TAG CYBER

IMPLEMENTING SIEM CAPABILITY FOR OT SECURITY: OVERVIEW OF THE INSIGHTCYBER PLATFORM

EDWARD AMOROSO, TAG CYBER

TAG CYBER

IMPLEMENTING SIEM CAPABILITY FOR OT SECURITY: OVERVIEW OF THE INSIGHTCYBER PLATFORM

DR. EDWARD G. AMOROSO

The use of security information event management (SIEM) for operational technology (OT) environments is explained and shown to provide a natural extension of existing operational security solutions to a more aggregated and correlated view of OT security. The commercial platform from InsightCyber is shown to implement the OT SIEM approach for enterprise environments. software environments.

INTRODUCTION

Every information technology (IT) security expert understands the value that security information event management (SIEM) offers through the aggregation and correlation of telemetry, logs, and other ingested data. Without the composite views offered by SIEM, usually obtained from vendors such as Splunk and IBM, security teams are forced to piece together trends and indicators using the various point solutions deployed across their IT enterprise.

In contrast, operational technology (OT) security experts have struggled with the goal of aggregating and correlating data from their operational environment. While vendor solutions have emerged that embed agents into OT devices to collect the telemetry in a proprietary engine, the objective of combining multiple OT security data feeds from different sources into a common analytic platform has not been achieved by any commercial tool.

In this report, we explain how the concept of SIEM for OT might work, and how it provides a natural extension of existing cybersecurity solutions for operational infrastructure. Implemented properly, an OT SIEM should handle multiple ingested data feeds through connectors and should allow for inventory and analysis. The emerging commercial platform from InsightCyber[1] is shown to implement this concept well.

OT SECURITY TRENDS

The need for OT is well-established in industry and government, as evidenced by the plethora of commercial solutions available for buyers. TAG Cyber tracks this category of control as part of its research, and several trends are evident across all aspects of the OT infrastructure and associated commercial marketplace. These trends inform OT security experts in their strategic planning to address increasing threats:

- *Automation* – OT security is shifting from physical, manual protections to automated, computerized protections.
- *IT Standards* – OT security is shifting from non-standard proprietary technology to standard -use IT systems using internet protocol (IP) networking.
- *Reduced Effectiveness* – Operational security is experiencing a reduction in effectiveness as the threats to these systems have become more severe.
- *OT Security Analytics* – With the shift to IT systems and IP networking for OT support, the need for conventional cybersecurity analytics has increased accordingly.

