CYLUS

WHITE PAPER

An Introduction to Rail Security Operations Center (SOC)

Introduction

A Security Operations Center, or SOC, is an essential organizational component. It contains individuals, procedures, and technologies that monitor and effectively respond to cybersecurity threats. In addition to threat monitoring, some SOCs may assume other cybersecurity responsibilities, including incident response, forensic investigations, management of organizational security solutions and technologies, ownership of vulnerability management processes, and more.

A Railway SOC is the railway industry's dedicated SOC, featuring a specialized team, processes, and technologies to monitor and respond to cybersecurity threats specific to operational rail technologies.

Various approaches may be considered when establishing a SOC for railway infrastructure. These include running the SOC internally, outsourcing its operations, or adopting a hybrid approach. Another approach is creating a specialized SOC dedicated solely to rail technologies or expanding an existing SOC that initially focused on monitoring other corporate systems.

This paper will explore the different considerations, challenges, and specifications of building a rail SOC. These include:

- The threat monitoring process and the importance of rail data sources
- Defining the proper organization and skills for a Rail SOC
- The challenges of performing alert triage in a Rail SOC
- Responding to an incident involving rail technology

Building a Dedicated Rail SOC vs. Integrating into the Corporate SOC

When planning your rail SOC, consider whether your organization wants to develop a dedicated SOC designed explicitly for the rail environment, focusing on monitoring the operational rail technology systems, or views extending the existing corporate SOC as the preferred option. The corporate SOC typically monitors and manages cybersecurity for various IT systems, such as corporate websites, servers, workstations, etc. Focusing on those technologies requires the right expertise, knowledge, and know-how relevant to OT and Rail systems.

When integrating a railway SOC, it is crucial to assess various factors to guarantee its effectiveness and adaptation to the distinctive challenges of the rail industry. While each scenario requires individual evaluation, the prevailing approach leans toward enhancing the existing SOC for several reasons:

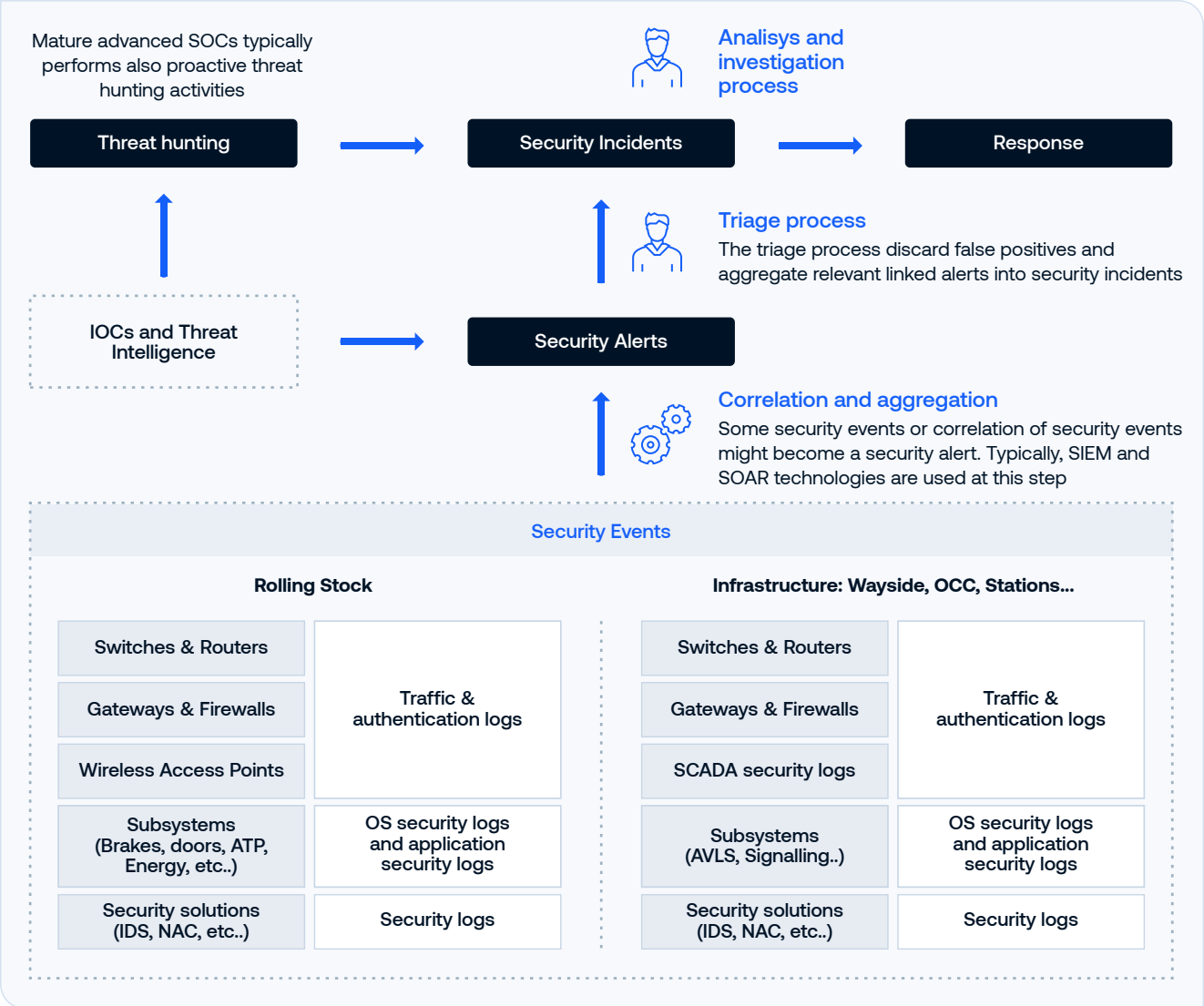
1. An existing SOC already possesses skilled analysts and processes that can be leveraged to a certain extent. In most cases, those analysts will be experienced in IT environments.
2. Utilizing the existing triage, investigation, and management tools, such as SIEM, SOAR, ticketing systems, etc., allows for efficient and streamlined operations. However, it is important to validate that those tools suit the specific needs of OT and Rail systems.
3. Consolidating under the existing SOC helps eliminate the overhead of maintaining separate management tiers for multiple SOCs.
4. The integration will inherently enforce the creation of a multidisciplinary team, proving exceptionally valuable when addressing intricate incidents that impact various systems and environments.

