PROTECTING INDUSTRIAL CONTROL SYSTEMS AND SCADA NETWORKS

Starting with the Industrial Revolution in 18th-Century Manchester, the manufacturing industry has typically undergone a revolution every hundred years. In an age of ever increasing technological advancement, though, times are changing at a faster pace, as we see the era of controller-based automation gradually replaced by the 'Smart Factory', otherwise known as Industry 4.0 or Smart Grid in the Energy market.

While this progress aims to streamline manufacturing processes, these changes also bring new cyber risks and threats to Industrial Control Systems (ICS) that are vulnerable from exploits that are now freely available on the Internet. The vulnerabilities vary from basic issues like systems without passwords or with hard-coded passwords to configuration issues, software bugs and hardware vulnerabilities. Once an attacker is able to run software on a host that has access to a controller, the likelihood of a successful attack is very high.

This paper presents a summary description of the threats to Industrial Control Systems used in Critical Infrastructure and manufacturing and suggests guidelines for mitigating this risk using a multi-layered security strategy.

ICS/SCADA NETWORKS

ICS/SCADA networks and devices were designed to provide manageability and control with maximum reliability. While their implementation is often proprietary, SCADA controllers are essentially small computers. As a result, the familiar challenges associated with vulnerabilities and exploits apply to ICS/SCADA systems, with the additional challenge of such systems operating in environments that can be physically difficult to reach or that can never be brought offline.

Industry, manufacturing and critical infrastructure facilities (electricity, oil, gas, water, waste, etc.) as well Building Management Systems (BMS) rely heavily on electrical, mechanical, hydraulic and other types of equipment. This equipment is monitored and controlled by Industrial controllers (PLC, RTU, and HMI) and sensors. These systems are connected to management systems such as SCADA (Supervisory Control and Data Acquisition) or DCS (Distributed Control Systems) and form an ICS (Industrial Control System) solution

ICS enables efficient collection, monitoring and analysis of data and automation of production and industrial processes. The benefits that these systems provide have contributed to their wide adoption. Their ruggedness and stability enable critical infrastructure-related facilities to use ICS/SCADA solutions for long periods of time—often in excess of 10 and sometimes 20 years and beyond.

ICS/SCADA THREATS

However, the benefits provided by ICS/SCADA systems make them equally capable of damaging infrastructure operations and processes. By altering the commands sent to the controllers, changing the controller logical sequence or by changing sensors readings, attackers can create changes in the industrial processes. These changes can introduce sudden and apparent or slow and hard to notice modifications to factory processes.

Threats with no focus can be as destructive as targeted attacks. In the first half of 2018 Check Point found that crypto miners attacked 32% of the organizations in the Utility sector. As in the IT sector, crypto mining software can overload and negatively affect the operation of the enterprise's ICS components. At the very least impede operators from interacting with the controlled process in real-time.

Likewise WannaCry infections in the industrial networks also caused unexpected damages leaving operators incapable of monitoring and controlling industrial processes.

Targeted APT attacks from individuals or organizations with a detailed understanding of ICS environments can be especially devastating. These can be disgruntled employees, foreign governments, business competitors, criminals or political/ideological activists.

In order to alter a controller command or change a sensor reading, an attacker needs to either access the controller/sensor itself or to access a remote system which is communicating with it. This requires either physical or remote access to some computer or network that is connected to the controller/sensor.

Most ICS/SCADA networks have some level of perimeter defense, including network segmentation and firewall technologies. Bypassing such perimeter defenses from the outside is typically relatively difficult, and so attackers are always looking for alternative ways to get inside - for instance, through a gate that is left open, or by triggering some operations from inside the organization that opens up a communication channel to the outside.

Once inside, the attackers might leverage information that they have about the network, or else conduct reconnaissance to learn the environment. Or, they might just try well-known access methods to see if they work due to weak or incomplete network security policies. Very frequently, weaknesses in specific vendor implementations of a protocol or typical system/security configuration mistakes are the threat actors' first target.

December, 2017

A new malware dubbed Triton has been spotted targeting safety controllers in Critical Infrastructure in Saudi Arabia, causing a shutdown.

February, 2018

A Monero cryptocurrency miner was installed in a European water utility provider network after first infecting a Human Machine Interface (HMI) of the SCADA network.

March, 2018

Russian scientists arrested by the FSB for trying to use the computing power of a petaflop supercomputer in the Russian Federal Nuclear Center to mine Bitcoin.

