RKON Security Log Monitoring (SLM)

Why do you need security log monitoring?

SLM is a comprehensive solution that includes a set of industry-leading tools and mature processes designed to deliver the following benefits:

Compliance & reporting: Virtually every regulatory mandate requires some form of log management, and SIEM directly supports this requirement. Alerting and correlation capabilities also satisfy routine log data review requirements, a tedious and daunting task when done manually.

Operations support: The complexity of today's enterprises is growing exponentially, along with the number of IT personnel needed to support it all. A SIEM can pull data from disparate systems into a single pane of glass, allowing for efficient cross-team collaboration.

Zero-day threat detection: Firewalls, IDS/IPS and AV solutions all look for malicious activity at various points within the IT infrastructure, from the perimeter to the endpoints. However, many of these solutions are not equipped to detect zero-day attacks. A SIEM can detect activity associated with an attack rather than the attack itself.

Advanced persistent threats (APT): Many experts claim that APTs were responsible for the high-profile breaches at RSA, Lockheed Martin and others.

Forensics: Since log data represents the digital fingerprints of all activity that occurs across IT infrastructures, it can be mined to detect security, operations and regulatory compliance problems. Consequently, SIEM technology, with its ability to automate log monitoring, correlation, pattern recognition, alerting and forensic investigations, is emerging as a central nervous system for gathering and generating IT intelligence.

Why Cloud-Based MSP vs. Build and Buy?

Discipline, Objective Viewpoint, Bandwidth, Consistency

Speed to execution and speed to maturity: The tools and technology are extremely complex from a management and administrative standpoint—and need people and processes to be implemented properly.

Discipline: You buy the discipline so that someone's always moving the security model forward—and keeping the system in a high state of operation regardless of the client's internal priorities.

Objective Viewpoint: You buy external advisement and a point of opinion and validation for future growth and priorities—from a source that's vested in the outcome. (A bad outcome makes the system noisy.)

Bandwidth: When the system gets noisy, during internal change or new deployment, you'll have external bandwidth to tune the system while the client's internal team is busy tending to the change that caused it.

Consistency: It's important to keep up with important updates and new functionality without the R&D time associated with major releases to prevent the system from becoming outdated.

Testimonial: Large Financial Institution

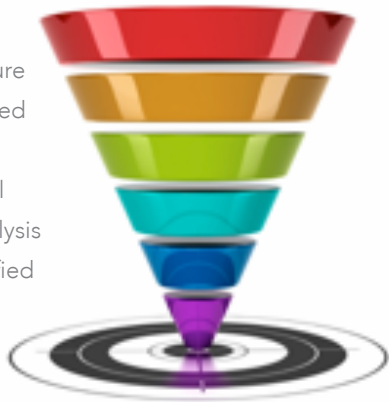
> *"We originally brought a SIEM solution in house and found learning those systems was a much bigger administrative challenge that we thought. They look simple in the demos but configuring and managing them is quite a different story. We had trouble keeping up with the new updates and versions over time. Finally, we had to deal with the inevitable turnover, disruption of service to the organization, and cost of retraining associated with those events and decided to outsource this function to RKON. Now it costs us less, and we're able to focus more on our core business of security and deliver more value to our business."*

What's included in the RKON SLM Solution?

Security Information and Event Management (SIEM) is not a security control or detection mechanism by itself, but it makes the security technologies you have more effective. It enables the whole to be greater than the sum of its parts. SIEM is about collecting logs, and then mapping information about your infrastructure and business processes to them. It empowers security analysts to make reasoned, informed investigations into activities on the network to determine their impact on security integrity and business continuity. The SIEM should act as your single portal to activity on your network, decoupling your analysts from a need to have product-specific knowledge about security capabilities.

RKON SLM comprises three major components:

Security Log and Event Monitoring



Hosted in RKON datacenters, the SIEM collects and aggregates logs from critical infrastructure components in the customer environment. The logs are continuously correlated and compared against a security policy, and alarms are generated when potential threats or anomalies are detected. Security experts in the RKON Security Operations Center (SOC) provide additional analysis, validation and response for security threats. The combination of the automated analysis and human verification in the SOC reduces false positives, ensuring that clients are only notified about real security events.

Logs are stored for one year, addressing a key security requirement. Customers can significantly improve their security posture by leveraging this industry-leading solution to provide:

1. Next Generation SIEM and Log Management
2. Independent Host Forensics and File Integrity Monitoring
3. Network Forensics with Application ID and Full Packet Capture
4. State-of-the art Machine Analytics

5. Advanced Correlation and Pattern Recognition
6. Multi-dimensional User/Host/Network Behavior Anomaly Detection
7. Rapid, Intelligent Search

Incident Management/SOC

A major component of the SIEM service, Incident Management is provided by the RKON Security Operations Center (SOC). The RKON SOC ensures that the SIEM systems is optimally configured to provide the greatest coverage and handles the management of all security events generated by that system. Specifically, this service includes:

1. Generation of incidents in ticketing system based on alarms generated by SIEM
2. Incident management of these tickets, including escalation to appropriate resources
3. Ongoing tuning of SIEM system
4. Creation of custom alerts and reports
5. Integration of new assets into SIEM system

Incident Response

This service is provided as a retainer for 40 hours of Incident Response activities in a calendar year, to be used toward the remediation, investigation and customer notification activities associated with a suspected security breach.