R10.1 Scope of Services

Security risk and compliance management

XDR Services solution enables SOC to detect both signature-based malware with precedence and zero-day threats without precedence, leveraging behavioral analytics, thereby thwarting the kill chain, minimizing the extent of damage (risks) and responding to the malware, viruses, attacks and suspcious activities quickly and effectively. Associated level of risk and urgency is derived through computational statistics and is varied across the life of the threat being monitored through Alert Management.

Threat intelligence services

By design, XDR Services enriches event information (from logs and network flow traffic) with Threat Intelligence data, Geo location and historical context in real-time. Threat Intelligence data is gathered from 70+ Public sources and optionally other private/3rd Party feeds, relating to URL Reputation, Bad Domain, Suspicious IP Adresses, BotNet channel etc. Insights drawn from this data result in Threat Indicators that are then correlated with user activities, host specific events and network behavioral analytics, resulting in Alert/Incident notification.
Refer to these sections in the document "aiSIEM Solution Doc":
- Section 4.1 (Threat Intelligence)
- Section 4.1.1 (Threat Intelligence Feed for Airgap Networks)

Threat monitoring (SIEM/UEBA)

XDR Services solution is defense in-depth by design, organically and seamlessly incorporating the essence of SIEM, UEBA, Threat Intelligence, IDS/IPS, Network Behavioral Anomaly Detection, SOAR and Vulnerability Assessment. The system looks for anomalies and correlates them to paint the complete picture while triggering alerts with minimal false positives and false negatives, ultimately recommending and/or invoking appropriate containment action. This entire process takes only a few minutes to arrive at Threat Indicators (TI), as compared with legacy SIEM that rely on human analysis and data ingestion over the course of several hours or days to determine severity of threats and suggest necessary actions.

Seceon’s aiSIEM solution addresses a comprehensive list of threats, exploits, attacks, suspicious activities and non-conformance/non-compliance items, including Zero-Day and advanced malware with sophisticated evasive techniques. A sample subset of threat coverage is captured in section 3 (XDR Services – Threat Coverage Overview) of aiSIEM Solution document.

Security Dashboard Reporting and Analytics

XDR Services comes with several (25+) high-level interactive reports (e.g Performance, Behavior Analysis, Alerts etc) and many more granular reports (e.g Hosts Status, Traffic/Flows, Inventory, Operations, NIST Compliance, HIPAA, PCI-DSS etc) presented through the on-screen dashboard and can be exported in different formats.

XDR Services portal has a powerful display that shows event trends (by origin and no. of instances) for each alert type, critical or major, plotted on a timeline alongside severity and confidence to create a cohesive picture for analysts, managers and senior leadership. Also, Security Posture report graphically presents historical trend over a selected period, going back several months

Incident Response & Remediation Capability

XDR Services has automated, semi-automated (Alert based) and playbook based (SOAR) remediation features as part of rapid and orchestrated response to incidents. The solution generates major and critical alerts, for external and internal threats/attacks, backed by Threat Indicators collated from host based events, network activities, user-entity behavioral analytics and threat intelligence. Also, vulnerability assessment data is added to the mix for better prognosis.

Refer to these sections in aiSIEM Solution doc:

- 4.17 (Automated Threat Detection & Remediation)

Threat hunting

XDR Services comes optionally with Network Traffic Analyzer (NTA) which acts as Intrusion Detection System (IDS) that is capable of deep protocol analysis. It runs on an ethernet interface and creates logs based on the analysis of the traffic that flows through the interface. By analyzing raw unencrypted network traffic, it generates log messages categorized by common protocol types such as HTTP, FTP, SMB, DNS, DHCP, SMTP, IRC etc. The system can also capture log for file exchanges and known services. These logs are forwarded to the APE for further processing.

Any alerts based on threat indicators arising from NTA will be displayed on aiSIEM Portal. Use cases addressed by NTA include Prohibited URL and Domain Verification, Undesirable File Hash Detection, Keyword Matching and Information Leakage Detection (e.g Credit cards, PII).

Vulnerability scanning, patching and management

XDR Services comes with aThreat Hunting tool called Deep Tracker. It is used effectively for deeper analysis of Threat Indicators, with the ability to drill down into raw event data and/or network flow attributes. Custom queries can be created using Lucene Query Builder or Syntax-based Command. Threat Hunting analysis can be spread across a variety of attributes over flexible time periods:

- Event Type (Abnormal File Access, Account Lockout, Anomalous Beacon Behavior, Blacklisted Site Access, Data Upload/Download, Evasion, Exploit, Host Port Scan, Privilege Change, Suspicious Process, TCP Recon etc)
- Source (IP Address, Host Name, Port, Country, Network)
- Destination (IP Address, Host Name, Port, Country, Network)
- User Name
- Email-ID
- Domain Name
- MITRE ATT&CK Technique-id
- Trusted Event

Single sign on integration for customer facing portal(s)

XDR Services Portal serves as the fusion plate for vulnerability assessment scan data, whether these are fed through Seceon's OpenVAS tool (optional add-on), or 3rd Party vulnerability scanners (QualysGuard, Nessus). As such, the Open Threat

Single sign-on integration for customer facing portal is available for standard authentication services such as Windows Active