BLUE Lightning AMPEX

Cyber Security for Operational Technology / Industrial Control Systems

Features

- Real-time monitoring of OT
- Defends your network behind the perimeter or air gap
- Protection down to 'Level 0' (older serial-connected systems)
- Focused on detecting anomalous network behavior and intrusion
- *Not* malware signature-based
- Detects the efforts of zero-day threats
- Provides secondary validation of data to prevent spoofing attacks
- Detects network anomalies that are leading indicators of maintenance issues, saving repair costs
- Can scale to any size network
- SIEM agnostic

BLUE Lightning provides cyber security for the unique networks and protocols that make up operational technology (OT). Often referred to as industrial control systems (ICS) or SCADA (referred to hereafter as OT/ICS), these networks differ from information technology (IT) and therefore require tailored cyber security solutions.

Benefits

BLUE Lightning stands out from most OT/ICS security devices for several reasons. First, BLUE Lightning protects against attacks that may have circumvented perimeter defenses or jumped an air gap. Additionally, it does not rely on known malware signature libraries so it can detect the effects of zero-day threats. BLUE Lightning can also detect spoofing attacks, avoiding the pitfalls of threats like STUXNET and its present-day successors, even if the malware has gained control of a programmable logic controller (PLC) or remote terminal unit (RTU). BLUE Lightning also provides physical layer protection down to "Level 0" for older, serial-connected industrial devices on the network. Finally, BLUE Lightning can assist with advanced warning of non-malicious wear and tear for preventative maintenance saving you money in repair costs.

How It Works

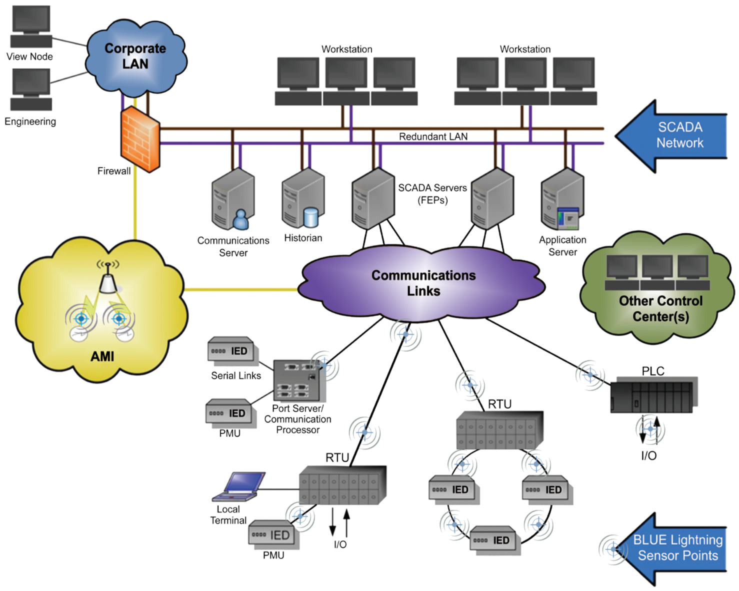
BLUE Lightning passively monitors OT/ICS networks to detect and alert operators to anomalous behavior using two patented algorithms. The algorithms focus on analyzing changes in the index variables associated with industrial processes (critical infrastructure, manufacturing etc). They also provide secondary validation of the data reported to human machine interfaces (HMI) to prevent spoofing attacks. The alerts are provided using a secure communication channel, and the information can be streamed to any security information and event management (SIEM) system. This revolutionary technique does not chase malware, but centers on conditions-based monitoring and makes BLUE Lightning a one-of-a-kind solution. The conditions-based maintenance benefit is derived from the fact that anomalous network behavior is often a leading indicator of normal wear and tear.

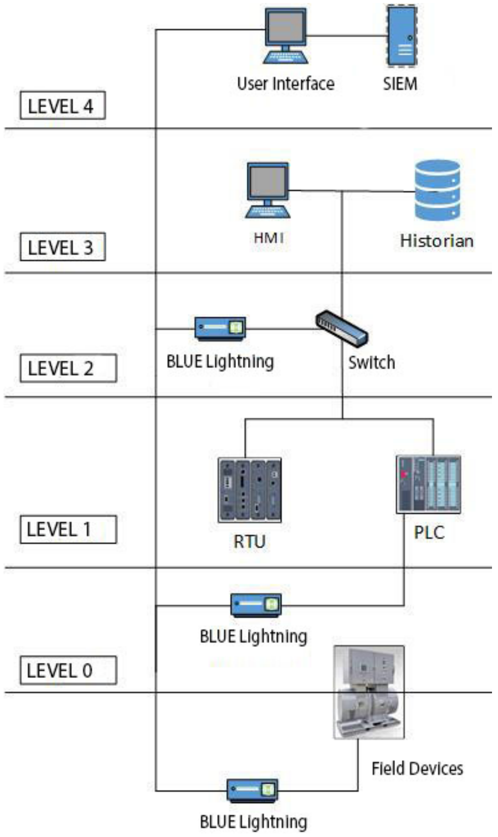
BLUE Lightning provides cyber security tailored to the OT/ICS used in critical infrastructure and manufacturing.

Deployment Architecture

BLUE Lightning can be deployed in line, between industrial systems and their control devices, or out of band via a network switch. It can also be deployed in concert with, or independent of, your control system provider's PLCs, RTUs, data concentrators, and other industrial control system devices. Tailored now to industry standard protocols such as Modbus, DNP3, BACNet, and GOOSE, BLUE Lightning can be adapted to any new OT/ICS protocols in the future.

Small, low power, and sufficiently rugged for harsh outdoor and indoor environmental extremes (temperature, humidity, etc), BLUE Lightning fits into any architecture – no need to rework your existing OT/ICS. Likewise, as control systems evolve and mature, BLUE Lightning can adapt and continue to operate, delivering first in its class data security at the lowest level – below your SIEM, below your routers, below your processing, and separate from traditional log reviews, which can be manipulated.


View Node
Engineering
Corporate LAN
Firewall
Workstation
Workstation
Redundant LAN
SCADA Network
Communications Server
Historian
SCADA Servers (FEPs)
Application Server
AMI
Communications Links
Other Control Center(s)
IED
Serial Links
Port Server/ Communication Processor
IED
PMU
PLC
RTU
I/O
RTU
Local Terminal
IED
PMU
I/O
IED
IED
IED
BLUE Lightning Sensor Points


User Interface
SIEM
LEVEL 4
HMI
Historian
LEVEL 3
BLUE Lightning
Switch
LEVEL 2
RTU
PLC
LEVEL 1
BLUE Lightning
LEVEL 0
Field Devices
BLUE Lightning