Rubidium™

Centralized cyber monitoring system

Features & Benefits

- VISIBILITY – single security dashboard for What, Who and When, displaying the type, targets and time of the attack
- REAL-TIME ALERTS – identification of potential attacks as they occur and warnings of anomalous network activity
- EVENT CORRELATION – Complex Event Processing (CEP) technology for reduced false positives and more effective detection
- ENHANCED ADMIN – control of access rights to applications, relevant sites, passwords and monitoring activity

THE CASE FOR CENTRALIZED CYBER MONITORING

PROBLEM

Nine out of ten sensitive networks can be compromised by sophisticated and unfamiliar cyber threats. Even networks protected by advanced cyber security tools are susceptible. Many of these cyber threats focus on confidential and classified information from heavily protected government and military networks, ultimately undermining national security. These attacks deliberately target selected high-profile targets, including mission critical control systems, national infrastructures, critical site security systems, safe-city networks and SCADA control networks.

To deal with a security breach one first has to see it. Today's security professionals use a range of different tools, each with its own operating system, user interface and dashboard. The use of multiple tools, as technologically advanced as they are, is only as effective as the eyes, brains and reflexes of the people who run them. A centralized security event management system empowers security personnel with single-screen visibility for more efficient detection and handling of cyber threats.

SOLUTION

Rubidium, Senstar's centralized cyber monitoring system, is a unique combination of a Network Management System (NMS) and an all-source cyber security situation awareness apparatus with the enhanced ability to facilitate operational responses to perceived threats.

Equipped with hassle-free, automated status collection from multiple sources, it provides wide-angle visibility of both operational and security status through a single console that displays "who, what and when".

Complex Event Processing (CEP) technology is used to perform sophisticated correlation analysis of system- and network-wide symptoms to reduce false positives.

Rubidium provides:

- Out-of-the-box online views and reports, which can be customized on the fly
- Real-time alerts to potential faults and threats, as they happen
- Notification of unusual or suspicious network activity

Rubidium can also be seen as a workflow enabling the delivery of best practices that support compliance initiatives. Designed with security in mind, it uses well-known and proven methodologies to “defend the defender” and features an intuitive user interface supporting PCs, tablets and smart phones.

SIMPLE APPROACH

Senstar’s SIEM offers an intuitive web based user interface which offers a simple to use operation while keeping the users on top of complex cyber security situations. The cyber threats and events are presented in three different views:

- SNAPSHOT of the current cyber security status of the network
- PHYSICAL presentation of the network on a geographical map
- NETWORK drawing of all elements and their connections

INTEGRATED ENDPOINT AND NETWORK SECURITY

Rubidium is fully integrated with various endpoint security suites for workstations and servers (disk encryption, media encryption, anti-malware and machine firewall) and with network-wide security systems (Firewall, VPN, IDS, IPS and Antivirus). The security threats and events identified by these applications are reported by the monitoring system, offering full visibility into the network’s cyber security status.

LAN MONITORING

Rubidium receives security events and threats reported by the Tungsten Cyber Security Ethernet Switch. It also generates security events according to analyzed data collected from various network devices (such as Ethernet switches and routers).

WIRELESS MONITORING

Major theft of data has been reported by attackers connecting wirelessly to access points from outside the site, simply bypassing the physical security perimeter. Our monitoring system actively detects any illegal wireless activity nearby.

DATA ACCESS CONTROL

In many environments, internal users have access to many of the informational and physical assets in a given facility. Once attackers have penetrated the network, they can easily find and extract important information with little resistance. Senstar’s centralized cyber monitoring system reports on abnormal use of servers, networks, and applications. Information is gathered from network-based sensors and reported back to Rubidium.

SYSTEM ARCHITECTURE

The monitoring system offers multiple connections to Senstar and third-party equipment, allowing you to monitor your network and discover suspicious behavior in all parts of your facility. It also integrates with PSIM and vulnerability-scanning tools, not only to detect threats but also, to provide advice on how to correct faulty configurations.

FEATURES

VISIBILITY

A single security dashboard presents What, Who and When, displaying the type, targets and time of the attack.

