RISK INTELLIGENCE FOR INDUSTRIAL CONTROL SYSTEMS

Booz Allen’s Security Analysis Framework for Industrial Control Systems (SAF-ICS)
INTRODUCTION
The evolution of the Industrial Internet—the collection of interconnected process and automation systems—presents a critical inflection point in the application of and reliance on operational technology (OT). While industrial leaders have used dedicated industrial control systems (ICS) for decades to automate and control machines, advancements in sensor technology, cloud computing, connectivity, and data analytics are transforming scattered systems into integrated and scalable OT ecosystems. These ecosystems enable machines and humans to collaborate with one another in real time based on operational intelligence, providing unprecedented applications for predictive maintenance, energy and cost efficiency, remote monitoring and analysis, and operational excellence.

However, increasing demands for access to industrial information from business operations, as well as new forms of wired and wireless communications, are exposing ICS to new vulnerabilities and increasing the cyber attack surface at the application, device, and platform levels. The growing interconnectedness across OT systems (driven by business needs) also amplifies the risk of any single threat having a profound impact on business operations. Companies must take a comprehensive and pragmatic OT security (OT-SEC) approach to mitigate potentially catastrophic security threats inherent with the Industrial Internet.

Booz Allen Hamilton’s (Booz Allen’s) Security Analysis Framework for ICS Security (SAF-ICS pronounced Safe ICS) provides a logical security approach to help businesses take advantage of the benefits of the Industrial Internet while mitigating expanding risks. The model provides a lifecycle approach to securing ICS and protecting the processes in the industrial environment, ultimately leading to a more effective and cost-efficient OT risk management strategy.

COMPREHENSIVE ICS AND OT RISK INTELLIGENCE
Booz Allen’s SAF-ICS is a pragmatic OT risk assessment lifecycle we use to prioritize and mitigate risks in the industrial environment. The model is based on realistic industrial risk scenarios; industrial threat modeling and analysis; likelihood assessment; and impact to safety, production, and the environment. SAF-ICS includes four key phases, each supported by a myriad of threat intelligence sources and evidence-based algorithms to provide a more accurate, efficient, and cost-effective risk remediation and mitigation strategy.

“IT'S EXTREMELY DIFFICULT, IF NOT IMPOSSIBLE, TO PROTECT YOUR ENVIRONMENT UNLESS YOU HAVE FULL VISIBILITY OF YOUR ASSETS, DEVICES, AND HOW THEY COULD BE ATTACKED OR COMPROMISED.”
PHASE 1: ASSET IDENTIFICATION AND SYSTEM CHARACTERIZATION

IDENTIFY AND CHARACTERIZE PROCESS-RELATED ASSETS

It’s extremely difficult, if not impossible, to protect your environment unless you have full visibility of your assets, devices, and how they could be attacked or compromised. You can deploy broad, comprehensive security controls in the name of “layered defense,” but in the end this may not be effective or cost efficient. Therefore, it is absolutely imperative that an organization identify all of its assets as thoroughly as possible. Many organizations stop there, but to ensure you are deploying effective and cost-efficient risk mitigation strategies, your organization must understand the potential cost of an incident for each asset and prioritize accordingly. While calculating this cost, organizations should include items such as lost production/revenue, environmental cleanup costs, and equipment replacement costs. Organizations should also include the intangibles, such as incident response time/cost, public relations costs, and legal fees and fines.

PHASE 2: THREAT MODELING

CREATE RISK SCENARIOS

There are different interpretations of penetration tests, vulnerability assessments, and risk assessments. The bottom line is that it is all about properly assessing and managing the risks. Everyone involved must have a clear and mutual understanding of the scope, the process, and the methods that will be used. There are several tasks that require varying skill sets and disciplines, all working in concert with one another.

When assessing risk, your ultimate goal is to start with the most critical assets. The SAF-ICS is fundamentally rooted in OT-specific risk scenarios that are realistic and directly relevant to your systems and environment. Creating these risk scenarios requires a thorough knowledge of your systems, as well as the threats and attack vectors.

What is OT-SEC?

Booz Allen defines OT-SEC as the overall strategy for securing OT, or “hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.” (Gartner)

This includes ICS, supervisory control and data acquisition (SCADA), process control systems, process control domains (PCD), process control networks, distributed control systems, and safety instrumented systems.

The Industrial Internet is the evolution of OT. It connects automation and control technology with complex physical machinery to enable complex data analytics and generate new value.
IDENTIFY ATTACK SURFACES

Identifying your entry points, attack surfaces, and communication paths is critical. Entry points, or attack vectors, can be thought of as the means by which assets receive data or communications. These entry points are ultimately how a hacker will attempt to attack your assets. Hackers look for entry points on all of your attack surfaces, so your organization needs to identify them quickly and assess the largest exposures first. The attack surface is any asset or information that could be exposed in a way that it could be obtained, used, or attacked by a hacker. This could be an Internet-facing system or product, or even exposed sensitive information that could be used to aid an attacker. An Internet-facing system or product would be considered a large attack surface, while an isolated computer would be a small attack surface.

Communication paths are an often over-looked critical point of the assessment. For example, while an Internet-facing enterprise asset might be given a low-criticality rating as compared to an ICS asset, it might have a communication path to a more critical asset in the PCD or the SCADA network. Therefore, a hacker could potentially compromise the lower-rated asset and “pivot” (i.e., use that system as a way to access other internal systems) into your network to access more critical systems. This type of communication path would go against the guidance of just about every industrial security standard and best practice, but it is still a very common scenario and a perfect example of why this step is necessary.

