CYLUS

Continuous Security Monitoring

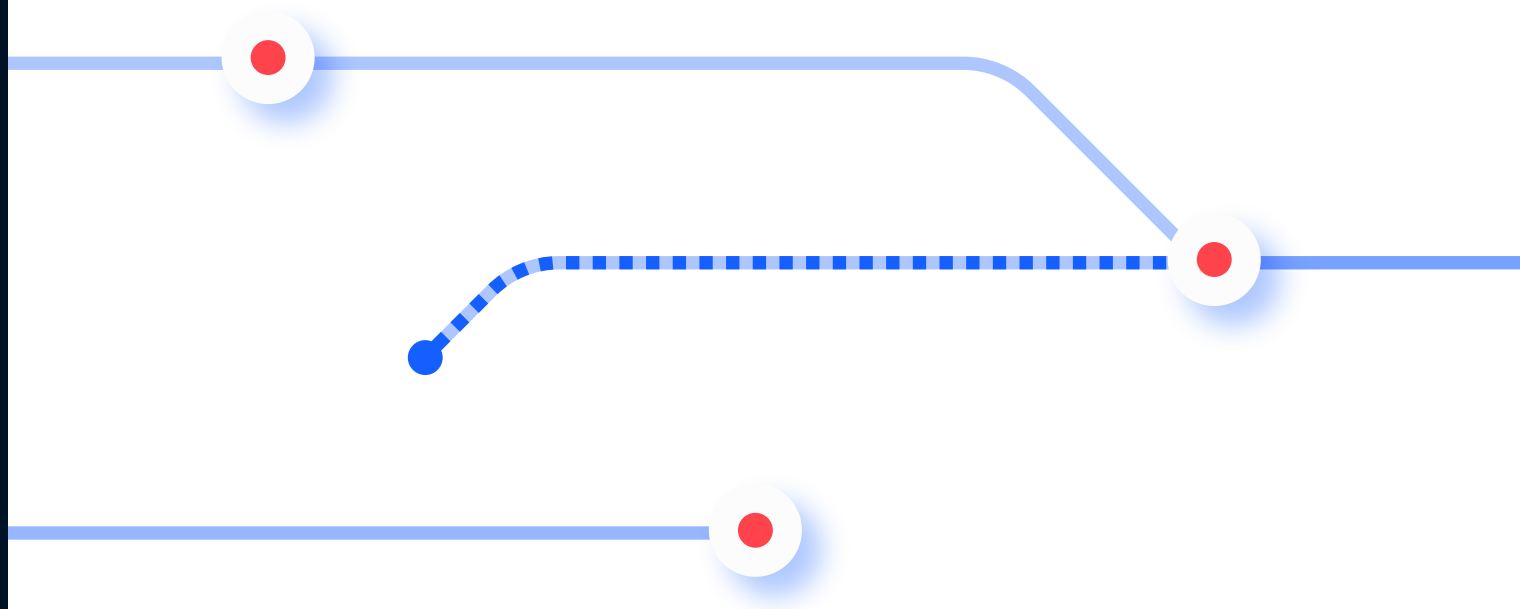
in Rail Technology Environments

Introduction

In its ongoing efforts to improve the United States' cybersecurity and defense of critical infrastructures, the Transportation Security Administration (TSA) issued its third Security Directive, 1580/82-2022-01, in late 2022. The Security Directive outlines the actions rail companies should take to protect the US and its citizens from malicious cyber intrusions affecting the nation's railroads.

Among the measures required by this directive is the implementation of continuous monitoring and detection policies and procedures for detecting and correcting anomalies that affect critical cyber-system operations.

In this paper, we will highlight what continuous security monitoring means in the context of Rail Technology networks and what techniques can be used to achieve it.



What is Continuous Security Monitoring

Monitoring is one of the main pillars of any cybersecurity program or strategy. It is a key point for the IEC62443 framework, ISO/IEC 27001, TS50701, and many other frameworks and standards. Looking at the NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity, the five core functions proposed are Identify, Protect, Detect, Respond, and Recover. Continuous security monitoring is necessary to cover and sufficiently implement the "Detect" function.

However, while "continuous security monitoring" is only three words, it includes an extensive group of security controls and activities.

Protection and prevention activities are fundamental to obtaining a sufficient security posture in any organization.

