tenable.ot™
Powered by Indegy

PREDICTION OF AN OT ATTACK

WHITE PAPER

Redefining the OT Security Paradigm

For the last 30 years, we have witnessed slow-but-steady changes to how operational technology (OT) work. With quantum advancements and technology intersection points in manufacturing and critical infrastructure environments, we can be more effective and efficient; while also achieving exacting required standards.

Concurrently, and particularly during the last decade, OT environments increasingly face a new challenge of maintaining secured environments. Much as we've seen in IT, OT is increasingly in the crosshairs of security incidents that can impact or fully disable operations.

Arguably however, the impact of a security incident on OT can have longer and more dire consequences when it involves shutting off processes such as water treatment, electricity, air transportation, or manufacturing of cars, medical devices or food items.

Historically, security grew up in an age of "cat and mouse" where the hacker "villain" and security "hero" are in a constant game of one upsmanship. The unique goal of both is to outsmart the other, thus creating a game of leapfrog between the attack and existing security designed to protect the target. Invariably, there are organizations and individuals that get caught in the security pinch and become the next victims.

This white paper examines current standard security practices and how we're beginning to change our response and embrace a new method to protect our OT environments—a move predicated on early detection and prevention before damage occurs.

Breaching the Device

Threat actors predicate most attacks by targeting a particular device such as a server, switch, PLC, etc. Finding a weak device in a network is reconnaissance's key goal for example, an unguarded device, a device that uses a default password or an exploitation based on an unpatched vulnerability.

Hackers need time to find a weak point in massive, often distributed infrastructures. Once attackers accomplish that, they make entry, map your network and deliver the attack, all without detection. It is not uncommon that reconnaissance can take weeks—or months—and may take more time than the actual attack itself.

Conversely, security personnel within your organization are responsible for making sure they harden devices through a robust system to identify targeted devices. For example, audit access management, passwords updates and/or addressing vulnerabilities . If and when an attack occurs, alarms should go off early before damage happens and a full arsenal of security measures should kick in to repel the attack.

Proliferating the Attack

Once a hacker gains a foothold through a compromised device, an attack can proliferate to other infrastructure areas. Attackers accomplish this by leveraging the thing that connects different devices—namely your network. Hackers don't just rely on a network to perform reconnaissance, but also to extend an attack and find additional devices they can defeat or use to get to other, previously secured parts of your environment. Such was the case in many recent attacks including LockerGoga, where an attack started in IT infrastructure and laterally proliferated to OT, or may have progressed in the opposite direction.

Security personnel, whether responsible for IT or OT, deploy "early warning beacons" to ensure successful attack proliferation detection. Typical security includes detection methods based on:

Policy

- Allow and deny rules sets. Think of these as laws with constant updates as researchers identify new threats when they hit the wild.

Anomaly

- Flag abnormal behaviors for the environment. IDS-type security measures, once fine-tuned, can detect potential attacks for which no policy is yet released, as is the case of a zero-day or targeted attack.

Signature

- An open-source database (ie: SNORT & Suricata) where the security community contributes as they discover new attack signatures. The notion here is: the more eyes on a threat, the more likely the community will identify attacks earlier. This in turn, allows the greater security community to protect themselves with everyone contributing to an attack database.

OT in the Crosshairs

While OT environments have been around for more than 50 years, the last decade has seen a marked increase in targeted attacks. This is due to the increase of new attack surfaces and vectors as new technologies are introduced to the OT environment such as IT/OT convergence and rapid adoption of IIoT. There have been documented attack cases that impact nearly every manufacturing vertical and critical infrastructure environment imaginable. There is evidence that other rogue factions have gained "red button" functionality; essentially owning the environment and waiting to launch an attack at will.

The reason for the increase in OT environment targeting is simply because they exist and are vulnerable. Whereas in the past, OT environments were largely sequestered and unreachable due to air-gapping. Today, this security measure is largely ineffective.

Organizations wanting to be more efficient and cost-conscious buy into IT-OT convergence, while others deploy Industry 4.0 or IoT technology. These two initiatives yield massive benefits, but also open up new attack vectors and surfaces not previously there, which puts unprepared organizations at significant risk.

Attack Vectoring

Decades of experience in IT security yields important lessons we can apply to OT. For example, we know that simple network tapping and "listening" does not catch all attacks. Driving deeper to the device level, the target of most attacks, is a key method of early detection before an attack starts to propagate and find new targets to conquer. This is particularly relevant in OT environments where up to 30% of OT assets are dormant; meaning, they never communicate over your network. In these situations, network or passive-only detection would never catch a dormant infected device.

