Closing the Operational Resilience Blindspot with ServiceNow and Armis

According to the latest statistics, the number of connected devices worldwide is expected to exceed 13.1¹ billion by the end of 2023, and this figure is projected to climb to almost 30 billion² by 2030. Maintaining operational resilience is fast becoming a strategic imperative to map your entire attack surface.

The global regulatory landscape, including the European NIS² (across industries) and DORA (in financial services) initiatives, is increasingly focused on maintaining the cyber resilience of critical services and maintaining service uptime while managing third-party risk. Knowing which assets underpin your critical services and the real-time security posture of those assets has become an imperative.

The integration between the Armis Asset Intelligence and Security Platform and ServiceNow allows you to gain complete visibility and control over IT, IoT, OT, and IoMT devices whilst helping improve your overall security posture by reducing the risks associated with unknown and vulnerable assets against weaponized and executable exploits.

Armis and ServiceNow have partnered to ensure your organization gets the most accurate view of your complete asset inventory, maximizing your investments in Configurations Management Database (CMDB), and bridging the gaps to unify unmanaged, IoT, OT, IT, and cloud assets to support your overall business operations and security.

¹ Techjury
² Statista

Key Takeaways

Unified and enriched real-time asset inventory: The Armis platform enables ServiceNow users to ingest and understand their entire enterprise asset base with the scale to support millions of global assets across all asset classes to include unmanaged, IoT, and OT.

Proactively respond to IoT and OT risk: Expedite and automate maintenance, vulnerability response, and remediation through digital workflows.

Prioritize and prevent threats: Based on business impact to availability/uptime with a single real-time view of all Industrial Control Systems (ICS) security and data risk mapped against NIST, CIS, and MITRE ATT&CK including priority based on active and weaponized exploits.

Centralize visibility: Get a visual map of interdependencies and vulnerabilities mapped across the Purdue Model with geographic and site level view across all IT, IoT, and OT assets.

Unify data silos: Act immediately on real-time data from multiple sources.
The Armis platform has four certified connectors into the ServiceNow platform enabling a real-time continuous de-duplicated feed into the CMDB. They offer a prioritized view on asset health based on NIST, CIS, and MITRE ATT&CK risk scores. They deliver service performance and remediation workflows by linking with SOC/SIEM platforms as well as GRC KPI triggers.

### Armis to ServiceNow - 4 Connectors

1. **Armis ServiceGraph Connector**
   Real-time and de-duplicated discovery against your full device inventory, including cloud workloads, IoT, OT, and unmanaged devices. Tagging metadata in Armis can be passed through the connector to facilitate business service mapping in ServiceNow so that core services can be monitored along with underlying asset health status to signal KPI alerts and remediation to prevent service uptime impacting events.

2. **Vulnerability Response**
   Prioritized vulnerability advice such as the ability to parse millions of assets, tens of thousands of high priority CVSS scores, and received curated remediation advice based on asset criticality including weaponized and executable malware associated at the asset level. This typically results in a manageable list of assets to remediate, freeing up the time of vulnerability remediation security teams so they can focus on the most consequential threats to the service.
3. Security Incident Response

Empowering SOC/SIEM platform teams to accelerate triage, drive threat investigation, containment, and hunts based upon device level incident details such as device type, classification, threats, and vulnerabilities across IoT, and OT/ICS.

4. Incident Integration

The Armis incident integration opens an incident in ServiceNow automatically. Tickets opened by the Armis platform include comprehensive device and incident details such as the device type, classification, threats, vulnerabilities, and more. The Armis platform encapsulates the user’s ticket creation logic and can accommodate unique logic, such as opening an incident ticket that triggers actions like a ServiceNow resolution workflow, a user-specific alert aggregation, or deduplication logic.

Integrations

Armis Vulnerability Manager to ServiceNow Vulnerability Response

The Armis Vulnerability Manager integrates with the ServiceNow Vulnerability Response to provide passive visibility across every asset class including managed, unmanaged, IoT, and OT. This passive capability is particularly useful for IoT and OT environments which cannot be ‘scanned’ with traditional scanning tools as they could disrupt critical services such as healthcare and manufacturing use cases, where understanding asset health and any risks is still mission critical.

The Armis Vulnerability Manager works to identify vulnerabilities at scale (millions of assets) and prioritize curated remediation advice at an asset level, creating time efficiencies when trying to locate assets from a rogue IP address, as priorities are based on what assets have weaponized and executable malware present.

The Armis vulnerability response connector ensures that ServiceNow always has the latest vulnerabilities matched to Armis discovered devices. Armis continuously and passively monitors all network devices in real time to ensure vulnerabilities are correctly matched, allowing ServiceNow to manage downstream remediation workflows and trigger KPI alerts where service uptime could be impacted.
The Armis platform’s cloud-based threat detection engine uses Machine Learning (ML) and Artificial Intelligence (AI) to detect when a device is operating outside of its normal known-good baseline. Deviations could indicate device misconfigurations, policy violations, abnormal behavior such as inappropriate connection requests or unusual software running on a device, or threats that indicate a device has been compromised.

Tickets opened by the Armis platform include comprehensive device and incident details such as the device type, classification, threats, vulnerabilities, and more.
**Key Features**

- Identify and mitigate risks of all devices automatically as they connect to your network, including unmanaged, IoT, OT/ICS, and medical devices.

- Receive additional and contextual information about devices and events from the Armis platform.

- Leverage policy-based actions in the Armis platform to remediate threats and update incidents for greater accuracy and efficiency.

- Import Armis alerts as ServiceNow security incidents.

- Guided setup and embedded help articles that deliver an intuitive user experience.

- Integration dashboards that help contextualize and prioritize alerts from Armis.
About Armis

Armis is the leading unified asset intelligence and security platform designed to address the new threat landscape that connected devices create. Our customers trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in San Francisco, California.

1.888.452.4011 | armis.com

About ServiceNow

ServiceNow (NYSE: NOW) makes the world work better for everyone. Our cloud-based platform and solutions help digitize and unify organizations so that they can find smarter, faster, better ways to make work flow so employees and customers can be more connected, more innovative, and more agile. And we can all create the future we imagine. The world works with ServiceNowTM.

www.servicenow.com