SANCTUARY Insight

Manage OT Security with Ease

SANCTUARY

INFO@SANCTUARY.DEV WWW.SANCTUARY.DEV HILPERTSTR. 31, 64295 DARMSTADT, DE

Effortless OT Asset Management

SANCTUARY Insight is a software tool that enables systematic, automated, and cost-efficient monitoring and management of the cybersecurity of OT systems. SANCTUARY Insight uses asset management functionalities to automatically identify all OT devices in production environments and aggregates information about them. Building on this, Insight enables cyber security management of the OT devices found by analyzing their software stacks and determining the security status of the device.

Figure 1 illustrates the architecture of SANCTUARY Insight using a typical production environment setup as an example. Insight consists of three main components, the Insight sensors are integrated into the production network to detect the IT and OT devices to be monitored. The sensors can be installed as stand-alone devices (hardware sensors) or as pure software components (virtual sensors) on existing devices in the form of virtual machines or software containers. Thus, Insight sensors can be deployed very cost-efficiently since also for the hardware sensors only minimal performance and memory requirements exist.

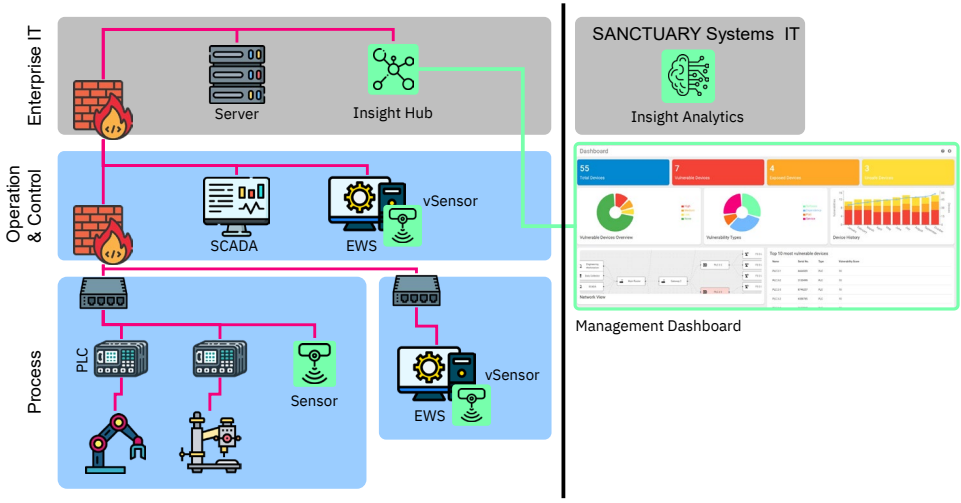


Figure 1: SANCTUARY Insight Architecture

The Insight sensors implement an active scanning methodology which can retrieve detailed information from each device (e.g., vendor, serial number, firmware version) by directly communicating with the device over the supported standardized OT protocols or vendor-specific protocols. The scan procedure is designed in a multi-step approach that minimizes the network impact and impedes any negative impact on the devices by considering each device's capabilities and by only communicating over protocols common for OT networks.

All device information collected by the sensors is centralized at the Insight Hub, which is located in the user's enterprise IT. For security and product information, the Insight Hub can query the Insight Analytics service provided by SANCTUARY Systems. Insight Analytics provides vulnerability and update information, EOL (end of life) dates, and even analyzes firmware images to find vulnerabilities in its components before device vendors know about them.

All device and security information is then presented in an interactive dashboard provided by the Insight Hub. OT operators can use this to monitor the status of the OT landscape on a daily basis and, in the event of security problems, recommendations are given on how these can be rectified. In this way, Insight offers companies a cost-effective way of managing the cyber security of their production environments and supports them in the implementation of risk assessments, such as those required by IEC 62443, especially in times of a shortage of skilled labor.

Hybrid Scanning for Unparalleled Insights

SANCTUARY Insight revolutionizes OT asset management with its hybrid scanning approach. Here's how it works:

Passive Discovery

Our solution initiates with passive detection of Ethernet-based devices. This initial phase provides a comprehensive overview of your network topology without disrupting operations.

Active Exploration

By engaging in non-intrusive communication, we extract detailed information about each device. This active interaction is indistinguishable from regular OT device communication initiated by PLC vendor software.

Minimal Network Impact

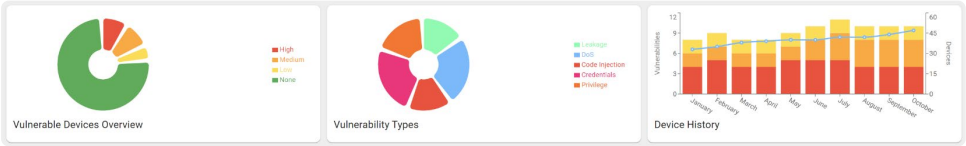
Worried about network congestion? Our communication is gentle, causing minimal traffic. We target specific devices, speaking their native protocols, ensuring both accuracy and efficiency.