A newer form of security takes both your network and both IT & OT devices —together—into account.
This is attack vectoring.

By identifying high-risk pathways an attack may take if introduced into your OT environment, attack vectoring redefines how you can address attacks by identifying the high risk pathways an attack may take if it were introduced to the OT environment. Running simulations can best determine weak points and where you need security interventions before an attack launches.

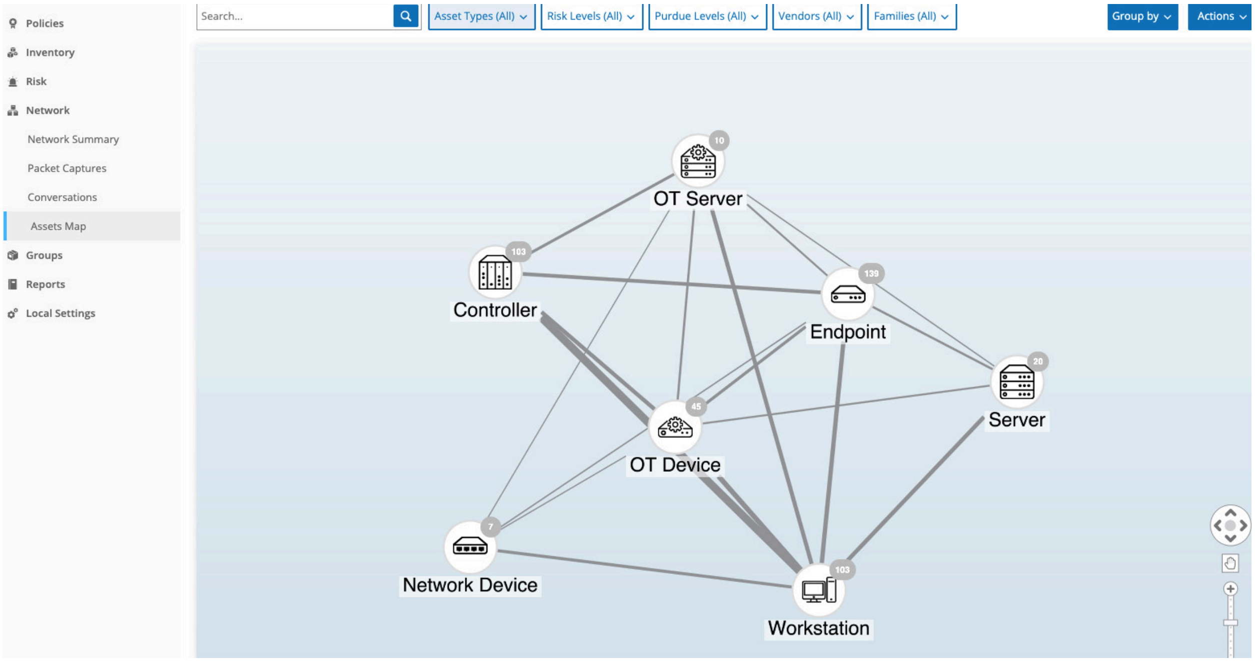


Fig 1: Tenable.ot groups assets by type along with communication links between asset groups.

As we see in Figure 1,Tenable.ot identifies and maps each asset by device type. Clicking into each device provides deep situational awareness into the device, including make, model, firmware version, vulnerabilities, device/software integrity, backplane details and much more.

