aiXDR™

Solution Brief

seceon

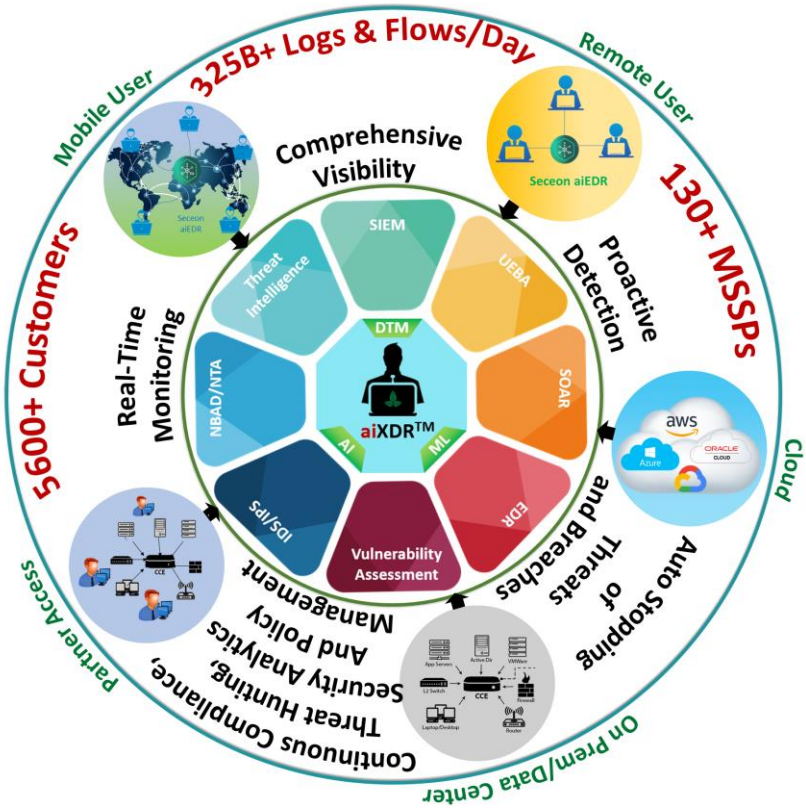
All-in-one aiXDR™

Provides Comprehensive Cybersecurity for Digital Era.

Seceon and its OTM Advanced Threat Detection and Remediation Platform is the industry's most highly awarded platform. Its novel approach is to focus on detecting and stopping threats automatically before data is compromised has redefined the work of today's analysts - freeing them from the difficult work of detecting threats and deciding how to stop them and allowing them to focus on how prevent them from happening in the first place. The OTM solution with MSSP multitenant capabilities has finally made it operationally profitable for MSSPs to move beyond only offering managed firewall services and offer customers of any size an ability to add advanced threat detection and remediation service – solving today's most vexing problem how to make threat analysis and remediation a task that takes minutes to perform when an incident arises by minimally trained staff.

Seceon's aiXDR is built on Seceon's Open Threat Management (OTM) platform providing integrated visibility, detection, prioritization, and response for unparalleled security and operational efficiency plus accuracy. It help organization to overcome the pitfalls of siloed EDR/EPP solutions with demanding integration with the other tools (SIEM, IDS, DLP, etc.), lack of deep security analytics to automate core processes with failure to integrate data from other sources (such as, DNS logs, Flows, VA scan, Active Directory, etc.), and partial threat coverage with limited visibility into the detection and response. It's an All-In-One experience that is organically and seamlessly fused together.

