ASSESSING SECURITY RISK IN INDUSTRIAL/OT ENVIRONMENTS

How to properly assess risk and develop a comprehensive security plan
When we think about compromised computer networks and systems, it’s natural to think in traditional terms: a hacker sitting at a computer keyboard, trying to worm his way into a vulnerable web server or sneak malware onto an unsuspecting user’s machine.

While those types of attacks still occur, security today is far more complex. One of the most vulnerable, yet often overlooked, targets is the industrial environment.

It’s home to operational technology (OT), which includes factory floor robotics, hospital monitoring systems, railway trains, oil pipeline valves, lab analysis equipment and more — just about anything used to produce, maintain, monitor, store or transport products or industrial data. A wide variety of devices and systems are used to control the operations of these assets, and that diversity makes securing OT environments particularly difficult.

When OT environments are compromised, the consequences can be catastrophic. Earlier this year the Norwegian metals and energy company Norsk Hydro was targeted by a ransomware attack, and the attackers successfully shut down production at several plants. (The company’s stock dropped two percent immediately after the attack and aluminum prices shot up in response.)

These attacks can come into the enterprise through any number of vectors ranging from traditional malware injections to Internet of Things (IoT) product vulnerabilities. As such, it’s critical for every industrial enterprise to understand and accept the reality of the risks involved in these networks. In this ebook, we’ll discuss how to properly assess risk, what types of systems are most in need of this analysis, and what other factors should be considered when developing a comprehensive risk assessment of an OT environment.

Security Posture Maturity

OT security is often a wholly foreign discipline to IT professionals, even those who work as traditional security experts. As a result, OT assets — many of which are often legacy equipment that have been operating for decades — are neglected. OT operators are more concerned with uptime and safety versus security or aren’t familiar enough with connected device security.

Remember that an enterprise’s security posture is not binary. There is no such thing as “secure” or “unsecure,” only levels of risk that may or may not be acceptable to the enterprise. Determining and managing these risks are likewise not binary activities. An enterprise just starting down the road to OT security will likely begin with manual, periodic reviews of its operations out of necessity. As this security posture evolves and matures, the enterprise may incorporate automated processes to streamline risk analysis and provide more timely, if not real-time, feedback. New connected devices may also further enhance analysis with predictive analysis tools to proactively and continuously monitor OT environments for potential threats.

What’s important is not just that an enterprise is evaluating OT security risks but that it’s continuously moving along the maturity curve, consistently improving its methodology and tactics to ensure the best possible understanding of its risk levels and the ways it can minimize them.
CONDUCTING A RISK ASSESSMENT

The first step in understanding and improving OT security is to conduct a thorough risk assessment of your environment. Risk assessments can be performed either in-house or with the help of third-party experts. If your organization already has a mature security function, it’s possible to go it alone. Those organizations that are less advanced will probably want to enlist some aid, at least at first. OT security tools can be simple or complex, but choosing the right one for your infrastructure is not a trivial task, and obviously more complex and security-heavy environments are likely to need more advanced tools.

Whether you assess your current risk posture alone or with the help of a consultant, these are the areas which should be included in the assessment.

Security policies, programs and procedures:
This is a logical starting point for any security assessment, as policies and procedures generally set the tone for the overall security profile of the enterprise. These policies and procedures need not be overly complex, but they do need to ensure adequate coverage of all relevant OT environments. OT policies can be integrated with and incorporated into existing IT policies, but specific rules and guidelines around unique OT environments will need to be established. These programs should take care to establish points of contact who are responsible for cybersecurity duties and incorporate key IT policies, including disaster recovery procedures.

Asset management:
The assessment should ensure that all devices and other assets within the OT environment are documented. Asset management should include IT infrastructure, industrial control systems (ICS), ancillary systems and applications (e.g., Active Directory, reporting services, file servers, and so on), as well as any devices deployed in the field and their related assets. Assets may be separated into logical groups based on factors such as their asset type or location. Manual tracking is a common way to start this process, but as a company matures, tools that can dynamically detect changes to the environment and automatically update the asset database are essential. The more centralized the asset management tool is, the more effective it becomes.

