Octoplant – Asset Inventory Service

The next evolution in
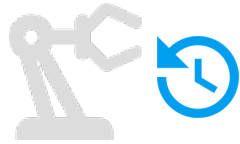Data Driven Manufacturing

John Boyd

AGENDA

01 | Market trends and company

02 | Threat Protection overview

Info

Today, we will guide you through our company and product offering

# Success in automated production requires mastering key challenges

AUVESY-MDT

Reduce unplanned production downtime

82% of companies experience unplanned downtime[1],
with a huge impact!
Average duration: 4 hours[1]
Average costs: 2 MUSD[1]

Mitigate cyber security risks

Effects of cyberattacks became more severe.
Downtime from ransomware attacks increased by 40% in 2022[2] alone.
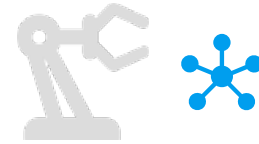
Effective cooperation between OT and IT

IT and OT worlds are historically poorly connected. E.g.: Experts estimate that only 10% of MES systems are connected to the OT, reducing ability to successfully steer production.

AUVESY-MDT

We secure
the world's
automation

We secure production for some of the world´s most known brands

AUVESY-MDT

Automotive | Automotive suppliers | Food & beverages | Healthcare & medical | Plant engineering
Raw materials | Steel | Utilities | Transport & logistics | Others

We are set up to service multi-national customers across the globe

We are the world's market leader in vendor-independent data management software for industrial automation

AUVESY-MDT

> 2500
customers

> 47
years of experience

> 100
global partners

> 50
regions worldwide

Our partner network can get you up to speed and operate effectively

AUVESY-MDT

OFFICE USA NORTH

OFFICE GERMANY

OFFICE USA SOUTH

OFFICE CHINA

With the support of our partner ecosystem

octoplant is the market leading solution to help you achieve your goal:

Keep production running

**octoplant is the market leading solution
to help you achieve your goal:** keep production running

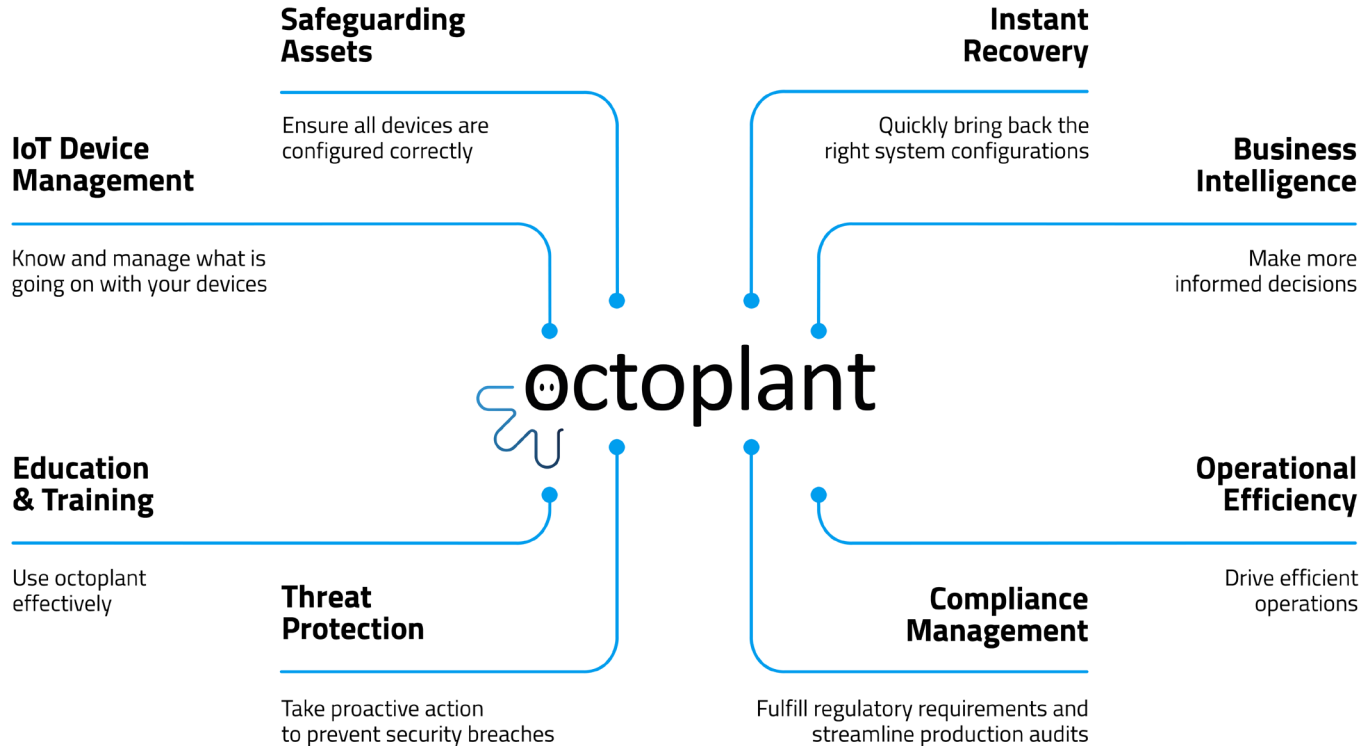Top class data management platform for your automated production assets

