SOC-CMM® whitepaper – Assessing and Maturing OT SOCs

1 Executive summary

Operational Technology (OT) environments, including Industrial Control Systems, Industrial Automation, and IIoT assets, are increasingly critical to organizational operations but are also becoming prime targets for cyberattacks. Growing connectivity between OT, IT, and cloud systems has elevated risk levels, making the security of OT environments a top priority.

OT SOCs face unique challenges compared to traditional IT SOCs. Monitoring at lower levels of OT systems is often limited, visibility into assets is constrained, and incident interpretation requires deep contextual knowledge. Response actions in OT environments can have significant operational impact, meaning effective security operations require close collaboration between SOC analysts and OT operators. Furthermore, legacy systems, physical access considerations, and the existence of OT-specific malware introduce additional risk factors.

Recent incidents, such as attacks on national power grids, critical infrastructure campaigns, and targeted intrusions into industrial sites, highlight the high stakes of OT cybersecurity. These events demonstrate that OT assets are targets not only for cybercriminals but also for nation-state actors, emphasizing the need for specialized monitoring and defence.

Emerging trends show an increase in managed OT cybersecurity services, widespread adoption of connected and cloud-enabled OT systems, and higher regulatory and organizational awareness. Modern OT solutions now incorporate security features, improving integration with SOC monitoring, while the OT threat landscape continues to evolve.

SOC operational models vary from fully separated IT and OT SOCs, to SOCs managing IT and OT assets in a fully converged manner, with a hybrid model blending separation and convergence of technology, processes, and staff. Assessment approaches must align with the SOC structure and organizational structure, ensuring that evaluation and reporting reflect both organizational requirements and the specific challenges of OT environments.

Assessing OT SOC maturity across business, people, process, technology, and services domains provides actionable insights to strengthen security operations. Considerations unique to OT, including detection engineering, knowledge transfer, threat hunting, and incident response, must be carefully addressed to accurately evaluate capability and identify improvement opportunities.

In conclusion, maturity assessments of OT SOCs are a vital tool for enhancing cyber resilience, reducing operational risk, and ensuring that critical OT assets are effectively protected. By systematically evaluating capabilities, organizations can implement targeted improvements, fostering more secure and resilient OT operations. This does not require a completely new approach to SOC assessment. Instead, existing methodologies such as SOC-CMM can be leveraged, when taking the uniqueness of OT environments into consideration.

2 Introduction

While physical security has long been a focus, there is increasing awareness of the importance of securing Operational Technology (OT) assets against cyber threats. Current incidents have continued to demonstrate that cyber threats to OT environments are real and that the overall threat level continues to rise. As connectivity between OT and Information Technology (IT) environments increases, OT systems are more exposed to cyber risks than ever before.

A critical component of securing OT environments is the ability to detect and respond to security incidents. This responsibility typically lies with the Security Operations Center (SOC). This whitepaper provides insights and best practices for assessing the maturity and capability of a SOC that monitors and supports OT environments. The results of such assessments can be used to strengthen cyber resilience and reduce the risk of disruptive or destructive cyber incidents.

2.1 Definition

In this document, the following definition of OT is used:

"Hardware and software that detects or causes a physical change via direct monitoring and/or control of equipment, assets, processes, and events."

This definition aligns with widely accepted standards and publications and emphasizes the direct relationship between digital systems and the physical world. This connection is particularly important, as cyberattacks against OT environments can have immediate and tangible real-world consequences.

Throughout this document, the term **OT** is used as an umbrella term encompassing related concepts and technologies, including Industrial Control Systems (ICS), Industrial Automation and Control Systems (IACS), Industrial Automation (IA), and Industrial Internet of Things (IIoT) assets.

While OT differs from IT primarily because it operates in and affects the physical environment, additional distinctions are equally important:

- OT relies on specialized, often proprietary, communication protocols.
- OT systems are designed with a strong emphasis on safety, availability and robustness.
- Security is typically not built in by design but added later as an afterthought.
- OT environments were often designed with the expectation of specific architectural constructs such as data diodes and air-gapped systems being in place.

As connectivity between IT, OT, and cloud environments continues to increase, these fundamental differences significantly elevate the cyber risk exposure of OT environments.

