SPOT Supply chain vulnerability management

Comprehensive supply-chain cyber risk management

The OTORIO Supply-chain Pre-installed OT (spOT) cyber risk discovery tool, is an offline portable platform, uniquely tailored to be operated by production-floor personnel. spOT enforces supply-chain vendor compliance to relevant standards and organizational policies, and pre-emptively identifies stealthy cyber vulnerabilities and operational misconfigurations.

Tighter Production Floor Integration Control

spOT gives the Business Information Security Officer (BISO) and operational teams tighter control over the production floor. spOT scans are based on best practices, open source, and proprietary researched vulnerabilities. The proprietary, industry-tailored scan engine was developed by world-leading cyber and engineering experts to enable safe OT integrations of lines, machines, and assets into the production floor.

Safe Industry 4.0 Digitalization

Introducing a new line, machine or other asset into the production/process network is not a straightforward and risk-free process in today's cyber threat landscape. Besides the potential impact on production and business continuity, the new asset must be confirmed to comply with organization and regulatory policies.

Early discovery of misconfigurations, outdated firmware or protocols, unnecessary communication, policy deviations, or hidden malware, is critical for policy compliance. At the same time, exhausting manual procedures in a resource-limited environmnent can often prevent production floor personnel from attending easily fixed cybersecurity risks before they impact production. When manual verification is time consuming and, can extend the machine introduction cycle period, spOT, being an automatic, fast and simple scanning tool can be a powerful business driver.

spOT Benefits

OTORIO's spOT generates automatic threat and vulnerability reports, as well as remediation guidelines, based on best industry practices, and incorporating unique threat intelligence. spOT reports can assist in decision making for enforcement of both proprietary and industry regulated compliance policies, as well as maintain an ongoing vendor risk score history.

- Automatic, fast, and intuitive industrial supply-chain vulnerability assessment
- Simplified offline supply-chain assessment of pre-installed IT-OT assets by production on-site personnel
- Pre-introduction OT inventory management and baseline configuration enforcement
- Supervise, verify, and collect vendor-based operations-related statistics history
- Automatic report generation, to significantly improve the acceptance cycle for new machines, cells, or lines into the production floor
- Easy integration with existing asset management and patch management tools, allowing for secure patch download and verification.

Reports

-

Outdated and vulnerable firmware or operation system
- Policy and compliance deviations
- Weak or default credentials
- Vulnerable protocols and implementations
- Compliance with vendor best practices and accompanying recommendations
- Stealthy malware

OTORIO - a global leader in safe Industry 4.0 digitalization.

OTORIO is an advanced Managed Security Service Provider, founded by Israeli defense cybersecurity experts, partnered with a leading global plant engineering group. OTORIO's unparalleled forward-looking products and services are delivered by world-leading "special forces" talents, leveraged by proprietary cutting-edge technology.

OTORIO's solution counteracts current and future industrial cyber risks, ensuring safe Industry 4.0 digitization, as an integral part of the operational life cycle. OTORIO's broad offering addresses the different stages and challenges a traditional industry faces when setting out on the journey of digital transformation.