CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

Complimentary SHIELDS UP support for energy, pipeline transportation, marine port, water, and wastewater organizations

An unprecedented situation

Geopolitical instability associated with the Russian invasion of Ukraine, combined with U.S. and North Atlantic Treaty Organization (NATO) aid to Ukraine defense efforts, have elevated the possibility of cyberattacks against critical infrastructure in the U.S. and NATO countries. The potential attack surface across the U.S. alone is enormous and includes critical infrastructure supporting:

- **55,000 substations across the electric grid**
- **360 commercial maritime ports**
- **2.6 million miles of pipeline**
- **14,000 wastewater treatment plants serving 240 million people**

The challenge

When you add NATO member critical infrastructure numbers to those of the U.S., Russian or state-sponsored threat actors have vast opportunities for causing disruption or chaos. In the U.S., the Cybersecurity and Infrastructure Security Agency (CISA) has indicated that attacks on Ukraine allies are likely to increase throughout 2022 as regional hostilities grind on. Given the unprecedented situation, it's paramount that every critical infrastructure Particularly those that are

Armis CIPP at a glance

Key Capabilities

- Map your IT and OT asset inventory and continually monitor asset behavior
- Assess risks to critical infrastructure with contextual asset intelligence
- Rely on near real-time alerts for threats and exploits
- Engage with Armis CIPP service partners who can rapidly utilize Armis intelligence data to provide recommended policy changes, incident response, operational management, and remediation.

defined as Systemically important Critical Infrastructure (SICI) and Systemically Important Entities (SIEs) in the U.S. and NATO countries be able to answer critical questions:

- **What is connected to my network?**
- **What are these devices doing while connected?**
- **Is my IT infrastructure an avenue to my OT operations?**
- **Are there active exploits crossing my enterprise?**
- **What is the risk posture of our devices and our organization?**
- **How safe is our critical infrastructure?**
- **Do I have critical vulnerabilities within my OT network?**

The solution

Specifically designed to meet the needs of critical infrastructure organizations, and in conjunction with specialist services partners and select system integrators like Kroll, Armis has launched the Critical Infrastructure Protection Program (CIPP). Through its ability to shine a light on invisible unmanaged and managed assets, CIPP helps eliminate the risks of the unknown within our critical infrastructure.

CIPP is for at-risk organizations in the U.S. and NATO aligned countries and includes three (3) months of complimentary access to the Armis unified asset intelligence platform and services. CIPP has been specifically designed to service the needs of the CISA critical infrastructure sectors: energy, pipeline, marine ports, and water and wastewater.

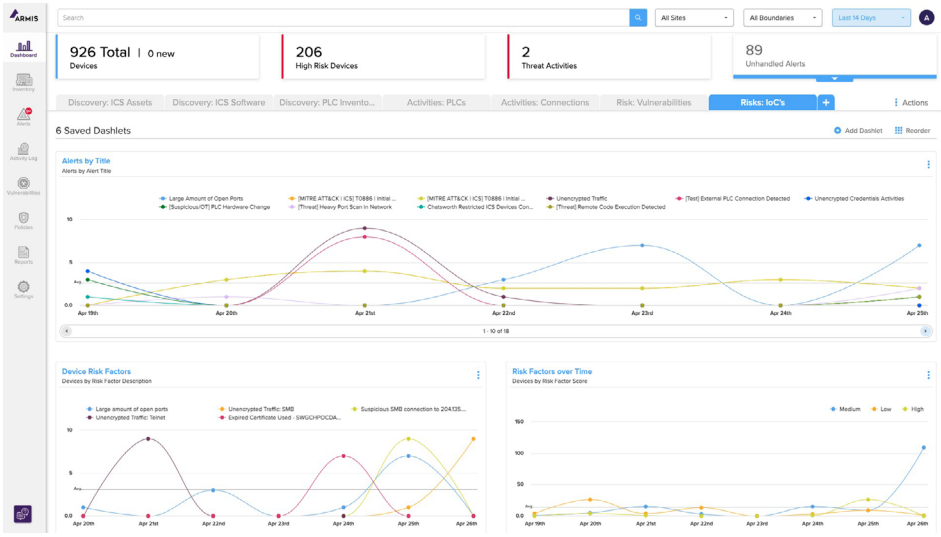

Figure 1: The Armis Platform shows you the big-picture view of enterprise assets and enables you to drill down into the details of each individual asset, including indicators of compromise.