2.2 Purpose

The purpose of this whitepaper is to provide guidance for organizations seeking to build, assess, and mature a Security Operations Center (SOC) capable of effectively monitoring and responding to threats in OT environments.

While the primary focus is on **assessing** OT SOC maturity and capability, the principles, models, and considerations described in this document can also be applied when **designing** or **evolving** an OT SOC.

3 Challenges, threats, and trends

Before exploring the assessment of a SOC that monitors OT assets, it is essential to understand the broader context in which such SOCs operate. OT SOCs deal with a unique set of challenges, threats, and trends that must be considered during assessment and maturity planning.

3.1 Top challenges in OT SOC

Several challenges are commonly encountered when operating a SOC for OT environments:

- **Limited monitoring at lower Purdue levels**
  At the lower levels of the Purdue model (levels 0–2), monitoring OT assets is often difficult or impossible. Most OT monitoring relies on network-based visibility, which is typically implemented at the IT/OT demilitarized zone (DMZ) or at the Operations/Systems management level.
- **Limited visibility into OT assets**
  Unlike IT assets, OT assets generally cannot be equipped with endpoint security tooling such as EDR. This is often technically infeasible and may introduce unacceptable operational risk due to potential disruptions.
- **Event interpretation and prioritization**
  OT environments are highly task-specific. SOC analysts may be required to interpret alerts from multiple OT systems, each with distinct operational roles. Accurate interpretation and prioritization require deep contextual knowledge, which must be transferred from OT operators to the SOC. OT operators, as a generalization, have limited cybersecurity knowledge. Therefore, a common language is often lacking.
- **Understanding the impact of response actions**
  Assessing the impact of response actions in OT environments requires a detailed understanding of processes and dependencies. As a result, SOCs are rarely able to take action on OT systems and must therefore closely collaborate with OT operators during incident response.

Addressing these challenges requires strong cooperation between SOC teams and OT operators, including bi-directional knowledge transfer, process alignment, risk alignment, and technical integration. Because OT and IT disciplines use different terminology, have different priorities, and often hold different perspectives, establishing a mutually understood vocabulary is often an additional challenge.

3.2 Threats, vulnerabilities, incidents, and trends

This section outlines key threats, notable incidents, and emerging trends relevant to OT SOCs.

3.2.1 Threats and vulnerabilities

The threat landscape for OT environments differs significantly from that of IT environments. Key threats and vulnerabilities include:

- **Inadequate OT perimeter protection**
  Weak segmentation between IT, OT, and cloud environments can expose OT assets to IT-based cyber threats.
- **OT-specific malware**
  While relatively rare compared to IT malware, OT-specific malware can pose a significant risk due to its ability to directly manipulate physical processes and remain hidden.

- **User errors**
  Human error remains a major risk factor. In OT environments, the consequences of user mistakes can be severe, including safety incidents or prolonged outages.
- **Physical access to OT assets**
  OT assets are often geographically distributed and located in remote or exposed environments. Physical access to such assets can enable easy introduction of malicious code, leveraging weaker remote sites to target physically protected centralized control systems.
- **Legacy systems**
  Many OT systems are legacy assets that have been in operation for decades. These systems are often outdated, vulnerable, and difficult or impossible to patch, significantly increasing cyber risk.

OT environments may also attract specialized threat actor groups, including nation-state actors and sector-focused adversaries with deep domain expertise.

3.2.2 Notable Incidents

Several notable OT-related cyber incidents have occurred in recent years, including:

- **The Norwegian dam incident (2025),** where a floodgate was remotely opened following a cyber intrusion.
- **A destructive attack on Danish water utility (2024),** where water pressure was changed, causing pipes to burst and households to lose water for several hours.
- Multiple cyber and physical attacks against the **Ukrainian power grid (2015, 2016, 2022 – now).**
- Cyber operations believed to have supported geopolitical actions, such as attacks on national power grids.

These incidents illustrate that OT systems are frequent targets of nation-state. In general, high-value and high-impact targets attract more capable threat actors.

