INTEGRATED TECHNOLOGY FROM DRAGOS AND SERVICENOW

Ensure Asset Visibility and Vulnerability Management to Safeguard OT Systems Across Operations

HIGHLIGHTS

- Scale your ServiceNow utilization by easily integrating OT asset details and vulnerability information into new and existing Operational Technology Management deployments.
- Centralized view of ICS/OT environments so you can assess, prioritize and react to events.
- Comprehensive ICS/OT vulnerability management with corrected, enriched, prioritized guidance that allows customers to manage the entire lifecycle of specific vulnerabilities.

OVERVIEW

Security operations require a combination of different technologies to complete the mission of effective threat detection and response. The integration between the Dragos Platform and the ServiceNow® Operational Technology Management Solution now allows users to expand the visibility of OT assets alongside traditional IT assets and provide continuous, automated collection of vulnerability analysis, giving security professionals a comprehensive view of their environment and improved vulnerability management within ServiceNow.

THE CHALLENGE

Having complete asset visibility is an essential step in any cybersecurity program, as defenders first need to understand the environment they are protecting before they can take measures to do so. OT environments are usually separated from IT networks, leading to challenges with typical enterprise security technologies, processes, and staff, as they are not designed to cover the entire IT and OT spectrum.

Furthermore, maintaining accurate asset inventory can be challenging within unique environments, as OT systems are heavily engineered and inextricably tied to specialized machinery, operating with unique protocols and vastly longer lifecycles than IT equipment. Any efforts to introduce automation in support of this activity can prevent costly labor and manual effort keeping track via traditional means (clipboards and spreadsheets).

ServiceNow is widely deployed across enterprise networks, giving IT assets and changes automatic visibility. However, detailed asset inventory is a prerequisite to enabling specific workflows and ticketing functions. Given the complexity and criticality of OT environments, ServiceNow has limited OT assets visibility, reducing available workflows to those systems.

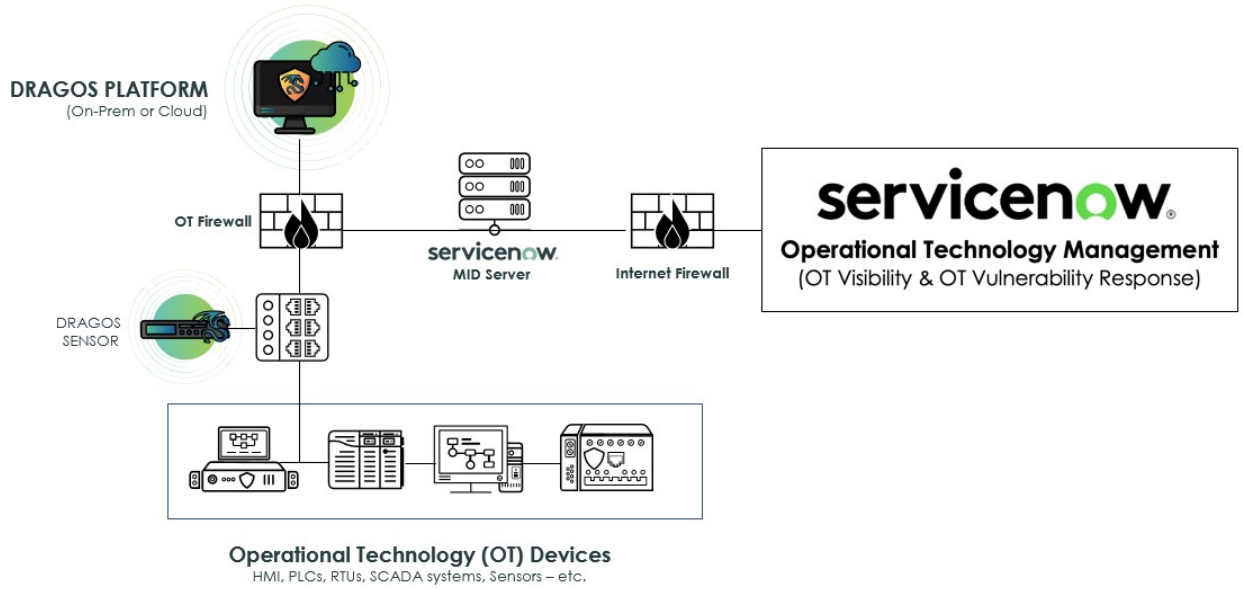
Targeted threats to OT networks are increasing in frequency, sophistication, and severity, further increasing the potential risk to business operations with potentially significant consequences. Therefore, the need to provide security professionals with a complete view of both IT and OT systems is essential for more effective threat detection and incident response.

THE SOLUTION

The Dragos Platform is Industrial Control Systems (ICS) cybersecurity technology that provides comprehensive visibility of an industrial company's ICS/OT assets and the threats they face, with best practice guidance to respond before a significant compromise.

The comprehensive asset inventory within the Dragos Platform can be shared with ServiceNow via an OT Management certified Service Graph Connector integration. This allows customers to utilize the asset visibility of previously unseen OT assets from the Dragos Platform within their existing ServiceNow deployments. Enabling customers to add OT assets to existing workflows, develop new and more informed workflows for OT assets based on specific attributes, further enhancing ticketing functions.

Through the OT Vulnerability Integration, users can now provide corrected, enriched, prioritized guidance that allows customers to manage the entire lifecycle of specific vulnerabilities in their environment, showing historical disposition – through continuous, automated collection and analysis. This includes prioritized guidance with "Now, Next, Never" giving customers the information needed to focus on the highest priority issues to mitigate risk, minimize downtime, and allocate cybersecurity resources where they are most needed.



