FAQ

Have any questions?

Frequently asked questions related from the ICS Cybersecurity Virtual Training.

Session 3 - Network Defense, Detection, and Analysis

Q 1. Can GrassMarlin be used passively to capture pcap data?

No. GrassMarlin can read in pcaps, but does not have the capability to create pcaps from traffic it reads live.

Q 2. How do you begin the discussion regarding the relationship between the OT and IT sections of an organization?

The discussion starts when one person decides it needs to happen. Create a calm environment with the necessary players explaining the benefits both sides can bring to the table. The skills, the knowledge, and contracts all play into a successful discussion. Many times, there is dissension because either IT has gone into OT demanding that certain patch processes be followed, or OT is not providing enough information to assist in an incident. All this needs to be put aside and start with what each sides role is. Sometimes it’s hard to put aside bad events but to move forward it is necessary.

Q 3. What are some ways to discuss Shodan, ICS Map, and ICS RADAR with stakeholders?

The best way to discuss Shodan, ICS Map and ICS RADAR is to do a demonstration. If you can have planned data from your company to use it will get your point across. Then be prepared how you would use this data to improve security.

Q 4. What type of firewalls are seen in an OT network?

Next Generation Firewalls are now providing support for OT networks and protocols. You will want to work with your vendors for an appropriate solution.

Q 5. Any suggestions for software to monitor just firewalls?

Talk to your vendor about monitoring solutions for your firewall.

Q 6. Is having a router at plant network that connects to the Corporate network secure to use from cyberattack? Does it require a firewall to protect? Is it necessary? Why?

You cannot use a router to securely separate networks. A firewall is required.

Q 7. Am I correct in understanding that Industrial IDS is not "a last line of defense" but an instrument of mitigation of impact consequences, as far as it can only discover compromised OT assets for roll-back, but it cannot protect them?

An IDS has the capability to identify malicious network traffic that could adversely affect your systems. It protects systems by letting the Cybersecurity Analyst know that malicious traffic has been sent or received by an OT asset. Once the analyst knows about the traffic, they can inspect the asset to determine if it was compromised or not.

Q 8. Is there any info about compare effectivity of industrial IDS based on deep packet inspection and one based on Honeypots?

An industrial IDS and a Honeypot are two different tools in your toolkit. IDS is monitoring and alerting on network traffic based on rules. A Honeypot is designed to fool attackers into thinking they are on a real system and encourage them to attack it so we can learn what the attackers are doing. You can learn from the Honeypot and apply the information to writing new rules for your IDS.

Q 9. When responding to an incident, what information is usually requested and what tools do you recommend.

Typically, organizations should have an incident response plan that will govern the response. The plan should be specific and address the OT environment.

Q 10. Do you have some options for considerations regarding checklists or guidance to promote OPSEC?

NIST 800-53 SC38 has guidance to OPSEC. There is also an INL paper regarding OPSEC and Control Systems. This information is available in the Appendix A.

Q 11. How can password vaults/managers be used for ICSs, specifically PLCs and similar components that often do not have easy I/O?

You can install a password manager on a shared/file server in the OT network and utilize it there when necessary.

Q 12. Why in OT do we delay for patches and what is the vendor's responsibility for patching and upgrades?

The typical mentality of OT should be never be first to install anything, even if it has been approved by the vendor. Also depends if a reboot is required, some machines cannot be rebooted without affecting the process. These machines might even have to wait for a process shutdown or Turnaround. The biggest concern in OT is to not affect the process. Patching is still important, just needs to be done carefully. Depending on the legacy system, vendors do a pretty good job at patching. Upgrades can be a mixed bag sometimes. With most control systems going to a windows platform, the vendors are tied to Microsoft which does not support the older systems. The best way to handle legacy systems is to have an upgrade plan and work towards it. Most vendors will help you with this.

Q 13. Will we be covering risk from mobile devices into trusted networks?

Mobile devices are discussed in the Defense section. They must be managed appropriately and not allowed on the OT Network.

Q 14. If you were to head a project integrating ICS security into a new facility, where would the most vulnerable location be and what could you do to prevent that from happening in the commissioning of the new facility?

Depending on the project and facility, your boundary defense will be the place to start. You will need to build in segmentation next to protect the assets.

Q 15. There was mention of having your docs only accessible by certain user groups. What would be your recommendation on how to maintain those sensitive documents to protect them from a network attack?

Place the documents on a file server in the OT Environment and only allow access to specific users or groups.

Q 16. Have you seen successful implementations, or are you able to provide examples of communicating the safety devices upwards to Operator minors through Diodes or other mechanisms, much like how remote logging is performed?

Yes. Remote logging is a great example. You can provide the same design as this and apply it to the items that need to speak up stream. You can also build a design that allows you to log that information local and replicate upstream to an SOC for analysis. This provides the ability for two sets of eyes, if available, to analyze the data and have redundancy in the data maintained.

Q 17. How do I effectively communicate all this to the corporate decision makers?

To communicate the importance to upper management, you need to understand what is important to management. They are concerned about profit, reputation, risk to the company.