Firedome Position Paper for NIST

Firedome respectfully submits this paper in response to NIST Call for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security (EO14028) areas 2 and 4.

Firedome advocates for the establishment of baseline cybersecurity requirements for IoT/OT brands to ensure strong security of internet-connected devices sold to the U.S. government, enterprise/industrial organizations and consumers.

Firedome would like to provide input for EO Section 4(e)(iv) and 4 (e)(F):

Firedome strongly believes that in order to properly adhere to these sections, a satisfactory secure software development lifecycle (SSDLC) must **include 24/7 security monitoring, especially when a device leaves the lab and is deployed on an end-user network.**
The establishment of criteria for a tool that **constantly monitors deployed devices** for attacks, checks for both known and potential vulnerabilities, and provides remediation has long been required. The criteria must include real-time security operations in order to discover and thwart all relevant threats.

The gap must be closed

The threat landscape for IoT devices has grown significantly, and today poses risks similar to the PC industry, leaving a gaping hole in security standards for IoT. Closing this gap in security standards for all connected devices is critical. The current static security approach and standards renders IoT devices completely vulnerable: most recent IoT malwares and attacks are exploiting IoT devices via weak spots and vulnerabilities that aren't able to be disclosed. Security guidelines for IoT manufacturers today include only static approaches, which constitute only a subset of the security facets (i.e. checking for known OS vulnerabilities on development time). The standards must be modified to **include proactive endpoint protection to monitor the device while it's actually being used,** as it did with personal computers 20 years ago.
For instance, the SSDLC today focuses only on the development phase, which in its core is a static process. For example, only a few of the SSDLC standards suggest testing the firmware for known vulnerabilities - even then it will be conducted only on compile time(!) Considering that the I/OT lifespan can reach 10-20 years, vulnerability testing based on compile time is ineffective. Moreover, practices such as penetration testing, are similarly lacking in their approach: they test the device on identifiable vulnerabilities known only at the time of the assessment. This practice neglects to identify recurring, intermittent vulnerabilities, which often happen over long periods of time and at variable frequencies, allowing threat actors to infiltrate.

Firedome is steadfast in our belief that the only way to close the gap in security for IoT devices is to require constant proactive endpoint protection, built into the device software, as a critical part of post deployment. All alternatives render the device vulnerable to malicious actors and dynamically evolving threats.

Technology is not a barrier

Considering that today all standards (ISO 27001, NIST 800-53..) for PCs require an Antivirus/EDR (Endpoint Detection & Response) installed - the same should be applied to IoT devices. Technology advancements in recent years enable device manufacturers today to introduce this type of monitoring and protection easily, with both open-source and proprietary solutions available in the market.

Increasing market adoption

Firedome welcomes and supports NIST's efforts to promote public education and clear directives in labeling in relation to security capabilities of IoT devices as mentioned in EO Section (4)(s) and we are keen in participating in this initiative.

Recognizing that the majority of manufacturers are not currently adhering to EDR security practices, we propose the introduction of tiers in labeling. The creation of security tiers within guided criteria and accreditation/grading will be inclusive and incentivize manufacturers to participate. Tiering enables the government to insist their devices adhere to the most secure tier (incl. applying EDR), while creating security standards and transparency in labeling for all IoT devices to serve organizations and private consumers. Tiered labeling will enable the government to lead the U.S. market to a secured and smart future.

Firedome strongly believes incentivizing and encouraging manufacturers and users to produce secure devices is unequivocally the right path for adoption of greater security in the U.S. industry. This can be achieved by:

1. **Introducing new criteria for IoT security standards that is equivalent to the PC industry and can mitigate the current threats: proactive endpoint protection and response (EDR) for IoT**
2. **Differentiating security tiers within the guidelines**
3. **Requiring governmental agencies to adopt the most secure tier of protection**

About Firedome

Firedome Inc. (https://firedome.io) is a leader in cybersecurity, driving IoT growth for IoT brands and manufacturers. Offering a robust IoT security and privacy platform including 24/7 monitoring and advanced marketing and cyber services, Firedome enables IoT brands and manufacturers to protect their devices and their users while growing their market share.

