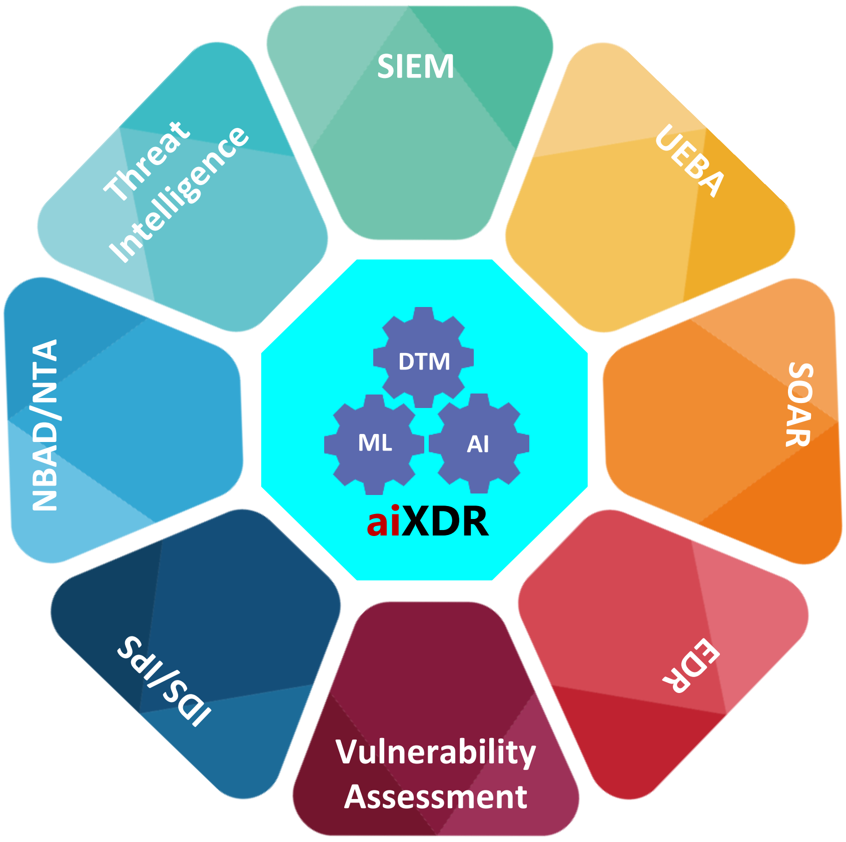
seceon

Datasheet

aiXDR™

Seceon aiXDR takes a holistic approach to cyber security by gathering deep insights from endpoints, servers, network devices, applications, IOT and security systems and applying user identity, threat intelligence and vulnerability assessment to establish threat profile, generate threat indicators, raise essential alerts and offer remediation path – automated or triaged. In essence, the solution ensures defense in-depth threat detection and response, relying on EDR, Network Behavior, Advanced Correlation (SIEM), Network Traffic Analysis, UEBA (ML based) and SOAR for an All-In-One experience that is organically and seamlessly fused together.

- ☑ Endpoint Security with agent-based and agentless technology for Windows, macOS and Linux OS
- ☑ Behavior baselining with applied Machine Learning for users and entities based on host centric insights (services, processes, file access, telemetry etc) and network flows
- ☑ Data Exfiltration (breach), Insider Threat and DDoS Attack detection with network traffic pattern analysis
- ☑ Exhaustive reporting across several key areas - security, compliance, operations and investigation.
- ☑ Rules based policy creation, enforcement and notification for appropriate action and governance.



Single Pane of Glass

Rest assured with total protection against cyber security threats, exploits and attacks across your servers, endpoints and applications in the Cloud, On-Premise, Edge (IIoT & IT-OT) and Remote Workplaces.

Automation with ML & AI for Accurate Detection

Reap the benefits of automation through Machine Learning for anomaly detection, and Artificial Intelligence for Dynamic Threat Modeling (DTM) as accurate decisions are made around threat indicators and risks are mitigated before they turn into incidents.

Securing Remote Endpoints

Apprehend brute-force attacks on endpoints leading to Compromised Credentials or, VPN browsing through covertly accessed torrent clients causing malware/webshell infestation, and ultimately protect your valued digital assets.

MITRE ATT&CK Modelling

Leverage MITRE ATT&CK Tactics, Techniques and Procedures to model actual intrusions and attacks, focusing on kill chain activities such as reconnaissance, beaconing, evasion, privilege escalation, lateral movement and exfiltration.

Instantaneous Response

Activate instant response to governance policy violations through user defined controls and initiate automated remediation to threats with high severity and confidence level, targeted at business-critical assets.

