Ensuring Operational Technology (OT) Cybersecurity in Life Sciences

15 Steps to Getting Started

VERISTA

Cyberattacks Such as Ransomware, Data Theft and/or Data Manipulation Are Not a Matter of Inconvenience – They Can Shut Down a Company's Operations

If you work in a Life Sciences company, you're probably hearing more and more about Operational (OT) security. But what does this mean? An OT network consists of all of the systems that support operations, such as industrial control devices, lab processing equipment, and QC test instruments. Often, automation engineers and IT system administrators suddenly find themselves in charge of an OT Network. Anyone in that position may be wondering where to start when it comes to securing the network or simply proving that it is, indeed, secure. As the late, great, Singer/Songwriter Harry Chapin once said, "When in Doubt, Do Something." (Korn, 2020)

Now, Harry said that when referring to his philanthropic endeavors to end world hunger in the 1970s. However, that quote is quite apropos when referring to Cybersecurity, especially in Life Sciences where the concept is relatively new. Some Life Sciences companies still have lab and manufacturing systems on the same network as their business systems, which means they are competing for network resources against enterprise systems like email, Zoom or MS Teams. Some organizations have migrated certain systems to an OT Network, or Industrial Control Network (ICN), but haven't completed the project. Others have segregated the networks nicely but aren't enforcing good security practices. Sometimes the list of things you need to do to properly secure your OT networks is simply overwhelming.

Regardless, whatever you do, do something. Surprisingly, the actions below don't have a large cost associated with them!

The approaches presented in this whitepaper are no / low-cost because they are based on the concept that your time spent on these activities are insignificant compared to the gains received by reducing costs and risk in your OT assets, network, manufacturing, and organization.

This paper explores 15 low/no-cost solutions you can implement to help ensure your networks, and therefore operations, are safe. The approach follows the Center for Internet Security (CIS) Controls v8 Implementation Group 1. (N.A., 2022)

STEP 1

Segment Your OT Network from Your Enterprise Business Network

Is your OT network segmented? Do you have any control systems that are connected to the Enterprise Business Network? Do any control systems have a connection to the Internet?

If your OT network is not segmented, plan to segregate it at the next opportunity. Some of the most publicized attacks on Life Sciences companies came to be simply because the control systems were connected to the Enterprise Business Network and/or the Internet. (Millar, 2021)

We recommend thinking about the Enterprise Business Network as the "untrusted" network. Since it is connected to the Internet, anything on it can be affected by one bad download or a cleverly crafted email that installs ransomware. Some malware kooks for OT devices so a segregated network prevents exposure of the assets to the malware.

In Figure 1 below, the network is segmented into industrial DMZ (Demilitarized Zones) and CZ (Control Zones). The iDMZ is split into the access and infrastructure zones. The access zone is used for remote desktop connections into the OT network, and the infrastructure zone includes the DMZ infrastructure servers to which users typically don't need access. The other parts of the business are separated into Control Zones (CZ's) that depict specific areas of the operation, such as a zone for infrastructure, manufacturing, building management systems, QC laboratory, material science and development. These zones include all virtual machines, hardware, machines, and instruments specific to that area. Each zone is assigned its own VLAN to assist in the segregation.