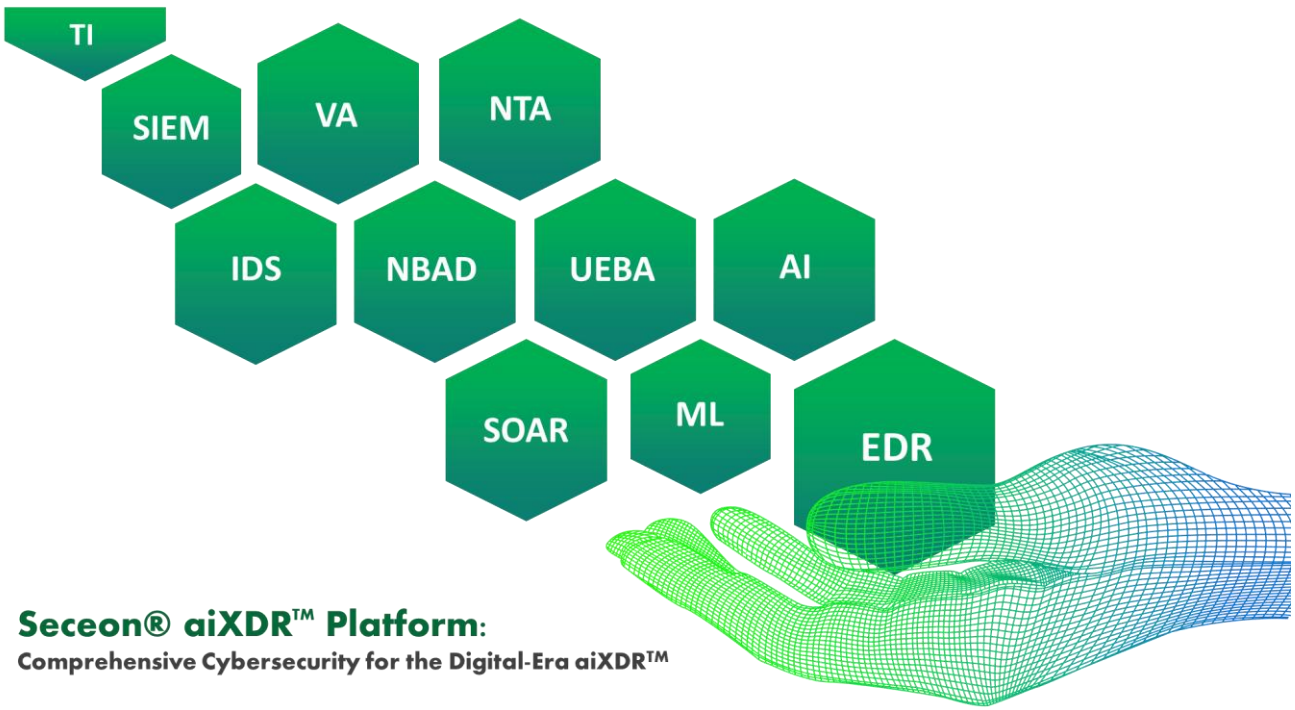
- ✓ Endpoint Security with agent-based and agentless technology for Windows, macOS and Linux OS
- ✓ Behavior baselining with applied Machine Learning for users and entities based on host centric insights (services, processes, file access, telemetry etc) and network flows.
- ✓ Data Exfiltration (breach), 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.



Operational flexibility is critical for a deployment across the Federal Enterprise. A hybrid deployment (utilizing both cloud and on premise) is key to operational flexibility. Legacy platforms are heavily oriented towards on premise deployment. From a technical standpoint, adaptation to Cloud would require multitenancy at the core with visibility of each tenant and its users limited within all applicable datasets for that tenant's assets. Built in a monolithic model, most legacy platforms struggle with this adaptation.

Seceon aiXDR™ was architected with multi tenancy from bottom up, giving the platform a flexible playing field across MSP, Cloud and On Prem. The Government could onboard agency customers (through a set of configurations) within an hour and assign security analysts from their SOC (Security Operations Center). Additionally, Seceon aiXDR™ allows multiple tiers of deployment and manageability. Hence the Government, hosting out of the cloud, would have a Master Portal (console) with the large enterprise and its distributed locations, each having its localized security posture for contextual benefits.

The aiXDR™` 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. Built for streaming fast big data, this platform is capable of ingesting volumes of logs and network flow data, while performing advanced correlation of the data sources and characteristics resulting in actionable alerts that can be remediated automatically, semi-automatically or with low touch human intervention. As the platform processes data in real-time and near real-time, running in-memory threat models, it can scale rapidly, updating and activating the threat models within minutes using intelligent ML. This imparts the ability to recognize patterns of interaction between systems, users, protocols and data transfers.



