Bastille

EXECUTIVE SOLUTION BRIEF

Continuous TSCM

Protecting Against Technical Surveillance

Technical Surveillance Countermeasures (TSCM) involves a comprehensive, systematic approach to discovering, pinpointing, and neutralizing harmful surveillance devices whose primary purpose is to capture and transmit/export sensitive data.

Bastille offers real-time, continuous radio frequency (RF) signal monitoring, crucial for modern surveillance detection. It detects, classifies, and locates unauthorized surveillance devices swiftly, integrating seamlessly into TSCM efforts for a more proactive security approach. Additionally, Bastille's ability to analyze historical RF data helps identify patterns that may indicate sustained surveillance efforts, making it a vital tool for securing sensitive information against complex threats.

Wireless Threats

Wireless threats are evolving rapidly, just like network-borne vulnerabilities and malware. However, they have a distinct advantage over network-centric attacks: wireless threats are not detectable on managed networks. They may exfiltrate data out-of-band from the complex firewall, intrusion detection, and malware scanning systems on the physical network. You must continuously monitor for threat activity to ensure your physical space is free of unknown wireless threats.

Wireless threats manifest themselves in forms such as:

- Rogue Wi-Fi access points and data ex-fil devices
- Rogue video and still-image cameras
- Bluetooth-based data harvesting devices
- Cellular voice, data and video ex-fil devices, which can bridge physical networks
- Industrial Control System jammers, blockers and signal interfering devices

These threats can compromise the security of the spaces where you hold sensitive discussions, process critical information, or have compliance obligations on securing the wireless airspace.

Threats Are Evasive

Wireless devices used for eavesdropping or data exfiltration would be ineffective if they were easy to find. They often attempt to avoid detection by transmitting during busy times (to blend in) or off-hours (fewer observers). A continuous monitoring TSCM system will detect threat devices whenever they transmit.

Threats Are Camouflaged

Advanced data exfiltration threat devices look precisely like cables and components typically present in your facility. The only way to detect the threat is to monitor the wireless spectrum for transmissions that violate security policy. Physical inspection cannot identify these threats.

EXAMPLE

The O.MG Cable™

The O.MG Cable hacking tool looks precisely like standard vendor-issued cables. It includes a miniature computer, controllable by Wi-Fi, that can gather and exfiltrate all the data that it sees, including logging keystrokes. These cables are undetectable unless you are scanning for wireless activity. Like many others, they are broadly available online and cost around one hundred dollars. Multiple customers have reported finding O.MG Cables using Bastille's solution.

Figure 1: O.MG Cable

EXAMPLE

Cellular Listening Device

Miniature eavesdropping devices that transmit using traditional cellular services can be placed or disguised nearly anywhere in your environment and relay sensitive audio and video anywhere in the world. Detecting these devices requires a continuous monitoring system to identify all cellular transmissions and devices with unusual behaviors.

In some cases, the device isn't anything more than a cellphone. Someone "accidentally" leaving it behind in a conference room with plausible deniability may be just as damaging as a well-placed espionage device.

Threats Built On Connectivity

Cellular data networks have expanding convenience and access for their users. However, they also allow for rapid data exfiltration without any inspection by the layers of firewalls and traditional security tools employed by security administrators. It takes only seconds for a picture taken on a cellular phone to synchronize with a cloud service. The same is true for a video recording or corporate data accessed by a phone.

Intelligent Wireless Threat Security

To detect these wireless threats and enable a modern security policy, an improved approach to cloud infrastructure security is required. This refined approach is:

- Intelligent
- Comprehensive
- Integrated
- Future Focused

Bastille Networks makes this refined approach available.

Bastille Solution

The Bastille solution combines Sensor Arrays deployed throughout your facility with the supporting infrastructure to collect, demodulate, and store RF data.

Sensor Arrays

Bastille Sensor arrays are deployed in a grid pattern and constantly sweep a broad frequency range. Signals are collected, demodulated, and analyzed.

Figure 2: Sensor Array

Fusion Center

Bastille's Fusion Center platform is an AI/ML-based intelligence engine that allows for the localization of RF signals and the detection of threats.

