The benefits of Security Configuration Management for OT environments

Author: Ben Jackman, CISSP - Tripwire

We all know it

OT organizations are struggling with legacy devices and a flood of vulnerabilities to ICS components. What's more, many industrial networks and servers were configured years ago - probably by someone with a degree in Chemical or Industrial Engineering degree - and most likely with out-of-the-box settings.

On one hand, we recognize that both scanning and patching vulnerabilities is not so simple in OT. But on the other hand, the OT security market continues to promote fear, uncertainty, and doubt - better known to marketers as FUD*: the attackers are already on your network, you need sophisticated threat intelligence feeds, and you better have the ghostbusters on speed dial for IR.* The security market continues to teeter back and forth between the spectrum of promoting prevention versus detection and response.

The truth is

The attack surface of your OT environment is actually more dependent on the security posture of traditional IT devices running on your industrial networks. Traditional IT vulnerabilities and misconfigurations are much easier targets for hackers - and these are the means the attacker will laterally (or vertically) move through your IT-DMZ-OT network chain.

Put another way, if an attacker is in a position on your industrial network to exploit an ICS component's vulnerability, then it's already game-over; they have elevated privileges and access to your engineering workstations, control database, etc. It would be much simpler for them to cause mayhem by deleting or modifying your process control algorithms and HMI diagrams than to exploit some peculiar ICS vulnerability.

Unfortunately

The configurations on network devices, databases, directory servers, workstations, operating systems, and applications aren’t secure by default. In fact, default settings on new devices are often set with ease-of-installation in mind, not for robust security. Further configuration changes that leave systems vulnerable often occur inadvertently through what’s called “configuration drift.”

Misconfigurations create entry points for hackers. With thousands of ports, services and settings, tracking configurations on even a single server can be a big task. If you multiply those same ports, services and settings across your entire industrial environment of servers, hypervisors, routers, switches and firewalls, the problem becomes overwhelming.

Using change to our advantage

OT teams aren't staffed and trained to search for IT misconfigurations within OT environments. But we do have one thing working in our favor: *OT environments don't change as frequently as IT environments*. In fact, most OT teams live by the motto: *if it ain't broke, don't fix it*. Therefore, if you discover a security configuration change, then you'd better take a look.

SCM – yet another acronym?

Security Configuration Management is the cybersecurity process of ensuring systems are properly configured to meet security and compliance standards, reducing cyber risk in the process. The practice of detecting and remediating misconfigurations combines elements of integrity monitoring, configuration validation, vulnerability assessment, and system remediation.

Before new misconfigurations can be identified, a secure configuration baseline must be defined. Then, deviations from this baseline result in test failures in the assessment process, and security teams remediate back to the secure baseline. This is the basis of what SCM looks like in action.

Rather than assuming your current system is clean and monitoring from its current baseline – consider more formal hardening principles from trustworthy sources. As an example, the Center for Internet Security (CIS) has become a de-facto standard for hardening baselines.

Four pillars of strong SCM:

1. Device discovery
2. Establish your baselines
3. Manage changes
4. Remediate

File Integrity Monitoring (FIM) is the security process that monitors and detects changes in your environment to alert you to cybersecurity threats and helps you remediate them. FIM data is the engine that drives SCM success—you can't have one working optimally without the other. Whereas SCM focuses specifically on assessing whether the current configuration is consistent with a predefined policy or expected state, FIM detects changes to files and system attributes that deviate from their prior baseline, including changes to servers, network devices, databases, virtual images, and more.

An ounce of prevention

Every incident begins with a change. Knowing who, what, when, where, and how those changes are happening in your OT environment puts you in a proactive defensive posture to prevent incidents - not react to them. The moment your system becomes misconfigured, you should be notified and offered detailed remediation instructions in order to bring the misconfiguration back into alignment.

Footnote: Yes, this can be done without agents.