ARMIS®

SOLUTION BRIEF

Armis Network Threat Detection & Analysis

The Problem

Security teams face many challenges when it comes to detecting threats in in their environment, inluding those targeting IT, OT, BMS, IoT, and IoMT assets. In complex network environments, security teams may lack full visibility into all assets across network segments and systems. This limited visibility can hinder threat detection and incident response efforts. Further, without sufficient contextual information about every asset in the environment, it becomes challenging to differentiate normal from abnormal behavior. Addressing these challenges requires the ability to collect a real-time and historical record of what's happening on the network.

Enterprise Wide Network Threat Detection and Analysis

Detecting threats through network monitoring is one of the cornerstones of threat management in security operations. The overall quality of threat management can be only as good as the input data. No security operations will be complete without strong network threat detection capabilities. Complete network visibility for every asset with full asset context allows SOC teams to automatically detect threats, exploit attempts, and suspicious/anomalous behavior across the entire environment - **IT, OT, BMS, IoT, IoMT.**

Monitoring network traffic allows security teams to detect threats and attacks in their early stages. By continuously analyzing network data and traffic patterns, they can identify anomalies and indicators of compromise that may indicate a potential security breach or threat actor's presence. This network traffic analysis ensures that security teams can proactively identify and mitigate potential threats before they can cause significant damage. Network traffic analysis can also be used to identify and block malicious activities, such as unauthorized access attempts, malware infections, or suspicious network communications, effectively preventing security incidents. Further, continuous network monitoring provides crucial data for incident response efforts. In the event of a security incident, monitoring tools capture relevant information, including the source and nature of the attack, the affected systems or devices, and the extent of the compromise. This information aids in the investigation, containment, and recovery processes.

The Armis Centrix™ Solution

The network threat detection and analysis capabilities of the Armis Centrix™ cyber exposure management platform provide security operations teams with full visibility to network-based threats in their environment. Armis detects known and unknown attacks by continuously analyzing the network traffic and identifying malicious and suspicious behaviour. This includes signature-based known attacks such as Log4j and SQL Injection, but also IOCs like Brute Force, Port Scan and abnormal asset behavior.

Centrix™ identifies and logs communication attempts to malicious or suspicious domains/hosts, allowing SOC personnel to investigate a device's network activity timeline before, during and after an incident.

With Armis Centrix™ network detection and analysis capabilities, security teams are better equipped to make informed, data-driven prioritization security response decisions based on data collected from the network.

Summary

The Armis Centrix™ cyber exposure management platform offers a single-source-of-truth for all data sources and eliminates the need for manual cross-referencing, saving organizations valuable time and reducing the risk of errors. By leveraging contextual intelligence provided by the Armis Asset Intelligence Engine, organizations can prioritize remediation efforts based on risk and criticality. Lastly, by streamlining the process of identifying and managing all assets, Armis helps organizations maintain a strong security posture, reduce their attack surface, and protect their brand.