tenable® OT Security

TENABLE OT SECURITY ASSET INVENTORY

Asset Inventory provides engineers and security administrators unparalleled visibility into their complex Operational Technology (OT). Tenable OT Security takes automated asset inventory to the next level with clear visualization into all of your ICS assets and the connections between them.

The Challenge: Achieving Deep Situational Awareness

Lack of visibility, security and control in decades-old OT environments has serious security implications. To implement an effective OT security strategy, you need to know exactly which assets you have, their configurations and related activities. However, as OT networks continue to grow, converge with IT and become more complex, it is more difficult to identify and manage all asset details, events, types of communications and protocols.

To address OT security challenges, critical infrastructure and industrial organizations need automated asset discovery tools that provides full situational awareness, thereby empowering you to see the big picture and simplify asset management.

Key Benefits

- Simplifies OT network complexity and hones situational awareness

- Provides unparalleled visibility into assets, their state, and their communications

- Attack vectors hunt for "at risk" weakpoints and proactively alerts you before a threat ever emerges

- Interactive views and intuitive, flexible and customizable templates

- Drill-down access to asset details to support forensic and mitigation efforts

- Enables identification of network flow issues and rogue device activity

The Challenge

- Lack of visibility into converged IT and OT assets in your industrial environment

- Growing complexity of ICS networks, make it harder to manage assets, communications and events

- Effective OT security requires comprehensive situational awareness of all IT, OT and IoT assets and connections and states.

The Solution: Interactive Inventory and Mapping

Tenable OT Security's Asset Inventory and mapping capabilities offers unmatched visibility into complex and converged IT/OT environments through an advanced set of discovery, visualization, analysis and drill-down capabilities.

Tenable OT Security's Interactive Asset Map reveals how ICS networks really operate in day-to-day production operations. The map helps engineers glean insight from newly discovered assets, visualize communication patterns by interacting with data and investigate suspicious activities.

Unfettered Visibility & Situational Awareness

Tenable's Asset Inventory increases situational awareness and supports forensics efforts by providing a comprehensive view of your OT network. The map shows all assets in your OT environment along with their communications paths. This includes controllers (PLCs, RTUs and DCS controllers), HMIs, operator workstations, engineering workstations, any computer or server, and even I/O devices.

The map enables users to easily view the whole network as a high-level illustration, with the ability to zoom in on a specific asset. By enabling users to see the big picture and drill down into a particular asset or communication link, Asset Inventory helps you cut through network complexity for more effective asset management.

Asset Inventory and Analysis

Tenable OT Security automatically discovers all devices in your network. It then creates a complete and inventory of assets along with gain deep insights into device state including firmware version, patch level, ladder logic details and much more.

A wide selection of interactive options lets you change views and manipulate layout patterns as needed to meet your exploration or forensic needs. Using this detailed information, Tenable OT Security's Attack Vector functionality can identify risky configurations and/or device state and alert the administrator of potential threats before an incident occurs.

You can also select any asset on the map to display its details or you can search for a particular asset and display only that asset and its connections to other devices.

By simply clicking on a line connecting any two devices, you can also drill down into protocol information for a specific communication.

Visualization Tools

Visualization is a powerful tool for simplifying network complexity. Tenable OT Security leverages innovative and advanced visualization and mapping techniques to help you gain visibility into OT network and device activity. The map distinguishes between IT and OT communications by assigning them different colors.

Interactive Asset Map

Tenable OT Security's Interactive Asset Map lets you view the entire structure of your OT environment in a single glimpse, while providing a set of drill-down options that reveal the full detail of every asset as well as nature of communications between connected assets. Device intelligence and communications between assets are constantly updated so that you always have the most up-to-date information on your dynamic operations.

The filtering mechanism lets you hone in on a specific subset of data by looking at traffic volume, filtering by time frames or conducting a textual search. The Interactive Asset Map automatically groups assets into logical clusters representing communication structures (e.g., star topology, mesh topology and more).

Detecting Unknown Devices and Connections

One of the key use cases supported is identifying connections that may be problematic—for example, communications between two environments that should be separated by a firewall. Such a connection may indicate problems with the firewall configuration or alternate network routes between environments.

When the system detects unknown communications, you'll be able to identify other connected devices that may be impacted. You can then drill down to further investigate communication between those assets and their properties (e.g., traffic volume and a list of used protocols). Asset Inventory lets you access more detailed information about asset properties.

Reconnaissance Activity and Cyber Threats

The combined functionality of Asset Inventory and the Interactive Asset Map enables you to gain deep insights into each and every device while also seeing the relationships between devices. This can identify patterns of reconnaissance, like network scans from an unexpected system. Since reconnaissance scans are often the stealthy first stage of a cyber-attack, identifying such patterns and impacted devices can provide an early warning of an unfolding threat.

Contact Us:

Please email us at sales@tenable.com or visit tenable.com/contact