OPSWAT | ISS Source

WHITE PAPER

Cybersecurity: Simplifying Complexity

See All Your OT Assets and
Understand How to Protect Them

Introduction

No one will deny the complexity behind cybersecurity. It comprises an ever-growing and always-changing web of nuances, standards, templates, formulas, devices, algorithms, technologies of all sorts, and humans working together to achieve a balance between ensuring systems are safe from intrusions while keeping the business up and running in a productive and profitable manner.

With all that complexity, one would assume only a very few people would be able to use the technology to understand what is going on at all times, but it doesn't have to be that way.

Today, there are plenty of choices when it comes to an asset management and visibility tools, but in an environment where workers often take on more than one role, one of the main goals is for the technology to have simplicity built in to ensure ease of use. Something where its operator has a sense of familiarity and has an HMI-style form factor where information is right there in front of you. The following will provide what to look for when assessing an asset management and visibility tool.

When there is a cyber incident—and sooner or later there will be—operators are the first line of defense. Having a tool that allows them to see if an attack is brewing is paramount, so they can escalate everything to the proper security professionals.

In addition, in this era of increased digitalization, communication levels need to increase from the Operational Technology (OT) space all the way up through the enterprise to the Information Technology (IT) environment where IT and OT teams are able to share data. They always have, and they will continue to share data when you need to get information from OT into IT, and where you need to get patches and updates from IT to OT. In those environments, getting the right amount of data with the proper context from OT into the hands of IT is important so they can understand whether a new asset has been plugged in, if we are communicating with an adversarial country, or if someone just updated firmware unexpectedly.

Expanding Risk Zone

While data sharing and purposeful, safe segmentation between IT and OT to enable business operations are beneficial, it also increases risks as OT environments are now exposed to cyberthreats of the IT world. To that end, conventional defenses are no longer sufficient to protect OT networks from sophisticated attacks.

Operators today now need to address risks to OT systems from traditional IT and specific ICS threats by gaining visibility into converged IT/OT operations that deliver situational awareness throughout the network. This way, it is possible to maximize visibility, security, and control across the entire operation—all while protecting critical assets effectively and staying compliant with regulatory requirements.

This can all happen with the use of advanced artificial intelligence (AI) technologies, knowledge of the attributes and requirements of OT environments, and deep understanding of OT usage preferences.

While there should be ease of use, that's not to say there isn't much complexity behind a tool that uses a neural networking approach, where machines learn like the human brain. When something happens, the machine begins to understand, processing the data to learn what is right. That knowledge can cut down on alarms created by models that aren't well tuned. Machine learning can fingerprint and identify what's on the network.

With machine learning, it is possible to cut down on the noise, getting the things that matter in front of the operator because the priority is uptime, safety, and production. This technology can ultimately help fill the skills gap left as OT workers age out as well as show the evolving threat landscape as attacks become more and more apparent.

February 2022

One of the largest tire manufacturers in the world, Bridgestone Americas, worked on recovery after suffering a ransomware attack by the LockBit ransomware gang.

Bridgestone investigated, "a potential information security incident" it detected. "Out of an abundance of caution, we disconnected many of our manufacturing and retreading facilities in Latin America and North America from our network to contain and prevent any potential impact," Bridgestone said.

The ransomware gang said at the time it would leak all data stolen from the company.

A Tool to Protect OT Networks in a More Converged Environment Should Include:

Full visibility into ICS assets and networks, employing smart and advanced discovery techniques for complete asset inventory without impact on OT networks and devices

The ability to visualize network topology and connectivity to provide a complete view of what is going on over the network in real-time

Predefined policies incorporating requirements in regulatory standards

AI algorithms for auto defining comprehensive security policies and proactively identifying a variety of threats and vulnerabilities

Continuous and real-time monitoring of asset and network connectivity with immediate alerts on any violation of security policies or anomalies

Purpose-built OT and IT views to help OT personnel and security professionals address cybersecurity issues with different views and preferences

Assessing Legacy Equipment

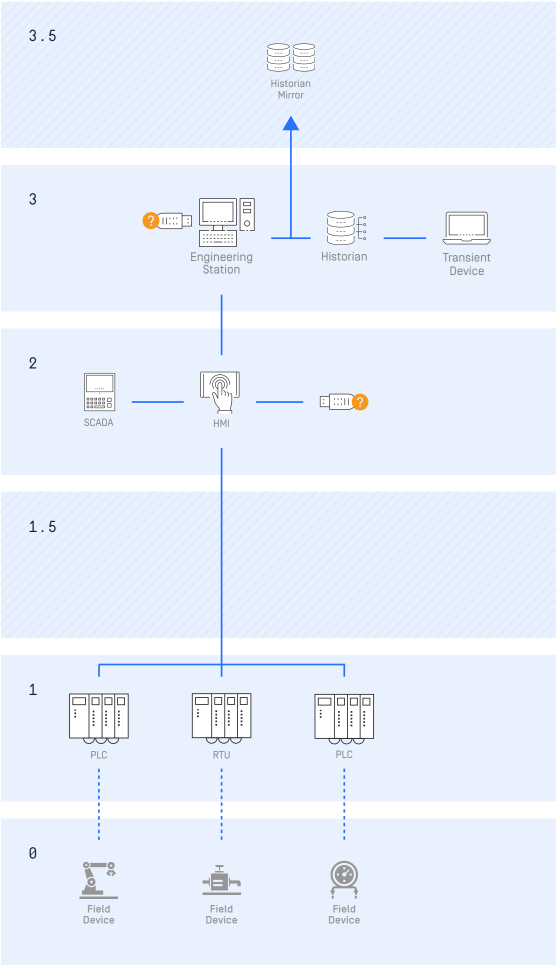
It may be a cliché, but it is also true that you can't control what you don't see, and the OT environment quite often consists of decades-old devices from a variety of vendors. This makes the ability to have full visibility into assets and a thorough understanding of what is happening on the network key to any effective OT cybersecurity program.

