Detection and Response Services in the ICS Environment

These days, it's critical to have good and adapted IT security in the production environments. Not only to ensure the needed stability in production, but also to have a proper visibility and thereby ensure good integrity as well. In general, the challenge is to obtain the right and necessary level of IT security that's adapted to the production and the individual organization.

This white paper will describe how to ensure good and adapted IT security in the production environment by using some general best practices in detection and response services: what information is needed, what are the general challenges, and what information is important to collect to create a good detection and response service for today's production environments in relation to IT security.

High availability with good integrity is critical

General challenges

Today, ICS (Industry Control System) network doesn't simply require tremendous availability. It also requires a flexible and secure system that's integrated with the business network, thereby making it easy to run and monitor the business processes. This sounds easy, but it generates some challenges in relation to the IT security.

The ICS processes are not the same as the ones IT departments usually work with. This often generates some challenges in the organization, due to lack of understanding and communication between the IT staff and the production engineers. This is primarily an organizational challenge, however, from a technical standpoint you will find some insight into how some of the obstacles can be minimized.

The ICS network is critical for the business. It requires high availability with good integrity. At the same time, it's important to have a high level of IT security in the ICS network, although it can't be done with the same systems and processes as in the administration network.

Architecture

To design a good detection in the ICS environment, there are some basic requirements needed. One of them is an architecture that makes it possible or easier to collect the necessary information. The Purdue model (SANS Institute) is one of the examples of a good architecture. The Purdue model is shown in Figure 1 below.

EZENTA A/S
KØBENHAVN – Hørkær 14, Herlev
Tel. +45 7020 1260 :: info@ezenta.com
www.ezenta.com

When we have the architecture, we also have the possibility of making a good detection structure.

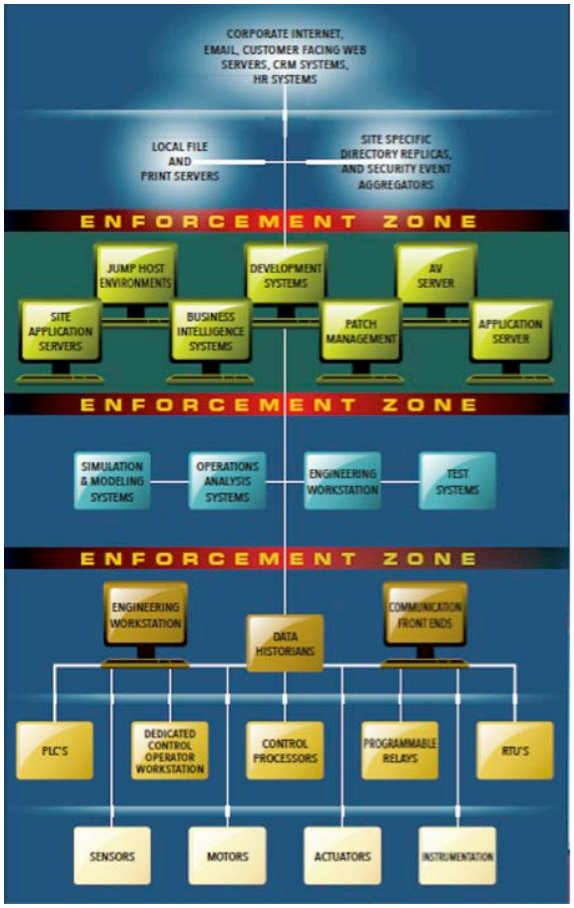


Figure 1 - Adapted SANS Institute Purdue model

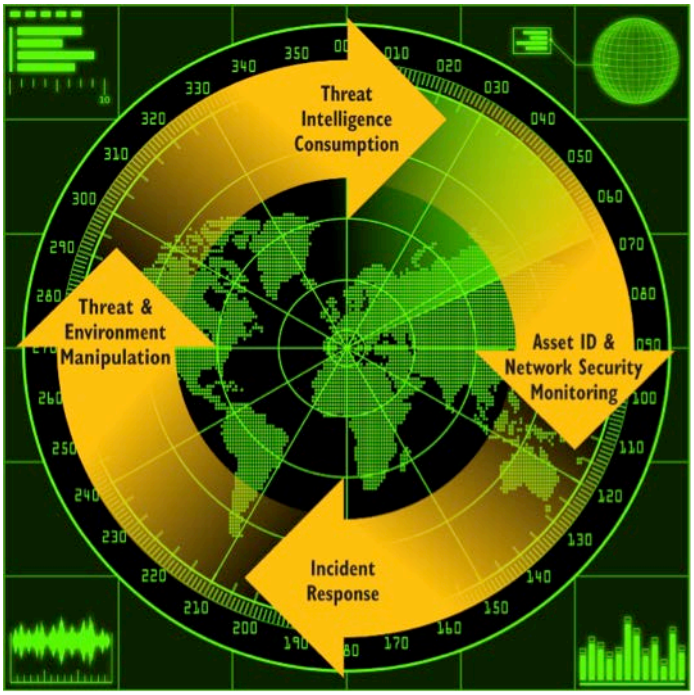
One of the main functions in the architecture is to implement chokepoints i.e. areas where traffic will go through which in addition it's great for monitoring. The enforcement zone is divided into subareas that also have possible chokepoints. This to be able to have the correct monitoring and integrity of the data in the ICS environment. One important piece of information to make the model even better is to highlight and increase the security level on the critical elements e.g. HMI, Historians and SCADA servers. These are highly critical elements and also possible primary targets for the adversary. It's important to have the possibility of monitoring the flow to and from the critical elements.

