FORTINET

Security Strategies for Confronting Advanced Threats to OT

Table of Contents

Executive Overview

Operational technology (OT)—the systems that control equipment, machinery, and mechanical processes in factories, power plants, the energy grid, and other critical infrastructure—has become a bigger target for cyber criminals. With the increased convergence of OT and IT networks, the "air gap" that once insulated OT systems from bad actors has all but disappeared. Plus, an attack on OT can have severe consequences, ranging from service disruption or outages to catastrophic threats to human life.

Cyber criminals are increasingly sophisticated and adept at exploiting OT vulnerabilities. Traditional IT security is simply not up to the task of protecting OT from advanced threats. CISOs need comprehensive strategies for confronting known and unknown threats, with a focus on mitigating the impact of breaches that have succeeded in evading security controls. Such strategies incorporate solutions that enable visibility, restrict access with precision and automation, detect and contain live breaches, thwart lateral movement, and minimize the attack surface within the OT network.

90% of OT sector organizations have experienced at least one damaging attack over the past two years, resulting in significant disruption and downtime.[1]

CISOs must assume that breaches are bound to penetrate the OT environment. It is critical to have measures in place that prevent them from moving laterally, compromising systems, and doing damage.

Target: OT

Bad actors are training their sights on supervisory control and data acquisition (SCADA) and industrial control systems (ICS). The motives behind these attacks are many. Criminals may seize control of critical infrastructure and demand a ransom. Industrial competitors, often abetted by nation-state actors, can infiltrate systems for the purpose of industrial espionage. In extreme cases, attackers are in a position to commit deliberate sabotage, such as cutting off power to a large population, to advance political or military objectives.

The determination of advanced threat actors is reflected in the sophistication of their methods. Once they succeed in evading security controls, they employ tools that tell them when their malware has been detected—something cyber criminals increasingly employ upon successfully infiltrating a network, device, or application. Here, they can then use post-intrusion obfuscation and advanced anti-analysis techniques to make it as difficult as possible to analyze the attack for its methodology, origins, and intent.[2]

OT systems are particularly vulnerable to advanced threats, largely due to the prevalence of legacy systems (some 20 to 30 years old), infrequency of updating compared to IT, and disparate vendors using a mix of proprietary protocols.[3] In addition, with the advancement of digital transformation (DX) initiatives and the Internet of Things (IoT), some two-thirds of OT devices are connected either to the internet or through an enterprise gateway.[4] While defenses against external threats are essential, in view of these vulnerabilities, CISOs must assume that breaches are bound to penetrate the OT environment. They need to familiarize themselves with the solutions, techniques, and practices that will give them the upper hand against today's advanced threats.

The sections that follow outline the key measures CISOs should prioritize in developing strategies to confront advanced threats to OT.

With the advancement of digital transformation (DX) initiatives and the Internet of Things (IoT), some two-thirds of OT devices are connected either to the internet or through an enterprise gateway.[4]

Segmentation: Minimizing the Attack Surface

Once attackers breach perimeter defenses, it is critical to have measures in place that prevent them from moving laterally, compromising systems, and doing damage. The exposed assets within the OT environment collectively create a large attack surface. The first order of business is to minimize it.

Segmentation refers to separating or isolating critical assets and defining security policies around them that restrict access to them—essentially building "rooms and walls" across the network and cloud infrastructure that require an explicit level of trust to enter. Segmentation can take a variety of forms:

- **Macrosegmentation** involves dividing the network environment into a series of functional segments or "zones" accessible only by authorized devices, applications, and users.
- **Microsegmentation** is the process of creating sub-zones at a more granular level, with fine-granular controls around individual or logically grouped assets.
- **Intent-based segmentation** refers to grouping assets according to business logic for segmentation purposes. Dynamic trust capabilities built into intent-based segmentation allows for automatic updating of access rights and business rules based on continuous trustworthiness assessments.[5]

By walling off groups of interdependent assets, segmentation effectively decreases the attack surface within the OT infrastructure (and IT infrastructure as well). In doing so, it restricts the ability of attackers to move laterally (viz., east-west) within the network. That means that a threat that has gained entry to the network cannot access applications running, for example, programmable logic controllers (PLCs).

