ANAMO
SUPERIOR CYBERSECURITY

Eliminate (SIEM) Blind Spots

(While Adding CVE’s, Vul-Scan, EDR, Forensics & eDiscovery)

Compare Traditional Rule-Based Log Parsing SIEM Systems with New “Log-Less” SIEM System Harnessing Forensic-Based Real Time Comparative HashID Analytics

Still using 20+ Yr old Splunk or another Log-Based SIEM? While obvious, it’s 2025, and there’s been new SIEM technology available for years! It’s Anamo, a log-less SIEM that’s eliminating traditional “Blind Spots” and various anomalies related to System-Based Indicators of Attack (IoA”s), Modifications of Users, Permissions, Ports and Transactions… and much more! Anamo is named after its ability to rapidly identify Host-Based attack vectors and other Indicators of Compromise (IoC’s) where all other Network-based SIEMs remain blind.

How does Anamo work differently?

Anamo is a SaaS which continuously and autonomously interrogates any computer (Windows or Linux OS) on almost any device (IT or OT) without the need for any Log or Rules that traditional SIEM system all require. Installed upon the core of each system, Anamo patented technology is focused on Comparative HashID Analytics as its methodology for threat detection and data management. Instead of relying on ingesting and storing massive volumes of raw log data, Anamo is light-weight, ultra-fast, and analyzes hashed metadata to identify threats, leading to easy deployment, improved scalability, simplified staffing, and substantial reductions in costs.

Anamo processes forensics that are impossible for external systems to identify resulting in a more expeditious method that eliminates the Dwell-Time of a technical adversary by monitoring every move or modification of a hacker who seeks the most critical problem facing Security managers today “Unauthorized Privileged Account Escalation.” Anamo compares behavioral identifiers (HashID’s) in real-time, reducing dependencies upon rules, massive log aggregation, and parsing for the identification of Cybersecurity anomalies. Traditional external network-based SIEM systems rely on collecting, normalizing, and analyzing larger volumes of rule-based log data, a very expensive solution and process known for high overhead and potential blind spots.

System-Based Interrogation Vs. Network-Based Log Parsing

Or Comparative HashID Analytics Vs. Traditional (Splunk-Style) SIEM

Feature	Comparative HashID Analytics SIEM	Traditional Log-Parsing SIEM
Data Collection	IT and OT Enabled” Captures lightweight, encrypted "HashIDs" that represent user, asset, and application behavior, sending only the forensics identifiers to the SIEM.	IT Enabled: Gathers massive volumes of raw log data from various sources across the infrastructure.
Analysis Method	Uses "Comparative Analysis" to detect anomalies by comparing behavior modifications metadata of HashIDs against baseline data. It doesn't need to read the full contents of the log to ID Cyber-risk	Relies on preset rules and parsing logs and correlating data from different sources to identify security incidents. This process is resource-intensive.
Performance and Efficiency	Is more efficient and scalable by not processing large quantities of log data. This leads to lower computational costs and faster analysis.	Can be slow and computationally expensive, especially when handling large volumes of data from cloud environments.

Contextualization	Gathers "deep software insights" on vulnerabilities, users, and permissions without needing to parse logs. It then correlates these insights to provide contextual information, alert notification, etc.	Provides context to network risks by enriching raw log data with threat intelligence and correlating events from different logs external to compute systems
Data Storage	Stores significantly less data since it only retains the HashIDs and contextual insights, not the full log content. This leads to lower storage costs.	Requires large storage capacity for log retention, which can be costly, especially with compliance requirements.
Maintenance	Requires less operational overhead for managing data pipelines and tuning parsing rules.	Requires extensive maintenance, including fine-tuning parsing rules and managing data collection integrations.
Data Ingestion Cost	Avoids the high, volume-based pricing often associated with traditional SIEMs, offering more predictable costs.	Often involves a pay-per-gigabyte pricing model, leading to unpredictable and high costs as data volumes increase.
Forensics	Captures and retains objective system-based data and behavioral timeline for immediate eDiscovery, forensics, and compliance, but does not provide access to the raw logs themselves.	Stores large volumes of raw data from log emitting devices, which are network based and often necessary for in-depth forensic analysis and compliance audits.
Cost and scalability	Reduced costs for data ingestion and storage. Since only hashed metadata is collected, the volume of data is significantly smaller, leading to lower infrastructure and storage expenses.	High costs for data ingestion and storage. Costs can scale dramatically as data volumes increase, particularly in cloud environments where pricing is based on ingested data.
Performance	Faster threat hunting and analysis. The smaller data footprint of metadata hashes allows for significantly faster search and query times compared to searching through vast quantities of raw log data.	Slower performance with large datasets. Search and analysis can become slow and inefficient as the volume of log data grows, causing "coffee break SIEM" latency.
Privacy and security	Inherently more secure. Because sensitive data is never collected or transmitted, privacy is maintained by design. This is particularly advantageous for organizations with strict compliance requirements.	Requires strong data security policies. Organizations must take precautions to redact and protect sensitive data within logs, which are often stored for long periods.
Operational complexity	Easier to manage and maintain. The streamlined nature of the log-less approach reduces the	Complex to implement and maintain. Requires extensive setup, including