It consists of the following:

1. Monitoring the network traffic to identify threats
2. Monitoring system and subsystem logs
3. Monitoring the physical environment to detect potential cybersecurity events
4. Monitoring the activity from employees or contractors, traffic or connections from third parties, and more.

Protection and prevention activities are fundamental to obtaining a sufficient security posture in any organization. However, threats evolve, unexpected attack scenarios occur, and security controls might not be as secure as believed. In addition, Rail Technology networks haven't been targeted as extensively as other sectors yet, which means that the available threat intelligence sources may be preliminary or lacking. For these reasons and others, maintaining a solid, Continuous Security Monitoring program is crucial in detecting and enabling an early response against known and unknown threats.

The Challenges of Continuous Security Monitoring

There are many challenges to establishing an efficient Continuous Security Monitoring program in Rail Technology systems. We have separated them into technical and non-technical challenges.

There are many challenges to establishing an efficient Continuous Security Monitoring program in Rail Technology systems

From a technical perspective:

1. **Log Collection Availability:** Rail operational technologies are only occasionally ready to provide reliable and complete cybersecurity logs. They often need support providing helpful cybersecurity logs, making identifying malicious activity in the systems challenging. In addition, it might prove difficult or even impossible to install monitoring agents or other means of endpoint protection mechanisms to audit such activity due to the lack of support by the Rail Technology equipment vendors for such agents.

2. **Safety Homologation:** Another significant limitation is safety homologation or operational constraints on railway environments. Any element that causes a risk to the safety-related

   functions or the reliability of operations shall be disregarded. Any technological approach to security monitoring in Rail Technology networks will be passive. This is a significant limitation to be considered while defining the security strategy.

3. **Geographic Dispersion:** Rail operators must deal with geographically dispersed Rail Technology networks and monitor a diverse ecosystem of technologies. For example, it is common to find multiple wireless technologies on the same installation, such as Wi-Fi, radio frequency, LTE, or other mobile communications. All these factors create an extensive attack surface that needs to be monitored.

4. Limited Threat Intelligence: Because railway cybersecurity is relatively immature, as well as the somewhat limited amount of information available about railway incidents that affect the safety of operations, there is limited threat intelligence available to enhance cybersecurity monitoring. It is always much more challenging than monitoring known threats.

5. Dealing With False Positive Alerts: A challenge when implementing security monitoring is finding the right balance between limiting the number of false positives and the number of false negatives. On the one hand, you don't want your monitoring team overflooded by alerts that do not pose a real risk to the organization, but on the other hand, you don't want to miss a relevant alert because you set the alert threshold too high. Balancing these two factors is always a challenge for any monitoring program.

6. Encrypted Data: Another important point to consider is how to monitor encrypted dataflows. To protect the confidentiality of the data, encryption is the better mechanism to be used. However, if you don't encrypt the data and the communication channel, it creates a side effect that makes it much more complex to monitor. There are multiple technological approaches to circumvent these limitations, but they should be analyzed case by case.

From a non-technical perspective:

1. **Security Budget:** Let's start with money. Typically, rail operators' cybersecurity budget is somewhat limited. Thus, railway operators' CISOs usually juggle budgets to prioritize the initiatives and investments to be pushed yearly. In this context, defining an effective Continuous Security Monitoring program with a limited budget is always a challenge. That's why prioritizing the objectives and the actions to reach these objectives will be critical to the program's success.

2. **Cyber and Rail Operations Expertise:** A particular challenge for the rail organization is the need for more expertise in railway cybersecurity. We know it is challenging to find railway system experts in today's labor market, as cybersecurity professionals are globally scarce. But finding experienced railway cybersecurity experts is almost an impossible mission. This brings additional difficulties to creating a Cybersecurity Monitoring team with relevant profiles.

While there are challenges, it's not all bad news.

While there are challenges, it's not all bad news. Let's look at some advantages of the opportunities specific to Rail Technology systems. For example, operational Tail Technology systems are often static environments with strong change control in place. This can be used to define a clear baseline for the system's activity being able to quickly identify anomalies from the baseline with a very low ratio of false positives, contrary to what happens in regular IT systems where the false positive ratio would be much bigger for this monitoring approach.

In addition, the limited number of rail operators and the uniqueness of most Rail Technology environments will probably dilate the reconnaissance and learning phase on the attack kill chain, giving the operators more chances to detect threats and attacks before they negatively impact the environment.