3.2.3 Trends

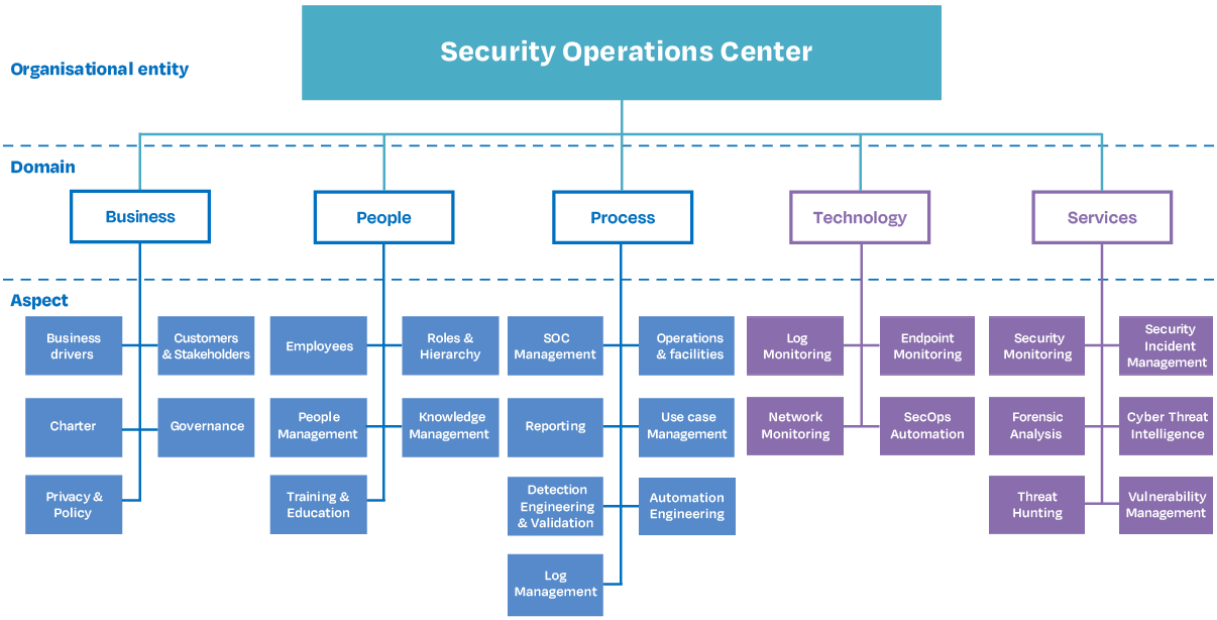
Several key trends are shaping OT security operations:

- **Growth of MSSPs offering OT security services**
  Many managed security service providers are entering the OT space. However, a lack of OT-specific expertise often limits the value of these services. Additionally, scalability is challenging because of the diversity of the OT landscape.
- **Increased connectivity of OT environments**
  Integration with IT and cloud environments enables remote access and operational flexibility but also expands the attack surface. Concerns regarding access control and sensitive information protection extend into the connected environments. Additionally interconnected 3rd party services could impact many critical infrastructure organizations who rely on cloud connected resources for operations.
- **Adoption of modern OT solutions**
  Newer OT systems increasingly include security features such as patching and logging capabilities, making integration with SOC tooling easier.
- **Rising awareness and regulation**
  High-profile incidents and evolving regulatory requirements are driving increased awareness and investment in OT security.

4 Frameworks and models

In this document, several models, frameworks, and standards are referenced. Some of these are specific to OT, while others are more generic. The most important references for this whitepaper are:

