ARMIS + SPLUNK FOR OT

CLOSE THE OT DEVICE VISIBILITY GAP

The security needs of Industrial Control Systems (ICS) and all Operational Technology (OT) environments are changing. These devices are critical to production, manufacturing, power, and utilities but they have no inherent security. And increasingly, these environments are connected to enterprise networks, exposing them to hackers and Internet-borne malware. The recent NSA/CISA Alert AA20-205A warns of a “perfect storm” for these attacks.

Armis® is an agentless, passive device security platform that secures all types of managed and unmanaged devices—OT, IT, and IoT. It discovers and identifies all devices in your environment and their associated risks, performs continuous, real-time risk analysis of device behavior, and detects and automatically responds to threats. Our Splunk® integration extends OT visibility and security to Splunk’s Data to Everything platform for a consolidated view of devices and risks that helps you keep your entire environment protected.

Along with the rich asset inventory, risk assessment, and threat detection Armis provides, the Splunk add-on for OT Security expands existing Splunk Enterprise Security frameworks to improve security visibility in OT environments. This add-on expands Splunk’s ability to ingest and monitor OT Assets, improves OT Vulnerability Management including defined applications of MITRE ICS ATT&CK framework, and interfaces and reports to support customer compliance and audit with NERC CIP.

KEY SOLUTION BENEFITS

- Extend your investment value in Splunk to unmanaged operational technology (OT) assets.
- Analyze device behavior for risks, threats, and attacks.
- Improve the efficiency of threat detection and incident investigation.

Identify and Classify OT Devices, Protocols, and More

Effective OT asset management requires visibility into every device in your environment, from the manufacturing line to the executive suite. This broad scope is essential because bad actors see your environment as one interconnected attack surface.

Armis automatically discovers and generates a comprehensive inventory of OT assets, including SCADA, PCS, DCS, PLC, HMI, MES, plus devices in your enterprise environment. Armis determines the make, model, OS, IP, location and more, and can track the connection history and activity history of a device through Profibus, Profinet, Modbus, and many other OT protocols.

Armis identifies and classifies instrumentation devices at Level 0 of the Purdue model, process control devices at Level 1, supervisory systems at Level 2, and all devices up to Level 5, including devices like network switches, firewalls, video cameras, and building management systems. And the Armis Device Knowledgebase of over 300 million device profiles provides you with a wealth of information about each, like device type, manufacturer, model, OS and version, location, reputation, applications used, and more.

Manage Risk Effectively, Respond to Threats Efficiently

With so many devices in a typical enterprise environment alone, it's challenging to know which ones most vulnerable to an attack. Adding an entire OT environment makes planning and prioritizing mitigation that much more difficult.

Armis automatically performs a security risk assessment for every device in your environment. Assessments include an overall device risk score along with detailed information about factors that make a device's risk profile, for example, connectivity methods, behavior, use of cloud resources, authentication, and manufacturer reputation. If a device's behavior is considered risky, Armis can block or quarantine the device automatically and generates an alert for your security team in your Splunk environment.

> "The stories of Armis being able to plug in and work as advertised, without a whole lot of setup or configuration were true. We can see all our different layers from zero to five."
>
> **Nathan Singleton**
> Manager of Cybersecurity at Helmerich & Payne

Comply with Security Frameworks

You likely model your security controls against one or more security frameworks like the Center for Internet Security (CIS) Critical Security Controls or the NIST Cybersecurity Framework. You might also use the Purdue Enterprise Reference Architecture to better segment your network to isolate your sensitive OT devices from your enterprise devices. Or, you might need a comprehensive way to address the cyber attack techniques in the MITRE ATT&CK for ICS matrix.

Armis is purpose-built to help you apply these frameworks throughout your environment—especially with critical OT devices. Our platform provides broad-spectrum coverage that supports 11 of 20 Critical Security Controls, and 16 of the NIST CSF controls across the Identify, Protect, Detect, and Respond categories. And Armis can help you audit your network connections to measure your network's integrity against the Purdue reference architecture.

Get Started Quickly

Armis deploys without installing any endpoint agents or additional hardware. It requires no learning period to start identifying devices or detecting threats, so you can get started seeing value right away. Integration with your Splunk's Data to Everything platform is quick and easy too, using Armis connectors you can access from Splunkbase. Integration makes all of the rich information Armis provides available to your security team right in the SIEM interface they already know and use every day.

LEARN MORE:

armis.com/splunk

ARMIS

1.888.452.4011
armis.com

ABOUT ARMIS

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately held company and headquartered in Palo Alto, California.

20201118-2