The Threat Monitoring Process in a Rail SOC

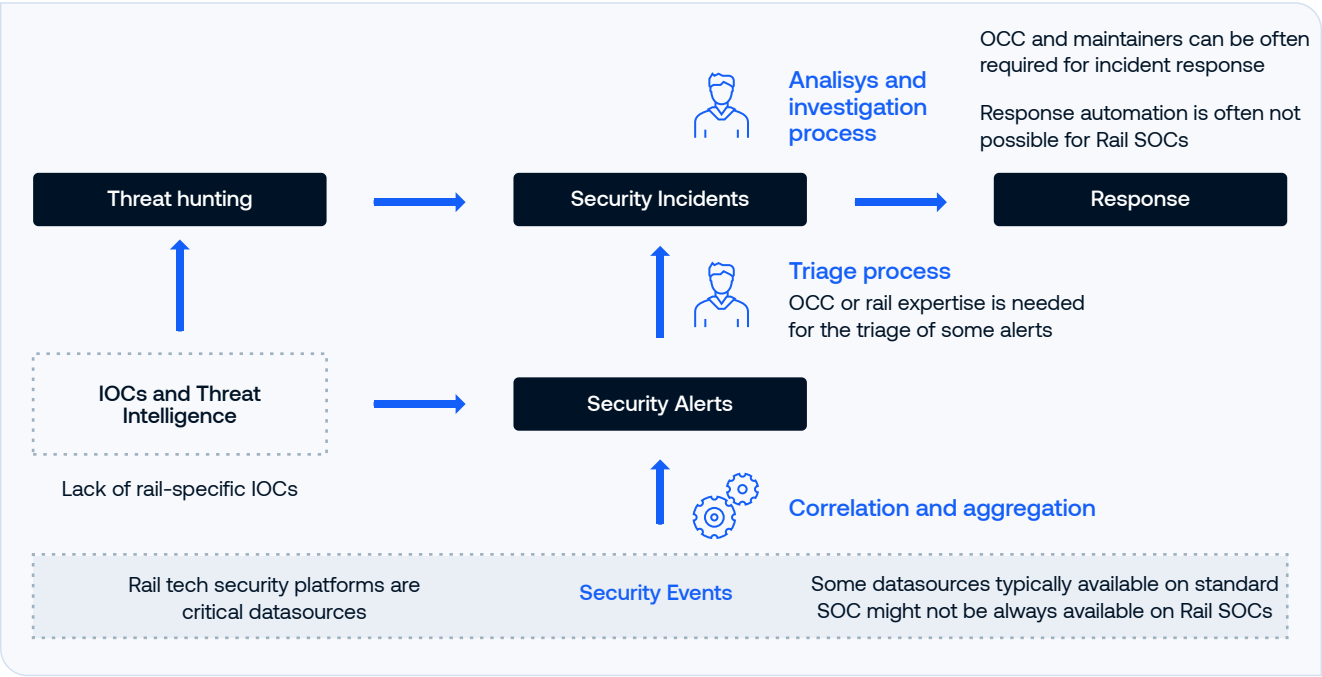
An operator's CISO faces several challenges, including defining the optimal strategy for monitoring cybersecurity in their operational rail environments, including OT technologies, proprietary protocols, and even non-ethernet buses.

