Security Information & Event Management (SIEM+)

WHY YOU NEED
SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)

A SIEM reduces the noise and complexity of multi-layered ecosystems, bringing information together to:

- close security gaps
- prevent breaches or discover them early so they can be remediated quickly
- increase productivity

A SIEM is a vital part of an incident response plan that minimizes data and revenue loss and ensures business continuity. Effective incident response is not possible without a SIEM as there would not be a system to raise incidents.

WHY CHOOSE NETWORK BOX USA
SIEM+

Delivered purely as a cloud-based solution, the Network Box USA Security Information & Event Management+ (SIEM+) solution integrates all security logs and incidents into one centralized system. This gives a business an overview of the entire network.

How is this done? An advanced Correlation Engine is at the heart of SIEM+. Designed to take a high-level perspective of individual data items, and correlate them into actionable security incidents, SIEM+ is used to co-ordinate an integrated, multi-level cyber defense posture. It provides:

- comprehensive network visibility
- a demonstrated compliance with automated cloud-based reporting and back-up
- the means to respond to incidents faster minimizing downtime, and any potential data or financial loss

SIEM+ also leverages security intelligence feeds from its Reputation Database (RepDB). These, as well as intel from other sources, are brought into the system to provide threat indicators. Today, it tracks tens of millions of reputation signatures, covering hundreds of millions of individual items. In fact, RepDB is growing by over 200,000 signatures every month.

SIEM+ IS POWERED BY NETWORK BOX USA

BEST-IN-CLASS THREAT INTELLIGENCE

ZERO-DAY THREAT PROTECTION

SELF-OPERATED SECURITY RESPONSE CENTER

3 ISO Certifications
PCI DSS 3.2 attestation
70+ threat intelligence partners

FULLY STAFFED SECURITY OPERATIONS CENTER

UNIFIED MANAGEMENT GUI

Network Box USA SIEM+ Provides an Overview of a Business Network

SIEM+ MONITORS EVERY DEVICE ON A NETWORK IN AN EFFICIENT AND COST-EFFECTIVE MANNER

SIEM+ FEATURES

Bird's Eye View of Network & Security Events

A holistic view of all your networks and every single device connected thereto. Event data from everything monitored streams into the Event Store. This includes network events from servers, switches, routers, servers, workstations, security devices, IoT devices and more. Also, security events from firewalls, virtual private networks, intrusion detection systems, intrusion prevention systems and databases.

Cyber Threats

The Correlation Engine analyzes incoming data and correlates it into actionable security incidents. Using rules, heuristics, and custom tuning, it identifies then classifies incidents. The engine also correlates your events with those from other parts of the world so we can spot trends of an oncoming attack and/or one that is being developed. A machine learning system augments the rule system to increase the ability to identify anomalies. Security incidents (both active and past) are maintained in a separate highly optimized, reliable, and scalable Incident Store.

Threat Intelligence & Analyses

True real-time threat analyses and data are garnered from over 70 global security partners. This and intel from 250,000 honeypots are housed in the Network Box USA RepDB (Reputation Database), a vast, ever-growing repository of info and data which analyzes and categorizes said analyses and data. After which, signatures are created and SIEM+ can use them to correlate them with your events.

Powerful Search Capabilities

Powerful online search facilities for events, incidents, assets and much more. Search facilities are also used to search across, and drill-down into, both security incident data, as well as the raw log records.

Alerting System

Notification and alerts for critical security incidents, in true real-time. Response management tools are provided to assign incidents, update, and respond appropriately. Filters identify information sources, classify, categorize, and store the raw event data in the Log Store.

Reporting Capabilities

True real-time, fully customizable reports. Periodic and on-demand reporting, as well as real-time dashboards are provided.

Data Storage & Log Retention

Geographical cloud clusters for data storage and log retention. All data is stored in triple copy.

NETWORK BOX USA SIEM+ DATASHEET (security incident & event management+)

SIEM+ SERVICE INCLUDES:

- ✓ SIEM Software
- ✓ Rules to correlate events and raise alerts on anomalies
- ✓ Machine Learning
- ✓ 15 days raw data Hot storage
- ✓ 75 days raw data Warm storage
  - This provides a total of 90 days of data accessible via the Dashboard
- ✓ Customizable raw data Cold storage for the total number of GB permitted
  - 275 data recommended by most compliance requirements, i.e., PCI DSS
- ✓ Reporting - preconfigured reports and dynamic reporting
- ✓ Service to add rules ad hoc for you
- ✓ Dashboard - to access the inline data, assets, information, incidents, and reporting.
- ✓ SOC services - with SOC II Type 2 certification
- ✓ Award Winning Network Box Threat intelligence Security Response integration
- ✓ SOAR
- ✓ IDS
- ✓ Free sensors for each device
- ✓ 8x5 support
- ✓ Incident Response