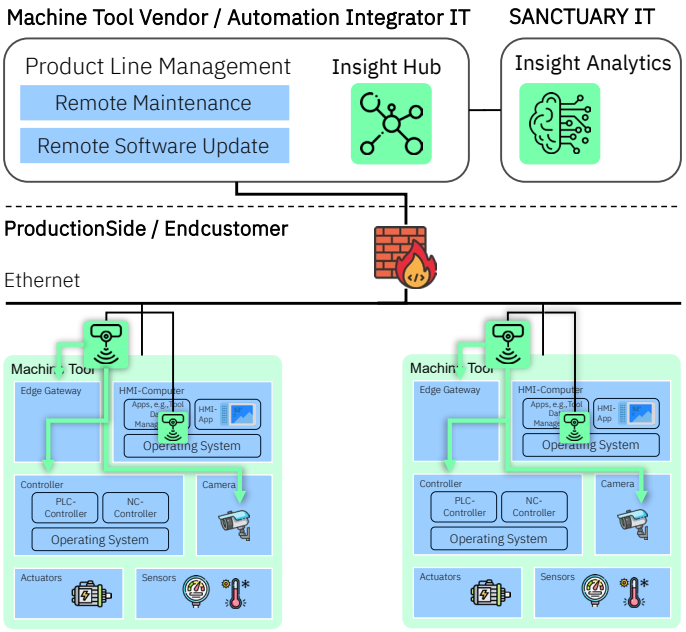
SANCTUARY Insight: System BOMs für Werkzeugmaschinen

Werkzeugmaschinen bestehen zunehmend aus einem heterogenen Verbund vernetzter Geräte: speicherprogrammierbare Steuerungen (SPS), numerische Steuerungen, Mensch-Maschine-Schnittstellen (HMI), Industrie-PCs, Edge-Gateways, Sensoren und Aktoren. Jedes Teilsystem führt Software und Firmware unterschiedlicher Anbieter aus, die in unterschiedlichen Zyklen aktualisiert und spät in der Lieferkette integriert werden. Diese Heterogenität erzeugt blinde Flecken, die das Schwachstellenmanagement und die Kontrolle des Lebenszyklus erschweren. Wird eine Maschine angepasst oder umkonfiguriert, weicht das Asset-Inventar schnell von ursprünglicher Entwurfsdokumentation ab. Betreiber und Hersteller benötigen daher einen zuverlässigen Mechanismus zur Erfassung der Hardware- und Softwarekomponenten, einschließlich exakter Firmware-Versionen und des Konfigurationskontexts, ohne dass Vorwissen über die Topologie vorausgesetzt werden kann.

Automatisches Generieren von „System Bill-of-Materials“ mit SANCTUARY Insight

Innerhalb einer Werkzeugmaschinenzelle oder -linie identifiziert SANCTUARY Insight automatisch OT-Geräte und deren Software-Stacks durch passive Netzwerksbeobachtung und Nutzung herstellerspezifischer Protokollabfragen. SPS, HMI und Steuerungen werden zusammen mit Hersteller-, Modell- und Serieninformationen erfasst, detaillierte Daten wie Firmware- und Betriebssystemversionen werden über industrielle Protokolle und authentifizierte Schnittstellen ausgelesen und mit der zugrundeliegenden Hardware korreliert. Das System erstellt anschließend ein systemweites Stücklistenmodell (Bill of Materials, „BOM“), das eine Hardware-BOM und eine Software-BOM integriert und Softwarekomponenten eindeutig den ausführenden Geräten zuordnet, um eine unmissverständliche Nachverfolgbarkeit sicherzustellen.



