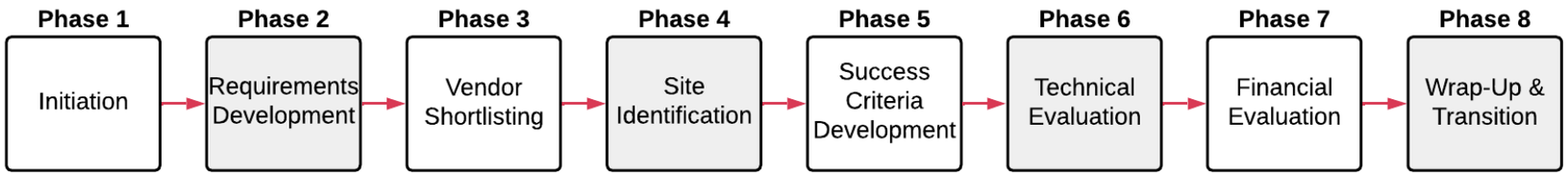
OT Monitoring Tools:

The Ultimate Guide for Conducting Multi-Vendor Proof of Concepts

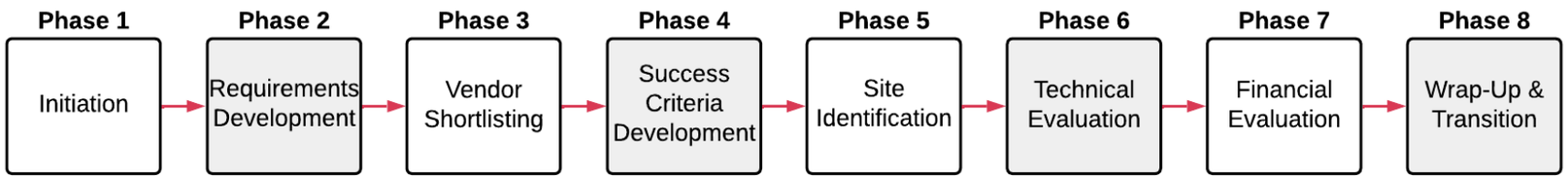
Raphael Arakelian
Prepared for CISA x ICSJWG | Spring 2023

Background: the purpose of this guide is to help organizations understand the current market offerings in OT monitoring as well as to provide a structured approach for conducting proof of concepts. This document is set up according to the first high-level flowchart shown below (variation A); however, other variations (in series or in parallel) can be used to execute the phases of this guide (e.g., variation B)

Variation A: the 8 phases are executed in series, following the structure presented in the guide



Variation B: a variation (out of many) that exemplifies how the sequence of the phases can be swapped



Phase #	Phase Title	Key Activity	Comments on Best Practices
1	Initiation	● Initiate the proof of concept as part of a formal cybersecurity project, following your organization's project management and documentation guidelines. Additionally, ensure that a business case document is associated with the proof of concept	● OT monitoring proof of concepts that are not formally associated with a project, but are loosely conducted through ill-defined interactions / demos with vendors, may not demonstrate sufficient due diligence from an engineering / procurement perspective and are less likely to transition into OT cyber monitoring programs ● A business case document facilitates the buy-in from various stakeholders (e.g., business leaders, site managers, etc.) into your vision for OT monitoring, which is required for executing the proof of concept as well as for its ultimate transition into an OT cyber monitoring program. Developing a business case early on can also facilitate budget planning and approval
		● Establish a steering committee for the proof of concept while defining the roles and responsibilities of its members. In addition to the standard stakeholders, as defined by your organization's governance structure for cybersecurity projects, ensure that the following stakeholders are included in the committee: ○ Operations / OT representative ○ Cybersecurity service provider representative (if applicable: optional) ○ System integrator representative (if applicable: optional)	● Setting up an OT cyber monitoring program is typically a multi-departmental journey (e.g., cybersecurity, operations, network infrastructure, etc.) which requires cross-functional collaboration. This collaboration, however, should not be sought after a tool has been selected by a specific department / sponsor but should rather be initiated at the proof-of-concept stage, increasing the likelihood of a suitable tool selection and minimizing resistance to change during its implementation ● A steering committee, with a representation from all key departments, facilitates cross-functional collaboration early on, expedites the removal of obstacles, and ensures that the progress of the proof of concept aligns with the established vision for OT cyber monitoring. Defining the roles and responsibilities of the various stakeholders, however, is required to ensure accountability ● Depending on the role of the cybersecurity service provider / system integrator within your organization, it is important to consider these stakeholders for the steering committee, as their input can influence the vendor selection process (e.g., requirements for technology integrations, lessons learned from similar evaluations, etc.)