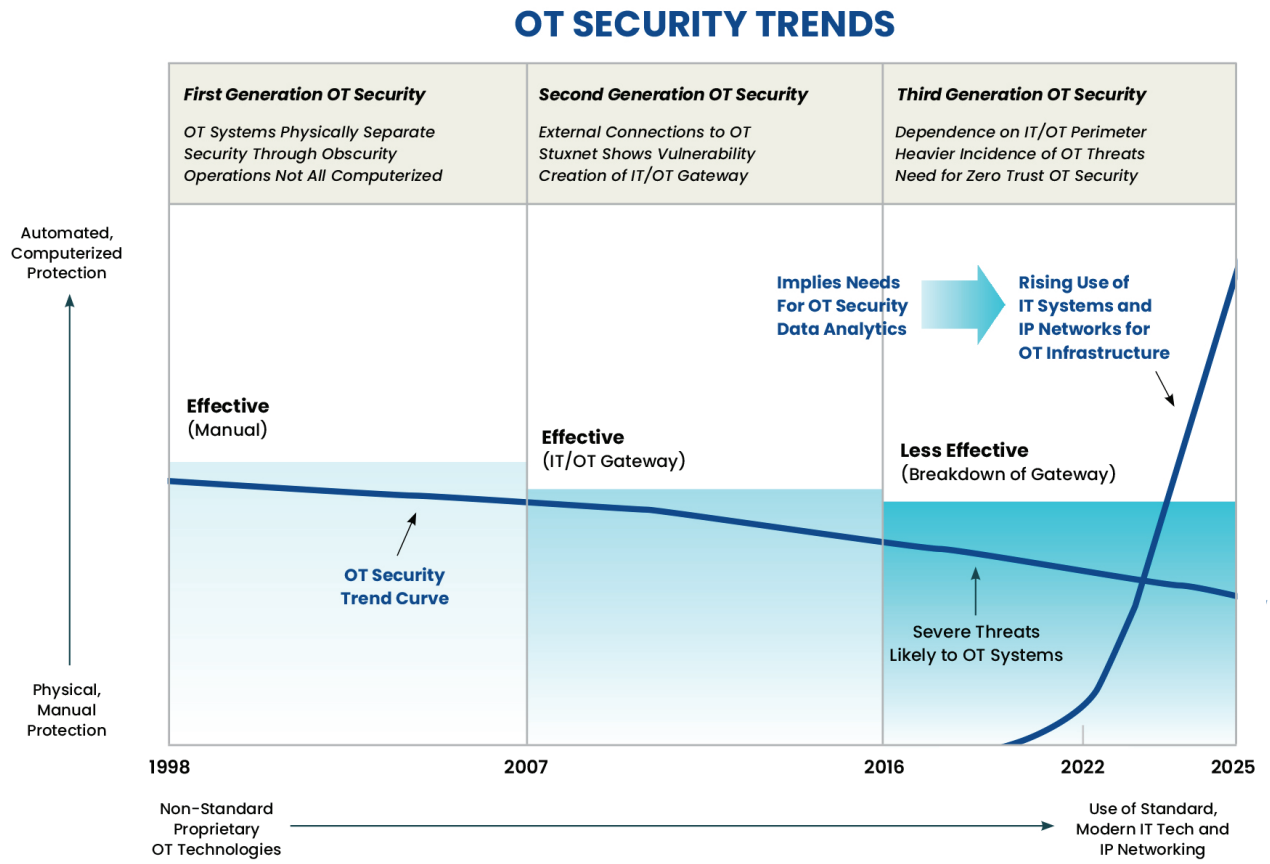

Figure 1. OT Security Trends

In general, the dominant trend for OT security is disturbing. The Stuxnet attack of 2010, for example, illustrated the significant consequence that can come from an expert attack on internet of things infrastructure.[2] It seems inconceivable that such an attack will not be repeated—and perhaps repeated frequently in the coming years. As such, OT-based infrastructure managers need to initiate protection programs immediately.

EXISTING OT ENVIRONMENTS

One type of conventional security control that can apply well to OT security environments, especially given the trends toward more IT-based systems, involves using an SIEM system. Designed to collect, normalize, and aggregate security telemetry and logs from disparate sources for the purpose of analysis, the SIEM has become a required element of every modern enterprise cyber protection program.

For OT systems, the challenge has been that existing deployments are still primarily built using technologies that operate mostly out-of-band from conventional IT systems. The well-known Purdue Enterprise Reference Architecture, for example, illustrates the type of operational support that a typical industrial control system would involve. It offers a means for standardizing the references and languages used across so many disparate industrial systems and components.

Figure 2. Purdue Enterprise Reference Architecture

Most IT security experts reviewing the Purdue model shown above do not feel comfortable with its elements since it does not include the normal type of IT- and IP-based references in conventional modern cybersecurity. This is exactly the challenge that exists in developing good security schemes for industrial systems of this type. The embedded data collection and security analysis will necessarily look different from their IT equivalent.

OT SECURITY THROUGH SENSORS AND PROCESSING

The most typical OT security architecture involves the deployment of data collection sensors, either into the target industrial control systems, embedded in a network used by the targeted systems, or utilizing existing feeds from these systems. The sensed data is aggregated in an OT security platform that is designed to support some level of correlation, analysis, and reporting to security teams for subsequent action.

Commercial vendors supporting this type of engagement are plentiful in the marketplace and have been supporting a variety of deployments across sectors ranging from factory manufacturing to transportation control. Some of the more prominent commercial vendors are listed below:[3]

- *Claroty* – The Claroty platform works to provide visibility, threat detection, vulnerability management, and mitigation for OT environments. Integrations exist with tools such as Splunk.
- *Dragos* – The Dragos platform analyzes multiple OT data sources such as logs, network traffic, protocols, and assets to detect anomalies. Add-ons exist for tools such as Splunk.
- *Nozomi Networks* – The Nozomi platform focuses on visibility into OT systems via detection of assets, detection of threats, and providing security guidance. Add-ons exist for Splunk.

The integration of OT security tools such as listed above into IT security infrastructure provides enterprise security teams with some measure of high-level monitoring and alerting in the context of their existing platforms, such as their SIEM. This arrangement requires, of course, that the data from the OT environment flow across IT/OT gateways to tools such as Splunk, and that the OT processing be performed using IT-oriented SIEM tools.