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 aiXDR™ can be broken down into three core components, all of which run on Linux (CentOS):

- Analytics and Policy Engine (APE): The Analytics and Policy Engine (APE) processes high-volume and high-velocity data in real-time using a contemporary big/fast data streaming engine. It employs state of the art machine learning and AI along with dynamic threat models to detect and remediate threats instantly.

- Collection and Control Engine (CCE): The Collection and Control Engine (CCE) orchestrates collection of data that has security relevance across various assets deployed within the enterprise (On-Prem) and cloud (Private, Public or Colo Provider). This includes structured and unstructured data in the form of raw log, syslog, network traffic, scan data and much more. Gathered data is further enriched at runtime, normalized (using standard syslog schema), classified, deduplicated and compressed before being routed to the APE. Also, CCE plays a major role in threat mitigation that is instrumented by APE through auto-remediation

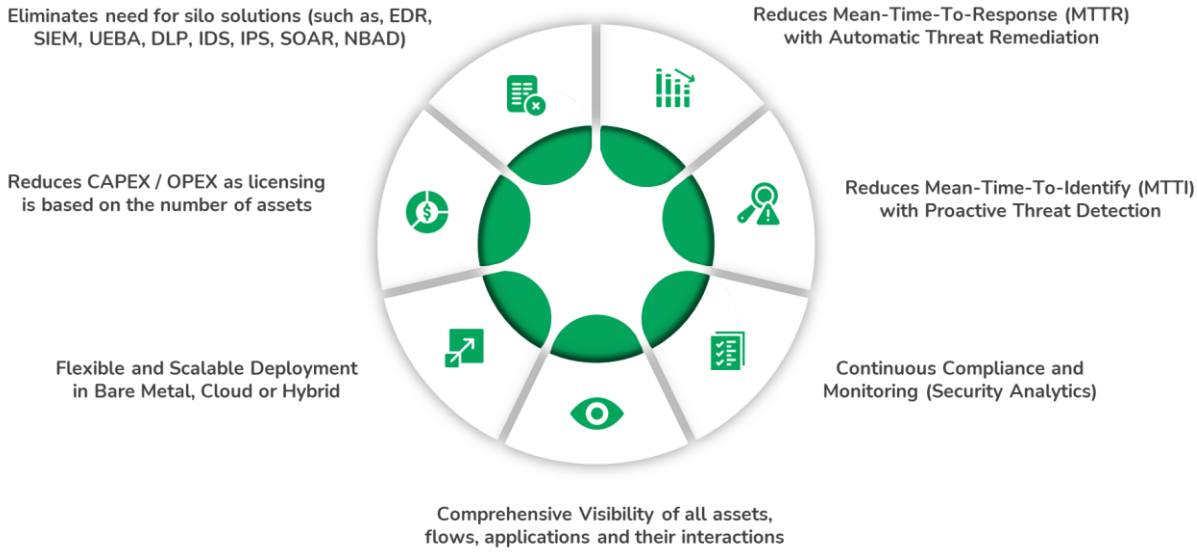
- Long Term Storage (LTS): Long Term Storage component of Seceon's solution offers log retention for up to 7 years in the form of raw log, serving requirements for regulatory compliance and forensic analysis. The Service Provider/MSP can selectively choose tenants on aiXDR™ console based on their archiving requirements. Log archiving can be set up on-premises or cloud, using aiXDR™'s storage repository, 3rd Party storage or Cloud storage.

The aiXDR™ uses state-of-the-art docker container technology and big/fast data stack to facilitate scalability while ensuring performance at speed. As per deployment guidelines, APE (Primary & Backup systems) and LTS components should be installed at Data Centre with a CCE at each site. Deployment architecture is resilient, can scale horizontally and is designed for aiXDR™ to continue its operation even if the centralized management console gets disconnected for any reason. Deployment of aiXDR™ can be achieved in 5 hours and the solution can be fully functional in 2 weeks.