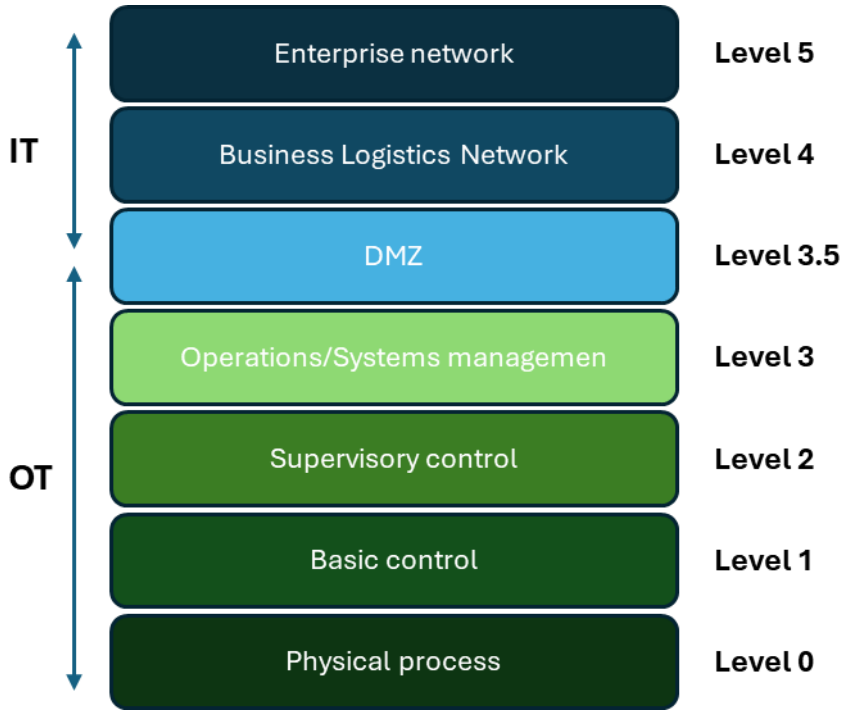
SOC-CMM® [1]. A capability maturity model for SOCs supported by an assessment tool, consisting of five domains and 27 aspects. SOC-CMM® is used as the primary framework for assessing OT SOC maturity and capability.



Purdue model. A reference architecture for OT environments that defines hierarchical levels and separates enterprise IT from OT systems. The model typically consists of 6 levels. For this whitepaper, the following representation of the Purdue reference architecture is used (based on [2]):

[1] SOC-CMM | Improving Security Operations Globally

[2] Figure 1: Purdue Model of Computer Integrated Manufacturing



This representation has a level 3.5 (DMZ), which is not an official part of Purdue, but rather an informal addition.

MITRE ATT&CK® [3]. A knowledge base of adversary tactics and techniques. MITRE ATT&CK® has an enterprise version that can be used to model attacks on IT infrastructure, and IT parts within OT environments. Additionally, there is MITRE ATT&CK® for ICS, specifically tailored to attacks on industrial control systems. These frameworks can be used for defensive gap analysis. MITRE also has a project[4] investigating how to best leverage ATT&CK® for purposes of defending OT networks.

Additional relevant standards and materials include ISA/IEC 62443 [5], NIST SP 800-82 Revision 3 [6], and the SANS Critical Security Controls for ICS [7].

5 OT security operations

Setting up a SOC to monitor an OT environment can be done in several ways. For this whitepaper, we differentiate between 3 approaches, each with their own challenges, advantages, and disadvantages.

1. **A fully separate SOC**. In this case, there is an OT SOC which is completely separated from the IT SOC. When using this model, it is important to understand where responsibilities of each SOC start and end. In terms of Purdue levels, levels 4 and 5 are clearly the domain of the IT SOC, whereas the levels 0 to 3 are the domain of the OT SOC. Clear responsibilities must be assigned at the DMZ level (3.5) to avoid overlap in monitoring or (even worse) gaps in monitoring. Where industrial DMZs exist and interconnected assets communicate across level 3.5, operations should own the responsibility of these connections as they can directly impact operational systems. The main *advantage* of this SOC type is that there is full knowledge and focus on their respective domain (OT or IT) within the SOCs. The main

[3] MITRE ATT&CK®
[4] Defending OT with ATT&CK | Center for Threat-Informed Defense
[5] ISA/IEC 62443 Series of Standards - ISA
[6] SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security | CSRC
[7] The Five ICS Cybersecurity Critical Controls | SANS Institute

disadvantage is that this is a more costly SOC operation to run. *Challenges* include alignment between the individual SOCs.

2. **A partially overlapping SOC**. In this case, there is some overlap between IT security operations and OT security operations. In most cases, this means that the same people will be operating the SOC, but that there is a difference in the processes and technology used for monitoring OT and IT environments. The main *advantage* is that there is increased focus on both domains, while making use of the staff. The *disadvantage* is that, compared to full separation, there is less focus and knowledge on an individual domain. *Challenges* include maintaining knowledge of both domains and managing a more complicated tech stack within 1 team.
3. **A converged SOC**. A fully converged SOC deals with both IT and OT assets uses the same people, processes, and technology to operate the SOC. The main *advantage* is that this is the least costly way to monitor both domains. The *disadvantage* is that there is no specific focus on OT, with the risk of more IT-focused monitoring being put in place. The main *challenge* is ensuring an adequate level of OT monitoring and OT knowledge.

