WHITE PAPER

Operational Technology Security - Best Practices

HOLM SECURITY

Protecting Your Operational Technology

Operational Technology security references not only the security solutions that will need to have in place to protect operational technology infrastructure, its people, and the data collected. It also references the best practices in identifying any vulnerabilities in your defenses that are protecting your OT. In this white paper, we will cover what are the recommended best practices, including recommended products, when identifying and, in turn, eliminating vulnerabilities in your OT security attack surface.

Operational Technology & Core Components

Every day, multiple technologies work in the background to make modern life possible. Two of the most important examples include Information Technology (IT) and OT. While most of us are familiar with IT what about OT?

Operational Technology

OT is the use of hardware and software to monitor and control physical processes, devices, and infrastructure. OT systems are found across a large range of asset-intensive sectors, performing a wide variety of tasks ranging from monitoring critical infrastructure (CI) to controlling robots on a manufacturing floor. OT is used in a variety of industries including manufacturing, oil and gas, electrical generation and distribution, aviation, maritime, rail, and utilities.

Industrial Control System

Industrial control systems (ICS) are the main component of operational technology. ICS includes different types of devices, systems, controls, and networks that manage a variety of industrial processes. The most common are supervisory control and data acquisition (SCADA) systems).

SCADA

Supervisory Control and Data Acquisition (SCADA) is a systems architecture for managing large and complex processes. SCADA systems are normally found in utility providers such as natural gas and electric power transmission, where control functions are distributed over a large geographic area.

SCADA systems consist of three main components:

- A central command center consists of all the servers running SCADA software.
- Multiple, remotely located local control systems directly control and automate process equipment.
- Communication systems connect the servers at the central command center to the remote locations.

The main purpose of SCADA is data acquisition: the networks consist of multiple remote terminal units (RTUs) that are used to collect data back at the central command center, where they can be used to make high-level decisions.

OT Security

Gartner defines OT security as, "The practices and technologies used to protect people, assets, and information involved in the monitoring and/or control of physical devices, processes, and events." Therefore OT security solutions include a wide range of security technologies to achieve such. However to minimize your attack surface a vulnerability management platform that continuously checks for gaps in your security defenses that covers both technical and human assets is also highly recommended.

OT Security Best Practices

Due to the reliance on traditional security for OT equipment and Industrial Internet of Things (IIOT) devices, the network must be secured to prevent cyber attacks. As OT-IT networks converge, next-gen vulnerability management helps security leaders gain visibility, insights, and recommendations for strengthening their security defenses. Next-generation vulnerability management solutions must deliver the following for consistent, effective IT and OT attack surface monitoring:

- Active and passive network scanning of your technical assets.
- Proactive cyber security training of your human assets.

Active & Passive Network Scanning of Technical Assets

With the expansion in types of technical assets connected to the enterprise network, nonstandard IT assets such as OT will benefit from passive observation using network-level scanners to achieve real-time visibility. Agent-based scans are suggested on laptops that rarely connect back to the enterprise network, and that would be missed with a network scan. It is therefore recommended for organizations to combine active scanning with passive and agent-based scanning to have real-time visibility resulting in improved asset coverage.

Passive Monitoring

Passive monitoring uses deep packet inspection to assess network traffic. Passive monitoring can determine which hosts are active on the network, when new hosts become active, which ports/services are active and inter-asset connections. Passive monitoring sensors must be placed in the network where they can “see” the network traffic to be monitored.

Active Scanning

Active scanning, unlike passive monitoring, generates network traffic and interacts with devices on the network. The advantage of active scanning is it provides more information about assets than passive monitoring does. This additional information may include open ports, installed software, security configuration settings, and known malware. Several active scanning variants are available, including unauthenticated scans, authenticated scans, and agent-based scanning.

Unauthenticated (Network) Scans

Unauthenticated scans also referred to as network scans, examine devices from the outside in by attempting to communicate with each of the IP addresses in a specified IP address range. Once a device is identified, the scanner attempts to get a response from each of the TCP ports to determine which ports/services are open. UDP ports may also be scanned. Unauthenticated scans can be run externally (from outside of the firewall) to see a network as an outside attacker would see it or behind the firewall. If behind the firewall this gives access to all systems accessible on the selected network segment. Unfortunately, some of the OT devices may be too sensitive to withstand active scanning. They may be sensitive for a number of reasons such as limited CPU power, design tradeoffs, custom OS, and more. It is therefore highly recommended to test in a lab environment first to ensure compatibility with the OT devices it will encounter during scanning.