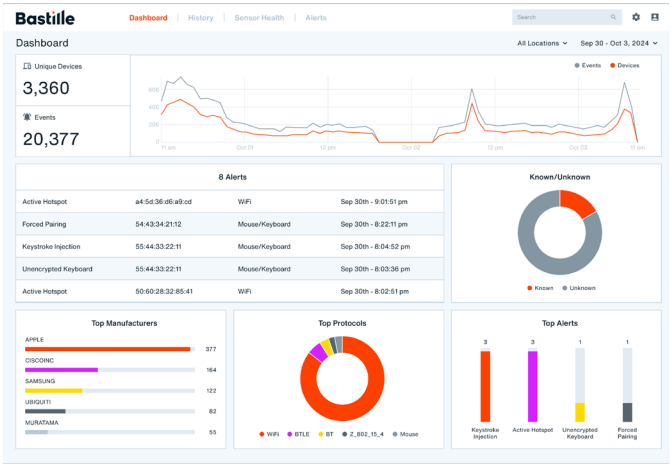

Figure 3: Sensor Array

How Bastille Assists the TSCM Mission

Continuous RF Monitoring

Bastille continuously scans the electromagnetic spectrum for RF signals, enabling real-time detection of any wireless transmission within the protected area. This capability is vital as it can identify threats that emerge anytime between bug sweeps.

The Bastille Enterprise Spectrum Survey helps operators detect radio frequency (RF) emissions other than the specific protocols that Bastille Enterprise monitors. A Spectrum Survey detects RF transmitters between 100 megahertz (MHz) and 6 gigahertz (GHz). Spectrum Survey can run periodically throughout the day, or an operator can run it manually. The Bastille Enterprise DVR Console can display Spectrum Survey data.

Identification and Classification of Signals

Bastille has over 35 patents in the wireless detection field. It uses sophisticated algorithms to identify and classify RF signals, distinguishing between legitimate and potentially malicious transmissions. This capability helps identify unauthorized devices such as hidden cameras, microphones, or other surveillance equipment.

Example

Advanced Bluetooth Device Detection

Bastille's unique approach simultaneously monitors all 79 Bluetooth and 40 Bluetooth Low Energy channels. This approach identifies Bluetooth-paired devices, explicitly noting the paired network endpoints, attributes of both ends of the pairing, and Bluetooth devices performing inquiries or scans.

Example

Individual Cellular Device Detection

Bastille provides comprehensive data on individual cellular devices that transmit in the monitored space. With Bastille's technology, you can track each cellular device's location, carrier, and specific attributes as it moves through the monitored facility.

Example

Wi-Fi Monitoring

Bastille monitors Wi-Fi access points and connected devices to help identify malicious activity that could result in data exfiltration or unwanted surveillance. These include spoofed MAC addresses, unknown access points, devices connected to a guest network, and devices connected to managed and unmanaged networks.

Location Tracking and Data Visualization

With the capability to localize the source of RF signals leveraging ML-based models, Bastille can accurately determine the position of hidden devices within a building. This geolocation feature enables security teams to swiftly respond, locate, and neutralize surveillance threats.

Bastille overlays stored wireless data clearly on your facility floor plan, including current device location to within 3m accuracy and a playback capability to show the historical position of each wireless device as it moves through your space. This playback functionality allows correlation with other systems to determine who brought the device in and when and where they traveled in the facility.

Bastille allows analysts to investigate RF data from well into the past. Analysts can examine data through search and filter functions with Bastille's playback capabilities.

The Fusion Center platform also offers highly customizable reports to visualize data for immediate use or reports to leadership.

Historical Analysis

Bastille can record and analyze historical data concerning RF activity, allowing for the detection of patterns or irregular activities that might suggest surveillance attempts. This long-term data can be crucial for understanding and mitigating sophisticated espionage strategies. Bastille's latest product uses AI and machine learning to revolutionize TSCM by enhancing the ability to quickly analyze vast amounts of data and detect anomalies more accurately.