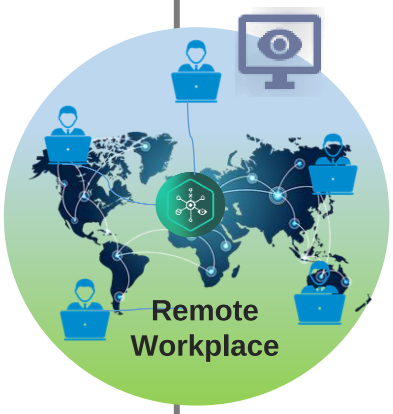
Exhaustive Visualization & Reporting

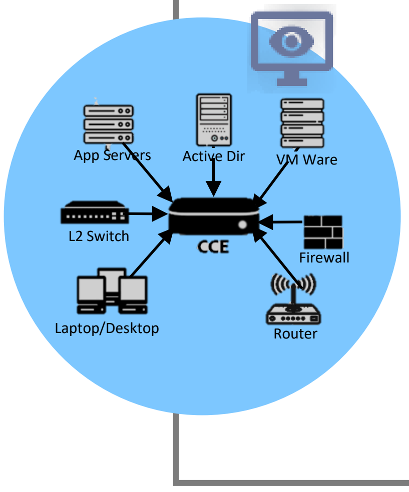
Monitor your IT assets 24x7 with myriads of behavioral attributes, prioritized statistics, performance indicators, drill-down datapoints and consolidated reports – visual and tabular – ensuring rapid attack / breach detection, regulatory compliance, threat hunting, operational oversight and executive summary.

CYBERSECURITY SOLUTION FOR ALL

1. Highly Scalable Solution for *all types of organization* – Small Medium Business to Large Enterprise
2. Hosted On-Prem or Cloud with *reduced operational complexity* for SOC Analysts
3. Managed SOC / MDR option for MSSPs to apply *multi-layered cyber security solution* through a *Single Platform*
4. Flexibility to activate *built-in options* – Network Traffic Analyzer (IDS), Vulnerability Assessment Scanner and Netflow Generator

Use Cases and Threat Types Addressed by Seceon aiXDR





- Cyber Crime
- Insider Threat
- Data Breach (Exfiltration)
- DDoS Attack
- Web Exploit
- Brute-Force Attack
- Vulnerability Exploit
- IoT-IIoT Security
- DNS Protection
- Endpoint Isolation
- Threat Containment
- Data Loss Prevention
- Deep Threat Hunting
- File Integrity Monitoring
- MITRE ATT&CK TTPs
- Policy Enforcement (Network, Database, Internet etc)

Extended Coverage with Seceon aiXDR

Amazon/AWS
➡ CloudWatch, CloudTrail, S3, RDS

Microsoft Azure Environment
➡ Network Watcher, Azure AD, NSG, Government Cloud, Cloud App Security, M365/O365

Google Cloud
➡ StackDriver Flow Logs, Pub/Sub APIs, G Suite

Other Cloud (IaaS / SaaS)
➡ Oracle Cloud, Service Now, Slack

Endpoints
➡ Windows, macOS, Linux Desktop

On-Premise Infrastructure
➡ Servers: Windows, Linux, DNS, DHCP, FTP, SMTP
➡ Database: Oracle, MS-SQL, MySQL, Postgres
➡ Other: Network based Anomalies, 3rd Party Security Tools, Vulnerability Scanners, IoT-IIoT Devices, IT-OT Systems

