OMNETRIC Group

A Siemens & Accenture Company

IT/OT integrated security log management

Introduction

Information Technology (IT) and Operational Technology (OT) have historically been designed with different objectives in mind and therefore managed separately. The desire to optimize performance and fine-tune control of an increasingly complex grid has since prompted the convergence of the two. This integration can be challenging, particularly in the grid cybersecurity domain.

This paper discusses the challenge of establishing sustainable security log management in the OT environment using traditional IT log monitoring resources and proposes a solution.

Many conclusions in this paper were drawn from the energy industry. However, the challenges discussed and the recommendations made can equally be applied to all industries using operational technology.

What is log management?

NIST SP 800-92 defines log management as the process for generating, transmitting, storing, analyzing, and disposing of computer security log data. The energy industry is bound by regulation, and log management is a key component of utilities' security monitoring and regulatory compliance initiatives. Utilities use log monitoring as evidence of due diligence in case of a security breach.

How utilities manage security log management

Typically, utilities base their security log management infrastructure on a Security Information and Event Management (SIEM) solution. These solutions offer log collection, event correlation and log analysis capabilities. These in turn provide the necessary reporting and alerts on security incidents that deliver the necessary proof of compliance with cyber security standards.

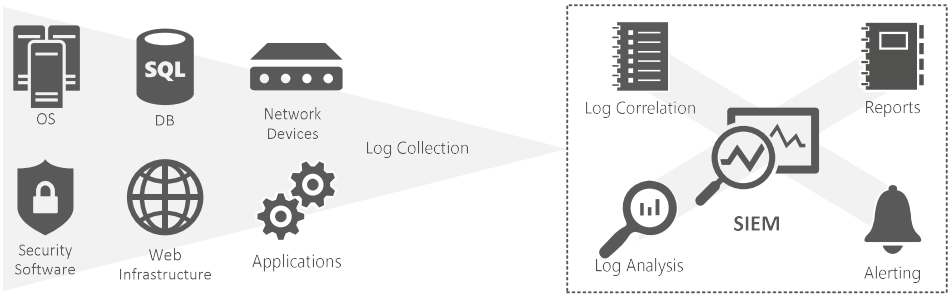

Figure 1: How log management works

Challenges with security log management

The investment is significant

Although SIEM vendors provide built-in correlation rules, reports and alerts, implementing a SIEM solution still requires significant investment to train or hire security specialists who will analyze and monitor collected data. This compels many organizations to try to conserve resources by outsourcing their log monitoring to a global Security Operations Center (SOC). Others might try to economize by implementing one single SIEM solution across different environments. Without the right integration, this rarely results in an optimal solution, given the different requirements, standards to adhere to, use cases to implement, user communities and monitoring strategies.

Solutions are often ineffective for the OT domain

Most SIEM solutions are based on IT log monitoring practices that don't consider the specifics of the OT environment. Compared to an IT environment, the OT domain usually uses proprietary technologies and non-COTS (commercial off the shelf) software, each with their own data format. This poses a challenge to utilities wishing to use a log management tool for event alerting and correlation. Additionally, the collected log data is often highly context-dependent, necessitating expert OT staff to understand it. This makes the SIEM built-in correlation rules ineffective for the operational domain.

Context needed for automation is often missing

Performing log monitoring efficiently and effectively requires automation. Automation is achieved by creating correlation rules that match multiple log entries based on common values, such as timestamps and attributes that represent the context in which the event was generated. However, the OT context dependent data is usually missing or the log entries contain a proprietary message or code that is meaningful only to the software vendor.

Context is key to overcoming challenges

Establishing context is key to overcoming the challenges faced by utilities in implementing security log management solutions.

Applying context to collected log data allows utilities to effectively monitor an OT environment and detect security incidents.

Establish context with an audit policy

An audit policy should be a cornerstone of a utility's OT log management strategy. It is an invaluable tool in establishing context for security incidents so that they can be handled effectively. An audit policy documents the events of interest, grouping them in categories that describe the security context in which these incidents were generated. These categories are commonly inspired by the guidelines contained in regulatory standards (see Figure 2). Having a written audit policy also helps prove regulatory compliance to auditors.