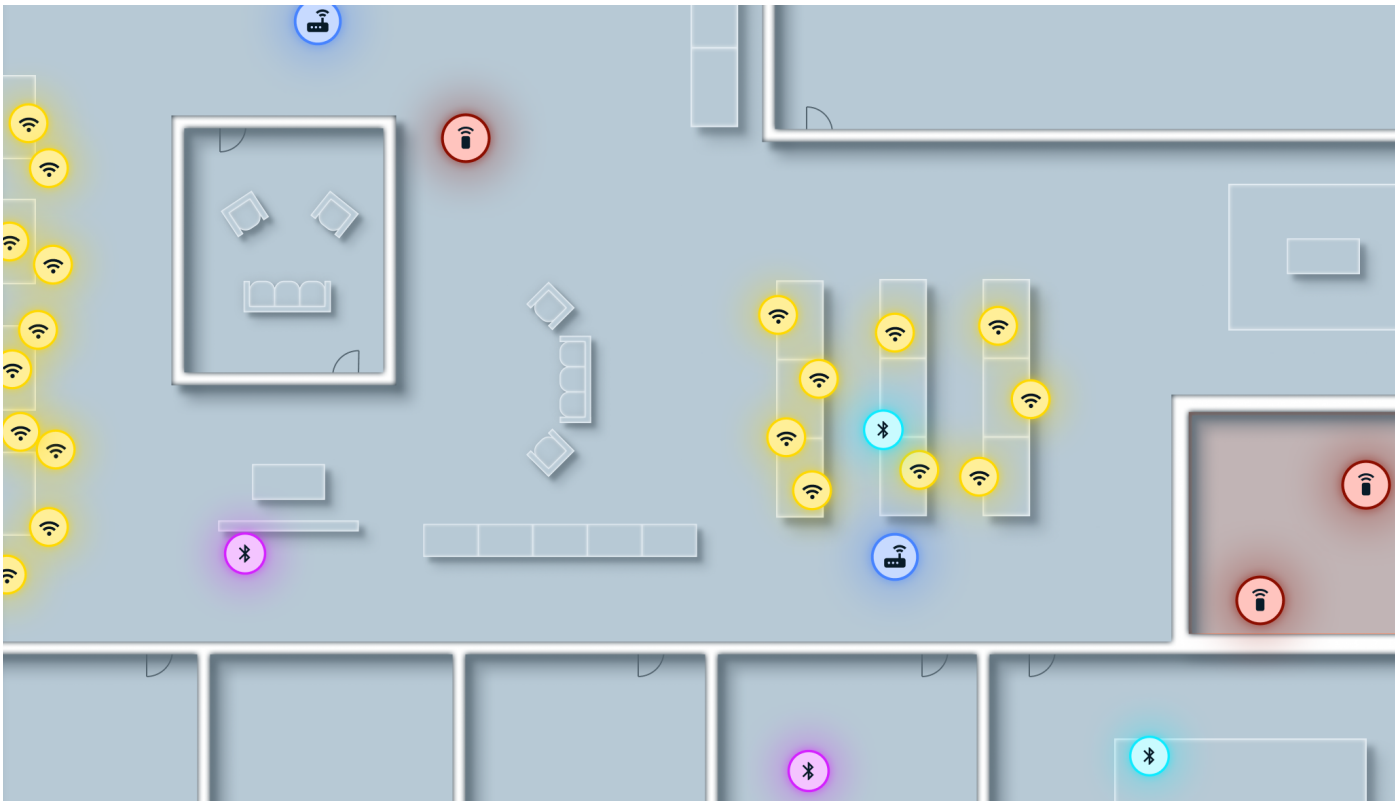

Figure 4: Device Location plotted on your floor plan

Threat Library

Bastille's Fusion Center automatically detects known wireless threats from its curated database of threats discovered by Bastille's Threat Research Team and industry-disclosed vulnerabilities. This feature ensures that Bastille can quickly identify and address known threats, leveraging internal research and broader industry insights.

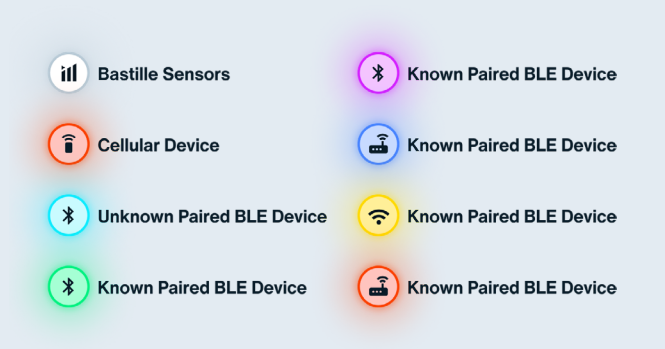

Figure 5: Device Location plotted on your floor plan

Integration with Security Systems

Bastille can be integrated into broader security systems, including spectrum analyzers, offering a holistic view of physical and electronic threats. This integration enhances security postures by allowing coordinated and quick responses across different security layers.

Automated Alerts

Users can configure Bastille to generate immediate, automated alerts upon detecting suspicious or unknown RF signals. This capability enables security personnel to react swiftly to threats and potentially catch eavesdropping attempts as they happen.

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