OCTAVE

BROCHURE

Obtaining a detailed, accurate OT asset inventory

Understanding options and selecting the right solution

Attacks on industrial infrastructure such as BlackEnergy, CrashOverride and Triton/Trisis have brought greater awareness of OT asset cyber vulnerabilities and risks. Obtaining an accurate and detailed OT asset inventory is a foundational first step for industrial organizations striving to improve their cybersecurity and reduce risk.

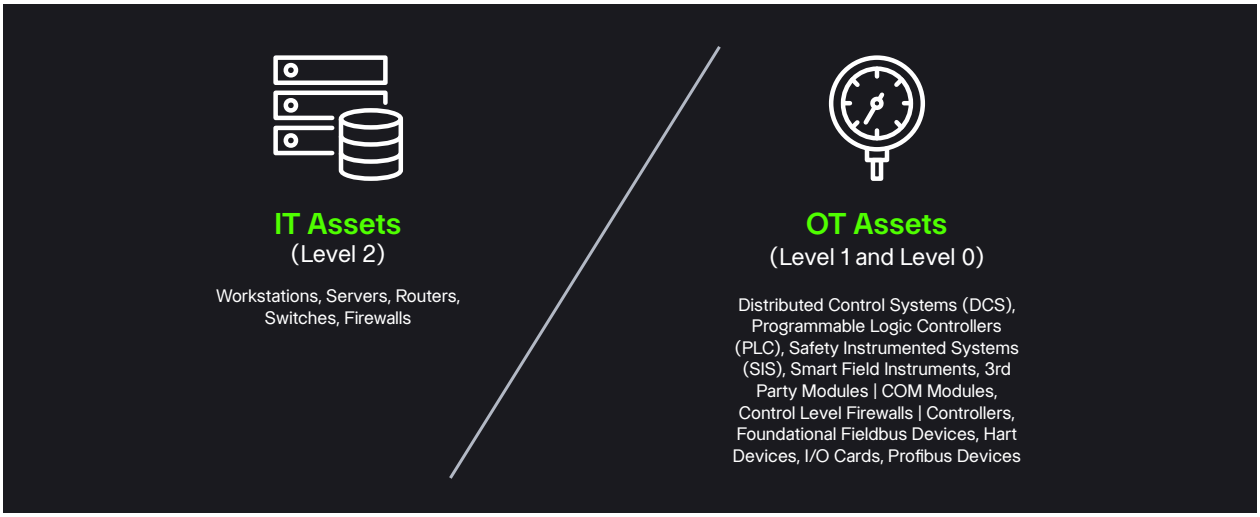
A multinational oil and gas company found that 40% to 60% of its OT assets were "islanded," or not connected to the network. Using a passive network detection/DPI solution to obtain visibility into asset inventory for these systems simply was not an option. This company also discovered that manual inventory collection – an approach used in the past – was inefficient, inaccurate and incomplete.

OT asset inventory: Foundational to OT cybersecurity, frequently lacking

A comprehensive, accurate, in-depth OT asset inventory is a core requirement for OT cyber vulnerability and risk management. It is also a prerequisite for establishing security baselines, managing change, automating closed-loop patch management, meeting internal and external compliance requirements, investigating incidents and understanding potential attack vectors. However, the definition of a "good" OT asset inventory is not universally defined.

OT asset inventory defined

A "good" OT asset inventory is an in-depth inventory of all systems running in the process control environment – one that includes both IT assets as well as OT assets.

