REPORT REPRINT

Analytics is making its security operations mark ahead of schedule

APRIL 25 2019

By Eric Ogren, Nancy Gohring

The security industry is retooling with analytics to proactively find threats inside the infrastructure, reduce the downtime between compromise and detection, and help security operations respond to alerts. Machine learning analytics embracing IT, network and security data sources is driving new approaches to security operations. A prime example is the powerful acceptance of SIEM in cloud architectures.

Introduction

Security information and event management (SIEM) vendors have been rightfully focused on meeting compliance requirements, alleviating security analyst staffing shortages and enhancing the ability to detect threats executing inside the network. SIEM performance ceilings were pushed to the limits to accommodate enterprises' appetite for more log data, more connector development for applications, and workflow tools to extract more value out of log data. Product acquisition costs, security operations costs and barriers to entry for new competitors escalated until the bubble burst. SIEM in the cloud is making traditional SQL-oriented SIEMs non-competitive with scalable architectures supporting advanced machine learning analytics, data lakes wildly extending data capacity, and new pricing models – making SIEM displacement a reality.

451 TAKE

The entry of Chronicle and Microsoft Azure into the SIEM market indicates that analytics with cloud-native architectures is transforming the space. Security operations count on machine learning analytics to rationalize alert streams, detect active threats by traces left in operational data, and support scripts for customized threat hunting. The foundation for a data-driven security operations strategy consists of massively scalable data storage along with computational cycles for executing machine learning algorithms. Enterprises aiming to get out of managing their own SIEM deployments now justify a transformation to cloud-based analytic SIEM products on the basis of enhanced security and lower operating costs.

Factors contributing to analytic SIEMs

In a perfect-storm scenario, many instruments of change have come true to enable analytic SIEMs in the cloud, including:

- Analytics for reducing dwell time. Let's be honest here – security products responsible for recognizing and filtering threats are not going to produce logs useful for detecting advanced threats that snuck by and are inside the network. Incidents are often first reported by operational disruptions, and that is the leading motivator for automated analytics. Machine learning algorithms incorporate diverse data sources to detect such issues as compromised hosts, stolen accounts, fraud campaigns, insider misbehavior and negligent users.
- Analytics for fighting alert fatigue. Deployed security offerings show they are on the job by constantly logging events and alerts. Making sense of all of the alerts and events is a significant problem for security operations staff. Machine learning analyzes alerts and events to produce prioritized, condensed task lists to streamline reactive corrections and proactive threat-hunting activities.
- Data lake maturation increases SIEM capacity to embrace new data sources. Cloud-based SIEMs can massively scale the amount of data managed without bumping into the performance ceilings associated with traditional SQL-based architectures. SIEMs can now consume log data for new applications or new sources of data for advanced analytics.
- Culture shift from compliance to security operations. Most organizations now have a handle on meeting compliance requirements and are shifting attention to improving their ability to detect threats, resolve critical alerts and remediate problems. There are no compliance mandates for analytics, yet enterprises are investing in analytic data-driven security for visibility into cloud operations.
- Security data is as safe in the cloud as it is on-premises. There used to be vociferous resistance from security operations to ceding control of security data, with the fear that a breach of the cloud provider datacenter would give hackers a blueprint of the network. The modern approach recognizes that much valuable business data exists in the cloud in places such as Salesforce, Office 365 and Oracle Peoplesoft – there is no evidence that data is any less safe in shared cloud datacenters than it is in private datacenters, and security operations can no longer justify being a laggard in realizing the economic benefits of transforming its infrastructure into the cloud.
- Aggressive pricing models encourage greater use of data and analytics. SIEM specialists are responding to demand for predictable expense control by offering pricing models based on number of employees or IP addresses, with unlimited data capacity for a given retention period.

Vendors on the move

The analytic SIEM is no longer security's file cabinet for log data waiting to be examined on a bad day. The following is a sampling of analytic SIEM vendors gaining market traction with cloud-based analytic SIEM products:

Different approaches of modern SIEM providers

ANALYTIC SIEM VENDOR	RATIONALE
AMAZON WEB SERVICES	Amazon Security Hub serves as a storage repository for Amazon findings, which can then be used to fuel threat hunting and analytics. Security Hub is designed to enhance the visibility and security management of AWS-hosted applications.
CHRONICLE	Chronicle Backstory is optimized for search and threat-hunting tasks. Utilizing Google Cloud Platform, Backstory consumes streams of data with promises of advanced analytics to uncover threats.
EXABEAM	Exabeam started life as a user behavior analytics firm with data gathered in an Elastic data lake. The company deemphasized its SIEM augmentation strategy, rebranding as an analytic SIEM provider with a product line led by Exabeam SaaS Cloud.
FIREEYE	FireEye Helix collects events from endpoint, network, email and threat intelligence security offerings. Helix's differentiation is its focus on the needs of incident responders and helping triage analysts get to the bottom of security alerts.
JASK	The Jask ASOC platform integrates security and network data to give security operations more end-to-end visibility into the business. The Jask product comes complete with Zeek sensors to incorporate enriched network data into its cloud-hosted analytic SIEM.
MICROSOFT AZURE	Azure Sentinel is intriguing for its potential to bring advanced security analytics to businesses that are not positioned to invest in security operations. Azure Sentinel includes links to Microsoft Windows configuration experts to consult on designing remediation actions.
PALO ALTO NETWORKS	Palo Alto Cortex acts like an analytic SIEM in collecting log data from firewalls, sandboxes and endpoint software to help manage the security infrastructure. The results of Cortex analytics can be pushed to controls in Palo Alto firewalls and endpoints.
SECURONIX	Securonix, an early mover in user behavior analytics, now generates more than half of its business from its cloud product line. Securonix SNYPR Cloud customizes security oversight without incurring acquisition expenses of an on-premises offering.
SPLUNK	Splunk's purchase of Caspida in 2015 spurred the move to analytic SIEMs. The company was one of the first to demonstrate the value of machine learning acting on log data. Splunk Cloud now delivers those capabilities as an analytic SIEM.
SUMO LOGIC	Sumo Logic is the first innovator on this list, having started its cloud-native analytic SIEM service in 2010. The company applies machine learning to both IT and security use cases, helping operational teams collaborate on resolving security issues.

Buyers now have more choices

Security operations now have more choices – and negotiating power – in their SIEM purchase decisions. Traditional on-premise SIEMs are excellent for many use cases. Analytic SIEMs in the cloud now give security teams greater automated capabilities without the hassle of having to build out a security operations infrastructure.

Analytic SIEMs making their mark

At an RSA Conference a couple of years ago, we talked with a security investor about the future of security operations. We made what we thought was a bold claim that analytics would be driving security operations centers within five years. The investor saw the future differently, had heard the machine learning story before, and believed analytics would soon be a passing fad. We ended up defending our positions by making a friendly wager. It is now time to collect!