June, 2018

New malware, VPNFilter, found targeting Critical Infrastructures that supply chlorine to water treatment and sewage plants across Ukraine.

August, 2018

Financially motivated threat actors conducted a surgical spear-phishing campaign targeting entities in the industrial sector, including at least 400 companies in Russia in the energy, manufacturing, oil and gas industries.

ICS/SCADA SECURITY CHALLENGES

While an ICS/SCADA implementation is often proprietary, cyber threats targeting ICS/SCADA are increasing rapidly and Critical Infrastructure sectors are beginning to recognize the need for better security. This is evidenced by the demand for ICS-CERT (Cyber Emergency Response Team) assessments which grew 16% from 2015 to 2016 and 35% from 2016 to 2017.

The core factors contributing to allowing a threat to exploit ICS/SCADA vulnerabilities are due to the nature inherently built into these environments. For instance they often use propriety operating systems that have not been subjected to security hardening. Out-of-box systems with default or simple passwords and baseline configurations make it easy for attackers to enumerate and compromise OT systems.

Their software cannot be updated or patched frequently, due to access limitations, concerns over downtime or the need to re-certify. OT systems typically run on legacy software that lack sufficient user and system authentication, data authenticity verification or data integrity checking features that allows attackers to inject commands and manipulate parameters to modify, delete, or copy information on controlled access systems. Additionally, operation managers don't use available software patches for known and published security vulnerabilities of their ICS equipment. With a reasoning of “if it works, don’t touch” to keep up time of the production systems as the highest priority.

They use proprietary or special protocols. Legacy SCADA controllers and Industrial protocols lack the ability to encrypt communication. Inherent security functions and encryption allow attackers to use sniffing software to discover username and passwords. They are often installed in locations that are difficult to access physically, e.g. on towers, on an oil rig, on a working robot and are environmentally more challenged than regular IT systems, e.g. outdoors, extreme temperatures, vibrations or require special input voltages and mounting options.

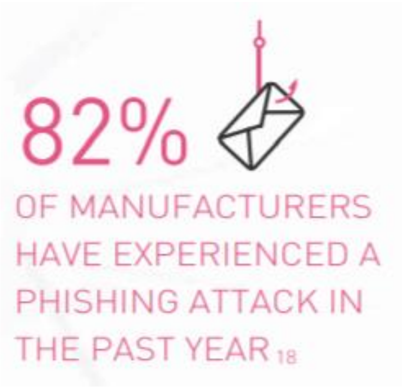
A common belief is that ICS/SCADA networks are physically separated from corporate IT networks. This might be accurate physically, in the sense that some companies operate distinct LANs or air gap their control and corporate networks from one another. In other cases, companies use the same LANs and WANs, but encrypt their ICS/SCADA traffic across a shared infrastructure. More frequently however, networks require some level of interconnectivity in order to obtain operational input from and/or export data to external 3rd party and ERP systems within the organization.

ADOPT AN END TO END SECURITY STRATEGY

ICS security must be built in layers to prevent attacks from external and internal sources. In the following we will present a segmented, multi-layer defense-in-depth strategy designed for the requirements that are unique to IT and OT networks. One solution does not fit all. ICS/SCADA infrastructures require dedicated security techniques that satisfy their unique operational requirements.

Prevent Threats at the Source in IT and OT Networks

Infrastructure attacks are a relevant and imminent threat to any organization. Many of the recent attacks on OT and ICS networks were found to be based on IT attack vectors, such as spear phishing via Email and Ransomware on Endpoints. Using Check Point Threat Prevention solutions such as SandBlast (sandboxing), network and endpoint security can prevent and eliminate those attacks prior to breaching the ICS equipment.


82%
OF MANUFACTURERS HAVE EXPERIENCED A PHISHING ATTACK IN THE PAST YEAR 18

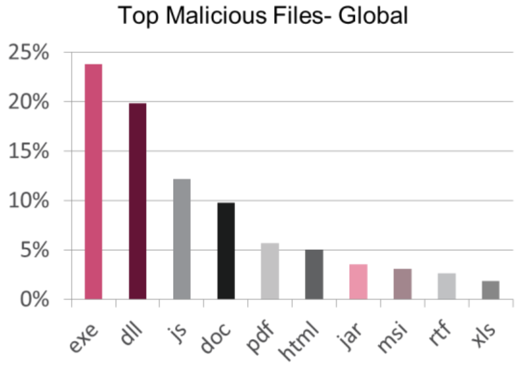
Threat Prevention technologies can also be effective when deployed in OT networks. For instance SCADA vendors continuously release vulnerability advisories for their ICS devices. Unfortunately, unlike the IT environment where patches are easily installed, the OT environment is not quick to install and upgrade their machines, leaving systems unpatched.

