Value of Cybersecurity for R&D: Beyond Just Attack Mitigation

FIREDOME

Firedome's tailormade solution for IoT manufacturers proactively prevents, detects, and responds to inevitable vulnerabilities in connected devices. Firedome's unique platform embeds an AI-driven agent on the device itself, creating a wide range of possibilities for R&D teams.

Our capabilities demonstrate how Firedome's technology creates additional value for R&D teams to streamline, refine and improve the design and maintenance of their IoT devices in a more secure manner.

Remote Device Connection

What is the issue: IoT manufacturers must connect to deployed devices daily for maintenance and issue resolutions. Today most devices reside behind a NAT (local network), which makes managing devices from the internet a difficult task. Some developers use port forwarding, an unsecured method to remotely access devices. RDC offers a secure way to connect remotely.

About the feature: Allows access to remote devices via an encrypted TCP tunnel, which is secured and provided by Firedome. With this connection, you can access remote devices (for example by SSH), that reside behind a NAT (Network Address Translation) without the security concern and technical difficulty of port forwarding or another vulnerable communication method or protocol.

Benefit to R&D team: Enables R&D teams to securely connect to deployed devices, resolving issues in real-time and without end-customer involvement or resources.

Real-life scenario: An end-user reports a malfunctioning device. As part of the troubleshooting process, you are now able to connect to the device and resolve the issue swiftly in a very secure & simple way.

Core/Memory Dump Retrieval

What is the issue: Getting a view of a program's state and log data at the time of the crash is invaluable to developers in order to understand the reason for the crash and fix the issues. However, retrieving the core dump file for already-deployed IoT devices that crashed is a difficult problem.

About the feature: This feature provides the option to retrieve the remote device core dump file, in an encrypted & secure manner.

Benefit to R&D team: Rapidly analyzing & fixing issues on deployed devices by conducting a post-mortem snapshot investigation of a crashed device/software.

Real-life scenario: After a new software version release, you notice that a high percentage of devices are constantly crashing due to an unknown bug. With this feature, you are now able to retrieve the core dump files and resolve the bug.

Monitoring of Precarious Devices

What is the issue: Deployed devices act very differently than in the lab. Therefore IoT manufacturers need a way to monitor and gain insights about all these operational behaviors, such as devices that suddenly stopped communicating or became unreachable, devices that suffer from network problems (jittering), and devices that frequently crash and restart.

About the feature: The feature provides real-time visibility to the fleet's dynamic behavior. It presents data about online, disappeared, network-jittering and constantly crashing devices.
Benefit to R&D team: Immediate detection of operational issues that severely impact the device base and end-customers. These can be caused by either a cyber attack or a software/hardware bug.

Benefit to R&D team: Immediate detection of operational issues that severely impact the device base and end-customers. These can be caused by either a cyber attack or a software/hardware bug.

Real-life scenario: A hacker detects a buffer-overflow vulnerability that can crash a device's main process, making it unresponsive. The feature detects and reports this. The bug is identified and fixed quickly, mitigating a denial-of-service attack, stopping it before it is executed on the entire fleet.

FireWaf - Embedded Web Server Protection

What is the issue: Web application vulnerabilities are the most targeted attack surface against on IoT devices. The need to implement the right input sanitization & validation method on every form and text field and secure the hosting process is resource-heavy for developers. That is why they often fail to secure 100% of all input fields, resulting in a vulnerable server and a great risk for the device to be hacked (command injections, remote code execution, buffer overflow, etc).

About the feature: The feature protects any embedded web server against command injection exploits, web application hacking methods and 0-day remote code execution vulnerabilities, without impacting performance.
Benefit to the R&D team: This feature provides a necessary security layer against the most common attack surface in IoT devices, offering peace of mind to the Product & R&D teams and enabling them to focus on product development instead of constantly validating every input.

Benefit to the R&D team: This feature provides a necessary security layer against the most common attack surface in IoT devices, offering peace of mind to the Product & R&D teams and enabling them to focus on product development instead of constantly validating every input.

Real-life scenario: A hacker discovers a shell command injection vulnerability in a device's server management dashboard, so he hacks to install malware, taking full control over the device. With this security layer, even if a vulnerability exists, the injection attempt fails and the device is kept secure.

FIREDOME

Securing the Connected Future

For ongoing support and questions about Firedome contact:
www.firedome.io | support@firedome.io | +1 (374) 826-6713