NAND RESEARCH

RESEARCH NOTE

ELASTIC SIEM UPDATES

STEVE MCDOWELL, CHIEF ANALYST
MAY 8, 2024

CONTEXT

At the 2024 RSA Conference, Elastic introduced significant enhancements to its Security Information and Event Management (SIEM) solution, Elastic Security. The upgrades, revealed at the recent RSA Conference, are a substantial leap in the evolution of security operations centers (SOCs).

BACKGROUND: ELASTIC SIEM

Elastic SIEM is part of Elastic Security, designed to provide organizations with advanced security analytics to help detect and respond to threats more effectively.

The Elastic SIEM system integrates seamlessly with other components of the Elastic Stack (including Elasticsearch, Logstash, and Kibana), allowing it to collect and analyze vast amounts of security data in real-time.

Critical features of Elastic SIEM include:

1. **Real-Time Data Analysis**: It leverages Elasticsearch's capabilities to perform real-time data analysis from various sources, such as logs, network data, and endpoint events.
2. **Interactive Visualizations**: Elastic SIEM utilizes Kibana for data visualization, offering dashboards that provide actionable insights and a comprehensive overview of an organization's security landscape.
3. **Anomaly Detection**: It includes machine learning-driven anomaly detection to identify unusual patterns and potential threats automatically.
4. **Integration and Scalability**: Elastic SIEM can integrate with a wide range of data sources and scales efficiently with the needs of large enterprises, making it suitable for monitoring complex and dynamic environments.
5. **Threat Hunting and Case Management**: It supports proactive threat hunting with a user-friendly interface for querying and examining data alongside tools for managing and tracking security incidents.

Elastic SIEM is designed to enhance the efficiency of SOCs by reducing the time and effort required to detect and respond to security incidents. It provides a unified platform that helps streamline workflows, improve detection capabilities, and accelerate incident response.

NEW SIEM FEATURES

Elastic announced significant enhancements to its SIEM, bringing several advanced features to automate and simplify security operations.

Here's a breakdown of the new elements in Elastic's SIEM:

1. **Attack Discovery**: This new feature leverages the Search AI platform to prioritize critical attacks over mere alerts. It uses a combination of search and retrieval augmented generation (RAG) technology to sift through large volumes of alerts efficiently, identifying and prioritizing actual attacks. This tool allows security teams to focus on the most significant threats with actionable insights, reducing the time and effort spent on triage.

2. **Elastic AI Assistant for Security**: Introduced as part of their ongoing efforts to enhance SOC operations, this AI assistant supports security analysts by assisting with rule authoring, alert summarization, and providing workflow and integration recommendations. This tool reduces the complexity involved in managing security alerts and improves the overall efficiency of security teams.

3. **Integration of Machine Learning**: Elastic's SIEM now includes over 100 pre-built machine learning-based anomaly detection jobs that help identify new and unknown threats more quickly. This feature enhances the system's ability to detect sophisticated cyber threats that might otherwise evade traditional detection methods.

4. **Enhanced Data Handling**: Built on the Open Cybersecurity Schema Framework (OCSF), Elastic's SIEM ensures rapid ingestion, normalization, and data processing from diverse sources. This capability is crucial for maintaining an up-to-date and comprehensive dataset for effective threat detection and response.

ANALYSIS

Elastic’s updates to its SIEM solution reflect a clear industry trend towards greater AI integration within cybersecurity tools, reflecting the broader industry movement towards automation and advanced analytics.

Its AI Assistant, introduced last year, and the newly unveiled Attack Discovery feature, powered by Elastic's proprietary Search AI platform, are a strategic pivot away from traditional, labor-intensive SIEM processes towards a model where AI-driven analytics

play a central role. This transition augments security analysts' capabilities and addresses the scalability challenges inherent in traditional SIEMs.

Elastic's approach—integrating machine learning and retrieval-augmented generation directly into its SIEM system—positions the company well ahead of competitors like Splunk. The ability of its Attack Discovery capability to sift through and prioritize actionable intelligence from a flood of alerts with minimal human intervention is a game-changer. It enhances operational efficiency and reduces the time to response, a critical factor in mitigating the impact of security breaches.

Elastic Security's enhancements to its SIEM are not simply incremental improvements but rather a broad expansion of what SIEM can achieve. For organizations, adopting such advanced tools will translate into better security postures and more efficient use of resources. For the broader cybersecurity industry, it sets new benchmarks in integrating AI into security operations, pushing competitors to also innovate or risk obsolescence.

NAND Research is a technology-focused industry analyst firm providing research, customer content, market and competitive intelligence, and custom deliverables to technology vendors, investors, and end-customer IT organizations.

Contact NAND Research via email at info@nand-research.com or visit our website at nand-research.com.