Salvio NC SensiOS

NETWORK AND INFORMATION SYSTEMS (NIS) CYBER SECURITY SENSOR APPLIANCE

Salvio NC SensiOS combines the power of open source, proprietary technologies and the best of intrusion detection network security monitoring, detection and response systems into a single solution that mitigates serious and imminent threats to critical assets and empowers rapid response. Easily deployed, compatible with most popular operating systems, based on widely accepted standards and protocols, don't require any upfront cost or lead to any vendor lock-in.

Salvio NC SensiOS can be a great solution for small / medium sized enterprises as well as large companies looking for a solution to cybersecurity risk and incident managment, IT infrastructure security and monitoring.

NETWORK AND INFORMATION SYSTEMS (NIS) CYBER SECURITY SENSOR APPLIANCE

Salvio NC SensiOS

ESSENTIAL SYSTEM ADMINISTRATOR TOOL

CYBER-SECURITY RISK AND INCIDENT MANAGEMENT

- Improving cybersecurity resilience of business operations
- Compliance to EU NIS2 directive
- Cyber-security incident handling and investigation efficiency
- Improving IT System Administrator's efficiency and productivity
- Full installation, configuration and operations support
- Next generation cyber-security technologies

IT INFRASTRUCTURE SECURITY APPLICATION FIELDS

- Network Infrastructure Health Monitoring
- Network Activity Monitoring and Registry
- Malware and Virus Protection
- Malicious Activity Detection
- Log Aggregation, Archiving and Investigation
- Security Event Management
- Messaging, Reporting and Alert

FEATURES

- Network Service Quality Monitor
- Live Network Traffic AntiVirus Scan
- Packet, SysLog, WebGet, NetFile Registry
- Local Area Deception HoneyNET
- Network Intrusion Detection System
- Host Intrusion Detection System
- Network Anomaly Monitoring System
- Host Metrics Collection and Monitoring
- Alert and Event management Console
- Aggregated Log Scrutinizing Console
- Network Monitoring Event Log Console
- Notification Manager via Alerting Rules

Salvio NC SensiOS
USED TECHNOLOGIES

Deception HoneyNET - LAN honeypots package

Complete set of low-high level qeeqbox honeypots for monitoring network traffic, bots activities, and username / password credentials. This honeypots set is python application package that contains all the following services : dhcp, dns, elastic, ftp, http proxy, https proxy, http, https, imap, ipp, irc, ldap, memcache, mssql, mysql, ntp, oracle, pjl, pop3, postgres, rdp, redis, sip, smb, smtp, snmp, socks5, ssh, telnet, vnc.

Network Intrusion Detection - SURICATA

The Suricata Engine is a Next Generation Intrusion Detection and Prevention Engine developed and maintained by Open Information Security Foundation, Boston, Massachusetts USA. This engine is not intended to just replace or emulate the existing tools in the industry, but brings new ideas and technologies to the field. This new Engine supports Multi-Threading, Automatic Protocol Detection (IP, TCP, UDP, ICMP, HTTP, TLS, FTP and SMB), Gzip Decompression and Fast IP Matching. Suricata is also used for Network Packet Capture, File Extraction and HTTP Session Registry.

Host Intrusion Detection - SAGAN/LOKI

Sagan is multi-threaded, high performance, real-time log analysis & correlation engine developed by Quadrant Information Security, Jacksonville, Florida USA, that runs on Unix operating systems. It is written in C and uses a multi-threaded architecture to deliver high performance log & event analysis. Sagan's structure and rules work similarly to the Sourcefire Snort IDS/IPS engine. This allows Sagan to be compatible with Snort or Suricata rule management software and give Sagan the ability to correlate with Snort IDS/IPS data. Sagan supports different output formats for reporting and analysis, log normalization, script execution on event detection, GeoIP detection/alerting and time sensitive alerting. Log aggregation from network devices is performed by rsyslog, developed since 2004, by Rainer Gerhards at Adiscon GmbH., Großrinderfeld, Germany, and is used on UNIX and Unix-like computer systems for forwarding log messages in an IP network. For further analysis, logs are ingested into Loki - horizontally-scalable, highly-available, multi-tenant, log aggregation system.

Network Anomaly Monitoring - BRO/ZEEK

Zeek is a network security monitor (NSM) which purpose is to inspect network traffic and generate a variety of logs describing the activity it sees. It is developed since 1996 at Lawrence Berkeley National Laboratory, University of California, USA. Zeek's primary use cases involves near real time cyber threat hunting. Zeek uses common ports and dynamic protocol detection (involving signatures as well as behavioral analysis) to identify network protocols. Zeek monitor perform application layer decoding, anomaly detection, signature matching and connection analysis.