The time between the moment the vulnerability is disclosed and the moment a patch is available is known as the Window of exposure or “vulnerability window”. This window is extremely large and can often last months and even years. Intrusion Prevention Systems (IPS) can significantly reduce the application vulnerability window when used as a “virtual patching” solution to protect known vulnerable Windows based workstations, servers and SCADA equipment.

Likewise antivirus can protect against well-known malware, preventing threats such as STUXNET, BLACKENERGY2, HAVEX, TRITON, and CRASHOVERRIDE that has been known to create havoc in the ICS/SCADA environments. Malicious code including a virus/malware/trojan can be extremely harmful to SCADA systems and underlying infrastructure. It is important to protect endpoint applications from malicious code as organizations can no longer rely on legacy solutions to protect ICS/SCADA infrastructure.

When a host or server does become infected, then detecting and mitigating the effect of the infection is of utmost importance. Anti-bot technologies perform the same precautionary functions as that of canaries in a mine, a defense dating back to the early 1900s.

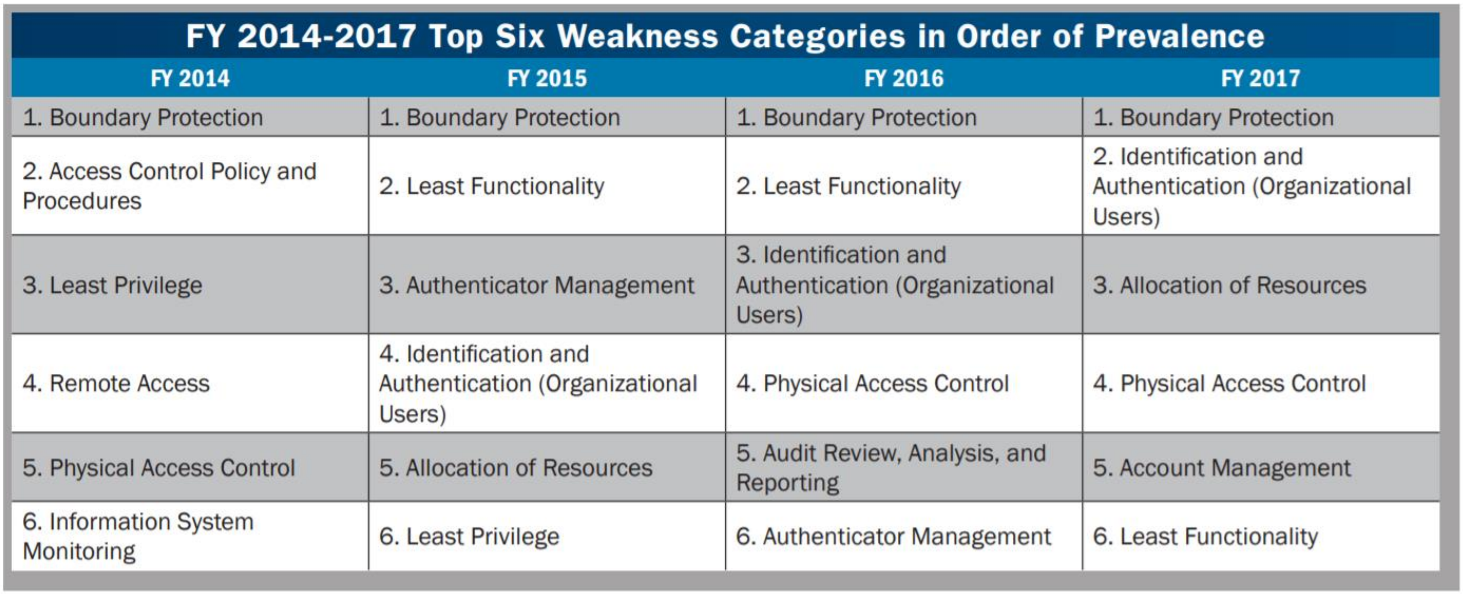
While not specifically designed to disrupt the operation of any industrial system, bot infections may pose a significant threat, causing network failures, denial of service (DoS) of the infected system and other devices on the network. Industrial Internet of Things (IIoT) devices are especially vulnerable. While you typically cannot deploy antivirus on these devices, network-based Anti-bot technologies can help detect and mitigate the damage done by infected IoT devices.



