Bastille

EXECUTIVE SOLUTION BRIEF

Bastille Airspace Defense Analytics Module (ADAM)

Overview

Bastille's **Airspace Defense Analytics Module (ADAM)** enhances enterprise security by detecting, analyzing, and responding to wireless threats in real time. ADAM leverages Bastille's 100% passive radio frequency (RF) monitoring to provide continuous visibility into wireless device activity. This capability enables organizations to detect anomalies, enforce policies, and mitigate risks associated with rogue or compromised devices. ADAM is an advanced analytics engine that processes real-time wireless observations, providing a holistic security view beyond traditional cybersecurity defenses.

Key Capabilities

- **Wireless Threat Detection & Analysis:** ADAM takes a proactive approach, continuously scanning RF emissions to detect unauthorized wireless activity. It identifies unauthorized devices, rogue access points, compromised Bluetooth connections, and suspicious behaviors such as MAC spoofing, connections bridging the facility's perimeter, and unexpected network activity. This proactive stance ensures that organizations can identify and address potential threats before they can cause harm.
- **Real-Time Wireless Inventory:** ADAM continuously catalogs wireless devices in the environment. It detects and updates the inventory for every wireless device in real time. Analysts can review this information in the Inventory Dashboard, which provides a comprehensive view of all wireless networking devices in the environment and allows operators to investigate device behavior from a central location.
- **Policy-Based Threat Evaluation:** Organizations can configure ADAM with tailored **threat policies** to monitor for specific security conditions. These policies define which behaviors, devices, or networks are potential threats, ensuring that only relevant security events trigger alerts.
- **Real-Time & Historical Investigation:** The Findings Dashboard provides security teams with an intuitive interface for examining current and historical security events. It allows them to filter incidents by severity, protocol, device type, location, and time, facilitating rapid threat investigation.
- **Event-Driven Incident Response:** ADAM enables security personnel to investigate, adjudicate, and annotate findings, expediting response workflows. It also allows teams to prioritize incidents based on severity, ensuring quick mitigation of high-risk threats.
- **Integration & Automation:** ADAM seamlessly integrates with other security products using Bastille's open API and webhooks, facilitating automated security responses and interoperability with third-party security information and event management (SIEM) platforms, network monitoring tools, and compliance reporting solutions.