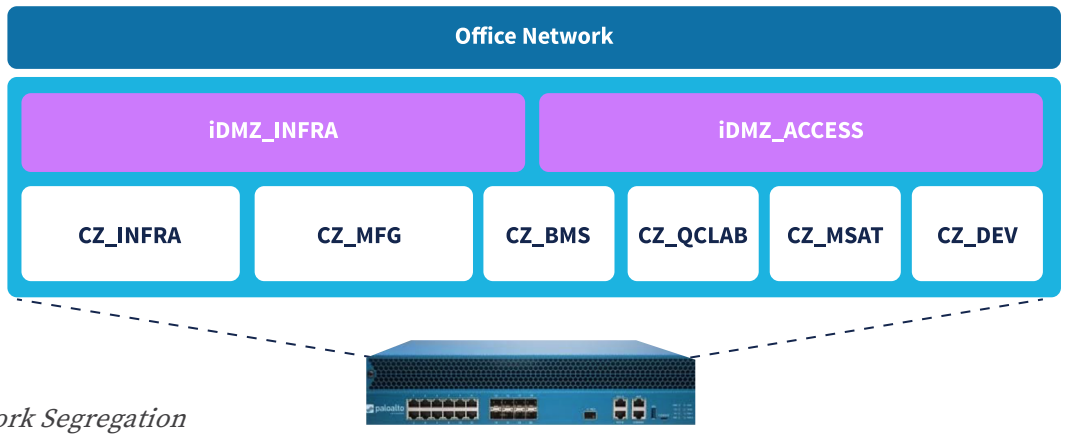

Figure 1: Network Segregation

STEP 2

Review Your OT Firewall Rules

When was the last time you reviewed the Firewall rules? What traffic is allowed in and out? What ports and protocols are allowed within those rules? Can we narrow it down further?

If you can't recall when you last reviewed the firewall rules, then now is the time. What we are looking for are rules that are too permissive. For instance, if the rule that allows files to be sent to an offsite storage location, and that rule allows communication over all protocols and all ports, then that rule is too permissive. Sometimes, when troubleshooting a network problem, firewall rules are created to solve the problem. When the problem is fixed, these rules can easily be left behind. As you can see from Figure 1, any time traffic moves from one zone to another, you need a firewall rule.

Are there any overlapping firewall rules?

As rules are added, especially during time-limited projects, sometimes overlapping rules creep into OT firewalls. Rules are said to be overlapping when they both allow the same traffic to pass to the same devices over the same protocols and ports. For instance, if rule #1 allows file sharing from the lab zone to the infrastructure zone and rule #2 allows file sharing from a particular server in the lab zone to the infrastructure zone, you have an overlapping rule and one that is too permissive in rule #1

Are there any 'deadwood' rules that can be removed?

Any firewall rules that aren't filtering traffic should be removed in the same way "dead code" is removed from a program. It isn't useful, and it isn't doing anything, so why have it in there with a relatively simple change.

STEP 3

Use a Standard Network Design Approach

Make sure your OT Network is separated from the Business Network with a next-generation firewall. These firewalls allow for deep-packet inspection, which aids in hunting threats on your network. Shown below in Figure 2, the OT Network is only connected to the enterprise network though the OT firewall, thus allowing us to control the traffic allowed in and out. The diagram also shows the redundancy implemented so that if one switch were to be down, the corresponding switch on the other side would take over routing traffic. In the Life Sciences industry, keeping

Step 3 (continued)

operations going is key to providing medicines to patients. This sample OT architecture provides the kind of robust, resilient structure needed in today's environment.

