seceon

Seceon aiXDR-PMax

Add endpoint protection, detection, and response, EDR, EPP, DLP, FIM and more to your security program

The Latest IBM Cost of a Data Breach Report Stats

- The average cost of a data breach reached an all-time high in 2023 of USD 4.45 million. This represents a 2.3% increase from the 2022 cost of USD 4.35 million.
- Phishing and stolen or compromised credentials were the two most prevalent attack vectors in this year's report, and both also ranked among the top four costliest incident types.
- The biggest cost amplifiers were security system complexity, security skills shortage, and noncompliance with regulations.
- Destructive attacks that left systems inoperable accounted for one out of every four attacks, and another 24% involved ransomware.

The results of the yearly report highlights the important role that Seceon's aiXDR can enable your team with deeper automation of threat detection and response. In today's threat landscape it is critical that teams gain access to the early detection of attacks such as ransomware, malware, vulnerabilities, and compromised user accounts.

Available EDR & EPP Solution with Seceon aiXDR-PMax

Seceon's powerful aiXDR can ingest events and logs and respond to threats with your existing EDR and EPP solution. Or, your organization can deploy Seceon's aiXDR-PMax with EDR + EPP for your endpoints. With Seceon aiXDR-PMax your team will get high-quality, actionable threat detection and automated responses to threats.

This flexibility enables our partners to customize their deployments for each organization they work with and when they deploy Seceon aiXDR-PMax, they get increased protection, visibility and context to uncover stealthy threats.

Context + Visibility

With today's expanding attack surface, and "bring your own device" (BYOD) practices and remote work, many organizations are finding it difficult to discover and then manage endpoints at scale wherever they are. With Seceon, your team will gain real-time visibility into all of the endpoints your team manages. It can then gather logs and events from all endpoints to gain a class-leading amount of context.

All alerts provide transparent visibility for all of the indicators that raised the alert. Analysts will understand how and when the attack happened across all infrastructure, from on-premises to the cloud.

Seceon aiXDR-PMax Capabilites

Device Control:

Device control - Secure and protect data on devices, including safeguards and measures to prevent unauthorized access. Block removable media (USB-Drives) access without admin permission on the devices.

FIM (File Integrity Monitoring)

Continuously captures details including the what, who and when in real time to ensure that you detect all changes, capture details about each one, and use those details to determine the security risk or non-compliance.

Data Control and Data Security

Includes data control and policy capabilities including the discovery and control of data (such has PII, PHI) and captures events at the system, user, and data level, both when connected to the corporate network, or offline. Polices let you fine-tune responses based on user, risk level, or other context. From simply logging all actions to automated blocking, you can prevent data loss before it happens.

Audit & Compliance

Report templates that support compliance and audit requirements. Offers capability to store endpoint data in compressed form for compliance purpose for up to 7 years.

On-network and Offline Visibility and Protection

Enables visibility, whether online or offline, with telemetry, network (IP, Adapters), and activity and summary based on events spanning across files, processes, services, registries, sockets, process connections, powershell scripts, shell scripts, plists, launched and network.

AI/ML Based Comprehensive Detection and Response

The system uses AI and ML to gain an understanding of your user behavior – ranging from abnormal logins and file access to potential insider threat activity and the ability to identify exploits, especially multi-layered attacks, zero-day attacks, and brute force attacks.

Example protection and detection categories and threat types that Seceon aiXDR-PMax protects endpoints against include:

1. Anti-malware: This set enables protection against hostnames that contain known malicious threats that can act on or take control of your system, such as malware command and control (C&C), malware download and active phishing sites.

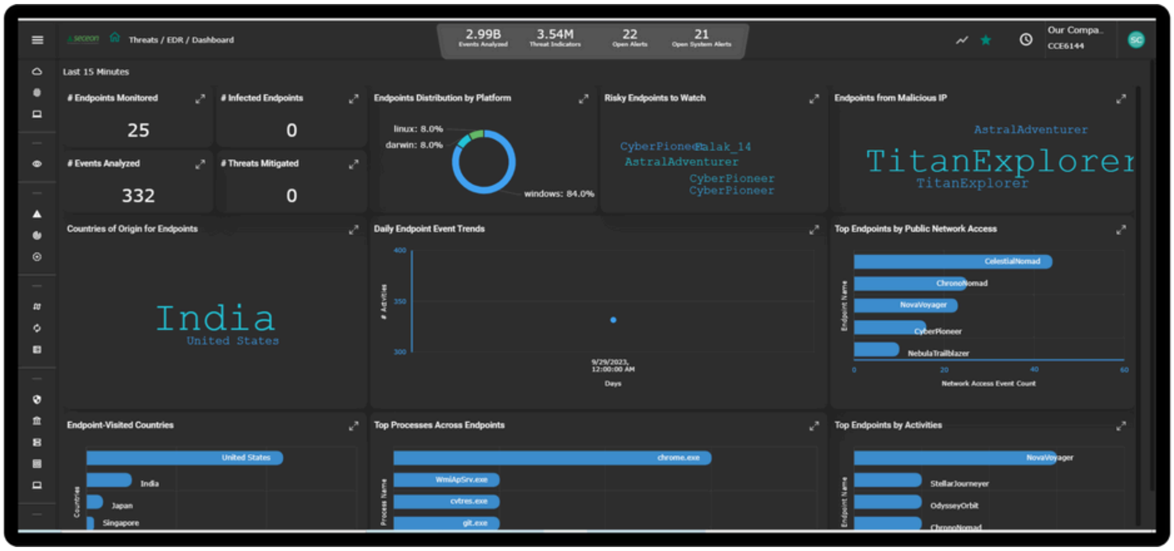
2. Ransomware: The ransomware set enables protection against hostnames that contain malware that restricts access to the computer system that it infects and demands a ransom for removal of the restriction. Some forms of ransomware encrypt files on the system's hard drive. Others may simply lock the system and display messages intended to coerce the user into paying.

