SOLUTION OVERVIEW

Tenable for Palo Alto Networks

Business Challenge

Industrial control systems (ICS) and ICS networks lack visibility and security controls.

Because of the rise of external and internal threats that target operational technology (OT) infrastructure, you need an approach that provides real-time visibility and security while addressing the unique technical and operational requirements for these networks.

Separating OT alerts from existing IT procedures and policies creates additional challenges for remediation and implementation of improved security protection rules.

Solution

Palo Alto Networks and Tenable have partnered to provide customers with a seamless offering to increase visibility into ICS and critical infrastructure, as well as protect them from cyber threats.

Tenable.ot's advanced, ICS-specific asset discovery and tracking capabilities integrate with Palo Alto Networks next-generation firewalls (NGFWs) via dynamic address group (DAG) technology. DAGs dynamically populate with assets based on tags, which allows Tenable.ot to provide continuous updates on the assets it identifies in your ICS network. It helps firewall administrators improve your overall cybersecurity posture.

Tenable provides detailed information on each discovered asset, such as IP address, device type, vendor and model, and delivers it to your security operating platform. Taking this into consideration, administrators can take advantage of this integration to extend policies across your IT and OT environments.

Technology Components

- Tenable.ot
- Palo Alto Networks NGFW

The Challenge

- Lack of a comprehensive view across your entire industrial infrastructure
- Inability to detect and mitigate threats impacting your IT and OT environments
- Inability to get alarm information to the right person and provide actionable information based on alarm specifics
- No automated OT asset discovery and inventory management

Key Benefits

- Single pane of glass view
- Get an in-depth view of external and internal threats targeting OT environments that can be addressed via firewall rules
- Address security and regulatory compliance and change management requirements
- Take advantage of automated asset discovery, classification and tracking to facilitate better firewall management
- Full inventory of all deployed industrial assets including state and configuration that enables change control tracking within your IT framework