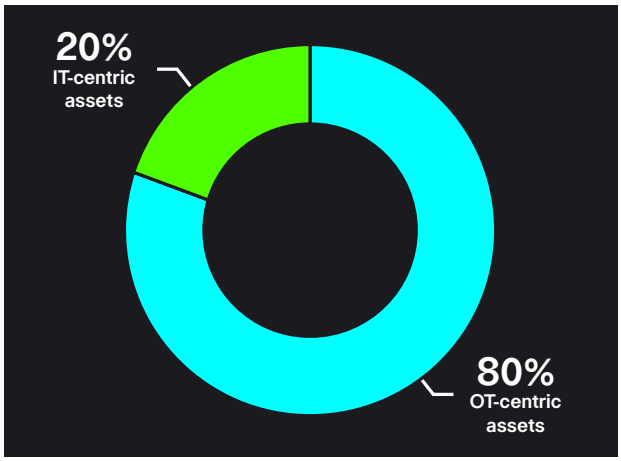


A complete OT asset inventory consists of all Level 2, Level 1 and Level 0 OT assets (see diagram on the next page). It includes a list of all hardware, software and firmware, and for each of those, the manufacturer, model, version and serial number.

Level 1 and Level 0 assets are the most important.

These are the devices and sensors that directly connect to process equipment, move molecules and ensure safe and reliable production. Unfortunately, when it comes to providing a comprehensive inventory of Level 1 and Level 0 assets, certain approaches fall short.

A 20% view of OT assets is not enough



Several vendors provide network-based anomaly detection tools. Industrial organizations have taken these tools and tried to use them for not only their primary purpose of anomaly detection, but also for IT and OT asset inventory discovery.

While anomaly detection tools can provide some visibility into Level 2 IT devices, these tools are unable to obtain a comprehensive Level 1 and Level 0 OT asset inventory. This is because architecturally they rely solely on network traffic analysis. In addition, the IT assets these tools can inventory typically make up only about 20% of the assets on the process control network (PCN). Level 1 and Level 0 assets, the assets that matter the most when it comes to industrial safety and reliability, comprise the other 80% of assets.

Level 1 and Level 0 asset inventory is a fundamental building block for OT asset visibility, security, and control. Without an up-to-date and accurate record of every Level 2 through Level 0 device – from the patch list on a Windows computer to a PLC backplane configuration – IT and OT security professionals cannot effectively secure and control their industrial environment.

OT asset inventory

To those new to OT, obtaining asset visibility can seem like an easy problem to solve – drop an appliance on a network switch, perform deep packet inspection (DPI) to gather device inventory information and display inventory information in a topological view. However, this approach has its limitations.

Proprietary architectures and lack of standard protocols in multi-vendor process control environments make passive Level 1 and Level 0 OT asset inventory discovery and management difficult. Level 1 and Level 0 industrial assets – the sensors and valves that control industrial processes – do not usually communicate on the network. If they do, they usually do not pass the detailed OT asset inventory and configuration information required for a comprehensive OT asset inventory over the network. Many OT assets in industrial environments do not connect to the network at all, further compounding the discovery problem.

To address passive DPI limitations, some vendors have started to claim they can provide a "more complete" inventory by using "active" data collection methods. Active methods use native OT protocols to query control systems for information. However, active methods have their own risks. Improper targeting can disrupt OT services. Existing control system network designs may severely constrain active data collection or prohibit it entirely. Active methods are also not well suited to islanded OT systems unconnected to the network.