The past shows that the IT environment, which is usually connected to the Internet, can be a channel into the operational technology environment. It is critical to use mechanisms such as Threat Emulation (sandboxing) to ensure an attacker is unable to run software that has access to a controller. Threat Emulation can identify malicious software embedded in files (Excel, Word, Power Point, PDF, EXE) reducing the likelihood of a successful attack from unknown and targeted threats to IT and the OT management networks.

SEGMENT IT AND OT, APPLYING LEAST PRIVELEGE ACCESS

According to the US ICS-CERT report: (Jan-18) - FY 2017 Most Prevalent Weaknesses, Boundary Protection is ranked Number 1, for 4 years in a row. For this reason, boundary protection enforcement should ensure the availability, integrity and confidentiality of this data by following these guidelines.



FY 2014-2017 Top Six Weakness Categories in Order of Prevalence

FY 2014	FY 2015	FY 2016	FY 2017
1. Boundary Protection	1. Boundary Protection	1. Boundary Protection	1. Boundary Protection
2. Access Control Policy and Procedures	2. Least Functionality	2. Least Functionality	2. Identification and Authentication (Organizational Users)
3. Least Privilege	3. Authenticator Management	3. Identification and Authentication (Organizational Users)	3. Allocation of Resources
4. Remote Access	4. Identification and Authentication (Organizational Users)	4. Physical Access Control	4. Physical Access Control
5. Physical Access Control	5. Allocation of Resources	5. Audit Review, Analysis, and Reporting	5. Account Management
6. Information System Monitoring	6. Least Privilege	6. Authenticator Management	6. Least Functionality

It is recommended to maintain physical network separation between the real time components of the SCADA network (e.g. PLCs) and other networks, especially the Internet. Deploy a secure remote access solution into the network such as client-to-site VPN that supports strong multi-factor authentication. To prevent tampering with legacy ICS/SCADA data that is communicated in open text without encryption, create secure site-to-site VPN tunnels between boundaries interconnects.

Security gateways should be installed at all interconnects, ensuring that only relevant and allowed traffic is entering/leavi ng the network. This validation should be done on all communication, protocols, methods, queries and responses and payloads using firewall, application control, IPS and antivirus.

Assign separate workstations for SCADA management software. Dual homed workstations that connect to both an internal critical network and to other less sensitive networks or even the Internet is a major risk. In cases where such configuration is mandatory, software and security configuration should limit the operations that can be performed on the workstation.

PROTECT OT WITH SPECIALIZED ICS/SCADA SECURITY

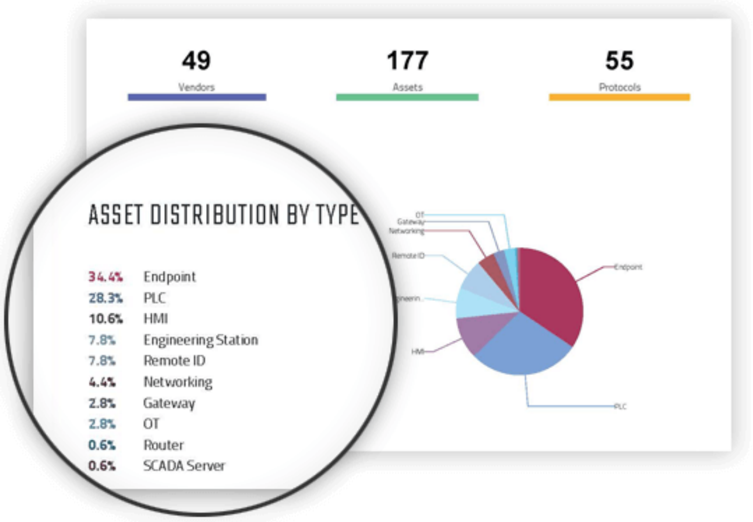
To achieve the level of protection needed for industrial and critical networks, security needs to grow from a collection of disparate technologies and practices to an effective business process. While no system is 100 percent secure, implementing security that is designed for ICS/SCADA networks can greatly improve the security posture of these networks.

Visibility **Baselining** **Enforce with Zero Impact**

Visibility

To properly define a security policy you must have solutions in place that provides visibility and understanding into the ICS/SCADA environment. More often than not, these environments are considered as a black box. An “if it works, don’t fix it” approach is taken. Some of these machines have been installed and working for many years; 5, 10, 20 or even more, and therefore the deep understanding of the communication may not even be known.

