WebSensing

Linux Kernel Integrity Monitor (LKIM)

Monitor the Linux Operating System and associated Device Drivers for Kernel-Level Zero-day Attacks with WebSensing's **Linux Kernel Integrity Monitor (LKIM) Gateway.**

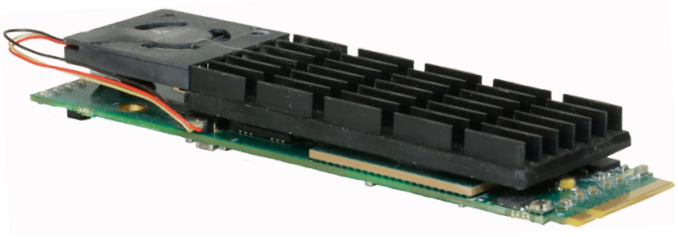
The Web Sensing Linux Kernel Integrity Monitor (LKIM) is a device that is hidden within a computer and monitors the Linux Operating System and its associated Device Drivers for Kernel-Level Zero-day Attacks.

A Zero-day Attack is an advanced cyber-attack that has not been seen previously by network defenders and consequently cannot be detected by anti-virus software.

Kernel-level Zero-day attacks are a particularly dangerous variant that allows the operating system to be high-jacked and coopted for use by an attacker. Because these attacks allow the attacker to operate as an administrator, the attacker is able to hide their activity, physically damage the computer, alter its behavior, or delete data.

The Web Sensing LKIM plugs into a PCIe slot within the computer and continuously monitors the Linux Kernel for change. If any change is made to the kernel, then the card issues an alert allowing the machine to be disconnected from the Internet and subjected to forensic analysis.

The Web Sensing LKIM is an all-hardware device, containing no vulnerable operating systems or other software. This renders them impervious to software attacks embedded in network traffic.



Solution shown using NiteFury PCIe card

Form Factor	PCIe
LED Indicators	On, Zero-day detected
Logic	Web Sensing LKIM[1]
OS Indicators	available
Kernel refresh	available

[1] US. Patents: 10,148,761 (Dec 4 2018).