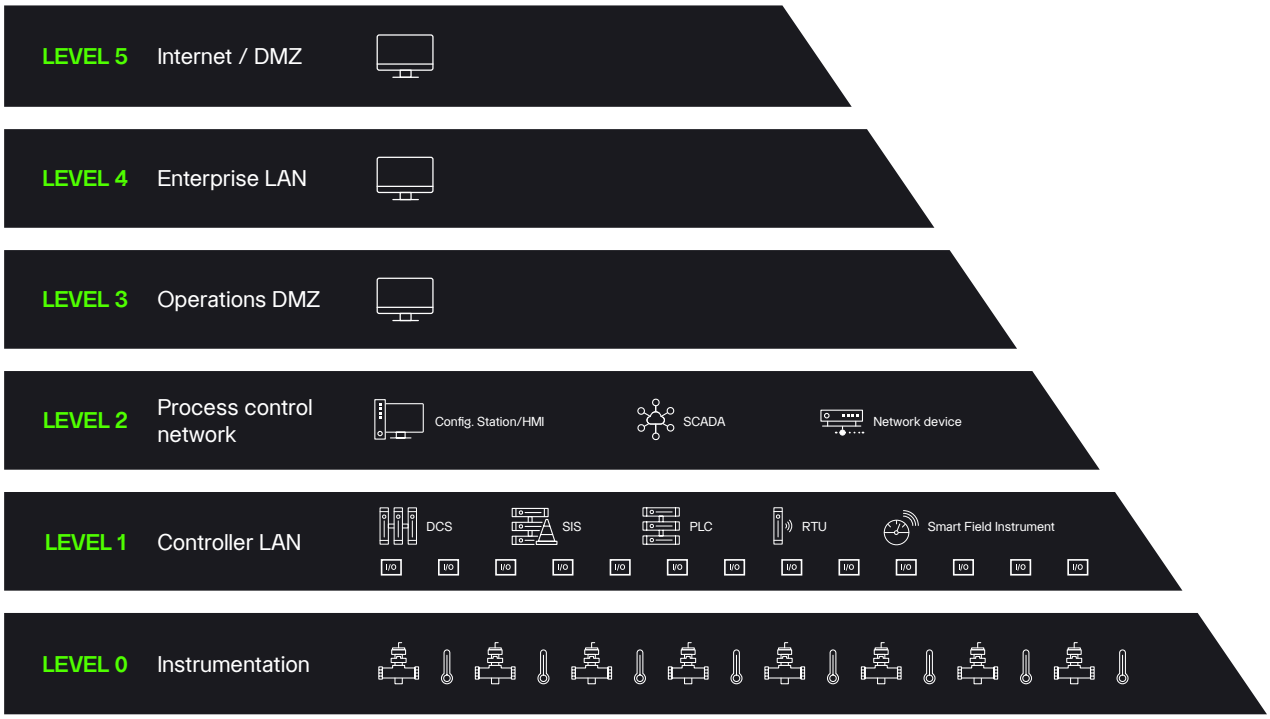
Accurate Level 2 through Level 0 inventory visibility requires more than passive network detection and/or active queries. While each of these methods can provide some visibility, and passive DPI can be useful for network-based anomaly detection, both methods still fall short when it comes to providing the visibility into all Level 1 and Level 0 OT assets required to ensure safe and reliable production.

Octave Cyber Integrity: Deeper OT asset inventory visibility

Octave Cyber Integrity automates inventory data collection and management for all control system assets – from Level 2 to Level 0, as well as Safety Instrumented Systems (SIS).

Cyber Integrity collects Level 1 and Level 0 OT asset inventory information for more than 120 cross-vendor OT systems – not by capturing network traffic, but by collecting and interpreting system configuration files and databases, which provide richer data. This includes detailed configuration data on I/O cards, control strategies, installed software and firmware for all major control systems regardless of vendor.

Cyber Integrity



Cyber Integrity can also import Level 1 and Level 0 OT asset inventory information from isolated, transient and air-gapped OT assets. When combined with the Level 2 information Cyber Integrity gathers from IT assets, companies can obtain the single, complete OT asset inventory required for accurate vulnerability and risk management, incident investigation and response, forensic analysis and obsolescence management.

Today, many companies focus on IT Level 2 asset inventory because information "on the wire" seems easier to get, and because OT asset inventory requirements have not been well-defined. However, only Cyber Integrity can provide the complete OT asset inventory – including Level 1 and Level 0 – required for OT cyber risk identification and management.

About Octave

Octave is a leader in enterprise software, turning data into decisive action and intelligence into your edge. Our software solves for and simplifies complexity, from the design and build to operations and protection of people, property, and assets– for any scope, at any scale. For decades, we've partnered with customers to sharpen performance, elevate efficiency, and amplify results. From factory floors to entire cities, our solutions are tuned to scale up what's possible from day one onward.