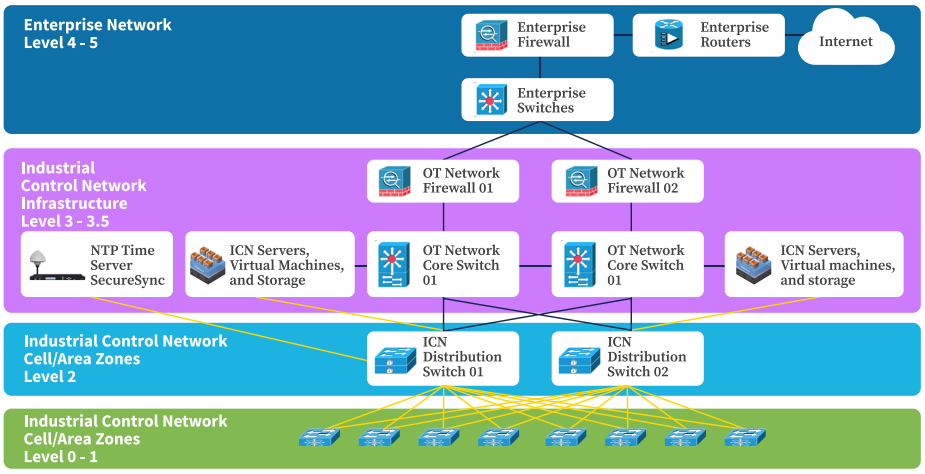

Figure 2: OT Architecture

STEP 4

Physical Security Should Not Be Overlooked

Physical security is not a significant challenge in the Life Sciences Industry since some form of perimeter security is already in place and an electronic badging system controls access to different areas of the building. With that said, all server rooms should have badge or key access, all OT network equipment should be secured in a lockable network rack, unused network ports should have port-locks installed, server enclosures should be locked, and the keys to these items should be controlled.

STEP 5

Control Access via Logical Security

Logical security should control access to the different areas or zones of the OT Network. Each user should have rights only specific to the information to which they need access. We can achieve that by creating a list of users and groups and mapping the users to those groups. Then, we verify that the user needs access to the groups to which they are assigned. Sometimes people move departments and retain access they shouldn't have. This is also a great way to find users that have left the company.

STEP 6

Asset Management: Take an Inventory of Your Devices

Do you *really* know what is on your network?

Most automation engineers can give a range of devices, but very few can give an exact number, even when given an opportunity to access an inventory tool. Also, when an exact number is readily available, it usually doesn't agree with other systems.

Therefore, it is recommended that you perform a scan of your network and make sure all devices are cataloged in some sort of an inventory system.

There are free and open-source Asset Inventory Systems that scan your network either actively or passively. Some are agentless, which is best, so nothing needs to be installed on the client workstations.

Once the scan is complete, I recommend you walk around each area of the plant and see what stand-alone systems exist. These systems may not be connected to the plant network, but you still may need to manage passwords and security updates on them.

Now, while you are collecting inventory, make sure to collect things like manufacturer part numbers and firmware version numbers. This will help you determine vulnerabilities.

Did you find any devices that weren't supposed to be on your network?

If so, determine what they are, where they are, and address them appropriately. While not always the most appropriate method, one company I was associated with used the "unplug it and see who yells" method. It was somewhat successful in finding things that were indeed, supposed to be on the network, but the proper process wasn't followed when they were added. Tracing wires and asking questions seemed to work better but requires time and resources.

Be sure to collect all software that is in use on the Industrial Control Network as well. That helps us track vulnerabilities, support contracts and end-of-life products just as much as the hardware inventory.

Did you find any software that wasn't supposed to be on the network?

Many times, users employ "Shadow-IT" in that they find a piece of software that works well for them and they install it on the workstation themselves. Many times, this is a productivity or comfort issue. In one instance, I found several workstations with an alternative text editor installed on them.

Many manufacturing facilities use their Computerized Maintenance Management System (CMMS) to track their OT assets. If yours does, add an annual or semi-annual preventative maintenance task to perform a network scan and update the CMMS inventory. For those that have an unwieldy number of devices, break the inventory up into quarterly or monthly scans. You can also inventory a manufacturing facility line-by-line, or room-by-room if that makes more sense.

Step 6 (continued)

Was it supposed to be on there? No. Was it inherently harmful? No. Was it helpful to the folks operating the equipment? Yes, it just never made it into the requirements document. So, we issued a change control and added it in. Often, communication is the key when it comes to things like this.

STEP 7

Manage Your Passwords

Do any devices still have the default or a 'backdoor' service password?

While you are connecting to your devices to perform that inventory from step 6 above, double-check that the devices don't have the manufacturer default passwords in them. These devices are at risk of being compromised and it doesn't require any real skill beyond knowledge of Google to do it. No one wants to explain to management that a device had the default password on it and that's why production is down. These devices include Industrial Network Switches, Data Loggers, PLC's, HMI's, Remote I/O, VFD's – literally anything that is connected to the OT Network, or standalone, but under your authority.

What about 'root,' 'administrator,' and any pre-configured vendor accounts on workstations and servers?