REAL-TIME ALERTS

IT and security teams use SIEM to help identify potential attacks or policy violations as they occur and to warn of anomalous network activity. Rubidium permits faster response times, allowing security teams to nip the threat in the bud. It also reduces damage from an attack and recovery time after an attack.

EVENT CORRELATION

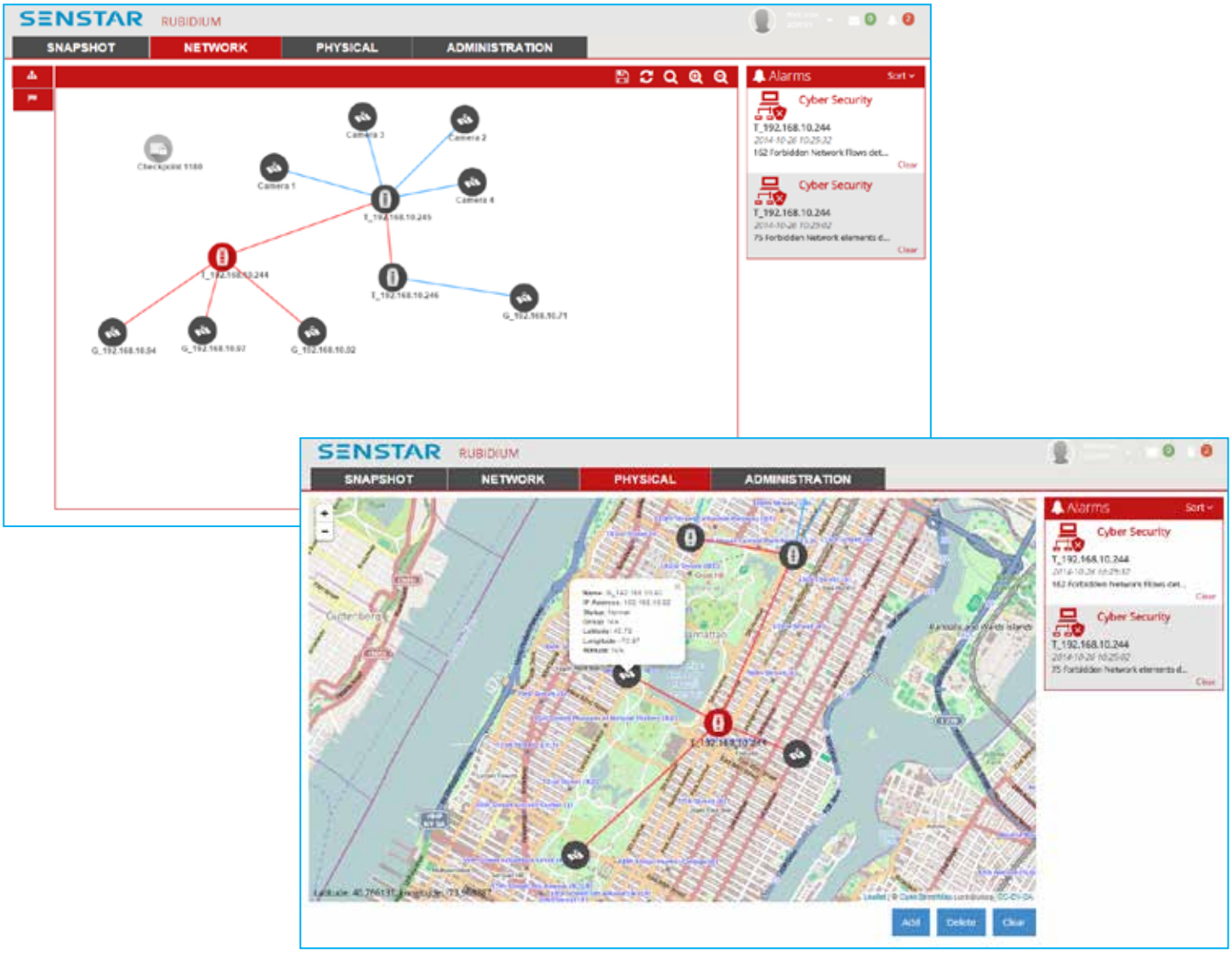
Complex Event Processing (CEP) technology performs a sophisticated correlation analysis of intrusion evidence for reduced false positives, more effective detection and to provide a bird’s eye view of incidents. Distributed architecture permits smooth processing and monitoring of numerous daily log entries.

