NOKIA

Security orchestration, analytics and response to complement traditional security management

White paper

NOKIA

Contents

NOKIA

Tackle the new challenge in cybersecurity

As the cyberattack surface has grown, many of the technologies used to address it have contributed to the complexity of security management, often creating segmented data that requires an excess of time and resources to unify. Many conventional security management solutions only provide limited insight into the networks' actual security posture, failing to show the big picture, and react only to threats already present. Threat and vulnerability data provides some of the underpinnings for answering the security state of your network, but lacks the scope and business relevance to put the data in context. Incident response technologies, such as traditional Security Information and Event Management systems (SIEM), are powerful for displaying current security events, but can overwhelm users with excess information while failing to provide context to the actual state of security. As a result, security teams are left with manually aggregating data from various sources to get a glance at the overall security state.

Security teams need a better way to not only gather the supporting information about the security state from a wider range of sources, but also to automate security processes. Security Operations, Analytics and Reporting (SOAR) can automate response workflow to gather and analyze security data from various sources and to make them available and consumable by different stakeholders. A platform that uses intelligent analytics, artificial intelligence and machine learning would continuously evaluate the risk posture and the state of the environment to enable informed decision making, formalize and automate responsive actions in real time. Such cognitive analytical and automated technologies measure rather than monitor to provide formalized workflows and enable informed remediation prioritization.

Enriching traditional security management systems

The recent increase in sophisticated, targeted security threats by both insiders and external attackers has increased the awareness and urgency of communication service providers, mission-critical network operators and utility enterprises for implementing comprehensive security strategies. The networks delivering video, voice, IoT-data, and cloud applications have millions of configurable parameters for optimizing service delivery and customer experience. As a result, the attack surface for security threats has dramatically expanded. Looking forward, new technologies like Network Function Virtualization (NFV) and Software Defined Networking (SDN) along with new business models, introduce additional security risks and implications.

The traditional security management system capabilities to detect and investigate unknown threats and exfiltration, are insufficient alone. There is an important distinction between an intrusion, when unauthorized entities gain access to the network, and exfiltration, when data leaves the network (or in other words, a breach is occurring). Traditional systems such as SIEMs typically do not provide the contextual analytics necessary to identify potential threats which may indicate exfiltration, nor are they able to determine post-incident what data may have been exfiltrated or which systems were compromised. They are typically deployed to look at the perimeter of the network. Outsiders that have already infiltrated the network, whether by stealing hardware or taking over an insider's account, can roam freely in a perimeter-centric security system. Malicious insiders pose a significant risk as well, as they are already inside the network.

NOKIA

As a result, there is a growing trend to implement cognitive security analytics systems as a enrichment to traditional existing SIEM solutions for advanced and context-aware detection and response provisioning. Security management enrichment with cognitive security software helps communication service providers achieve key strategic objectives including revenue growth, improving operational costs, regulatory compliance, and enabling and protecting new technology introductions such as SDN, NFV, video and voice over LTE, small cells, and Internet of Things.

It is a progressive security management solution that seamlessly delivers a holistic view of security posture, vulnerabilities, threats and breaches using advanced threat analytics.

Traditional SIEM and security orchestration

Alerts generated from SIEM deployments can be overwhelming. With the rise of Advanced Persistent Threats (APTs) and insider attacks, it became extremely difficult for security staff to detect all the risks. As a result, security teams are forced to implement a patchwork of tools across User Entity Behavior Analytics (UEBA), automation, ticketing systems, and SIEMs, etc. An average enterprise uses between 40-60 different security tools.

Many organizations invested heavily in their traditional SIEM solution yet are not getting full benefit out of them. SIEM solutions have to be tuned to accommodate the unique needs and use cases. Correlated security data from SIEM systems have typically been overly simplistic and hard to generalize, forcing the organization to keep producing rules to specific use cases, with the risk of being flooded with false positives.

Dealing with the vast number of alerts, events, and logs generated by SIEM and other security systems is one of the biggest challenges security operations teams face. While this simply correlated data contains valuable information, the sheer volume makes it practically impossible to effectively investigate every alert. SIEM pricing scales by the gigabyte and thus they are often tuned to aggregate only basic data, for instance, logs from VPNs, firewalls, and failed logons. Therefore, inaccuracy of data often makes SIEM systems unsuitable for large time-based analytics.

As a result, SIEMs' primary use cases are mostly smarter filtering and aggregation. For example, if SIEMs are only tracking unsuccessful logons, what about successful ones?

What SIEMs do well

SIEMs aggregate data: their purpose is to pull data from all the different security event sources of the perimeter, whether that's a firewall, active directory, an intrusion detection system, or antivirus, etc., and keep a long-term record of it.

Rules-based detection: SIEMs often provide the ability to create different rules for detections by their sources to detect if there are abnormalities inside the firewall or correlated with authentications in the active directory.

