octoplant

AMDT



SUMMER RELEASE

# BUILT TO SEE

## OCTOVISION

## + FULL LIGHT ON THE ASSETS YOU NEVER HAD A VIEW OF

Most industrial organizations can describe their OT estate. Far fewer can prove it. Asset records live in a discovery tool, a maintenance system, a spreadsheet and an engineer's memory — and no two of them agree. When an auditor asks which assets are protected, or a new vulnerability is disclosed, the answer takes days to assemble and still arrives with caveats.

The Newest Octovision Release (Summer) closes that distance. Assets from outside Octoplant can now be imported and enriched with vulnerability and lifecycle data, forming extended OT asset inventory alongside the assets Octoplant already protects. The gap between what you run and what you actually have covered becomes visible. Criticality context moves out of people's heads and into the asset record, ranking what gets fixed first. And vulnerability data refreshes regularly, so the risk picture reflects the present rather than whenever someone last remembered to update it.

octovision

Octovision is the intelligence layer on top of Octoplant and requires a connected Octoplant environment to work. That connection is also its advantage: it surfaces asset data no network scanner can reach, including devices that are disconnected and invisible to discovery tools.



# + VALUE ACROSS OPERATIONAL AND OT SECURITY ROLES

**From the PLC to the board report, Octovision Summer Release enhances what each role can see and prove. Here is what it means for the four closest to production.**

### IT & OT Security Managers gain a broader view of exposure and a shorter path to acting on it

Vulnerability management stops at the edge of what the inventory covers. Bringing external assets into Octovision and enriching them with CVE and lifecycle data widens that edge — and false positive management means a finding ruled out on an asset does not come back next cycle.

### CISOs gain coverage evidence that stands up to an audit

Managed versus unmanaged visibility turns protection coverage from an assumption into something reportable. Combined with documented criticality classification, it answers the two questions auditors and boards ask most: which assets are protected, and which ones matter most.

### OT & Automation Engineers gain clarity on what is protected on their lines

Engineers can see which devices sit under Octoplant protection and which do not, and flag gaps before a failure exposes them. Automated vulnerability updates mean newly disclosed CVEs affecting their assets surface regularly.

### Plant & Maintenance Managers gain a basis for planning rather than reacting

Criticality classification across process, protection and safety dimensions gives maintenance planning and spare parts decisions an operational rationale — instead of priority following whoever raises it loudest.

SUMMER RELEASE

AMDT

# WHAT'S NEW IN OCTOVISION

**Five changes, all pointing the same way – more of your assets visible, and better information attached to what you can see.**



## + EXTERNAL ASSET ONBOARDING & ENRICHMENT

Import assets that Octoplant does not manage by CSV - from discovery tools, maintenance systems or spreadsheets - and see them enriched with vulnerability and lifecycle data where they can be matched, alongside your Octoplant-managed assets. One rich OT asset inventory.

## + ASSET CRITICALITY CLASSIFICATION

Classify assets by process criticality, need for protection and safety relevance, with default values so large estates get a workable baseline. Criticality sits alongside vulnerability data in the same view, helping teams prioritize what matters most rather than working from CVSS score alone.

## + FALSE POSITIVE MANAGEMENT

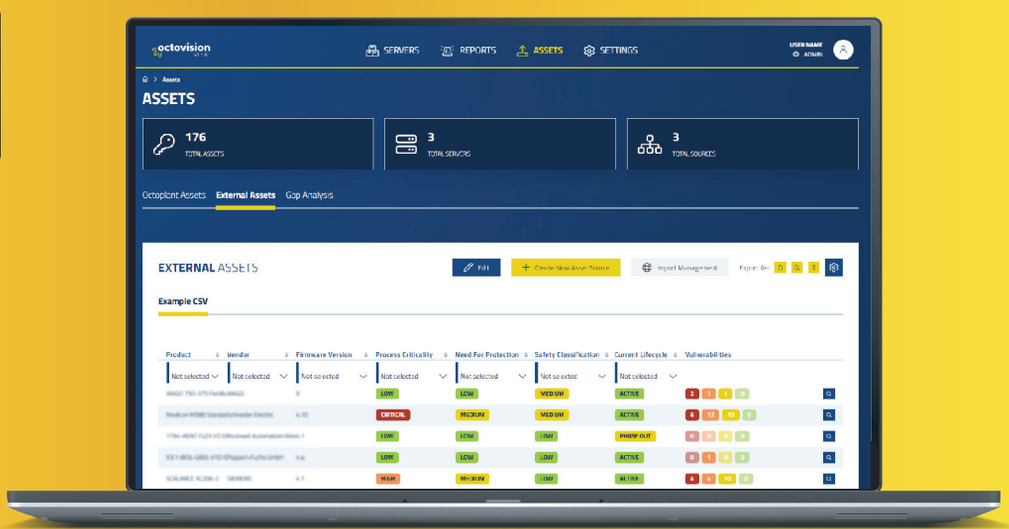
Mark a vulnerability as a false positive on the asset it does not apply to, and it stops returning for review. Less repeated validation each cycle, risk views that reflect real exposure, and vulnerability data that improves over time.

## + AUTOMATED VULNERABILITY UPDATES

CVE information refreshes automatically. No manual upload cycle, no single person responsible for remembering, and reporting that reflects the current threat landscape.

## + MANAGED VS UNMANAGED ASSET VISIBILITY

See how many of your crown jewels are actually protected. Assets under Octoplant management are backed up, versioned and recoverable; everything else shows as unmanaged. Gaps are grouped by asset type so the largest exposures surface first, and coverage becomes a metric you can track rather than an assumption you rely on.




*External asset onboarding and enrichment require the Asset Inventory add-on, plus the Vulnerability and/or Lifecycle add-ons. Automated vulnerability updates require myAMDT credentials and network access to myAMDT.*

AMDT

# AMDT

**AMDT is the global leader in backup, version control, and comparison solutions for industrial automation, built on nearly 40 years of specialized expertise.**

Our mission, "Production Resilience Delivered," reflects our commitment to ensuring that automated production systems are secure, resilient, and capable of fast recovery from disruptions, thereby safeguarding production output. Established in 2022 through the merger of AUVESY GmbH and MDT Software Inc., AMDT is headquartered in Landau, Germany, with offices in the USA and China. Our extensive global network includes over 100 partners, and we proudly support more than 3,000 customers worldwide, helping them maintain optimal performance and resilience in their production environments.

- **www.amdt.com**
- **www.octoplant.com**

## Octovision runs on Octoplant

Octoplant is a vendor-agnostic platform that backs up, versions and recovers the configurations of the automation systems running your production — across devices, lines and sites, whatever the vendor. Octovision is the intelligence layer on top of it and requires a connected Octoplant environment to work. That connection is also its advantage: it surfaces asset data no network scanner can reach, including disconnected devices that never appear on a discovery tool.

