Seceon UEBA Capabilities

AI-ML Powered User and Entity Behavior Analytics

UEBA Solutions in 2024

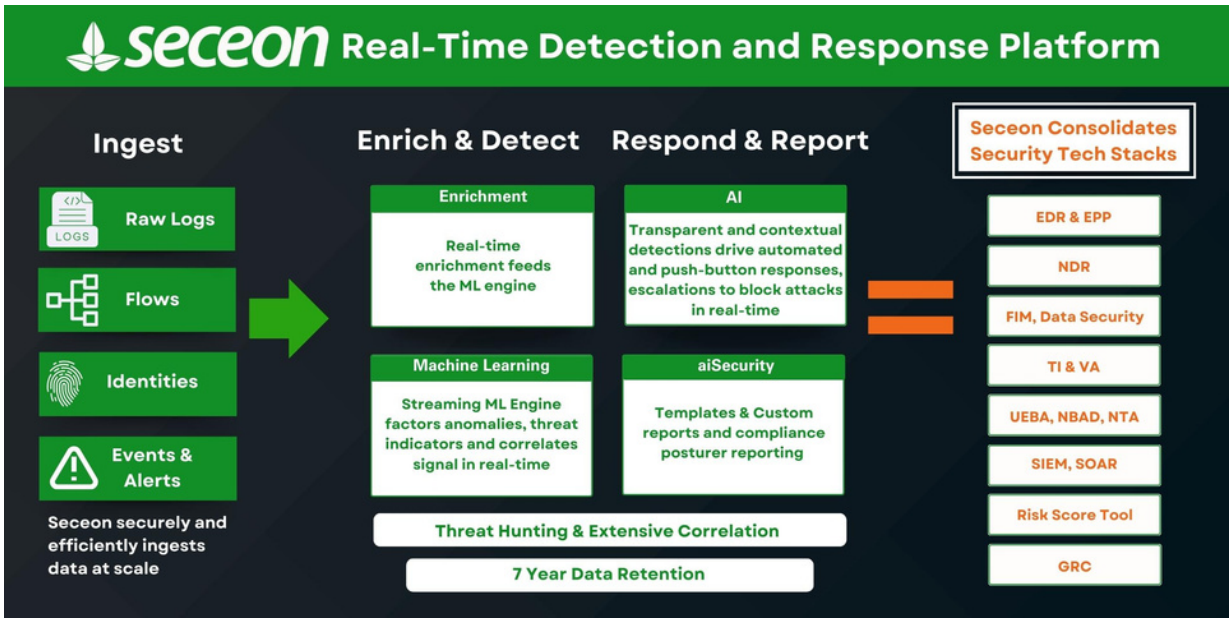
UEBA (user and entity behavior analytics) first used by Gartner Research in 2015 to describe the cybersecurity process of monitoring activity of devices, applications, servers and data with user activity. With the age of big data, cloud computing and high-speed networking, many legacy SIEM vendors and startups built solutions that enabled better threat detection and response. UEBA is an improvement over UBA and legacy SIEM systems because it overcomes the limitations of SIEM correlation rules. These rules can be problematic because they lack context, miss incidents that have never been seen before, and require too much maintenance. Improperly filtered rules can also slow down incident response execution. UEBA reduces false positives and alert fatigue, enabling AI/ML capabilities to detect potential threats and rank them on a risk scale to either alert analysts or automate a response.

How does Seceon's UEBA capabilities work?

