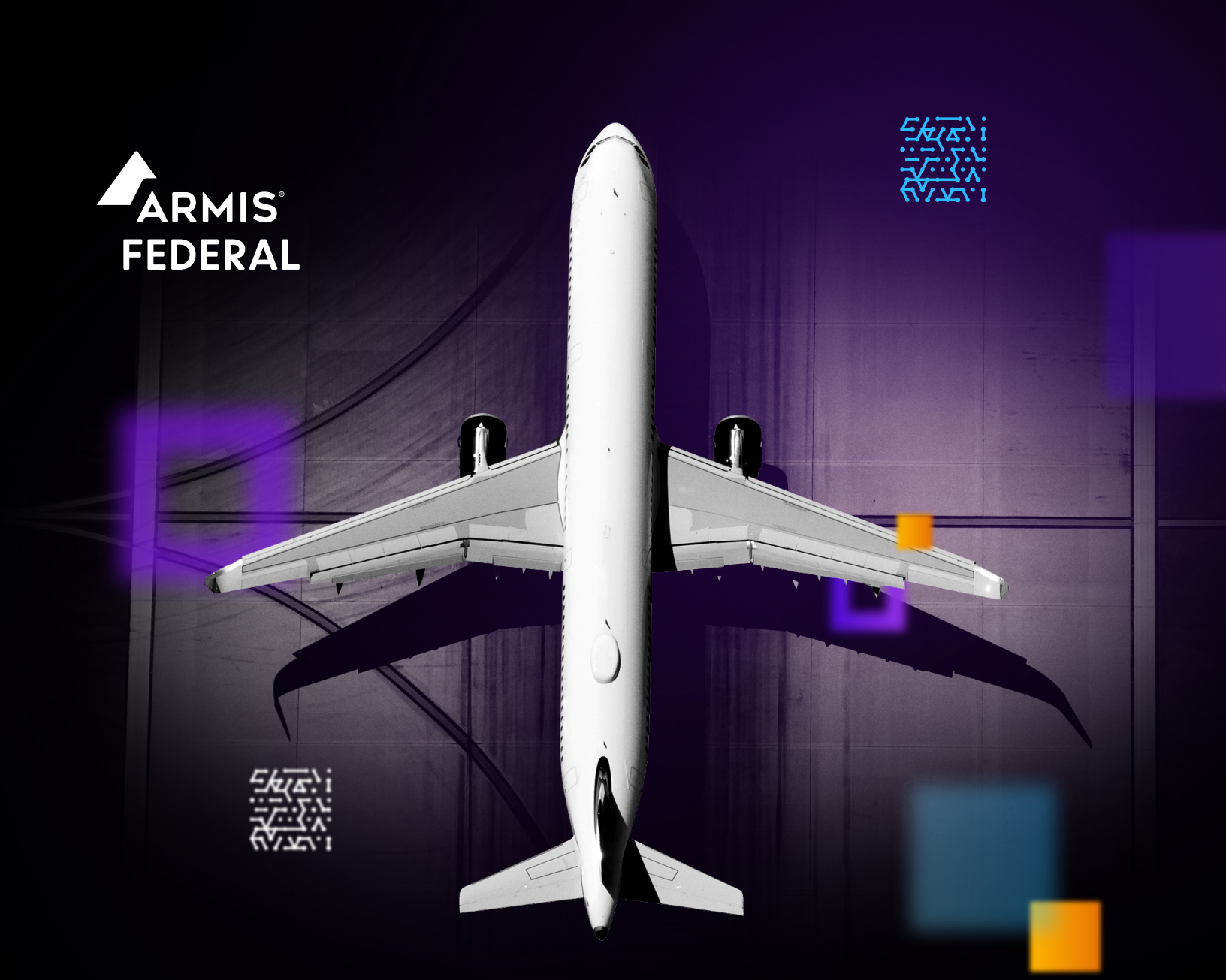
ARMIS®
FEDERAL



WHITE PAPER

Armis Successfully Captures Six of Six Cyber Attacks: Defend the Airport 2025

© Copyright Armis 2026

Defending Critical Infrastructure in an Era of Escalating Threats

The threat landscape facing critical infrastructure in the U.S. has reached a new level of urgency. From water utilities and transportation systems to energy grids and airports, cyber attackers are increasingly targeting the operational technology (OT) systems that underpin public safety and ensure continuity of operations at a national level.

