SIGA Multi-Level OT Cyber Process Resilience

Is Level Zero the Missing Link in OT Cyber Security?

Is Level Zero the Missing Link in OT Cyber Security?

Unlike celebrities and politicians, no Chief Information Security Officer (CISO) dreams of appearing on the front page of the New York Times. If anything, the best CISOs are the ones the public never hears about, because nothing noticeable occurs under their watch.

In the OT (Operational Technology) world, there is one scenario that may lead to the most consequential and newsworthy decision of the CISO's professional life: whether to continue production processes which could result in severe damage or to safely shut down these processes leading to lost production and costly downtime. Either option is a risk.

At stake are people's health and safety, the physical condition of machinery and other assets, and the production output - and business results - of an organization. When downtime is unplanned, the costs are particularly high due to lost production, spoilage, and the unintended consequences on the supply chain.

The Unintended Consequence of Progress

Cyber-attacks on Industrial Control Systems and OT are on the rise. According to the 2024 Threat Report, between 2019 and 2023, have grown at annual growth rate of over 90% per year. In 2023 alone, there were sixty-eight known attacks, impairing over five hundred sites.

How did we get here? It could be argued that it started with a 2012 speech by the previous Chancellor of Germany, Angela Merkel at the Hanover Messe conference. Merkel unveiled a vision for Industrie 4.0 or Industry 4.0, the digitalization of the industrial sector. The goal was for greater automation of production, efficiency, and improved decision-making across production lines.

At the core of digitalization are interconnected systems whereby data is extracted from sensors and IoT devices and data is provided to automate processes and support decision making. And from an OT cyber perspective, that's where the problems begin.

The Lure of Digital Assets

Cybercriminals, hacktivists and state sponsored hackers have found their way to the heart of Industrial Control Systems (ICS) through interconnected OT and IT systems. According to one study, 37% of ransomware attacks on industrial organizations also attacked OT systems.

This is how it works: many OT systems are managed remotely and compromised credentials or exploited remote access tools can give hackers direct entry into OT environments.

To demonstrate how an attack works, let's use the example of a Safety Instrumented System (SIS).

An SIS is designed for the purpose of protecting potentially hazardous or critical systems. If predefined conditions indicate a potential hazard, the SIS automatically shuts down the relevant component to prevent accidents or damage.

If the attacker's primary objective is to compromise all elements of control, the SIS itself becomes another target rather than a failsafe. A sophisticated attacker will understand the safety limits and launch an attack designed to either avoid meeting these conditions or exploit them. The SIS is not designed to address unpredictable attack behavioral patterns, and attackers can therefore exploit this limitation.

What I've outlined above is not a theoretical scenario. In 2017, attackers were able to penetrate Saudi Aramco's Petro 3,000-acre Rabigh Petrochemical Refinery, using the Triton malware to target the Triconex SIS controllers manufactured by Schneider Electric. The attackers reprogrammed the SIS to stop it from triggering safety measures, meaning that the safety system itself became vulnerable.

This particular episode ended with a (relatively) happy ending: although there was a short period of downtime, the doomsday scenario of massive explosions and the release of toxic hydrogen sulfide gases were avoided.

The incident also served as a stark reminder that cybercriminals are becoming increasingly daring, and the very systems designed to prevent attack or limit the potential damage are also at risk.

The importance of Level Zero

There is a mindset within OT cyber security: prevent, prevent and prevent.

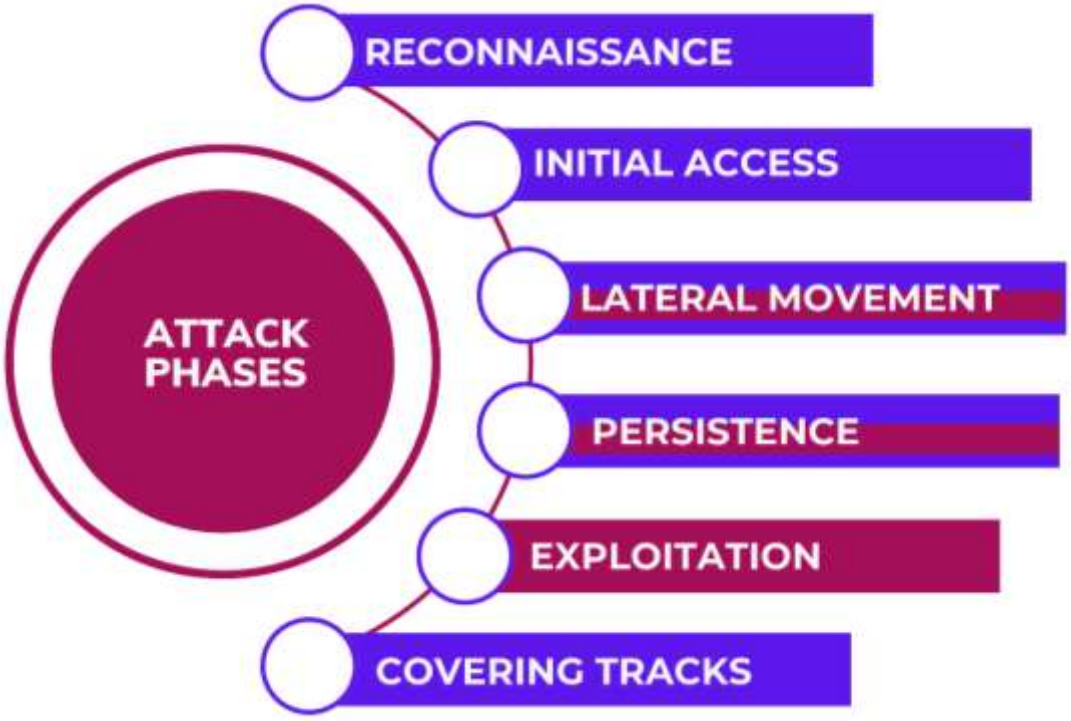
Billions of dollars are invested in protecting critical infrastructure from cyberattacks. And that's a good thing. The problem is that prevention is fallible, and it is not a question of if an attack will occur but a matter of when.