Visibility means seeing all of the assets in the OT environment, knowing what they are and what function they perform. Further it is about understanding granular configuration information for each asset, how the assets are communicating in the network and specific details about the application-level (layer 7) process automation conversations.



Assets and Network Architecture Elements

Communication	Asset Information	Network Mapping
Understanding protocol & commands, are those serial based protocols or IP based? Asset connections within the ICS network, who communicates with whom?	IP and MAC address Equipment vendor and type Equipment model, serial # and version	Network mapping based on Purdue model Asset communication channels Asset inventory

We do this with a process called multispectral data acquisition which supports passive and active collection methods. The data is enhanced and enriched with our App DB technology.

The least intrusive asset detection method is the passive collection method. This is continuous, real-time monitoring of OT Networks which discovers network communications and asset details to the I/O level. This is a field proven technique that is 100% safe for OT networks.

Our active collection method is designed to be safe for OT networks. This method uses precise and periodic queries that add enhanced visibility into asset configurations and enhances the context for alerts. Active collection provides data that is not available via the passive collection method.

There are two main ways that traditional active collection causes harm in OT networks. First, queries can end up saturating the small pipes that make up many industrial networks. Further, it can impact the legitimate OT traffic. To avoid the saturation issue, the system has the ability to rate limit the number of concurrent queries. For the incorrect protocol issue, we employ a combined passive and active approach.

Our App DB technology provides an offline enrichment of OT asset data. This process ingests and parses PLC/RTU project and other configuration files and binaries and adds nearly 100% to the asset coverage and configuration details.

We find that both active and passive collection methods are needed and complement each other. A passive capability provides a rather impressive, and often startling array of data about the assets on an ICS network. For many environments this level of detail is adequate. But some use cases need more lower-level detail, and this type of passive scanning can't discover everything. In addition passive techniques are not able to yield some endpoint configuration data, e.g. which patch level a Windows or Linux machine is running, which software packages are installed on these nodes or the version of virus definition files.

There are also instances where devices don't communicate on the network, or communicate very infrequently, so passive is not able to capture data about these nodes. And in a few situations, we simply don't have access to devices, e.g. they are on a different network segment or the customer has an unmanaged switch without SPAN or mirror capabilities. In these cases the use of multispectral data collection enriches our already robust dataset.

Lastly, and very importantly, some plants or operational environments simply cannot easily or cost effectively deploy passive Deep Packet Inspection (DPI). Some plants don't have a modern switching infrastructure that supports SPAN/Mirror ports. And even in plants that do, internal change management processes add substantial time constraints. In these cases active and App DB may prove to be more cost effective and substantially the reduce asset collection time.

Baselining

With the above techniques we have a behavioral baseline that characterizes legitimate traffic. To enhance our baseline we rely on two approaches, traffic logging and behavior analysis. The Security Management server logs each SCADA and IT protocol or command seen by the Security Gateways. This provides both forensic information and assists in the creation of baseline security policies. In addition our Asset and Anomaly Detection (AAD) system creates Behavior Analysis profiles of all of the communications that happen between assets in the network, such as frequency and type of communication. This generates a very high-fidelity baseline that can be used to detect anomalies, create virtual zones and hunt for threats in the OT network.

Virtual zones are created automatically, providing and maintaining a view of the current state of OT/ICS process-level communications. This is not simplistic net flow. It is a deep understanding about how the industrial assets in the environment are communicating and the actual process automation conversations taking place between assets. With this understanding of how the industrial automation system is configured and communicating, our proprietary algorithms create logical groupings of assets and add new assets to the appropriate groups. This automatically generates an ideal segmentation strategy and a virtual segmentation scheme of the OT network.

Virtual segmentation is a cost effective way to rapidly enhance the security of the plant or operational environment. In addition virtual segmentation is a practical option for segmenting the lower layers of the OT network where blocking is prohibited because of the very negative impact it can have on operational processes, e.g. between Layer 1 and Layer 2 of the Purdue model. In addition with virtual segmentation, alerts based on cross-zone violations receive high risk status, saving your Security Operations Center (SOC) team valuable time.

Enforce with Zero Impact

Securing ICS and SCADA networks is critical for ensuring manufacturing capability, service continuity and public safety. Whil e, the IT world has gained significant experience in protecting computer networks, the same can only be done in OT networks when understanding the difference between OT and IT environments. First and foremost, operation managers are not keen on preventing any communication within the ICS networks.

