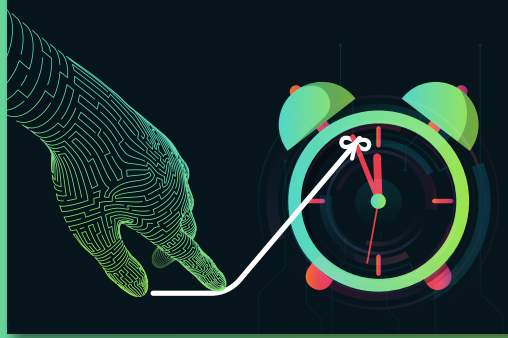
DRAGOS

10 TIPS FOR SUCCESSFUL OT VULNERABILITY MANAGEMENT

Building out a mature OT vulnerability management program can be a slow, methodical process that will take resources and wherewithal to get right. There is certainly no cookie-cutter path for an industrial organization to follow, but Dragos has put together some suggestions on getting started.

Here are 10 WAYS to tackle the challenges of OT vulnerability management.

01 DON'T RUSH IN



Doing OT vulnerability management right requires security and operations staff to slow down, think through risk implications so they can help leadership create the right mandates for resolving vulnerabilities, and create a repeatable system for making good decisions that truly lower overall risk to the business.

02 EVERYTHING STARTS WITH AN ASSET INVENTORY & VISIBILITY

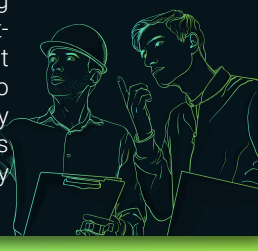
To get started properly, organizations need to undergo an asset discovery process that can not only dig up all those assets, but also classify them by a range of attributes, map their connections, and track their configuration state.

03 DON'T FEAR AUTOMATION

Prioritization of assets can be automated with the data provided by discovery and assessment. Similarly, vulnerability assessment and the process of tracking configuration baselines and instances of configuration drift provide opportunity for a lot of automation. Prioritization of assets can also be automated with the data provided by discovery and assessment. Don't discount the time saved by automatically patching non-critical OT systems.

04 PERIODIC WALK DOWNS ARE A MUST

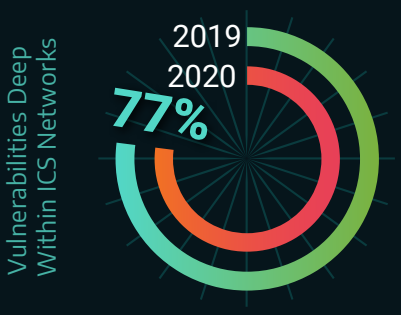
Start by mapping high-level architectures and performing comprehensive facility walk downs to start physically identifying hidden assets that will need to be accounted for. Walk downs are crucial throughout the vulnerability management process to validate what automated asset discovery is producing and to fill in the gaps across the environment that may not necessarily be covered by monitoring and telemetry.



05 DOCUMENTATION IS CRUCIAL

Documentation of processes brings discipline to bear to ensure that they're not done on an ad hoc basis. An organization should try to spin that documentation into compliant workflows that ensure that everything is standardized, repeatable, and provable.

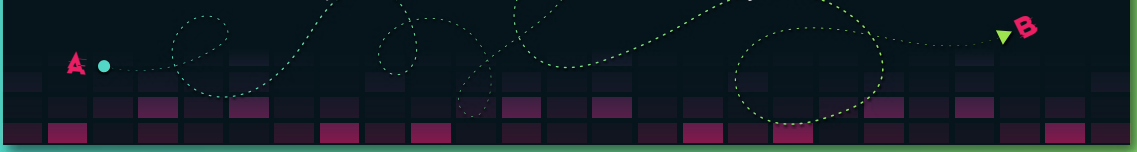
06 UNDERSTAND OT VULNERABILITY PRIORITIZATION IS DIFFERENT



OT vulnerability prioritization is very different than in IT, where the focus is primarily on severity scoring of the flaw and, ideally, business criticality of an asset. The added dimensions of operational risk and physical world ramifications changes how things are calculated. The industrial space has also exceeded a key threshold: in 2020 more than one high severity vulnerability in industrial products was disclosed for each working day of the calendar year.

07 MASTER THE ART OF COMPENSATING CONTROLS

In many OT systems, patching simply is not an option due to the operational risks involved with changing those assets. In fact, data gathered for the 2020 Dragos Year in Review found that among the OT vulnerabilities disclosed in 2020, more than one in five didn't even have a patch available when announced by vendors.



08 ACTIVELY MANAGE VENDOR RELATIONSHIPS

Organizations need to actively manage their vendor relationships to not only validate that the services are upgrading or mitigating systems as agreed, but also to document the status of vulnerabilities across all vendors and the entire asset inventory.

09 CHANGE MANAGEMENT

For many critical ICS assets, change management governance is extremely rigid due to compliance for safety management. An asset like a PLC, for instance, would always go through a formal change management process mandated by process safety management according to the requirements of different industries. If the asset is involved with an industrial process, the requirements will likely be much more rigorous.

10 HIRE DEDICATED STAFF

An effective OT vulnerability management program is an ongoing concern that requires dedicated resources to maintain. While many duties in discovery and assessment can be automated, there's a considerable amount of work necessary to coordinate with asset owners, update systems, employ compensating controls, validate, and track progress.

Contact Us at sales@dragos.com or request a demo at dragos.com/request-a-demo.

DRAGOS