Sharing permissions:
In many OT environments, sharing rights are often created without security in mind, with access granted to a wide swath of users who may or may not need access to these systems and ease of use prioritized over legitimate protection of these systems. OT systems often use unencrypted data and plaintext password storage; therefore, it’s critical to provide restricted access to these systems.

Ability to ensure security tools are installed on machines:
Purchasing a suite of OT security tools is one thing. Verifying that those tools are installed on the assets which they are designed to monitor is another. All security assessments need to include an analysis of methodology that is used to ensure security tools such as monitoring systems and endpoint protection services are working and available.

Ability to monitor security devices:
The assessment should ensure that organizations are able to successfully and accurately monitor critical security devices such as firewalls, intrusion detection systems, intrusion prevention systems and OT-specific security devices.

Ability to detect system changes:
Organizations should be able to detect when changes are made to security devices or applications, whether these are planned/intended or malicious. All changes to these systems should be logged and monitored in real time. In mature environments, systems should be in place to approve all such changes before they’re rolled out.

Compliance and auditing:
Compliance is one of the biggest drivers behind cybersecurity initiatives, and it’s often completely lacking in OT environments. Many professionals assume that existing IT compliance and auditing tools as well as their corporate policies will cover their OT compliance needs, but this is rarely the case. OT systems are often viewed as inherently secure and thus in compliance with any relevant regulations, even if these systems have never actually been audited or subject to monitoring.

Review of insecure communications:
Because of their design, many OT environments rely on insecure communications processes and outdated protocols. These communications should be documented, and the assessment should record this documentation. Documentation should be reviewed on a periodic basis to ensure that it matches with the actual environment — and to determine if more secure protocols or communication systems have become available.
Effective monitoring of the OT operational environment is an essential component of OT security. More specifically, real-time insights into the environment are essential in order to properly assess risks. Unfortunately, most industrial organizations lack basic visibility into their OT devices beyond a cursory examination of a few systems on the perimeter of the network. Only in rare cases do they drill meaningfully into the components of the operational environment that matter most. Even in cases where OT security data is being collected, it’s rarely analyzed or utilized for practical purposes.

These are the key components of a security monitoring strategy which should be analyzed and considered during any assessment of OT risks.

**Centralized Visibility**

As with most technology monitoring and reporting tools, a centralized design is key to maximizing the utility of the system. Logs should be aggregated and cross-indexed across all of the operational environments and security zones in the enterprise. The following devices or applications are designed to collect and process log information from the following types of systems/device types:

- **Perimeter:** The perimeter is defined by the entry points into the OT environment, of which there are usually more than one. The perimeter usually consists of security devices such as firewalls or systems that allow for remote access, such as VNPs or jump servers. In some cases, OT devices may be directly accessible without an intermediary, making them part of the perimeter as well.

- **Systems:** Within any OT environment, you will find numerous staples of the IT world, including routers, switches and file servers, as well as related services such as Active Directory (AD), management systems, and so on. These may be internal to the network or reside in the DMZ. The variety of these systems are critical to OT functionality and should be included in a risk assessment.

- **Applications:** Various applications such as SCADA systems, distributed control systems, leak detection tools, and other function-specific OT applications are critical for the safety and availability of industrial systems. They are often unsecure and should be reviewed and monitored. In addition, more traditional IT applications should be monitored as part of this assessment. For example, an antivirus application should be monitored to ensure that clients are running a secure version of the software and are receiving updates and patches in a timely manner.

- **Field devices:** Field devices include programmable logic controllers (PLCs), remote terminal units (RTUs), laptops, tablets/handheld devices, sensors and other physical devices that are deployed in the field. Many of these devices have well-known vulnerabilities and should be assessed, documented and monitored for changes in firmware and configuration. Many of these devices use unsecure protocols to communicate, and should be monitored to detect rogue commands being sent to the devices.