BENEFITS

The key benefits of a comprehensive and integrated solution include:

- **Reduces Mean-Time-To-Response (MTTR) with Automatic Threat Remediation in Real-time**: Seceon aiXDR™ performs automatic threat containment and elimination in real-time. It also provides clear actionable steps to eliminate the threats that can either be prompted automatically by the system or manually by the security expert post-analysis.



- **Reduces Mean-Time-To-Identify (MTTI) with Proactive Threat Detection**: Seceon aiXDR™ proactively manages threats in real-time without an agent or alert fatigue. It performs threat management across the cloud, on-premises, and hybrid environments for MSSPs and Enterprises.

- **Continuous Compliance and Monitoring (Security Analytics)**: Seceon aiXDR™ provides continuous compliance and scheduled or on-demand reporting for HIPAA, PCI-DSS, GDPR, NIST, ISO and many other similar regulations.

- **Comprehensive Visibility of all assets, flows, applications, and their interactions**: Ingests raw streaming data (Logs, Packets, Flows, Identities), enriches and extracts meaningful features to provide real-time view of all assets (users, hosts, servers, applications, traffic) that are on premise, cloud, or hybrid. The solution provides a single pane of glass view for all events and incidents across the organization and provides real-time analysis and reporting.

- **Automatically discovers and reports on new assets in the environment**: Automatically discovers new assets introduced in the environment, such as laptops, PDAs, mobile devices, IoTs etc. These are automatically monitored without any human intervention to ensure the comprehensive security of all assets in the environment. This not only helps the typical commercial environments but is extremely critical for university, sports arena, public places such as train stations and airports.

- **Flexible and Scalable Deployment in Bare Metal, Cloud or Hybrid**: The solution, wrapped in containers and database, can scale horizontally to accommodate growing requirements (EPS, hosts, servers, firewalls etc.) of the customer and can be deployed on-premises (bare metal or virtual machine), in-cloud or hybrid using hardened Operating Systems. Initial sizing allows for 1.5 times the estimated data volume, thus allowing for increased events (beyond EPS limits). All data in transit is encrypted for safe storage and tamper prevention.

- **<u>Reduces CAPEX / OPEX as licensing is based on the number of assets</u>**: Licensing is based on the number of critical and non-critical assets as opposed to the amount of data being ingested which enables low, fixed CAPEX/OPEX expenses.

- **<u>Eliminates need for silo solutions (such as, UEBA, DLP, IDS, IPS, WASF)</u>**: Seceon aiXDRTM platform assimilates events, network traffic data, environment information, user identity, process intelligence and 3rd party intelligence/alerts to process, correlate and apply behavioral analytics (ML based) along with dynamic threat models (AI guided), thus bolstering an organization's security posture comprehensively and eliminating the need to rely on siloed solutions.

1. ***How an EDR solution be designed, configured, and deployed to provide an "enterprise deployment" where-by the following objectives are achieved:***

a) ***Sub-organizations can still maintain operational autonomy***

b) ***Exhaustive and complete visibility and control of all known endpoints of a large enterprise (e.g., Department or Agency) are accessible through a "single pane of glass", such that there are minimal needs to re-authenticate and/or pivot to alternative consoles to access EDR functionality needed to secure specific endpoints.***

Seceon's aiXDR™ Open Threat Management platform provides multi-tier, multi-tenant functionality that combines the power of dynamic SOC with the unparallel advantage of integrating EDR, Network Behavior, Advanced Correlation (SIEM), Network Traffic Analysis, UEBA (ML based) and SOAR into a comprehensive solution to offer defense in depth cyber security, managed and monitored by the MSSP.

Seceon's multi-tenancy is supported on a single hardware platform with logical segregation of the data using unique IDs for each tenant. AI & ML rules for each tenant are treated separately and ensures that the rules and configurations for one tenant doesn't affect the other tenants on the MSSP or other departments of an enterprise or business. Each tenant or a client can also create their own users who can only access that client data, whereas a SOC at an MSSP or enterprise level can access the clients assigned to the SOC.