State of the art visualization and analysis of your OT backup processes

Advanced cyber security solution to protect your OT environment

Our all-covering data management platform comes with a commitment: To always keep production running

AUVESY-MDT

Safeguarding Assets

Ensure all devices are configured correctly

Instant Recovery

Quickly bring back the right system configurations

IoT Device Management

Know and manage what is going on with your devices

Business Intelligence

Make more informed decisions

octoplant

Education & Training

Use octoplant effectively

Operational Efficiency

Drive efficient operations

Threat Protection

Take proactive action to prevent security breaches

Compliance Management

Fulfill regulatory requirements and streamline production audits

10

octoplant: **Threat Protection**

Safeguarding Assets

Ensure all devices are configured correctly

Instant Recovery

Quickly bring back the right system configurations

IoT Device Management

Know and manage what is going on with your devices

Business Intelligence

Make more informed decisions

octoplant

Education & Training

Use octoplant effectively

Operational Efficiency

Drive efficient operations

Threat Protection

Take proactive action to prevent security breaches

Compliance Management

Fulfill regulatory requirements and streamline production audits

**Solution:
octoplant
Threat Protection**

Thanks to our
Threat Protection
function,
you can:

**Conduct
performance and
security checks**

Understand the performance and
security level of your assets and receive
tangible recommendations

**Create a
vulnerability report**

Receive a complete vulnerability
exposure overview of your assets,
incl. mitigation recommendation

AUVESY-MDT

Learning: Mitigating cyber security risks will be the key challenge to reduce unplanned downtime over the next years

Both OT environments and IIoT devices are more and more in the focus of hackers:
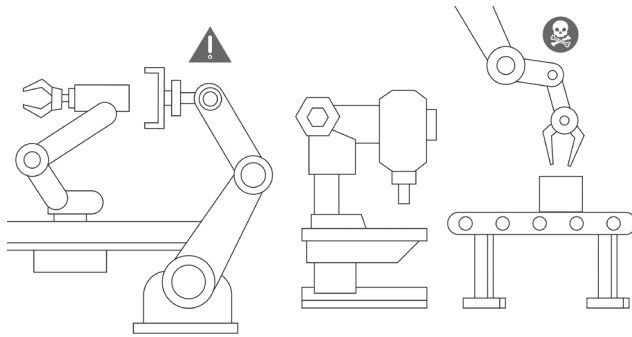
OT attacks in PLC and SCADA relevant attacks increased by 2204% between Jan and Sept 2021. [1]

Threat protection
Take proactive action to mitigate vulnerabilities

The solution:
Monitor and identify potential risks, **vulnerabilities**, or **intrusions**, and receive recommendation on **required actions** to ensure maximum uptime and safety