Seceon User Entity Behavior Analytics (UEBA) is one of the detection engines in our comprehensive AI/ML powered cybersecurity platform: aiSIEM and aiXDR. Here's how it works:

1. **Holistic Approach:** Seceon aiSIEM & aiXDR takes a holistic approach to cybersecurity gathering deep insights from networks, endpoints, servers, devices, applications, IoT, and OT. It combines user identity, threat intelligence feeds, and vulnerability assessment to establish threat profiles, generate threat indicators, alerts and, manual or automated responses via playbooks.
2. **Behavior Baselining:** It applies machine learning for users and entities based on host-centric insights (services, processes, file access, telemetry, etc.) and network flows.
3. **Threat Detection with ML & AI:** Seceon uses 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.
4. **Insider Threat Detection:** Insider threat detection uses the UEBA capabilities and machine learning algorithms to identify various tactics and techniques used by the perpetrators. For example, a compromised credential is a clear indicator of an insider trying to gain access to information that they could potentially misuse.
5. **Alert:** Seceon can alert analysts and technicians multiple ways and provides the correlation and situational awareness of the where, when, how of the threat timeline.
6. **Respond:** Seceon's platform has comprehensive response capabilities including manual and automated blocking, stopping and quarantine of attacks and breaches, and a drag-and-drop playbook designer.

In essence, Seceon's UEBA is a key component of its aiSIEM and aiXDR platform, providing a comprehensive solution for threat detection and response.



Seceon UEBA use cases:

Seceon's User and Entity Behavior Analytics (UEBA) can be applied in various use cases:

1. Malware Detection: Seceon's UEBA can detect malware tactics and techniques that have evolved to avoid detection by software tools and security controls. It relies primarily on machine learning and behavioral patterns across users and entities while questioning suspicious processes, file changes, connections, scans, etc.
2. Zero-Day Threats and Ransomware Detection: Seceon's UEBA can catch zero-day threats, ransomware, and other malware variants with a high degree of confidence.
3. Brute Force Attack Detection: In a brute force attack, the adversary tries to guess the username-password combination repeatedly to gain access. Seceon's UEBA can detect such attempts.
4. Insider Threat Detection: Seceon addresses insider threat detection through User Entity Behavior Analytics (UEBA) riding on machine learning algorithms to identify various tactics and techniques used by the perpetrators.
5. Data Exfiltration (Breach) Detection: Seceon's UEBA can detect data breaches by analyzing network traffic patterns.
6. MITRE ATT&CK Modeling: Seceon leverages MITRE ATT&CK Tactics, Techniques, and Procedures to model actual intrusions and attacks.
7. Policy Enforcement: Seceon's UEBA can 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.

Benefits of Seceon UEBA in threat protection:

Seceon's User and Entity Behavior Analytics (UEBA) is crucial for threat protection today due to the following reasons:

1. Proactive Approach: UEBA strengthens security by monitoring users and other entities, detecting anomalies in behavior patterns that could be indicative of a threat. It's a proactive approach to security and gains more visibility into user and entity behavior.
2. Improved Detection: UEBA represents an important improvement over traditional SIEM and standalone UEBA solutions for a number of reasons. It overcomes the limitations of traditional correlation rules and leverages both user behavior and entity behavior-based analytics, and models threats based on individual user behaviors.
3. Reduced False Positives: UEBA also reduces false positives, helping to eliminate alert fatigue. And by enabling teams to prioritize their alerts, UEBA makes it possible for your security experts to focus on the most credible, high-risk alerts.
4. Protection Against Insider Threats: UEBA can help weed out compromised accounts before a hacker can do any harm. It also detects when power users were created and monitors if they still have unnecessary permissions.
5. Efficient Use of Resources: UEBA can also help organizations save money by reducing the need for manual investigations of suspicious activity.

About Seceon

Seceon enables MSPs and MSSPs 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 and MSSP security services with an AI and ML-powered aiSIEM, aiXDR, and aiMSSP 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 350 partners are reselling and/or running high-margin, efficient security services with automated cyber threat remediation and continuous compliance for over 7,600 clients.

Learn more about Seceon UEBA

Schedule a Demo www.seceon.com/contact/



© 2023 Seceon Inc. All rights reserved. aiSIEM, aiXDR, aiMSSP are trademarks and registered trademarks of Seceon Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.