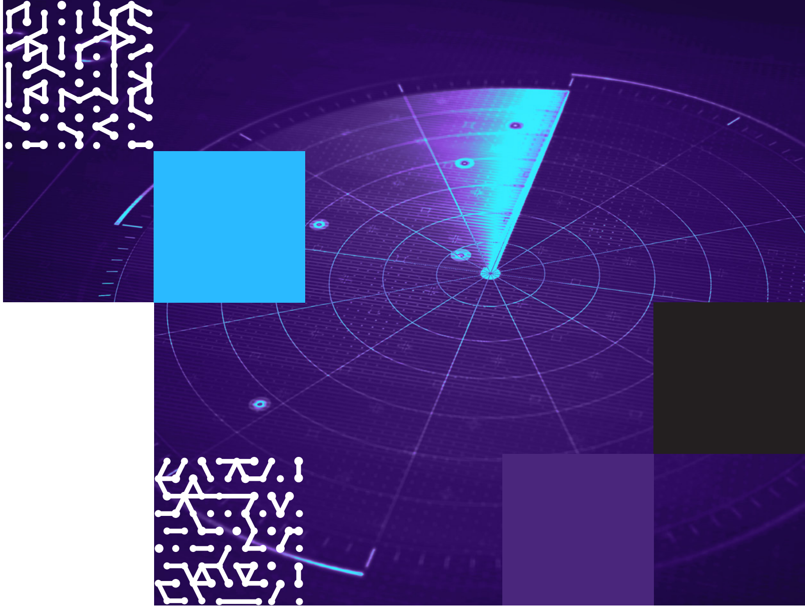
ARMIS

Armis Centrix™ Feature | **Traffic Anomaly Detection**

Dynamic, AI-driven anomaly detection powered by the world's largest aggregated asset intelligence dataset



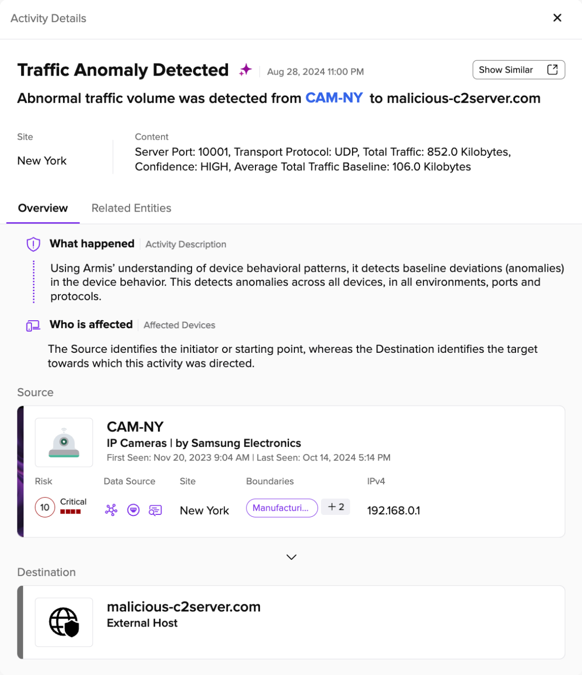
Eliminate the Noise of Alert Fatigue and False Positives, to Focus on Anomalies That Really Matter

Imagine if you could detect malicious behaviors at their most subtle, granular level before they become a wide-scale attack. Armis Centrix™ provides a more accurate, intelligence-driven approach to aggregated anomaly detection that ensures you are always one step ahead of potential threats.

Detect Early Indications of Cyber Attacks with Confidence

Modern cyberattacks are increasingly sophisticated and involve multiple stages. Anomaly Detection can help uncover these complex attack patterns that traditional signature-based detection might miss. Anomalies can indicate the presence of a suspicious or malicious event that is not yet known to the wider community.

Armis Centrix™ has a cloud-based threat detection engine, using machine learning and artificial intelligence to detect when a device is operating outside of its "known good" baseline. Our multi-detection technology supports both anomaly detection and policy-based detection for more comprehensive protection. Monitor any device's communication in your environment and respond quickly and effectively to suspicious deviations.



Activity Details ✕

Traffic Anomaly Detected ✦ | Aug 28, 2024 11:00 PM — Show Similar

Abnormal traffic volume was detected from CAM-NY to malicious-c2server.com

Site: New York

Content: Server Port: 10001, Transport Protocol: UDP, Total Traffic: 852.0 Kilobytes, Confidence: HIGH, Average Total Traffic Baseline: 106.0 Kilobytes

Overview | Related Entities

What happened | Activity Description

Using Armis' understanding of device behavioral patterns, it detects baseline deviations (anomalies) in the device behavior. This detects anomalies across all devices, in all environments, ports and protocols.

Who is affected | Affected Devices

The Source identifies the initiator or starting point, whereas the Destination identifies the target towards which this activity was directed.