Sources:
1) IBM Security, X-Force Threat Intelligence Index 2022; references attacks on Port 502, which allow access to PLCs and SCADA.
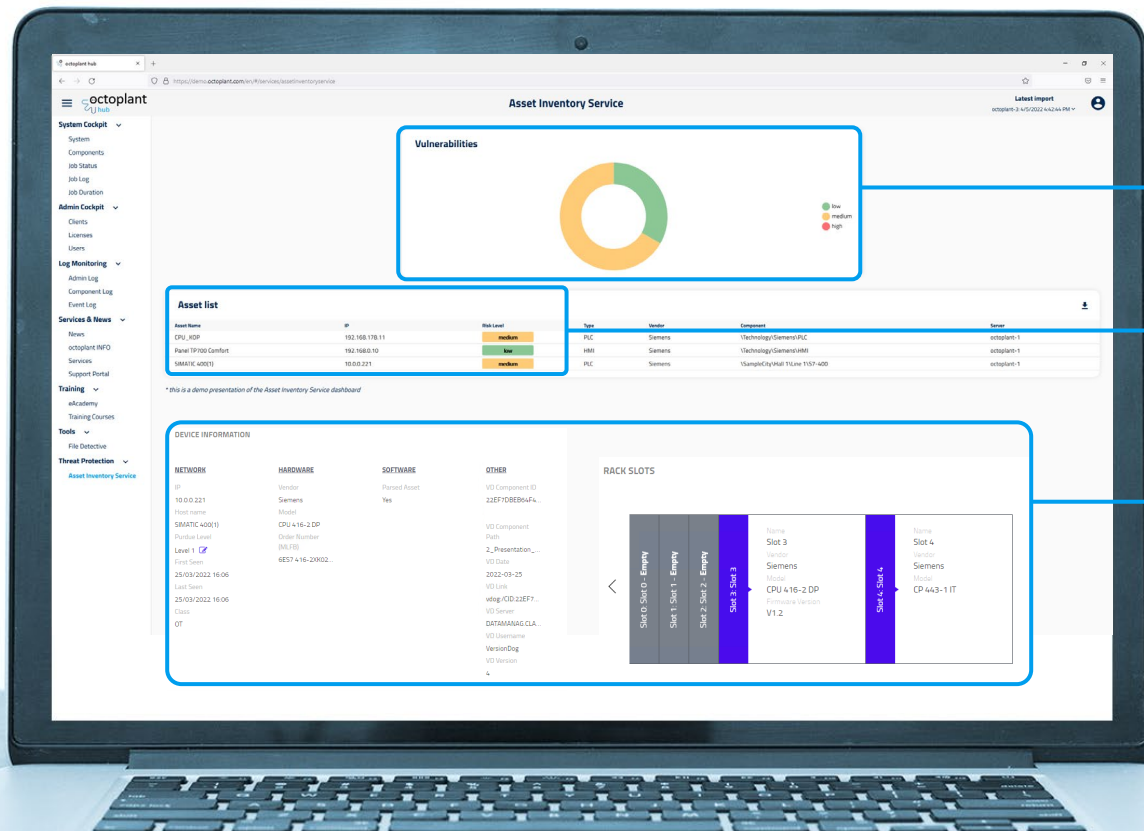
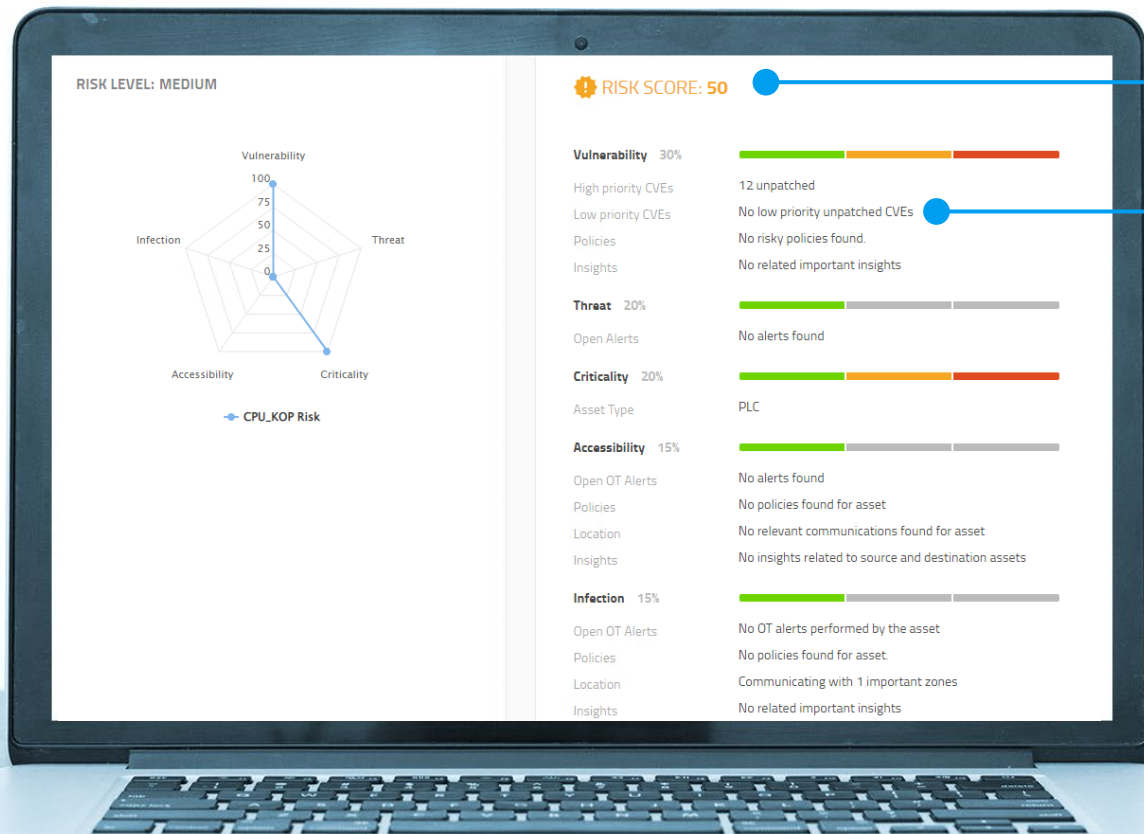# Get an aggregated overview of your risk status