Phase #	Phase Title	Key Activity	Comments on Best Practices
1	Initiation	● Identify and document the cybersecurity requirements / guidelines (regional, federal, industry-specific) that can be supported by OT monitoring or are related to it : ○ ***Example (regional, industry-specific):*** multiple North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) requirements can be supported by the implementation of OT monitoring (e.g., CIP-002-5.1a, CIP-003-8, etc.) ○ ***Example (regional, industry-specific):*** the European Union Agency for Network and Information Security (ENISA) emphasizes the role of OT monitoring throughout their guidelines on securing Industry 4.0 and smart manufacturing organizations (e.g., PS-13, PS-23, etc.) ○ ***Example (federal):*** based on the Binding Operational Directive 23-01, the United States' Cybersecurity and Infrastructure Security Agency (CISA) mandates that all Federal Civilian Executive Branches (FCEB) conduct automated asset discovery every 7 days	● Documenting the role of OT monitoring with respect to cybersecurity requirements / guidelines helps build a more compelling business case and can contribute to the urgency for an OT cyber monitoring program ● Cybersecurity requirements / guidelines can present an unbiased examination of the best practices in OT monitoring as well as of its use-cases and limitations - this can ultimately enable better informed decision-making in the vendor selection process
		● Compile a list that classifies your organization's operational sites using the following parameters: ○ Business unit ○ Business criticality ○ Size (estimated number of network-connected assets, estimated throughput) ○ Connectivity to a centralized network (corporate network, operations network, cloud, etc.) ○ Communication infrastructure (fiber, radio, satellite, etc.) ○ Network topology (ring, bus, mesh, etc.) ○ Network infrastructure maturity (high, medium, low) ○ Availability of site documentation (asset inventory, network diagram)	● This key activity allows you to develop a complete picture of your sites, identifying their unique constraints for OT monitoring. Evaluating vendors without a comprehensive understanding of your current state may result in the selection of a vendor which is compatible with some sites but not with others, potentially introducing significant costs for rework ● This key activity also ensures that the members of the steering committee are engaging in information gathering and sharing, both of which are needed for building a unified vision for an OT cyber monitoring program ● Classifying your operational sites by business unit and criticality helps you determine any specific business and technical requirements, which should be accounted for in the vendor evaluation process (e.g., if your organization has multiple lines of business, such as electricity generation vs. gas production, each business unit might have specific constraints, such as requirements for data residency) ● The size of your sites is an important factor that impacts the design and / or pricing proposed by OT monitoring vendors. Most vendors size and / or price their offerings based on the estimated number of network-connected assets per site, while a few vendors do so based on the estimated throughput per site. If you are uncertain of the sizing and / or pricing practices of a candidate vendor, classify your sites using both parameters

Phase #	Phase Title	Key Activity	Comments on Best Practices
1	Initiation	***Continued***	• A centralized network is any form of network, whether on-prem or in the cloud, to which multiple sites connect (e.g., corporate network, SCADA network, etc.). This parameter helps you determine how each site can be monitored at an aggregate level, by means of a central appliance (i.e., consolidation of multiple sites) • The communication infrastructure of a site (e.g., fiber, radio, etc.) can impact how you consolidate the monitoring of multiple sites, while the network topology (e.g. ring, bus, etc.) can impact where you deploy the monitoring in the site itself. The first parameter is usually relevant for any type of monitoring, while the latter may be more relevant for network-based monitoring (the different types of monitoring are discussed in the next phase) • Network infrastructure maturity refers to the presence of managed switches with port mirroring capabilities and can be classified as follows: ○ High maturity sites have all their switches as managed switches with port mirroring capabilities ○ Medium maturity sites have their core network switches as managed switches with port mirroring capabilities, while the remaining switches are either unmanaged or cannot support port mirroring (or vice versa) ○ Low maturity sites have all their switches as unmanaged switches or cannot support port mirroring. These sites are typically unsuitable for network-based monitoring, unless network taps are installed or the network infrastructure is upgraded • Site documentation (i.e., asset inventory, network diagram) can be helpful for the following reasons: ○ First, the availability of asset inventories, as well as where and how they are maintained, can be a strong indicator of the maturity of your asset management practices. This can help you determine the urgency in addressing asset management as part of your OT cyber monitoring program, and should therefore be prioritized accordingly in your vendor evaluation process ○ Second, asset inventories, regardless of the common spreadsheet format, can be leveraged by many OT monitoring tools as a