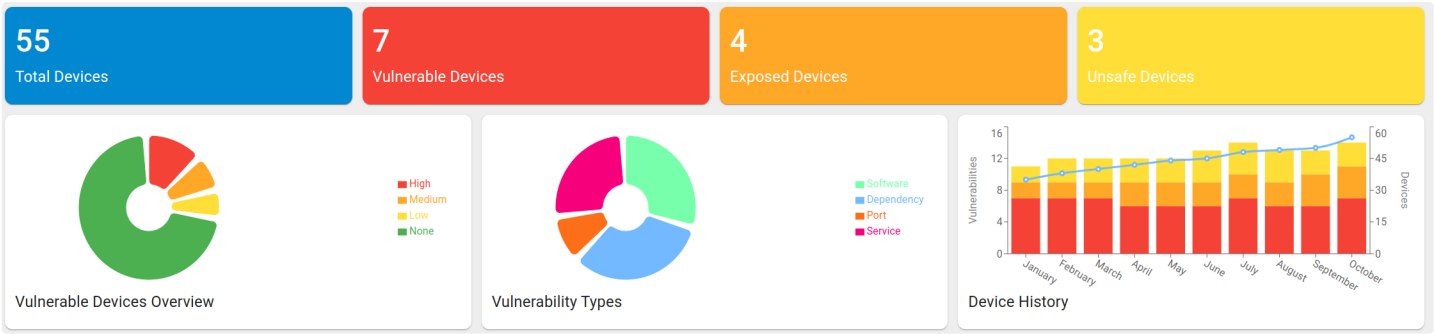
Auszug unterstützter Protokolle

Unsere Insight-Sensoren ermöglichen eine vollständige und detaillierte Sicht auf OT-Assets, ohne das Netzwerk oder die Geräte zu belasten. Dafür werden pro Gerät nur die auf Grundlage bereits gewonnener Informationen relevanten Protokolle eingesetzt und bevorzugt solche verwendet, die auch von herstellereigener Software genutzt werden. Ziel ist es, selbst die spezifischsten OT-Geräte zu erfassen – von SPS über Kameras bis hin zu QR-Code-Lesegeräten. Nachfolgend ein Auszug der wichtigsten unterstützten Protokolle:

- 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

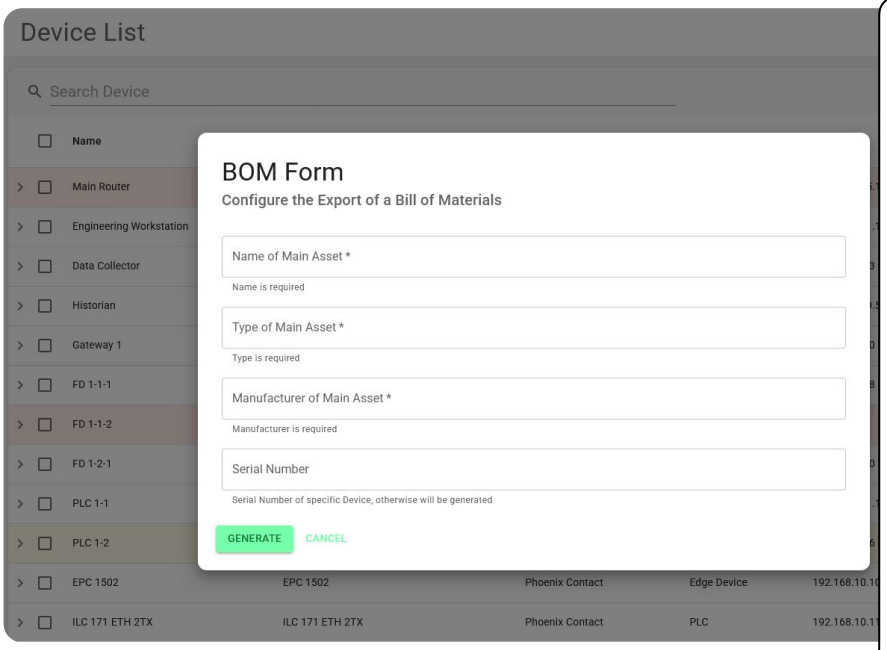
Weitere Protokolle auf Anfrage

Umfassende Cybersecurity-Analyse und Reporting



Insight geht über die grundlegende Asset-Management-Funktionalität hinaus und bietet umfassende Cybersecurity-Analysen von OT-Geräten, darunter:

- Abgleich mit Schwachstellendatenbanken
- Erkennung unbehandelter Schwachstellen
- Analyse der Firmware-Images um bekannte Schwachstellen zu finden
- Identifizierung potenzieller Angriffspunkte
- Informationsgrundlage für den EU Cyber Resilience Act und IEC 62443



Anforderungen für die Inbetriebnahme

SANCTUARY Insight erfordert den Anschluss kleiner Insight-Sensoren an einen Switch mit einem Standard-Ethernet-Port in jedem Subnetz sowie eine korrekte IP-Konfiguration (statisch/DHCP) innerhalb des jeweiligen Subnetzes. Die Kommunikation zwischen Sensor und Insight Hub kann entweder über vom Sensor initiierte TCP-Verbindungen oder über unidirektionale UDP-Verbindungen für maximale Sicherheit erfolgen. Der Insight Hub lässt sich als Container oder virtuelle Maschine (VM) auf einem bestehenden Server bereitstellen und benötigt eine VPN-Verbindung zur Insight Analytics-Plattform, um eine nahtlose Datenintegration und Analyse zu gewährleisten.