In the threat monitoring process, the organization identifies ongoing threats in the attack chain as early as possible to respond accordingly.

The following figure shows a theoretical threat monitoring process for a rail SOC:



However, this process faces specific challenges and requires considering aspects that differ from a regular SOC. The following diagram highlights the main points that need to be considered explicitly for the threat monitoring process on Rail SOCs:



The quality and coverage of data sources are key factors in proper threat monitoring. However, for a Rail SOC, many of these data sources might only be partially or unavailable. This is especially true for brownfield projects, where we need to deal with plenty of legacy systems that were designed without any cybersecurity focus.

For this reason, it is essential to count on a **rail-specific cybersecurity platform** as a critical data source to identify security events occurring at the rail-specific protocol levels. For example, if an attacker is abusing weaknesses of protocols such as Train Real-Time Data Protocol (TRDP) or custom Communications-based train control (CBTC) protocols, having a solution that can inspect and understand rail protocols is critical to achieving a successful monitoring strategy for rail tech environments.

The following screenshot from CylusOne® highlights how a dedicated solution can facilitate communication between SOC and OCC teams. SOC operators identify assets on the network using their tools and terminology, often by network names or IP addresses. In contrast, OCC teams refer to equipment based on its function within rail operations, not by network identifiers. CylusOne® bridges this gap by providing specific information to SOC operators about assets, allowing them to communicate effectively with OCC operators. For example, they can specify that "it is part of the interlocking system," "this is the identifier of a specific device in the interlocking system," "this device is located at station X," or "this asset is critical for operations." This shared understanding ensures both teams speak the same language, enhancing situational awareness and coordination.

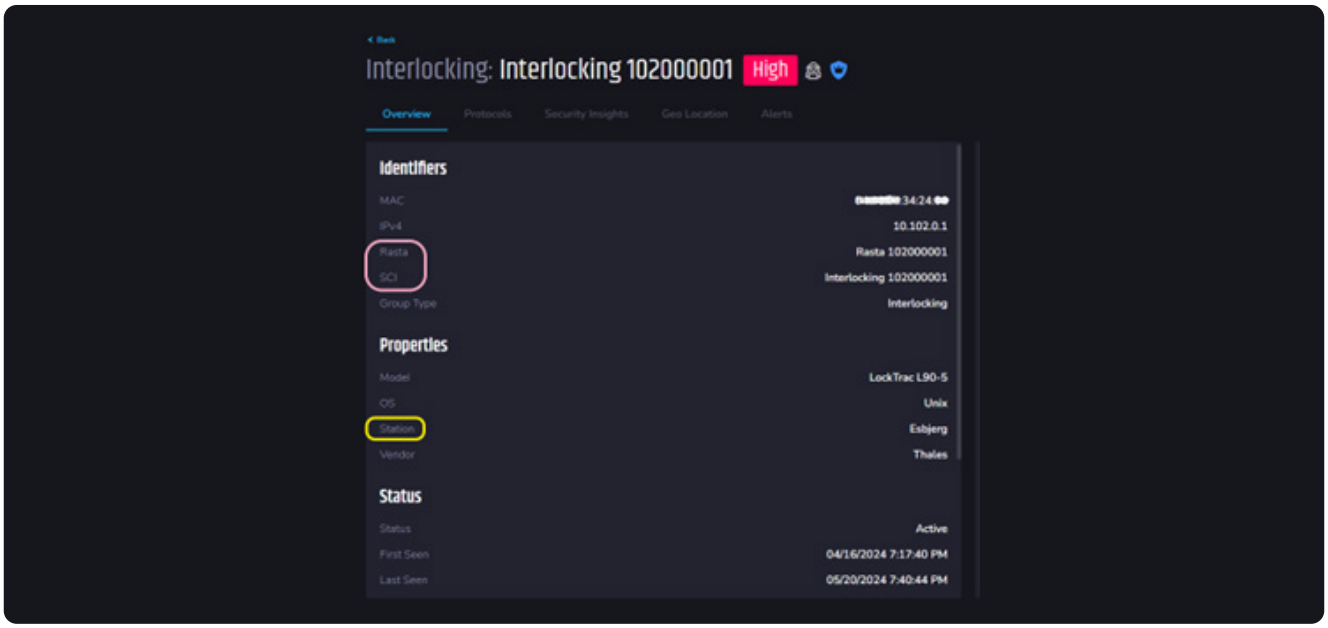


Figure 1 - Example of a sample of the attributes that CylusOne provides for assets in the network

On the other hand, some security logs typically available in non-rail technology systems, such as those provided by anti-malware agents, Endpoint Detection and Response (EDR) solutions, host-IDS solutions, etc., might not be available on rail tech systems due to operational constraints that prevent the usage of such solutions. These limitations make it even more critical to count on reliable rail cybersecurity platforms to cover the gap left by the absence of the events that such missing solutions would generate.