What SIEMs don't do well

Cyber attacks are often difficult to trace as hackers avoid to make an impact on security systems. This is a challenge for SIEMs, and can only be identified by intelligent analytics from more data sources. Therefore, attackers try to avoid SIEMs by stealing credentials and/or tricking insiders to run malware. Often, attackers try to access a shell of a system, as they are not monitored for active shells and outbound traffic in most cases. Attackers use known infrastructure, like privileged accounts, and try to mimic already existing patterns. Many privileged accounts already have permission to move in the entire network. If it's typical for that account to access a given system, it's unlikely that it will set off alarms.

Attackers go after data in places not covered by SIEM, for instance, data or information stored outside the perimeter, such as in clouds. This shows the importance of UEBA.

Once an attacker is in, they stay local: using local accounts, local credentials and local hashes to move laterally around the network. While SIEMs are good at aggregating this data, most SIEMs are not configured to pull local logs from different systems. East-West traffic is basically not monitored at all. Therefore, integrating other data sources, like network performance data, is important.

SOAR intelligence for more efficient security operations

SOAR complements SIEM by providing a consolidated view of the security threats and posture, with intelligence-driven, automated incident response resulting in more efficient security operations management. SOAR helps operationalize security data by consolidating and correlating data from a wide variety of vendor-specific solutions and sources to provide contextual intelligence.

SOAR streamlines automation, analytics and reporting coming from the many cross-vendor tools in use, helping analysts to integrate disparate tools. Using multiple tools from multiple vendors creates unnecessary complexity. Previously siloed information can be put into context, and viewed as part of an unfolding storyline.

SOAR complements SIEMs by providing:

- Context of the alerts
- User and Entity Behavior Analytics (UEBA)
- Better alert prioritization
- Incident response automation
- Centralized security information
- Aggregation and correlation of data not easily handled by traditional SIEMs, including network configuration data.

Aggregated data from SIEMs, when analyzed with additional data sources in SOAR, can provide a richer and more comprehensive view of threats. Some SIEMs will aggregate data based on IP and time, but the goal remains aggregation and alert reduction, not correlation. SOAR systems supporting User and Entity Behavior Analytics (UEBA), on the other hand, measure and report on risk levels, for example:

- Threat intelligence data
- Endpoint data
- Network performance data
- Behavior analytics and machine learning algorithms
- Configuration and asset data
- Vulnerability data
- Malware.

SOAR helps saving time spent on incident investigation in numerous ways:

- Elimination of pre-identified false positives
- Establishing workflow to consistently route alerts to the correct parties for action

- Enhanced communication between security teams and other impacted parties
- Improved security through focusing on real security incidents
- More efficient utilization of resources for true analysis.

SOAR integrates alerts from SIEM into an automated workflow that provides comprehensive command and control. Each orchestration and automation platform typically uses APIs to connect to infrastructure management systems. This may be a SIEM, next-gen firewall, endpoint, IDS, or other security infrastructure.

SOAR provides a consolidated and prioritized view of overall threats and risks, and executes fully or partially automated responses. A dynamic workflow engine can replicate security management processes using cyber playbooks. This enables incident response teams to reduce labor and mitigation costs, while also eliminating confusion and frustration. When integrated with pre-aggregated data from SIEM, SOAR solutions obtain more contextual intelligence to initiate appropriate, automated responses.

Benefits SOAR brings to SIEM solutions:

- Optimized threat response – prioritize alerts and standardize workflows
- Real-time overview – generate reports and use threat response KPIs to understand current capabilities and determine future security needs
- Improved staff utilization – better utilize staff expertise and reduce turnover
- Reduced mean time to resolution – respond to more alerts in the same amount of time
- Contextual incident response – leverage streamlined SIEM alert logic to analyze and resolve security alerts faster.