By integrating the two technologies, customers now have a more complete view of all assets across IT and OT, providing well-established workflows that equate to improved business efficiencies and a more effective response program when performing incident response across both networks.

HOW IT WORKS

Through the integration, users can now visualize their OT environment with their ServiceNow deployment. The Dragos Platform Site Store responds to scheduled queries set by the administrator of the ServiceNow ServiceGraph Connector App, to deliver Asset Information, and related Vulnerability information to the ServiceNow instance, such as Asset Type, Vendor, Model, Addresses (MAC, IP, Hostname), VLAN, Location, Firmware version and Operating System (OS).

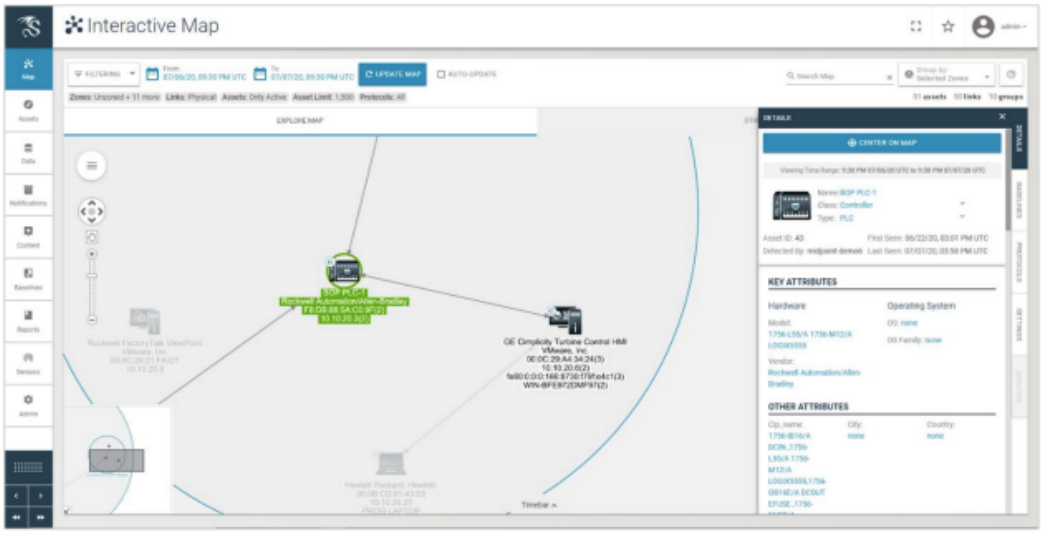


Figure 1. Example of an asset in the Dragos Platform and some of the available attributes.

Once configured, the integration allows the Dragos Platform to automatically synchronize and reconcile assets within ServiceNow per the defined frequency interval providing users with an accurate inventory that can be used to serve many different functions.

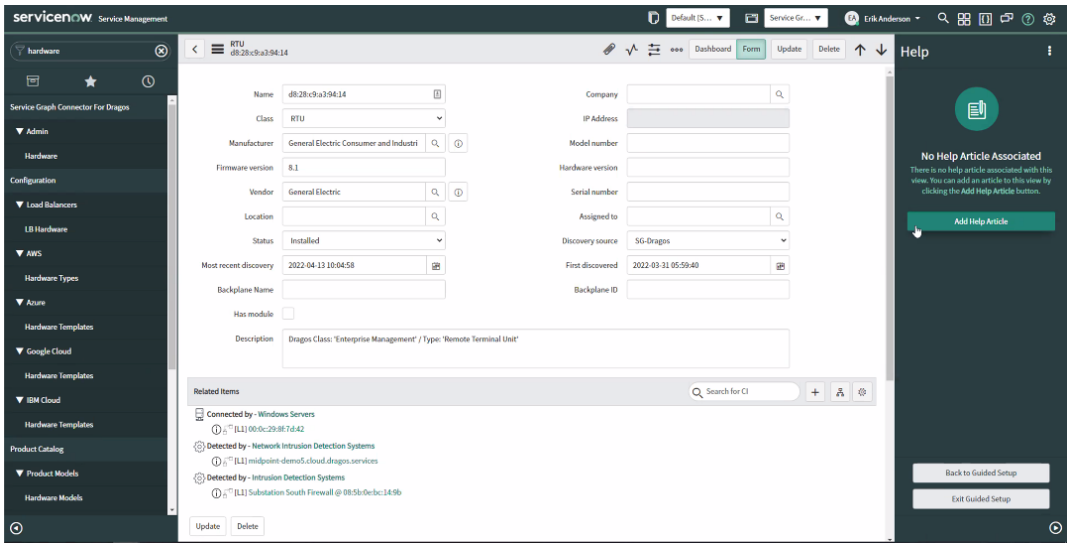


Figure 2. Example of assets and attributes available within ServiceNow..

ADVANTAGES OF THE INTEGRATED SERVICENOW AND DRAGOS SOLUTIONS INCLUDE:

- More accurate asset inventory across IT and OT networks.
- Automatically synchronize assets per defined time interval.
- Continuous, automated collection for ICS/OT vulnerability management analysis with prioritized guidance.
- Enhance or develop new ServiceNow workflows inclusive of important OT assets.
- Enhanced workflows can enable more efficient SOC operations and incident response.

For more info, please visit www.dragos.com/partner/servicenow or contact us at info@dragos.com