The Triage Process on a Rail SOC

Alert triaging is a key activity for any SOC. A first layer of security analysts discards false positives and escalates the alerts that need further investigation. Artificial Intelligence technologies have enabled modern SOCs to highly automate the triage process, reducing the alerts that need to be manually triaged by analysts. Counting on reliable threat intelligence sources and having good IOCs (Indicators of Compromise) also enables SOCs to optimize the triage process.

When an L1 analyst is unsure about a given alert, (s)he usually escalates it to the L2. However, on a Rail SOC, there will be cases where the skills needed to triage an alert differ from those of a more senior security analyst to those of someone with rail tech-specific knowledge. For instance, it can be demanding for a cybersecurity analyst lacking rail-specific expertise to differentiate whether an alert regarding an unusual "section clear" message detected on the signaling network is accurate or a false positive. Similar situations arise with alerts related to the train control and monitoring system (TCMS) traffic or other onboard networks.

In that sense, the Rail SOC might adopt different strategies to address this gap, for example:

1. Suppose the rate of false positives is low enough. In that case, the Rail SOC can decide to automatically escalate alerts related to rail technologies to be further investigated by analysts with the proper skills and rail knowledge.
2. Having rail specialists on the team can improve triage and the development of an interface with the OCC. A multidisciplinary team, including both rail specialists and cybersecurity experts, can effectively manage alert triage.

Proper selection and fine-tuning of the rail cybersecurity platform are essential for any Rail SOC. This will minimize the number of false positives while maintaining an adequate detection rate.

Threat-Hunting on a Rail SOC

The threat-hunting activity consists of leveraging threat intelligence to prioritize and search proactively for indicators of attack or indicators of compromise across the monitored systems. This is a practice commonly performed on corporate SOCs, but can face some challenges when being implemented on a Rail SOC:

- The current number of feeds with threat intelligence relevant to rail technology is minimal.
- A deep understanding of rail technologies is necessary to conduct effective threat hunting. It's not enough to look for generic network indicators; one must also identify threats at the rail application and rail protocol levels.
- Threat-hunting activities are often performed using EDR technologies, which are typically unavailable in rail tech environments.

To implement optimal threat-hunting capabilities, the following would be necessary:

1. Identify and implement reliable rail-related threat intelligence sources able to provide IOCs relevant to the rail tech environment.
2. Use anomaly-based detection technologies in the rail environment, as anomalies can cover the gap of unreliable IOCs in these environments.
3. Rely on rail cybersecurity analysts who can understand rail tech and look for relevant indicators within the monitored environment.

The Investigation and Response Processes on a Rail SOC

Once an alert has been triaged, confirmed, and escalated as an incident, the next step is for senior analysts to investigate and respond to it. When discussing operational rail technologies, we encounter incidents that span various expertise domains, including corporate IT equipment and the technologies employed by different rail systems. This can make the investigation of rail tech incidents especially challenging.

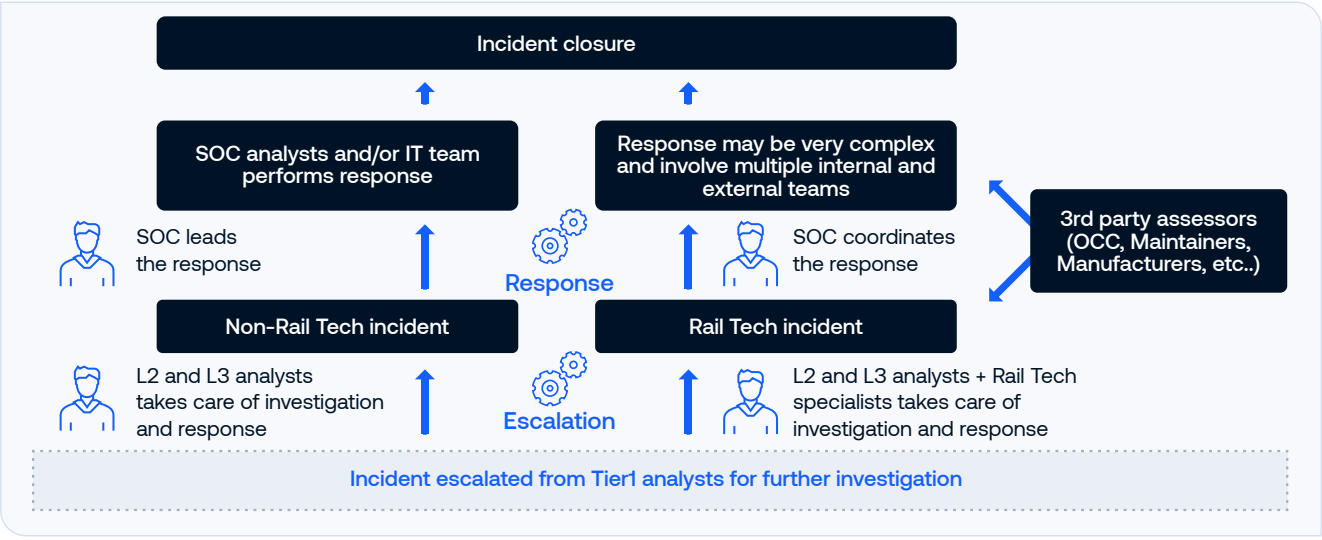
To illustrate this with an example, imagine an incident where an attacker compromises a maintainer's workstation with VPN access to the OCC network. Once inside the OCC network, the attacker pivots through the network, gaining various levels of access to the ticketing system, the wayside signaling system, and even the train-to-ground communication based on 4G connectivity within the rolling stock. In such a scenario, the defender team will need a certain level of knowledge and expertise in:

