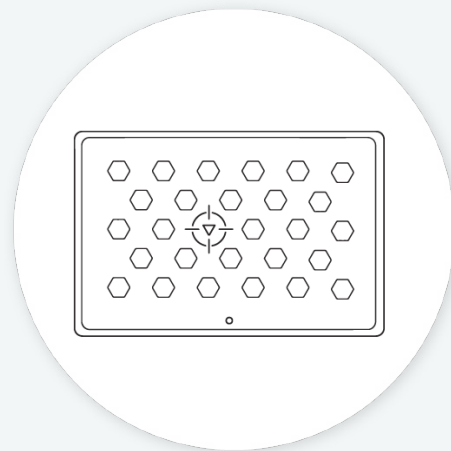# pch technologies
POWERED BY SKOUT

Network Security Monitoring

AI Powered Network Protection

SKOUT Network Security Monitoring is a managed security product that provides network intrusion detection with a physical or virtual appliance. Suspected threats are correlated for AI-enabled analysis using SKOUT's analytics platform, SIEM, threat intelligence, and 24/7 365 Security Operations Center. Detect potential threat activity on your network like command and control connections, denial of service attacks, data exfiltration and reconnaissance.

DENIAL OF SERVICE (DOS) ATTACKS

Identifying unusual traffic from organization-owned devices, being leveraged to perform a denial of service attack

CROSS-SITE SCRIPTING

Identifying web server–client network traffic patterns indicating cross-site scripting attacks (XSS)

SQL INJECTION

Identifying layer-7 network signatures indicating a SQL injection attack designed to exfiltrate data from vulnerable web applications

FTP & CLOUD STORAGE EXFLITRATION

Monitoring network traffic over protocols that facilitate large data transfer and alerting when unusual quantities or file types are being transferred, or when the target is unknown or malicious

COMMAND & CONTROL COMMUNICATION

Correlates network traffic to discover malware communicating with external attackers, which is a sign of a compromised account

KEY FEATURES

Network Intrusion Detection

SIEM Analysis

AI Analytics Engine

Multi-tenancy Dashboard

Self-service Reporting

Physical or Virtual Appliance

Supports key industry and regulatory compliance standards such as continuous monitoring and network monitoring

pchtechnologies.com

info@pchtechnologies.com

(856) 754-7500