aiXDR™

Seceon aiXDR takes a holistic approach to cybersecurity by gathering deep insights from endpoints, servers, clouds, network devices, applications, IOT, and OT and applying user identity, threat intelligence, and vulnerability assessment to establish threat profiles, generate threat indicators, raise essential alerts, and offer remediation path – automated or triaged. In essence, the solution ensures multi-layered 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 platform 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.

Advacned Security for Endpoints and Networks
Block brute-force attacks on endpoints leading to compromised credentials, VPN, early detection of malware and ransomware, network based attacks, and ultimately protect your users, data, applications, infrastructure and systems

Real-time AI/ML Based Detection and Response
Benefit from security automation through Machine Learning for anomaly detection and Artificial Intelligence for Dynamic Threat Modeling (DTM) as accurate risks are quantified based on threat indicators. Stop threats and limit blast zones before they turn into major incidents.

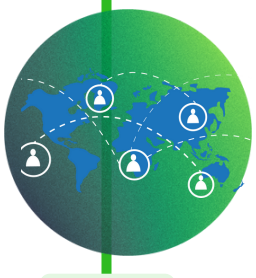
Instant 24/7 Response
Enable instant responses to governance policy violations through user-defined controls and initiate automated remediation to threats with high severity and confidence level, targeted at business-critical assets.

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.

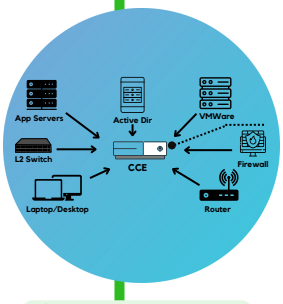
Single Pane of Glass
Rest assured with total protection against cyber security threats, exploits and attacks across your servers, endpoints and applications in the Cloud, On-Premise, Edge (IIoT & IT-OT) and Remote Workplaces.

Complete Attack Surface Visualization
Monitor your IT assets 24x7 with full details 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

Sample Threat Types & Use Cases Addressed by Seceon aiXDR



Remote Workplace



On Prem/Data Centre

- Early Malware & Ransomware Detection
- Insider Threats
- Data Breach (Exfiltration)
- DDoS Attacks
- Web Exploits
- Brute-Force Attacks
- Vulnerability Exploits
- 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 Environments

➤ M365, OneDrive, SharePoint, Network Watcher, Azure AD, NSG, Government Cloud, Cloud App Security

Google Cloud

➤ Google Workspace, StackDriver Flow Logs, Pub/Sub APIs

Other Cloud (IaaS / SaaS)

➤ Oracle Cloud, Service Now, Slack, others

Endpoints

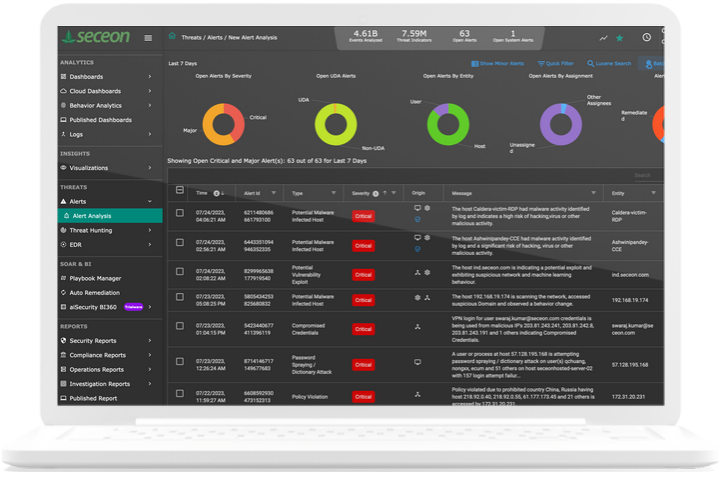
➤ Windows, macOS, Linux Desktop

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



Seceon Dashboard

PRODUCT FEATURES	aiSIEM	aiXDR
Automated Threat Detection with Real-time Processing	✓	✓
Automated and Semi-Automated Remediation	✓	✓
Advanced Correlation with Contextual Enrichment	✓	✓
Network Behavior Anomaly Detection and Network Traffic Analysis	✓	✓
User Entity Behavior Analytics	✓	✓
Visualization, Alerts, Notification and Incident Management	✓	✓
Threat Hunting and MITRE ATT&CK Framework	✓	✓
Log Collection, Retention and Forensics	✓	✓
Administration and Provisioning	✓	✓
Continuous Compliance, Audit and Reporting	✓	✓
Multi-tenant, designed for isolation between clients or organizations	✓	✓

aiXDR adds 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, stopping malicious processes and quarantine malicious files	✓
• Enriched set of TI feeds with 8+ million malicious hash files	✓
• Enriched set of indicators with actual virus malware names	✓
• Capability to auto update agents on endpoints	✓
• Multi-tenant by design with logical separation of data, analytics, ML and AI rule-set	✓

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	✓

Learn more about Seceon aiXDR and

Schedule a Demo www.seceon.com/contact/