- IT cybersecurity.
- Network cybersecurity, including wireless technologies.
- Specific operational rail technology such as signaling systems, ticketing systems, and more.

For this reason, correctly defining a Rail SOC's investigation and response processes is a challenging task. The following points are essential to implement an efficient investigation and response process for rail tech cybersecurity incidents:

- Ensure the security analysts team on the Rail SOC has the rail balance on cybersecurity and rail tech expertise. As discussed, this can be achieved by having the right mix of profiles within the team.
- Have clear, predefined internal communication channels with the relevant teams, such as the OCC, maintenance, and operations teams. These channels can provide information and context for the investigation or be needed to actively participate in incident containment and resolution.
- Clearly define which external organizations' sources can be helpful and supportive of the investigation and the channels and processes to contact them when needed: Relevant government CERTs or CSIRTs, cybersecurity service providers, rail integrators, rail manufacturers, other rail operators, etc.
- Continuous improvement, practice, and training. When serious and relevant incidents are relatively low, it is essential to keep the team well-trained to be ready when incidents come. You don't want your Rail SOC analysts trying to figure out the processes in the middle of an actual incident. In that sense, regular tabletop and hands-on exercises will be invaluable when an urgent and stressful actual incident materializes. However, when we reach a situation where the volume of incidents is high enough to consider that the simulations and tabletop exercises are not required anymore, it is still key to ensure there is a solid continuous improvement process where retrospectives and lessons learned on incident handling can help to fine-tune and improve the existing processes.

The following diagram describes a high-level process that is typically in place for the investigation and response to incidents on a Rail SOC:



Notice that the main difference is that the SOC team investigating and responding shall be multidisciplinary for operational rail tech incidents, including cybersecurity AND rail tech expertise. Also, typically, it will require much more advice from and coordination with external agents such as the OCC, the maintainers, the manufacturer or integrator of the rail technology, etc. That means that, meanwhile, on a regular cybersecurity incident, the SOC team leads the resolution of the incidents, on a rail tech incident, the role of the response team will be more focused on coordination and alignment of the response.

A rail-specific cybersecurity solution must provide tools to manage investigation and response processes while considering the critical function of the OCC. As shown in the following screenshot, CylusOne® enables SOC operators to investigate cyber events and coordinate efforts with OCC teams. In the alert view, operators find essential details to investigate a cyber alert, such as an alert overview, the list of involved assets, and the detection time. Additionally, CylusOne® offers:

- Identification of alerts using MITRE ATT&CK TTPs, aiding cybersecurity personnel in assessing the situation and collaborating with external teams (purple frame).
- The ability to download a PCAP with specific traffic that triggered the alert for further forensic analysis (yellow frame).
- A dedicated "playbook" for each alert, containing recommendations for event management and containment. These playbooks, written by Cylus, include relevant communication with the OCC and are fully customizable by the SOC manager. This feature allows the SOC and OCC managers to add their own recommendations, reflecting their unique operational culture (blue frame).
- Additional cyber insights to assist operators in the investigation, such as identifying other related events that the system has analyzed and connected, suggesting they are part of the same attack chain (green frame).