**Dashboarding and Reporting**

How the above information is delivered to the user is also important. Both can be assessed and reported via dashboards and reports that consider at least two tiers of analysis, including:

- **Enterprise level:** A high-level dashboard should cover the entire environment and provide an overview of the risk levels and status of all critical systems and applications. Grouping systems together may also allow for individual asset types to be easily inspected and assessed. For example, all refrigeration or all factories may be part of a single group.

- **Facility/site level:** From here, the dashboards/reports should drill down to offer an assessment of risk at the facility or site level, allowing for more granular analysis. Within each facility/site, these reporting tools may monitor multiple production lines as a collective group.

**Alerting**

Alerting is the flipside of reporting, and it is essential in any security ecosystem. Alerting involves the notification of security personnel when security risks are detected. Alerts may be centralized in a security information and event management (SIEM) system or may be generated by standards applications and services. Either way, these alerts should provide enough information to be actionable by the recipient without requiring further research. On the flipside, excessive alerts or “alert storms” can overwhelm security teams with false positives and/or cause them to miss or ignore genuine problems that require immediate attention.

**Correlation with multiple data sources**

OT environments involve a multitude of different technologies, data sources, formats and protocols. Being able to consolidate and correlate all of this information to create a more holistic picture of the organization’s security risk is key. Correlating multiple data sources leads to better overall visibility of the organization’s security and a fuller understanding of the complexities of the environment.

**Asset monitoring**

All OT systems and equipment should be monitored directly to provide an overall better understanding of their operating environment — both at present and tracked over time. This information includes data about the actual operation of the equipment: revolutions per minute (RPM), temperature, widgets produced per minute, etc. This information is relevant to security, and if these industrial metrics deviate from expected norms, they may indicate that security has been compromised.

**Configuration management**

Finally, the configurations of OT systems and applications should be monitored and tracked over time. The goal is to ensure that any time a system's configuration is changed that it's in accordance and compliance with a risk management policy that directs how such changes should be made and documented.
INVESTIGATION AND FORENSICS

What happens if a security breach is detected? How does the organization respond to this type of event? A quality risk assessment needs to consider how a company undertakes investigations into breaches and the forensic methods it uses to determine the root cause of the breach and how to remedy it. The more effective these investigation processes are, the better the organization’s overall risk management will be.

These are the key components of an investigation and forensic program that should be included in a risk assessment.

Automated searches that identify and provide relevant information about assets, users, and networks:

-能力 to detect remote access by vendors:
-能力 to detect infiltration:
-能力 to detect data exfiltration:
-能力 to detect the installation of applications by users:

While external attacks tend to dominate the headlines, the truth is that while external attacks from beyond the firewall may result. Insiders who have access to OT systems or their documentation may also be conduits to a security breach through blackmail or other types of offline exploitation.

An effective risk management system will manage these types of insider risks by including the following capabilities.

- Ability to detect remote access attempts by support staff:
- Ability to detect infiltration:
- Ability to detect data exfiltration:
- Ability to detect the installation of applications by users:

Not all of these attacks are malicious or even intentional. If an employee misconfigures a device, forgets to set a password or hands out login credentials after falling into a social networking or phishing attack, a large-scale security breach may result. Insiders who have access to OT systems or their documentation may also be conduits to a security breach through blackmail or other types of offline exploitation.

An effective risk management system will manage these types of insider risks by including the following capabilities.

- Ability to detect remote access attempts by support staff:
- Ability to detect infiltration:
- Ability to detect data exfiltration:
- Ability to detect the installation of applications by users:

While it’s a common policy to restrict direct access to OT system interfaces, it’s important to consider all avenues that an attacker might be able to use to control the OT environment.

- Classification of risk by asset, user and the overall environment:
- Risk can be calculated as a single level for the entire organization, but it’s more useful when it is broken down into specifics. Risk factors are more useful when classified by asset, user, or other factors.
- By management. The ability to weigh these risk level scores gives the organization the ability to prioritize tasks designed to reduce risk.

INSIDER THREATS

While external attacks tend to dominate the headlines, the truth is that attacks from inside the firewall are probably more common. In fact, one recent study found that a whopping 70 percent of security breaches were driven by insiders.

