

A data-driven SIEM solution can combine IT operational data and security intelligence so that teams can quickly identify potential vulnerabilities and security gaps within their infrastructure. Armed with this data, security teams can remediate known threats and proactively respond to new threats in real time.

Cybersecurity has always been a hard job, but the last few years have made it even harder. Fortunately, with a robust, data-driven SIEM solution, security teams can gain visibility across their entire environment, keep up with security and compliance regulations, and stay one step ahead of attacks in an ever-evolving threat landscape.

Learn More

splunk>

22-26030-Splunk-7 Essential Capabilities of a Data-Driven SIEM-EB-101