CYSIV SENSOR

Continuous endpoint telemetry collection for enhanced threat detection and response

Conventional endpoint security tools miss many types of advanced threats including ransomware and phishing attacks. However, raw telemetry generated at the endpoint provides critical data that broadens visibility and improves the processes of threat detection and response.

Cysiv Sensor is a lightweight software agent that continuously collects raw telemetry in the form of system data from Windows desktops, laptops and servers, and routes it to the Cysiv SOC-as-a-Service platform. This telemetry is then used to identify suspicious activity or behavior, add important context to the threat investigation process, and further reduce false positives. Cysiv Sensor improves visibility for Cysiv SOC-as-a-Service clients that do not have an endpoint detection and response (EDR) tool that collects raw telemetry.

KEY FEATURES:

- **Comprehensive telemetry collection:** Collects system activity data on running processes, network connections, files created/modified, executed commands, loaded drivers, registry modifications, DNS queries and responses, URL access, login sessions, and Windows Event Logs
- **Event filtering and enrichment:** Collects only security-relevant events. Enriches events with valuable data including geo-location, file hashes, volume and file system details
- **Dynamic routing / cache:** Forwards events to hosted Connector if on-premise Connector unreachable. If connectivity drops, stores events on disk and forwards when restored
- **Flexible deployment methods:** Supports interactive EXE installer, MSI through GPO, command line, PowerShell, silent install, Microsoft Intune deployment package. Installs no driver and requires no reboot
- **Remote management:** Manage Sensor configuration for event collection remotely, including Windows audit and group policy settings
- **Sysmon install:** Automatically downloads, installs and configures Sysmon, which is optional, but necessary for advanced features such as registry tracking
- **Low resource footprint:** Typically utilizes <1% CPU / <150MB RAM / <200MB HDD
- **Automatic updates:** Features optional automatic updates to Sensor software

EVENTS COLLECTED

DNS	Query, Response
File	Create, Create Stream, Delete, Rename
Image Load	Image Load
Network	Connect, Flow
Process	Start, Stop
Session	Connect, Disconnect, Start, Stop, Lock, Unlock
URL	Access
Windows	Event Logs, Security Event Logs
Registry*	Create, Delete, Modify (* requires Windows Sysmon data too)

SYSTEM REQUIREMENTS:

- Windows 10 version 1703 or newer
- Windows Server 2012 or newer

KEY BENEFITS:

The addition of Cysiv Sensor will further enable Cysiv, through its SOC-as-a-Service, to deliver better detection and faster response of true threats, in these ways:

Improved Threat Detection

Raw telemetry provides better detection of threats that have evaded existing security controls. Cysiv Sensor can increase MITRE ATT&CK coverage by ~58% (+125 techniques), and expand Cysiv Indicator & Detection rule coverage by ~26% by potentially triggering an additional 246 Indicator rules. The data it collects makes it possible to detect anomalous user and system activity such as data leakage, insider threats, phishing, and ransomware. It also helps gain increased visibility to unwanted or harmful applications, and expand the pool of activity and behavior data to better support threat hunting.

Accelerate Security Response

In case of an incident, Cysiv Sensor helps you assess its scope and security impact more quickly, and respond faster than ever. It enables faster determination of infected endpoints and servers through server-side IoC sweeping. Cysiv Sensor also expedites incident investigation by searching for specific malware, network communications, registry activity, account activity and running processes, and reduces false positives by corroborating security tool alerts.

ABOUT CYSIV:

Cysiv SOC-as-a-Service provides enterprises with better detection and faster response of true threats. We do this by uniquely combining our cloud-native next gen SIEM, with a data-centric approach and a team of experts that operate as a seamless extension of your SOC. All of this is delivered as a subscription-based service, with predictable and flexible pricing, that can be operational in weeks. Cysiv's modern approach to threat detection and response helps reduce risk, ensure compliance, and improve the efficiency, effectiveness and maturity of your security operations.