The entire platform is centrally managed by the SOC team and can scale horizontally on-demand, with just a single deployment of the core (Analytics and Policy Engine). The capability for a master MSSP who can in-turn provide services to their clients who are themselves MSSPs with their own clients. Such capability when combined with horizontal scaling enables our master MSSPs to expand their offering in a significant way and leverage the economies of scale that is industry first.

aiXDR™ multi-tier, multi-tenant architecture enables enterprise to:

- **<u>Do more with less</u>**: Automated Threat Detection and Remediation will allow the Government to serve more customers with fewer analysts that would otherwise require hours and days of tuning (correlation rules) or manual analysis by SOC.

- **<u>Build Credibility with Surplus Value at Scale</u>**: Create outstanding value with comprehensive defense in depth solutions that overcome silos and scales across the enterprise.

- **Drastically Reduce CAPEX and OPEX**: Reduce Capital Expense and Operating Costs by up to 80% through single unified cyber security platform for monitoring, detection, remediation, policy governance and compliance.
- **Streamline Operational Efficiencies**: Deliver value to customers with essential tools and dashboard elements for easy navigation, cloud security, endpoint deployment, threat hunting, log archival and operational oversight.

What minimum critical requirements should an EDR solution include for a federal agency to down- select an EDR tool (e.g., role-based access control, preferred "response" mechanisms, automated analytics as a force multiplier, etc.)?

Considering the cybersecurity challenges confronting the Government today, the minimal critical requirements should include:

Integrated Platform: the proliferation of independent security tool sets has resulted in a siloed architecture that is both costly and operationally complex. Achieving the objectives outlined in this RFI requires an integrated platform that organically and seamlessly incorporates SIEM, UEBA, Threat Intelligence, IDS/IPS, Network Behavioral Anomaly Detection, SOAR and Vulnerability.

Dynamic Threat Models and AI guided Advanced Correlation: The growing number of devices and environments to protect requires mandatory reliance on machine learning to develop a better understanding of the context (users, devices, events, apps) associated with security events and more accurate, prioritized, and meaningful alerts. These capabilities are particularly important given the scarcity of qualified information security professionals at a time when additional staff is needed to optimize, analyze, and respond to data from silo products. Most of these generate a lot of events causing alerts fatigues.

Network Behavior Anomaly Detection: Death of perimeter requires comprehensive visibility of all assets, flows, applications network traffic data, NetFlow and sFlow metadata streams and their interactions to provide greater visibility of network traffic moving across the organization is needed.

Applying Machine Learning creates a baseline of traffic behavior allowing aiXDR to detect anomalous behavior without the need for decryption.

Machine Learning based Behavioral Analytics: The sophistication of cyber adversaries is growing rapidly resulting in the need for a comprehensive threat detection and remediation built into single platform based upon Behavioral Based modeling vs Signature Based.

Automated and Semi-Automated Remediation: Define specific criteria for auto-remediation based on severity type, confidence level, security alert type and asset category, including action path (Firewall, NAC, EDR) and schedule, causing minimum disruption to business.

Continuous Compliance, Audit and Reporting: Continued growth of compliance regulations requires an integrated solution that covers compliance and a broad spectrum of use cases.

The aiXDR™ Open Threat Management Platform took all of these challenges into consideration when being developed. Our holistic approach to cyber security enables us to detect both signature-based malware with precedence and zero-day threats without precedence by gathering deep insights from endpoints, servers, network devices, applications, IOT and security systems and applies user identity, threat intelligence and vulnerability assessment to

Our comprehensive behavioral analytics (Machine Learning based), Dynamic Threat Models and Advanced (built-in) Correlation guided by Artificial Intelligence, Seceon aiXDR™ generates threat indicators, raises only essential alerts, and offers a remediation path –automated or triaged.

What minimum sets (types) of critical EDR data should be collected by security analysts to* identify advanced threats *or evidence of an active breach?

a) What are the recommended retention periods per dataset to balance operational effectiveness against costs?

