Seceon aiENT™

Comprehensive Visibility and Intelligence with aiENT™

Enterprise visibility and intelligence are key to any organization's success to ensure optimum investment, performance, and efficiency. Seceon aiENT™ offers AI-based visibility and operational excellence at the scale.

Key Features:

1. **Log Retention Period:**
   - Your security system should retain logs in raw form for up to seven years. This ensures historical data availability for investigations, audits, and compliance purposes.

2. **Event Logging Scope:**
   - The event logger will capture all security-related events from perimeter security devices (firewalls, intrusion detection/prevention systems) and the host IPS (Intrusion Prevention System).
   - These events include successful and failed login attempts, policy violations, malware detections, and other security incidents.

3. **Event Details:**
   - Each logged event should include essential details:
     - Timestamp: When the event occurred.
     - Event type: The nature of the event (e.g., login, firewall rule violation).
     - Source IP address: The origin of the event.
     - Destination IP address: The target system affected.
     - Area affected: Specific components impacted (e.g., server, network segment).
     - Type of intrusion: If applicable (e.g., brute force attack, SQL injection).

4. **Graphical Trend Displays:**
   - Visualizing trends helps identify patterns and anomalies.
   - Consider implementing graphical displays that show event frequency, severity, and other relevant metrics over time.

5. **Log Protection and Tamper Prevention:**
   - Store logs on a separate, secure logical device.
   - Protect logs from unauthorized access.
   - Implement tamper-evident measures to detect any alterations.

6. **Time Synchronization:**
   - Ensure all systems involved in logging have synchronized time.
   - Accurate timestamps are crucial for correlation and analysis.

7. **Log Management Framework:**
   - Establish a comprehensive log management framework.
   - Define policies, procedures, and responsibilities for log collection, storage, and analysis.



Capabilities:

Scalability in log management is crucial for handling increasing data volumes without compromising performance or requiring major software changes. Here are some considerations for achieving seamless scalability:

1. **Horizontal Scaling:**
   - Design your log management system to scale horizontally. This means adding more resources (such as servers or nodes) to handle increased data ingest.
   - Horizontal scaling allows you to accommodate growing data volumes without rearchitecting the core software.

2. **Resource Addition:**
   - As your data ingest grows from gigabytes (GB) to terabytes (TB) per day, ensure that your log management solution can dynamically allocate additional resources.
   - Adding more servers, storage, or processing power should be straightforward and transparent.

3. **Licensing Flexibility:**
   - log management solution that offers flexible licensing models.
   - Licensing enhancements should allow you to seamlessly expand capacity without disrupting existing operations.

4. **Data Ingest Optimization:**
   - Optimize data ingestion processes to minimize resource utilization.
   - Consider compression, batching, and efficient parsing techniques.

5. **Indexing and Search Efficiency:**
   - Efficiently index and store log data for quick retrieval.
   - Use distributed indexing mechanisms to distribute the load across nodes.

6. **Load Balancing:**
   - Implement load balancers to evenly distribute incoming log data across available resources.
   - Load balancing ensures that no single node becomes a bottleneck.

7. **Monitoring and Alerts:**
   - Monitor resource utilization, system performance, and data throughput.
   - Set up alerts to proactively address any capacity-related issues.

8. Seceon's platform is designed to handle petabytes of log data efficiently.

9. It ensures high performance with low resource utilization, crucial for managing large-scale data.

10. Comprehensive log management solutions include the ability to handle both structured and unstructured data efficiently.