Phase #	Phase Title	Key Activity	Comments on Best Practices
1	Initiation	****Continued****	starting point for asset discovery and can be used by your steering committee to validate a tool's performance (whether during the proof of concept or in a formal deployment) ○ Finally, network diagrams can help you identify different variations in the architectures of your sites, which can be then shared with vendors for design and pricing purposes
2	Requirements Development	● Develop an understanding of the types of OT monitoring, including their strengths and limitations. Based on the current market offerings, this guide distinguishes between the following types of OT monitoring: ○ Network-based monitoring ○ Host-based monitoring ○ Integration-based monitoring ○ Targeted active scanning	● ***Important overview on the types of OT monitoring and their strengths as well as their limitations -*** the following are the major types of OT monitoring currently present in the market: ○ Network-based monitoring: with this method, the monitoring tool passively ingests mirrored traffic from your network switches and / or network taps. Network-based monitoring is used for its quick deployment, negligible resource consumption, and its non-intrusive nature. As long as your network infrastructure is compatible, network-based monitoring can have a wide coverage of your assets while alerting on network anomalies and / or attack signatures in real-time. The downside is the limited visibility into individual assets as well as a large number of false positive alerts ○ Host-based monitoring: this type monitors threats at the endpoint level, alerting on anomalies and / or attack signatures based on audit trails and other types of logs. This method provides much more visibility into the host assets, thus augmenting asset management, configuration management, and vulnerability management capabilities while unlocking additional cybersecurity functionalities (e.g., patch management). The downside is its slower deployment process, consumption of endpoint resources (potentially minimal), and limited compatibility with different types of endpoints (i.e., host-based monitoring is typically used for IT-type endpoints; only one vendor currently offers host-based monitoring on specific types of PLCs) ○ Integration-based monitoring: this type of monitoring can be a feature in network-based monitoring tools, host-based monitoring tools, or can be its own standalone product. It involves integrating with various types of data sources in the operational network (e.g., SCADA system, OPC software, security tools, etc.). Manual ingestion of inventory / configuration files, despite not being automated, is also a type of data integration that belongs in this

Phase #	Phase Title	Key Activity	Comments on Best Practices
2	Requirements Development	****Continued****	category. Integration-based monitoring is mostly focused on developing comprehensive asset inventories, in addition to tracking configurations and vulnerabilities with a high degree of confidence. The downside is the dependency on the availability of data sources and the need for custom integrations with each new software / application ○ Targeted active scanning: this type of monitoring can be a feature in network-based monitoring tools, host-based monitoring tools, or can be its own standalone product. Targeted active scanning is the polling of specific endpoints using their native protocols, for specific responses only. It is important to not confuse targeted active scanning with traditional active scanning, the latter which is used by IT tools for vulnerability assessments and can cause major disruptions in operational networks. Targeted active scanning (labeled in the market using various names, including active queries, polling, selective probing, smart polling, smart scanning, etc.) is specifically designed for OT environments and has little to no impact on the scan cycle of non-legacy equipment. This method can be used for developing comprehensive asset inventories, in addition to the detailed collection of configurations, both of which ensure tracking of vulnerabilities with a high degree of confidence. The downside is the limitation in deployment options (especially for the stand-alone, software-only vendors) and the manual initial configuration for each targeted scan, keeping in mind that the product might not have a targeted scan option that is compatible with every type of device and / or protocol ● ***Important background of the developments in OT monitoring technology -*** historically, network-based technology has been the de facto method of OT monitoring, considering its minimal interference with the network due to its passive mode - this has aligned well with operations' priorities for system availability and the minimization of any potential disruptions. Despite the need for network-based threat detection, via anomalies and / or attack signatures, using this type of technology alone means that most of the tool's other cybersecurity functions (i.e., asset management, configuration management, vulnerability management) are dependent on the quality and content of the network traffic, often leading to limited visibility and gaps. This,

Phase #	Phase Title	Key Activity	Comments on Best Practices
2	Requirements Development	****Continued****	in addition to the alert fatigue experienced with network-based detection, has led to various shifts in the industry: ○ First, the development of targeted active scanning in OT monitoring tools, which, along with the adoption of credentialed active scans, has played a compensating role to enhance the asset detection, asset identification, configuration detection, and vulnerability detection functions ○ Second, the adoption of host-based monitoring for OT environments, which can provide, in addition to threat detection at the endpoint level, more visibility into asset attributes, configurations, and vulnerabilities ○ Third, the decoupling of threat detection from the remaining cybersecurity functions in OT monitoring tools, meaning that some vendors (and organizations) focus on asset management, configuration management, and vulnerability management only ○ Fourth, and finally, a mix and match of vendor offerings to address some / all of these cybersecurity functions or to simply compliment the gaps in the products of their peers (e.g., network-based OT monitoring vendor that supports targeted active scanning but also offers host-based agents for enhanced endpoint visibility; OT monitoring vendor that focuses on targeted active scanning only but integrates with network-based monitoring tools to enhance the latter's asset inventory) ○ In summary, each type of OT monitoring has its strengths and limitations, dictated by the cybersecurity challenges it is trying to address. The key takeaway for the steering committee is to first determine its cybersecurity priorities and then evaluate vendors accordingly (discussed in the next key activity)
		● Based on the steering committee's cybersecurity priorities for operational sites, identify the cybersecurity domains that that you would like to be supported by the OT monitoring implementation, ranking them from highest to lowest priority: ○ ***Example:*** asset management (highest priority) ○ ***Example:*** threat detection ○ ***Example:*** vulnerability management ○ ***Example:*** configuration management ○ ***Example:*** incident response (lowest priority)	● Cybersecurity domains can be renamed according to the cybersecurity framework / model that your organization follows (e.g., National Institute of Standards and Technology Cybersecurity Framework, Cybersecurity Maturity Model Certification, etc.) ● To validate the relevance of other cybersecurity domains to OT monitoring, refer to the cybersecurity requirements / guidelines from the previous phase. Vendors' solution briefs may also be insightful, despite being presented from a marketing standpoint. Examples of

