SOLUTION BRIEF

Armis Attack Path Mapping

Challenges in OT Security - Following The Proliferation of an Attack

Operational Technology (OT) environments are the backbone of industrial and critical infrastructure operations. However, these systems have become more converged with IT networks and IoT devices, thus introducing new vulnerabilities and a larger attack surface that adversaries can exploit. Organizations face several significant challenges in securing OT environments:

Complexity and Diversity of Systems - OT environments encompass a mix of legacy and modern systems, each with unique vulnerabilities, making uniform visibility, security enforcement and management across all assets and devices difficult.

Operational Disruptions - Unlike IT systems, OT assets operate continuously, making it challenging to schedule maintenance windows and/or perform security updates. In some cases, legacy systems may not even have applicable security updates to deploy.

Limited Visibility - Many OT devices communicate using specialized and proprietary industrial protocols that lack traditional IT monitoring capabilities. Up to 50% of OT assets are dormant, meaning they do not communicate over the network. Due to the sensitive nature of OT devices, scanning for threats can destabilize the integrity of devices. Each of these limitations can lead to security blind spots.

Cyber-Physical Convergence - Cyberattacks on OT can have direct physical consequences, such as equipment damage, safety hazards, and production halts.

Regulatory Compliance - Industries such as energy, healthcare, and manufacturing must adhere to strict security and compliance mandates, further complicating risk management.

Attack Path Mapping & Its Role in Cyber Exposure Management?

Attack Path Mapping is the process of systematically identifying, visualizing, and analyzing potential attack vectors within an OT environment. By going beyond simple device inventory, mapping attack paths empowers organizations in gaining a proactive understanding of how an adversary might exploit vulnerabilities to move laterally between IT and OT or to interconnected systems via east-west traffic attack proliferation.

As a crucial component of **Cyber Exposure Management**, Attack Path Mapping helps organizations:

Focus on and Prioritize Risks Based on Context - Instead of focusing solely on isolated device specific vulnerabilities without full context, Attack Path Mapping assesses risks based on the path an attack proliferates, reachability of target the, operational impact and interdependencies across IT, OT, and IoT environments.

Improve Incident Response - Understanding attack paths enables security teams to anticipate potential threats and develop preemptive mitigation strategies that accounts on not only where an attack impacts, but also on where it is likely to go.

Superior Mitigation Strategies - Attack Path Mapping provides cost-effective mitigation strategies for exposure reduction through configuration changes in the network. The suggested exposure mitigation recommendations also provide alternatives to patching, which is rarely an option in OT environments.

Enhance Resilience - Continuous attack path analysis ensures that organizations can adapt and fine tune their cyber exposure management and security defenses to evolving threat methodologies, paths and landscapes.

How Does Armis Attack Path Mapping Work?

