SIGA ML²

The Case for Process-Oriented OT Cybersecurity

Data Center Cyber Attack Scenarios

Contents

Introduction

Data Centers are increasingly recognized as critical infrastructure. The UK has officially classified data centers as Critical National Infrastructure (CNI), and countries like Singapore are considering similar measures. This shift reflects the growing understanding that data centers are fundamental to the functioning of modern economies and integral to sectors like healthcare, finance, and energy.

This growing importance also increases their exposure to cyber threats. It is significant to note that while Uptime Institute 2025 research reports that overall outage frequency is declining, incidents involving IT and network systems - often linked to cyber activity - are becoming more prominent and harder to detect.

In this document we use real world examples of cyber-attacks on Data Centers to show how Process-Oriented OT Cybersecurity can enhance protection for such critical infrastructure.

The framework is based on the principle that breaches are not just possible but inevitable. This necessitates the strengthening of Incident Response phase through a multi-level strategy spanning Levels 0-4 of the Purdue model.

Process Oriented OT Cyber Security Defined

At a high level, Process-Oriented OT Cybersecurity is a framework for identifying potential cyber disruptions or manipulating industrial processes. This approach is based on two core components: a Multi-Level (Purdue Model) strategy and the use of advanced Machine Learning techniques.

Multi-Level (Purdue Model Levels 0-4)

Unlike traditional cybersecurity methods that offer only a partial view of an ICS, Process-Oriented OT Cybersecurity covers Levels 0-4. This comprehensive view is essential because higher levels of the ICS (Levels 1-4) are more susceptible to manipulation during cyberattacks. For instance, in a false data injection attack where the HMI or PLC is blinded, only an unfiltered view of Level 0 can reveal the true nature of the attack. Level 0 data—directly from physical processes—offers a reliable baseline against which to verify higher-level information, especially when that data may be compromised.

Machine Learning

Suspicious behavior within the ICS is indicative of a potential or ongoing attack. This is critical information can be derived from advanced Machine Learning models, which are applied to vast datasets to detect anomalous patterns both **within** and **between** different levels of the ICS. Unsupervised ML models are used to learn the expected or predicted behavior of an asset or process and then identify deviations from the expected data patterns that are indicative of a potential cyber incident.

Alignment to NIST Incident Response Processes

The **NIST Incident Response (IR) Framework** is a structured approach to handling cybersecurity incidents. It's detailed in NIST Special Publication 800-61, "Computer Security Incident Handling Guide."

Process Oriented OT Cybersecurity provides critical support during each four key phases of the NISR IR framework:

Phase 1: Preparation

The goal is to ensure readiness for handling incidents efficiently by setting up and training an incident response team (IRT), establishing policies, and preparing tools. Injecting simulated anomalies helps train Cyber and Operations teams and develop IR playbooks, all without disrupting ongoing operations.

Phase 2: Detection and Analysis

Involves identifying potential incidents through monitoring and alerts, followed by analyzing their scope and impact. Level 1-4 data is verified using a subset of Level 0 data for real-time attack detection. AI models and the MITRE database classify events as operational or OT cyber breaches, identifying False-Data Injection attacks. This provides IR teams with insights for effective containment.

Phase 3: Containment, Eradication, and Recovery

Aims to limit damage, eliminate threats, and restore operations. A real-time decision support system assists in making critical containment choices. Multi-level data offers

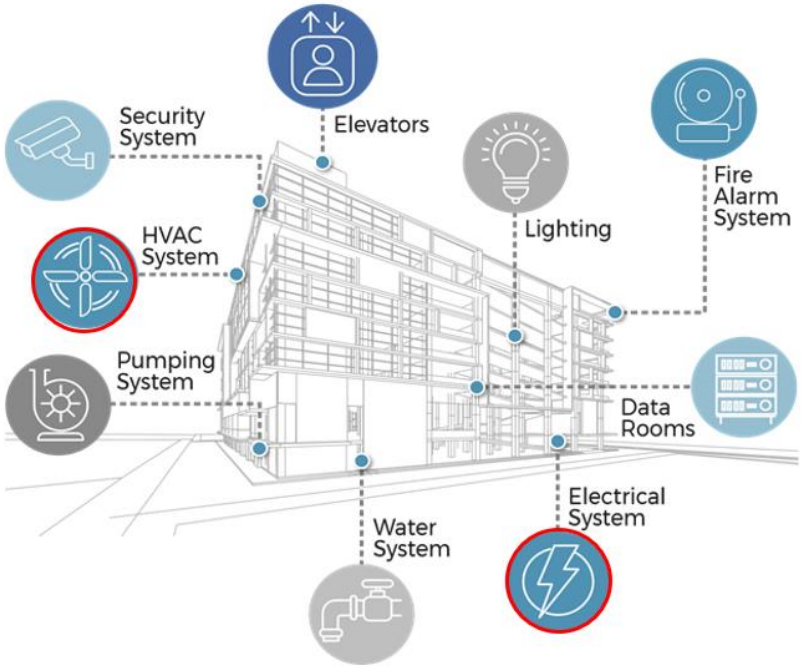
real-time assessments of physical assets, helping identify attack vectors and aiding in the eradication process.