Source

CAM-NY
IP Cameras | by Samsung Electronics
First Seen: Nov 20, 2023 9:04 AM | Last Seen: Oct 14, 2024 5:14 PM

Risk	Data Source	Site	Boundaries	IPv4
10 Critical		New York	Manufacturi... +2	192.168.0.1

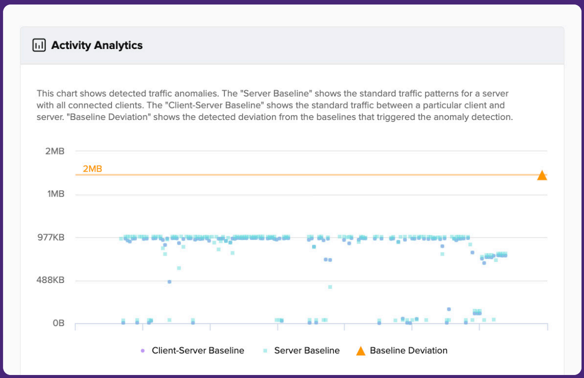
Destination

malicious-c2server.com
External Host

Anomaly Detection Use Cases:

Accurate Threat Detection

Detect behaviors as suspicious based on the source and destination, as well as the total traffic that was detected. Multi-detection engine and artificial intelligence (AI) threat detection models streamline alerts to focus efforts on abnormal behaviors.



Activity Analytics

This chart shows detected traffic anomalies. The "Server Baseline" shows the standard traffic patterns for a server with all connected clients. The "Client-Server Baseline" shows the standard traffic between a particular client and server. "Baseline Deviation" shows the detected deviation from the baselines that triggered the anomaly detection.

Early Threat Hunting

Look for anomalies from an external host or source, which can represent bad actors trying to gain access to internal devices prior to the identification of a unique threat signature. Quickly identify and action anomalous behavior for consistent protection. Detect and report on Detect and report on common MITRE Tactics, Techniques, and Procedures (TTPS) such as Initial Access, Exfiltration, Command and Control, Collection, Discovery, Lateral Movement, and Impact.

Actionable Alerts

View detailed information on each device, including its normal behavior and expected business usage. Enhance anomaly detection by eliminating alert fatigue and false positives and focus on meaningful anomalies and risky events across all devices.

See, **protect**, and **manage** your entire attack surface

Visit **Armis.com** to find out more

How It Works

Armis Centrix™ establishes a baseline of network traffic data over an average period of six months. Baselines are established for client-server pairs and devices with all hosts. Known and Unknown hosts are compared against the behavioral baseline to identify any anomalous activity. Multiple detection models are compared and aggregated to confirm potential threats with certainty. Traffic volume spikes are flagged and alerted for rapid response and mitigation.

Other key features that make Armis the go-to platform for threat detection, prevention and exposure management:

Dynamic Baselines

Device-specific baselines are typically established over six months to reduce noise of repetitive but infrequent behaviors. New behaviors are taken into account, alerted on, and incorporated into the baseline over time.

Asset-Centric Behavior Monitoring

An asset-centric approach linked to device identifiers for a consistent behavioral profile over time. Monitor and analyze device traffic from various parameters such as traffic volume and destination.

Confidence Scoring

View only the most accurate, prioritized results to eliminate alert fatigue and reduce noise. Confidence scores are assigned to filter on already high confidence detections.

Dashboards and Interactive Analytics

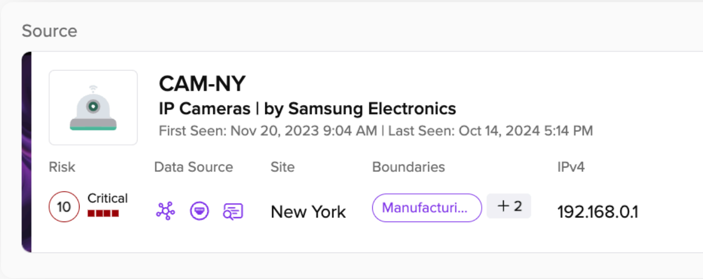
Powerful visualization capabilities for reports and dashboards. Manage activity analytics graphics and drill down into anomalous communications for full behavioral insights.

Armis Asset Intelligence Engine

Core to Armis Anomaly Detection is our Asset Intelligence Engine. It is a giant, crowdsourced, cloud-based device security data lake—the largest in the world. It includes over 5 billion devices, roughly 20% of the devices connected to global networks.

Each profile includes unique device information such as how often each asset communicates with other devices, over what protocols, how much data is typically transmitted, and more.

These asset insights enable Armis to classify assets and detect threats with a high degree of accuracy. When an asset operates outside of its "known-good" baseline, Armis issues an alert or can automatically disconnect or quarantine an asset.



Source

CAM-NY

IP Cameras | by Samsung Electronics

First Seen: Nov 20, 2023 9:04 AM | Last Seen: Oct 14, 2024 5:14 PM

Risk	Data Source	Site	Boundaries	IPv4
10 Critical		New York	Manufacturi... +2	192.168.0.1

With Armis Centrix™, achieve **more precise anomaly detection** with always-on awareness and dynamic device baselines.

View actionable and contextual alerts enhanced by the details of your own environment to detect threats early and focus efforts where they matter most.

See, **protect**, and **manage** your entire attack surface

Visit **Armis.com** to find out more