carahsoft

FORTINET

Webinar Key Insights: Fortinet & Armis from ServiceNow Better Together

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASPO ValuePoint, GSA, Texas DIR and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Fortinet, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/FortinetResources

Join Events & Webinars:
carah.io/FortinetEvents

Discover Technology Solutions:
carah.io/Fortinet

Learn About Procurement:
carah.io/FortinetContracts

Connect With Our Team:
Fortinet@carahsoft.com
(866) 468-3868

Webinar Key Insights:
Fortinet and Armis from ServiceNow Better Together

Kam Chumley-Soltani,
Managing Director,
OT Security,
Armis from ServiceNow

Benjamin Scott,
National Director, OT & Critical Infrastructure Programs,
Fortinet

1) How do Armis from ServiceNow and Fortinet solutions integrate to protect critical infrastructure?

Kam Chumley-Soltani, Armis from ServiceNow:
"Armis from ServiceNow handles the discovery of every IT, OT, and IoT device, and contextualizes traffic to map communications, behaviors, threats and vulnerabilities. We then send that threat intelligence to Fortinet to automatically block attacks and segment the network."

Benjamin Scott, Fortinet:
"Where Armis from ServiceNow establishes asset intelligence and behavioral context, Fortinet leverages that data to enrich Fortinet security operations and enforce policy across the environment."

2) What are the most overlooked factors to securing smart infrastructure?

Kam Chumley-Soltani, Armis from ServiceNow:
"Whether you are managing urban rails, water utilities or a university campus, foundational security practices such as risk management, network visibility and segmentation apply universally. The biggest blind spot is that smart infrastructure is deeply interconnected, yet the teams responsible for securing these environments often operate in complete silos."

3) Why is collaboration essential for securing IT/OT environments for critical infrastructure?

Benjamin Scott, Fortinet:
"Because everything is interconnected, risk does not stay where it starts - it spreads. Attackers don't respect organizational boundaries. By defending agencies together, we can help prevent risks from spreading."

4) How does the FortiNac fit into the Armis from Service Now & Fortinet Integration?

Kam Chumley-Soltani, Armis from ServiceNow:
"Using Armis from ServiceNow to provide visibility and threat context, we deliver threat identity and association data to each FortiNAC instance. This highlights anomalies like unauthorized code changes, suspicious outbound internet connections and malicious behavior like ransomware or malware, allowing FortiNAC to enforce the appropriate security policies."

Benjamin Scott, Fortinet:
"When integrated, Armis from ServiceNow improves the quality of what the FortiNAC is able to know about an asset, then becomes one of the control points in the environment."

5) What is a growing area of exposure for cyber-attacks on critical infrastructure?

Benjamin Scott, Fortinet:
"In the systems that serve citizens, like water, power and electric utilities, there is a lot of human data. As these systems become more connected, concerns around sovereignty continue to grow. This makes segmentation and visibility increasingly important, as exposure is growing. In today's geopolitical climate, we are seeing more nation-state attacks targeting smaller utilities, as adversaries attempt to gain an initial foothold in these environments to test new capabilities."

6) How much administrative configuration and alert review is required for a single pane of glass approach, in a small to medium organization?

Kam Chumley-Soltani, Armis from ServiceNow:
"The integration itself is easy. To start, you connect Armis to FortiManager using a username and password. From there, Armis sends device IP addresses to FortiManager to enforce firewall policies. This enforcement process can be either manual or automated. You can trigger it manually for a specific device, or you can automate it by creating a custom Armis policy designed to detect specific anomalies, theats or unauthorized behaviors, which will automatically trigger the enforcement of the device's IP address in FortiManager."

7) What do organizations need to overcome the risks of IT/OT convergence?

Benjamin Scott, Fortinet:
"It depends on how an organization works together as a team to connect its systems. A shared understanding of the assets across IT and OT environments is essential because, without shared visibility across systems, organizations become more exposed to cyber threats."

Watch the webinar recording:

Learn More:

Fortinet

(866) 468-3868
Fortinet@carahsoft.com

Armis from ServiceNow

(888) 662-2724
Armis@carahsoft.com