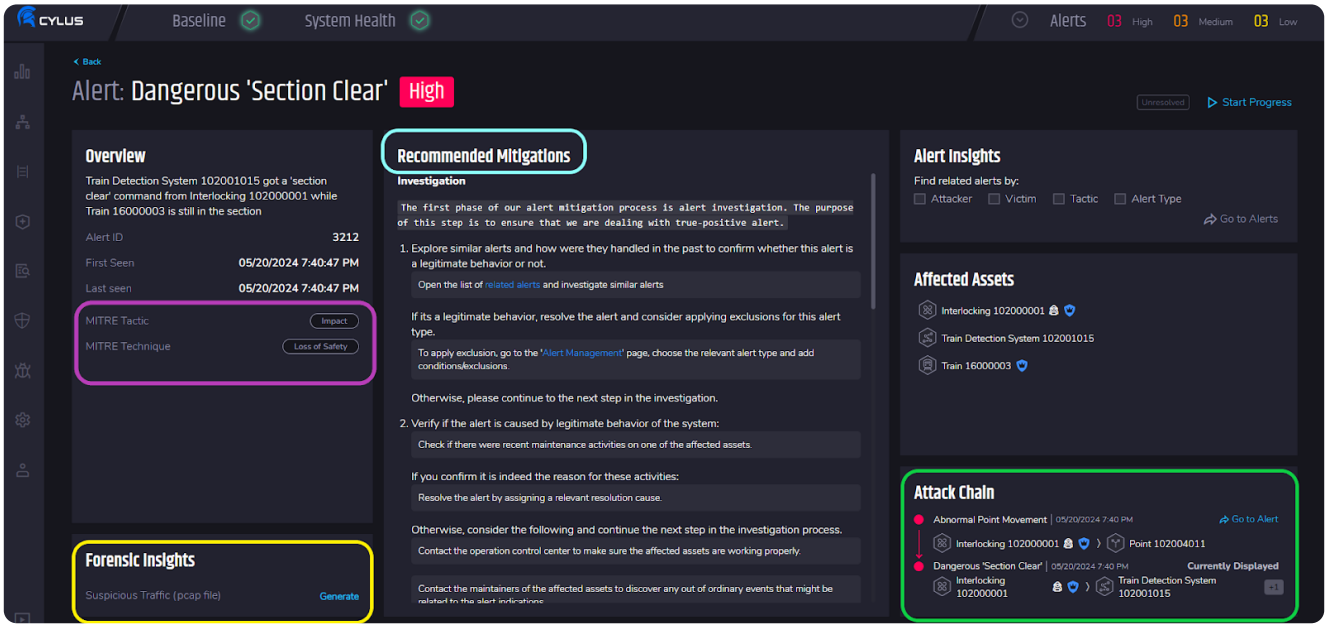


Figure 2 - CylusOne alert view

The Rail SOC Organization

A typical corporate SOC has two or three layers of security analysts with different levels of seniority, allowing security incidents to be adequately escalated depending on their complexity. It also has a management layer to coordinate and drive the teams. Depending on the functions allocated to the SOC, it can also have dedicated teams for security device management, vulnerability management, threat intelligence, malware analysis, and more.

This structure can be effectively replicated in a Rail SOC with the unique requirement that each analyst level possesses specific rail technology skills. While it's unrealistic to have an expert for every rail system, it is essential to have team members capable of gaining a high-level understanding of incidents and efficiently communicating with operational teams. These teams can then support the investigation and resolution of such incidents.

Some of the knowledge areas that are key to support the Rail SOC functions are:

1. High-level understanding of the existing rail systems and subsystems and how they relate and communicate with each other.
2. Understanding of the primary communication flows across the system, as well as some basic knowledge about the protocols in use
3. Understanding the networks, buses, and subsystems on the rolling stock.
4. Understanding of the signaling system and the communications flows from and to the OCC and from and to the rolling stock
5. Understanding the SCADA systems used to monitor and control the power supply and the station's facilities.

When dealing with an incident, especially if lateral movement is involved, counting on this sector-specific knowledge can help discern between false positives and actual attacks and understand the attacker's targets. In the same way, getting people in the team with a low-level technical understanding of the rail specifics protocols used by the system (e.g., Modbus, TRDP, etc..) can prove invaluable to be able to analyze the PCAPs of suspicious traffic and be able to understand what is going on.

A rail-specific cybersecurity solution aids SOC operators by providing **rail-specific context and intelligence**, allowing them to focus on incidents more effectively. The following screenshots illustrate how CylusOne®'s dedicated user interface enables quick comprehension of a cyber alert's relevance. It shows the device's location, type, and the criticality of the impact. Moreover, it facilitates smooth communication with OCC operators, ensuring both teams speak the same language.