This means an operator needs visibility down at the plant or on an individual product line level. However, OT is so dispersed and isolated that you really need to have that visibility tool down at levels one, two, three, and 3.5 zone of the Purdue Model, passing what you find along to the enterprise. The tool needs to be tailored and specialized for that 3.5 zone down to level one or possibly even level zero, if there are devices IP-enabled.

At level zero, you really are looking at controlling the physical process, currents, and temperatures, which are all very sensitive. That is why it is important to have a tool that understands industrial protocols so you are not doing full network scans, sweeps, or running an Nmap or something intrusive.

From a passive monitoring standpoint, everything appears limited to where the communication is and where it flows. However, if you add in active monitoring (provided you have active routing to the environment) it is possible to safely add discovery packets to find anomalies.

With all the monitoring in the manufacturing zones it is possible to integrate with security information and event management (SIEM) systems and other enterprise level visibility tools, but in the end, the OT operators need basic contextual awareness and a heads-up view that allows them to pass events along to the security team.



Purdue Model

Helping Responders Act

A tool focused on visibility when there is an incident makes it possible to look at the historical and/or current data to determine how to respond. At present these tools don't have any response built in, but with them it can arm incident responders with the right data they need with the proper context.

With some upfront information such as policies and procedures added in by the asset owner, it is possible for the visibility tool, through its machine learning capability and built-in templates, to align to common cybersecurity frameworks like NERC CIP and NIST. This makes it possible to start up very quickly and begin learning the environment. It is also possible for the asset owner to further tailor the machine-generated baseline or the templates.

In terms of ready-made components, the tool should also help when it comes to complying with standards and regulations. A tool should support global, regional, and industry regulatory requirements for OT cybersecurity such as NERC CIP, NIST, NIS Directive, NEI 8-09, and IEC 62443 with purpose-built policies and reporting for compliance standards to help organizations assess and improve their cybersecurity status and meet regulatory requirements.

When you do have an audit, there is push button reporting to show an asset list or generate communication flows that prove a specific zone is segmented from another, and that you're only communicating on one approved protocol. It's about empowering the security or compliance program with repeatable data as opposed to running around with spreadsheets or doing a one-time analysis, whether that be from a professional services-style assessment or your own internal walk down.

In terms of savings to the asset owner, if an operator must do a walk down of a manufacturing line and manually record every make, model, firmware, and connection, that could take a week if you include the time needed to write the report. A proper, well-tuned tool can easily save you days of work.

May 2022

Smartphone manufacturing giant Foxconn suffered a LockBit ransomware attack that disrupted operations at one of its Mexico-based production facilities, according to officials.

This is the second attack the company has suffered in as many years. The affected plant specializes in the production of medical devices, consumer electronics, and industrial operations.

View Changes in Real-Time

Speaking of productivity and time saved, something else to consider is that you don't have to wait for your next assessment to understand all your changes; you can understand the changes made in real time.

Another advantage is having a separate screen to help operators and security personnel focus on what is happening on the network. While an operator oftentimes has more than one screen running at a time, having a separate screen can be an advantage. Simply put, if you don't have a dedicated screen front and center, it leaves it up to chance for how often they're going to check on the tool and see what it's telling them.

The tool should be indicating what an operating device's make, model, firmware, and serial number is, but it shouldn't stop there. You can also find out if there is a chassis built-in or if there are additional logic cards, to name a couple of things. Once that is established, it is then possible to pivot to the non-inventory items: What connections is it making? What ports are open? How does it communicate? Is it using insecure protocols?

Machine learning helps when it comes to learning the system, but an area where a strong visibility tool needs to help is when malware has already been planted on a system.

May 2022

Smartphone manufacturing giant Foxconn suffered a LockBit ransomware attack that disrupted operations at one of its Mexico-based production facilities, according to officials.

This is the second attack the company has suffered in as many years. The affected plant specializes in the production of medical devices, consumer electronics, and industrial operations.

Policy Statement

If malware is already in the environment and the tool is already absorbing its actions, it has just learned bad behavior. To combat this, some of the policy-based initiatives kick in. If there is a policy where a PLC is never supposed to talk to another PLC, that is something the tool will pick up saying, “hey, why is this PLC jumping to another PLC? I had all my traffic set up for only the historian to do reads. Why is the historian doing writes?” Now, that might be normal behavior with all the machine learning, but you’ll have a policy violation on why this endpoint is doing something not in the normal policy. This way, there is a system of checks and balances between the machines, where humans can define good policies and catch anomalies.

