network perception

10 Building Blocks to Preventing OT Networks from Cyber Attacks

+1 (872) 245-4100 info@network-perception.com https://network-perception.com

Introduction

From the last few years, it is clear that cyber threats are increasingly common, getting more sophisticated, and expensive.

The majority of organizations still lack proper visibility to efficiently defend themselves. The urgency to improve the situation is heightened in the case of operational technology (OT) networks where cyber attacks could cause heavy damage to industrial equipment, disruption to the utilities many rely on, or even loss of life.

+1 (872) 245-4100 info@network-perception.com https://network-perception.com

How to solve this?

To be proactive and reduce risk, OT network operators need to develop cyber resiliency, which means the ability to keep running mission-critical operations despite being under threat.

Security and risk management leaders need to partner with other departments to prioritize digital supply chain risk and put pressure on suppliers to demonstrate security best practices.

These best practices are part of the NIST Special Publication 800-160 on Developing Cyber-Resilient Systems aim to help organizations reach the capability to anticipate, withstand and recover from, and adapt to adverse conditions.

Cyber Resiliency Building Blocks

1. **Analytic Monitoring**
   Monitor and detect adverse actions and conditions in a timely and actionable manner.
2. **Dynamic Representation**
   Keep representation of the network current. Enhance understanding of dependencies.
3. **Substantiated Integrity**
   Ascertain whether critical system elements have been corrupted.
4. **Coordinated Protection**
   Implement a defense-in-depth strategy, so that adversaries must overcome multiple obstacles.
5. **Redundancy**
   Provide multiple protected instances of critical resources.
6. **Diversity**
   Use heterogeneity to minimize common mode failures, particularly attacks exploiting common vuln.
7. **Segmentation**
   Define and separate system elements bases on criticality and trustworthiness.
8. **Privilege Restriction**
   Restrict privileges based on attributes of users and system elements as well as on environmental factors.
9. **Realignment**
   Minimize the connections between mission-critical and noncritical services.
10. **Non-Persistence**
    Generate and retain resources as needed or for a limited time. Reduce exposure to compromise.

Implement Analytic Monitoring

VISIBILITY AND UNDERSTANDING

Monitor and detect adverse actions and conditions in a timely and actionable manner.

Many organizations have a process to add new rules to firewalls, but they lack an efficient process to remove them. As a result, rulesets become bloated after a few years and nobody dares to clean up old rules for fear of breaking something. **The solution is for the compliance team to define baseline access policies that correctly implement internal controls and respect regulatory requirements.** This way, network engineers have a reference to use when evaluating changes, and **compliance teams can easily check for deviations from the baseline.** It is also important to include rule justification directly in the baseline record so one can understand the business reasons for specific accesses.
Once baselines have been defined, a process should be put in place to monitor changes continuously or at least periodically. It is recommended that compliance teams use a system that is independent of the IT change management process to verify changes externally.

Our advice is to leverage read-only configuration monitoring solutions that compliance analysts can easily use without having to add to the workload of the IT and networking team.

+1 (872) 245-4100 info@network-perception.com https://network-perception.com

Ensure Dynamic Representation

VISIBILITY AND UNDERSTANDING

Keep representation of the network current and enhance understanding of dependencies.

One of the key building blocks of a network compliance program is the ability to go back in time and understand precisely how firewalls, routers, and switches have been configured and modified. This means setting up a backup system to keep a copy of network device configuration files at least once a day. It also requires defining file storage and data retention policy to organize and timestamp every configuration version for at least a year. An efficient backup system will enable compliance analysts to search and retrieve records when preparing for an audit.

We cannot protect what we do not know and accurate knowledge about an organization's network starts with a complete asset inventory. Once the inventory has been created, a process should be put in place to update it periodically. This also applies to the network topology diagram, which should clearly indicate where critical equipment is located and how networks are segmented into different access zones. A network map is crucial to enabling the compliance team to gain the same clear understanding of configurations in order to work efficiently with the security and networking teams.

For incident response teams who have to investigate a breach inside their environment, a lack of detailed knowledge of networks and connected assets can turn an investigation into month-long efforts filled with frustration.