What's included?

- 3 months complimentary of the Armis Platform
- Operational Technology (OT) Policy Library
- One collector for passive network traffic analysis within IT or OT segments
- Vulnerability, threat detection and threat intelligence engines
- Armis Security Architect and Deployment Manager
- Access to the Armis partner community, including Kroll, for detection, incident response, and forensic services
- CIPP also includes pre-built integrations into existing security platforms such as scanners, firewalls, NACs, and xDR solutions, to compound overall efficacy of enterprise protection.

What you can expect

- Expose the unknown
- Understand risk
- Device connection study report
- Segmentation and boundary analysis
- Software and hardware gap analysis
- Compliance support
- Automated threat responses
- Advanced reporting and analysis
- Timely response to threat activities and incident response

Sign up now

For more details, send an email to:

cipp@armis.com

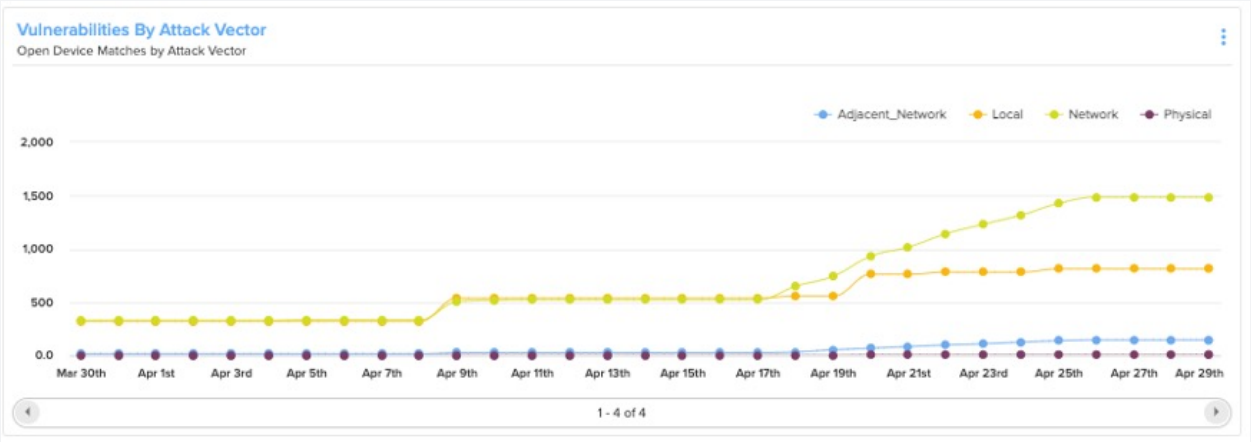

Figure 2: Intelligence from the Armis platform enables you to focus efforts on attack vectors.

Gain complete visibility into OT and IT assets

The Armis platform performs continuous, non-invasive monitoring of every wired and wireless OT and IT asset in your environment. The platform:

- **Monitors devices communicating in the airspace via peer-to-peer protocols, which are invisible to traditional security products.**
- **Protects your business from disruption by relying on the world's largest crowd-sourced, device behavior knowledgebase to detect threats with a high degree of accuracy.**
- **Enables you to automatically disconnect or quarantine devices operating outside of "known-good" baselines.**