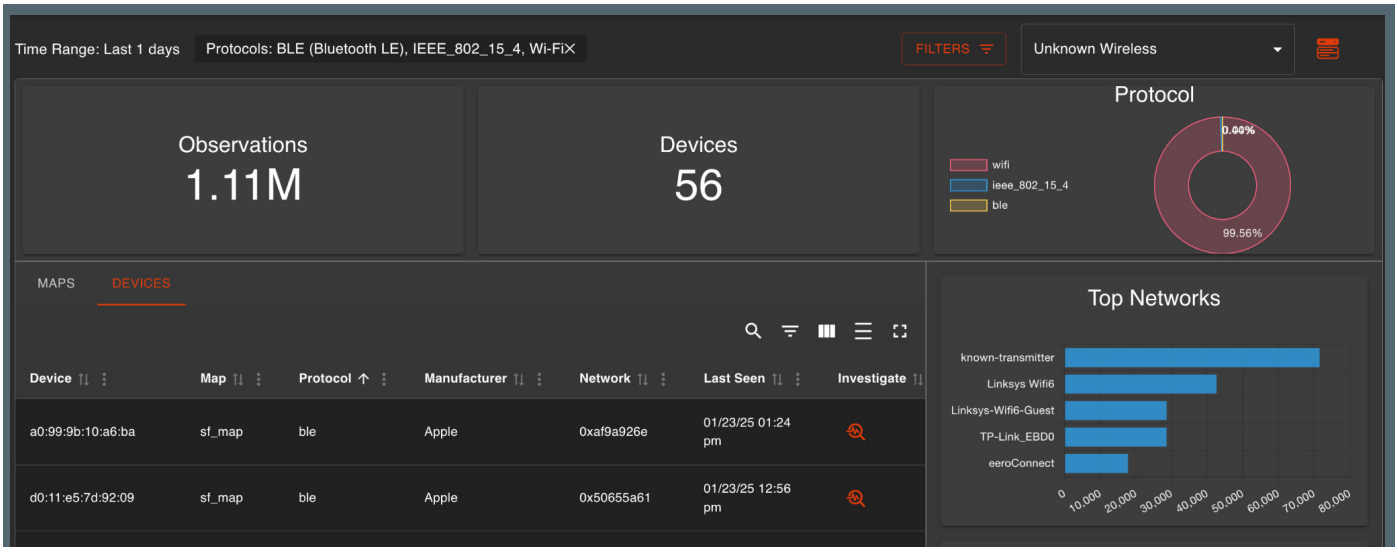

Figure 1: ADAM Interface

How ADAM Works

- **Wireless Data Collection:** ADAM ingests RF emissions from Bastille's proprietary sensor network, which covers a frequency range of 25 MHz to 7.125 GHz.
- **Threat Analysis:** ADAM evaluates real-time wireless observations using machine learning algorithms and predefined security policies. It detects unauthorized network changes, signal spoofing, and suspicious device behavior.
- **Automated Findings:** When security concerns are detected, ADAM generates findings categorized by severity, type, and location. It automatically highlights abnormal patterns in device behavior, location, encryption, etc.
- **Security Event Management:** The dashboard visually represents findings, which security teams can use to analyze threat trends, search for specific devices, and correlate events over time.
- **Incident Investigation, Adjudication, and Resolution:** ADAM enables security teams to investigate, classify, and act on findings by assigning threat levels, adjudicating risks, and integrating results into existing security operations.

Benefits

- **Enhanced Wireless Security:** ADAM detects and responds to RF-based threats invisible to traditional security tools such as firewalls, endpoint protection, and intrusion detection systems.
- **Operational Efficency:** ADAM reduces investigation time through automated findings, event filters, and intuitive security workflows, allowing security teams to focus on high-priority threats.
- **Seamless Integration:** ADAM supports multiple formats for third-party integration, including an open API and JSON webhooks, ensuring compatibility with enterprise security tools.
- **Regulatory Compliance Support:** ADAM provides detailed logging and reporting capabilities for industries with stringent compliance requirements, including government, healthcare, and financial sectors.

Sample Use Cases

Enterprise Airspace Protection

ADAM safeguards enterprises from unauthorized RF activity, preventing rogue access points, device spoofing, and illicit surveillance attempts.

Data Center Security

ADAM helps colocation and cloud data centers enforce strict wireless security policies by detecting unauthorized wireless devices that could compromise essential equipment.

Critical Infrastructure Defense

ADAM supports essential industries, such as energy, oil/gas, water, manufacturing, and telecommunications, by identifying and mitigating threats targeting wireless-connected assets in high-security environments.

Government & Military Security

ADAM can detect wireless threats in sensitive and classified environments, making it an essential tool for national security applications.

Figure 2: ADAM Interface

Conclusion

Bastille's Airspace Defense Analytics Module (ADAM) is a robust analytics engine that gives organizations deep visibility into their wireless environment. It offers real-time monitoring, advanced threat intelligence, and actionable security insights. By detecting unauthorized wireless activity and integrating with existing security operations, ADAM ensures robust protection against evolving RF-based threats. Its ability to analyze, categorize, and mitigate wireless threats positions it as an essential tool in modern cybersecurity strategies.

As wireless attack surfaces expand, organizations must stay ahead of adversaries by leveraging AI-driven analytics, continuous monitoring, and proactive threat mitigation. ADAM provides unparalleled visibility into RF activity, streamlines security workflows, enhances compliance efforts, and integrates seamlessly with broader cybersecurity ecosystems.

With ADAM, enterprises can move beyond traditional security postures, adopting a proactive and intelligence-driven approach to wireless security. Whether securing corporate environments, data centers, or critical infrastructure, ADAM delivers real-time situational awareness and automated threat detection to protect against modern RF-based threats.

Bastille

About us

Bastille specializes in providing security solutions for wireless environments. Bastille uses a network of Software-Defined Radios (SDRs) to continuously monitor a facility's entire wireless environment, including cellular, Bluetooth Classic, Bluetooth Low Energy (BLE), Wi-Fi, Zigbee, and other protocols. Our sensors detect, analyze, and localize transmissions in real time, providing a comprehensive view of wireless activity.

Bastille's system goes beyond just identifying signals; it analyzes data to uncover real-time and long-term threats. By capturing the entire wireless spectrum, Bastille offers unparalleled visibility into potential security risks, empowering organizations to proactively safeguard their wireless infrastructure.

Learn more

To learn more please visit
www.bastille.net

or follow us on