Key Components

Secure Access to Critical ICS Assets

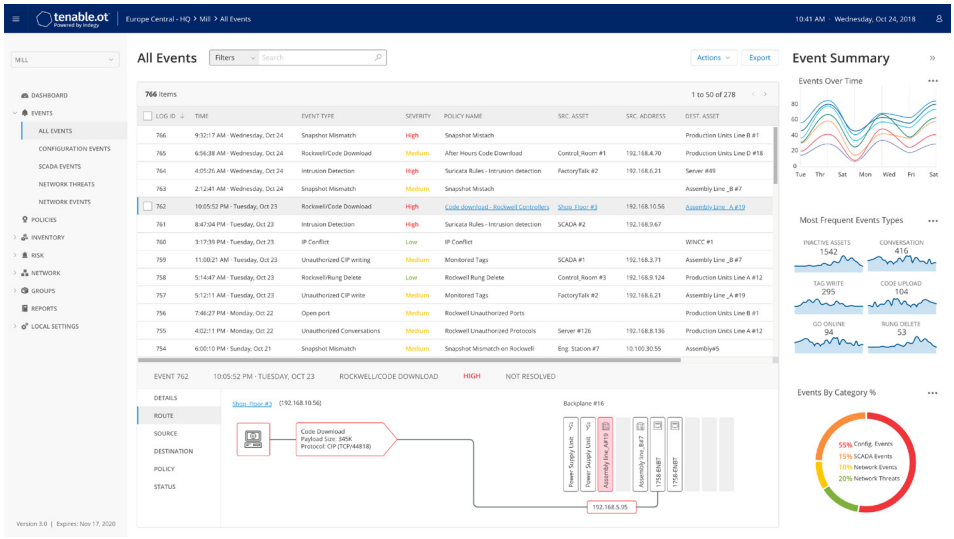
Challenge

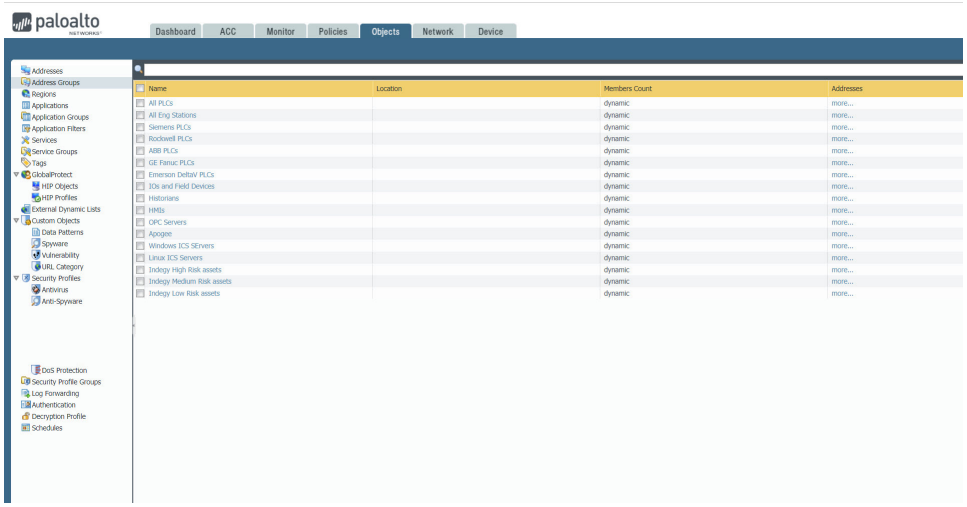
Maintain strict security policies, while still allowing critical operational maintenance activities that require network connections to sensitive devices. NGFW administrators face the challenge of effectively managing access and approving or revoking it on short notice, without having detailed asset inventories or clear visibility into ICS networks.

Solution

With the integration of Tenable.ot and Palo Alto Network NGFW, your administrators can now easily make changes to policies and gain complete access control over ICS networks using DAG.

Administrators can configure policies that apply to your specific ICS assets, taking their various characteristics into consideration. For example, when access to your ICS network requires only updating engineering stations, your NGFW administrator can set a policy that applies only to these devices without relying on manual mapping based on IP addresses that can change over time.





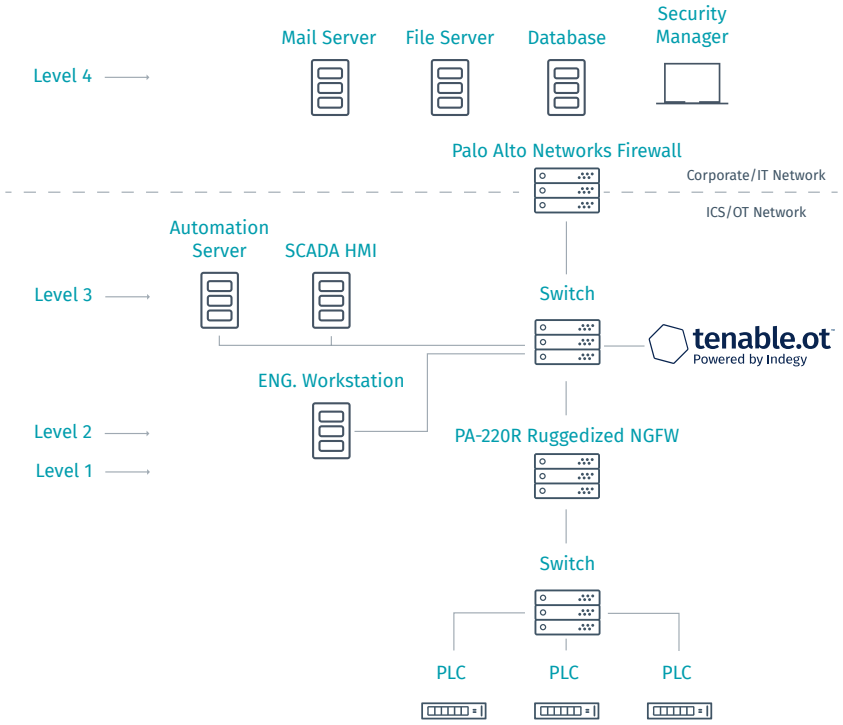
ABOUT TENABLE

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**.

ABOUT PALO ALTO NETWORKS

Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of changemakers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and mobile devices.

Learn more at
paloaltonetworks.com



Safeguarding Network Connections Between ICS and IT Environments

Challenge

Facilitate secured network connections between assets in your ICS network and IT applications that reside on your corporate network. Firewall administrators are currently forced to set permanent firewall rules that are too permissive and can't automatically adapt when changes occur. This increases security risks by expanding your potential attack surface.

Solution

With the integration of Tenable.ot and Palo Alto Networks NGFWs, administrators use DAGs to configure rules addressing individual ICS assets and groups ICS assets by their type or vendor. You don't need for prior knowledge of the network or address specifics. For example, your administrator can set a rule to allow only necessary communications to facilitate data-gathering by a manufacturing efficiency system to other devices in your OT network.

More Information

For support please contact: **support@tenable.com**