This focus on prevention comes with a price in that OT cybersecurity professionals are often unprepared for an actual breach.

We do not know all the facts in the Triton malware attack, but from media reports it seems that during the discovery of the breach, there was no objective way to verify the actual state of the refinery's equipment. In other words, if the ICS responsible for monitoirng asset behavior is compromised, any decisoin made based on SCADA data is inherently risky.

This is where Level Zero comes in. Level Zero or Level 0 in the Purdue Model is the foundational layer that includes the physical devices and the actual process. Embedded within Level Zero are the **sensors** that measure the physical properties, **actuators** that receive control signals and perform physical actions and the **field devices** used to monitor and control physical processes.

Here is the scenario that every CISO needs to plan for: during the beginning and middle of the attack i.e., the lateral movement, persistence and exploitation phases. At the very time that it is most critical to understand the behavior of the physical assets to check on the physical manifestation of the cyberattack, the ICS monitoring of Level Zero data could be compromised. Decisions on critical decisions such shut down or continuing operations normally need to be made with a direct view of the physical asset.



One common attack vector is false data injection. This is when attackers manipulate the data reported by sensors and control systems to give the appearance that all operations are normal when an attack is underway. By injecting false data, attackers can mislead operators into making incorrect decisions or failing to take necessary actions to mitigate the attack. For example, if a temperature sensor is reporting normal levels while the actual temperature is rising dangerously, the operators might not take action to cool the system, leading to potential equipment damage or safety hazards.

Level Zero from the Source

In the case of the Triton malware attack, physically checking operations at a 3,000-acre refinery was impossible. What was needed was a direct and unfiltered view of production processes, free from manipulation. Known as "out of band," it requires collecting data directly from the physical layer, bypassing the potentially compromised ICS layer.

How does it work? Out-of-band monitoring uses separate communication channels to gather and analyze data directly from Level Zero. This unfiltered data can then be compared with the data from the ICS to identify discrepancies and detect any signs of false data injection or other cyber manipulation.

This adds an important layer to an OT Decision Support System – enabling decision making based on verifiable and accurate information.

It is also worth noting that there is growing recognition of the criticality of including Level 0 detection in OT cyber security practices. NIST is now recommending that organizations make risk-based decisions about implementing separate field I/O monitoring tools and networks to detect incorrect data in their SCADA systems. In other words, Level Zero information sources.

The Role of Process-Oriented Cybersecurity

While access to out-of-band Level Zero provides unfiltered, real-time data about physical processes, OT cyber security is about the integrity of all layers of the ICS.

A CISO's decision to continue or halt operations during an attack doesn't rely solely on data from Level 0. It also depends on understanding whether there are indications of suspicious behavior both within and between each Level (0-4).

The Multi-Level (0-4) approach is based on the recognition that the higher Levels can be trusted by continuously cross-referencing it with accurate process-level data.

Process-Oriented cybersecurity is designed to protect the entire operational flow from the physical processes at Level Zero to the more strategic and business-related decisions made by the organization.

Conclusion

Every's CISO's nightmare: an OT cyberattack, a non-functioning Security Operation Center and no visibility into physical processes. Critical decisions need to be made about whether to shut down or continue operations, balance the risk of losing revenue or damage to assets.

The missing piece is the ability to understand what is happening in real time at the oil refinery, data center or manufacturing plant.

Process-Oriented Cyber Security based on access to Level Zero insights are not a nice-to-have. They could be the difference between continuous operations and catastrophic failure.