CYBERSECURITY FOR LIFE SCIENCES

Your Guide to a Secure OT Environment

ZETHER

+1-844-ZAETHER www.zaether.com

Table of Contents:

Consider the numbers:

38%

Manufacturing organizations experienced 950 cyberattacks per week in 2022 – an increase of 38% compared to the previous year

(Source: Check Point Research)

$4.35M

The average total cost of data breaches in 2022 was $4.35 million

(Source: IBM and Ponemon Institute report)

45%

By 2025, 45% of organizations globally will experience a supply chain attack

(Source: Gartner)

20%

Nearly two out of three mid-sized organizations have suffered a ransomware attack in the past 18 months, 20% of which spent at least $250,000 to recover

(Source: ConnectWise)

INTRODUCTION

Operational Technology (OT) drives the economy and supports our way of life, from the medicines we take to the water we drink. Historically, OT systems were less exposed, but as Information Technology (IT) and OT systems increasingly converge and OT systems move online, they become more vulnerable to cybercriminals.

As companies invest in new systems to increase safety, capacity, uptime, and performance, cybercrime remains an omnipresent threat to create catastrophic disruptions. These can result in economic loss, compromised safety, and tarnished reputation.

IT and OT teams face numerous challenges, including protecting OT environments from cyberattacks, maintaining compliance with continuously changing industry regulations, managing complex, interconnected technology environments, and ensuring uptime and systems availability. Teams now need to increase OT security without compromising manufacturing productivity.

To address these challenges and mitigate risks, technical, organizational, and procedural measures must be put in place to maximize security without affecting manufacturing operations. Stakeholders across organizations must increase security awareness and implement best practices with proper reporting to evolve their cybersecurity stance.

In this guide, **ZAETHER** shares its expertise in proven cybersecurity frameworks, industrial automation, and digital transformation to map out OT vulnerabilities and help companies develop measures to secure the OT environment without negative impacts.

Know the OT Environment

IT/OT Convergence: Digital Transformation Carries Risk

The first step in securing industrial systems is to understand the relationship between IT and OT systems. While these two areas of expertise have traditionally operated separately, convergence of IT and OT systems has blurred their boundaries.

IT is typically responsible for data systems with enterprise-level functions such as finance, HR, and email while OT systems control and monitor industrial processes such as pharmaceutical batch processing, chemical processing, and power generation.

IT/OT integration brings physical equipment into the digital realm with the goal of optimizing processes and improving plant-wide performance. This is often referred to as Digital Transformation and includes innovations such as wireless communication between machines and systems, the collection of real-time manufacturing data to empower decision-making, and automated and autonomous operations. These advances reduce unplanned downtime, increase efficiency, and lower operational expenses. They also expose OT environments to cyberattacks.

Cybersecurity Assessments: Understand Your OT Vulnerabilities

A thorough evaluation and analysis of infrastructure – hardware, software, network – is essential to protect an OT environment. An assessment gives insights into the risk exposure of assets, evaluates existing security controls, and identifies threats and potential vulnerabilities. With these insights, businesses can develop a plan to address system weaknesses.

A typical OT assessment includes asset inventory, vulnerability scanning, penetration testing, and risk analysis. Correctly identifying risks and vulnerabilities is critical to the security and resilience of any OT infrastructure regardless of industry.

Network Segmentation: Keep Your Data Separated

Network segmentation can be a complex process, but it is a critical step in securing OT environments against evolving cyber threats. Too often, companies are unable to identify network segmentation issues that exist in their OT environment.

ISA-99 provides a framework for segmenting Industrial Control System (ICS) networks into six distinct layers with defined components and logical network boundaries. Segmenting the network allows organizations to control data access and limit the spread of cyberattacks, making it more difficult for malicious actors to move laterally through the network.

A well-segmented network provides increased security and resilience by creating barriers to entry and containment zones. Appropriate security controls and policies can be applied to each network segment to simplify incident response by limiting the scope of an attack, reducing downtime, and speeding up recovery efforts.

