INTRODUCTION

With more than 65,000 people in over 120 countries, Nokia Siemens Networks is one of the largest telecommunications hardware, software and services companies in the world. The organization was formed in 2007 as a result of a merger between Siemens and Nokia with a mission to help communications service providers (CSPs) build more valuable customer relationships by improving efficiency and experience.

Key to this mission is Nokia Siemens Networks’ pioneering, centralized Global Service Delivery model which consists of integrated multi-technology, multi-vendor Global Network Solutions Centers which drive the world’s most efficient networks. More than 600 CSPs around the world tap into the products and services available through this network to reduce complexity within their businesses and networks, grow and retain their customer base and deliver innovative services.

THE CHALLENGE

As Nokia Siemens Networks established its global network which includes six data centers on four continents, the company knew it would face significant challenges related to data privacy and managing sensitive information in a highly distributed environment. Regulatory concerns differ widely around the world with compliance requirements for international data privacy laws varying by jurisdiction. Not only were sophisticated IT security solutions required but determining a way to optimize processes to identify high priority incidents and remediate based on risk would be essential.

Seeking a partner that could help, Nokia Siemens Networks turned to Host Integrity Systems, a professional services company capable of integrating different security and asset management programs into a uniform optimized escalation management system and process for multinational corporations. Together the companies addressed the challenge by deploying a suite of complementary IT security solutions, including the Sourcefire IPS™ and the HIS-developed Remediation Escalation Management System (REMS) Security Knowledgebase.

THE SOLUTION

Working closely with Host Integrity Systems and after extensive evaluation, Nokia Siemens Networks selected three security technology tools to create their security platform, the Sourcefire IPS for Intrusion Detection/Prevention, Qualys for vulnerability management and network auditing and LogLogic for log management. These systems were deployed in each of the six data centers around the world.

Nokia Siemens Networks used the following architectural criteria in the selection of the Sourcefire IPS:

- Placement of Sourcefire sensors as near as possible to assets being protected
- Visibility of network traffic: contextual awareness
- Manageability of remote site via out-of-band networks
- Scalability in terms of event correlation
- Comprehensiveness of policy coverage

Sourcefire Customer Case Study:
Nokia Siemens Networks: Creating Actionable Security Intelligence in a Global Infrastructure

About Host Integrity Systems

Host Integrity Systems, Inc. provides a variety of co-managed professional services and integration products to help organizations increase process efficiencies, reduce operational costs, increase stakeholder communications and maximize the effectiveness of the overall information security and risk management program. Host Integrity Systems has deployed remediation escalation management systems and processes at a range of leading global organizations and has several implementations currently underway.

www.hostintegritysystems.com

Benefits of the Sourcefire IPS to Nokia Siemens Networks include:

- Ability to identify critical issues more proactively
- Reduction in manual work related to management of policies due to intelligent automation
- Ability to customize scripts and signature
- Improvement of operational efficiency
- Effective use of existing infrastructure

Tim Larson

President and Founder, Host Integrity Systems, Inc.
“Sourcefire’s presence in the market, the coverage by industry analysts, and strong testimonials by other customers using the Sourcefire IPS were also important in the decision to select Sourcefire,” added Tim Larson, president and founder of Host Integrity Systems, Inc. “We deployed multiple Sourcefire appliances in the largest global data centers.”

The Nokia Siemens Networks Security Operations Center (SOC) could now begin receiving vast amounts of security information including vulnerability data, log data and attack data. The challenge then became how to consolidate the information from multiple systems and gain operational intelligence to remediate based on risk assessment in real time. In order to gain actionable security intelligence Nokia Siemens Networks needed a way to:

- Integrate SOC security data
- Amend that security data to include relevant asset and ownership information
- Push that information out to globally distributed CSPs that are multitasking with other organizations and managing those assets
- Establish remediation processes and enable Service Level Agreement (SLA) performance monitoring and centralized IT auditing

An Automated, Integrated Approach to Remediation Escalation Management
To tackle the challenge of turning security data into actionable security intelligence, Host Integrity Systems and Nokia Siemens Networks determined they would need a comprehensive approach that included discovering and changing processes in parallel with assessing and deploying technologies. They began with a detailed project plan that included eight phases—developing use cases, the business case, process discovery, solution concept, deployment, user acceptance, documentation and a next step roadmap. Working with Nokia Siemens Networks they established a Technology Integration Group and a Stakeholder Integration Group, held weekly meetings to foster ongoing communication and collaboration, and created a software tool to identify the stakeholder and technology integration gap and provide actionable security intelligence.