Aggregated overview on risk status per device

Asset level overview of risk status and asset details

View of the asset, enriched by details such as the asset's rack slot, model, and IP

15

Get a detailed Risk & Vulnerability Correlation

AUVESY-MDT

RISK LEVEL: MEDIUM

Vulnerability
100
75
50
25
0
Infection   Threat

Accessibility   Criticality

CPU_KOP Risk

⚠ RISK SCORE: 50

Vulnerability 30%

High priority CVEs   12 unpatched
Low priority CVEs   No low priority unpatched CVEs
Policies   No risky policies found.
Insights   No related important insights

Threat 20%

Open Alerts   No alerts found

Criticality 20%

Asset Type   PLC

Accessibility 15%

Open OT Alerts   No alerts found
Policies   No policies found for asset
Location   No relevant communications found for asset
Insights   No insights related to source and destination assets

Infection 15%

Open OT Alerts   No OT alerts performed by the asset
Policies   No policies found for asset.
Location   Communicating with 1 important zones
Insights   No related important insights

Breakdown of the Asset Risk Score automatically assigned to and continuously updated for each asset in the inventory

Comparing the details of each asset to the latest common vulnerabilities and exposures (CVE) data and an extensive library listing insecure protocols, misconfigurations, and other security weaknesses

Receive a risk assessment report and drill down to understand vulnerabilities at asset level
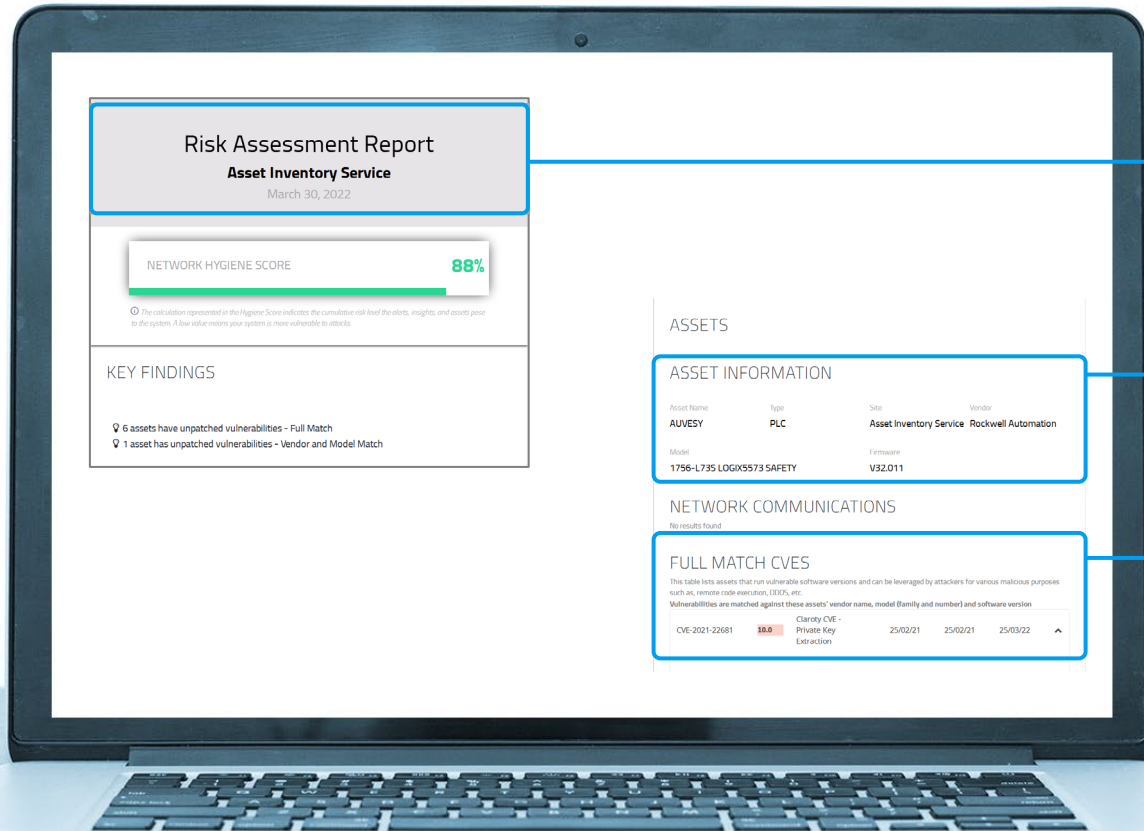
Generate Risk Assessment Report on your assets

Detailed asset information (e.g. vendor, model number, Firmware, etc.)

Get latest common vulnerabilities and exposures (CVE)

Benefits & Capabilities

AUVESY-MDT

Single Source of Truth

Delivers comprehensive OT visibility and a centralized, fully automated OT asset inventory that includes the hardware, firmware, model, rack slot, IP, vendor, and related details for all assets.

Expands disaster recovery

Reveals and integrates any critical assets that are not included in your disaster recovery plan and ensures that they are backed up.