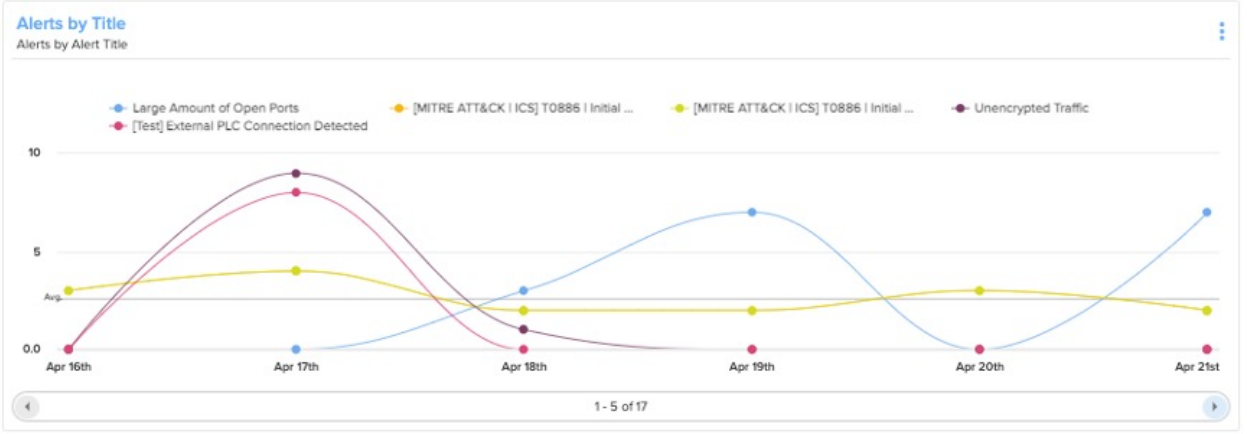

Figure 3: Track specific alerts and Indicators of Compromise by Alert Type.

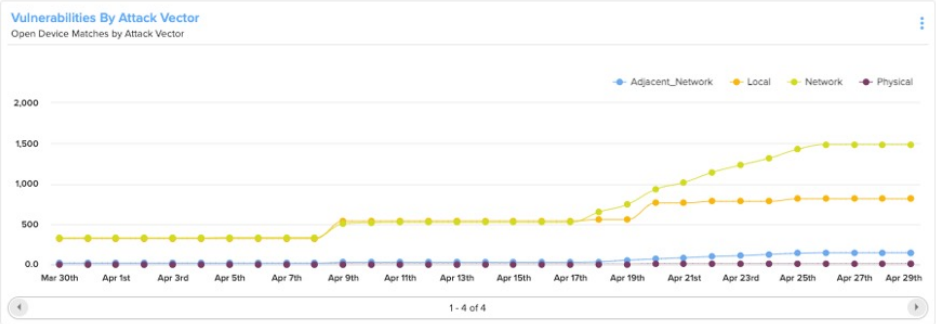

Figure 3: Track specific alerts and Indicators of Compromise by Alert Type.

Follow SHIELDS UP guidance more easily

The Armis platform performs continuous, non-invasive monitoring of every wired and wireless OT and IT asset in your environment. The platform:

- **Expose the unknown – Full inventory of all wired and wireless devices connecting to the critical infrastructure and operational collaboration with a solution that gives you real-time situational awareness about your total environment**
- **Understand risk – Full device risk analysis, including vulnerability and behavioral analysis**
- **Device connection study report – Expose vector of attack with device connectivity and interdependency mapping**
- **Segmentation and boundary analysis – Actionable analysis to fortify boundaries and eliminate unauthorized connections**
- **Software and hardware gap analysis – Understand hidden software and hardware gaps and risks**
- **Compliance support – Documentation and intelligence to comply with NERC-CIP, NIST, NISTIR 8228, and other compliance and regulatory requirements**
- **Automated threat responses – Alerts of real-time threats and exploits forwarded to your SIEM, SOAR, or xDR solution**
- **Advanced reporting and analysis – Reports to satisfy compliance, regulatory, and auditing requirements**
- **Timely response to threat activities and incident response**

Learn more or request access to Armis CIPP by emailing cipp@armis.com

202200516-1

The Armis advantage

Comprehensive
Discover and classify all devices on your networks.

Agentless
Nothing to install, no configuration or asset disruption.

Passive
No device scanning or network impacts.
.

Frictionless
Installs in minutes using existing infrastructure.

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 assets across IT, Cloud, IoT devices, medical devices (IoMT), operational technology (OT), industrial control systems (ICS) and 5G. 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. Visit www.armis.com.

armis.com

1.888.452.4011

ARMIS