PROTECTING U.S. CRITICAL INFRASTRUCTURE

The government has put our nation's critical infrastructure operators on alert.

As tensions between Russia and the rest of the world heighten with the invasion of Ukraine and the economic sanctions against Russia, the Biden Administration is warning of potential cyberattacks against U.S. organizations. In the past year, cyberattacks from Russian hackers have crippled critical infrastructure organizations – the upcoming anniversary of the Colonial Pipeline attack and the recent indictments by the Dept. of Justice regarding Russian hacking actors is a sobering reminder that these warnings should be taken seriously!

The increase in cyber-physical devices – managed and unmanaged connected to enterprise networks along with interconnectivity between networks is at an all-time high. IT/OT systems convergence has become the norm. A cyberattack could endanger citizens through the operational downtime in lifeline services such as water, power, communications, financial services, and healthcare services.

As a result, the Cybersecurity & Infrastructure Security Agency (CISA) has organized a repository of advisories, guidance, services, and response processes as part of the Shields Up initiative. Specific CISA recommendations include actively hunting for Russian tactics, techniques, and procedures (TTPs) within your networks, watching for any anomalous behavior in ICS/OT devices, and keeping reporting thresholds low to promptly share threat intelligence with other organizations.

Critical infrastructure in the U.S. is an attractive target for Russian hackers as non-kinetic disruption is the new goal — the greater the impact, the greater the chance of creating chaos in the daily lives of civilians. The private sector maintains the majority of the nation's critical infrastructure. Within many of these organizations there exists a "visualization gap" where IT and security leaders cannot see all of the vulnerable assets within their environment.

Even if an organization isn't the direct target of a cyberattack, networks, and devices might be affected or have vulnerable devices co-opted into botnets and used as part of a DDoS cyberattack against critical infrastructure targets. Organizations need to strengthen their cybersecurity postures to withstand these cyberattacks with clear situational awareness of their risks, interconnected assets, IT governance, and response plans.

Armis is committed to working with our public and private sector customers and partners to provide responsive and transparent collaboration, closing the visualization gap with complete visibility of every asset so every organization can be protected. We agree with CISA recommendations and can help with a structured defense-in-depth response in the following areas:

We agree with CISA recommendations and can help with a structured defense-in-depth response in the following areas:

- **Asset Visibility –** Armis sees and identifies every asset for 100% complete visibility: across IT/OT/IoT/IoMT managed and unmanaged assets both on the network and in the cloud. This eliminates the visualization gap.
- **Risk Assessment –** Armis can help you map out the devices and applications in your environment, identify the specific devices requiring further review (e.g., confirming exact software versions), and zero in on configurations or deployments potentially impacted by such exposures.
- **Threat Assessment –** Armis researchers continuously develop queries that will quickly identify active attempts to exploit flaws so that you may isolate or quarantine vulnerable systems and initiate patching efforts.
- **Protect Your Environment –** Isolate vulnerable systems and initiate patching efforts. Next, deploy active asset management and security to manage them continuously. Armis easily integrates with your existing security and management tools and provides an extra layer of knowledgebase that can detect and respond to exploits.

We'll help you Identify all assets connected to critical infrastructure and determine what assets in your environment are vulnerable to confirm potential exposure to threat. Armis can help you map out assets and applications, identify the specific assets requiring further review (e.g., confirming exact software versions), and identify configurations or deployments potentially impacted by such exposures.

Let Armis help discover, control, protect and strengthen your asset security in light of increased global tensions and cyber threats to our nation's critical infrastructure.

To learn more or see a demo, contact us today!

Armis - **armis.com/contact-us**

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies 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 Palo Alto, California.

armis.com

ARMIS.