When it comes to SOC assessment, each setup will require a slightly different approach. For fully separate SOCs, separate assessments are required. For partially separated SOCs, it is recommended to do a single assessment but create 2 reports: 1 for each environment. This way, there is still opportunity to manage OT and IT SOC maturity separately. Finally, in a fully converged SOC, there will be a single assessment, with a single report presenting all results.

The table below shows the 3 different types of SOCs and the recommended approach for assessment and assessment reporting.

	People	Process	Technology	# assessments	# reports
Fully separate	Different	Different	Different	2	2
Partial overlap	Same	Different	Different	1	2
Fully converged	Same	Same	Same	1	1

Note that the assessor should always perform an intake to determine the correct approach. Deviating from this table may be necessary because of specific organizational requirements. In a converged environment, an intake will help the assessor determine how different the processes and technology truly are. This will impact the focus areas of the assessment.

6 Assessing and maturing an OT SOC

Capability maturity assessment of any SOC is important to determine strengths and weaknesses in its operations. These insights are subsequently used to create improvement roadmaps. Conceptually, OT SOC **maturity** is not different from IT SOC maturity. The same definitions and interpretations for maturity levels apply. However, there can be distinct **capabilities** that are specific for OT environments.

6.1 Setting maturity and capability targets

One of the first things to do in a SOC-CMM capability maturity assessment is setting the target values for maturity and capability levels. These target values represent the desired levels against which to measure. This can be a target based on expectations of how the SOC should currently be operating. It can also be a target that represents an ambition for the SOC over a longer period. With a fully separate SOC, 2 maturity and capability targets need to be set, one for each SOC. These values may differ because the desired maturity and capability for an OT SOC may be higher than the IT SOC. This

is common in a risk-based approach to SOC maturity. Note that often, target capability levels for OT SOCs will be lower, as there are technological restrictions that result in lower capability scores.

6.2 Assessing the business domain

When assessing the business domain, there are a few aspects of the SOC-CMM model that require specific attention:

- **Business drivers**. Business drivers may differ, especially in case of a fully separated SOC. The OT SOC may have different stakeholders, legal, and customer obligations than the IT SOC. Identification of each, and identification of differences between IT and OT SOC efforts is essential in ensuring the SOC operation matches the SOC business expectations.
- **Customers & stakeholders**. The customers and stakeholders for the OT environment may be different from those for the IT environment. It is important to identify both IT and OT stakeholders and understand their information requirements.
- **Governance**. This is an important topic for any SOC. Primary stakeholders identified in the previous step must give their input into SOC strategic direction to ensure that the SOC remains properly business-aligned. For any type of SOC design, it is important that governance is done in a consistent manner. If there are multiple SOCs (fully separated), governance needs to be in place that ensures alignment between both entities. Using a single SOC steering committee can be an effective way to ensure consistent governance. Mandate is another important part of governance. The SOC may not be empowered to autonomously act in OT environments, but they do need adequate authority to initiate response actions together with the OT operators.
- **Privacy & policy**. This aspect deals also with compliance requirements that apply to the SOC. Specific requirements may apply to the OT environments and need to be considered as they can impact data handling, and process execution within the SOC.

6.3 Assessing the People domain

For the People domain, there are not many specifics that need to be taken into consideration when assessing an OT SOC. The most significant differences may be found in the SOC-CMM aspects *roles & hierarchy* and *knowledge management*. For *roles & hierarchy*, there may be specific roles defined for OT SOC staff. Alternatively, an OT specialist could be part of the SOC. For *knowledge management*, it is important to define how knowledge on OT environments is documented and maintained. This will require active collaboration between the SOC analysts and engineers and the OT operators. Regular knowledge transfer sessions will be required to ensure that knowledge in the SOC is kept current.