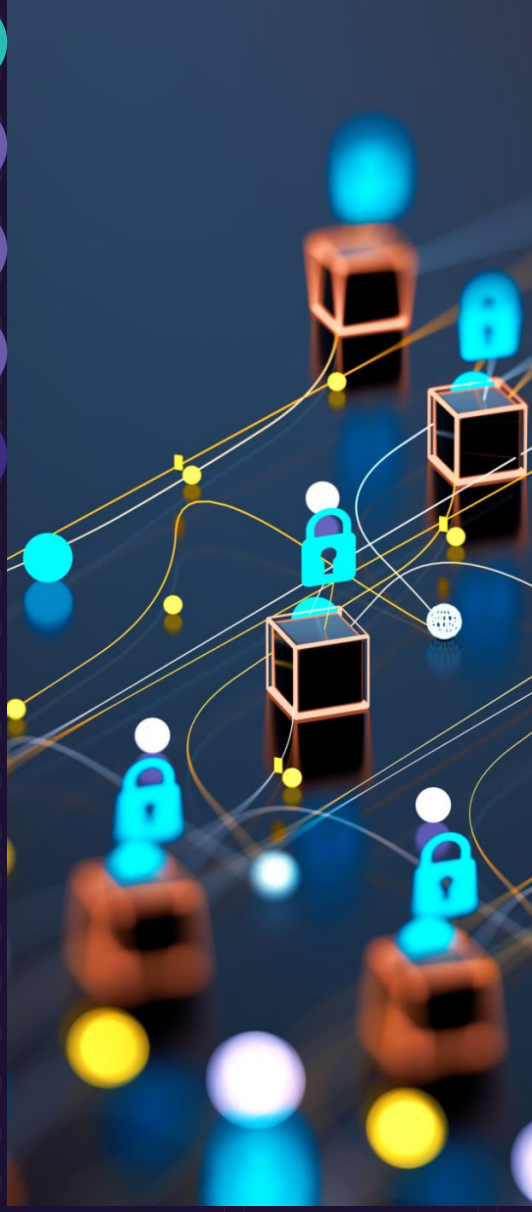
Asset Management: Know the Facility

A comprehensive understanding of all OT infrastructure assets identifies where assets live in a network infrastructure and whether any are improperly segmented.

Identifying, tracking, and managing all hardware assets can improve performance, reduce downtime, and minimize costs associated with maintenance and upgrades. Regular updates should be prioritized by level of risk and performed according to a set plan. These policies and procedures include specified roles and responsibilities of all stakeholders, the frequency of asset reviews, and the tools and technologies used to collect and analyze asset data.

Continuous monitoring identifies any rogue devices that may have been connected to a network. Keeping inventory accurate and current greatly improves overall cybersecurity posture and enhances OT systems' resilience.

Protect the OT Environment



Perimeter Protection: Is the Environment Properly Protected?

Firewalls are a key component to securing network perimeters by filtering traffic and preventing unauthorized access. A well-designed perimeter firewall can significantly reduce the risk of a successful cyberattack and protect against a variety of other threats. Internal firewalls assist with securing network segmentation and controlling traffic flow between different internal networks.

Properly configured firewalls can prevent unauthorized access to sensitive data, stop the spread of malware and viruses, and help ensure compliance with industry regulations and standards.

Firewalls are not impregnable and can be bypassed by skilled attackers. They should be continuously maintained by keeping security patches and firmware up-to-date, regularly reviewing logs for unusual activity, configuring Access Control Lists (ACLs) to deny unauthorized traffic across networks, and ensuring that firewall rules are regularly reviewed and updated to reflect network changes. Firewall configuration changes should always be tracked to ensure compliance and standardization of firewall rules.

Next-Generation NGAV/EDR: Protect Assets

In today's complex threat landscape, next-generation antivirus (NGAV) and endpoint detection and response (EDR) technologies are game-changing.

Unlike traditional antivirus software that relies on known threats and known file signatures, NGAV and EDR detect and prevent malware and other threats by monitoring networks for threat behaviors and indicators. By analyzing patterns in behavior, these technologies can detect previously unknown threats and updated known threats that traditional antivirus software would miss.

NGAV and EDR provide better visibility into network endpoints, allowing for improved access control and protection. These technologies can be configured to provide real-time alerts and notifications to security teams, enabling them to respond quickly and effectively to threats, and to ensure that actions are not taken that would negatively impact production.

Whitelisting: Control Applications

Whitelisting allows only pre-approved applications and processes to run on a system. Whitelisting reduces a system's attack surface and potential attack vectors, making it more difficult for cybercriminals to gain access or execute malware or ransomware on OT systems.

Whitelisting can also help businesses comply with regulatory requirements, providing a clear audit trail of all the applications and executables allowed to run on systems. The larger an organization, however, the longer the list of applications and systems – making it more challenging to implement and maintain a whitelist.

Continuous monitoring, timely updates, and regular testing will keep existing applications secure and provide a framework to safely integrate new ones.

Monitor the OT Environment

Network Monitoring:
Know How Data is Flowing

By capturing and analyzing network traffic data, potential security threats can be identified and mitigated. This process involves monitoring all network traffic to detect any unusual, unexpected, or suspicious activity that may indicate an attack. Proper network monitoring provides actionable insights to rationalize environment communications and proactively manage networks to mitigate risk. OT departments need to develop passive monitoring practices to ensure that manufacturing processes are unaffected.

A comprehensive network topology map provides a visual representation of the network infrastructure. This allows network administrators to quickly troubleshoot problems, make informed decisions to improve network design, and identify improperly configured network segmentation rules.

Endpoint Log Collection:
Another Layer of Defense

Collecting and analyzing endpoint logs can detect threats and attacks that standard security measures may miss. Endpoint log collection can provide valuable insight into user activity, system changes, and network traffic that can help security teams detect, identify, investigate, and respond to potential security incidents.

