RECONSENTINEL
ONLINE SECURITY, ALWAYS ON DUTY
Powered By: CIGENT

WHAT DOES A RECON SENTINEL DO?

Recon Sentinel is designed to add a layer of detection and defense to anyone's network. It does this by looking for behaviors that are associated with the first stage of a cyber attack: Reconnaissance.

Currently, The Recon Sentinel has the following capabilities:

Network Inventory (Devices and Services)
The Recon Sentinel easily connects to any ethernet port on your network and takes a baseline inventory of all the devices, and all the network services that are running. Any new devices are alerted on, and any new services are shown to the user through the App.

Network Scanning Detection
Malware and Attackers use network scanning to find devices and services on a network that may be misconfigured or vulnerable. Recon Sentinel alerts the user to any network scanning activity.

Cyber Deception
The Recon Sentinel runs deceptive network services, making it look like a device on the network that has interesting and possibly vulnerable services. Any device interacting with these services is considered compromised, as the services are purely deceptive. An alert is generated informing the user of the offending device (attack).

Device Blocking
The Recon Sentinel can "Block" a device on the network by sending specially crafted low-level packets to the device, causing the affected device to send all it's Internet traffic to the Recon Sentinel, which it in turn discards.

Active Defense Countermeasures (ADC)
If ADC is turned on, any new ("Untrusted") devices that are attached to the network (wired or wireless) or any devices that are attacking the Recon Sentinel are automatically "blocked" until the user unblocks it.

RECONSENTINEL
ONLINE SECURITY, ALWAYS ON DUTY
Powered By: CIGENT

WHY SHOULD SOMEONE BUY A RECON SENTINEL?

Cybersecurity defense is like an onion… it is best to have multiple layers of detection and defense. Recon Sentinel is an essential layer in the cybersecurity onion.

Recon Sentinel is designed to work with existing firewalls, antivirus, and antimalware software solutions. It is an additional layer of defense, not a replacement of existing defenses.

You Can't Defend What You Don't Know.
Knowing is half the battle, and Recon Sentinel makes it easy for anyone to know exactly what devices are on their network, what services those devices run, and if any new devices get connected to their network (think kids giving away WIFI passwords to neighbors and friends).

Understanding if devices on your network are performing reconnaissance scanning can be a early indicator of a malware/virus infection.
No cybersecurity solution (firewalls, antivirus, etc.) is 100% effective. New exploits and vulnerabilities are released everyday that can get around antivirus/antimalware software. "Scanning" is one technique used by attackers and malware to find other devices on a network. Detecting and alerting on this behavior can give users an advantage in detecting an issue and getting it corrected.

"**All Warfare is Based on Deception - Sun Tzu".**
Cyber Deception is an effective detection mechanism of malicious or unwanted behavior on a network. Since the Recon Sentinel runs no "real" services, anything on the network trying to interact with the "fake" services is doing something it shouldn't. Malware and attackers will often try and interact with devices on the network to gain a stronger foothold in the network.

Disruption of Command and Control Traffic.
If an untrusted device or and attack on a deceptive service is detected, the Recon Sentinel can automatically block the Internet traffic from the offending device, hindering an attackers ability to control the device, or blocking malware from calling home.

Unlike antivirus/antimalware software, the Recon Sentinel is always on, looking for new devices, services and reconnaissance behavior and automatically updating itself without user intervention.