Phase 4: Post-Incident Activity

Focuses on analyzing the response to understand the incident and evaluate response effectiveness. This phase includes "lessons learned" sessions and updates to the incident response plan to improve future performance and security strategies.

Real World Examples of Data Center Cyber Attack Scenarios

The following are two examples of potential OT cyberattacks targeting data centers, illustrating the severity of consequences these attacks can cause:



Example 1: Interference with Cooling Systems

Deliberate interference with the data center's cooling systems.

Consequence: Manipulation of cooling components leads to a temperature increase in server rooms. As temperatures rise beyond safe operational limits, servers shut down automatically to prevent overheating and damage.

Impact: This results in unplanned downtime and can severely disrupt data center operations. In some cases, there may be permanent server damage, leading to data loss and costly repairs.

For more information on how attackers were able to manipulate Data Center cooling systems, please refer to the Eastern Australian Microsoft Data Center Attack of 2023.

Example 2: Targeting Power Supply Components

Direct targeting of power supply components, such as electrical systems or Uninterruptible Power Supply (UPS) units.

Consequence: This attack causes interruptions in the data center's operations by creating electrical deficiencies or causing UPS failures, resulting in a sudden power loss.

Impact: The immediate outcome is service outages, which can disrupt critical operations and result in financial losses and reputational damage. In environments where uptime is crucial, even brief outages can have significant repercussions.

For more information about the threat of targeting power supply components, please refer to the April 2022 alert by the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Energy (DOE).

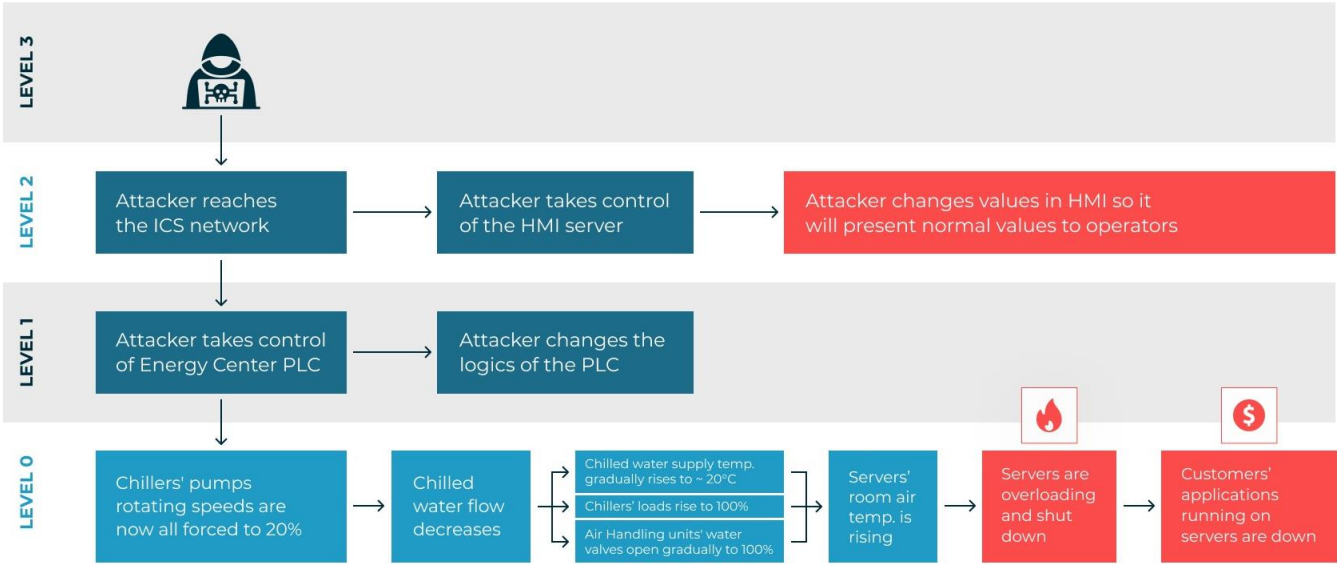
Drill-Down into Cooling Systems Attack Scenario

This scenario outlines a cyberattack on a data center's cooling system, leading to the failure of critical cooling and server shutdowns. It demonstrates the role of Process-Oriented Cyber OT in Incident Response.

Manipulation of Chiller Pump Rotating Speed

The attacker alters the PLC logic controlling chiller pumps, reducing their rotating speeds and compromising the cooling system, resulting in server shutdowns due to overheating.

