

OT Security and Vulnerability Management for Production

Octoplant offers a powerful solution for industrial customers seeking to enhance their cybersecurity. By identifying, assessing, and providing actionable insights on Common Vulnerabilities and Exposures (CVEs) affecting production assets, octoplant plays a critical role in safeguarding industrial environments from potential threats. Our capabilities not only secure production but also support companies in meeting compliance requirements, such as NIS2 and NIST, enabling proactive vulnerability management and ensuring production continuity.

octoplant



Enhanced Security Profile

Octoplant enables manufacturers to proactively manage vulnerabilities, mitigating risks associated with production downtime, data breaches, and unauthorized access.

3,000+

customers worldwide



Change Detection

Get instant alerts on configuration changes to detect all modifications, internal or external, including direct machine edits. Discrepancies appear in automated or subsequent backups, adding extra security and oversight.

100+

partners across the globe

octoplant



CVE Mapping and Assessment

With access to criticality scores and detailed asset information, customers can prioritize and address high-risk vulnerabilities, ensuring a targeted and effective cybersecurity strategy.

60%

of the world's largest manufacturers use octoplant



Compliance Management

Octoplant ensures NIS2 and NIST compliance by enhancing production transparency with configuration and asset management, enabling quick recovery, and reducing downtime.

1,000,000

industrial devices rely on octoplant everyday

Vulnerability Management Features in octopant pro hub

Comprehensive CVE Detection

Octopant's vulnerability management matches asset information with public CVE databases, providing visibility into known security vulnerabilities for both hardware and software on the production floor.

Criticality Assessment

Each CVE includes a criticality score from the Common Vulnerability Scoring System (CVSS), enabling users to prioritize vulnerabilities by impact and exploitation risk, with a focus on high-risk threats requiring immediate attention.

Asset-Specific Vulnerability Insights

Customers receive detailed information on all assets affected by specific vulnerabilities, including vendor details, model, firmware version, and network address, with the "Asset Deep-Dive" feature linking to official sources for guidance.

Multi-Site Scalability

Octopant's CVE management scales across multiple sites, making it ideal for large industrial organizations with complex asset inventories.

Proactive Vulnerability Management

Octopant's automated matching and continuous training adapt to new CVEs, improving detection accuracy over time. The system leverages data from the latest automation projects, providing an up-to-date view of vulnerabilities without requiring manual scans or backups.

Octopant stores, versions, and compares all shopfloor devices and documents, providing enhanced management for over 150 common OT and IT-related devices

