NetGuard Security Management Center

Nokia’s NetGuard Security Management Center (SMC) is a security orchestration automation and response system that aggregates, analyses, 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, and control costs and risks. It enables trends or anomalies to be quickly identified and initiates automated responses by triggering cyber playbooks. It performs the tasks of detection and incident management.

The NetGuard SMC solution provides incident management and includes an automated workflow/orchestration component that manages orchestration processes by automating security service deployments and management of security policies and provides security policy lifecycle management. Nokia’s solution makes use of Cyber playbooks (security operations workflows) to drive automated responses and actions to various threats and security alerts. Playbooks can integrate with other systems such as threat intelligence feeds, trouble ticket systems such as Remedy ARS, as well network management solutions.

NetGuard SMC aggregates inputs from various network and system data sources and correlates the 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.

NetGuard SMC is a single point of control of multi-vendor, multi-technology networks and environments. It is easy-to-use software to enable operators to monitor and control multi-vendor systems, network-wide. Integrating with other security systems, regardless of vendor, SMC can measure security status and manage incidents, vulnerabilities security policies and network access.

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.

NetGuard 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.
Active Security use cases

E2E SOAR use cases
- Continuous security audit and compliancy enforcement
- Detection & mitigation of malicious internal identities
- Detection of high rates of failed login attempts
- Detection of high rates of denied traffic
- Direct access anomaly detection
- Detection of firewall central management disablement
- APT detection correlating multiple cases

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

Data analytics and reporting
- NSMC provides big data architecture and customer defined, configurable dashboards and ad-hoc data feeds.
Key features and benefits

NetGuard SMC addresses the complex, heterogeneous, and demanding needs of security and network operations teams. The product 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. NSMC delivers contextual security issues alerts help reduce attack surface and time.

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

NSMC is delivered as VM based software using Kubernetes containers and following Nokia Software’s Common Software Foundation model.

Supported deployment models are:
- VMWare vSphere with with ESXi as the hypervisor
- OpenStack (Cloudband CBIS) with KVM as the hypervisor

Data collection interfaces

Syslog forwarding, REST API calls, RabbitMQ and Logstash connectors can be used for data ingestion

Technical specifications and list of features

Platform details
- High availability
  - Utilizing clustering techniques
- Scalability
  - Scalable Kubernetes based deployment
- Database technology
  - Elasticsearch (Non-SQL)
- Virtualization
  - VMware vSphere
  - KVM/OpenStack
- Platform OS – RHEL 7.6
Pre-built Incident Management for NetGuard Security Management Applications

- Continuous security audit and compliancy enforcement
- Detection & mitigation of malicious internal identities

Extras

- Flexible workflows allowing for easily modifiable semi or fully automated incident responses
  - Library of building block actions enable more rapid customization through simple drag and drop re-use capabilities
- Ability to customize Kibana based dashboards
- Custom incident management available from Nokia (data ingestion, incident types and playbook responses)

About Nokia

We create the technology to connect the world. Only Nokia offers a comprehensive portfolio of network equipment, software, services and licensing opportunities across the globe. With our commitment to innovation, driven by the award-winning Nokia Bell Labs, we are a leader in the development and deployment of 5G networks.

Our communications service provider customers support more than 6.4 billion subscriptions with our radio networks, and our enterprise customers have deployed over 1,300 industrial networks worldwide. Adhering to the highest ethical standards, we transform how people live, work and communicate. For our latest updates, please visit us online www.nokia.com and follow us on Twitter @nokia.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2020 Nokia
Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Product code: SR2009046880EN   CID: 200822