The diagram below shows the cyberattack progression across various ICS Levels, focusing on the data center's cooling infrastructure.



Level 2: HMI

The attacker gains unauthorized access to the ICS network, which oversees the cooling systems. They take control of the HMI (Human-Machine Interface) server, which operators use to monitor and control processes. The attacker manipulates the displayed values to show normal conditions, misleading operators and masking the ongoing attack.

Level 1: PLC

The attacker takes control of the Energy Center PLC, which manages the physical operations of the energy systems, including the data center's cooling infrastructure. By altering the PLC's logic, the attacker changes the behavior of devices like pumps and valves, causing harmful operational outcomes.

Level 0: Chiller Pumps

The chilled water supply temperature gradually rises to around 20°C, reducing the cooling effect in the data center. As a result, the chillers are forced to operate at full capacity, reaching 100% load, straining the system. The air handling units fully open their water valves to lower the temperature, but this measure fails due to the rising water temperature and reduced flow. Consequently, the server room temperature rises, causing the servers to overheat and automatically shut down to avoid damage.

This shutdown leads to application failures and service disruptions for customers.

Preventing Cooling System Attack with Process-Oriented OT Cyber Security

To illustrate how a Process-Oriented Cyber OT approach could have mitigated the attack, we align it with each NIST Incident Response (IR) Framework phase.

Preparation: Focuses on readiness to handle incidents. Simulating realistic attack scenarios trains teams to detect and respond effectively.

- **Simulated Anomalies:** Simulating scenarios like chiller pumps at low speeds or altered HMI displays exposes attack symptoms, preparing teams for real incidents.
- **Training Teams:** Training helps teams recognize symptoms like unexpected equipment behavior or discrepancies between process data and HMI displays, enabling early detection.
- **Incident Response Playbooks:** Creating detailed playbooks outlines steps to isolate compromised PLCs, verify HMI data, and mitigate the cooling system's impact.
- **Safe Simulations:** Repeated training with simulations ensures teams can respond effectively without disrupting actual operations.

Detection and Analysis: Identifying incidents quickly through real-time data verification and AI analysis.

- **Verification Using Level 0 Data:** Real-time comparisons between Level 0 and Levels 1-4 data detect discrepancies, like altered HMI values not matching actual pump speeds.
- **AI-Driven Event Classification:** AI models classify anomalies to distinguish between operational issues and cyber breaches, identifying patterns like reduced pump speed as attack indicators.
- **Detection of False-Data Injection:** Comparing real-world data with HMI displays detects false-data injections, flagging attacks even when HMI shows normal conditions.
- **Real-Time Detection:** Continuous monitoring catches anomalies immediately, providing operators with critical time to respond before overheating causes server shutdowns.

These capabilities directly address the types of failures that Uptime Institute identifies as increasingly common - where operational errors, missteps, misconfigured systems, or network anomalies go undetected until service-impacting failures occur.

Containment, Eradication, and Recovery: Limiting damage, removing the threat, and restoring normal operations.

- **Real-Time Decision Support:** Multi-level visibility enables precise containment decisions. For example, accurate data on chiller pump status helps decide whether to isolate compromised systems.
- **Collaboration Between Teams:** Shared data allows Cyber and Operations teams to jointly decide on containment actions, balancing security and operational continuity.
- **Informed Recovery Decisions:** Real-time assessments of physical assets guide recovery decisions even when SCADA is compromised, ensuring safe operations during the recovery process.

Post-Incident Activity
Involves reviewing incidents and improving future responses based on insights from both physical and cyber operations.

- **Data-Driven Incident Review:** Analyzing data from all levels helps identify what worked and what needs improvement in detection and response.
- **Lessons Learned:** Reviewing discrepancies between Level 0 and HMI data highlights areas for enhancing detection, while decision-making analysis informs better containment strategies.
- **Updating Response Plans:** Insights lead to updated response plans with new strategies and improved communication protocols.
- **Improving Security Strategy:** Implementing additional safeguards and refining AI models strengthens defenses against future threats.

Financial Considerations

While Data Center IT cybersecurity is well protected, the OT part of the Data Center Building Automation Systems (BAS) often remains unmonitored. This oversight exposes data centers to OT attacks that can compromise operations, damage servers, and lead to data loss.

Each Data Center downtime incident incurs an estimated cost of $50K per day (for 20MW). Heavy penalties - up to 20% of Average Monthly Billable Revenue (AMBR) - can apply after the first 2 hours of disruption.

AMBR is a significant penalty because while monthly operator revenue is typically $1 - $1.5 million USD for 10-Megawatt data center, ABMR is based on the customer (co-locater) revenue of $20 - $40 million USD for 10-Megawatt re-rental to end customers.

