seceon

DATA SHEET

Vulnerability Management

Vulnerability Scanning and Assessment is necessary for maintaining information security. It helps you identify the weak spots in your ecosystem and take corrective actions befare attackers can exploit to steal data or disrupt business. Vulnerability assessment sean identifies and reports known system' vulnerabilities.

Seceon aiSIEM provides deep integration with the vulnerability scanning and assessment product OpenVAS as an integral part of the solution. The platform includes provisioning of the scheduled automated vulnerability sean, identification of CVES, report generation, and delivery to stake holders. All of these is done automatically along with audits of these activities. Threat hunting capability integrates identified vulnerability for very effective analysis by the SOC team. The platform's AI engine correlates identified vulnerabilities into security alerts for continuous rich threat detection and response. Also, the platform's comprehensive integration of vulnerability assessment substantially separates itself and provides a competitive edge to our customers against silo vulnerability assessment tools with minimal integration by other SIEM platforms.

KEY BENEFITS

COMPREHENSIVE COVERAGE AND VISIBILITY

Continuously scans and identifies the vulnerabilities with accuracy, protecting your devices on premise, in cloud and endpoints.

CONTINUOUS MONITORING AND ALERTING

Proactive alerts about the potential vulnerabilities which can be addressed before turning into gateways for threats.

ACCURATE AND PRIORITIZED SCAN RESULTS

Powerful and accurate data analytics and reporting.

UNIFIED SOLUTION

Single platform with VA functionality without the need for integration and license maintenance.

PREDICTABLE TCO

No additional capital expenditures, SMEs, infrastructure or software to deploy and train the SoC.

As part of a complete package of security monitoring and management capabilities far efficient threat detection, VA Sean offers visibility of vulnerabilities that exist in the network:

Host: Need to enter the name of the target host you want to sean

Network: Need to enter the network range you want to sean

IP Address range: Need to enter the IP range you want to sean

The VA sean requirements are driven by customer use cases and evolving IT Infrastructure technologies & environments. This includes,

On Demand: Any changes to the devices (adding a new device, open/close a port or apply a patch etc.) should immediately be followed by another vulnerability sean.

Scheduled Sean: Regular vulnerability scanning is necessary for maintaining information security.

Continuous Vulnerability Management calls on security practitioners to Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Organizations should maintain baseline reports on key equipment and should investigate changes in open ports are added devices. VA sean will detect issues such as missing patches and outdated protocols, certificates, and services.