FORTINET

How to Design Security for OT Network Environments

Prevent, Detect, and Properly Manage Advanced Threats

Table of Contents

Executive Overview

Sophisticated cyberattacks are putting industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems at risk. As operational technology (OT) networks converge with information technology (IT), the expanded attack surface opens the door for advanced cyber-threat actors to target these critical systems. ICS and SCADA systems on OT networks possess unique operational requirements that can make them more difficult to secure than their IT counterparts. As such, OT networks require security approaches and solutions that are designed specifically for them.

Employing automated security practices and deceptive technologies can help to detect advanced threats within OT networks. Network-level security solutions identify and control the spread of hacker-provoked cyberattacks across an OT network. A centric element of this strategy is OT-specific threat intelligence, which supports rapid identification of, and response to, threats targeting multiple OT sites or global threats to the industry.

64% of OT decision-makers say that sophisticated cyberattacks are a top challenge.[1]

Introduction

OT systems are facing new cyber threats. In the past, OT networks were physically isolated from IT systems with an "air gap." However, as a byproduct of digital innovation, many organizations are eliminating or minimizing air-gap dependence. As a result, OT and IT networks are more often connected, and cyber criminals leverage IT networks as a stepping stone to gain OT network access.

OT systems are often long-lived assets, integrating components that have field life cycles of 20 years or more in some cases. It would hardly be uncommon for these devices to host numerous easily exploited vulnerabilities that have been discovered over the years—old threats. Now, new threats are evolving in the criminal ecosystem with the dark web enabling new and sophisticated attacks that are multipronged and targeted specifically at OT operators.

The unique availability requirements of OT infrastructure mean that security solutions must be carefully designed to ensure minimal impact on operations. Additionally, OT networks must achieve and maintain compliance with OT-specific regulatory guidelines, such as those created by the National Institute of Standards and Technology (NIST), the European Commission's Directive on Security of Network and Information Systems (NIS Directive), and the North American Electric Reliability Corporation (NERC).

Automated threat detection and response, OT-specific threat intelligence, deceptive technologies, and network segmentation are four key elements of a robust OT security approach to address the advanced threat landscape.

Nearly three-quarters of OT organizations have connections between IT and OT networks.[2]

Automated Threat Detection and Response Improves System Availability

Advanced threat actors have the resources and sophistication required to design attacks that evade traditional detection mechanisms. Organizations require deep network visibility and situational awareness to differentiate between actual threats and false-positive detections and to perform attribution, recognizing attack behavior and identifying the threat actor.

Achieving the required level of visibility and situational awareness for rapid incident response requires automation. Automated collection, aggregation, and analysis of security data helps to pinpoint actual threats (instead of an overwhelming number of false positives) and provides the context that is required for accurate threat response and remediation.

Automation can also enable more rapid response to an identified threat. By creating threat playbooks codifying responses to common threats, an organization can automate parts of the threat detection and remediation process. This helps to support the high-availability needs of OT systems since, once an analyst has identified an active threat, some or all of the remediation steps can be performed instantaneously, minimizing the threat's impact on operations.

Increased situational awareness and automated incident response help to ensure the security and availability of OT systems. Targeted responses, which identify and remediate threats at the process level, minimize the impact of incident response on system availability.

78% of organizations have only partial centralized visibility of their OT environments.[3]

Automation boosts system availability by enabling rapid, targeted response to cyber threats.

OT-specific Threat Intelligence Identifies Unique Threats

OT systems are high-value targets. Adversaries are willing to invest the time and resources required to identify and exploit vulnerabilities in these systems. Cyber-threat actors commonly perform reconnaissance against OT-specific systems and leverage the fact that OT uses custom network protocols—which are often not understood by cybersecurity solutions designed for IT networks—to conceal their activities.

Cyber-threat management on OT networks requires a similar level of OT-specific knowledge and multiple years of experience securing OT environments. OT network security requires access to OT-specific threat intelligence. Since OT organizations integrate equipment manufactured by a select set of vendors, visibility into vulnerabilities within these vendors' products is essential to security. This enables OT vendors to harden systems against exploitation and deploy virtual patching to effectively protect vulnerable systems during long gaps between maintenance windows.