What to Consider Before You Start

The first step when creating a Continuous Security Monitoring program is to have a solid strategy. In our case, that means setting clear objectives and priorities for the Continuous Security Monitoring program. Being such an intricate topic, this might not be tackled all at once, but clear priorities for the action plan are needed to define the optimal path to move from the "as is" situation toward the desired status.

Clear priorities for the action plan are needed to define the optimal path to move from the "as is" situation toward the desired status.

To set these priorities, one important aspect to consider before starting is a clear picture of the current situation. Some useful questions that might help to establish it are:

1. **Do I already have good visibility on my networks and technological assets?**

   As already known, you can't protect what you can't see. Having good visibility will be vital to establishing an optimal monitoring strategy.

2. **What is considered my Crown Jewels? Where should I put my monitoring focus?**

   Prioritization is crucial in identifying the most critical assets to protect. Or, in other words, which are the assets that the attackers will ultimately try to compromise?

3. **What are the primary cybersecurity risks in my organization, and what is my attack surface?**

   Knowing the attack surface and the existing vulnerabilities will allow the establishment of specific monitoring use cases to cover those or at least ensure that these are reasonably covered with the security monitoring strategy.

5. **What am I already monitoring? Are any security monitoring processes in place to be used as a foundation?**

   There is already some monitoring in place for the IT or the corporate environments and security monitoring processes for physical security. Consider repurposing or improving these when you increase coverage.

6. **Do I want to have my Security Monitoring team in-house or externalized?**

   Are you planning to implement a Security Monitoring program internally or externally? A hybrid approach may be more suitable for some organizations, having a first tier performed by an external company but escalation and response internally driven. The idea can evolve and change, but it is best to start thinking about these early on.

7. **What skills and expertise does my Security Monitoring team require?**

   You may need to create or expand your team. Examine what skills are required and what you have available. As mentioned, finding relevant profiles is not trivial, so a mix between hiring and training will be required in many cases.

Methods to Address Continuous Security Monitoring

Continuous security monitoring of Rail Technology networks can be addressed from different angles and perspectives. We will begin by looking at the specific requirements outlined in the TSA Security Directive, but later we will also look at other angles.

Continuous security monitoring of Rail Technology networks can be addressed from different angles and perspectives.

1. **Capabilities to Defend Against Malicious Email**

   The Directive requires the rail owner or operator to defend against malicious email to preclude or mitigate adverse impacts to operations. That includes, for example, implementing solutions to analyze incoming emails to identify malicious links, implementing secure browsing solutions to prevent users and devices from accessing malicious web domains or applications, blocking and preventing unauthorized code from executing on the endpoint, and others. These solutions are already mature since they are typically deployed on IT networks and don't need to be rail specific.

2. **Audit Unauthorized Access to Internet Domains and Addresses**

   The Security Directive also requires the rail owners and operators to audit any unauthorized access to internet domains and addresses, document and audit any communication between the OT system and any external systems that deviate from the identified baseline of communication, and identify any execution of unauthorized code. That means that monitoring solutions shall be implemented to cover these communications between the Rail Technology environment and the IT world with capabilities to establish a baseline and identify and report deviations or anomalies from such baseline.

   Different technological solutions might be used to achieve this requirement depending on the quantity and the nature of the data flows between these two environments. For example, in most cases, an IDS solution with anomaly detection capabilities and firewall technology to control the data flows should cover this requirement.

3. **Continuous Collection and Analysis of Data**

   According to the Security Directive, data must be continuously collected and analyzed for potential intrusions and anomalous behavior in Critical Cyber Systems and other operational and information technology systems directly connected to Critical Cyber Systems. The data shall be kept for sufficient periods to effectively investigate cybersecurity incidents, usually at least three months and, optimally, a year.

   This requirement can be achieved by implementing a SIEM solution to aggregate, enrich, consolidate, normalize, and correlate all the cybersecurity logs available. In addition, it requires continuous collection and analysis of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other rail technology systems that directly connect with Critical Cyber Systems. This coverage should consider IT and Rail Technology network monitoring, including non-IP networks, when present and relevant for the operations, as well as endpoint monitoring and the monitoring of the cybersecurity logs generated by the systems.

However, the success of any SIEM solution is always limited by the quantity and quality of its data sources. That means an exhaustive analysis of the available data sources (e.g., the cybersecurity logs already produced by the existing systems and network devices) should be performed to identify the blind spots where additional monitoring technologies will be needed to increase the monitoring coverage. For example, if the available logs provide good visibility on the endpoints, but we lack network visibility, we might need to consider adding network monitoring capabilities to our program or the other way around.

