tenable.ot
operational technology

SOLUTION OVERVIEW

ARE SILOS BETWEEN TEAMS CAUSING SECURITY BLIND SPOTS?

Digital Transformation has helped organizations make significant shifts in adopting new technologies to increase efficiency. But it is not without risk.

Industry 4.0 initiatives have brought operational technology (OT) online, thus embedding the world of OT with IT. While this is beneficial, it has also expanded the cyber attack surface and can cause critical security blindspots if your teams aren't aligned.

Though some organizations intentionally connect IT and OT environments, others experience **accidental convergence**, or unintentional points of connection between IT and OT, in environments intended to be "air-gapped," or physically separated. In both scenarios, maintaining security posture across converged environments is crucial to reduce unnecessary cyber risk.

Today, air-gapping is **virtually impossible to upkeep and risky to rely on**. Routine activities like plugging in an external laptop or USB drive could allow attackers access to operational environments. Relying solely on air-gapping without proper security measures in OT environments leaves the door wide open for vulnerabilities to be exploited. Without visibility into those segmented networks, it's likely you wouldn't find out about an attack until it is too late.

Whether an organization is aware of their IT/OT convergence or not, security teams can't protect what they can't see. A blind spot to a security team is an open opportunity for an attacker. In connected environments, an attack can come from all sides, making it critical for traditional IT and OT teams to work together.

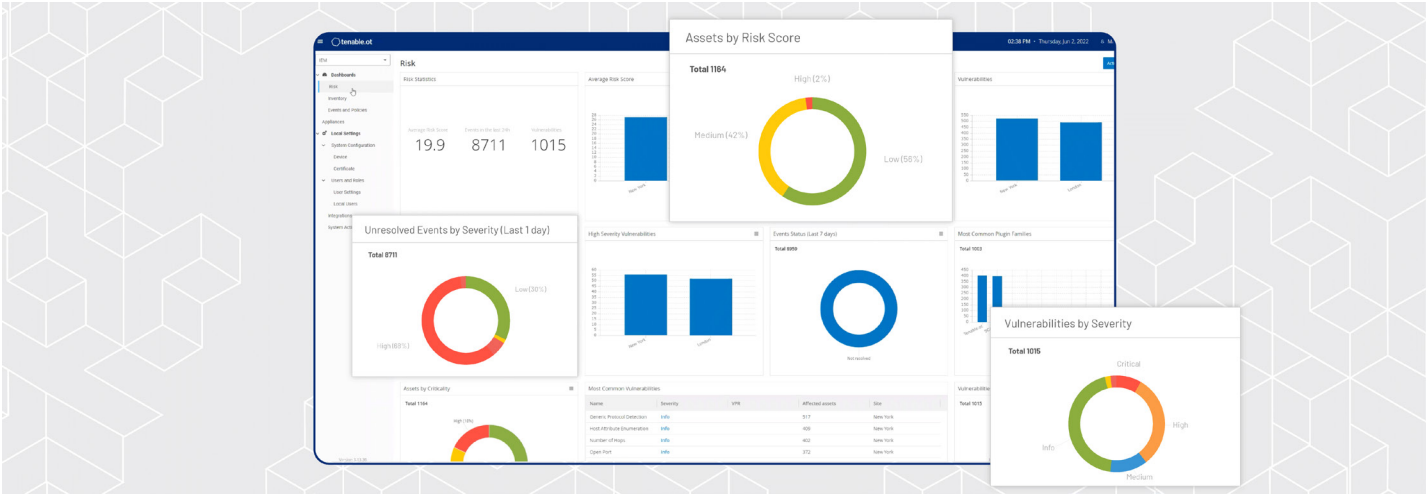
With increased threats against OT infrastructure, effective security means breaking down silos between IT and OT teams. Organizations must start with **unified visibility across their connected environments** and work together to secure their infrastructure holistically.

However, finding the common ground to align the two disciplines can be a challenge. Here are a few best practices to align your IT and OT teams.

#1: COMMUNICATE IN A COMMON LANGUAGE

The priorities between IT and OT teams can vary significantly, as do their day-to-day tasks. However, these differences in approach and priority can actually be an asset when it comes to security. The more eyes you have on security the better the outcome, so aggregating data from all sites in a common language will keep your teams focused on the most mission-critical tasks.

Consolidated global dashboard reports provide actionable insights and a single source of truth for security teams to work from.

