SUPPORTING CYBER PROTECTION TEAMS_

Warfighters need to have absolute confidence in all their equipment when deployed in the field. Yet, while teams have the training and tools to verify and maintain their tactical equipment, the same is not true for hunt-forward cyber mission assets such as laptops, servers, and networking gear. Eclypsium closes this gap by allowing Cyber Protection Teams (CPTs) to quickly scan critical mission assets to validate their integrity and authenticity, and to detect the presence of vulnerabilities or threats hidden at the hardware or firmware level.

THE CHALLENGE_

Mission systems rely on many types of critical code that run below the level of the operating system including boot code, system UEFI firmware, and code within hardware components such as drives and network adapters. This code has become a key target for adversaries because it is often vulnerable and outdated, and threats can allow attackers to remotely subvert or disable the asset. Such threats have been used by state-based adversaries for years such as the LoJax UEFI rootkit used by the Russian GRU group APT 28 and most recently replicated by BlackLotus, CosmicStrand, and MoonBounce.

Unfortunately, there are many ways these threats can be introduced into critical assets. Even small vulnerabilities or misconfigurations can allow adversaries to gain control of a system, and compromises in the technology supply chain can allow attackers to insert malicious code into a system before it is ever delivered to teams in the field. Threats at this level are particularly hard to detect because the threat arrives in the guise of valid, "trusted" code, and by running below the OS, threats can easily hide or provide false information to traditional security tools running in the OS level.

THE SOLUTION_

Eclypsium provides a simple, automated way to verify the integrity and posture of mission kits in the field. The solution is deployed in an offline assessment kit with a virtual machine for analysis and removable media for checking mission systems without the installation of any software.

> **"Eclypsium turns one of the most complex areas of cybersecurity into a simple, automated scan that teams can use in the field to ensure their systems are secure. By incorporating Eclypsium into fly-away kits, teams are able to secure their systems at the most fundamental level no matter where they are."**

A simple scan verifies that the asset and all of its components are authentic and have not been tampered with either in the field or in the supply chain. The scan will also validate that the equipment is using up-to-date code and is free from vulnerabilities. The technology identifies the presence of known threats and monitors the behavior of the firmware and other critical code to detect the presence of unknown threats. Most importantly, these tests require no firmware expertise, pose no risk to the systems themselves, and can be performed fully offline.

ABOUT ECLYPSIUM_

Eclypsium is an established leader in supply chain and firmware security and is a contributor to the National Cybersecurity Center of Excellence (NCCoE) and SP 1800-34B, *Validating the Integrity of Computing Devices*. Eclypsium's cloud-based or offline platform provides digital supply chain security for critical hardware, firmware and software. Eclypsium defends enterprises and government agencies from the deep implants and exploits that have become the vector of choice for modern adversaries. For more information, visit eclypsium.com.