These accounts could be exploited in an under-the-radar attack since the attacker would have the "keys to the kingdom." Work with your vendors. Explain the issue of a machine having the same vendor maintenance password as the company down the street or within the same service area. It is best to change these and store them securely. The vendor's technician can request them from you when they come onsite – then change them after the visit. Worst case: If these passwords cannot be changed for whatever reason, disable the accounts and the vendor technician can request the passwords to be enabled when they come onsite to service the machine.

For every password leaked on the dark web, there is a corresponding article with a process on how to secure your passwords. Everyone seems to have a different system and every company seems to have different password requirements. I recommend a password manager to which all the people that would respond to an emergency on the OT Network have access. I recommend keeping the list small and rotating the passwords on a scheduled preventative maintenance task that aligns with your company policies. If those policies don't exist, create them.

Whether you use randomly generated passwords, or a password structure that you created, is immaterial. All the typical password suggestions apply: password length, upper and lower case, special characters, and

Step 7 (continued)

numbers should be defined in a policy. Additionally, the maximum time allowed between a forced password change, password change reminders, and the number of old passwords that are not allowed, should also be defined in that policy.

STEP 8

Enforce Auto-Logout

Auto-logout is a tricky issue in the OT world. Some vendors design their system assuming a service account is logged in all the time and if it logs out, the process stops. It is a poor design, but we sometimes have those constraints in OT. Lab equipment, filter integrity testers, blood gas analyzers, and particle counters are examples of devices that were not designed to be integrated into a modern, secure OT network. Many times, this equipment implements the bare minimum needed to connect to a network with no security features in mind.

All endpoints and servers should have an auto-logout policy in place if possible. This helps avoid the issue of one operator running the machine under another operator's login. The operators should also be trained to log out when they are done with a task and to NEVER share passwords.

For systems that don't meet your policies and procedures, document the risk. Let the organization decide if they want to continue using the device or find an alternative.

STEP 9

Implement an Account Management Policy

Does everyone have a unique login to every piece of equipment?

They should. There should be no shared logins. This one can be difficult to implement depending on the equipment and vendors, but the policy should be in place that everyone is unique and should have their own login. This way, if anything happens on a machine, it is easier to determine who did what and when. Not to blame anyone. But to find the cause and fix it so it won't happen again.

Do you have any people who have left the organization in which their user account is still enabled?

Work with HR and request a list of people who have left the organization within the past year and search for their accounts in the domain controller. If there are any stand-alone systems, search those too. Disable (but don't delete) any accounts found that aren't attached to users.

Step 9 (continued)

Then work with HR to get that list every month. You aren't breaking any confidentiality here. You are trying to protect the organization and even the person who left. You don't want an audit trail to reflect that someone pressed a button on a machine after they left the organization.

What about accounts that haven't been used in the past, say, 45 days? Are the accounts still enabled? Do the people attached to the accounts still work there?

These accounts should be disabled. If you can put a rule in place that does this automatically, even better. Now again, this needs to be considered thoughtfully. Why haven't the accounts been accessed? Is it a training issue? Are they using someone else's account? Do they only use that piece of equipment once-in-a-while? Talk to the people and find out. Set your policy to suit the organization.

How do people get access to assets upon new hire, or role change of a user?

Is there a process or form for the request? What about revoking access? If an operator moves from one department to another, do they still have access to the original department information?

Who has access to what in your organization?

Create a matrix of users and security groups and map the security groups to which each user is a member. The results can be surprising. Next, get the managers of those security groups engaged and do a quick review. Is the access appropriate for these users? Note that this is also a great way to capture users who have left the organization, but whose accounts are still active. This is also an opportunity to develop relationships with users and supervisors and have discussions about Cybersecurity.

STEP 10

Update Outdated Operating Systems

Do you have any devices running on Operating Systems that are no longer supported? Do they have to run on that OS?

Reach out to the vendor and plan an upgrade project. The project may not be no/low-cost, but the communication and planning certainly is.