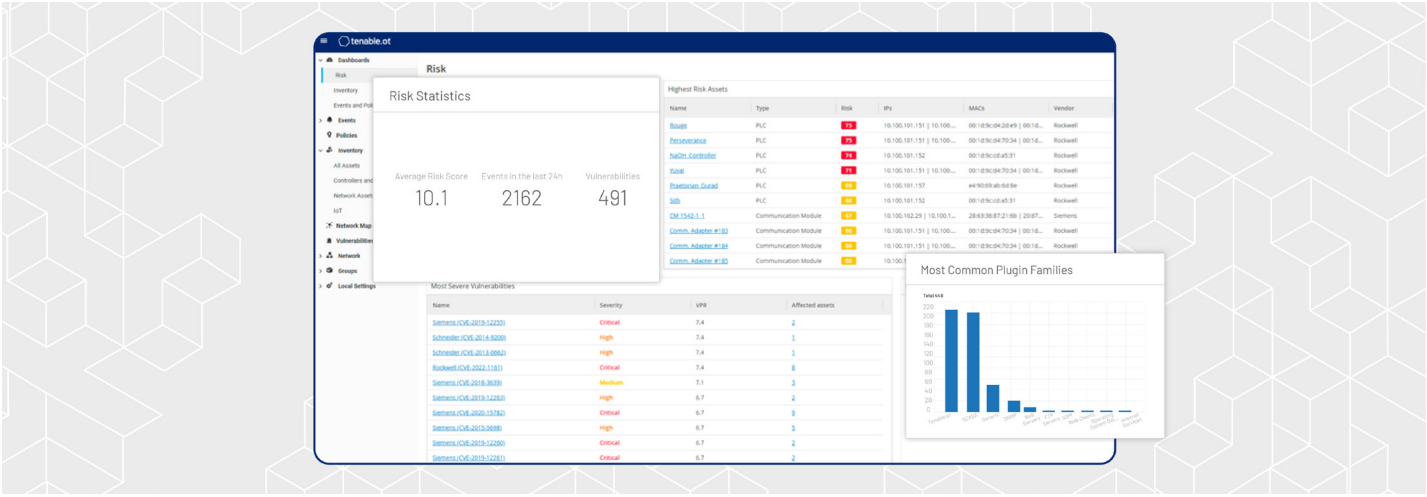


#2: PRIORITIZE THE VULNERABILITIES THAT MATTER

In 2021, over **28,000 new vulnerabilities** were disclosed, affecting OT devices as well as traditional IT assets. However, less than a quarter of these vulnerabilities actually had an available exploit. Most security professionals are already stretched thin and can't spend precious time on anything less than the most critical tasks.

Gaining full awareness of the vulnerabilities that are relevant to your environment allows you to prioritize the threats with the highest risk score during maintenance windows.

This gives your team more time to focus on fixing these vulnerabilities and work proactively to disrupt attack paths that malicious actors can leverage.

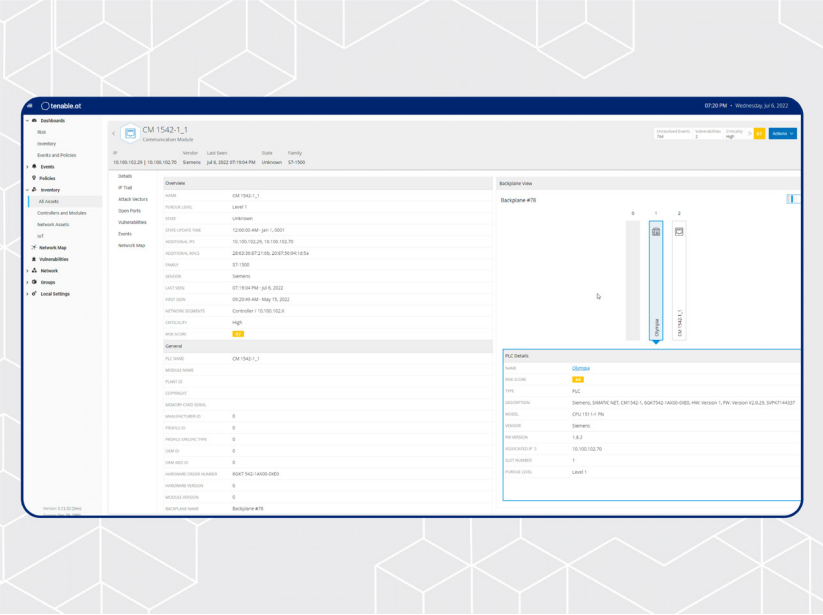


#3: ALIGN ON A LAST KNOWN GOOD STATE

Can you tell when changes are made and who made those changes? How about the last time your system was in good standing with its policies?

With configuration control your teams can work together to align in points of convergence and make sure no authorized changes were made. Compare snapshots from your last known good system state and compare with your current system to stop any unauthorized changes from doing damage to your system.

OT security solutions that work in conjunction with IT security solutions can be the catalyst that give your organization complete visibility, security and control that it needs to comply with evolving government regulations.



Today's security teams need to embrace a proactive approach to securing modern, converged environments to reduce risk factors of both planned and accidental IT/OT convergence. Understanding points of convergence, ensuring robust visibility and maintaining strong situational analysis across IT/OT will have substantial, positive impacts on security posture. These measures allow critical infrastructure and industrial organizations to fulfill mission-critical operations efficiently and securely.

For More Information: Please visit **tenable.com**
Contact Us: Please email us at **sales@tenable.com** or visit **tenable.com/contact**

About Tenable

Tenable® is the Cyber Exposure company. Approximately 40,000 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 approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at **tenable.com**.