The Collection and Control Engine (CCE) orchestrates collection of data that has security relevance across various assets deployed within the enterprise (On-Prem) and cloud (Private, Public or Colo Provider). This includes structured and unstructured data in the form of raw log, syslog, network traffic, scan data and much more. Gathered data is further enriched at runtime, normalized (using standard syslog schema), classified, deduplicated and compressed before being routed to the APE (Analytics and Policy Engine). Also, CCE plays a major role in threat mitigation that is instrumented by APE through auto-remediation.

Collection and Control Engine can ingest feed in various forms across different sources:

- Networks traffic data and metadata streams such as NetFlow and sFlow.
- Cloud infrastructure security feeds such as NSG, Azure AD, Office 365, Azure Network Watcher Logs, AWS CloudTrail, GCP StackDriver Flow Logs etc.
- Syslog from network devices (firewalls, gateway, routers etc), application servers, file servers and database servers, DNS/DHCP servers, SMTP servers and FTP servers.
- Operating System logs (Windows, Linux etc.) and Windows Event Logs (NXLog).
- Threat information from Security systems such as EDR in the form of logs and/or API calls.
- Raw logs from several applications like MS-SQL, MS Exchange, Windows Active Directory, RADIUS, Office365.
- Vulnerability Assessment scan data.
- Raw logs from physical security devices and access control systems.
- Traffic from IoT devices in the form of flows as well as logs from the standardized lightweight *NIX or windows systems in SCADA/ICS environment.
- Database Activity Monitoring based on queries conducted on stored log in database tables.
- Collects data (events, alerts) from 3rd Party APIs (RESTful or otherwise).
- Collects data from a remote system via FTP, SFTP, and SCP.

Note, users can send feeds from their own sources, as well. In case of unsupported devices, new parsers can be developed within 2 to 4 weeks for syslog, non-syslog and multi-line logging formats (e.g., NXLog). Seceon's aiXDR™ supports many industry standard event collection methods such as syslog, OPSEC,WMI, SDEE, ODBC, JDBC, FTP, SCP, HTTP, text file, CSV, XML file etc.

CCE can collect data with or without an agent. Only security related (meaningful) logs are forwarded to the APE for analysis, enrichment, and correlation. All logs are converted to UTC time standard to maintain a uniform chronology of events while preserving original timestamp.

What considerations should organization take into account for future, long-term EDR requirements? Forexample:

a) API integration support today versus future (e.g., SOAR, SIEM)

b) Support for "cloud native" or "cloud powered" deployments (i.e., FEDRAMP)

c) How to proactively hunt in-memory "at scale" in the enterprise, to detect advanced malwarethat exists only in memory (e.g. fileless attacks")

d) EDR evasion techniques and what EDR product/service vendors are doing to compensate

Organizations should consider going straight to an XDR solution vs just looking into an EDR solution. EDR solution provide Endpoint protection vs having a solution that is continually monitoring all network traffic across the entire environment. Seceon's aiXDR will provide an all-encompassing platform that monitors everything including the Endpoints and provides the ability to remediate any threats that are detected.

An API is vital for any solution to permit integration with other platforms and packages that an infrastructure might require. Seceon's aiXDR platform has a robust API that has been used to integrate with dozens of platforms and application (i.e. Connectwise).

aiXDR™ has been deployed in Azures Gov Cloud for multiple customers. aiXDR has been designed to work in all the cloud environments (Azure, AWS, Google, Oracle).

aiXDR™ collects all relevant information (Logs, Netflows, User information, etc…) from your network devices, hosts, servers, IoT, etc., and uses that data to create behavioral models for each host and device. Those models are stored in memory and reviewed and update in real time providing the fastest response to for any malicious activity in your network. By monitoring behaviors and using Netflows, aiXDR™ can detect any activity that correlates to an attack. It does not require nor is it dependent upon a file to have initiated the attack as an EDR device would need.

Does your EDR solution set provide cloud capabilities for software as a service offering?

The aiXDR™ Open Threat Management platform enables flexible and scalable deployment in Bare Metal, Cloud or Hybrid. aiXDR has been deployed in every available cloud environment with multiple instances (AWS AZURE, Google, Oracle).