Organizations also require the ability to share this threat intelligence inside and outside the organization and to leverage third-party threat intelligence. This enables identification and rapid response to widespread OT-specific attack campaigns using artificial intelligence (AI) and machine learning (ML).

85% of OT threats target machines running the OPC Classic, BACnet, and Modbus protocols.[4]

Cybersecurity solutions for OT systems require knowledge of OT-specific threats and protocols.

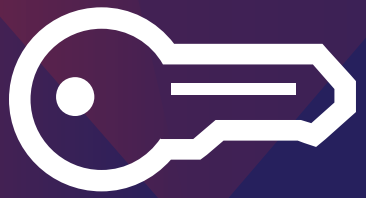
Deceptive Technologies Enable Detection of Advanced Threats

Advanced threat actors often craft “low and slow” attacks that evade traditional network defenses, with an attacker present on an organization’s network without detection.

The use of deceptive technologies can help to expose these evasive threats. Honeypots can be configured to resemble realistic OT systems, increasing the probability that a threat actor or their malware will opt to interact.

If this occurs, it indicates the presence of a threat within the shadow network since no legitimate operation will use these systems. Additionally, by examining the details of the attacker’s operations on the system, it may be possible to extract valuable threat intelligence regarding the attacker’s tools, techniques, and capabilities. This threat intelligence supports more efficient detection and remediation of these threats on other systems within the OT network and may enable the organization to identify zero-day attacks that traditional, signature-based detection systems would not be capable of identifying.

OT security also benefits from the deployment of sandboxes capable of emulating OT-specific systems. Automated instrumentation and machine learning enable the detection of unknown threats based upon detection of anomalous or suspicious behaviors when executed in these emulated environments.



“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.”[5]

Network Segmentation Isolates and Contains Threats

OT environments have extremely high availability requirements that affect OT cybersecurity. Due to tight maintenance windows and uptime requirements, many devices run end-of-life operating systems and software. Often, older hardware lacks the resources to run traditional antivirus systems. Finally, if an incident occurs, taking down impacted systems for remediation may not be possible.

All of these factors contribute to the fact that OT security must often be performed at the network level rather than on the endpoint. Through the use of network segmentation and virtual patching, the risk posed by unpatched and vulnerable devices can be reduced. Instead of applying updates to the device, which may impact system availability, virtual patching ensures that traffic attempting to exploit a known vulnerability is blocked before it reaches the vulnerable device.

Network segmentation can also help to reduce the impact of a cybersecurity breach by limiting the lateral movement of an adversary through the network. Segmentation ensures that all communications between devices are scanned for malicious or anomalous content and that strong user authentication and access controls are enforced throughout the network.

Top-tier OT organizations are 51% more likely to use network segmentation than bottom-tier organizations.[6]

Network segmentation is necessary to prevent lateral movement of advanced threats through OT networks.

Conclusion

OT networks are increasingly a target of advanced cyber threats. These attackers are familiar with OT systems and develop custom malware designed to exploit vulnerabilities in systems commonly used in OT environments.

Network operations leaders need to understand the broadening attack surface and consider security automation, OT-specific threat intelligence deception technologies, and network segmentation to combat advanced threats.

Some questions network operations leaders need to ask when doing so include:

- Do we have automated incident response and event management workflows in place to mitigate successful intrusions before they propagate and have an impact?
- Is our security infrastructure integrated so that threat intelligence can be shared in real time across all security elements?
- 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] "Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?" Siemens and Ponemon Institute, 2019.

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

[3] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, June 30, 2020.

[4] "Fortinet 2019 Operational Technology Security Trends Report," Fortinet, May 8, 2019.

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

[6] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, June 30, 2020.

www.fortinet.com

726519-0-0-EN

July 23, 2020 9:42 PM

eb-how-to-design-security-for-ot-network-environments