11. The solution is capable of capturing events from any source, regardless of the log format.

12. Offer robust processing capabilities to synthesize and analyze the data for actionable insights.

13. Solutions offer security, scalability, and compliance with regulatory requirements.

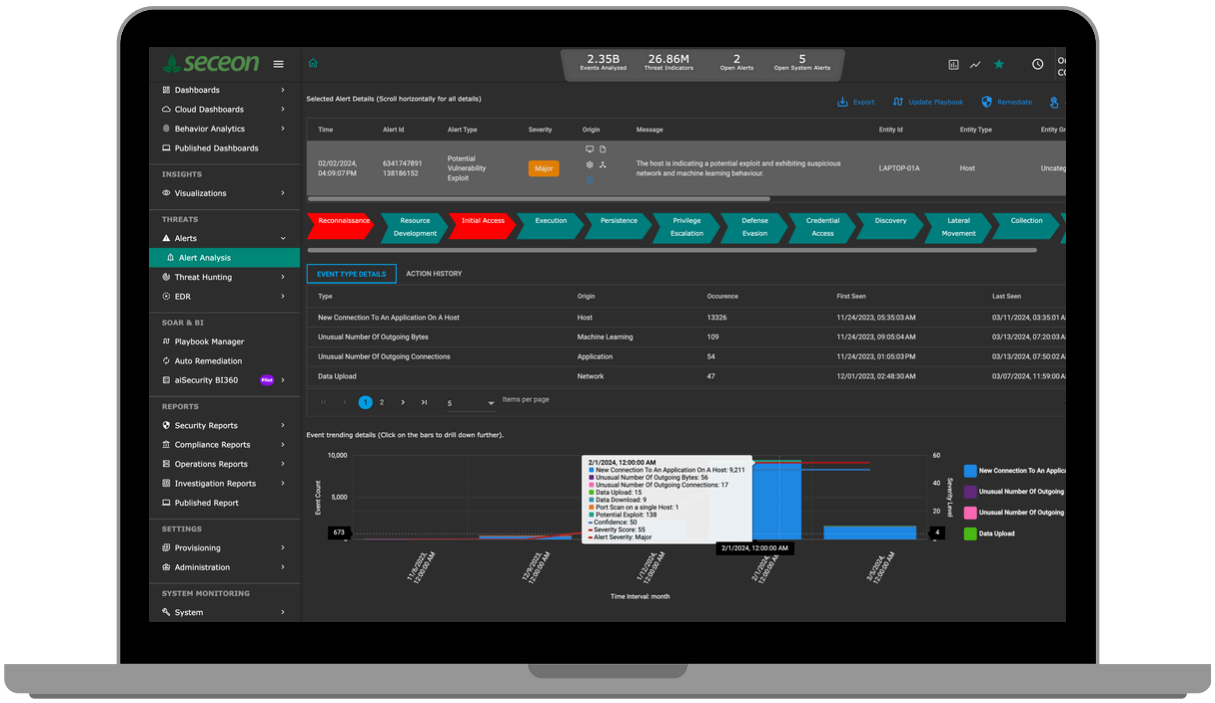
14. aiENT™ offers advanced search and indexing features, which are essential for quick retrieval and analysis of log data.

15. The system supports real-time monitoring and alerting for proactive issue resolution and system health assurance.

16. Integration with existing infrastructure and applications should be seamless to ensure a unified view of log data.

17. Facilitate compliance with industry standards and regulations through proper log retention and disposal policies.

18. For enhanced security, the system includes features for detecting and mitigating threats based on log analysis.



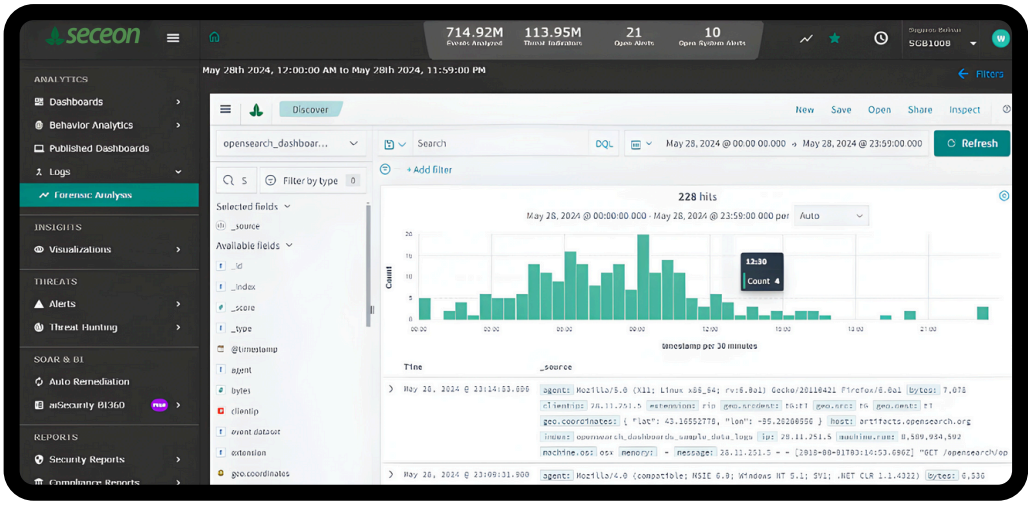
19. Seceon's Log Management solution is designed to handle vast amounts of data from various sources, both IT and non-IT. It can ingest text format logs from a wide range of applications, including those from IP CCTV systems, providing a comprehensive view of an organization's security posture. The platform utilizes advanced AI and ML algorithms to analyze and correlate data, enhancing threat detection and response capabilities. This allows for a more proactive approach to cybersecurity, ensuring that all aspects of an organization's infrastructure are monitored and protected.

