Nokia NetGuard Security Management Center

NetGuard Security Management Center (SMC) is an easy-to-use security operations analytics and reporting solution that enables operators to prevent, pinpoint, and address security threats before they result in breaches. NetGuard SMC aggregates and analyzes and enriches security data from a variety of sources with a service provider context to help security and network operations teams assess business risks, improve decision making, control costs and risk. NetGuard SMC integrates security systems, regardless of vendor, to analyze security posture and manage incidents, vulnerabilities, as well as security policies and network aces. NetGuard SMC helps shrink detection time by 80 percent, accelerate recovery time by 75 percent, and investigation time by more than 50 percent.

As the cyberattack surface has grown, many of the technologies used to address it have contributed to security management complexity, often creating segmented data that requires a great deal of time and resources to unify. Many conventional security management solutions provide limited insight into the actual security posture of networks.

The SMC allows security and network operations teams to dramatically improve situation awareness, while improving operational efficiency by automating and guiding threat responses. SMC Analytics and Reporting provides insight into user and network entity behaviors, delivering an ability to extract and visualize insight from a variety of security intelligence sources.

Simplifying complexity

Flexible, future-ready, powerful
- NetGuard SMC supports physical and virtual, as well as traditional and software-defined networks.
- Dashboard reporting delivers real business intelligence to CxOs and technical stakeholders.

Proactive prevention
- SMC measures risk posture and the state of the environment.
- SMC risk detection engine recommends corrective actions and supports workflow automation.

Data analytics and reporting
- SMC provides big data architecture and customer defined, configurable dashboards.
Features and benefits

NetGuard SMC is a single point of control for multi-vendor, multi-technology networks and environments. Its easy-to-use software enables operators to monitor and control multi-vendor systems—network-wide. By integrating with other security systems, regardless of vendor, SMC can measure the security status, as well as manage incidents, vulnerabilities, security policies, and network access.

The SMC addresses the complex, heterogeneous, and demanding needs of security and network operations teams. SMC rationalizes the output of multiple, siloed security technologies, such as vulnerability assessment (VA) and SIEM systems. Rationalizing multiple sources of security data, and providing contextual intelligence allows organizations to develop a more complete risk posture profile. Security operations teams are continuously challenged to direct limited resources at their most important problems. The SMC delivers contextual security issues alerts help reduce attack surface and time.

Figure 1. NetGuard SMC to monitor and control network wide

NetGuard SMC is a security operations automation, analytics, and reporting platform specifically developed to address the unique and growing challenges faced by communication service providers and large enterprises. The SMC allows security and network operations teams to dramatically improve situation awareness, while improving operational efficiency by automating and guiding threat responses.

Deployment
Software is deployable under VMware ESXi/ vSphere. SMC software can be installed from images in the customer virtualized data center.

Data collection interfaces
REST, JDBC
Technical specifications and list of features

Platform details
- High availability
  - Not supported
- Scalability
  - Horizontal (Elasticsearch DB nodes)
- Databases technology
  - Elasticsearch (No-SQL)
- Virtualization
  - VMware vSphere 6 Standard
- Platform OS
  - RHEL 7.2
- Hypervisor
  - Type 1 (ESXi)

Virtual capacity footprint

Collection
- vCPUs
  - 4
- RAM
  - 48G
- Storage
  - 32G

Elasticsearch DB
- vCPUs
  - 4
- RAM
  - 48G
- Storage
  - 2T

Master node
- vCPUs
  - 4
- RAM
  - 48G
- Storage
  - 168GB

Tested load model
- Sessions collection from IAM
  - 1,100,000
- Fly out filter loading
  - 25,000 NE Ids
- Complex audits handling
  - Up to 3,500 parameters

Security issues creation on IAM O&M interface
- 800 parallels sessions on REST API

Smart security alers (IAM REST interface)
- ENSUS (Exceeded Number of Session for User)
- ENSEL (Exceeded Number of Sessions to Element)
- ENSIS (Exceeded Number of Session in System)
- COFUS (Connection from Unauthorized
  - COSA (using shared account)

Identify access manager analytics
- Number of sessions per network element over time
- Session duration per network element over time
- Most active users (user with the highest number of sessions)
- Most active users grouped by their function
- Most active users grouped by their IP Network elements with highest number of sessions split by user
• Total number of network elements by vendor and model
• Number of active sessions
• Number of connected users (users with sessions)

Security configuration compliance analytics
• Number of sessions per network element over time
• Session duration per network element over time
• Most active users (user with the highest number of sessions)
• Most active users grouped by their function
• Most active users grouped by their IP
• Network elements with highest number of sessions split by user
• Total number of network elements by vendor and model
• Number of active sessions
• Number of connected users (users with sessions)
• Device counts by vendor by day
• Device counts by model by day
• Top 5 resource types and subtypes
• Number of audits by model - start date
• Number of audits by model - end date
• Audit coverage info
• Device counts (vendor and model)
• CM NE count (vendor and model)
• Attr details
• Device list
• Top 5 NEs matched and mismatched

Audit compliance manager analytics
• Overall network compliance
• Executed audits
• Audited network elements
• Total number of matched parameters
• Total number of mismatched parameters
• Total number of missing parameters
• Compliance trend over time
• Audits per vendor
• Score by NE with standard
• Number of mismatched attributes over time
• Number of non-compliant audits over time