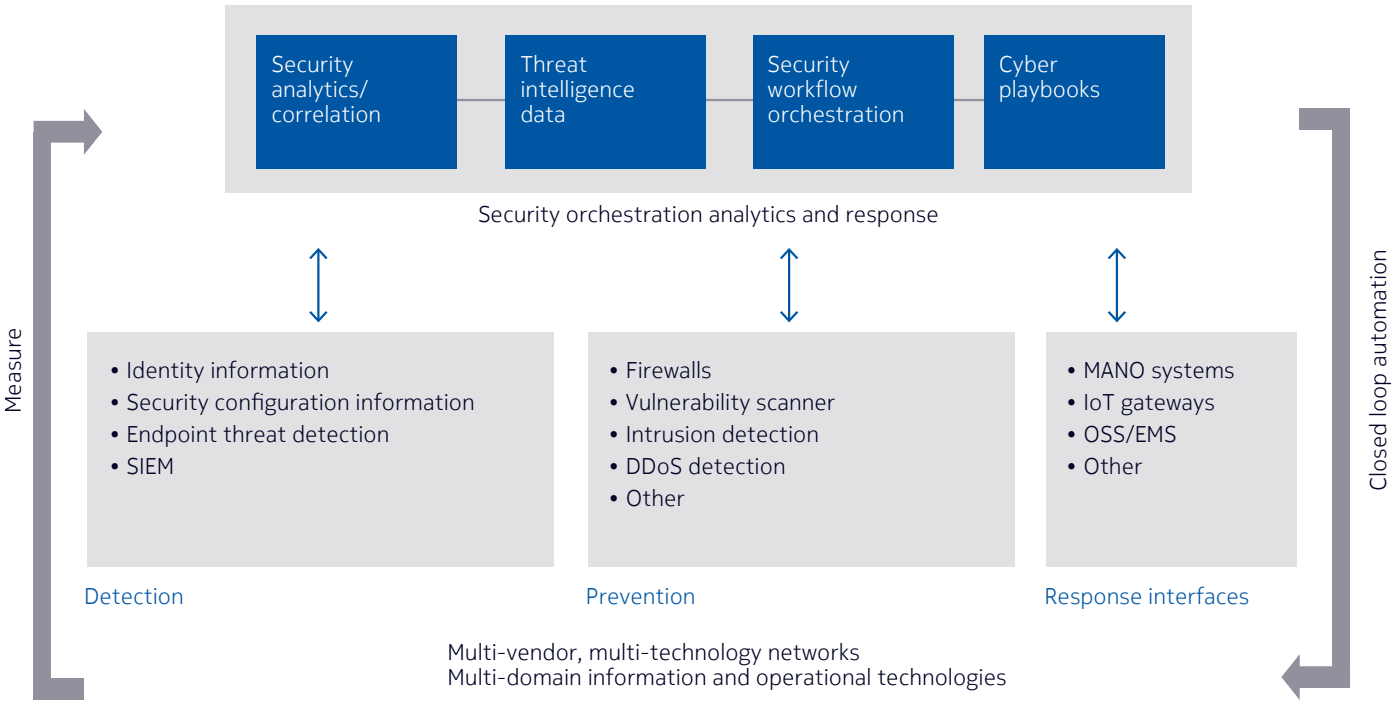
Nokia's NetGuard Security Management Center: a new solution for a new reality

NetGuard Security Management Center (SMC) is Nokia's portfolio brand for SOAR. The solution provides cognitive analytics, aggregates and correlates security data from a variety of sources, enriching it with a telco context to help security operations teams assess business risks, improve decision making processes, and better control costs and risks. It makes it possible to quickly identify trends and anomalies, and initiates automated responses by triggering cyber playbooks.

NetGuard aggregates inputs from various network and system data sources, and correlates this data to identify patterns that match specific threat vectors. As new threats are identified by Threat Intelligence, updated detection algorithms and playbooks are provided to meet these threats.

The NetGuard SMC solution includes an automation of typical day-to-day workflow, automation of analysis to increase efficiency and effectiveness of security investigation, and automation of threat responses to take automated countermeasures to respond to threats before data is exfiltrated. The solution manages orchestration processes, security policies and their lifecycle. Nokia's solution uses cyber playbooks (security operations workflows) to enable automated responses.

Figure 1. Nokia NetGuard security for workflow, analytics and threat response automation



NetGuard SMC is a single point of control for multi-vendor, multi-technology networks and environments. The easy-to-use software enables operators to monitor and control multi-vendor systems across the network. After integrating it with other security systems, regardless of the vendors, SMC can measure security status, manage incidents, vulnerabilities, security policies, and network access.

User and network entity behavior analytics

NetGuard's SMC analytics capabilities transform security data into security insights, delivering rapid identification of anomalies, threats, and network misconfiguration vulnerabilities. SMC analytics extracts and intertwines identity and network compliance information. Correlation of network configuration settings and security access events allow operators to learn normal behavior and trends to improve resolution of incidents and visibility into network deployment. SMC analytics learns network behavior, correlates network security access events and network configuration state to detect anomalies. It allows operators to anticipate, prevent, pin-point, and isolate security policy violations. Service providers can proactively prevent data loss, reduce performance outages and degradations to preserve revenue, improve customer experience, reduce costs, and exceed compliance.

Transforming security operations management

NetGuard SMC is part of a holistic security assurance strategy, providing a contextual view of security posture. NetGuard addresses the complex, heterogeneous, and demanding needs of security and network operations teams. NetGuard SMC rationalizes the output of multiple, siloed security technologies such as vulnerability assessment (VA) and SIEM systems. Rationalizing multiple sources of security data while providing contextual intelligence allows organizations to develop a more complete risk posture profile. Security operations teams are constantly challenged to direct limited resources at their most important problems.

SOAR is a key enabler for transforming security organizations from manually driven operations to intelligence driven security operation centers based on automation. NetGuard SMC is a security operations automation, analytics and reporting platform that consolidates data and extracts actionable insights from a variety of intelligence sources, and existing security technologies. By analyzing user behavior to identify bad actors, it provides threat indicators to potential insider threats. These capabilities help security professionals prioritize risks and automate security operations activities in the context of the attack surface and the business, and improves alert management by correlating and consolidating alerts from existing systems.

NetGuard SMC automates security processes to reduce resource drain and threat response times, while streamlining alert and incident investigations by reducing the time and number of staff required to investigate those alerts.

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code: SR1707013982EN (August)