Not all of these attacks are malicious or even intentional. If an employee misconfigures a device, forgets to set a password or hands out login credentials after falling into a social networking or phishing attack, a large-scale security breach may result. Insiders who have access to OT systems or their documentation may also be conduits to a security breach through blackmail or other types of offline exploitation.

Not all of these attacks are malicious or even intentional. If an employee misconfigures a device, forgets to set a password or hands out login credentials after falling into a social networking or phishing attack, a large-scale security breach may result. Insiders who have access to OT systems or their documentation may also be conduits to a security breach through blackmail or other types of offline exploitation.

Not all of these attacks are malicious or even intentional. If an employee misconfigures a device, forgets to set a password or hands out login credentials after falling into a social networking or phishing attack, a large-scale security breach may result. Insiders who have access to OT systems or their documentation may also be conduits to a security breach through blackmail or other types of offline exploitation.

Not all of these attacks are malicious or even intentional. If an employee misconfigures a device, forgets to set a password or hands out login credentials after falling into a social networking or phishing attack, a large-scale security breach may result. Insiders who have access to OT systems or their documentation may also be conduits to a security breach through blackmail or other types of offline exploitation.
CONCLUSION

It’s important to note that a proper OT security risk assessment does not merely involve following a checklist on a clipboard. It requires a deep dive into the core systems installed in the organization, the technologies used to manage and secure those systems, and the people tasked with operating and managing their security. The procedures used to operate the systems on a daily basis and the procedures in place to oversee the security and safety of the operations are also critical.

The process of assessing security risk typically consists of in-person interviews, written assessments and hands-on analysis of key technologies. Existing tools and security strategies must be evaluated and assessed, with weak points identified and weighed to establish their overall contribution to the overall risk profile of the OT environment. Naturally, it’s essential that trained and experienced staff are put in position to effectively manage this process.

Remember that OT risk is different than traditional IT risk. OT devices are commonly designed with less thought on security, which means it often falls on your shoulders to secure them after the fact. Patching an unsecure OT device is rarely as simple as clicking a few icons to download an update from the internet, which makes things even more difficult. If an OT device becomes compromised, the damage can quickly become catastrophic, taking your entire business offline for hours or days. Ultimately, determining how to properly assign an acceptable level of risk in such a complex environment is as much an art as it is a science.

INCIDENT RESPONSE

The final piece of the OT security puzzle is found in the response to security incidents. Procedures must be documented in detail and key technologies must be brought to bear in order to preserve information and provide an expedient response and recovery in the event of an attack. A proper incident response strategy should include the following elements, all of which should be considered in a risk assessment.

Well-defined roles and responsibilities:
Incident response begins with a well-defined chain of command and a responsibilities matrix which is used to help teams understand their roles during an active security incident. These tools also help employees understand how to report incidents and how and when to escalate issues.

Written workflows, procedures and documentation:
The steps that need to be followed during an incident response should be documented, including specific workflows or procedures. This information may include who should report an incident, who is involved in triage, and the technological components of the system. This documentation should be maintained in both electronic and written form. Printed documentation is important because a security incident may take key computers or servers offline, and digital documentation may not be available for incident response when it’s needed the most. This documentation should be up to date, and all copies should be kept in sync whenever revisions are made.

Ability to document results:
Incident response programs and policies should provide examples of how to document the results of triage in order to improve future responses. These examples may include specific steps taken, mistakes made during an investigation and any lessons learned.

Tabletop exercises and/or simulation procedures:
Incident response plans should be regularly exercised via tabletop exercises or simulations. These practices run ensure that a plan is effective and efficient, and should be performed on a regular schedule. The results of any tabletop or simulation exercises should be documented as if they were live security incidents in order to allow for continuous improvement.

The final piece of the OT security puzzle is found in the response to security incidents. Procedures must be documented in detail and key technologies must be brought to bear in order to preserve information and provide an expedient response and recovery in the event of an attack. A proper incident response strategy should include the following elements, all of which should be considered in a risk assessment.
ABOUT SPLUNK.

Splunk Inc. makes data accessible, usable and valuable to everyone. Learn how Splunk can help you better assess and bolster your OT security risk.