Safeguarding Your xIoT (IoT/OT/IoMT) Devices: Addressing the Limitations of Traditional Security Solutions

Executive Summary:

Traditional security tools and even leading xIoT security solutions, which rely exclusively on either active scanning or passive monitoring, fail to comprehensively detect xIoT vulnerabilities. IoTSecure's innovative approach integrates these techniques to close security gaps, providing complete protection for xIoT devices. Our unified security strategy ensures thorough device identification, vulnerability detection, and device protection.

I. The Shortcomings of Traditional Security Tools

Active Scanning (e.g., traditional vulnerability scanners)

Claimed Benefits: Active scanning is purported to be an effective solution that utilizes network scanning and endpoint agents to analyze accessible ports and running processes, enabling device identification. The scanner then matches the identified profile to known vulnerabilities.

Limitations for xIoT Devices:

1. **Profiling constraints:** xIoT devices can lack support for endpoint agents and have limited or no open ports, which are crucial for traditional scanners to profile and identify devices accurately. This leads to identification failures and undetected vulnerabilities.
2. **Intrusiveness:** Traditional scanners can overwhelm xIoT devices with traffic while attempting to locate open ports, potentially causing disruption or damage. This leaves devices untested and vulnerable and may result in downtime.
3. **Inadequate detection of default credentials:** Despite being a top vulnerability category, traditional scanners struggle to detect default credentials, which vary widely across devices from numerous manufacturers. IoT manufacturers also create unique default credentials for each service, further necessitating comprehensive default credential detection.

Passive Monitoring (e.g., existing SIEM, ZTNA and leading IoT security solutions)

Claimed Benefits: Passive monitoring is believed to effectively profile devices by observing traffic, matching profiles to vulnerabilities, and identifying devices.

Limitations of Exclusive Passive Monitoring:

1. **Encrypted traffic challenge:** Encryption conceals essential profiling information, and passive monitoring does not actively scan to gather this data, rendering it ineffective at identifying devices and detecting vulnerabilities.
2. **Restricted vulnerability detection:** Without active scanning, passive monitoring cannot identify certain vulnerabilities, such as default credentials, the #1 IoT vulnerability according to the latest OWASP IoT Top 10 Vulnerabilities list.

II. IoTSecure's Cutting-Edge Solution for xIoT Devices

IoTSecure has developed a groundbreaking, agentless approach to bolster the security of xIoT devices by addressing these detection gaps. By seamlessly integrating non-intrusive active scanning with AI-enhanced passive monitoring and leveraging an extensive library of device profiles, IoTSecure accurately profiles devices and uncovers vulnerabilities that traditional tools miss. Our solution is safe for even sensitive and resource-constrained IoT devices and it's continuously active, automatically profiling devices upon connection and providing near real-time vulnerability detection.

IoT Vulnerability Detection Requirements	Traditional Active Scanning	Passive Monitoring	IoTSecure™
Identifies & profiles devices that don't run endpoint agents	⚠	✓	✓
Safe, non-intrusive	✗	✓	✓
Supports devices that encrypt traffic	✓	✗	✓
Strong, default credential detection for multiple services	⚠	✗	✓

*Though not in scope for this security brief, IoTSecure also provides automated malicious and anomalous behavior detection and zero trust micro-segmentation for xIoT devices.

To learn more or to request a free evaluation, visit: https://iotsecure.io/iotmini