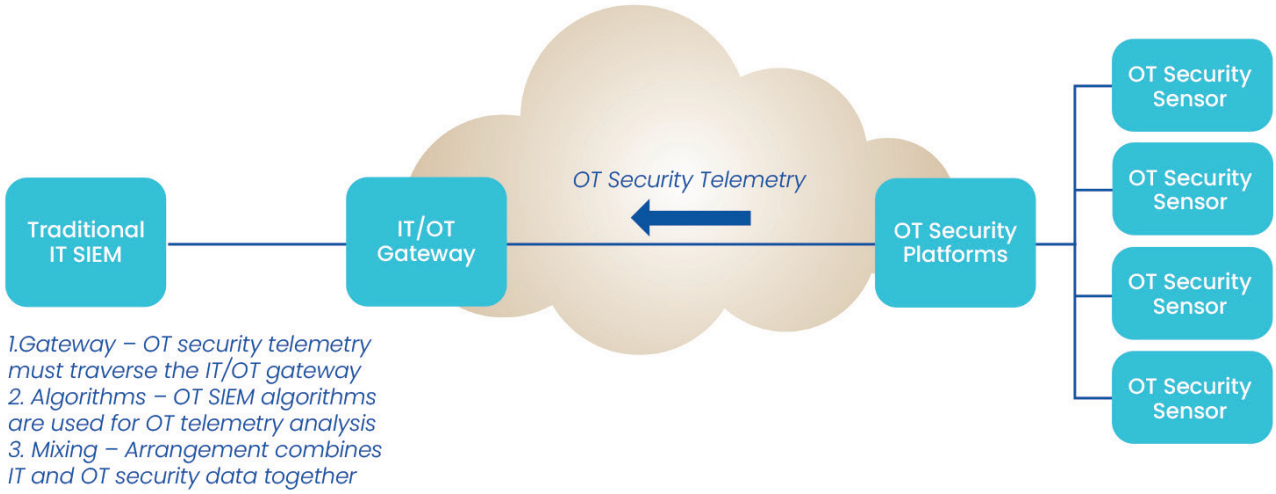

Figure 3A. IT SIEM for OT Environments

The arrangement shown in Figure 3 suggests the need for more tailored processing of industrial control system infrastructure, perhaps located within the OT and SCADA network. This would require a solution that can recognize OT protocols and systems natively, but that would also ingest the output of other commercial OT security tools to support a local analysis, perhaps even as a pre-processing step to the IT-oriented SIEM.

HOW AN OT SIEM WORKS

The concept of an OT SIEM is straightforward: it collects data through connectors and data ingest for the purpose of normalization, analysis, review, and action. Every existing commercial SIEM works in this manner for traditional IT-oriented security data sources, so the concept is both familiar and well-tested in practical environments. An OT SIEM would simply extend the approach natively into OT infrastructure.

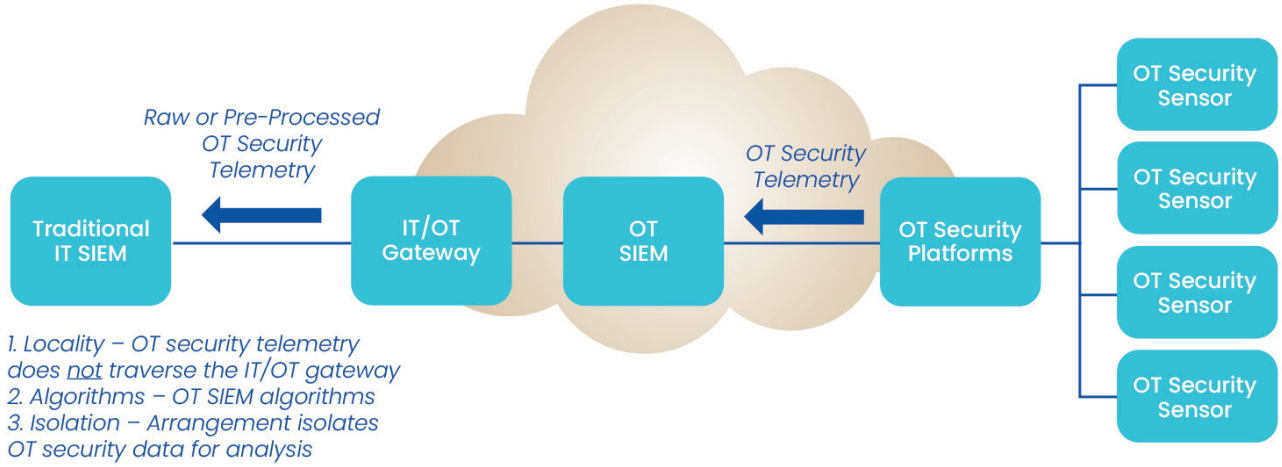

Figure 3B. OT SIEM in OT Environments

The advantages of an OT SIEM include the locality of processing inside an IT/OT gateway, which is valuable since security experts agree that traffic should always be minimized across any domain-separating gateway. In addition, the algorithms in an OT SIEM would be designed specifically to work in the OT context with data that are not mixed with other out-of-band data. This arrangement also enables a pre-processing approach for IT SIEM processing of OT security.

