Apica

Data Sheet

SIEM Platform Overview

Apica's SIEM platform employs a scalable architecture that enables users to detect, analyze, and immediately respond to threats that jeopardize enterprise security. With Apica, enterprises can implement security processes that mature and evolve with their ever-changing threat landscape.

The Apica SIEM platform has the following components.

- Multiple integrations
- Centralized logging
- HIDS using OSSEC
- Incident response
- Security Orchestration, Automation, and Response
- Built-in security Rule Packs

Log collection from multiple sources

By employing readily available and popular agents in the log forwarding and management ecosystem like Syslog, Logstash, Fluent Bit, etc., Apica's SIEM platform can collect logs generated across every component of monolithic, distributed, and cloud IT architectures. This expansive log collection enables security professionals and experts to conduct threat forensic analysis and investigate and remediate vulnerabilities.

Centralized logs

Apica's infinite-scale architecture enables enterprises to centrally store all collected logs on any object-based storage without the need for storage tiering or rehydration. This unique approach to log management and storage allows enterprises to establish a Single Source of Truth for business-critical machine data for any duration with real-time search and analytics on huge volumes of data. By eliminating storage tiering, enterprises can witness never-seen-before levels of data agility necessary for security threats and vulnerability analyses.

Application of security rules

Apica ships with Rules Packs with over 1500 rules covering commonly-used applications that users can apply to all collected and stored events and logs. Rule Packs help enterprises enhance data value by augmenting security-related events within logs almost immediately after generation and gain faster and deeper insight into vulnerabilities. Apica's Rule Packs are constantly updated to cover the latest threats, such as the Log4j zero-day vulnerability.

Host intrusion detection system (HIDS) using OSSEC

Apica uses OSSEC that empowers enterprises to perform server intrusion detection across multiple platforms like Linux, Solaris, AIX, HP-UX, BSD, Windows, Mac, and VMware ESX. Enterprises can meet compliance requirements such as PCI-DSS as they can detect and issue alerts on unauthorized file system modification and malicious behavior that could cause non-compliance. Apica allows customizations across dashboards, alerts, and GUI configurations to give enterprises the flexibility they need to stay on top of the constantly evolving threat landscape.

Incident Response

The Apica platform's rich incident response integration enables enterprises to trigger responses and remedial action as soon as critical and non-critical events that need remediation occur. Apica integrates with platforms like PagerDuty, ServiceNow, and many more, enabling enterprises to trigger incident responses as soon as incidents are detected within log streams.

Security Orchestration, Automation, and Response (SOAR)

Apica's platform is SOAR-ready, allowing enterprises to trigger immediate orchestration and remediation responses. Enterprises can now enable their security teams to confidently respond to cyber threats and automate responses to ensure accurate and fast remediations.