NOTE: This is an area in which a true “penetration tester” or “ethical hacker,” possessing the same skill and mindset as a malicious hacker, could be employed to help significantly. For ICS systems, experience with these industrial systems and the industrial application is an absolute must. We highly recommend that an ICS and/or SCADA engineer be employed for the project.

IDENTIFY AND PRIORITIZE VULNERABILITIES

As your organization conducts the analysis, you should identify as many potential vulnerabilities as you can, starting with your critical assets. This is where many organizations become confused by a misunderstanding in scope—often interchanging the terms “penetration test” and “vulnerability assessment”—and consequently leave critical gaps. Nomenclature aside, what matters is a proper and thorough approach, whether you are assessing a single product or an entire network. These are the three major things to consider: known vulnerabilities, unknown “zero-day” vulnerabilities, and information disclosure (login credentials). While there are varying methods and a multitude of tools to identify known vulnerabilities and information disclosure, most mid- to senior-level cybersecurity professionals are quite capable of performing these tasks.

“The number and types of threat sources that could be targeting your assets are directly proportional to your level of risk exposure.”
NOTE: Industrial systems experience is a must for ICS environments because many assessment tools and techniques can have serious adverse effects on these sensitive systems. Simply reusing an IT methodology that worked for another system just isn’t effective.

Although discovering and managing known vulnerabilities does reduce a significant portion of your risk exposure, zero-day vulnerabilities—the ones you don’t yet know about—can often prove to be the most costly. Such vulnerabilities are used by more advanced malware and hackers, and there are often no patches, intrusion detection signatures (IDS), or antivirus signatures available for exploits that take advantage of these vulnerabilities. Zero-day vulnerability discovery methods are a specialized skill set, which only a relatively small percentage of cybersecurity professionals possess. To ensure this aspect of your risk assessment is covered, your organization will need these specialized individuals, often referred to as “vulnerability researchers” or “penetration testers.” Note that not all penetration testers possess zero-day vulnerability discovery skills. When performing this phase of the risk assessment, it is important to verify that the person assigned this task is experienced with zero-day vulnerability discovery.

UNDERSTAND THREAT SOURCES

Identify the potential threat sources along with their motives, means, and capabilities. The number and types of threat sources that could be targeting your assets are directly proportional to your level of risk exposure. Consider the organization’s potential attackers, as well as how and why they would want to attack—for instance, whether the organization is a large ICS vendor, a target of a “hacktivist” who is trying to deface the website, or a major energy producer with production and safety systems to protect. The attacker’s means and capabilities will also play a large part in the level of effort and financial commitment required to counter these threats. For example, is the organization simply the target of random, lower-skilled “script kiddies” getting into mischief, or
could the organization be the target of an organized crime syndicate or even a nation state with the resources to hire highly skilled hackers and produce advance malware? Answers to each of these questions will provide clues as to where the organization needs to focus its assessment and defensive strategies first.

Knowing what the vulnerabilities are, who might attack you, and how they might attack, is the first step in understanding where the organization needs to begin focusing their efforts. Performing “red team” exercises with qualified penetration testers will give a clearer understanding and expectation of how feasible an attack really is on any given attack surface. With a qualified team and a well-organized, properly executed process, this effort will provide the most significant returns when it comes to developing a risk mitigation strategy that is focused and efficient. As previously noted, penetration testers and red teams must have industrial systems experience when performing tests in an ICS environment, and we highly recommend employing an ICS and/or SCADA engineer on these projects.

PHASE 3: RISK MITIGATION
With the gathered information, the organization should build a mitigation strategy that is focused first on the most likely threats and where they are most likely to strike. Throughout the entire assessment process, the assessment team should be working with the organization’s cybersecurity team, your asset owners, and custodians to discuss results and mitigation strategies. This review should also include estimated mitigation costs. Armed with all of the information needed, you can now make informed business decisions about which mitigations to deploy, where, and when. The focus is on mitigating the risks that have the highest impact first and working down from there in a way that meets your budget.

PHASE 4: VALIDATION
Once mitigations have been deployed, they should be validated with another penetration test or red team exercise. It’s important to remember that risk management is an ongoing process. At a minimum, this entire process should be repeated at least once or twice a year, depending on which standard you are referencing. In reality, you should go through this process as often as your budget can support. Finally, at least some form of risk assessment should be included in your change management policy and executed each time there is a significant change to your assets.
CONCLUSION

Many OT asset owners and operators have fallen victim to inefficient and overly costly risk mitigation strategies, and often neglect certain important components of the assessment process. Using a logical OT-specialized approach, such as the SAF-ICS, OT asset owners and operators can achieve a much more accurate and comprehensive risk assessment that leads to a more effective and cost-efficient risk mitigation strategy.

At Booz Allen, we refer to this overall strategy as OT-SEC. Our OT-SEC experts apply their cybersecurity and industrial systems expertise through our proven models to help our clients identify and mitigate potential risks before they expose critical assets to threat sources.

For More Information

PATRICK NAGEL
Senior Lead Engineer
nagel_p@bah.com

MICHAEL VELLUCCI
Senior Associate
vellucci_michael@bah.com

www.boozallen.com/cyber
About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology for more than 100 years. Today, the firm provides management and technology consulting and engineering services to leading Fortune 500 corporations, governments, and not-for-profits across the globe. Booz Allen partners with public and private sector clients to solve their most difficult challenges through a combination of consulting, analytics, mission operations, technology, systems delivery, cybersecurity, engineering, and innovation expertise.

With international headquarters in McLean, Virginia, the firm employs more than 22,500 people globally, and had revenue of $5.27 billion for the 12 months ended March 31, 2015. To learn more, visit www.boozallen.com. (NYSE: BAH)