When the architecture is in place, the chokepoints should be where you want to monitor traffic and even implement firewalls in order to prevent the adversary to be successful. When we have the architecture in place, we also have the possibility of making a good detection structure. To be able to detect the advisory, we need to understand our ICS environment and monitor it.

What data to collect

This white paper will not go into the tools used to collect the necessary information. There are many different tools that can be used, both open source and commercial. However, when selecting a tool, it's important that the tool understands the protocols being used, and that it provides information that shows what's happening within the network.

In ICS environment, the communication flow is more structured than compared to normal IT communication. This provides an advantage when designing the detection and response service. The goal is to get as much information as needed in order to get a good visibility and details on what's happening in the ICS environment. The Active Cyber Defense Cycle (R. Lee, Dragos) is a good illustration of what kind of information that's necessary to collect. The Active Cyber Defense Cycle (ACDC) is shown in Figure 2 below.



Figur 2 - Active Cyber Defense Cycle

Firstly, it's important to understand the ICS network. It's not only important to understand the data flow, but also the elements in the ICS network and what it is they do. The asset identification is the process of understanding the ICS elements. This is e.g. HMI, OPC server, PLC or RTU. The important information to record is brand, type, address, protocols, and role. The information should be placed in the architecture to understand the position logically in relation to the Purdue model.

With the asset information, we now have an overview of the elements e.g. PLC and its placement logically. Next step is to get information about the data flow in the ICS network. This is critical, not only in regards to the data going through the firewalls, but also data in the ICS network i.e. east – west traffic, such as traffic between SCADA server and PLCs. The recommendation is to collects PCAP files and information. A PCAP shows the actual data flow on the specific collection point in the ICS network. Be aware that it isn't possible to collect all data. The most important points are the chokepoints in the Purdue model, and the points collecting data from critical elements.

Having a good architecture and collected information from assets and network is critical

With this in place, we have an overview of the ICS network and collection of data flow from important points in the ICS network. The last, but not least, important information needed comes from the ICS elements (assets). The information recommended to be collected from the assets, especially the critical assets, comes from event logs, services running and memory dumps.The windows event logs show e.g. failed login, applications and other security related information that's important to monitor. It's recommended to make a memory dump approximately every 9 months. The dump will show e.g. the processes running, last used registration keys, and IP addresses used. But only at the actual time of the dump.

Having good architecture and the collected information from assets and network, we now have the information needed to create our baseline for the ICS network which is important for the detection and response services. Having a good baseline is critical. This because abnormal traffic is one of the most important pieces of information when doing detection service in the ICS environment.

People

Always have ICS aware people on the team!

Before explaining how to detect a possible adversary and the process of the response service, it's important to understand the ICS business and network. Having the right team with proper knowledge is crucial when creating a functional detection and response service. The necessary knowledge not only relates to the IT security, but also understanding the ICS environment, communication and the differences between IT and ICS. Therefore, it's important to have people on the team with experience and a decent understanding of the ICS protocols in use, as well as communication, assets and business related to the production i.e. a subject matter expert. If this isn't the case, there's a high risk of decreasing the availability rather than increasing it. In short, **always have ICS aware people on the team!** Indeed, IT security people can be seen doing more harm than good in an incident response situation.

EZENTA A/S
KØBENHAVN – Hørkær 14, Herlev
Tel. +45 7020 1260 :: info@ezenta.com
www.ezenta.com

What to look for

Having a good baseline makes an Incident Response (IR) situation easier. This baseline is created by a collection done as described in the previous section. With the baseline and ICS understanding, it's easier to find the adversary.

Having the information and understanding of the ICS environment makes it easier to locate possible problems. There are several elements recommended when doing active detection in the ICS environment. Some of the general things to look for are abnormalities, top and low speakers, and encrypted traffic.