The speed at which incident response teams can answer key questions during an attack is crucial to prevent a catastrophic failure. For instance, they may need to understand which ports and services are accessible when accessing the control network from a jump host connected to the corporate network. In addition, they need to be able to answer this type of question without relying on network management toolset that can write into the network since they may be part of the issue.

For these reasons, incident response teams need to be equipped with their own highly-usable solutions that can run outside of the network fabric. This means either offline or through an indirect and read-only connection.

Develop Substantiated Integrity

VISIBILITY AND UNDERSTANDING

Ascertain whether critical system elements have been corrupted.

Cyber risk alerts should be designed through collaboration with cybersecurity experts to ensure that any misconfigurations and cyber vulnerabilities are instantly identified. Each time a change in the network is detected, the cyber risk analysis checkers are automatically running over the modified configuration files to report possible issues.

Continuous visualization and risk assessments can verify network segmentation and identify network vulnerabilities before they become breaches.

Ongoing network risk assessments should include:

- Assessing the correctness of network segmentation
- Identifying risky network connectivity paths and misconfigurations in configuration files
- Understanding exposure of vulnerable assets
- Detecting overly permissive rules
- Reporting unsecured network protocols
- Cleaning up unused rules and object groups
- Importing security advisories to check for vulnerabilities

We compiled a list of the most frequent network access vulnerabilities discovered in OT networks over the past few years. The table and descriptions below present the top 5 vulnerabilities along with best practice recommendations to remediate them.

RANK	RISK	RECOMMENDATION
1	Lack of egress access control	Verify that outbound communications are controlled
2	Insecure remote access	Analyze connectivity paths and verify remote access security
3	Incorrect segmentation	Clean up overly permissive access rules
4	Exposed vulnerabilities	Identify vulnerabilities and verify exposure through path analysis
5	Lack of change review process	Adopt a change review and firewall rule justification workflow

Ensure Coordinated Protection

DEFENSE IN DEPTH

Defense in Depth is one key component of any successful proactive OT protection strategy. According to CISA, the concept of defense in depth is to manage risk with diverse defensive strategies so that if one layer of defense turns out to be inadequate, another layer of defense will hopefully prevent a full breach.

Implement a defense-in-depth strategy so that adversaries must overcome multiple obstacles.

The most important concept in coordinated protection is understanding cyber risks in the context of your network segmentation and access policies. Gaining accurate visibility of your networks is fundamental to strengthening your cybersecurity posture.

One of the easiest ways to visualize your network without any system is to leverage a visual topology diagram of your architecture to understand your risk exposure precisely.

A visual topology diagram can automate network visibility to:

- **Eliminate blind spots:** Do we understand our current attack surface?
- **Assess vulnerability exposure:** Do we understand the details and the big picture?
- **Make informed decisions:** Strengthen network understanding and ensure defense in depth strategy covers all OT / IT risks

This should go without saying for any OT / IT personnel, but it doesn't always happen. Outdated systems lack protection and can leave you vulnerable to new attacks. Offline, encrypted backups can save the day when hackers hit – including ransomware attacks. Ensure you are backing data up at acceptable intervals - any lapse in time may be the amount of data you lose.

Establish Redundancy

DEFENSE IN DEPTH

Provide multiple protected instances of critical resources.

One way to establish redundancy is to architect OT / IT networks with independent verification. This means you can increase the frequency of monitoring controls based on criticality and network dynamics, highlighting vulnerabilities and creating a user-friendly way of visualizing your complex ecosystem in order to ensure redundancy in your systems at all times.

To identify vulnerabilities and establish redundancy, a network risk assessment can be helpful. Network risk assessments are an assessment of the networks your business/employees use daily.

These assessments help identify what the risks are to your critical systems by using risk assessment tools to:

- Assess the correctness of your network segmentation
- Identify risk in network connectivity paths
- Understand the exposure of vulnerable assets
- Within a few hours, your critical infrastructure can be continuously monitored to give a clear understanding of your network and its vulnerabilities.

+1 (872) 245-4100 info@network-perception.com https://network-perception.com

Implement Network Diversity

DEFENSE IN DEPTH

Use heterogeneity to minimize common mode failures, particularly attacks exploiting common vulnerabilities.