Having the tool act behind-the-scenes allows it to be simple to operate in the case of an attack.

What to Look for in a Visibility Tool

Make sure it understands the protocols and vendors in your environment.

You want to make sure if you're using Rockwell, ABB, etc., the tool can provide visibility into those vendors and protocols. Visibility is only as good as your dictionary.

Active and passive monitoring.

Passive monitoring is great, but it relies on the environment's ability to communicate or get the traffic over to the spanner or tap port. A lot of these environments were built a long time ago, before spanning and tapping. Mirroring was a feature within the network switch, and it's not always easy to retrofit that sort of information or architecture into your environment. The best part about active monitoring is that as long as you have a routed connection between where you want to put your networking sensor, networking appliances, and the devices you want to monitor, it cuts through the need to re-architect and rethink how the communication flows go.

Make sure it's simple and easy to use.

A lot of solutions aren't providing a more IT-centric than OT-centric function. Ease of use is the big thing. Make sure it is designed for OT.

Look for a solution and a company you can grow with.

There are plenty of point solutions and vendors out there in the visibility space, but they stop at visibility and don't bring you much further along in your security maturity curve. Look at a vendor and put yourself on a path where you can grow and mature in your security journey.

For instance, during a possible attack a prompt will appear on-screen saying there is a possible supply chain violation along with an image of the associated device. Maybe someone's plugged in something that has been weaponized; something doesn't look right. Is this something you want to alert on or is this normal behavior? This visualization is presented as opposed to putting a lengthy set of log lines on the operator's display, leading them to look at dials and charts potentially missing a threat that is otherwise obvious.

In essence, the operator is looking at a familiar HMI-style user interface and gets a clear red flag on-screen prompting them to stop and look at what is happening.

Whether there is one issue occurring or multiple, the device should additionally be able to establish context for the type of attack arising.

If a PLC is under attack, it becomes easy to trace what it has recently interacted with, that it has talked to these countries, that it has these open vulnerabilities, and it looks like someone is trying to exercise them based on the communication flow and ports that are open.

In terms of context, each asset gets a risk score that is low, medium, or high. For example, if there is an issue with a historian, you learn it is not critical to the operation because if it goes down, you can keep all other processes going. How about an HMI or a core switch? Since an abnormality or vulnerability detection there could cause significant downtime, they receive a much higher criticality level, ranking them much higher.

Protecting Against Ransomware, Supply Chain, and Zero-Days

The device should also be able to help in the asset owner's defense against supply chain attacks, ransomware, and zero-days.

For a supply chain attack, the tool could be set up to detect country and device manufacturer of origin with rules that flag when someone plugs something in that appears as though it's not genuine or doesn't match the typical identity information of different controllers. The tool could also look at make and model of firmware going across the wire.

In terms of ransomware, if a contractor shows up with tainted removable media or software, the tool is going to notify you your device is now communicating in a much different pattern than what is normal. It's attempting to phone home; it wants to communicate with that ransomware server to give the attacker visibility into your environment. This is an excellent stopping point to show the device in question is talking to a different part of the world or in an unexpected way. It is understanding the device's communication path.

Traditionally in an OT environment, there is consistency in processes. When something appears or acts even a little bit differently, there could be cause for concern. The tool should pick up on that and alert its operator.

In a normal scenario, the PLC would talk to the HMI ten times a day. But suddenly, one of those parameters has changed. Did someone make a network change? Was it a zero-day? Are we having an outage? Are we being attacked? It appears as if something is abnormal. It may be a zero-day, or it could simply be an operator who made a mistake and changed a parameter. It could be the safety system firing off because they had an event.

January 2022

A British snack food provider, Kenyon Produce (KP) Snacks, suffered an attack by the Conti ransomware group, which affected product distribution to supermarkets.

The German-owned company said it became aware of the attack on January 28, 2022, and it immediately took steps to contain the attack. A letter from KP Snacks sent to store owners February 2, 2022, said its systems had been, "compromised by ransomware," and they, "cannot safely process orders or dispatch goods."

All those scenarios can play out right in front of the operator or the security professional in real time with the right tool employed.

Yes, there's no denying the complexity of cybersecurity continues to grow, but having the right tool to see what is happening across your OT environment can ease the strain of that growing complexity and ensure the network stays up and running and the asset owner remains secure, productive, and profitable.

About the Author

Peter Lund is Vice President of Products—OT Security at OPSWAT. He is responsible for overseeing and managing OPSWAT's OT and Industrial Cybersecurity business unit. Prior to OPSWAT, Peter brought new features to the market for Industrial Defender serving as the head of product management and CTO and held roles at Dell (EMC), Schneider Electric and KVH Industries. Peter studied Electrical and Computer Systems Engineering at Rensselaer Polytechnic Institute.

OPSWAT.

Protecting the World's Critical Infrastructure