ENHANCED ADMIN

For a more secure environment and convenient operation, the appliance enables the administrator to control access rights to applications, relevant sites, passwords and monitoring activity.

SOLUTION ARCHITECTURE

Senstar’s SIEM provides easy access to cyber security information by dividing the network to several default security domains which represents the physical, wireless networks, network security and servers and workstations. The administrator may edit the default domains and add new ones as needed.



OUR CYBER SECURITY VISION

CONVERGENCE

Perhaps the first official acknowledgment of the unavoidable link between physical and cyber security came in the form of US President Barack Obama's Executive Order on Improving Critical Infrastructure Cyber Security and his Presidential Policy Directive on Critical Infrastructure Security and Resilience in 2013. Those directives state that the protection of critical infrastructure is dependent on strengthening cyber security measures and increasing collaboration with IT and physical security stakeholders. They empower US federal agencies to implement holistic security measures to protect critical infrastructure, buildings, assets, information and people.

DEFENSE IN DEPTH

The Defense in Depth concept helps assure business continuity by defending a system against any kind of attack, using several different methods. Originally, the term Defense in Depth referred to a military strategy that aimed to delay, rather than prevent, the advance of an attacker by yielding space in order to buy time. In terms of network security, Defense in Depth tactics not only prevent attacks, but also buy an organization time with a forensic approach that detects and responds to threats, thereby reducing and mitigating the consequences of a breach.

MULTI-LAYER PROTECTION

Multi-Layer Protection describes the practice of combining multiple mitigating security controls to protect resources and data. A key Defense in Depth component, Multi-Layer Protection derives from a military strategy that involves multiple layers of defense that resist quick penetration by an attacker. The basic theory is that as an incursion progresses, resources are consumed and progress is slowed until it is halted and turned back. Within the Senstar context, Multi-Layer Protection is not only used as a delaying tactic but also as a first-layer threat detector and neutralizer.

Power Supply

AC Input	100-240V/50-60Hz
Power Consumption	750W
Power Supply	Single or Redundant (Optional)

Environmental Info

Operating Temp	+10˚C to +35˚C
Storage Temp	0˚C to +50˚C
Relative Humidity	10 to 80%
Dimensions	19” width /1U height
Weight	14Kg
Environment	RoHS compliant

Southbound Interface

Supported Protocols	SNMP v1/v2c/v3, Telnet, SSH/SSHv2, TR069, HTTP/HTTPS, TCP RAW Socket, UDP stream, REST JSON, Web Services, CORBA, RMI, FTP/SFTP/SCP

User Interface

Security	User authentication, Flexible profiles, Audit trail
Access	HTTPs, up to 10 concurrent user sessions
Technology	Install free, web UI thin client
Supported Browsers	Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari
Supported Clients	PCs, Macs, iOS and Android Tablets, Pablets and Smart phones

Optional Configurations

Site Rubidium	Level 1 server configuration, limited to 1,000 network elements
Extended Rubidium	Level 2 server configuration, unlimited number of network elements

Level 1 Server Configuration

CPU	Quad-core Intel® Xeon® processors 3400 series
Memory	Signal 8GB RDIMM 1600MHz
Disk	500GB, 7200 RPM, SATA 3Gbps
Network	4 x 10/100/1000Mbps auto-negotiate ports
Video	1280x1024 pixels, 32bits color, VGA port
Input Devices	Mouse, Keyboard

Level 2 Server Configuration

CPU	Dual Intel Xeon® E5-2620 2.00GHz
Memory	Dual 16GB RDIMM 1600MHz
Disk	500GB, 7200 RPM, SATA 3Gbps
Network	4 x 10/100/1000Mbps auto-negotiate ports
Video	1280x1024 pixels, 32bits color, VGA port
Input Devices	Mouse, Keyboard

Product Variations

Rubidium-T-50	SIEM appliance, Tungsten support, 1-year warranty and software license
Rubidium-T-SRV	Rubidium annual extended warranty and software license