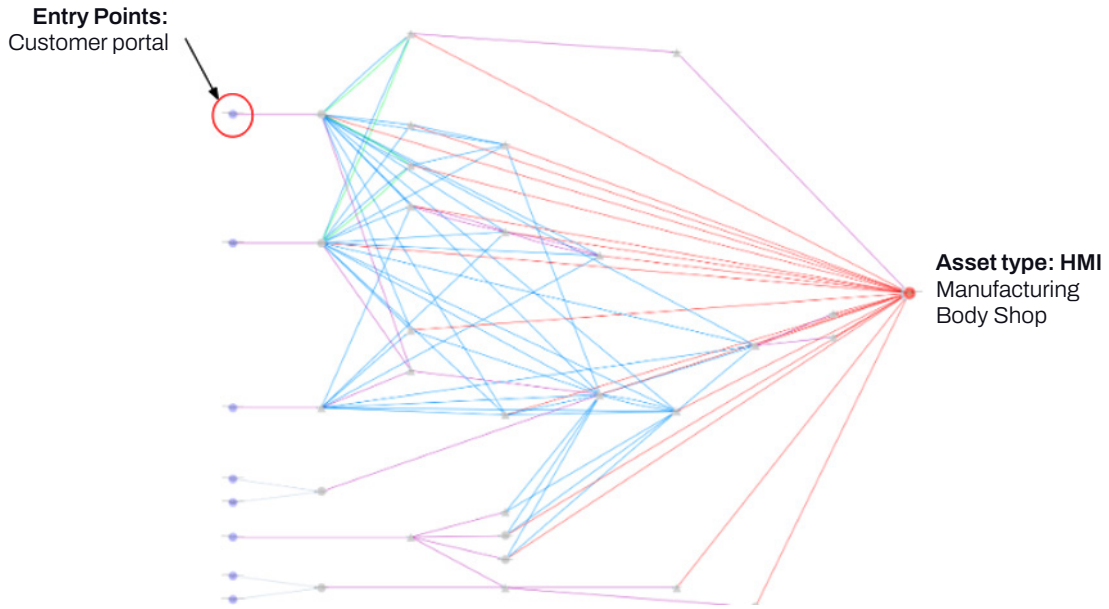

Fig 1: The Armis attack graph is a specialized OT network graph representing the potential attack paths within the network. It identifies the ways an attacker could move through the network to compromise critical assets. The attack graph is based on a powerful, AI based engine that extracts actionable insights based on network topology and traffic flow.

Attack path mapping starts with comprehensive asset discovery, identifying all OT, IT, and IoT assets, mapping their interconnections, and establishing a full inventory. Once all assets and their relationships are inventoried, Armis performs a contextual risk analysis which evaluates vulnerabilities and threats based on asset criticality, business impact, potential attack paths and exposure to both internal and external threats. This helps not only prioritize the most severe threats to the business based on asset criticality, but also the pathways of an attack. Lateral movement simulation models how attackers could exploit weak points to pivot across the OT network, giving security teams visibility into potential attack paths before adversaries can take advantage. With this insight, organizations benefit from prioritized mitigation recommendations, providing actionable strategies to reduce risk in a way that aligns with operational and security priorities. Furthermore, continuous monitoring and updating keep risk assessments dynamic, ensuring organizations stay ahead of emerging threats and vulnerabilities as they evolve.

Key Benefits & Outcomes of Attack Path Mapping

Organizations that implement Armis Attack Path Mapping can achieve:

01 **Reduced Attack Surface -** Identifies and eliminates exploitable entry and further proliferation points before attackers can leverage them.

02 **Optimized Risk Prioritization -** Ensures critical vulnerabilities, risk and pathways with the highest operational impact are addressed first.

03 **Regulatory & Compliance Assurance -** Simplifies adherence to industry-specific security mandates (e.g., NIS2, IEC 62443, NERC CIP).

04 **Improved Threat Response -** Enables security teams to anticipate holistic threats beyond “just the asset” and respond faster to potential incidents.

05 **Operational Continuity -** Reduces the likelihood of cyber disruptions affecting production and service delivery.

What Sets Armis Attack Path Mapping Apart?

Armis offers a best-in-class Attack Path Mapping solution that stands out from competitors by providing:

Deep OT/ICS-Specific Context - Unlike generic IT security tools, Armis integrates deep industrial expertise and provides coverage beyond OT only assets to assess risk both at the point of impact as well as to their potential proliferation paths.

Seamless IT-OT Integration - Bridges security visibility across IT, OT, and IoT assets for a unified defense strategy and offers both on premises and SaaS based options.

Customization Multi-Detection Engines - Armis provides continuous threat exposure management (CTEM) and assessments by giving customers the freedom and flexibility of leveraging both passive as well as safe active querying without disrupting critical industrial processes.

Automated Risk Prioritization - AI-driven insights ensure that mitigation efforts are prioritized and focused on the most pressing threats based on business context.

Actionable Intelligence & Remediation - Offers clear, proactive action for exposure reduction that goes beyond the simple mapping of attack paths. Armis provides recommendations regarding adjustments to firewall rules, restriction of connections, hardening of assets and mitigation of vulnerabilities that enable lateral movement towards critical targets.

Real Traffic Analysis - Analyze both real network activity — captured through passive traffic monitoring—and firewall rule configurations, which represent potential access paths. This distinction allows for a comprehensive view of what is actively happening in the network versus what could happen, even if no current communication is occurring or certain assets remain dormant. Additionally, the capability to simulate various attack scenarios in a sandbox environment, aligned with your threat model, enhances preparedness by identifying vulnerabilities before they can be exploited.

Conclusion

As OT environments become more connected, the risks they face continue to grow. Armis Attack Path Mapping is a vital tool for proactively securing these environments, enabling organizations to understand, map and mitigate potential threats before they materialize. By leveraging Armis advanced Attack Path Mapping capabilities, organizations can enhance resilience, ensure compliance, and protect critical infrastructure from dynamic cyber exposure threats.

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