Excerpt of Supported Protocols

Our Insight sensors have the goal to achieve complete and detailed OT asset visibility without stressing the network or the devices. For this, we 1) reduce the protocols tried per device to the minimum based on previous device information, 2) use the protocols already used by the vendor software installed on your engineering workstations – which already produce more traffic than what the Insight sensors are emitting. Here is an excerpt of the most relevant protocols supported so far:

- SNMP
- LLDP (and similar implementations like CDP)
- ARP
- DNP3
- UPnP/SSDP
- mDNS
- UDP (discovery for various manufacturers)
- NetBIOS
- SSH
- PROFINET
- Ethernet/IP
- Ethernet Powerlink
- Modbus/TCP
- OPC UA
- BACNet
- Siemens S7
- Beckhoff ADS
- Phoenix Contact PCWorx
- ABB Netconfig
- Schneider Electric Protocol
- Low Level Reader Protocol
- GigE Vision (for Cameras)

Comprehensive Cybersecurity Analysis

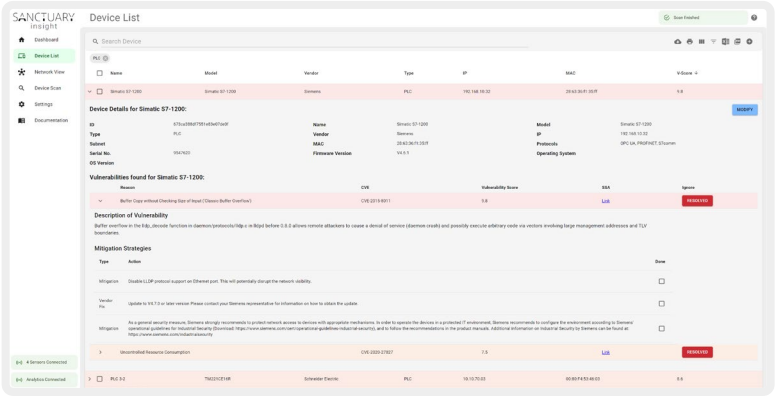


Insight goes beyond basic asset management functionality and offers extensive cybersecurity analyses of OT devices, including:

- Matching against vulnerability databases
- Detection of unpatched security holes
- Analysis of firmware images for known vulnerabilities
- Identification of potential attack points
- Information basis for IEC 62443

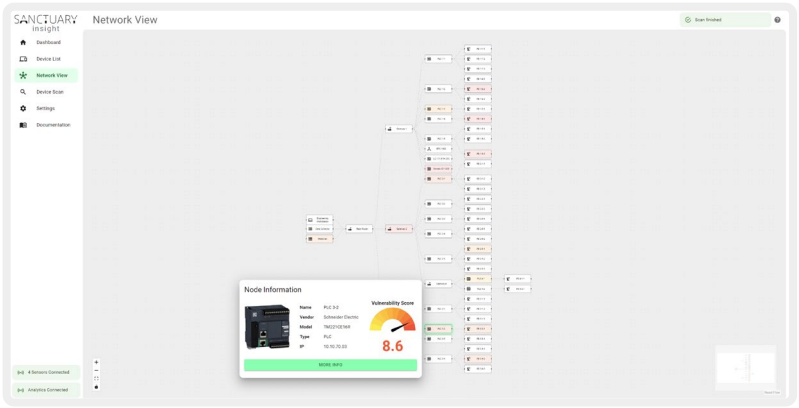
Extensive Information

SANCTUARY Insight delivers detailed information about your devices, including comprehensive vulnerability data, mitigation options, and end-of-life information. Mitigation strategies can be applied to remediate vulnerabilities and document risk resolution. Flexible data export options and integrations (e.g., CSV/Excel, PDF, SBOM, ServiceNow) ensure seamless integration into your existing workflows.



Topology Overview

SANCTUARY Insight provides a comprehensive overview of your OT network architecture, enabling a clear understanding of its structure and connections. With Insight Analytics capabilities, it identifies vulnerabilities and highlights critical weak points, enabling precise network segmentation to enhance security and resilience.



Requirements for Deployment

SANCTUARY Insight requires tiny Insight sensors to be connected to a switch with a standard Ethernet port in each subnet and correct IP configuration (static/DHCP) within the respective subnet. Communication between the sensor and the Insight Hub can be established via sensor-initiated TCP connections or one-way UDP connections for maximum security. The Insight Hub can be deployed as a container or virtual machine (VM) on an existing server and requires a VPN connection to the Insight Analytics platform for seamless data integration and analysis.

LET'S TALK

Interested in testing SANCTUARY Insight?

Contact us at info@sanctuary.dev