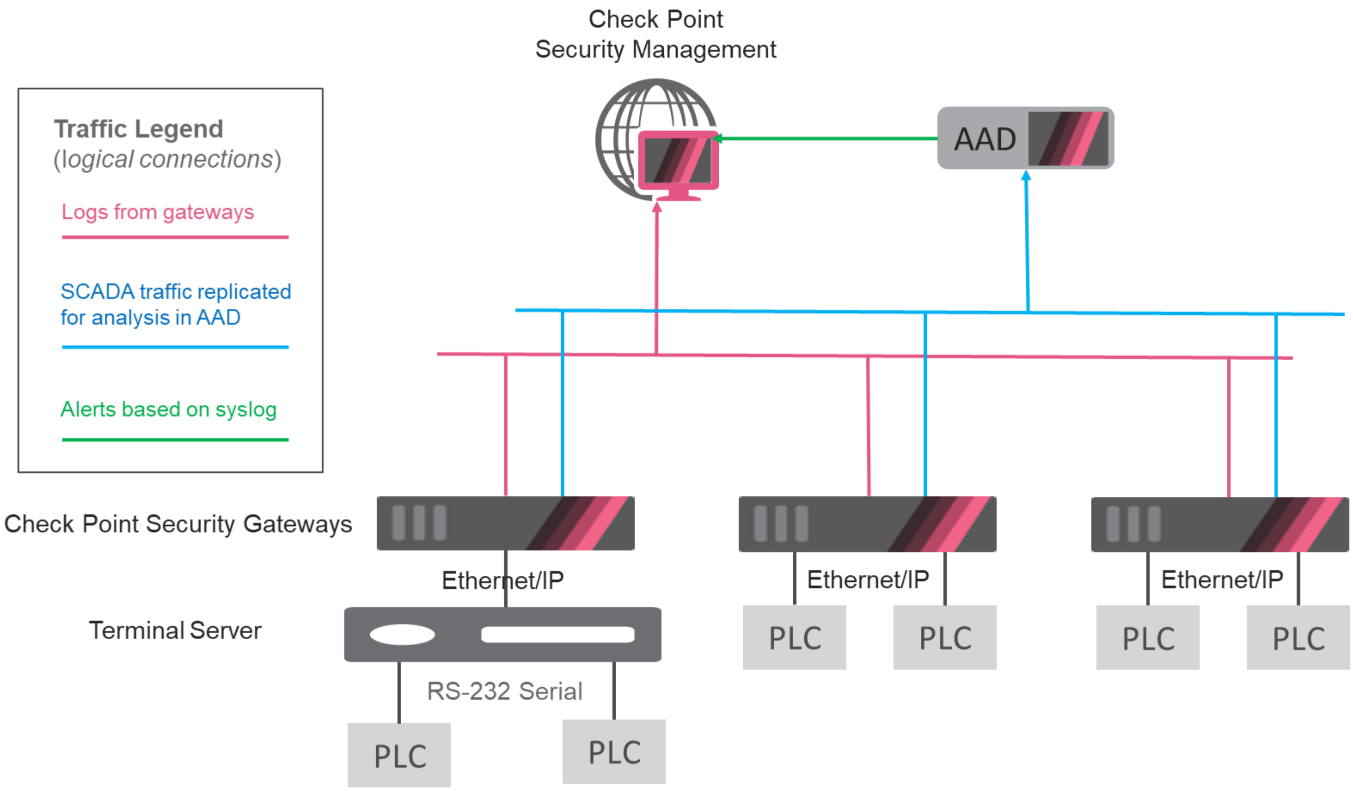
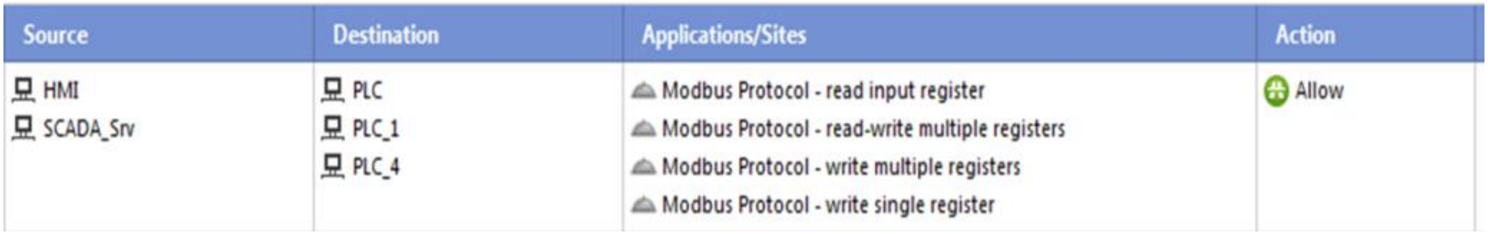


