CASE STUDY_

Eclypsium Helps Florida Law Enforcement Agencies Achieve CJIS Compliance

Recent Criminal Justice Information Services (CJIS) regulations have introduced stringent new rules that define how law enforcement agencies must protect criminal justice information (CJI). These changes require agencies to manage risk, vulnerabilities, and threats down to the firmware within their assets—well below the level covered by EDR and other traditional security tools.

By partnering with Eclypsium, multiple local Florida law enforcement agencies were able to easily meet these new regulatory requirements and greatly enhance their cybersecurity without burdening IT and security staff.

CHALLENGES_

- Needed to safely enable staff to access and work with sensitive criminal justice information.
- Needed to meet firmware-related security controls defined by section SI-7 of the CJIS Security Policy.
- Existing security tools were not able to meet requirements for securing firmware IT and Security teams had limited time for new projects.

RESULTS_

- Enabled deep vendor-agnostic visibility into a wide range of assets including laptops, servers, and networking gear.
- Automated assessments to identify vulnerabilities, threats, or changes to device firmware and proactively verify firmware and supply chain integrity.
- Simple, easy-to-deploy solution that met CJIS requirements without burdening the Security and IT team.

BACKGROUND_

Every law enforcement agency needs access to sensitive criminal justice information such as fingerprint data or information on known criminals or missing persons. At the federal level, these and many other forms of sensitive information are managed by the FBI's Criminal Justice Information Services division known as CJIS. Naturally, the FBI needs to ensure that its data remains safe when shared with outside agencies. This is the goal of the CJIS Security Policy, which lays out detailed and auditable requirements for agencies that use CJIS information and services. Like other standards governing federal data such as FedRAMP, CJIS requirements are based on NIST's SP 800-83. Specifically, the CJIS Security Policy requires agencies to manage risk, vulnerabilities, and threats down to the firmware within their assets. Firmware and supply chain security requirements are called in several CJIS security controls including SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY. With the latest DOJ CSA audit cycle beginning on October 1st of 2023, law enforcement agencies will now have to meet these new requirements.

CHALLENGES_

The latest CJIS requirements introduced a regulatory gap affecting many local Florida law enforcement agencies. The new regulations brought several challenges that were common across agencies including:

- **Lack of coverage by traditional tools** - The traditional EDR security tools that the agencies used on their devices lacked the required ability to monitor for changes, risks, threats, and vulnerabilities at the firmware layer. Specifically, EDR tools could only look for hashes of known threats, but were not able to proactively verify the integrity of firmware.
- **Highly diverse device environments** - Agencies needed to cover a wide range of vendors and devices including user laptops, servers, and networking devices such as firewall appliances.
- **Limited IT and Security resources** - The affected agencies needed to address the new requirements with their existing staff. Teams needed simple tools and processes that could extend to the firmware layer without the need for extensive training or new skills.

SOLUTION AND BENEFITS_

Using the Eclypsium Platform, agencies were able to significantly enhance their cybersecurity practice and quickly demonstrate the ability to comply with the latest CJIS controls. Eclypsium was able to provide value in the following key areas.

Security Capabilities

- **Integrity checks for firmware and components** Organizations were able to verify the integrity of firmware and critical components as defined in the CJIS section SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY. This covers a wide range of potential risks including unapproved or accidental changes to firmware, tampering or changes made in the supply chain, as well as malicious changes made by internal or external attackers.
- **Vulnerability management and flaw remediation** - Control SI-2 FLAW REMEDIATION requires organizations to “identify, report, and correct system flaws” down to the firmware level. Eclypsium was able to provide simple automated assessments to identify and prioritize vulnerabilities both in system-level firmware such as UEFI or BIOS as well as firmware within system components such as storage drives, network adapters, and system controllers.
- **Detection of out-of-support components** - Control SA-22 UNSUPPORTED SYSTEM COMPONENTS requires agencies to identify components that are no longer supported by the vendor including hardware and firmware. Code that is no longer supported can lead to perpetual vulnerabilities that can be exploited by attackers.

Simple Security Operations

- **Fast evaluation and deployment** - Within just a few hours, agencies were able to install the Eclypsium platform and begin seeing results on laptops as well as server infrastructure.
- **Vendor agnostic solution** - Eclypsium provided consistent coverage across a wide range of vendors as asset types. This included a diverse fleet of laptops as well as servers and networking devices.
- **Automated assessments and guidance** - Eclypsium assessments were able to automatically identify and explain firmware and supply chain risks without the need to hire firmware specialists. Staff could simply scan their devices and quickly detect and remediate threats.

ABOUT ECLYPSIUM_

Eclypsium’s cloud-based platform provides digital supply chain security for critical software, firmware and hardware in enterprise infrastructure. Eclypsium helps enterprises and government agencies mitigate risks to their infrastructure from complex technology supply chains. For more information, visit eclypsium.com.