4. **Implement SOAR Capabilities**

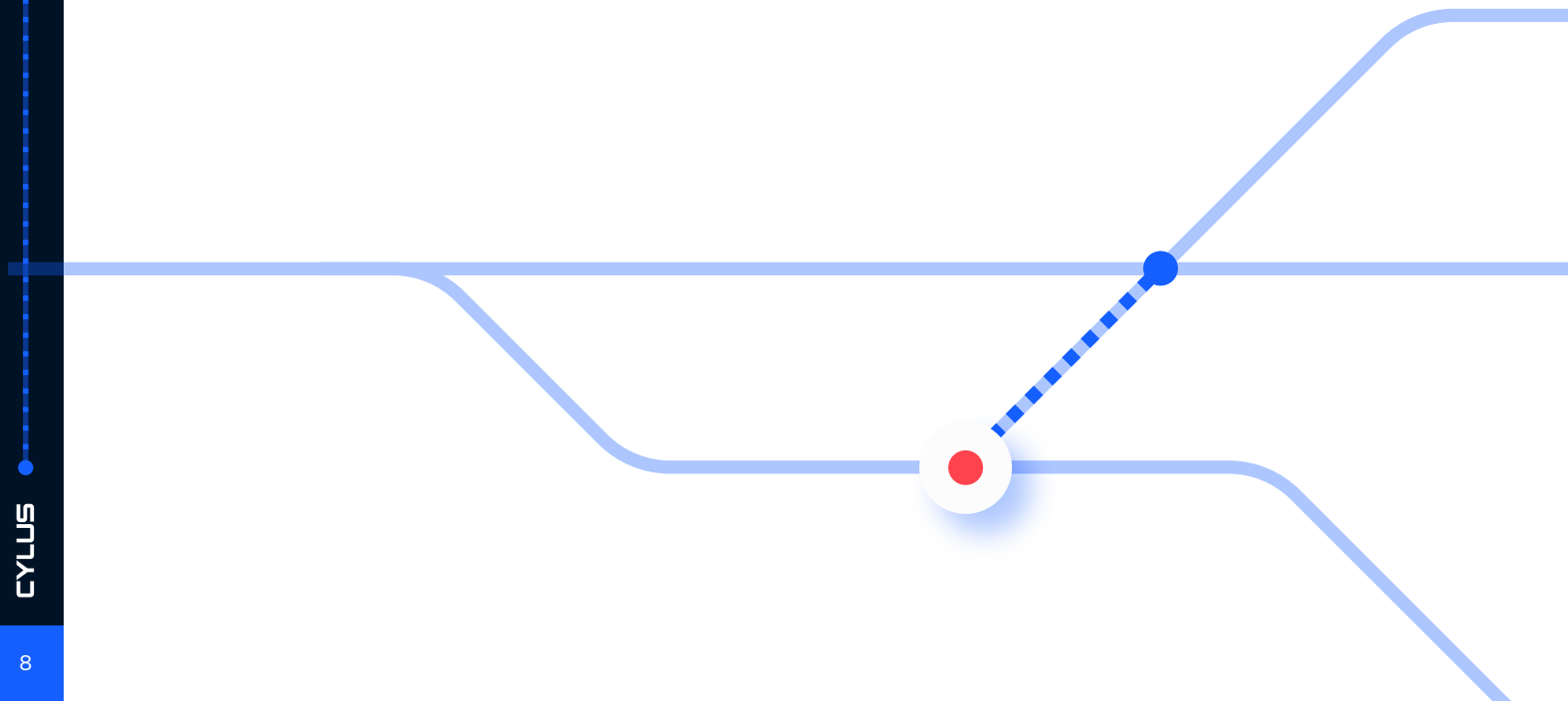
   The Security Directive also mentions implementing security orchestration, automation, and response (SOAR) capabilities to define, prioritize and drive standardized incident response activities. SOAR technologies typically enhance SIEM capabilities using artificial intelligence (AI) and machine learning to get and adapt insights to make recommendations and automate future responses. For this reason, response playbooks are an essential part of SOAR technology, allowing the automation of response activities to speed up the reaction against ongoing threats.

5. **Implement Mitigation Measures or Manual Controls**

   Finally, rail owners and operators should implement mitigation measures or manual controls to ensure that the OT systems can be isolated when cybersecurity in the IT environment creates a risk to the safety and reliability of the OT system. Although this topic is more part of the response function than the actual security monitoring, the Security Directive includes it in this section.