Reference from IEC 62443-3-3 → *The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events.*	Reference from NERC CIP-007-6 → *Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: Detected successful login attempts; Detected failed access attempts and failed login attempts; Detected malicious code.*

Figure 2*:* Examples of regulatory requirements that could be considered in defining the audit policy

Integrate threat intelligence

In response to the increasing sophistication of cyber-attacks, SIEM solutions have evolved to provide an anomaly-based approach, which in theory should help detect unknown threats. However, the anomaly-based approach significantly increases the false-positive rate, thereby placing more demands on the security team to investigate issues, and increasing the chances of missing a true-positive. To proactively dismiss these invalid indicators and help focus on actual threats, a SIEM solution needs to integrate threat intelligence.

Threat intelligence is the act of formulating an analysis based on the identification, collection, and enrichment of relevant information[1]. Generally, threat intelligence is generated through analysis of adversaries and their methods. However, there is a significant lack of insight into the OT threat landscape as traditional security vendors have not had the data sources, incident response data, and expertise required to generate OT threat intelligence. Going forward, solution vendors can support utilities in generating actionable threat intelligence through threat assessments and threat modeling activities.

To enable security professionals to create correlation rules and thus determine indicators of compromise, the context information presented in threat intelligence needs to be reflected also in the collected log data. Creating an audit policy ensures that this cross-referencing occurs (see Figure 3).

[1] Levi Gundert, Vice President of Intelligence and Strategy at Recorded Future

Audit policy category event	Threat intelligence
An event in the *Privilege Use* category for a service user or a built-in account could indicate a possible escalation of privileges	Acceptable use policy for the target product.
Multiple events in the *Access Control* category that record different users performing activities in the same area of responsibility could indicate possible collusion	The recommended configuration of the separation of duty control for the target product.
An event of the *System Change Control* category that records a mayor application change and absence of other events that confirm the update process was followed could indicate unexpected patching of system with intent to introduce vulnerabilities	Definition of the update process for the target environment.
Combination of an event of the *System out of Bounds* category that records when communication thresholds are exceeded and an event in the *Access Control* category that records successful file write access in a shared directory could indicate a possible data aggregation and exfiltration attempts	Definition of the product's baseline system and user activities.

Figure 3: Examples of where a possible cyber-attack can be indicated by comparing audit policy categories in the SIEM with threat intelligence

Achieving IT/OT integration in security log management

To effectively monitor an OT environment and detect security incidents, it is necessary to apply context to collected log data. The organization's audit policy and the software vendor's threat intelligence can be used as the source for this context.

While this context can be built-in to utilities' OT log management solutions, utilities face a dilemma when attempting to establish a security log function across IT and OT domains. While it is highly unlikely that a software vendor can support and deliver correlation rules that work across the two domains, sustaining separate SIEM solutions for IT and OT environments is unrealistic, given the investment required.

A solution to this dilemma is to implement an integrated security log management solution to bring the utility's IT and OT log management strategies together. This solution (see Figure 4) meets regulatory requiremetns (see Figure 5) by fulfilling the following functions:

- **Extract** – collecting log data from where they have been stored and shipping the data to a central component.
  Normalize – transforming data from different sources into a consistent format. The format should include information such as what happened, when it happened, where it happened, who did it, or how it happened.
  Enrich – adding security descriptors (i.e. audit policy categories) to log data (e.g. as an attribute) that describe the context in which the event was generated.
- **Filter** – taking a selective approach, where only events of interest are analyzed. Filters are commonly based on data with which the logs have been enriched.
- **Transfer** – sending the relevant log data securely to the target SIEM solution.
  Persist – keeping a redundant copy of log data to guarantee availability and integrity in case of system failure or tampering by malicious users.
- **Visualize** – providing ad-hoc forensics for the OT staff.