“What set this effort apart was undertaking the process integration in lock step with the technology integration and the extra consideration we gave to the stakeholders,” said Larson. “We needed to extend the technology platform to ensure that the data the systems gathered was presented within the right context, time and format for a variety of audiences. We gave considerable attention to capturing the use cases of the stakeholder environment.”

THE RESULT
Within nine months Nokia Siemens Networks and Host Integrity Systems launched an integrated, risk-based remediation escalation management system (REMS).

The REMS brings in data from four security technology solutions—alert data from the Sourcefire IPS, asset and vulnerability scan data from Qualys, security intelligence from VeriSign and log data from LogLogic. The effectiveness of the Sourcefire IPS, not just in detecting a threat within the network, but, equally, in helping determine the severity level of the threat, rooting out false positives and negatives and focusing on mitigating the threat are key factors contributing to the success of the REMS.

Each security event is automatically ranked based on risk, for example a one for a low risk event and up to a five for the highest risk event. The REMS correlates this data with asset classification and ownership data that is also given a ranking, again a one for a low-priority asset and up to a five for the highest priority asset. Multiplying the two numbers, a total risk factor is automatically...
“Nokia Siemens Networks has been able to reduce its mean time to remediate by a third so, for example, where it used to take six hours to remediate a vulnerability it now takes only four—the value of the Sourcefire solution and the other security technologies is undeniable.”

The effectiveness of the Sourcefire IPS, not just in detecting a threat within the network, but, equally, in helping determine the severity level of the threat, rooting out false positives and negatives and focusing on mitigating the threat are key factors contributing to the success of the REMS.

assigned to each event. Incident tickets are sent in real-time to CSPs for action and are prioritized based on the risk factor. The REMS tracks and provides additional relevant information to other stakeholders, including management and auditors, for example, SLA performance reports, notification and escalation reports, case history reports and operational reports.

By taking an automated, integrated approach to remediation and escalation management Nokia Siemens Networks has been able to:

• Protect access to and storage of sensitive data
• Reduce IT operational costs
• Reduce risks to business critical assets
• Increase Computer Emergency Readiness Team (CERT) and CSP productivity
• Facilitate compliance with regulatory agencies
• Track the remediation and escalation management process and monitor SLA obligations

“Organizations—particularly multinational entities—are looking to reduce operational costs by automating the flow of information,” observes Larson. “Automation is at the heart of the REMS—beginning with automatically integrating attack, incident and log data with asset and ownership data; to automating incident monitoring and escalation; as well as tracing of remediation processes. As a result, Nokia Siemens Networks has been able to reduce its mean time to remediate by a third so, for example, where it used to take six hours to remediate a vulnerability it now takes only four, and the value of the Sourcefire solution and the other security technologies is undeniable.”

Nokia Siemens Networks is realizing the following benefits based on the Sourcefire IPS:

• Ability to identify critical issues more proactively
• Reduction in manual work related to management of policies due to intelligent automation
• Ability to customize scripts and signature
• Improvement of operational efficiency
• Effective use of existing infrastructure

Looking ahead Nokia Siemens Networks and Host Integrity Systems are considering expanding the data provided by the Sourcefire solution to include real-time awareness of operating systems, services, client applications and protocols as they are added to the network.

Larson concludes, “Sourcefire integrated efficiently into the Nokia Siemens Networks global IT landscape. Now that we have an automated, robust system in place to streamline processes and decision making, we will continue to seek opportunities to feed more IT security data into that system and derive even more value.”