Authenticated Scans

Authenticated scans, also called credentialed scans, remotely log in to devices to examine them from the inside out. Because authenticated scans interrogate devices from the inside-out they can gather a wealth of security-related information about installed software, security configuration settings, and known vulnerabilities. Although authenticated scans do not require software to be installed on the target, they use memory, processing power, and network bandwidth and can therefore cause degradation and disruption. Authenticated scans are best suited to the IT systems in the upper layers of the OT environment. They are often used in conjunction with unauthenticated scans to deliver both inside-out and outside-in views.

Agent-Based Scans

As the name implies, agent-based scans are performed by software agents installed on the target devices. Similar to authenticated scans, agents see the device from the inside out and can provide detailed information. Agents are best suited to the IT systems connected to the SCADA control environment. The downside to agent scans is that the agents must be installed on a device and will consume memory, disk space, processing power, and network bandwidth that will no longer be available to the primary application.

Proactive Cyber Security Training of Human Assets

Employees of your organization is often the weakest link in your cyder security defenses as they have access to the production systems and if such access is unintentionally shared with cybercriminals e.g. the login information is captured through a phishing attack, any technical security defenses are powerless. Therefore protecting only your technical assets leaves you open to cyber-attacks targeted at the employees of the organization, your human assets. According to CISCO's 2021 Cybersecurity Threat Trends report, about 90% of data breaches occur due to phishing. Spear phishing is the most common type of phishing attack, comprising 65% of all phishing attacks.

It is, therefore, crucial to protect your organization's employees, the most vulnerable targets, against cyberattacks and should therefore be your highest priority. In other words, building your human firewall with personalized automated phishing and awareness training to limit the attack surface is a critical component of your security defense strategy.

Holm Security's OT Solution

Holm Security provides various products as part of our Next-Gen Vulnerability Management Platform that will be able to assist you in identifying and remediating vulnerabilities in your OT security defenses.

System & Network Scanning

Holm Security's System & Network Scanning product provides you with all the features you need to discover, assess, prioritize and remediate vulnerabilities through automatic and continuous scanning of your OT environment. Given the size and complexity of your growing converged IT and OT environments not only do we help you discover all of your technical assets but we also help you understand what vulnerabilities to remediate first through ransomware and exploits threat intelligence.

Device Agent

As part of the System & Network Scanning product, Holm Security offers a lightweight endpoint agent called Device Agent (DA). The agent helps you improve coverage and accuracy - not least when it comes to your remote workforce. As the boundaries of the traditional workplace, expand and organizations work remotely and still need to manage the OT environment via the Supervisory Control and Data Acquisition (SCADA) control system while on the go and the DA from Holm Security will ensure that such on the go devices are covered.

Phishing & Awareness Training

Build up your human firewall by training your employees to recognize targeted phishing attempts in a safe and controlled environment with Phishing & Awareness Training from Holm Security. The phishing campaign results give detailed statistics that help identify user weaknesses and allow you to measure overall risk levels across entire user groups. You can follow how your user resilience develops over time with user our human risk scoring system.

Conclusion

Market opportunities and competitive pressures are driving oil and gas suppliers, utilities, and manufacturers to adopt initiatives to reduce cost, drive innovation and improve sustainability. The expanding attack surface resulting from these digital transformation initiatives that span IT and OT creates a cyber risk that must be measured and managed. Passive monitoring identifies and assesses vulnerabilities in both IT and OT assets if they are active on the network and will not disrupt the operation of sensitive OT devices. Active scanning identifies and thoroughly assesses IT assets and applications, including workstations, network devices, databases, virtual infrastructure, and the cloud. Combining passive monitoring and active scanning, as well as phishing and awareness training, provides a holistic view of security risks across converged IT and OT organizational environments.

Why Holm Security?

Leading Attack Vector Coverage

The broadest coverage of attack vectors in the industry which includes both technical and human attack vectors.

More Than Just Another Vendor

Your most important partner within cyber security heping you stay one step ahead of cybercriminals.

Data Privacy

Any vulnerability data we collect is stored and encrypted in data-neutral locations so you can be assured that only you will have access to your data.

How can we help?