PRODUCT FEATURES	aiSIEM	aiXDR
Automated Threat Detection with Real-time Processing		
Cyber threats, attacks and compromise detection automated across physical and virtual hosts (On-Premise, Cloud and Hybrid)	✓	✓
Threat Indicators (IoCs) with underlying evidence, frequency and contextual significance for both internal and external adversaries	✓	✓
Threats, alerts and events focused on hosts, users and entities (IP Address, Port, DNS, DHCP, Applications etc)	✓	✓
Dynamic Threat Models with preconfigured, self-adjusting rules sorting out actual "threats" among thousands of indicators	✓	✓
Threat detection across wide spectrum - known vectors/signatures, unknown vectors (Zero-Day) and advanced evasive techniques	✓	✓
Customized threat detection to capture policy violation and user, host or entity based activity tracking	✓	✓
Suppress false alarms by flagging and notifying AI engine to adjust Dynamic Threat Model	✓	✓
Automated and Semi-Automated Remediation		
Built-in automation to enforce instant remediation, eliminating human intervention and business disruption	✓	✓
Multi-pronged remediation - policy enforcement, isolating host and blocking user (credential) - through seamless integration with Firewall, NAC and IDS/IPS	✓	✓
One-click action to enforce rapid remediation within the context of an alert without the need to create playbooks	✓	✓
Advanced Correlation with Contextual Enrichment		
AI with Actionable Intelligence leading to alerts with appropriate severity and confidence level	✓	✓
Event correlation across various time slices, source and event type	✓	✓
Contextual enrichment with Threat Intelligence (70+ sources), geo-location, vulnerability scan data and historical information	✓	✓
Network Behavior Anomaly Detection and Network Traffic Analysis		
Network protocol analysis with built-in Intrusion Detection System (IDS)	✓	✓
Detailed network traffic view across the network infrastructure	✓	✓
Domain Verification, Undesirable File Hash Detection, Keyword Matching and Information Leakage Detection (e.g Credit cards, PII)	✓	✓
User Entity Behavior Analytics		
Leverage Machine Learning algorithms to create models of user, host, application and network behavior	✓	✓
Profile user activities and capture suspicious behavior with unsupervised and semi-supervised Machine Learning	✓	✓
Constantly improve ML prediction with historical data	✓	✓
Visualization, Alerts, Notification and Incident Management		
Dashboard with unified view of all events, threat indicators and alerts across the protected environment	✓	✓
Graphical and tabular representation of network flows, events, alerts, trends, activities, asset interactions, application traffic and Windows/Linux services	✓	✓
Comprehensive interactive visual interface to drill down into threats related to affected sources and targets	✓	✓
Alert notification to SOC Analysts via email and integration through interfaces such as OpenDXL and aiSIEM's API functions	✓	✓
REST API based queries into alerts, events, flows and Threat Indicators for 3rd Party Systems	✓	✓
Integration with Service Desk/ ITSM platforms like Service Now, Jira, BMC Remedy etc for end-to-end Incident Management	✓	✓
Threat Hunting and MITRE ATT&CK Framework		
Deeper analysis of Threat Indicators, with the ability to drill down into raw event data and/or network flow attributes	✓	✓
Custom queries with Query Builder or syntax-based commands across a variety of attributes over flexible time periods	✓	✓
Insights on adversarial tactics and techniques based on MITRE ATT&CK framework directly mapped with threat indicators	✓	✓
Log Collection, Retention and Forensics		
Structured and unstructured data collection (agentless) from raw log, syslog, network flows, scan data, security tools etc	✓	✓
Cloud infrastructure security feeds from Azure, AWS, GCP, Oracle, Azure AD, M365 /O365, G Suite	✓	✓
Logs and traffic from standardized lightweight *NIX or windows systems in SCADA/ICS environment and IoT devices	✓	✓
Log Archived optionally upto 7 years in On-prem, 3rd Party or Cloud (Amazon S3) storage	✓	✓
Logs stored in raw form with original timestamp and audit data for chain-of-custody, regulatory compliance and forensic needs	✓	✓
Rapid Forensic analysis with filtered search and standard queries using Boolean operations	✓	✓
Administration and Provisioning		
Centralized administration and provisioning with geographically dispersed deployment	✓	✓
Provisioning for Blacklisting (IP Address, URL, domain, country, application) and Trusted List (devices, domains, entities)	✓	✓
Auto-discovery of assets for classification, alert prioritization and remediation measures	✓	✓
On-Portal configuration for Azure, AWS and GCP	✓	✓
Custom network policies for control, tracking and alerting against violation	✓	✓
100+ connectors and parsers for event collection across applications, tools and databases	✓	✓
Data encryption for data at rest and in motion	✓	✓
Multi-factor user authentication	✓	✓
Continuous Compliance, Audit and Reporting		
Security Posture Report with executive dashboard	✓	✓
Regulatory Compliance Reports focused on NIST, PCI-DSS, HIPAA etc	✓	✓
Operations Related Reports with IP Flows, Asset Groups, Hosts, Applications etc	✓	✓
Investigation Oriented (FTP Activity, SMTP Activity, Remediation Report etc)	✓	✓
On-demand and scheduled reports delivered to users selectively	✓	✓
De-risking of remediation by tracking and reporting all actions for audit	✓	✓
Multi-tenancy		
Multi-tenant by design with logical separation of data, analytics, ML and AI rule-set	✓	✓
Visibility to data limited to users and access privileges within each tenant	✓	✓
EDR		
Gain deeper insights into processes, services, executables and files with lightweight EDR agents		✓
Track endpoints (Windows, Linux and macOS) that are online versus offline		✓
Detect malware footprint with advanced correlation of data gathered through pre-built rules running on endpoint agent		✓
Contain threats by isolating affected endpoint, enforcing policy changes or stopping malicious processes		✓
File Integrity Monitoring		
Detect changes to privacy protected files and folders in high-value assets instrumented by any user		✓
Detect changes to OS specific files instrumented by any user		✓
Detect various operations on files - Create, Delete and Update		✓