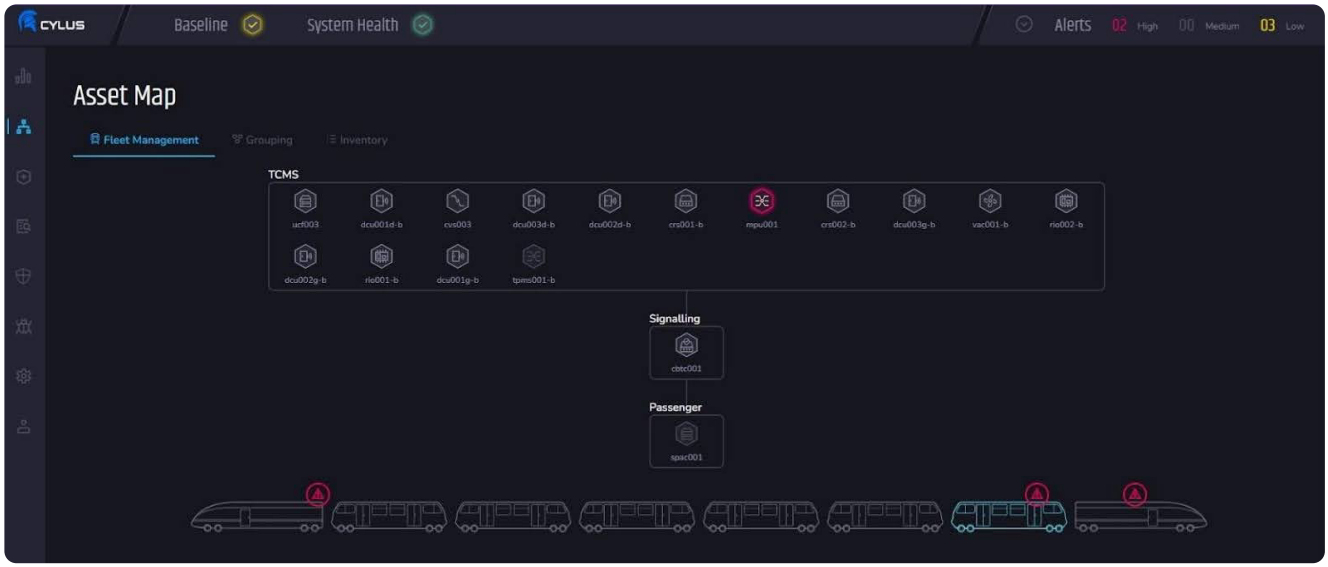


Figure 3 - CylusOne Rolling Stock asset map

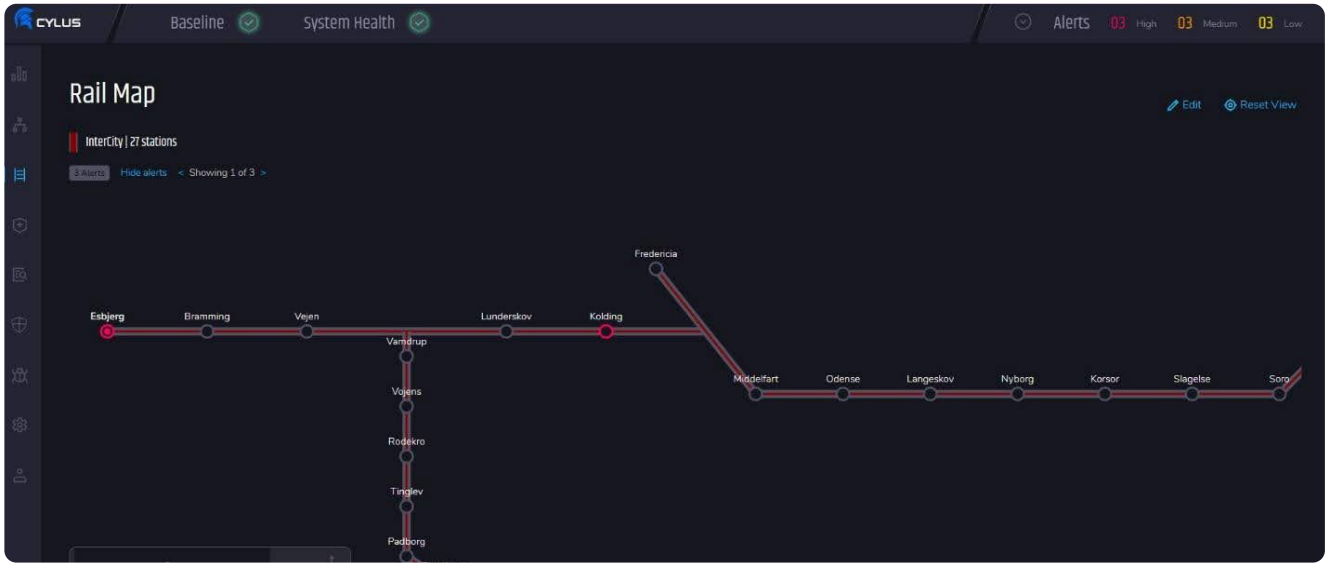
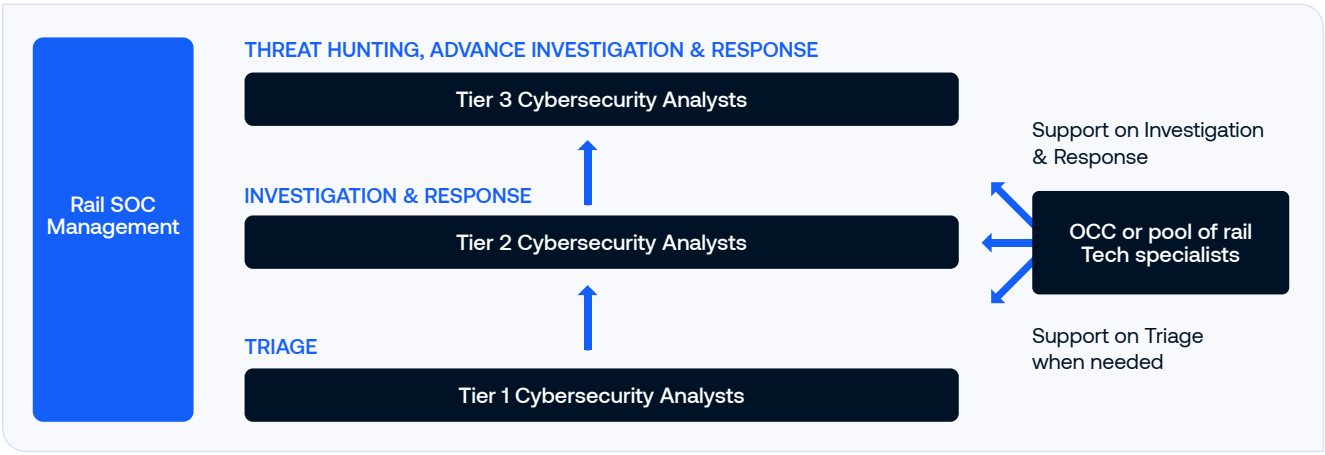