Want to get in touch? We'd love you hear from you. Here's how you can reach us.

☎ +46 8-550 05 581

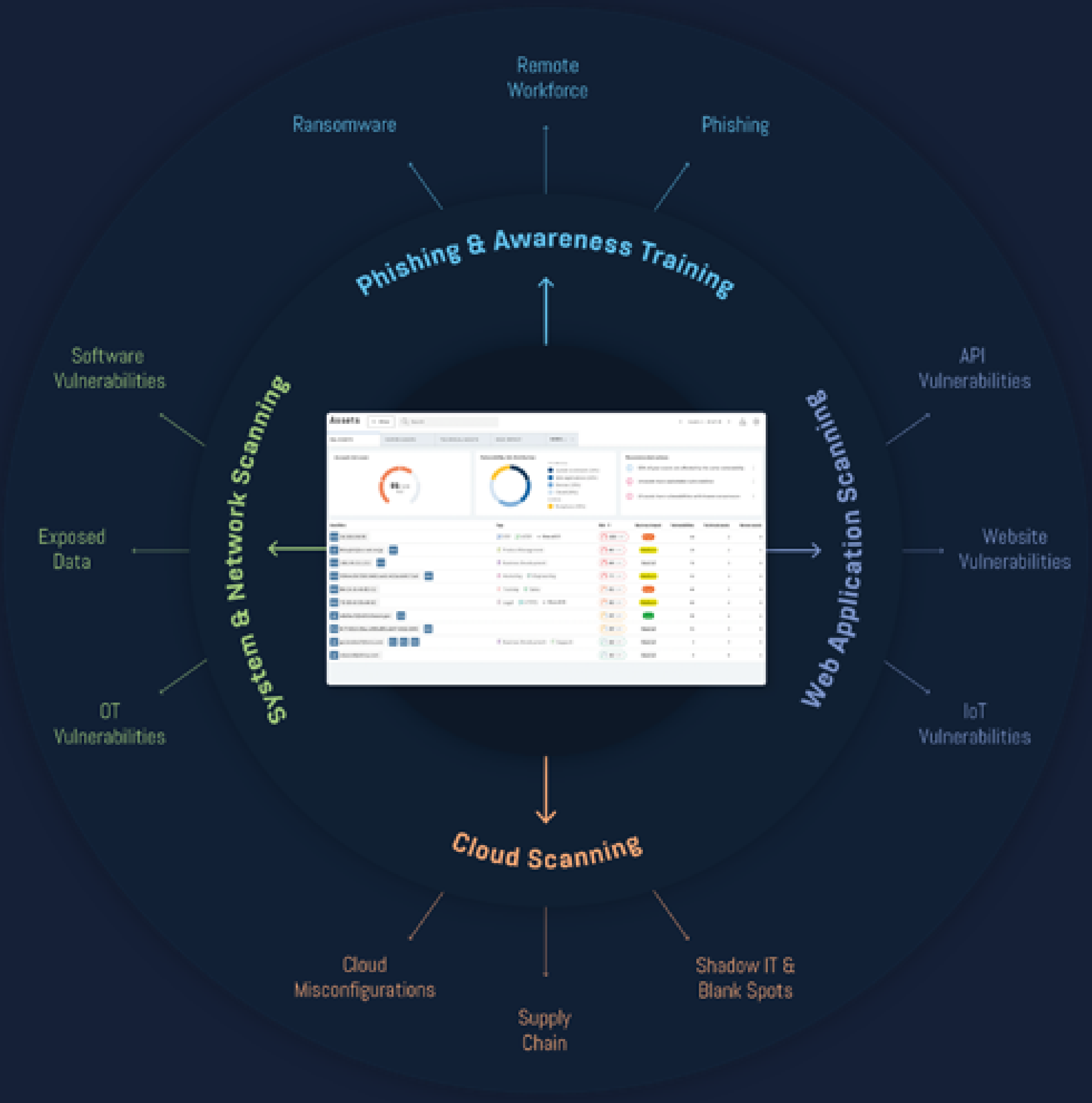
✉ info@holmsecurity.com

www.holmsecurity.com

HOLM SECURITY

One Platform - One View

We collect information from all of your risk sources and present them back to you in a unified view, prioritizing critical vulnerabilities as decided by risk algorithms. View your risk from vulnerabilities from the organizational level right down to a singular laptop port.



HOLM SECURITY