Figure 1: Single Site Basic Configuration

With a baseline based on traffic logs, we can create rules based on learned protocols and commands to safely protect the OT network with zero impact on operational processes. The baseline policy allows only what has been learned from earlier log analysis. Any other command will generate an alert for an operator. In addition, policies can be defined to implement time of day and traffic pattern policies to quickly and effectively detect, counter, and expel an adversary, on a single or group of commands.



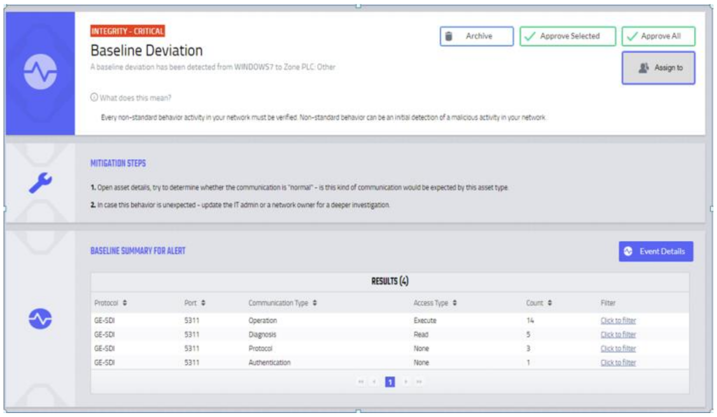
Source	Destination	Applications/Sites	Action
HMI SCADA_Srv	PLC PLC_1 PLC_4	Modbus Protocol - read input register Modbus Protocol - read-write multiple registers Modbus Protocol - write multiple registers Modbus Protocol - write single register	Allow

Figure 2: Baseline Policy

In addition with our behavior analysis baseline and knowledge about how ICS systems work, the AAD system employs advanced pattern matching techniques, generating rich alerts when anomalous activity or critical changes occur. We separate alerts into two types: process integrity and security alerts.

For example, the system can spot a single deviation from an assets' baseline such a new card in a PLC or a Windows endpoint issuing a write command to a controller it has never communicated with before. More complex events comprising multiple baseline deviations are possible. The system can analyze and consolidate events into a single, human readable alert. In both cases, the system provides detailed context with the alert enabling rapid investigation and response.

Examples of security alerts are those issued for Wannacry malware or Man-in-the-Middle attacks.



INTEGRITY - CRITICAL

Baseline Deviation

A baseline deviation has been detected from WINDOWS7 to Zone PLC: Other

What does this mean?

Every non-standard behavior activity in your network must be verified. Non-standard behavior can be an initial detection of a malicious activity in your network.

MITIGATION STEPS

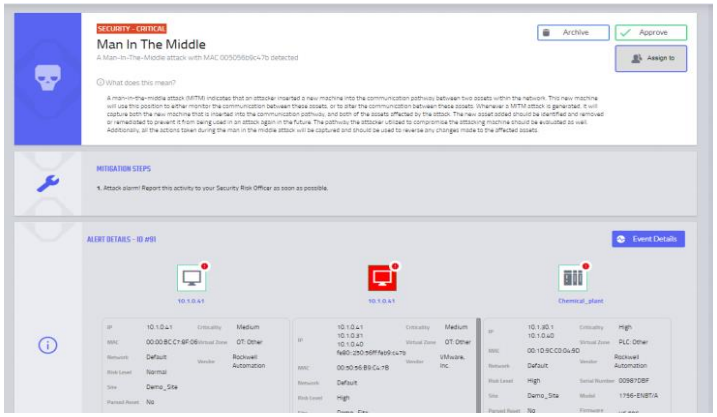
1. Open asset details, try to determine whether the communication is "normal" - is this kind of communication would be expected by this asset type.
2. In case this behavior is unexpected - update the IT admin or a network owner for a deeper investigation.

