Bastille

Wireless Threat Intelligence

EXECUTIVE SOLUTION BRIEF

Continuous TSCM

BASTILLE.NET

Continuous TSCM

TSCM Is Critical For Effective Security

Organizations which care about their security have historically done monthly or quarterly "bug sweeps", otherwise known as Technical Surveillance Countermeasures (TSCM). While effective at that moment, without a continuous TSCM solution in place, you can't ensure the security of your facility from wireless threats.

Every security officer knows that even when your facility has been "swept," a bug planted after the sweep won't be found until the next sweep. Before there were billions of cell phones or could easily buy "spy bugs" on eBay, these extended periods of vulnerability might have been OK. Today, you intuitively KNOW that's not enough. You need to know at every moment, every device that enters your facility and whether it leaves or stays behind in a conference room or a research lab.

- You want to be sure there are no unauthorized wireless devices or transmissions in the locations you expect to be secure.
- You need to know the ownership and intentions of every device in the space.
- You need to quickly assess whether a detected wireless device is a threat or not.
- You need to know where every wireless device is now and where it's been while in your facility.

You need Bastille's Continuous TSCM solution.

Wireless Threats

Wireless threats are evolving at a rapid pace just like network-borne vulnerabilities and malware. However, wireless threats have a distinct advantage over network-centric attacks: Wireless Threats are not detectable on managed networks. Wireless threats can exfiltrate data out-of-band from even the most complex firewall, intrusion detection, and malware scanning systems on the physical network. To ensure your secure space is free of unknown wireless threats, you must continuously scan for wireless threat activity.

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

Any one of these threats can compromise the security of the spaces where you hold sensitive discussions, process critical information, or have compliance obligations on wireless security.

Threats Are Evasive

Wireless devices used for eavesdropping or data exfiltration would not be very effective if they were easy to find. Oftentimes, they attempt to avoid detection by either transmitting during busy-times (to blend-in) or off-hours (fewer observers). A continuous monitoring TSCM system will find the threats whenever they transmit.

Threats Are Camouflaged

Advanced data exfiltration threat devices are often designed to look like cables and components that are normally present in your facility; the only way to know if a true threat is present is to monitor the wireless spectrum for transmissions that violate security policy. Physical inspection will not identify these threats.

EXAMPLE: USB Ninja Cable

The USB Ninja Cable is a hacking tool which is designed to look exactly like common vendor-issued cables, but includes a miniature computer, controllable by Bluetooth, which can gather and exfiltrate all the data that it sees, including keystroke logging as well as keystroke injection to deliver malicious payloads to the target computer. These cables are undetectable unless you are scanning for wireless activity. The USB Ninja cable, and many others like them, are broadly available online and cost less than one hundred dollars.

INPUT DEVICES

USB Ninja Bluetooth Remote

~~$60.00~~ $50.00

\- 1 + ADD TO CART

EXAMPLE: Cellular Listening Device

Miniature eavesdropping devices which 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 ensure all cellular transmissions are identified and devices with unusual behaviors are investigated.

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 Are Built On Connectivity

Cellular data networks are heralded for their expansion of convenience and access for their users; though at the same time allow for rapid exfiltration of data 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 be synchronized with a cloud service, same for a video recording, same for 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

This refined approach is made available by Bastille Networks.

Bastille Solution

Bastille provides intelligent and comprehensive, continuous monitoring for wireless threats within your secure location. The Bastille solution is a combination of Sensor Arrays deployed throughout your facility, Concentrators to aggregate and process sensor data, and the Fusion Center platform which analyzes and augments the wireless data and enables integrations with your existing security systems. This tiered architecture allows the Bastille solution to scale from monitoring a single room to many campuses across the world with a single management interface.

Sensor Arrays

Comprehensive monitoring is achieved through deployment of Bastille's sensor arrays throughout the monitored facility. Bastille sensor arrays detect wireless emitter activity from 25 MHz to 6 GHz and this RF traffic is decoded, processed and sent to the Bastille Concentrator for further event correlation. The sensor arrays are 100% passive, which means they never transmit, are plenum rated, are available for indoor and outdoor use, and are manufactured in the United States.