Conclusion

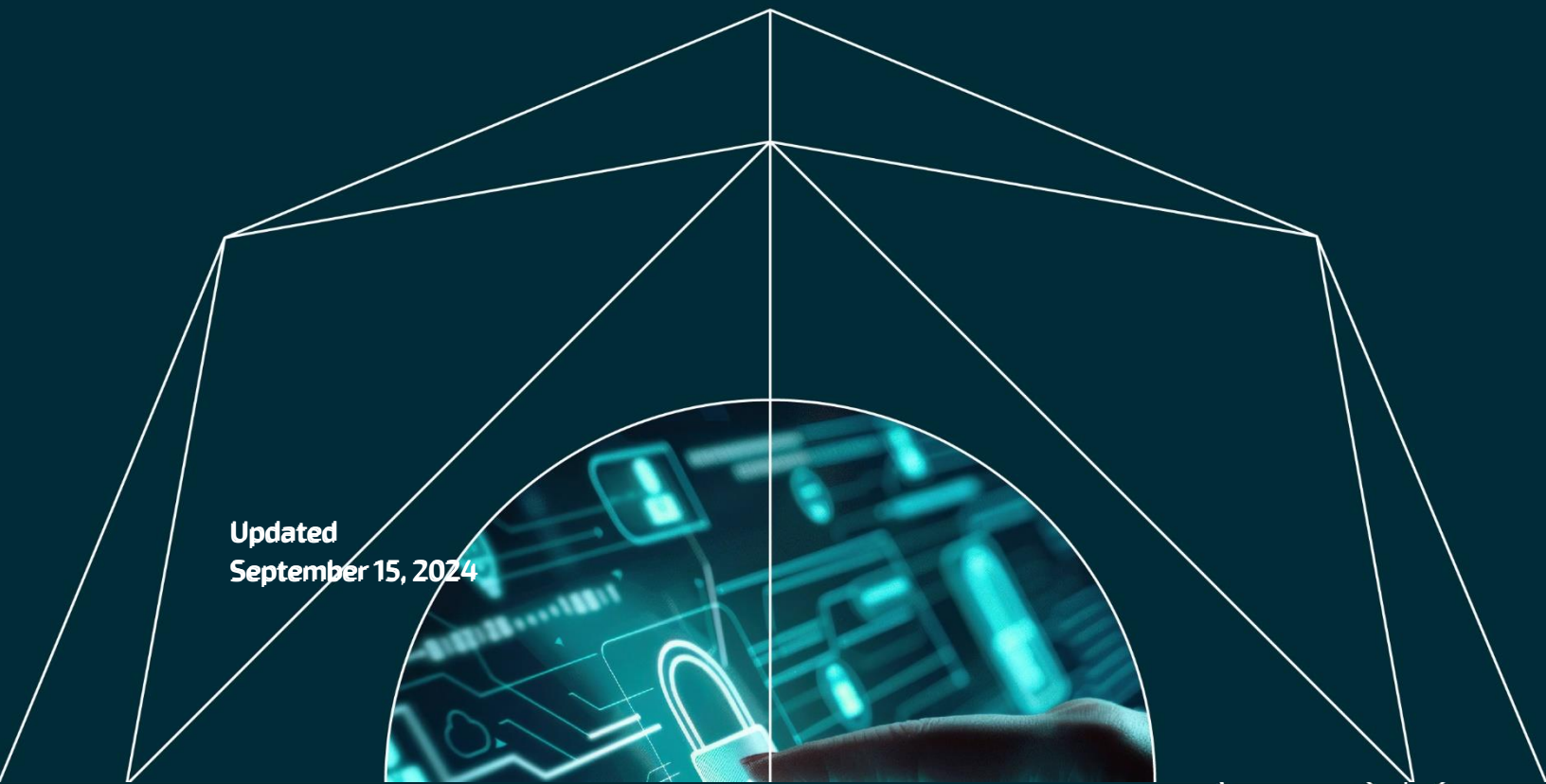
This document highlights the need for a shift to Process-Oriented OT Cybersecurity in response to rising cyberattacks on Data Centers and critical infrastructure. By using Machine Learning and a Multi-Level strategy, this approach enhances the NIST Incident Response framework across all phases: preparation, detection, containment, and post-incident activity. Simulated attacks, team training, and AI analysis enable more precise threat detection and response. Integrating this method is crucial for bolstering resilience against evolving cyber threats in OT environments.

About SIGA

SIGA's provides a Process-Oriented OT Cybersecurity for real-time decision-making capabilities for managing all Incident Response phases of an OT cyberattack – including Detection, Containment and Cyber Forensics. Unlike other solutions, SIGA detects all expressions of a cyber-attack based on its unfiltered view of all Levels of Cyber OT, including Level Zero visibility.

Founded in 2014, SIGA has global customers in multiple sectors including Oil & Gas, Power Utilities, Data Centers and Water.

For more information visit:
www.sigasec.com



Updated
September 15, 2024