Machines and instruments that communicate to a PC still running Windows XP are a security risk. If you can't upgrade it or get rid of it, then isolate it. Add an industrial firewall to isolate it from the OT Network by allowing only LDAP authentication, NTP and file backups through the firewall. Encourage the organization to begin researching newer technology.

STEP 11

Remediate Vulnerabilities

Do you know what vulnerabilities exist on your network assets?

This can be done manually or with a scanner. There are excellent open-source vulnerability scanners such as OpenVAS by Greenbone. Download a Kali Linux virtual machine and work through a tutorial on getting started, like the one on linuxhint.com. Scan the network for vulnerabilities in the same way you approached the inventory either all at once for small networks or in groups for larger networks.

There are commercial vulnerability scanners that are more specific to OT, and many have free trials available. Starting off small, this will give you a report listing vulnerabilities that need to be remediated. From here, start to remediate them. Some may require a minor configuration change, or an update to a new firmware, or a security patch applied to an operating system or application. For more complex remediations, find time in the production schedule or the next shutdown to perform the necessary remediations, develop a step-by-step mitigation plan, and document how you will test that it was successful and execute it.

STEP 12

Install Endpoint Security and Firewalls and Run Scans Regularly

Do you have Endpoint Security installed on all your Endpoints?

All workstations should have endpoint protection installed on them and the definitions should be updated daily. Scans should be scheduled to ensure protection against malware from things like USB drives.

Is a Firewall installed, configured, and enabled on the network's endpoints and servers?

While it is true that the OT Network should be segregated from the Enterprise Business Network, many times engineers rely on the OT firewall for all the protection. This is not an effective strategy when an intruder on your network wants to pivot to another device where they can continue their attack. An endpoint that is limited to communications to/from certain servers and devices over certain protocols and ports greatly limit an attacker's options.

Step 12 (continued)

Many endpoint protection software packages come with antivirus and a firewall. Regardless of whether you are using the Windows firewall or a third party, make sure it is configured to allow only the appropriate protocols through the firewall and only allow them to communicate with the proper servers and workstations. This approach helps prevent an attacker from being able to make lateral movements on the network.

STEP 13

Patch Then Test the OT Network

There is a difference between a patch and an upgrade. By applying security patches, you are keeping the network secure. But there have been Windows updates that have broken the Operating System. That's why applying the latest patches blindly is not a good idea. It is best to check with the vendors and see if the latest Microsoft Windows updates are OK to install.

Many vendors like Rockwell Automation and Siemens have information on which Windows updates have been tested with which products. For instance, an older FactoryTalk View SE installation on Windows 10 will work with the cumulative update from a month ago. The tricky part is scheduling the downtime to install the update since it takes about an hour and requires a reboot. It is also good to test the system after the update has been installed. A test cycle is sometimes sufficient to be sure that everything is working as it should. Just because it boots up into Windows and the user can login doesn't mean that nothing has been affected. As patching has evolved over the past two decades, the ability to rollback an update has become a normal feature. But testing the system remains a crucial part.

Some literature even suggests that you should install the update offline. This is not a bad idea, but it requires some setup and planning to perform. I wouldn't consider this no/low-cost unless you have the infrastructure already set up. In that case, I recommend a copy of the virtual machine (VM), or a virtualized copy of the workstation, located on a segregated area of the network. This ensures that the copy VM can't interact with the rest of the network. The update can then be applied and the VM can be rebooted and tested without any effect on the actual machine or process. How much testing you can do without a connection to the rest of the network depends, but it is one way to test updates offline.

Patching frequency is a hot topic of debate in OT circles. I typically recommend that "Infrastructure Servers" on the OT network, such as the domain controllers, database servers, mail servers, antivirus servers and file servers need to be patched monthly. The automation servers for

Step 13 (continued)

SCADA, data historian, and DCS servers can be patched quarterly. Note: This should be done after contacting the vendors to determine if the update numbers you provided are acceptable to be applied on the version of automation software.

STEP 14

Audit Logs

Do you know how a digital forensic expert determines the attack vector after the fact? One way is to analyze the audit logs of the machines in the attacked environment. Sometimes an entry in the log that had been there for months shows when the attack started.

