SANCTUARY Insight: System BOM Generation for Machine Tools

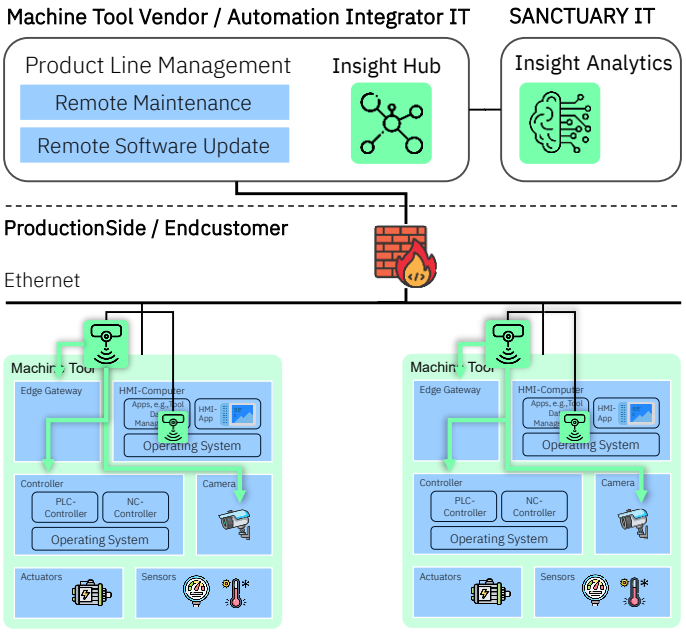
Machine tools increasingly comprise a heterogeneous set of connected devices: programmable logic controllers (PLCs), numerical controllers, human–machine interfaces (HMIs), industrial PCs, edge gateways, sensors, and actuators. Each subsystem runs software and firmware supplied by different vendors, updated on different cadences, and integrated late in the delivery chain. This heterogeneity creates blind spots that hinder vulnerability management and lifecycle control. When a machine is customised or reconfigured, the inventory rapidly diverges from design documentation. Operators and builders therefore need a reliable mechanism to enumerate hardware and software components, including exact firmware versions and configuration context, without assuming prior knowledge of the topology.

Automatic BOM Generation with SANCTUARY Insight

Within a machine tool cell or line, SANCTUARY Insight automatically identifies OT devices and their software stacks using passive network observation and selective, protocol-aware queries.

PLCs, HMIs, and controllers are discovered along with vendor, model, and serial information where available. Firmware and operating system versions are extracted through industrial protocols and authenticated interfaces, and correlated with the underlying hardware.

The system then composes a system-level BOM that integrates a hardware BOM and a software BOM, linking software components to their executing devices for unambiguous traceability.



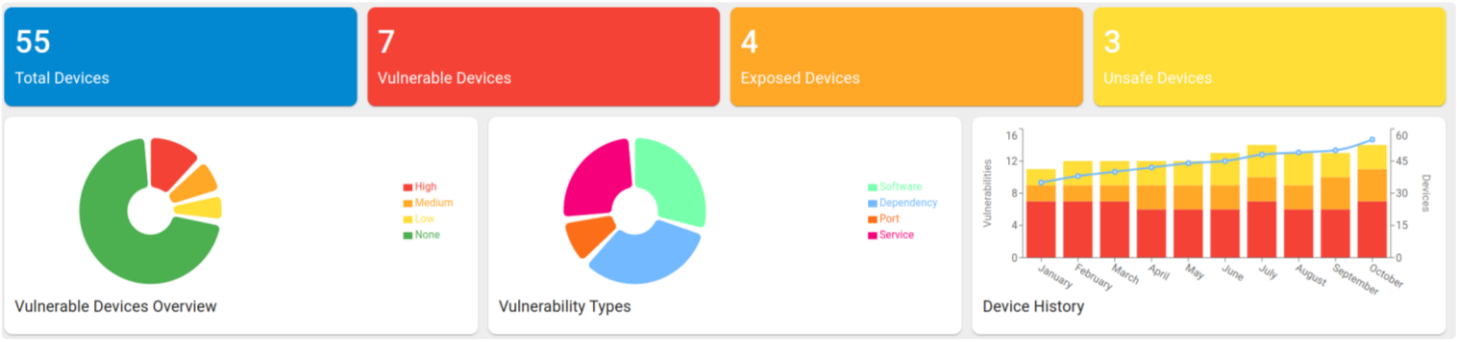
Excerpt of Supported Protocols

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

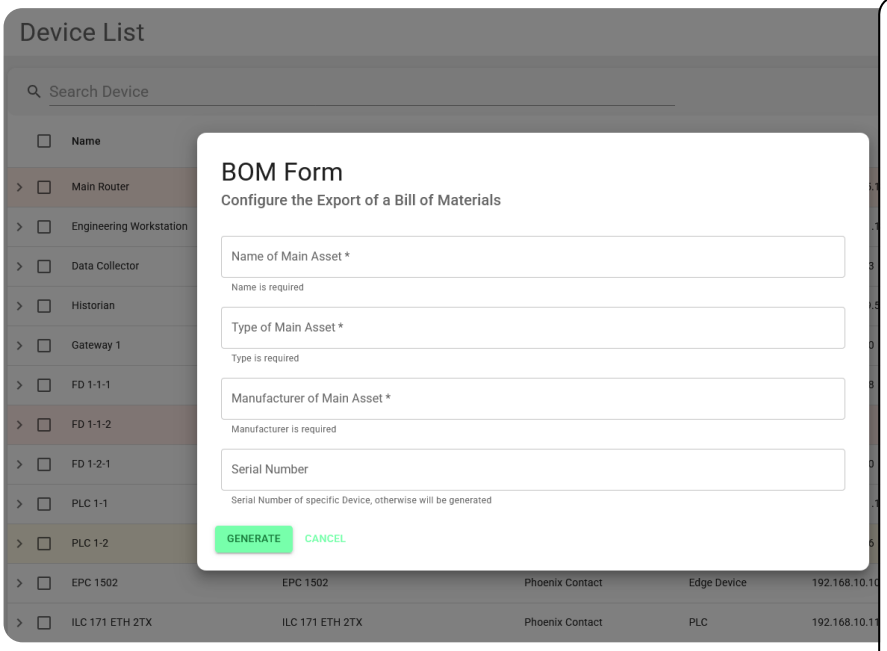
Additional protocols can be added on request!

Comprehensive Cybersecurity Analysis and Reporting



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 the EU Cyber Resilience Act and IEC 62443




```
{
    "bomFormat": "CycloneDX",
    "specVersion": "1.6",
    "serialNumber": "123",
    "version": 2,
    "metadata": {
        "timestamp": "2025-08-21T12:51:12.116940Z",
        "component": {
            "type": "CNC Machine",
            "name": "Maschine B",
            "manufacturer": {
                "name": "MyCompany"
            }
        }
    },
    "components": [
        {
            "bom-ref": "d7d55745-8571-4363-bead-4ee23c6085f1",
            "type": "device",
            "name": "Main Router",
            "manufacturer": {
                "name": "Cisco"
            },
            "properties": [
                {
                    "name": "cdx:device:model",
                    "value": "Catalyst 8500-12X"
                },
                {
                    "name": "cdx:device:serialNumber",
                    "value": 6504761
                },
```


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.