Abnormalities make for a big topic and are one of the best ways to spot adversary access or try accessing the environment. This can be caused by the adversary trying to get access to the HMI or a malware running in the environment. Most malwares will attempt to get access to a C&C server, and most adversaries will need to have access to the ICS environment from a remote site. If we have a good baseline, and we're able to monitor the network, discovering the network communication from a possible adversary or malware isn't that difficult. The challenge is to discover the difference between what is malicious traffic, and what is not. An understanding of the protocols and business processes of the ICS environment will help a great deal in understanding and analyzing the new traffic discovered. Abnormalities can also be in the assets e.g. HMIs. Instead of network traffic, the asset log files deliver good information.

Another area to look into is top and low speakers, not only based on the total communication, but also on ICS protocol communication. In the baseline, we have information on normal amount of traffic, to and from assets in the ICS network. Top speakers can be related to malware. This was seen in Stuxnet. Stuxnet had a large increase in S7 communication between the HMI and PLCs. This increase wouldn't necessarily alarm IT personnel, however a process engineer would discover that something was wrong. When doing a MiM (Man in the Middle) attack in the ICS environment, there will also be a large increase in ICS protocol related communication. The low speakers are also an area of interest when hunting for adversaries, since it's all about not getting spotted by the adversary. There will often be new assets or communication patterns, but only with a small amount of traffic. Therefore, both high and low speakers are important to look for when doing detection services in the ICS environment.

The last area to look at is encrypted traffic. Not because there are only these three areas to look at, but because these three are important areas in the detection process of ICS detection and response service in the ICS environment. Encrypted information isn't often used in the ICS network. Encryption is normally used between sites or other remote services, but within the local ICS network it isn't seen often.

EZENTA A/S
KØBENHAVN – Hørkær 14, Herlev
Tel. +45 7020 1260 :: info@ezenta.com
www.ezenta.com

It's important to know that many malware or adversaries first enter the business network and, from there, try to access the ICS network.

One of the great things about not using encrypted traffic is that we can look into the protocols and see what's happening. If there's encrypted communication in the local ICS environment, and this isn't something we know or are aware of, there's a possibility that it's malicious communication because many malware and adversaries use encrypted communication.

These were the three most important points to look for during the detection process in the ICS environment. It's important, however, to know that many malware or adversaries first enter the business network and, from there, try to access the ICS network.

Incident Response

When events aren't normal and appear as if they might include some malicious activity, the Incident Response (IR) process begins. However, only brief and high level information about the IR process is described subsequently.

The Incident Response (IR) process requires time, focus and personnel. This is not something to be done by one person. Some of the high-level pieces of information needed in addition to the baseline are PACP and memory dump files from the possibly affected assets. When collecting information, the order of volatility (SANS Institute, 2016) is critical. To minimize the destruction of possible evidence, the order of volatility is to collect the most volatile data first i.e. cache and register data, network information, memory, system processes, temporarily file-system, data on disk, remote logged data and data on archives.

Best practice is to ensure a good baseline, as described above. In addition, the packet capture files (PCAP) should be collected from the same possibly suspected areas, as well as the memory dump images. This data includes valuable data from both the network and the assets suspected of being malicious. To analyze the memory dump files, free tools like Redline or Volatility work well. With an add-on, Volatility can even compare the differences between two memory images.

In order to analyze data properly, it's important to have a good understanding and view of the ICS environment. Firstly, compare and analyze the data between the information areas i.e. memory dump and PCAP. This is necessary to obtain a proper overview of what's happening within the network. Here, a time analysis will provide some valuable information. Another area to address is in regards to tools like Redline or others that are designed for IT networks. Don't use or trust the automatic recommendations. ICS development is often not done the same way as IT software development. In Redline e.g. you have an MRI score; don't trust that recommendation when analyzing data from an ICS environment.

Incident Response (IR) is a big topic requiring both practice and knowledge. This passage has only looked at high-level information in the IR process, although it's an important area to prioritize when doing detection and response services in the ICS environment.

About the author

Søren Egede Knudsen has worked as an IT consultant since 1996 with more than 8 years of experience in ICS environments. He is a subject matter expert in ICS environments and has worked with ICS as a consultant in 5 different countries. Søren is CTO of Ezenta A/S and has designed the Ezenta MDR (Managed Detection and Response) service for ICS.

References and bibliography

Purdue model (www.sans.org)
Robert Lee, (Dragos), Active Cyber Defense Cycle model
SANS Institute, (2016), ICS active defense and incident response (515)
Gartner, (2016), Designing an Adaptive Security Architecture for Protection from Advanced Attacks
Gartner, (2017), Top 10 Strategic Technology Trends for 2017: Adaptive Security Architecture
Clint. E. Bondungen, Bryan L. Singer, Aaron Shbeeb, Stephen Hilt, Kyle Wilhoit, (2017), Hacking Exposed – Industrial Control Systems.