BASELINE SUMMARY FOR ALERT

RESULTS (4)

Protocol	Port	Communication Type	Access Type	Count	Filter
GE-SDI	5311	Operation	Execute	14	Click to filter
GE-SDI	5311	Diagnosis	Read	5	Click to filter
GE-SDI	5311	Protocol	None	3	Click to filter
GE-SDI	5311	Authentication	None	1	Click to filter

Figure 3: Process Integrity Alert



SECURITY - CRITICAL

Man In The Middle

A Man-In-The-Middle attack with MAC 005056b9c47b detected

What does this mean?

A man-in-the-middle attack (MITM) indicates that an attacker inserted a new machine into the communication pathway between two assets within the network. This new machine will use this position to either monitor the communication between these assets, or to alter the communication between these assets. Whenever a MITM attack is generated, it will capture both the new machine that is inserted into the communication pathway, and both of the assets affected by the attack. The new asset added should be identified and removed or remediated to prevent it from being used in an attack again in the future. The pathway the attacker utilized to compromise the attacking machine should be evaluated as well. Additionally, all the actions taken during the man in the middle attack will be captured and should be used to reverse any changes made to the affected assets.

MITIGATION STEPS

1. Attack alarm! Report this activity to your Security Risk Officer as soon as possible.

ALERT DETAILS - ID #91

IP 10.1.0.41 Criticality Medium
MAC 00:00:BC:C7:8F:06 Virtual Zone OT: Other
Network Default Vendor Rockwell Automation
Risk Level Normal
Site Demo_Site
Parsed Asset No

IP 10.1.0.41 10.1.0.31 10.1.0.40 fe80::250:56ff:feb9:c47b Criticality Medium
Virtual Zone OT: Other
Vendor VMware, Inc.
MAC 00:50:56:B9:C4:7B
Network Default
Risk Level High
Site Demo_Site

IP 10.1.30.1 10.1.0.40 Criticality High
Virtual Zone PLC: Other
MAC 00:10:9C:C0:04:9D
Vendor Rockwell Automation
Network Default
Risk Level High Serial Number 00987DBF
Site Demo_Site Model 1756-ENBT/A
Parsed Asset No Firmware

Figure 4: Security Alert

The result of these techniques is real time threat monitoring of your OT network. Any critical change that may pose a potential or actual impact to the industrial process is rapidly detected. In addition known and unknown threats will be identified when their anomalous behavior and other indicators reveal their malicious presence.

Anomaly detection has also been proven effective for detecting threats. The National Institute of Standards and Technology's (NIST) National Cybersecurity Center of Excellence (NCCoE), in conjunction with NIST's Engineering Laboratory (EL) released NISTIR (Interagency Report) 8219 which demonstrates behavioral anomaly detection capabilities support cyber security in manufacturing organizations.

> "… *enables manufacturers to detect anomalous conditions in their operating environments to mitigate malware attacks and other threats to the integrity of critical operational data. With the correct Platform you can assess the security posture of your ICS network, protect critical systems, control access to network assets, continuously monitor and detect vulnerabilities and threats, and rapidly investigate and respond to cyber incidents.* "
> --NISTIR 8219

SUMMARY

The mission of protecting industrial control systems (ICS) is so vital it cannot be left to just any security solution. Every day, we expect water to flow from our faucets, our lights and electricity to work, and traffic lights to move traffic along quickly and efficiently. As citizens and customers, we have zero tolerance for interruptions in essential services even for a few hours, much less days or weeks.

ICS services span everything from electrical grids to water management, oil pipelining to gas refineries, waste treatment to traffic control and more. However, all these services deal in huge capacity volumes that require heavy-duty electro-mechanical controllers and sensors.

Control of these sensors is typically through dedicated networks using a unique industrial control method called SCADA (supervisory control and data acquisition). Demands for greater efficiencies have driven more of these devices to be network accessible. They're now subject to the same infections, malware, and bot attacks of any other computer-based device.

Protecting these industrial control systems requires a deep understanding of the unique challenges and characteristics of these environments. This can be achieved with advanced threat prevention that prevents known and unknown threats at the source – with security that provides virtual patching for known vulnerable and unpatched systems - with security that provides edge and internal boundary protection - with security that baselines normal asset and network communications within the OT network – with security that alerts when an anomaly deviates from normal baseline – and with security that does all of this with zero impact to normal operational processes. You should demand nothing less than this. The stakes are too high to consider otherwise.

REFERENCES

[1] NCCIC/ICS-CERT Monitor November-December 2017, Gaithersburg, MD, Jan., 2018 [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2017_S508C.pdf
[2] “Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection” NIST, Gaithersburg, MD, Nov., 2018 [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8219/draft