3. Blackisted & Exploit IPs: The blacklisted IP set enables protection against known malicious or compromised IP addresses. These are known to host threats that can act on or control a system by way of C&C malware downloads and active phishing sites. Exploit IPs contain malicious programs used to execute “drive-by download" attacks to infected users with malware. These exploit kits target vulnerabilities in the user's machine (usually due to unpatched versions of Java, Adobe Reader, Adobe Flash, Internet Explorer and other applications) to load malware onto the victim's computer.

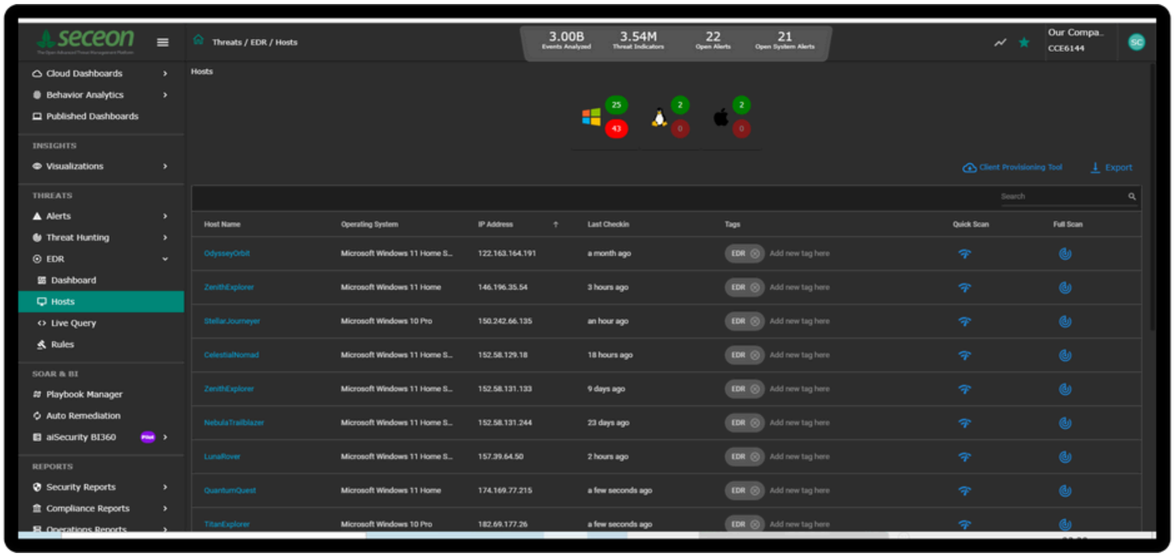
4. **Malware DGA hostnames:** Domain generation algorithms (DGA) appear in various families of malware used to periodically generate many domain names that can act as rendezvous points with their C&C servers. Examples include Ramnit, WannaCry, Conficker etc.

5. **Zero-Day Malware**: With its real-time monitoring and detection, Seceon's aiXDR-PMax is continually using anomaly and correlation insights to identify and protect against even latest malware exploits.

Seceon aiXDR-PMax



Seceon aiXDR EDR Dashboard



Host Name	Operating System	IP Address	Last Checkin	Tags	Quick Scan	Full Scan
OdysseyOrbit	Microsoft Windows 11 Home S...	122.163.164.191	a month ago	EDR Add new tag here		
ZenithExplorer	Microsoft Windows 11 Home	146.196.35.54	3 hours ago	EDR Add new tag here		
StellarJourneyer	Microsoft Windows 10 Pro	150.242.66.135	an hour ago	EDR Add new tag here		
CelestialNomad	Microsoft Windows 11 Home S...	152.58.129.18	18 hours ago	EDR Add new tag here		
ZenithExplorer	Microsoft Windows 11 Home S...	152.58.131.133	9 days ago	EDR Add new tag here		
NebulaTrailblazer	Microsoft Windows 11 Home S...	152.58.131.244	23 days ago	EDR Add new tag here		
LunaRover	Microsoft Windows 11 Home S...	157.39.64.50	2 hours ago	EDR Add new tag here		
QuantumQuest	Microsoft Windows 11 Home	174.169.77.215	a few seconds ago	EDR Add new tag here		
TitanExplorer	Microsoft Windows 10 Pro	182.69.177.26	a few seconds ago	EDR Add new tag here		

Seceon aiXDR EDR Host List

Comprehensive Endpoint Support

Seceon’s lightweight aiXDR-PMax agent is available for endpoints including

- Windows 10 and 11
- Windows server 8 and later
- MacOS
- Linux

About Seceon

Seceon enables MSPs, MSSPs, and IT teams to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon augments and automates MSP, MSSP, and IT security services with an AI and ML-powered aiSIEM and aiXDR platform. It delivers gapless coverage by collecting telemetry from logs, identity management, networks, endpoints, clouds, and applications. It’s all enriched and analyzed in real-time with threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 430 partners are reselling and/or running high-margin, efficient security services with automated cyber threat remediation and continuous compliance for over 8,000 clients.

Learn more about Seceon aiXDR

Schedule a Demo www.seceon.com/contact/