Once you establish practical measures for identifying your baseline, you can plan for accelerating your response to future attacks. Establishing diversity in your organization's network with a heterogenous approach ensures you can remain functional in an attack.

By connecting to other operating systems, networks and / or protocols, and working with OT / IT systems collaboratively, OT operators can prepare for the inevitable. Adding layers of protection (firewalls, antivirus, intrusion detection, etc.) and training employees on cyber resilience can also help mitigate risk.

The crux of the problem is that traditional network-centric, point-solution security tools are no longer sufficient to combat the speed and complexity of today's cyberattacks. This is particularly the case as operational technology (OT), which connects, monitors and secures industrial operations (machines), continues to converge with the technology backbone that processes [an] organization's information technology (IT).

Gartner

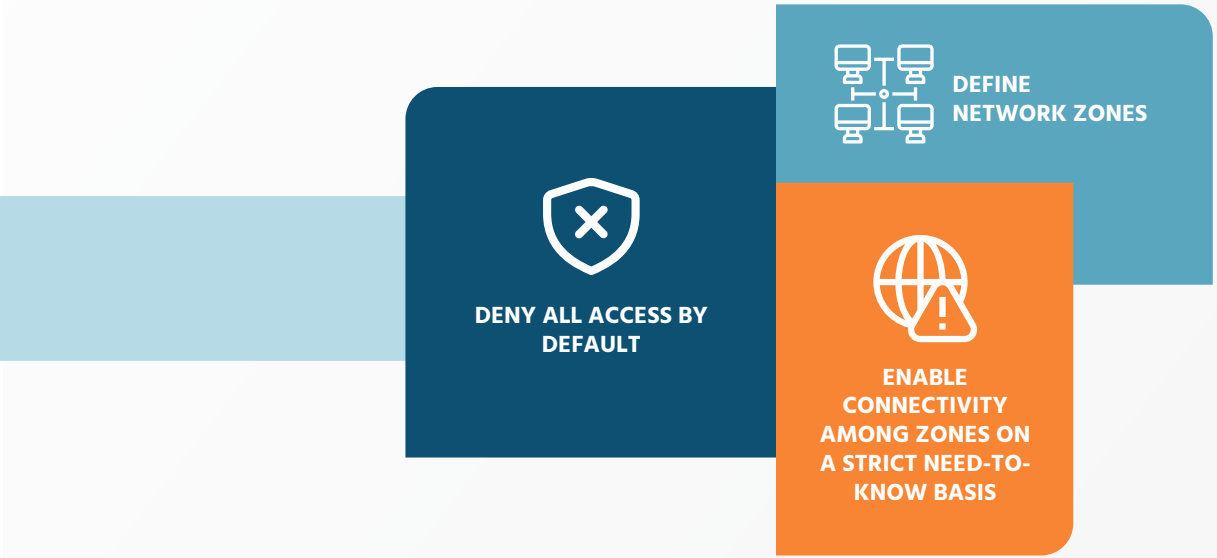
Establish Network Segmentation

LEAST PRIVILEGE PRINCIPLE

Define and separate system elements based on criticality and trustworthiness.

Segmenting a network is the most efficient way to prevent attackers from extending their reach through lateral movement. Unfortunately, network segmentation is easier said than done. Complex network environments going through frequent changes are prone to become more porous over time.

We recommend adopting a **3-step network access policy** hardening approach:



If starting from a clean slate is not possible, then one should at least verify rulesets to identify overly permissive rules (e.g., “any” source or “any” destination) and reduce their scope.

8

Privilege Restriction

LEAST PRIVILEGE PRINCIPLE

Restrict privileges based on attributes of users and system elements as well as on environmental factors.

By leveraging the Principle of Least Privilege, utilities can achieve a faster time to value and protection over longer traffic analysis solutions. The principle states that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Also known as Network Segmentation, this strategy enables organizations to understand the criticality of assets and to separate dependencies to avoid catastrophic failure.

Realignment

LEAST PRIVILEGE PRINCIPLE

Minimize the connections between mission-critical and non-critical services.

