

# Real-Time Situational Awareness for SIEM Solutions

Security Information and Event Management (SIEM) solutions provide two main functions:

- Security Event Management (SEM), where security event data is processed in real time for incident response and threat management. Event data sources include firewalls, intrusion detection and prevention systems, networking equipment, security software, and host activity logs.
- Security Information Management (SIM), where log data is analyzed for compliance reporting and privileged user and resource access. Log data sources include host system and security logs, database activity and audit logs, directories, identity and access management (IAM) systems, application logs, and transaction logs.

One of the main obstacles faced by an organization implementing a SIEM solution is the overwhelming number of potential incidents produced, even a fraction of which may prove to be too difficult and time consuming to investigate.

The number of incidents reported must be considerably reduced to enable IT security to focus on and investigate those incidents that require their utmost attention. To this end, the automatic filtering of non-relevant incidents is imperative.

Despite receiving event and log data from multiple sources, SIEM solutions still lack the knowledge regarding the devices and users they are tasked to report about. This absurd situation helps inflate the number of potential incidents reported about the enterprise network.

Insightix BSA resolves this problem.

## **Total Network Visibility with Real-Time Network Intelligence**

Insightix BSA provides 24x7x365 network, device, and user intelligence, maintaining a real-time inventory of ALL assets connected to the enterprise network, their profiles, and the identities of those using the assets. Network information is continuously collected to reflect the actual real-time state of the network.

Insightix BSA detects 20%-50% of additional devices residing on an enterprise network, which otherwise would remain unknown.

BSA Visibility maintains a comprehensive profile for each device operating on the enterprise network according to its device type. An asset profile may include multiple parameters, such as MAC address, VLAN ID, VLAN name, IP address, device type, device capability, operating system, operating system type, patch information, switch and port connected to, open network services, user intelligence information, and so on.

Insightix BSA uses a powerful change detection engine capable of notifying information security and/or network operations when changes occur to the enterprise network (for example, a new device connects) and/or to a connected device (for example, a configuration change) in real-time.

Insightix BSA integrates with SIEM solutions using the Common Event Format (CEF). The network, device, and user intelligence information provided by Insightix BSA enables SIEM solutions to correlate event and log data with the actual assets for which incidents are reported. As a result, the number of incidents that may need further processing is reduced to a minimum. The following are a few examples of incidents that can be automatically ruled out:

- IPS event reporting a potential attack against a non-existent IP address
- IPS event reporting a potential attack against a different operating system than the one used on the target device
- IPS event reporting a potential attack against a network service not available on the target device, and so on.

## The User Intelligence Effect

Insightix BSA provides user intelligence, whereby user IDs are matched with IP addresses to form accurate identity discovery supported by comprehensive user identity information, including the user ID, real name of the person using the asset, email address, telephone number, access rights, and so on.

Correlating between the information provided by Insightix BSA and its other sources of information allows a SIEM solution to support multiple use cases relating to incident response:

- Manual efforts to track users are no longer required
- Users that are a target for an attack can be identified and notified minimizing the potential impact (correlation with IPS data)
- Malicious internal users can be tracked (correlation with IPS data)
- Users affected by a malware can be identified (correlation with network behavior anomaly detection system data), and so on

## True Device and User Identity Tracking

The vast majority of information coming from event and log data relates to IP addresses as the means for identifying the sources and targets of activities occurring on the network. The fact that IP addresses are dynamically assigned and reassigned, and the high frequency at which many devices connect, disconnect, and reconnect to the enterprise network, create an issue for organizations.

Insightix BSA provides the information that enables the correlation of event data indexed by IP addresses with the device for which the event was reported and with the user identity of the actual user that is either causing or impacted by the event.

Insightix BSA provides this capability by tracking devices by their MAC address, by correlating user IDs with the IP addresses they use, and by maintaining this information in real-time, updating a SIEM solution regarding any changes made.

## Completeness of Deployment

Using the information provided by Insightix BSA, additional sources of event and log data can be identified, thereby allowing the completeness of operation of the SIEM solution. Insightix BSA can be used in the pre-planning stage of SIEM solution implementation, identifying ALL event and log data sources that may need to send their information to the SIEM solution.

Network Utilities (Systems) Limited  
Liberty House, 516 Walton Road,  
West Molesey, Surrey KT8 2QF

Tel: +44 (0)20 8783 3800  
Fax: +44 (0)20 8783 3810  
Email: [sales@netutils.com](mailto:sales@netutils.com)  
Web: [www.netutils.com](http://www.netutils.com)