The solution, wrapped in containers and database, can scale horizontally to accommodate growing requirements (EPS, hosts, servers, firewalls etc.) of the customer and can be deployed on-premises (bare metal or virtual machine), in-cloud or hybrid using hardened Operating Systems. Initial sizing allows for 1.5 times the estimated data volume, thus allowing for increased events (beyond EPS limits). All data in transit is encrypted for safe storage and tamper prevention.

Seceon's aiXDR™ solution supports multiple network segments - LAN, WAN, DMZ, Wi-Fi Networks and MPLS Links - simultaneously on a single instance of platform core (APE). These networks may be zoned across different On-Prem and Cloud environments.

Does your EDR solution intend on expanding its capabilities to address other types of security telemetry (networking devices, network logs, cloud logs, etc.) to expanding into the XDR/NDR space,if so please detail.

The aiXDR™ solution already integrates the examples noted in the Governments question. aiXDR™ incorporates SIEM, UEBA, Threat Intelligence, IDS/IPS, Network Behavioral Anomaly Detection, SOAR and Vulnerability Assessment. Built for streaming fast big data, this platform is capable of ingesting volumes of logs and network flow data, while performing advanced correlation of the data sources and characteristics resulting in actionable alerts that can be remediated automatically, semi-automatically or with low touch human intervention. As the platform processes data in real-time and near real-time, running in-memory threat models, it can scale rapidly, updating and activating the threat models within minutes using intelligent ML. This imparts the ability to recognize patterns of interaction between systems, users, protocols, and data transfers.

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.

Identify any recommended technical performance standards or best current practices that are relevant for EDR?

aiXDR™ provides EDR capability as part of its XDR platform. Therefore, we strongly recommend that along with all relevant EDR performance requirements that you require monitoring of all network devices and servers and require correlation of all activity across all of them. You should also require the ability to remediate any attacks by pushing policies to FW's, shutting down User accounts and blocking ports in networking devices. Many attacks do not start from an endpoint and do not require a malicious file to execute to initiate an attack.

How does your EDR solution set address "alert-fatigue" and prioritize detecting the most significant threats that are valid?

Most of the SIEM platforms require security analysts to write correlation rules to identify actual threats from a plethora of events analyzed by the platform and reported as potentially suspicious. This is a complex human intensive task, often prone to error. Seceon's aiXDR™ leverages Dynamic Threat Models to automate this task. These threat models are based on patented technology with preconfigured rules, adjusted dynamically based on an organization's usage pattern.

Here are some salient points on aiXDR™'s Threat Detection capabilities:

- It can identify malicious activity and infections on devices that are outside traditional perimeter defense and split VPN connection
- It can identify advanced threat infection vectors irrespective location, whether inside or outside corporate network

- It can detect infection without the presence of any file analysis software
- It can detect infected hosts and endpoints irrespective of the OS involved.

In Seceon aiXDR™, only the threats with high probability (Confidence Level) are translated into alerts, thus reducing alert fatigue and wasteful work. These selective alerts can be sent as notifications to Security Operations Centre (SOC) teams via emails. Also, syslog notifications and Webhook interfaces are included. Additional interfaces such as OpenDXL and aiXDR™'s API functions can be blended to enhance the security data exchange model.

The automation is complemented by built-in alert workflow and audit capabilities for security analysts that prefer manual steps. An alert can go through a typical workflow with these actions - Assign, Comment, "Not an Alert", Remediate, Trusted Threat Indicator and Close. The entire lifecycle is preserved for alert analysis and presented graphically to show evolution trends.

Primary focus is placed on proactive approach to threat detection and response with minimal SOC/analyst involvement such that security incidents can be averted or reduced considerably. Hence incident management translates into critical and major alerts in Seceon's methodology. An incident can be further investigated by drilling into the alert and stepping through the validated Threat Indicators all the way down to the event data (suspicious activity type, executable, parent/child process, OS vulnerability, date detected etc.). Also, further investigation can be conducted at asset level, device level or user level through the Deep Tracker tool.

Does your company recommend EDR as a standalone solution, or to be coupled with other network detection and response activities?

