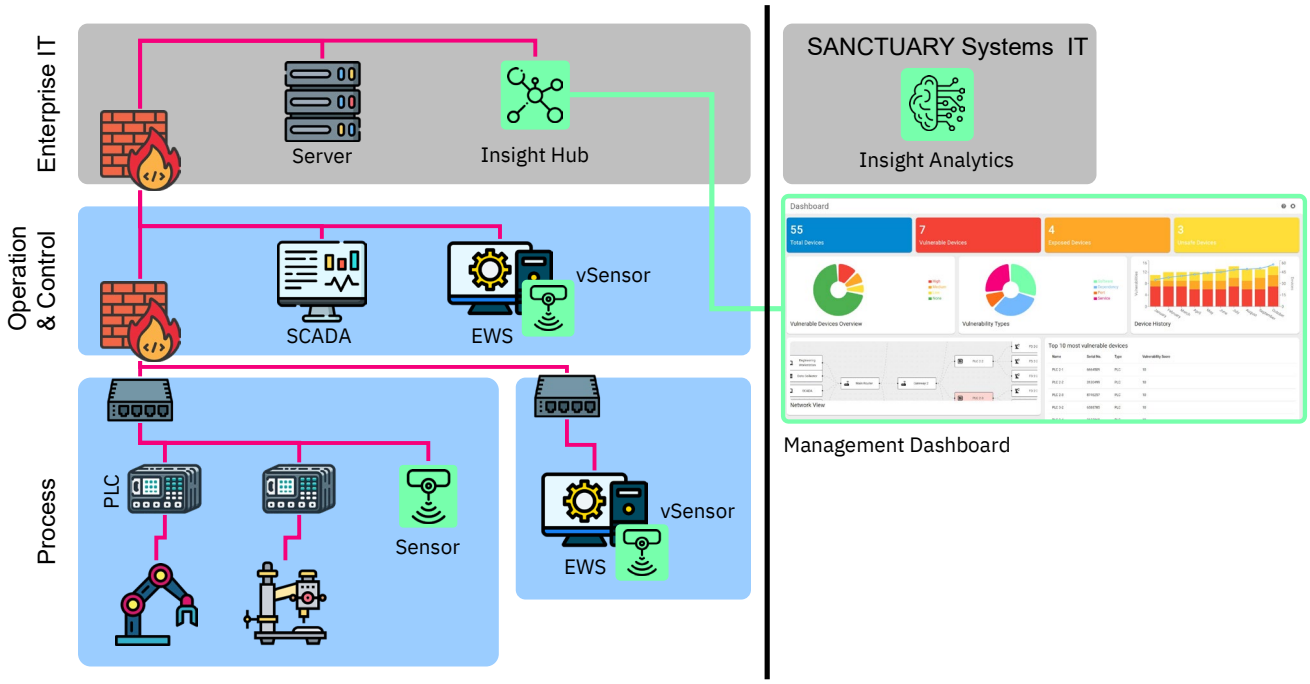
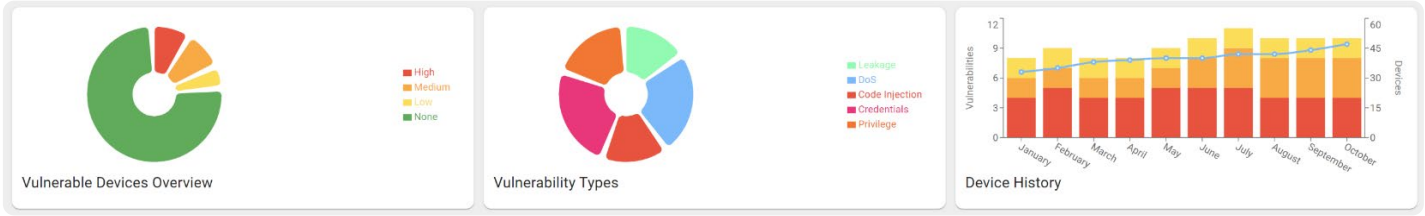
SANCTUARY Insight: Manage OT Security with Ease

SANCTUARY Insight provides a systematic approach to identifying, monitoring, and securing operational technology environments. At its core, the platform deploys lightweight sensors that can be integrated as either dedicated hardware appliances or as virtual instances on existing infrastructure. These sensors combine passive network observation with active, protocol-aware interrogation to discover the full range of IT and OT devices present in a production setting. The discovery process accounts for vendor-specific protocols and device capabilities, ensuring that detailed information such as vendor, serial numbers, and firmware versions is collected without disrupting ongoing operations. By correlating device attributes with their software stacks, SANCTUARY Insight enables a precise mapping of assets and their security-relevant properties.



Asset Management in the Insight Hub



Collected information is consolidated at the Insight Hub, which is typically deployed within the enterprise IT environment. From there, data can be enriched with vulnerability intelligence, end-of-life information, and firmware analysis provided by SANCTUARY Systems' analytics service. This enables the identification of latent risks, even those not yet publicly disclosed by device vendors. The resulting knowledge base is presented in an interactive dashboard that allows operators to assess the security posture of their OT landscape in real time. Recommendations for remediation are generated in response to identified issues, supporting structured risk management and compliance with standards such as IEC 62443. In this way, SANCTUARY Insight extends beyond asset visibility to deliver an integrated capability for lifecycle security management in industrial environments.

Excerpt of Supported Protocols

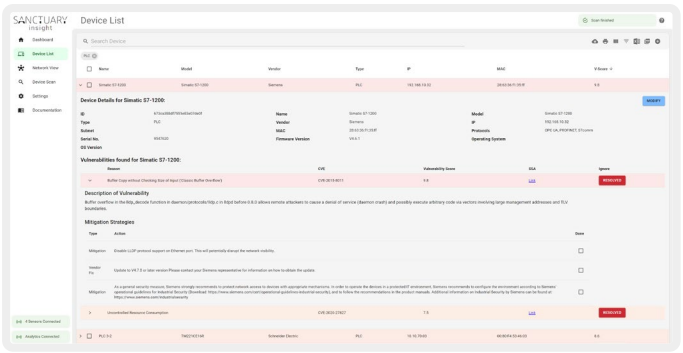
Our Insight sensors achieve complete and detailed OT asset visibility without stressing the network or the devices. For this, we 1) reduce the protocols tried per device based on previous device information, 2) use the protocols already used by vendor software. Our aim is to find even the most specific OT devices – from PLCs over cameras to QR code readers! Here is an excerpt of the most relevant protocols supported:

ARP
BACNet
CIP
Ethernet/IP
GigE Vision
HART/IP
IEC 60870-5-104 & 61850
LLC
LLDP
Modbus/TCP
NetBIOS
ONVIF
OPC UA
PROFINET
SNMP v1/v2c/v3
SSH
UPnP/SSDP
ABB Netconfig
Beckhoff ADS
Bosch ctrlX
CodeSys v2/v3
FESTO NFS, WAY
Moxa
Phoenix Contact PCWorx
Siemens S7
Schneider Electric Protocol
SE UMAS

Additional protocols can be added on request!

Comprehensive Cybersecurity Analysis and Reporting

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.



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.