Managing and analyzing endpoint logs is a challenging process, especially in organizations with large and complex IT environments. It can be invaluable to hire a third-party provider with the right technology and know-how to collect, store, and analyze endpoint logs and data without interfering with production.

Maintain the OT Environment

Vulnerability Management: Find Weaknesses

Vulnerability management is an ongoing, regular practice to identify and remediate weaknesses before they can be exploited by attackers.

Due to the complexity of OT and Industrial Control Systems (ICS), vulnerability management often requires specialized tools and expertise that may not be available to a typical IT security team, and a third-party provider may be the best option. Unlike many IT-managed applications, OT and ICS are designed to run continuously, making it critical to carefully schedule maintenance windows for patching and remediation.

Temporary alternative remediations may be needed before a scheduled downtime; however, the impact of an update or patch on an OT or ICS can be difficult to predict, as even small changes can have unexpected consequences. A careful balance must be struck between maintaining security and avoiding disruptions to critical operations.

Identity Access Management: Who Can Do What?

Identity Access Management (IAM) ensures that only authorized individuals have access, and only to the resources they require to perform their job functions. IAM policies provide secure authentication, authorization, and access controls to protect sensitive information.

Maintaining a log of access rights and how they were granted is an important component of this process. Centralized management and control of user access provide a comprehensive view of user activity and potential security threats in real time.

Configuration Change Management: Proceed with Caution

When well-designed and executed properly, configuration change management provides an audit trail of all system changes. This is invaluable in troubleshooting and identifying the root causes of any issues that arise.

The key to successful Configuration Change Management is controlling a system's configuration in a structured manner because even minor changes to ICS configurations can cause system disruptions or unscheduled shutdowns. Changes that are approved, tracked, and tested in a controlled environment before they are deployed to the production system minimize the risk of downtime or other operational issues that could impact your bottom line.

Strong communication and collaboration between different departments, e.g., operations, engineering, and IT, are required to maximize this strategy's effectiveness. By involving all relevant stakeholders in the change management process, potential issues can be identified and addressed as early as possible to minimize risk.

Be Prepared to Recover the OT Environment

Backups: Recover Quickly When Incidents Strike

The importance of backups for cyber resilience cannot be overstated. Without proper backups, companies struggle to continue business operations during and after cyberattacks. Backups are particularly vital when dealing with ransomware attacks as attackers will typically encrypt the victim's data and demand payment in exchange for the decryption key. With up-to-date and easily retrievable backups, data can be restored without paying the ransom, saving money and discouraging future attacks.

Backup processes should be conducted and tested regularly, with data stored off-site or uploaded to a secure cloud environment. The data needs to be recoverable, with a clear recovery plan in place. "Impermeable backups" cannot be altered once taken. This guarantees file integrity and should be part of any robust backup strategy.

Incident Response: Prepare for the Unexpected

Securing an OT environment is a high-stakes game; the consequences of a successful attack can be disastrous, resulting in shutdowns, outages, and much worse. Systems availability, employee safety, and business reputation can all be jeopardized. Developing a proper incident response plan can minimize the impact of a cyberattack and enable normal operations to quickly resume.

The plan should include procedures for identifying and containing an attack, minimizing damage to systems and data, and quickly restoring operations. It should also address both internal and external communication protocols to ensure that all stakeholders are informed of the situation and that the right personnel are involved in the response effort.

In addition to being well-designed, an incident response plan must also be reviewed, updated, and tested regularly. To be effective, the plan should always reflect the threat landscape and system changes, and all personnel must understand their roles and responsibilities.

Conclusion

23%	65%	76%
Global cybercrime costs are projected to grow 23% per year, reaching $23.84 trillion annually by 2027 (Source: Statista)	65% of U.S. organizations experienced cyberattacks and cybersecurity compromises to their OT systems that impacted their business (Source: Forrester)	76% of organizations were targeted by a ransomware attack in 2022 – with only 50% of them able to retrieve their data after paying the ransom (Source: Proofpoint)

No one wants to be part of those statistics and without a robust cybersecurity program, a cybercrime incident is a matter of “when”, not “if”.

Cybersecurity is not a one-time, “set it and forget it” fix. It is a programmatic, continuous process that requires consistent attention and investment, particularly as the reliance on digital infrastructure increases. It’s imperative to stay up to date with the latest news, technology, and best practices to combat increasingly sophisticated threat actors.

When it comes to securing an OT environment, a proactive approach is key to developing a mature cybersecurity posture. Leveraging the right strategies and tools, working collaboratively across IT and OT teams, and fostering a culture of security awareness within an organization can help build a resilient and secure infrastructure that supports operational evolution goals.

While the strategies outlined in this document provide a solid foundation for an OT security posture, it can be daunting to tackle these challenges alone. ZAETHER’s cybersecurity solutions team is here to help.

ZAETHER

Contact ZAETHER today to learn more.

+1-844-ZAETHER www.zaether.com