20. For instance, Seceon's aiENT™ platform could potentially employ algorithms that enable searching through unstructured data or use parallel processing to expedite the search process. This approach can be particularly beneficial in situations where indexing might be impractical or where the data is too dynamic for traditional indexing methods. The key is to design a system that is both efficient and capable of handling complex queries without the constraints of indexing.

21. Seceon's aiENT™ is designed to offer a seamless and intuitive user experience, with a focus on simplicity in constructing queries. The interface allows users to easily create alerts, dashboards, and reports.

22. Seceon's solutions are designed to deliver high-performance query results, ensuring that responses are returned swiftly, often within seconds, regardless of the query's complexity or the volume of data being searched. This is achieved through advanced correlation techniques and machine learning algorithms that optimize data processing and threat detection. With a focus on behavioral analytics and real-time automatic threat remediation, Seceon aims to provide a robust security posture without compromising on performance.

23. Seceon's advanced threat detection solutions are designed to provide real-time alerts on anomalous patterns, ensuring immediate identification of potential threats. By focusing on data streams rather than indexed data, the system allows for more dynamic and proactive security measures. This approach enables the correlation rules to be applied directly to the live data, offering a more accurate and timely response to security incidents.

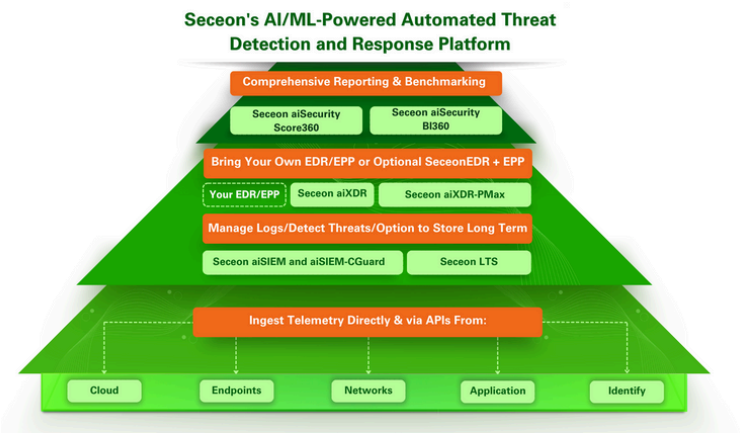


24. Seceon's aiENT™ is designed to handle the streaming of live logs into various tools such as SIEM, visualization tools, and reporting and dashboarding systems without compromising performance, even at scale. This capability is crucial for organizations that require real-time data analysis and threat detection across a vast array of assets.

25. The Seceon platform is designed to efficiently handle and compress vast amounts of log data, significantly reducing storage requirements while maintaining the integrity of the data for analysis and compliance purposes. Its advanced compression algorithms are capable of delivering at least 10 times compression, taking into account all indexing overheads. This level of compression is achieved without compromising the speed or accuracy of data retrieval, ensuring that users can access the information they need when they need it.

26. Seceon solution available and consume On-Prem, Cloud Hosted, or SaaS as per growing business needs

About Seceon



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 and MSSP 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

Schedule a Demo www.seceon.com/contact/



© 2024 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.