WATCHER V6.0

FRONTLINE CYBER SOLUTIONS

Overview of Watcher

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

Watcher Details

Asset Management

Watcher ingests and processes full network packet of any network. In doing so, it builds an accurate asset list of devices that are detected communicating on the network. Watcher has the ability to compare assets detected against assets that are known and visually mark between known and unknown devices for the operator. This allows for automatic alerting for any unknown devices that might appear on the network.

Watcher extracts and tracks unique asset identifiers such as: MAC Address, Device Type, IP Address, vendor, etc... and creates a digital dossier 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 Framework to be able to determine security state of the asset.

IOC Information

While Watcher is processing data packets, it monitors the 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. Additionally, it detects 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 from the Center Command Server in order to detect and alert on those specific IOCs. This allows clients to be able to use any threat intel sources that they have to be able to monitor both North / South (external) network traffic as well as East / West (internal) network traffic.

SNORT

Watcher comes with the option to have a fully licensed installation of snort on the device. This increases the level of situational awareness on the network. Watcher will process all network traffic through the SNORT engine to detect any intrusion events that might be happening.

WATCHER V6.0

Industrial Control Systems (ICS) / Operational Technology (OT)

ICS / OT

Watcher has the unique ability to operate on OT / ICS networks as it does with traditional IT networks. Watcher performs the same tasks outlined above but with an added feature. When enabled, Watcher utilizes custom built ICS data libraries that allows Watcher to ingest and monitor ICS specific protocols and alert on ICS events.

ICS Commands

When Watcher is deployed on an OT network, it has the ability to communicate with other Watcher devices in a mesh implementation covering from the point of data creation at level 0 to the top level of the Purdue model. Watcher monitors and tracks ICS commands that are sent to PLCs, it tracks the command across the 5 layers and verify the sender asset of the command based on the asset management above. Watcher has the ability to ingest serial data and provide the same level of security on a serial device as an IP device

PLC Index Variables

Watcher inspects the application layer of the packet and process all the index variables for known PLCs / Data type (BacNET, ModBus, DNP3 and more). Watcher process each customer defined index variables and maintains an understanding of the value, monitors for any change in each value. Our process detects network anomalies, security threats, and ZeroDay events. When a value change is outside of the parameters it alerts the operators via the GUI or SIEM. Watcher operates “out of band” to monitor for spoofing events that would cause the HMI to show altered numbers versus what is actually happening on the PLC.

Technical Specifications

Hardware:

- 3x LAN
- AMD GX-412TC CPU
- 4 GB DRAM
- 256GB Drive

Network Detection:

- Source / Destination Traffic
- URLs / URIs
- Files
- FQDNs
- Countries (City, State, Lat/Long)

IOCs:

- IPs
- Files
- FQDNs
- URLs / URIs
- Countries
- Inspect for classified IOCs

Asset Management:

- IP
- Mac
- Hostname
- OS
- Patch Level
- Services
- WMI Calls
- Service Account Access
- MITRE Framework
- CVE / NVD

ICS Libraries

- DNP3
- Modbus
- BACNet
- Customized

Sales Contact

Jeramie Crabtree 303.868.1954 | jcrabtree@frontlinecyber.us