Realtime Network Flow Antivirus Scan - ClamAV

ClamAV antivirus is used for real-time scan of Suricata extracted files transmitted over the network. ClamAV is a cross-platform antimalware toolkit able to detect many types of malware, including viruses. The ClamAV virus database is updated at least every four hours and as of June 2023 contains more than 6 mln. virus signatures. Since 2007, by joining Sourcefire, the ClamAV team merged with the Sourcefire Vulnerability Research Team (VRT). In turn, Cisco acquired Sourcefire in 2013. The Sourcefire VRT became Cisco Talos, and ClamAV development remains there.

Post-processing Event Management Framework - EveBOX, PROMETHEUS, GRAFANA

EveBox is a web based alert and event management tool for sagan and Suricata IDS/NSM Engines. It provides the user an “inbox” style approach to event management if that is their preference, an additional method of searching events to log scrutinizing tools like Grafana Loki or Unix style lnav. Prometheus is a cross-platform application used for event monitoring and alerting. It records metrics in a time series database (allowing for high dimensionality) built using an HTTP pull model, with flexible queries and real-time alerting. Grafana is a multi-platform analytics and interactive visualization web application. It provides charts, graphs, and alerts from Prometheus time series database, acts as scrutinizing console for Loki log aggregation platform and is developed and maintained by international company Grafana Labs, with offices in New York City and Stockholm. In 2021, Grafana Labs secured a Series C funding round of $220 million.

Physical (x86-64) / Virtual Appliance - Unix type GNU Linux Debian OS

The small form factor of Lanner, SuperMicro, HP, Dell, Lenovo desktop and network/rack appliances can be used for system implementation, altogether with virtual machine installations on x86-64 processor type hosts. Stable version of Debian GNU/Linux OS, developed and maintained since 1993 by the Debian Project nonprofit organization is used for running all security applications. Agents/collectors can be installed on windows/apple workstations, logs, configs and network flows/statistics can be collected from all major network equipment manufacturer endpoints. The Debian Project is an association of individuals who have made common cause to create a free operating system. Debian's headquarters are located in Hauppauge, New York, US. The cost of developing all of the packages included in Debian 5.0 Lenny (323 million lines of code) has been estimated to be about US$8 billion, using one method based on the COCOMO model.

Salvio NC SensiOS

OPTIONAL FUNCTIONALITY AVAILABLE

Network infrastructure monitoring and alert - SNMP/IPMI/TCP over HTTP

Extra monitoring web dashboard displays brief review of the system and is accessible via openvpn or ssh tunnel. All monitored data is collected by Prometheus time series database. Operation system and application metrics are exposed by Netdata application. Log parsing is done by Grok, hardware tags and status of network interfaces is collected by Prometheus SNMP exporter directly from SNMP agents of network devices. Alarms and Alerts can be configured for any metrics of the dashbords, allowing briefly react to sensitive monitored system state changes. Each and every Graph(Panel) or Dashboard can be automatically converted to PDF document and mailed to pre-configured recipients based on predefined schedule. It allows system administrators present periodical report to company management without manual intervention.

Distributed Network Backup System - BAREOS

Bareos is a set of computer programs for managing backup, recovery, and verification of computer data across a network—providing a backup solution for mixed operating system environments. It is enterprise-level computer backup system for heterogeneous networks, its services communicate with each other over the network, and authentication is TLS/SSL-encrypted -– either via certificates or via pre-shared keys. Bareos encrypts the backups themselves (on the clients) as well as the communication between the individual computers.

Inspection of SSL/TLS encrypted Traffic - HTTPs/SMTPs/IMAPs Proxies

SSL/TLS inspection of HTTPs, SNMPs and IMAPs traffic is a way to identify malicious activity that occurs via encrypted communication channels. SSL/TLS inspection works like an authorized man-in-the-middle (MitM) attack, where the encrypted traffic between the client and the server is decrypted and examined. It allows to prevent data breaches by finding hidden malware and stopping hackers from sneaking past defenses, see and understand what employees are sending outside of the organization, meet regulatory compliance requirements, ensuring employees aren't putting confidential data at risk, support a multilayered defense strategy that keeps the entire organization secure

FOR ADDITIONAL INFORMATION PLEASE CONTACTS US

e-mail: salvio@montm.art
Tel: +370 698 36598
Web page : http://salvio.montm.art:796
Demo at : http://snc-sensios.montm.art:3000