Segmentation also strengthens breach detection; any unauthorized access attempt is an indicator of a possible intrusion, with next-generation firewalls (NGFWs) blocking such attempts automatically alerting all affected applications to the presence of a threat. This is particularly important as bad actors shrink the windows between intrusion and enactment of the malicious action—operational disruption or outage, ransomware demands, or data theft.

Network segmentation efforts lag in the OT sector, with 45% of ICS/SCADA users not making use of privileged identity management.[6]

The determination of advanced threat actors is reflected in the sophistication of their methods.

Secure, Centralized Access Control: Users, Devices, and Applications

In spite of all the defensive technologies available, the weakest point in any security infrastructure is most often the point of human contact. Many damaging security breaches have been the result of compromised user accounts and passwords or inappropriate levels of access.[7]

Devices, users, and applications need to be authenticated before they access the OT environment or any of its segmented assets. CISOs need solutions that can accurately validate who or what is trying to connect. This calls for roles-based controls that restrict access permissions based on responsibilities as well as the means to manage permissions on an ongoing basis. Intent-based segmentation can help restrict access to specific segments of the network by specific individuals based on business logic. With network access control (NAC), OT teams can implement policies governing device and user access.

In addition to the above, OT is increasingly leveraging wireless connectivity for remote monitoring and management, connecting cloud-based controllers to the sensors and embedded devices that operate equipment and generate data. This certainly helps increase operational agility and automation, but it adds a new level of vulnerability. To ensure they are protected from advanced threats, OT teams need the ability to secure wireless traffic, wireless access points, and switches. This enables them to block threats from exploiting these over-the-air connections.

Devices, users, and applications need to be authenticated before they can access the OT environment or any of its segmented assets. CISOs need solutions that can accurately validate who or what is trying to connect.

Advanced Threat Protection and Detection

As attackers become better at avoiding detection and masking intent, CISOs need advanced solutions in their arsenals that match the increasing sophistication of threats. While many solutions have been designed to stop known attack types, OT teams need the ability to recognize and thwart unknown and zero-day attacks—namely, those that exploit vulnerabilities that have just been discovered but not yet patched.

Threat-deception techniques can help mitigate and minimize the damage of a live breach.[8] Deception involves the deployment of decoy virtual machines (VMs) or applications within the infrastructure that attract, engage, confirm, and contain attackers. It is an important method for ferreting out unknown and zero-day threats. Deception tools serve as an early warning system by providing accurate detection and tracking lateral movement activity, frequently allowing attacks to proceed under close observation and providing threat intelligence to inform the appropriate security response.

Sandboxing has also proven effective against emerging and zero-day threats. The term refers to isolating suspicious activity from general traffic and observing it in a simulated environment, first to confirm whether it is malicious and, if so, to automatically initiate mitigation. To effectively protect OT, a sandboxing solution needs to support the types of operating systems encountered in the OT environment. OT-specific sandboxing is a critical addition to the security fabric for uncovering advanced threats that have succeeded in eluding traditional malware detection.

"The key to a good decoy is its believability. It must not be too heavily guarded that it cannot be breached, nor must it be so vulnerable it cannot be believed. If attackers can recognize a decoy, they can avoid it; so, it must look, feel, and behave like the rest of the network."[9]

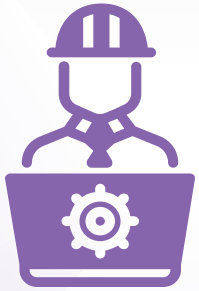
AI-powered Threat Protection, Detection, and Response

Advanced threats increasingly incorporate artificial intelligence (AI) and machine learning (ML). Malicious actors are employing AI to map networks, test vulnerabilities, and build custom attacks on their targets—and this includes OT environments.[10] They also are well aware that security staff and resources are often stretched thin. Organizations need to respond with their own AI and ML capabilities. AI, ML, and automation can help augment and increase the effectiveness of security teams, strengthening their detection capabilities, enabling them to prioritize investigations, and minimizing false positives.[11]

Comprehensive strategies should include integrated and automated threat-intelligence sharing. CISOs need solutions that will automatically communicate the presence of any discovered threats between the IT and OT environments and across each security element—from the data center and main campus to the edges of the network.