As described, aiXDR™ incorporates network detection as part of its holistic approach to cyber security. The solution ensures defense in-depth threat detection and response by integrating EDR, Network Behavior, Advanced Correlation (SIEM), Network Traffic Analysis, UEBA (ML based) and SOAR into a comprehensive solution that is organically and seamlessly fused together.

Network Traffic Analyzer (NTA) is a powerful network-based analysis framework capable of deep protocol analysis along the lines of a powerful intrusion detection system (IDS). 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 aiXDR™ 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).

As part of IT governance, aiXDR™ offers the ability to enforce network policies based on one or more rules. Access to specific network resources can be denied, based on values matching source or destination entity, with provision for nested conditions. For example, network policy for access to "Guest Network" could deny hosts (multiple) with certain host names and Private IP Addresses. Also, controls can be set with host domain, username, asset group and country name etc.

Additionally, a rule could be created as exception to another rule with broad base coverage. For example, access to “Guest Network” could be denied for all hosts, except for a few. In that case, all the rules are evaluated and applied with the rational of exclusivity. Violated network policy will be displayed as “critical” alert on aiXDR™ Portal and Dashboard.

How does your company leverage robotic process automation (RPA) and machine learning techniques to continuously improve your EDR solution?

Seceon® aiXDR solution is built upon its Open Threat Management (OTM) Platform enabling organizations to detect both signature-based malware with precedence and zero-day threats without precedence, quickly and effectively, thereby thwarting the kill chain and minimizing the extent of damage across business and enterprise environments. Towards that end, aiXDR™ has estranged itself from static rules-based threat detection in favor of dynamic threat models and behavioral analytics, relying heavily on elastic compute power and advanced machine learning. Furthermore, AI with actionable intelligence and anomaly detection algorithms with definitive indicators are synthesized to eliminate threats in real-time, thus eliminating the need for investing hours and days to establish predefined static rules.

The system incorporates variety of algorithms, unique feature engineering technique, user feedback integration and big/fast data technologies for actionable outcomes while supporting current and not-before-seen threats in real-time. The combinatorial actions and proprietary correlation aid in eliminating false positives without compromising on comprehensive detection capabilities. The continuous feedback and most current security actors are used in real-time to not only predict the threats, change assessment and its impact but also to adapt and augment the Machine Learning features, algorithms, models and proprietary correlation for most up-to-date context based situational awareness for effective threat prediction.

What are the cost-basis and model for your EDR offerings (pricing arrangement, includes a hosting/logging requirement/software development (APIs)?

Seceon’s aiXDR™ pricing is based on the number of assets being protected. It is not based on EPS (events/second) and storage requirements. We can provide a consulting cost for software/API developments.

How is Seceon aiXDR better than industry’s other XDR

Industry Other aiXDR lack complete organizational context and do not have capabilities to put in context what has happened in past with current activities. By the time threat is found out, Botnet + Encryption has been triggered.
aiXDR CMDS "Continuous real-time Monitoring, pro-active Threat Detection & auto stopping of any Ransomware in early stages so that you have to never deal with Ransomware attack" Just ask one of 5000+ customers to know the difference. aiXDR enables organizations of any size to afford the best cybersecurity solution with disruptive innovations and Multi-Tenancy based SaaS offering and easy deployment within an hour.

Other XDR v/s Seceon aiXDR

23% Threat Coverage

18% Threat Coverage

41% Threat Coverage

39% Threat Coverage

34% Threat Coverage

62% Threat Coverage

EDR + anything else = XDR

aiXDR™ *all-in-one* with 99.9% threat coverage.

Industry Best Cybersecurity EFFICACY, EFFICIENCY & ROI

Industry Best CMDS "Continuous real-time Monitoring, Detection & Stopping the threats and breaches"

*Includes On-premise, Remote/WFH and Clouds PaaS, IaaS (AWS, AZURE, GCP, OCP & SaaS (M365, GSuite, Salesforce, Zoom etc. 700+ Apps/Data Sources & 2000+ Uses Cases supported out of box)

The above diagram shows Industry's other Vendor XDR vs Seceon aiXDR.