SOLUTION BRIEF

Armis Centrix™ Digital Twin for OT/ IoT Security

Overview

Armis Centrix™ Digital Twin is an advanced, non-intrusive, and automated virtual model of an organization's operational technology (OT) / Internet of Things (IoT) network. By replicating the operational environment in a sandbox setting, Digital Twin enables organizations to understand their exposure, test security measures, and proactively address risk with no impact to the live environment. This improves risk mitigation strategies, and strengthens cybersecurity defenses.

Challenges That Make Digital Twin Necessary

In OT (Operational Technology) environments, Cyber Exposure Management is uniquely complex due to the convergence of legacy systems, real-time processes, and physical safety concerns. Oftentimes, maintaining operational resilience while also applying the security necessary can often feel like the two goals are diametrically opposed. Challenges may include:

- **High Risk of Downtime -** Any security testing or misstep in OT can lead to production halts, equipment damage, or safety incidents.
- **Legacy and Unpatchable Systems -** OT often runs on decades-old systems with no patching ability or vendor support.
- **Limited Visibility & Asset Context -** Many OT environments lack full visibility into device types, firmware, communication protocols, operational processes and behaviors.
- **Inability to Run Live Pen Tests or Scans -** Traditional vulnerability scanners and red-teaming tools can crash OT devices or disrupt SCADA communications.
- **Maintenance Windows Are Infrequent -** Security updates and infrastructure changes often require maintenance shutdowns which may only happen quarterly or annually.
- **Converged IT/OT Attack Surface** The IT/OT boundary is porous, exposing OT to threats that can propagate laterally.
- **Low Tolerance for False Positives -** Even a false alert can trigger fail-safes or shutdowns in sensitive environments (e.g., energy, pharma, manufacturing).

- **Strict Regulatory & Safety Requirements** Industries like power, oil & gas, and healthcare have safety-critical systems subject to NERC, IEC 62443, FDA, etc.
- **Limited Incident Response Maturity -** Many OT teams lack mature IR processes and tooling integrated with IT security.

In OT, where "fail fast" isn't an option, a Armis Centrix™ Digital Twin provides the visibility, control, and safety net that traditional cybersecurity tools cannot. It becomes the foundation for safe cyber exposure management, bridging operational continuity with robust security.

Armis Centrix™ Digital Twin

Armis Centrix™ Digital Twin is a virtual representation of an organization's OT/IoT environment, providing a detailed, dynamic model for security assessment and analysis. It solves key cybersecurity challenges by:

1. **Simulating Real-World Threat Scenarios -** Running breach and attack simulations (BAS) to identify segmentation gaps and attack paths.
2. **Enabling Safe Security Testing -** Allowing organizations to test security strategies without disrupting live operations.
3. **Providing Actionable Insights -** Delivering prioritized mitigation recommendations based on real exposure and operational impact.

Key Features

- ✓ **Comprehensive Asset Visibility -** Consolidates network data and topology to provide a unified and contextualized, real-time view of all assets and their interdependencies.
- ✓ **Attack Graph Analysis -** Identifies potential attack paths, segmentation gaps, and high-risk vulnerabilities in the environment.
- ✓ **Automated Security Controls Assessment/Validation -** Runs breach and attack simulations to assess security weaknesses and validate security measures.

Key Benefits and Outcomes

- **Proactive Exposure Identification -** Continuously simulates your real-world environment to detect vulnerabilities, misconfigurations, or gaps before attackers can exploit them. This enables preemptive cost-effective remediation, reducing risk of breaches and compliance violations.

- **Safe Testing Environment for Threat Scenarios -** Provides a safe environment for the execution of attack simulations in an isolated replica environment. This empowers security teams to understand potential blast radius and refine incident response plans without affecting production.

- **Change Impact Analysis -** Tests the impact of system updates, new asset deployments, or policy changes before rolling them out. Testing on a non production system prevents unintended security gaps or business disruptions caused by changes in the production environment.

- **Enhanced Threat Hunting and Forensics -** Recreates breach scenarios to replay and investigate attacker behavior in full fidelity. Outcomes include deeper and more detailed forensic insight thus accelerating root-cause analysis without risking data integrity or uptime.

- **Security Control Validation -** Continuously verifies the effectiveness of security controls against evolving threats in a controlled environment. This can help validate investments and prioritize future security spending based on real world performance data rather than fuzzy projections.

- **Dress Rehearsals -** Security teams can safely rehearse patching, segmentation, and other remediation strategies.Doing so can reduce mean time to detect (MTTD) and mean time to respond (MTTR).

- **Regulatory and Compliance Readiness -** Simulates scenarios to ensure systems meet compliance standards like NIST CSF, IEC 62443, NIS 2, TSA, HIPAA, or ISO 27001.

Conclusion

Armis Centrix™ Digital Twin empowers organizations to take control of their OT/IoT security posture, reducing cyber risks while ensuring operational efficiency. By providing unmatched visibility, advanced threat simulations, and actionable risk mitigation strategies, Digital Twin is a critical capability for securing industrial environments while maintaining full fidelity and resilience of the production environment.

ARMIS®

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization’s cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform

Industries

Solutions

Resources

Blog

Try Armis

Demo

Free Trial