	complexity of configuring collection agents and managing data normalization rules.	parsing rules for different log formats, which are often inconsistent. It also needs continuous tuning to reduce false positives.
Forensic analysis	Less granular for deep forensics. Without access to the raw log data, the level of detail available for in-depth forensic investigation may be limited. However, Anamo provides the "what" and "where" of a threat, guiding analysts to the original data.	Comprehensive for deep forensics. Analysts have access to the raw log data, which allows for thorough, in-depth investigations and root-cause analysis.
Threat detection	Focuses on comparative behavioral analytics. By comparing metadata hashes, it can detect unusual patterns or anomalies in behavior, signaling a potential threat without needing to know the content of the data.	Relies on rule-based and signature-based detection. Threats are identified by applying a series of rules or signatures against the log data. Some modern SIEMs incorporate machine learning, but they still operate on the raw data.
Cost and scalability	Reduced costs for data ingestion and storage. Since only hashed metadata is collected, the volume of data is significantly smaller, leading to lower infrastructure and storage expenses.	High costs for data ingestion and storage. Costs can scale dramatically as data volumes increase, particularly in cloud environments where pricing is based on ingested data.
Area of Service	Agent compatible System-Based for IT and OT computing and personal devices seeking Indicators of Attack and Compromise	Non-Agent compatible Network-Based for Log emitting IT and OT devices seeking indicators of Attack and Compromise

Anamo’s approach: Advantages and disadvantages

Advantages:

- Reduced overhead and cost: Eliminates the computational and storage burden of log management, significantly lowering operational costs.
- Enhanced performance and scalability: By processing only lightweight identifiers, the system can scale more effectively without performance degradation.
- Focus on behavior, not noise: By analyzing core behavioral patterns, it minimizes alert fatigue and focuses on true security events rather than routine log noise.
- Faster threat detection: Real-time behavioral analysis can lead to quicker detection and response compared to parsing and correlating millions of individual log entries.

- Faster Implementation: Light-weight Agent-based visibility for IT and OT devices is novel and sought by sophisticated practitioners. Coupled with autonomous discovery and zero data entry, advantages are recognized immediately.

Disadvantages:

- Limited forensic depth: Without access to the original log files, investigations and post-incident analysis may lack granular details.
- Potential blind spots: If a threat doesn't have a clear behavioral signature for a HashID to detect, it could be missed. The system's effectiveness relies entirely on the accuracy and scope of its behavioral models.
- New implementation challenges: Adopting a non-traditional approach may require adapting existing security workflows or presenting a minor learning curve for teams trained exclusively on traditional log-based, rule driven, SIEMs.

Conclusion

Anamo's Comparative HashID Analytics approach offers a fundamentally different and more modern security model compared to traditional SIEMs. It addresses the well-known challenges of high cost, complexity, and slow performance associated with collecting and analyzing massive volumes of log data.

While Anamo may offer less granular forensic detail, its strengths lie in its proactive, scalable, and privacy-conscious threat detection, making it highly effective for identifying emerging threats and behavioral anomalies resulting in “Unauthorized Privileged Account Escalation.” Traditional SIEM remains an option for organizations that require the highest level of raw log data for post-event deep forensic investigations and have the resources to manage the associated costs and complexity. The benefits of traditional external SIEM’s are substantially enhanced with the internal strengths of Anamo’s rapid ability to identify anomalous behavior. Sophisticated and mature environments all seek a layered approach to Cybersecurity where network devices and system devices are both interrogated continuously to eliminate blind spots.

For more information, contact US ProTech or Anamo:
https://www.usprotech.com/ | https://anamo.io/
###