6.4 Assessing the Process domain

In the process domain, there are several aspects that are relevant:

- **Architecture**. Good architecture is imperative to properly protect OT assets. This is again where the Purdue model plays an important role, especially in segmentation across IT and OT environments, which is commonly done by creating appropriate industrial DMZs. Connectivity between the SOC and the OT environment must in any case be set up securely, to make sure that this cannot become an attack vector against the OT environment. For example, trusted technology communications from the DMZ are used to attack the OT environment from the IT environment, or the DMZ is leveraged to suppress visibility of the monitoring of the OT environment.
- **Use case management and detection engineering**. Specific use cases for OT must be created. These use cases address specific risks and attack methods against OT assets. The

uses cases should be created in a top-down way: starting with the risks and drilling down to tactics and detection rules. This allows SOC managers to connect detections to business risks and report on them as such.

- **Visibility**. As argued previously, lack of visibility is one of the bigger challenges in OT SOCs. The assessor must make note of how visibility in OT environments is measured and improved. Lack of visibility increases the likelihood of false negatives.
- **Automation engineering**. Automation engineering in OT SOCs is usually limited to analysis automation, and internal SOC automation such as ticket creation and report generation. Response automation in OT environments should be avoided as this may have unforeseen and potentially catastrophic consequences.
- **Threat modelling**. This activity is not a formal part of the SOC-CMM model. However, some SOCs do perform threat modelling for OT environments. The SOC should look specifically at attack vectors, attack paths, and impacts from validated news sources and cybersecurity threat intelligence reports. MITRE ATT&CK® for ICS, along with MITRE ATT&CK® for enterprise, can serve as important pieces of input. When performing threat modelling, the Purdue model will also be an effective way to structure attack path modelling. More complete approaches to threat modelling are also possible when adopting methodologies like TRIKE, STRIDE, or PASTA.
- **Log management**. Log management in OT assets is challenging, as many solutions in OT space are unable to any generate logs. Architectural requirements for moving logs out of an air-gapped environment can also pose a significant challenge for log-based monitoring. A data diode can be used in such cases. Installing agents for monitoring purposes on endpoints is, in general, not an option.

6.5 Assessing the Technology domain

For the technology domain, the regular approach for assessment can be applied to the OT environment as well. Keep in mind that the technology used for monitoring the OT environment will not have the same level of capabilities as the tooling used for the IT environments, resulting in lower capability scores. Additionally, use of technologies such as SecOps automation (using SOAR) or end-point monitoring (using EDR) will likely not be possible in OT environments. Thus, the technology stack for monitoring OT environments will commonly be less extensive than the IT monitoring stack. Working with OT product vendors and building testing environments is advised.

6.6 Assessing the Services domain

The SOC-CMM services domain addresses the most common SOC services. For each of these services, there are specific considerations for OT environments:

Security monitoring. For maturity in security monitoring, the same rules and concepts apply as in IT environments. However, when it comes to capabilities, there will be a significant difference between OT and IT. The SOC-CMM assessment, lists 7 types of detection and 16 types of monitoring. These monitoring types include monitoring of endpoints, identities, applications, behavior, access & usage, databases, and others. Many of these will not be applicable to- or technically feasible in OT environments. To ensure that the SOC-CMM assessment score is accurate, the assessor must choose between setting the score to '*no*' or '*not applicable*'. '*No*' is used in case the monitoring type is applicable but not implemented or not technically feasible. '*Not applicable*' is used only when the type of monitoring mentioned is not applicable to that environment because there are no such components, tracking the thought process and rationale of your choice is advised.

Incident management. For capability in the incidents management service, the SOC-CMM assessment addresses the distinct phases of IR, as specific in NIST SP800-61. These include preparation, identification, containment, eradication and recovery, and post-incident analysis. For OT environments, incident response is usually not performed by SOC personnel. Instead, the incident is handled by OT operators who have a better understanding of the environment and impact of certain response actions. The assessor should make sure to evaluate the OT response process and pay special attention to responsibilities and handover between different teams. Additionally, the assessor should pay attention to specific rules of engagement when it comes to OT incident response. Incorrect response may have worse adverse effects than the actual incident would have.