The sensors capture all available attributes of the wireless devices including dozens of identifiers such as vendor name, Bluetooth network definitions, Wi-Fi device characteristics, and Cellular network information.

Bastille's Sensor Arrays are based on Software Defined Radio (SDR) technology which allows them to receive in-place upgrades ensuring future protocol support and decoding.

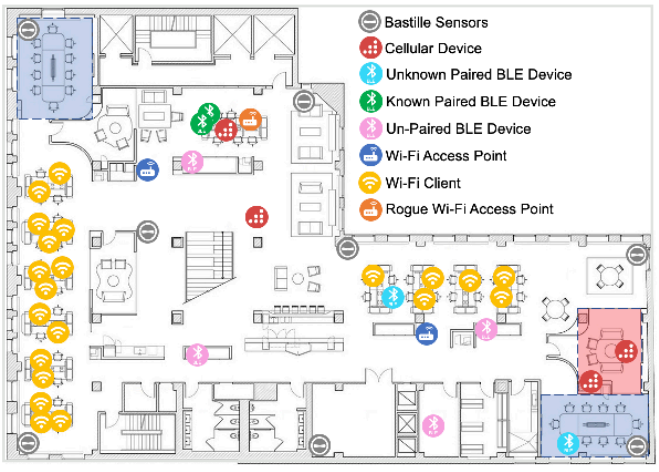
Concentrator

The Bastille Concentrator receives data from all of the sensor arrays in a facility, refines and consolidates the data into events, and sends them to the Fusion Center. The Premium Concentrator is used to gather additional data from cellular device transmissions.

Fusion Center

Bastille's Fusion Center platform is the only NIAP certified product in this market and provides you additional assurances on the quality and security of the Bastille solution. Fusion Center receives wireless data from the Concentrator(s), compiles and analyzes the data, and displays all data on current and historical wireless device activity. Any detected wireless device is clearly overlayed on your facility floor plan, including current device location to within 3m accuracy and a playback capability to show the historical location of each wireless device as it moved through your space. This playback functionality allows correlation with other systems to determine who brought the device in, along with when and where they traveled within the facility.

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. The Fusion Center platform offers highly customizable reports, provides rich API capabilities for integration with SIEM/SOAR systems, and is fully maintained and supported by Bastille along with the sensor arrays for the life of the subscription.



Bastille's Solution for Continuous TSCM

Continuous TSCM

Examples Of Bastille's Differentiation

Bastille has 30 patents in the wireless detection field and maintains significant advantage in detecting wireless threats.

Threat Signatures & Event Intelligence

Bastille's Threat Signatures filter through all detected devices and apply categorizations to them so you can focus your resources on the critical threats. Bastille's solution brings wireless data to your security policy enabling you to evolve your policy to match the reality of your environment.

Bastille's comprehensive categorization capabilities allow you to rapidly detect new RF emitters and assess their threat posture while maintaining visibility to approved devices such as cellphones, bluetooth devices, and Wi-Fi clients used by your employees.

Advanced Bluetooth Device Detection

Bastille's unique approach simultaneously monitors all 79 Bluetooth channels 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. Other vendors only show when Bluetooth devices are looking to pair; after they've paired they become invisible. After a device is paired is when it has the capability to exfiltrate data and cause disruption; you need this visibility to protect against Bluetooth surveillance threats.

Individual Cellular Device Detection

Bastille provides comprehensive data on all individual cellular devices which transmit in the monitored space. With Bastille's technology, you can track the location, carrier, and specific attributes of each cellular device as it moves through the monitored facility, all while adhering to data privacy concerns.

Device location plotted on your floor plan

To find out how Bastille can detect Wireless Threats visit **bastille.net**

Follow us on Twitter **@bastillenet** and on **LinkedIn**.

INFO@BASTILLE.NET
800.530.3341

Bastille
Wireless Threat Intelligence