"In its most recent annual Cost of a Data Breach report, the Ponemon Institute reviewed more than 500 incidents around the world. The results were sobering: the average data breach costs an organization **$4.24 million** and takes **287 days to identify and contain**." (Kizzee, 2021) Can you imagine having an attacker in your network undetected for 287 days (9.4 months)?!

Set up a syslog server to collect all logs from your OT assets. This includes Windows and Linux servers; network routers, switches, and firewalls; virtualization platforms like VMware or Hyper-V; and the workstations. If the automation controllers, operator interfaces, and other automation devices support logging and can transfer the logs to a syslog server, all the better. This collection of logs in one place allows an administrator to view, sort, and analyze these logs to look for patterns that indicate problems on the systems. Alerts can be configured to look for known attack patterns and alert an administrator before the attack can progress. This approach limits any loss the organization may suffer and limits the amount of time an attacker is in your network.

STEP 15

Have a Data Management Plan

Does your company have a plan for how to treat its most sensitive manufacturing data? Do you know where that data is located? Do you know who has access to that data?

If you answered "No" to any of the above questions, this section is for you. If your company doesn't have a policy to control its most sensitive manufacturing data, work with them to create it. Determine a central repository for the data. Note that it doesn't need to be stored together, but the data needs to be stored somewhere that is secured and access is limited only to the people who need it.

Step 15 (continued)

If your organization must store data for a particular retention period, make sure those retention times are enforced by the server on which it is stored. Any data past its retention date must be disposed of using the organization's secure disposal process. If one doesn't exist, create it.

Lastly, make sure any data that is stored on endpoints is encrypted. Windows offers BitLocker, Apple uses FileVault, and Linux employs dm-crypt and LUKS to accomplish this.

WRAP-UP

To the experienced Cybersecurity reader, these steps may seem to just scratch the surface. However, they do fall in the category of "in the direction of goodness," meaning that implementing any of the steps above will only help your overall security posture on your OT Network. Naturally, there is so much more to do! Verista is experienced in OT Network Infrastructure Cybersecurity, including design, build, management, auditing, gap analysis and remediation. Life Sciences companies have very complex and challenging solution environments as they migrate systems from enterprise networks to OT Networks and begin to implement Cybersecurity best practices, all while maintaining operations. We help companies understand the best path to secure their OT Networks, making them redundant, resilient to attack, compliant with regulations, and ensuring data integrity. With our deep understanding of the business processes and technology, we guide companies to the right choices for their specific situation while mitigating their risk.

REFERENCES

Korn, R. (2020). When in doubt, do something [Film]. In Plain View Entertainment.

Kizzee, C. (2021). This October: Commit to Being Cyber-Aware. CIS Newsletter. 16(10).

N.A. (2022). Center for Internet Security. Retrieved from https://www.cisecurity.org/controls/v8

Otieno, J. (2021). How to install and configure OpenVAS on Kali Linux. Retrieved from https://linuxhint.com/install-openvas-kali-linux/.

Greenbone. (N.D.). OpenVAS – Open Vulnerability Assessment Scanner. Retrieved from https://www.openvas.org/.

Millar, A. (2021). Five pharma cybersecurity breaches to know and learn from. Pharmaceutical Technology. Retrieved from https://www.pharmaceutical-technology.com/features/pharma-cyber-attacks/.

Verista is a leading business, technology and compliance company that enables clients to improve health and improve lives.

We help clients solve their most critical and complex challenges across the GxP lifecycle, from preclinical and clinical to commercialization, manufacturing and distribution - bringing together decades of knowledge, the most advanced engagement platforms and transformative technologies. This allows clients to benefit from the ease, efficiency, and trust that results from working with one partner who excels across specialties.

Verista's clients trust the company's 650+ experts to deliver consistent, safe, and high-quality results across the product development lifecycle in the areas of quality and compliance, manufacturing solutions and life sciences consulting.

For more information, visit Verista.com

VERISTA