WATCHER

FRONTLINE CYBER SOLUTIONS

Overview of Watcher

Watcher is a network device that monitors all communications that it can ingest from any span or mirror port. Watcher processes the information through a series of different events to create a visualization that displays your network nodes and communications pathways.

- Do you have full network visibility?
- Do you know where cyber-attacks are coming from?
- Do you have real-time continuous situational awareness for your IT, IOT, & OT?
- Can you monitor for behavior and signatures?

Who's watching your network?

- Creates a live nodal model of your network in seconds
- Geolocation and Metadata
- Indicators of Compromise (IOC) Information
- Assesses, alerts, and responds to real-time network events
- Identify, characterize and alert on anomalous activity

Highlights

Asset Management
Network Anomaly Detection
SNORT
ICS/OT
Encrypted Removable Storage
Full Packet Capture
Network Forensics
Data Validation
Conditions Based Maintenance

Applications & Environments

Information Technology (IT)
Operational Technology (OT)
Internet of Things (IoT)
Healthcare
Industrial
Manufacturing
Banking & Finance

CONTACT US

Jeramie Crabtree
303.868.1954
jcrabtree@frontlinecyber.us

Watcher Details

Asset Management

When processing the network packets, it also builds out an asset list of devices that it detected communicating on the network. Watcher can compare assets detected to assets that are known and display both known and unknown to the operator while also alerting for any unknown devices that might appear on the network.

Watcher will track the MAC Address, Device Type, IP Address and build the list to monitor from. Watcher will also take and preform different passive scans to build a full understanding of the asset. Watcher will compare any services or device information against the MITRE ATT&CK Framework to be able to determine security state of the asset.

IOC Information

When Watcher is processing the packets, it will look at FQDNs, URLs, IP Address, GEO Location, and Files to compare against known IOCs and GEO Location to detect any compromised devices that would be communicating outbound from the network. It can also detect known C&Cs IPs or FQDNs. If any IOCs are detected an alert will be sent to the GUI or passed on to any SIEM that Watcher is connected to.

Clients can upload custom IOCs to the Watcher devices from the Center Command Server to detect and alert on those IOCs. This allows clients to be able to use any Threat Intel Sources that they have and to be able to monitor both North / South network traffic as well as East / West network traffic.

SNORT

Watcher comes with the options to have a fully licensed install of snort on the device, this provides another level of situational awareness on your network. Watcher will process all network traffic through the SNORT engine to detect any intrusion events that might be happening. This is updated with the latest SNORT signatures weekly.

ICS / OT

Watcher can operate on OT / ICS Networks and preform the same tasks above but with an added feature. When enabled the ICS Libraries Watcher will monitor and alert on ICS Events.

ICS Commands

When Watcher is deployed on the OT Network, it's able to communicate with other Watcher devices that have been deploys throughout the Purdue model 7 layers. This gives the ability to Watcher to monitor and track ICS Commands that are sent to PLCs, it will track the command across the 7 layers and verify the sender asset of the command based on the asset management above. Watcher can integrate into serial devices and provide the same level of security on a serial device as an IP device.

PLC index variables

Watcher can inspect the application layer of the packet and process all the index variables for known PLCs / Data type (BacNET, ModBus, DNP3 and more). Watcher will process each index variables and maintain an understanding of the value and monitor for any change in value. This process can help detect abnormalizes, security threats, and ZeroDay events. When a value change is outside of the parameters it will alert the operators through the GUI or SIEM that Watcher is connected with. Watcher operates out of band to help monitor for spoofing events that would cause the HMI to show altered numbers vs what is happening on the PLC.

Sales Contact

Jeramie Crabtree
303.868.1954 | jcrabtree@frontlinecyber.us