Organizations also need to centralize security incident response and event management. A security strategy will not be effective if solutions operate in silos. Integration across the security infrastructure is essential to enable the automated aggregation of data from prevention and detection solutions. This, in turn, is necessary to provide contextual awareness of threats in the OT environment.

Finally, an advanced threat detection and mitigation strategy should incorporate user and entity behavior analytics (UEBA), typically used to identify insider threats. Insiders account for a significant percentage of intrusions, usually through negligence, but sometimes with malicious intent. A 2019 Deloitte study of cyber risks in the electric power sector cites human error and disgruntled employees as the "most common threats."[12] In order to address these issues, UEBA needs to leverage ML and advanced analytics to automatically identify noncompliant, suspicious, or anomalous behavior and alert any compromised user accounts.



Comprehensive strategies should include integrated and automated threat-intelligence sharing. OT operators need solutions that will automatically communicate the presence of any discovered threats between the IT and OT environments and across each security element.

Conclusion

The growing volume and sophistication of advanced threats raises the stakes for CISOs—and the risk is for both IT and OT environments. Attacks on OT can have dire consequences, not only for industrial enterprises and infrastructure operators but also for the general public. CISOs need to understand the advanced threat landscape, review their security posture, identify gaps and vulnerabilities, and figure out the solutions needed to counter these threats. Some of the questions CISOs need to ask when doing so include:

- Is our security infrastructure integrated so that threat intelligence can be shared in real time across all security elements?
- Does our threat intelligence use AI and ML to identify unknown and zero-day attacks?
- Do we have automated incident response and event management workflows in place to mitigate successful intrusions before they propagate and have an impact?
- Do we have advanced threat- and breach-detection capabilities in place such as sandboxing and decoys?
- Do we have measures in place to shrink the attack window and block access to network assets post-intrusion?

[1] "Cybersecurity in Operational Technology: 7 Insights You Need to Know," Ponemon Institute, March 2019.

[2] "Threat Landscape Report Q2 2019," Fortinet, August 7, 2019.

[3] "Operational technology cybersecurity: A vision for the industrial sectors," EY, August 2018.

[4] Barbara Filkins, "The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns," SANS Institute, July 18, 2018.

[5] "Reducing Complexity with Intent-base Segmentation: Best Practices for CIOs," Fortinet, April 5, 2019.

[6] "Independent Study Pinpoints Significant SCADA/ICS Security Risks," Fortinet, June 28, 2019.

[7] Paul Yung, "Security Think Tank: Many breaches down to poor access controls," ComputerWeekly, March 8, 2016.

[8] Gary S. Miliefsky, "Why Deception Technology Will Change the Game in Our Favor Against Cyber Crime and Breaches," Cyber Defense Magazine, June 30, 2019.

[9] Kevin Townsend, "How Deception Technology Can Defend Networks and Disrupt Attackers," SecurityWeek, June 5, 2019.

[10] Derek Manky, "The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware," CSO, August 29, 2018.

[11] "Using AI to Address Advanced Threats That Last-Generation Network Security Cannot," Fortinet, June 8, 2019.

[12] Steve Livingston, et al., "Managing cyber risk in the electric power sector," Deloitte Insights, January 31, 2019.

www.fortinet.com

448135-0-A-EN

September 26, 2019 2:58 PM

eb-Advanced-threat-landscape-for-OT-CISO