These systems are often interconnected with IT environments, including many devices with limited visibility, expanding the attack surface and opening new pathways for exploitation. Airports, in particular, represent a dense convergence of vulnerable assets, from baggage systems and radar to lighting and fuel control, making them a priority target in both peacetime disruptions and geopolitical conflicts.

The TAC's "Defend the Airport" Simulation

To evaluate real-world readiness, the Technology Advancement Center (TAC) hosted a full-scale, two-day white-hat cyber exercise, titled "Defend the Airport" [DTA]. TAC's model, called Adega Airport, replicated the infrastructure of a modern commercial airport that is co-located with an important military airfield, including systems for security, operations, fuel, and air traffic control. As a defender through the multi-phase DTA exercise, Armis was provided access to the Adega Airport to provide actionable intrusion detection alerts.

The goal was to simulate coordinated cyberattacks against critical airport systems using realistic tactics, techniques, and procedures (TTPs). The exercise brought together leading cybersecurity vendors and government stakeholders to test the strength of their technologies in a live operational environment. Armis participated as a defender, demonstrating the capabilities of its cyber exposure management platform, Armis Centrix™.

Armis Centrix™ delivers:

- Unified visibility across IT, OT, IoT, and unmanaged assets
- Automated risk scoring and prioritization
- Real-time threat detection through behavioral anomaly analysis
- Seamless integration with existing federal cybersecurity toolsets

© Copyright Armis 2026

Realistic Attacks, Real-Time Defense

During the exercise, Armis successfully detected six advanced attacks. The white-hat attacks were led by a former government employee with a sophisticated level of cyber tradecraft. Each exploit simulated how a real-world adversary might attempt to disrupt operations, pivot across systems, manipulate physical infrastructure, and put lives at risk. Here's how Armis responded:

1. "Disabling Security"

The Attack: An attacker compromised an industrial control system to gain unauthorized access to the airport's security gate and video surveillance system. They used a Linux device named "iPad" to perform a port scan and send "Write Commands" to a Rockwell PLC, an industrial control system. This attack could have disabled surveillance cameras and opened security gates.

> **Armis Response:** Armis identified the rogue device as behaving abnormally. Its risk score was immediately raised to critical. Armis flagged the asset.

In an intrusion prevention role, Armis could have prevented further lateral movement, and neutralized the threat before physical access could be fully exploited.

2. "Fuel System Attack"

The Attack: This attack demonstrated a vulnerability in the airport's fuel system. It involved a compromised ECS device named 'aofuelmgr.hnlairport.local' that saw its risk level increase. The attack involved the use of PowerShell and PLC write commands, showing how a malicious actor could have potentially disrupted fuel systems.

> **Armis Response:** Armis detected the communication between the attacker and the fuel manager system and spotted a 5 MB payload delivery.

© Copyright Armis 2026

3. “Cutting the Lights”

The Attack: A sophisticated 18-step attack targeted a workstation tied to the runway lighting system. The attacker found a host vulnerable to the RemoteMouse exploit and ran an ExploitDB payload on that host. They then started a remote PowerShell session to the ALCMS landing lights system and downloaded and ran a program that triggered the landing lights.

> **Armis Response:** Armis detected reconnaissance and deviations from expected network behavior and confirmed remote PowerShell activity in the lighting environment. SECURITY09 and ALCMSENG01 were verified as targeted and flagged as high risk due to the use of deprecated software and hardware. Armis correlated PowerShell process creation with simultaneous HTTPAPI traffic, consistent with the establishment of a remote PowerShell session to ALCMSENG01.

Subsequent use of Armis in an active defense role would have isolated the threat actor before they could trigger disruptions to airfield lighting and endanger incoming flights.

4. “Aquarium Network Breach”

The Attack: The attacker exploited a new access point into the airport’s core network through the untrusted aquarium network. They manipulated aquarium systems by activating pumps without circulation and turning on the water heater, risking harm to the fish and infrastructure. This activity gave the attacker access to the aquarium subnet, which served as a pathway into the airport’s core network.