In the next section, we introduce a new commercial solution that is being designed specifically to handle the use cases listed above. Certainly, commercial tools for OT security will typically include their own approach to telemetry collection natively from targeted OT data sources, but the inclusion of SIEM processing capability for pre-analysis of OT security platform output in the local OT/SCADA environment is a new concept to the industry.

OVERVIEW OF THE INSIGHTCYBER PLATFORM

InsightCyber was founded in 2022 by industry veterans including Francis Cianfrocca, founder of Bayshore Networks. InsightCyber is focused on securing industrial control system and OT environments using sensors that collect data natively from OT sources, but also through SIEM processing of telemetry output from other commercial OT security platforms. The targeted arrangement tracks closely with the ideas suggested earlier in this report.

The InsightCyber platform supports a four-phase methodology: Discovery, Identification and Protection, Advanced Modeling, and Incident and Breach Response. These phases combine to form a stepwise methodology for both deployment of OT security data collection and analysis, as well as support for collection of disparate inputs from OT security systems. The result is a modern OT SIEM deployment. The diagram below shows the four phases of the approach.

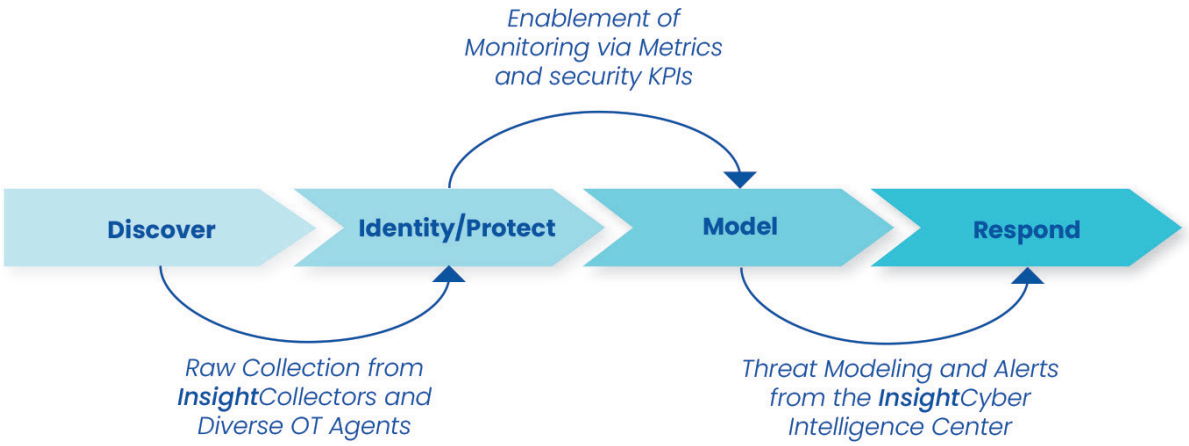

Figure 4. InsightCyber OT Security Phases

Discovery

This first phase includes the deployment of "InsightCyber Collectors" to perform the raw network and asset data collection. The platform also includes support for diverse collection from other commercial OT security agents. The goal here is to validate the asset to ensure that it originates from a confirmed asset, a process that considers site location, facility zones, and user information.

Identification and Protection

This second phase includes a variety of tasks that enable monitoring, including establishing tags for confirmed assets, determining risk for networks, validation of network connectivity, and cross-referencing of assets with vulnerabilities. An output of this phase is a proposed set of metrics and key performance indicators from the InsightCyber Intelligence Center that can be used by customers as the basis for cyber risk identification and protection.

Advanced Modeling

The third phase involves data science support for threat modeling from the InsightCyber Intelligence Center. Real-time review and data analytic processing are completed for all telemetry from the InsightCyber Collectors, as well as data from other OT agent collectors. In this manner, the InsightCyber platform introduces SIEM-like functionality for the OT security team. Alerts are generated based on playbooks, risk ratings, and asset criticality.

Incident and Breach Response

This last phase includes 24/7 monitoring, alerting, and reporting for InsightCyber customers. The service combines generalized processing from the InsightCyber Intelligence Center while also offering tailored support based on customized metrics and playbooks. This service represents a new managed security service for OT, something the industry has not seen operated at scale previously.

[1] *https://www.InsightCybercyber.com/*

[2] *https://en.wikipedia.org/wiki/Stuxnet*

[3] The TAG Cyber Research as a Service (RaaS) platform covers OT security vendors with guidance on dozens of excellent commercial solution providers. Claroty, Dragos, and Nozomi Networks are included here as sample OT security companies with prominence in the marketplace. Buyers should not take their inclusion in this report as any patent conclusion as to their suitability over other vendors for a given environment.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.