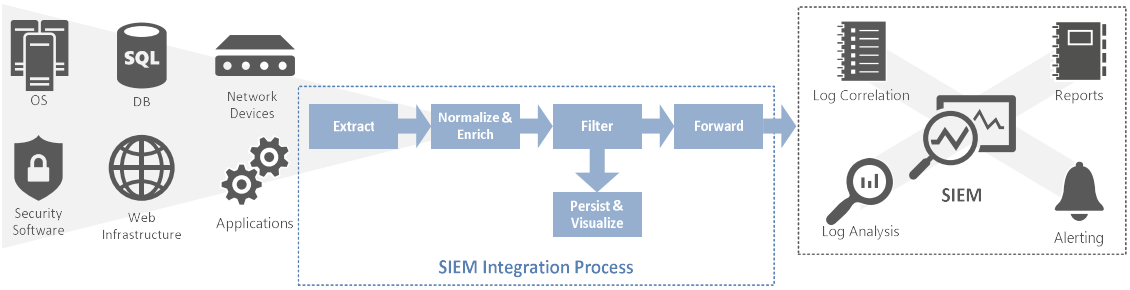

Figure 4: IT/OT integrated security log management

IT/OT integration function	Regulation fulfilled
Extract – collecting log data from where they have been stored and shipping the data to a central component	BDEW Whitepaper → *A mechanism for automatic transfer of the log files to central component shall be available* IEC 62443-3-3 → *The control system shall provide the capability to centrally manage audit events and to compile audit records from multiple components throughout the control system into a system-wide (logical or physical), time-correlated audit trail*
Normalize – transforming data from different sources into a consistent format. The format should include information such as what happened, when it happened, where it happened, who did it, or how it happened	IEC 62443-3-3 → *Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result* BDEW Whitepaper → *The system shall log user actions and security relevant actions, events and errors to an audit trail using a format which is appropriate for later and central analysis*
Enrich – adding security descriptors (i.e. audit policy categories) to log data (e.g. as an attribute) that describe the context in which the event was generated	BDEW Whitepaper → *Security events shall be highlighted in the system logs to allow for an easy automatic analysis*
Filter – taking a selective approach where only events of interest are analyzed. Filters are commonly based on data with which the logs have been enriched	
Transfer – sending the relevant log data securely to the target SIEM solution	IEC 62443-3-3 → *The control system shall provide the capability to export these audit records in industry standard formats for analysis by standard commercial log analysis tools, for example, security information and event management (SIEM)*
Persist – keeping a redundant copy of log data to guarantee availability and integrity in case of system failure or tampering by malicious users	NERC CIP-007-6 → *Where technically feasible, retain applicable event logs for at least the last 90 consecutive calendar days*
Visualize – providing ad-hoc forensics for the OT staff.	

Figure 5: Regulations met with IT/OT integrated security log management

Conclusion

Integrating information technology with operations technology to realize the benefits of a digital grid can be challenging for utilities. This is especially true in security log management, where, to date, the tools have not been available to effectively monitor security in the OT environment, or bring log management together for IT and OT.

This paper proposes a solution that bridges the gap between utilities' IT and OT log management strategies. Founded on an audit policy, and using threat intelligence, the solution defines what functions are required to successfully integrate these two strategies. The functions include shipping data to a central component, standardizing the format of the data, enriching it with contextual information, filtering out irrelevant logs and then sending the relevant log data to the SIEM.

The advantages of implementing such a solution for utilities include improved adherence to regulatory requirements, enhanced security monitoring and effective use of resources.

Bibliography

1. NIST SP 800-92: Guide to Computer Security Log Management, September 2006, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf
2. SANS Whitepaper: Successful SIEM and Log Management Strategies for Audit and Compliance, November 4, 2010, https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528b
3. Ipswitch Inc., BEST PRACTICES: EVENT LOG MANAGEMENT FOR SECURITY AND COMPLIANCE INITIATIVES, July 2010, https://www.ipswitch.com/resources/best-practices/log-management-compliance-for-the-healthcare-industry
4. BALAJI N, Security Information and Event Management (SIEM) – A Detailed Explanation, May 31, 2017, https://gbhackers.com/security-information-and-event-management-siem-a-detailed-explanation/
5. Cyber Threat Intelligence (https://dragos.com/Dragos-Insights-into-Building-an-ICS-Security-Operations-Center.pdf)
6. IEC 62443-3-3: System security requirements and security levels
7. NERC CIP-007-6 (Systems Security Management)
8. BDEW Whitepaper

About the author

Ugljesa Novak is a Security Architect at OMNETRIC Group and a Certified Information Systems Security Professional. With almost ten years of experience in IT security, Ugljesa has designed and developed security controls for grid control systems on many smart grid projects. His experience ranges across multiple vendors, and he has worked in project teams for vendors such as Schneider Electric and Siemens.

About OMNETRIC Group

OMNETRIC Group is dedicated to helping energy providers reap the benefits of the digital energy system by integrating their energy operations with IT to support their business goals. Our global team of engineering, IT, security and data experts brings extensive industry experience to help customers discover and exploit data intelligence to capitalize on industry change, and realize new business models.

Helping customers since 2014, we are an inventive, technology services company and a joint venture between Siemens AG and Accenture. For more, visit www.omnetricgroup.com.