> **Armis Response:** Armis confirmed that the attacker used the untrusted aquarium network to access the airport core. It identified critical systems, including the aqmonitor Raspberry Pi, acqeng Windows workstation, and industrial control devices, as compromised. Suspicious DNS queries linked to a web shell indicated the persistence of the attacker. Armis also detected multiple Linux vulnerabilities and mapped the network path from the aquarium subnet to core systems.

In an active Armis deployment, this would have enabled responders to remove the compromised asset before cascading effects could develop.

© Copyright Armis 2026

5. "Taking Down Baggage"

The Attack: A sophisticated 24-step attack targeted the baggage system. The attackers used gobuster to enumerate directories, exploited phpMyAdmin to gain elevated privileges, uploaded socat to the compromised web server to enable SSH access to the process historian, proxied connections from the historian to the baggage handler using socat, and executed a baggage payload that routed through the new SSH channel to the baggage handler. This would have allowed the attacker to disrupt baggage processing, cause delays or lost luggage, and potentially pivot further into critical airport systems.

> **Armis Response:** Armis confirmed SSH access to attacker-controlled hosts and victim systems and identified compromise of the Guest WiFi boundary used for initial access. The platform detected extensive network reconnaissance, observed suspicious file download activities that elevated multiple device risk scores to 100, and recorded access to critical systems including the process historian and the baggage handling environment.

Leveraging Armis in an actual deployment would have allowed the security team to respond immediately.

6. "Blinding the Radar"

The Attack: This most serious scenario involved compromising a device to impersonate a legitimate network service. The attacker used a Linux device named 'activedirectory' to perform an ARP poisoning attack and sent PLC write commands directly to the radar dish.

> **Armis Response:** Armis flagged the spoofed service through anomalous communication patterns and multiple alert triggers, and immediately identified and alerted the security team on the critical activities, including the ARP poisoning attack, providing the necessary visibility to protect air traffic control systems.

In a real deployment, the attempted man-in-the-middle attack would have been contained by Armis before any radar data could be redirected.

"At TAC, we are committed to fostering collaboration that strengthens the cybersecurity of our nation's critical infrastructure," said Alexis Davis, Chief Operating Officer at TAC. **"During our recent Defend the Airport 2025 exercise, we were impressed by the ability of Armis to detect and remediate every attempted exploit against airport defenses, across both IT and OT devices."**

© Copyright Armis 2026

Armis Centrix™: Delivering Unified Visibility and Control

The strength of Armis' response lies in **Armis Centrix™**, the cyber exposure management platform purpose-built for complex, asset-rich environments. Powered by a global **AI-based Asset Intelligence Engine** that monitors over 6 billion devices, Armis Centrix™ demonstrated:

- **Comprehensive device visibility** and behavioral context
- Dynamic risk scoring for **effective prioritization and response**
- **Granular, early threat detection** with network traffic inspection and anomaly detection
- **Prevention of lateral movement** and further risky communication
- **Isolation and segmentation** without downtime
- **Real-time alerting for a rapid response**

In this exercise, Armis Centrix™ provided a reliable and aggregated source of truth for defenders navigating the IT/OT convergence, enabling them to take timely and precise action against multi-vector threats. It also exposed how attacks on IT systems—like guest Wi-Fi or domain controllers—can be used as springboards into OT environments. Armis neutralized these "IT-to-OT" jumps in real time, demonstrating the necessity of unified asset intelligence in securing modern infrastructure.

A Proven Partner for Federal Cybersecurity

As the risks to national infrastructure continue to grow, Armis remains committed to supporting federal agencies with the tools and intelligence needed to protect mission-critical environments. The "Defend the Airport" exercise validated that securing infrastructure from "tarmac to terminal" requires more than reactive tools. It demands continuous, contextual awareness and an integrated approach to defense.

Armis stands ready to help federal partners monitor, secure, and harden the systems that keep the country running, no matter where the next threat emerges.

© Copyright Armis 2026

ARMIS®
FEDERAL

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.

armisfederal.com

888.452.4011

in

Armis Centrix™ is a FedRAMP and IL authorized solution for the U.S federal government.

© Copyright Armis 2026