Once you understand cyber risks in the context of your network segmentation and access policies, you can develop a robust vulnerability mitigation workflow to ensure your ecosystem of IT / OT tech and solutions is protected 24/7 and to enable multiple ways to achieve your mission during a critical attack period.

This strategy involves the integration of multiple layers of data and systems protection to ensure 100% uptime and security regardless of the failure of one or more systems.

Non-Persistence

LEAST PRIVILEGE PRINCIPLE

Generate and retain resources as needed or for a limited time. Reduce exposure to compromise.

The current critical infrastructure threat landscape includes sophisticated and capable hackers from state actors and organized criminal gangs. They often share the latest and most effective hacking tools and tactics with each other.

A breach can have catastrophic consequences for OT industrial systems, and it is essential that security measures require speed to mitigate threats. This operational velocity is required for monitoring ports and services, security patch management, malicious software identification, and especially rapid incident response.

You can reduce exposure and accelerate your ability to recover by transitioning from snapshot assessments to continuous network monitoring, including regular scans to identify and address vulnerabilities, especially those on internet-facing devices.

There is no one size cyber resilience framework that fits all cases, even in the same industry such as utilities. The ability to be cyber-resilient starts with a risk management focus and allocation of resources and training to varying threat scenarios to get to the end goal of being able to recover quickly and remain operational. It also requires a customized strategy augmented by automation tools to keep systems optimally prepared and running.

Don't stay in the dark when it comes to your critical networks. Cyber resiliency starts with understanding the entire OT / IT network so we can protect and make it as difficult as possible for an attack to take place. Then, make sure you can still operate when attacked, respond, and, most importantly – recover.

As part of a defense-in-depth strategy, backups should be regarded as the last line of defense - not the first. After all, it's better to prevent a ransomware infection from happening in the first place than to have to restore your backups in response to an infection that has already occurred.

Next Steps

- Engage in a conversation with your team about cyber resiliency
- On which cyber systems do our critical operations depend?
- How are those systems connected, and how are communications controlled?
- Schedule a cyber resiliency review (CRR)
- Harden your network access policies and adopt independent network change review
- Identify your mission-critical assets & services
- Deny all access by default
- Grant network access on a need-to-know basis
- Separate responsibilities between change implementation and change review

It's never too early – or too late, to protect our vulnerable utilities and infrastructure systems. Contact us and let us help you with your cyber resiliency strategy. Assess your risks today with Network Perception and see what you can do to become cyber-resilient.

+1 (872) 245-4100 info@network-perception.com https://network-perception.com

Why Network Perception

NETWORK ACCESS VISIBILITY IS VITAL TO PROTECTING CRITICAL ASSETS.

At Network Perception, we believe organizations can safeguard and maintain critical infrastructure by virtue of their ability to anticipate, withstand, recover, and adapt to adverse conditions.

Like an immune system that continuously monitors and alerts, organizations are architecting their IT / OT networks with independent verification. This means they can increase the frequency of monitoring controls based on criticality and network dynamics.

Our purpose is to guide them on their journey to become cyber-resilient by highlighting vulnerabilities and creating a user-friendly way of visualizing this complex ecosystem. Network Perception helps organizations address network compliance and security while driving sustainable cyber resiliency in the future.

Network Perception proactively and continuously assures the security of critical OT assets with intuitive network segmentation verification and visualization.

Our platform takes essential auditing technology and makes it continuous for proactive OT network security that builds cyber resiliency. NP-View creates intuitive topological maps that serve as a GPS for both technical and non-technical users, providing a unified ruleset review and insight into how to ensure network security.

Threats don't wait for an audit, and neither should you. With Network Perception, you know your risk now and always and protect your critical networks with:

+ **Network Visualization and Firewall Ruleset Software** for visualizing and analyzing your network topology
+ **Network Risk Assessment and Architecture Review** to protect your business with network segmentation and cybersecurity solutions. Our accurate connectivity paths, vulnerability visualizations, and topology mapping help you identify and secure your cyber assets.
+ **Firewall Ruleset Representation and Policy Review** for a detailed analysis and report of your network security configuration.

+1 (872) 245-4100

info@network-perception.com

https://network-perception.com

Request a Demo