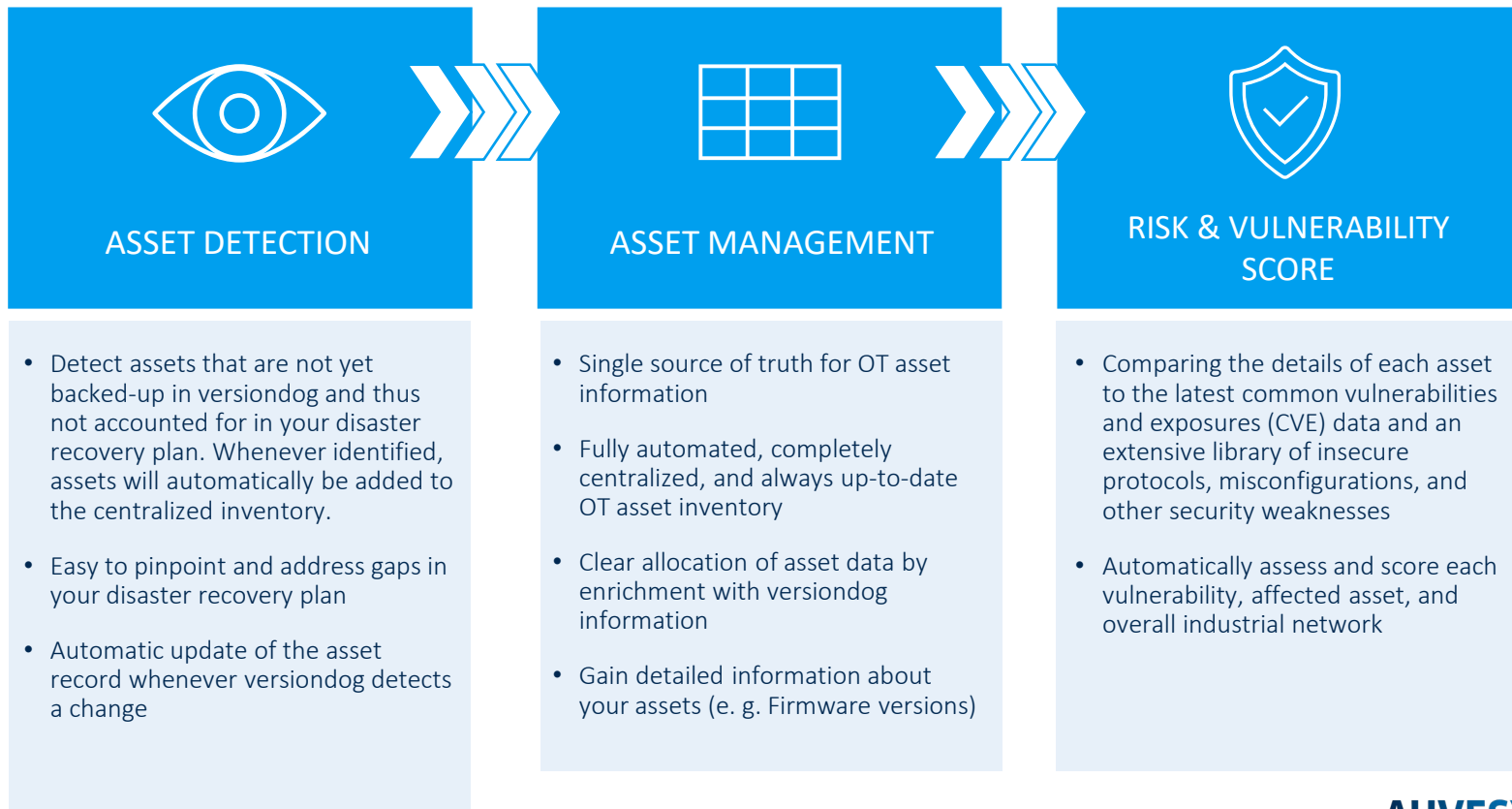## More efficient and effective governance

Allows centralized access, management and reporting for all asset, risk and vulnerability data and reporting processes.

Less Total Cost of Ownership (TCO)

Boosts labor productivity, reduces prevalence of human error, and allows personnel to focus on what matters most by reduced manual work and lean reporting processes.
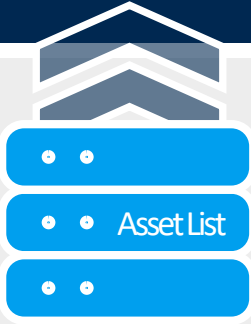
Asset Inventory Service

ASSET DETECTION

- Detect assets that are not yet backed-up in versiondog and thus not accounted for in your disaster recovery plan. Whenever identified, assets will automatically be added to the centralized inventory.

- Easy to pinpoint and address gaps in your disaster recovery plan

- Automatic update of the asset record whenever versiondog detects a change

ASSET MANAGEMENT

- Single source of truth for OT asset information

- Fully automated, completely centralized, and always up-to-date OT asset inventory

- Clear allocation of asset data by enrichment with versiondog information

- Gain detailed information about your assets (e. g. Firmware versions)

RISK & VULNERABILITY SCORE

- Comparing the details of each asset to the latest common vulnerabilities and exposures (CVE) data and an extensive library of insecure protocols, misconfigurations, and other security weaknesses

- Automatically assess and score each vulnerability, affected asset, and overall industrial network

AUVESY·MDT

How it Works
Automated OT Asset Inventory

AUVESY-MDT

Thank you
for your
attention!