Three Key Attack Vectoring Capabilities

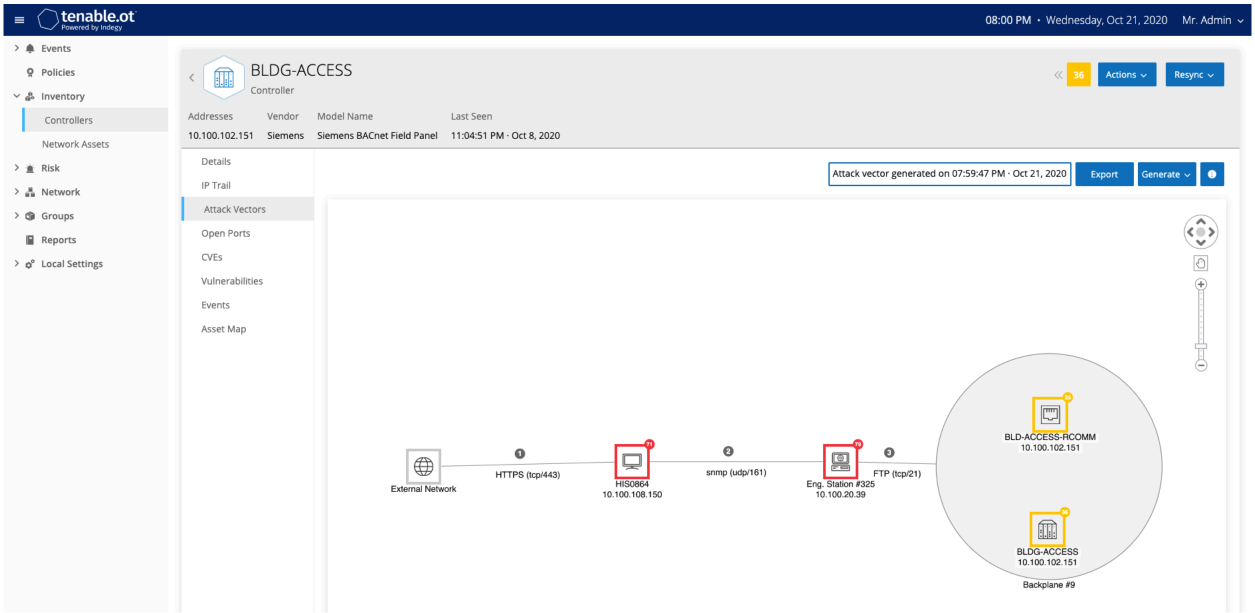
Visiblity into both IT and OT Devices

Deep situational awareness into device state and risk

Identification and prioritization of vulnerabilities and risk

We can also see communication paths between devices in the network, which can include IT, OT and IoT devices. Tenable.ot analyzes each pathway and device as well as likely vectors an attack would take if one introduced into your environment. We can further identify which assets are reachable by whom and from where, and then potentially close paths or limit unneeded access, thereby further reducing exposure.

Attack vectors group devices that share a backplane such as PLCs. Different devices that share a backplane (PLC, comm. adapters, I/O cards) calculate and impact risk. Mapping pathways illustrates instances where reducing or eliminating risk closer to the demarcation point may reduce risk further down the line and deeper into your network.



08:00 PM · Wednesday, Oct 21, 2020 Mr. Admin

BLDG-ACCESS
Controller

Addresses	Vendor	Model Name	Last Seen
10.100.102.151	Siemens	Siemens BACnet Field Panel	11:04:51 PM · Oct 8, 2020

Attack vector generated on 07:59:47 PM · Oct 21, 2020

Figure 2: Attack vectoring can zero-in on specific areas of your environment that require specific attention.

Sorting capabilities can zero-in on particular devices, sectors or locations in your OT environment that require special attention or interventions.

You can—and should—run attack vectoring regularly on critical assets to identify weak points and changes to the ever-changing risk profile unique to each individual environment.

Redefining the Security Paradigm

As noted, the cat-and-mouse game between hackers and security personnel dates back to the earliest security incidents. Security builds a mousetrap that holds until a hacker finds a way around the mousetrap. Security builds a new mousetrap and the vicious cycle continues. The unfortunate result of this paradigm is: someone must first suffer breach consequences before improved security product development and adoption.

The reality is that there is always an organization that suffers a breach and becomes a real-life test case. With this in mind, the security community is shifting the operating paradigm away from intrusion detection to prevention—or simply thwarting an attack before it starts.

Predicting a Weakness, Leads to OT Strength

OT environments touch every sector of modern society and we can't live without it. New advances in technology and business practices present innovative ways to leverage OT more efficiently and effectively with substantial cost-savings,—but is not without risk. Security incidents targeting OT environments are just the beginning. Without appropriate, built-in OT security, these systems, which society depends on, are in clear and present risk.

OT security is undergoing a palpable paradigm shift. Air-gapping is no longer a reliable means of security. In many instances, IT/OT convergence and adoption of IoT technology completely eliminated the air-gap. We know from IT lessons-learned that waiting for a successful attack to get through before implementing new security methods can directly impact your organization's long-term security and viability.

Security-at-large is rapidly embracing a more proactive approach to securing OT environments, including a more proactive approach to identifying and stopping attacks before they occur.

Gaining deep situational awareness about each and every device in your environment, identifying communication paths, access information and more, can help highlight weak spots and potential embarkation points for new attacks. It further empowers the security community to reduce risk and cyber exposure. This will strengthen and reinforce organizations running OT systems and strengthen their cyber security profile, rather than dealing with an incident after the fact.

About Tenable

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

tenable.ot™
Powered by Indegy