panther

Evaluating a SIEM Solution

WHAT IS A SIEM

SIEM solutions centralize relevant security data to provide wide visibility into an organization's digital environment. The goal of implementing a SIEM is to identify areas of high risk and proactively implement detection strategies aimed at reducing incident-related costs and accelerating incident response.

Why a SIEM?

Lack of Visibility and Control

Without a SIEM tool, security teams may have difficulty collecting, aggregating, and analyzing security data from various sources across their environment, and may miss important signals or indicators of compromise.

High Complexity and Cost

Before introducing a SIEM, security teams often rely on multiple point solutions or manual processes to perform security tasks, which increases complexity and total cost of ownership.

Ineffective and Inefficient Security Workflows

Security teams have difficulty prioritizing and triaging security alerts, correlating security events, investigating suspicious activity and responding to incidents without a centralized system of record. Poor compliance and reporting Without a SIEM tool, security teams have trouble meeting regulatory compliance standards and generating audit reports.

Key SIEM Benefits

Accelerated Threat Detection and Response

By centralizing visibility and enabling workflows for detecting and responding to suspicious activity SIEMs help reduce the mean time to detect (MTTD) and mean time to respond (MTTR) to security incidents.

Improved Security Posture

SIEM tools help organizations prevent or minimize the impact of security breaches, protect their reputation, and enhance their customer trust.

Compliance Reporting

SIEM tools help organizations meet regulatory compliance standards by tracking and logging security data and generating audit reports. This can help organizations save money, avoid fines, and demonstrate their security posture to auditors and stakeholders.

©2024 Panther Labs Inc.

Evaluating a SIEM

The performance of a SIEM depends on its underlying architecture, scalability, and how it can be deployed. When evaluating a SIEM, be sure to understand the following:

	KEY EVALUATION CRITERIA
Architecture	☐ Is the SIEM cloud-native? ☐ Was the SIEM built in the cloud originally or moved there? ☐ Does the SIEM require configuration of operational components like servers?
Scale	☐ How does the SIEM scale up or down as the organization's security needs change over time? ☐ How do you handle the volume and velocity of security data generated by cloud infrastructure?
Deployment	☐ Does the SIEM require an on-premise footprint? ☐ Does the SIEM require dedicated personnel to maintain its availability and reliability? ☐ Does the SIEM require a professional services contract to set-up?

A SIEM's core functionality includes:

- **Collecting and transforming logs into structured security data**
- **Detecting suspicious activity in organizational environments**
- **Alerting teams to take action on identified threats**
- **Enabling investigation to verify malicious activity and contain incident impact**

These functions are essential for any security team that wants to gain visibility into their environment, identify and prioritize risks, respond to incidents effectively, and comply with regulatory requirements.

©2024 Panther Labs Inc.

	KEY EVALUATION CRITERIA
Data Collection	☐ Does the SIEM integrate with all major cloud providers? ☐ Does the SIEM integrate with key applications from the organization's environment? ☐ Is there an option for direct integration with the SIEM? ☐ Can I easily integrate nontraditional or custom log sources into the SIEM? ☐ Are logs normalized upon ingestion into the SIEM? ☐ Does the SIEM support log filtering to maximize the security value of ingested data? ☐ Does the SIEM enable data transformation upon ingest to refine data for use in detection and response? ☐ How long does the SIEM retain data? ☐ Are there different types of data storage in the SIEM (ex: "hot" or "cold")?
Detection	☐ Are detections invoked in real-time upon data ingestion? ☐ Does the SIEM provide useful out-of-the-box detection logic? ☐ Are detections mapped to relevant frameworks like MITRE ATT&CK? ☐ Can detection logic be easily edited and optimized to meet organizational requirements? ☐ Is detection logic written in a vendor-specific language? ☐ How are detection versions tracked over time? ☐ Is it easy to test detections against single cases or historical data? ☐ Can detection logic support custom enrichments?
Alerting	☐ Do alerts provide relevant context for triage? ☐ Is it easy to assign alerts and track their status? ☐ Is it simple to route alerts to relevant collaboration or workflow tools? ☐ Is it easy to gather context from users related to suspicious activity?
Investigation	☐ How is query performance impacted at high data volumes? ☐ Is it simple to search normalized fields across all log types? ☐ Is it possible to save common queries for future use? ☐ Are search results presented with useful visual and tabular summaries of the data? ☐ Is it easy to curate and refine search results for use in the next pivot?
Licensing & Pricing	☐ How is the SIEM priced? ☐ Are there typically additional costs outside of a basic license (e.g. extra storage costs)? ☐ Are there additional charges based on data retention? ☐ Are there different charges based on type of storage? And, converting between those types? ☐ Are there additional required SKUs to make all features work? ☐ Are there additional services or third-party providers that are required/recommended as a part of the contract? ☐ How does pricing scale to meet very large data volumes?
Governance, Legal, & Compliance	☐ Is the SIEM SOC2 Type II compliant? ☐ Is the SIEM ISO217001 compliant? ☐ Is the SIEM PCI compliant? ☐ Is the SIEM architected in a single tenant fashion? ☐ Can data storage be isolated to a particular geographic region?

©2024 Panther Labs Inc.

	KEY EVALUATION CRITERIA
Architecture, Scale, & Deployment	☑ Cloud-native architecture ☑ Zero-ops overhead ☑ Security data lake enables lightning-fast data processing and analysis ☑ Always-hot storage ☑ Year-long data retention
Data Collection	☑ Seamless integrations with all major cloud platforms ☑ Native integrations with popular applications and security tools ☑ Easily integrate custom log sources ☑ Robust filtering functionality so only valuable security data is ingested and stored ☑ Data transformation to enrich data across log sources
Detection	☑ Useful out-of-the-box detections that map to relevant frameworks like MITRE ATT&CK ☑ Simple, granular ways to edit and tune detection logic ☑ Seamless workflows for tracking relevant versions of detection logic and testing and deploying new detections ☑ Support for relevant enrichment context and nuanced, complex detection logic
Alerting	☑ Useful alert context & enrichment informs triage ☑ Easy-to-use alert assignment and alert management functionality ☑ Seamless alert routing to relevant tools (ex: Slack, Asana) ☑ Slack Bot functionality gathers helpful user context on alerts
Investigation	☑ High-performance query engine that leverages a scalable and cost-effective security data lake ☑ Data validation and normalization that ensure data quality and consistency across all log sources ☑ Simple filterable search across all ingested logs ☑ Search results returned with helpful visual summaries ☑ Search results displayed in interactive table where data can be refined and manipulated for further analysis
Licensing & Pricing	☑ Transparent pricing based on monthly data ingest ☑ No additional feature, infrastructure, or service fees ☑ Pricing scales cost-effectively with exponential data growth
Governance, Legal, & Compliance	☑ Compliance: SOC2 Type II, ISO27001, PCI ☑ Single-tenant architecture ensures data privacy ☑ Data storage in the geographic region of choice

In short, Panther offers:

- **Seamless and efficient data collection** that maximizes the security value of ingested data
- **Flexible and powerful workflows** that enable easy creation, editing, testing, and deployment of detection logic
- **Intelligent alerting** that helps reduce alert noise, prioritize alert risk, and accelerate alert triage
- **Fast and intuitive investigation** that helps get answers to the most pressing security questions

See for Yourself →

©2024 Panther Labs Inc.