   This will typically involve a mix of technology means, such as firewalls or other network devices able to perform the isolation, together with human actions or validations. This is the perfect example where a customized response playbook on the SOAR solution can help to speed up the process once the monitoring solutions have identified the threat and can help coordinate or bring the response actions of security teams and rail operations teams into alignment.

The limited number of rail operators and the uniqueness of most Rail Technology environments will probably dilate the reconnaissance and learning phase on the attack kill chain,



Other Methods to Address Continuous Security Monitoring

We can analyze the topic above and beyond the Security Directive requirements by, for example, considering how the organization's monitoring processes will be implemented. There is no doubt that the mentioned SIEM and SOAR technologies will help by centralizing and automating tasks, but still, we need to plan where the manual analysis and activities will be performed and by whom. Rail operations typically perform this on a dedicated Cyber Security Operations Center (CSOC) embedded within the Operational Control Center (OCC). In that sense, key success factors will be the CSOC and the OCC interfaces to retrieve context information to direct the response activities.

We can analyze the topic above and beyond the Security Directive requirements by, for example, considering how the organization's monitoring processes will be implemented.

1. **Determine What Level of Monitoring is Required**

   When looking specifically at network monitoring capabilities, it is essential to determine which level of monitoring is required. For example, a solution monitoring the communication headers might be enough to identify the most common network-based attacks. However, more advanced threats could require technologies to understand the application layer (e.g., deep packet inspection capabilities). For example, almost any IDS technology can identify a typical ARP spoofing attack. At the same time, an unexpected signaling message of section clear is sent. In contrast, the section is occupied requires the technology to understand the specific signaling protocol the operator uses.

2. **Consider Who is Monitoring**

   We should also consider monitoring the activity performed by personnel and third parties, and contractors since it is common for attackers to use credentials from authorized users to perform their malicious activity or to convince, coerce or trick authorized users into performing these. We saw an example of this in the attacks against the Ukrainian electric grids in 2015 when the attackers stole VPN credentials from maintenance engineers and used them to enter the rail technology environment to carry on with the malicious activities.

   Special focus should also be put on monitoring the activity related to third-party connections, such as vendor connections for maintenance purposes and third-party connections to deliver services. Finally, any remote access connection should be carefully monitored to identify abnormal or malicious activity.

3. **Threat Intelligence**

   Another important point to consider is which threat intelligence sources can be used to enrich and enhance continuous security monitoring. These can be internal sources to give the internal context to the security alerts, for example, the identification of the exact properties such as vendor, version, criticality, or geolocation of the affected assets, or external sources, such as information about the known threat actors that might target our infrastructure or the known techniques and tactics used on attacks to similar infrastructures. Establishing a mechanism to share this intelligence between owners and operators within the country and with operators from ally countries will also benefit the whole ecosystem.

4. **Long-Term Strategy**

   The organization should also consider its long-term strategy to enhance continuous monitoring by adding additional detection capabilities, such as deception technologies, to detect an ongoing threat as early as possible during the attack kill chain. These technologies can deceive attackers allowing the defenders to gain reaction time to stop these ongoing threats.

5. **Implement Threat-Hunting Activities**

   Another key aspect will be to accomplish reactive monitoring and implement threat-hunting activities once the Security Monitoring program is mature enough, allowing it to uplift significantly any organization's security posture. Although today threat hunting activities are mainly done through the expertise of human cybersecurity analysts, the improvements in SOAR technologies will bring massive enhancements in this field.

6. **Periodically Test Monitoring Capabilities**

   Finally, it will be necessary to periodically test the monitoring capabilities to assess that their coverage is enough and that the defined processes and technologies work as expected. In this sense, automated testing use cases, complemented by manual tests (e.g., red team exercises), will increase the overall maturity of the monitoring processes. It also allows the defenders to keep up with training and be better prepared when real threats arise.

How This Method Addresses Current Regulatory Requirements

The method proposed in this post will more than address the current Security Directive. It will also enable operators to be better prepared to cover future requirements that might arise while enhancing their organization’s security posture and threat detection capabilities. Perhaps most importantly, it will reduce the risk of suffering an incident that might have severe consequences for the operations or the safety of the passengers and employees.sets.

The method proposed in this post will more than address the current Security Directive.