Figure 4 - The CylusOne Rail Map view provides a logical understanding of the assets and the locations of alerts.

Finding profiles in the market with knowledge of rail tech cybersecurity might be impossible, so a reasonable approach is training professionals with expertise in cybersecurity to get a basic rail understanding of rail tech cybersecurity. Combining these two profiles has proven to be a very effective strategy to cover the skills and expertise the rail SOC team needs.

The following diagram proposes a possible structure for a Rail SOC team:



Tier 1 Cybersecurity Analysts: The first tier of cybersecurity analysts, typically the less experienced ones, perform the triage process to discard false positives and escalate potential incidents to further analysts' tiers.

Tier 2 and Tier 3 Cybersecurity Analysts: The second and third tiers of cybersecurity analysts are in charge of incident investigation and response. Tier 3 analysts, the more senior analysts, typically drive the threat-hunting activities and handle the most complex or impactful incidents.

Rail Tech Specialists: Typically, a small team is compared with the cybersecurity analysts who have a deep knowledge of rail tech and some cybersecurity fundamentals, which supports the different tiers of cybersecurity analysts in developing their tasks when rail tech knowledge is required. They also typically interface with other rail tech departments during the investigation and response of incidents (e.g., engineering, maintenance, OCC, rail tech manufacturers, etc..).

For some organizations, these rail tech specialists might directly be the OCC personnel, who could work hand in hand with the SOC team on the triage, investigation, and response whenever rail tech is involved.

Rail SOC Management: Every Rail SOC requires a layer of management that will oversee and be responsible for the SOC operations. Depending on the size of SOC, it might go from a single manager to a complex management team composed of several roles and layers. The main tasks to be performed by the Rail SOC Management are as follows:

1. Leadership: SOC management owns and drives the SOC roadmap and the Use Case priorities. It is also the layer to which the rest of the SOC personnel report.
2. Governance: Synchronization with the organization's overall cybersecurity governance function is fundamental to the Rail SOC's ability to ensure that the SOC's cybersecurity objectives are aligned with the organization's risk management priorities.

Lastly, when additional functions other than threat monitoring, such as security solutions management, vulnerability management, etc., are allocated to the Rail SOC, it would likely require the implementation of additional dedicated teams in addition to the ones described here. It is also standard for big SOC teams to count on a small engineering team to develop, implement, and maintain the internal tools needed to deliver the SOC processes.

Final Words

Although a Rail SOC shares many similarities with a regular SOC, it also has specific nuances to consider when designing and implementing this critical component of a rail cybersecurity strategy. This requires careful planning and specialized expertise in the rail field to avoid common pitfalls, establish the correct processes, implement the right solutions, and assemble the right team. Simply replicating the approach used for monitoring the corporate environment in a Rail SOC will likely fail. Instead, it is crucial to understand the unique aspects of a Rail SOC and adapt the planning and execution accordingly for a successful initiative.