Forensic analysis. Conducting forensic analysis in OT environments is often much more complicated, especially in legacy environments. It is important to integrate forensic analysis into the incident response procedures, instead of performing it after the event. The reason for this is that the state and information is volatile, and often not retained in OT assets. Therefore, forensic analysis after the event may not yield any viable results. Specific procedures will need to be in place for OT forensics. Input and review from the OT operators is required for the deployment of such procedures. Ease of use by non-cyber staff is paramount for assuring success. For example, a simple to run, tested and validated collection script in an agreeable format (such as a USB if allowed or a DMZ server file share) servers as a “one step” action for an OT operator. Analysis of the collected material is done by knowledgeable SOC or MSSP staff. Considering OT specific applications like data historians, alarm packages, sequence of event data, and operator logs can be useful in forensics analysis to allow the integration of process data along with traditional network and endpoint data sets.

Cyber threat intelligence. For CTI, the SOC should focus on gathering intelligence that is specific to the OT environment. This includes tracking of threat actors and threat actor campaigns specifically to relevant OT environments and tracking OT vulnerabilities and active exploitation of such vulnerabilities. The intelligence gathering and analysis process itself is the same as with CTI for IT environments. The assessor should focus on the specific sources for OT intelligence and the quality and reliability of such sources.

Threat hunting. At the very least, analysis of Indicators of Compromise (IoCs) must be performed for OT environments. Where possible, this should be fully automated for previously discovered IoCs and implemented as an ongoing practice requiring effort to absorb emerging externally provided TTPs and new ideas by SOC staff. Again, MITRE ATT&CK® for ICS and Enterprise can serve as important sources to hunt for signs of specific attack techniques. Note that the effectiveness of threat hunting is limited by the visibility into the OT environments. Limited visibility will mean limited options for threat hunting. Threat hunting at the DMZ (level 3.5) is most common, but SOC management should pursue availability of playbooks with cooperation from OT operations to perform threat hunt activity at level 2 and under certain criteria look for options of hunting at the lower Purdue layers.

Vulnerability management. Performing vulnerability scanning and analysis is more challenging in OT environments. Simply deploying a scanner in the OT network and scanning all assets is not an option, as it may cause unintended interruptions. Rather than active scanning, the SOC should focus on passively gathering vulnerability information. This requires a good inventory of asset types and configurations and the ability to track vulnerabilities for those specific assets. Since direct patching is often not possible, the SOC should investigate other options for dealing with vulnerabilities. This can be virtual patching in the DMZ, deployment of IDS signatures against known exploits, or other compensating controls (both technical and procedural). In some cases, mitigation or compensating

controls may not be possible, and the SOC should aim for risk quantification and acceptance by the asset owner.

6.7 Assessment follow-up

Once the assessment is completed, the next step is to create a report and roadmap for improvement. Capability and maturity improvement in the SOC should follow best practices, including the creation of an improvement program in which improvements are executed through an iterative approach. The SOC-CMM best practice on advancing SOC capability and maturity [8] provides recommendations on SOC maturity growth.

7 Summary

This whitepaper has outlined the critical considerations for assessing Security Operations Centers that monitor and support OT environments. As cyber threats increasingly translate into operational, safety, and reputational risk, boards and executive leadership must recognize that OT cyber resilience is a matter of enterprise risk management. OT SOC maturity and capability assessments, as enabled by SOC-CMM, enable objective oversight, informed decision-making, and risk-based prioritization of investments. When embedded into governance and assurance cycles, these assessments provide a measurable foundation for strengthening resilience, ensuring accountability, and protecting critical operations against disruptive and destructive cyber incidents.

[8] Best practices & whitepapers | SOC-CMM - Improving security operations globally

8 Acknowledgements

This whitepaper was created in a joint effort between SOC-CMM and the following SOC-CMM support partners:

- **Nettles Consulting** (Jan Kopriva)
- **Montance® LLC** (Chris Crowley)
- **Sopra Steria** (Bert de Jong)

Montance®

sopra steria

SOC-CMM® – Improving Security Operations Globally

About

This publication is part of the SOC-CMM® library of best practices and is the result of a joint effort between SOC-CMM® and several SOC-CMM® support partners. SOC-CMM® support partners are verified partners that have trained and certified individuals and verified references for successful SOC service delivery from support partners is ensured. A current list of support partners organised per region and type of partnership (gold / silver) is available on the website: https://support.soc-cmm.com/

This publication is released under Creative Commons license
https://creativecommons.org/licenses/by-sa/4.0/

© SOC-CMM 2026

https://www.soc-cmm.com/