Phase #	Phase Title	Key Activity	Comments on Best Practices
2	Requirements Development	****Continued****	other cybersecurity domains which can be supported by OT monitoring include: audit and compliance, network security, patch management, risk management. Integrations with other cybersecurity tools can broaden this list to additional possibilities (e.g., credential management, security analytics, etc.) ● Prioritization of the cybersecurity domains should be conducted from a general perspective (i.e., at a high level) and not on an individual site basis. One possible option that can facilitate this prioritization process is to reference your organization's risk management framework, which ideally covers your operational environment ● In this example, a hypothetical steering committee has identified asset management as its highest cybersecurity priority, followed by threat detection, vulnerability management, configuration management, and incident response
		● With respect to each cybersecurity domain, identify the key functionalities that the steering committee is seeking in an OT monitoring tool: ○ ***Example (asset management):*** detect network-connected assets; identify the following attributes of the detected assets: asset class, asset type, vendor, model, OS / firmware version, serial number, protocols used ○ ***Example (threat detection):*** establish a network baseline and alert on any deviations in it; detect signatures associated with the most common network attacks in OT environments ○ ***Example (vulnerability management):*** detect full match CVEs based on the OS, firmware version, or model of the network-connected assets ○ ***Example (configuration management):*** establish a configuration baseline of the network-connected OT assets and alert on any deviations in it ○ ***Example (incident response):*** facilitate the post-mortem investigation of security incidents	● The key functionalities of an OT monitoring tool are the basic capabilities that support one or more cybersecurity domains. In addition to the cybersecurity requirements / guidelines from the previous phase, other sources of insight into the art of the possible include: conferences, market research publications, white papers, peer groups, vendor showcases / demos. Taking note of any vendor names during this key activity can help you develop an initial list of candidates to evaluate ● The following is a high-level overview of the key functionalities of OT monitoring tools with respect to each cybersecurity domain in this example: ○ From an asset management perspective, OT monitoring tools are used to create an asset inventory, through the automated discovery of network-connected assets as well as their attributes. The generated asset inventory can be then consolidated with your organization's asset / configuration management database ○ For threat detection, OT monitoring tools (either network-based or host-based) can alert on deviations in a behavioral baseline and / or on signatures associated with adversarial attacks, thus corresponding to anomaly-based threat detection and

Phase #	Phase Title	Key Activity	Comments on Best Practices
2	Requirements Development	****Continued****	signature-based threat detection, respectively. The generated alerts can be then integrated into your enterprise / operations SIEM platform, enabling event correlation with other sources of data ○ For vulnerability management, OT monitoring tools are used to detect CVEs or vulnerabilities without an assigned CVE. The resulting database of vulnerabilities can be then integrated with the broader vulnerability management tools used in your organization ○ To support configuration management, OT monitoring tools can identify the configuration of the detected assets and establish a configuration baseline to report on - this functionality can then integrate with the applicable configuration items in your configuration management database ○ For incident response, OT monitoring tools can be used to investigate and respond to a security incident, given that they are monitoring network-level and / or endpoint-level events - this functionality can be integrated with your case management system ● Every steering committee should specify 1 - 3 key functionalities per cybersecurity domain, with the upper end of this range being suggested for the highest priority domains ● Based on its review of the applicable cybersecurity requirements / guidelines and relevant white papers, the hypothetical steering committee from the previous example identifies two key functionalities for both asset management and threat detection as well as one key functionality for each of the remaining domains. You may notice that the committee in this case is already leaning towards network-based monitoring due to its need for threat detection at the network level ● At this stage, however, not every steering committee may have a clear picture of which type(s) of OT monitoring to evaluate - the next key activity is intended to help with that

Phase #	Phase Title	Key Activity	Comments on Best Practices
2	Requirements Development	● The following is a list of the most common constraints that impact the technology, design, and implementation of OT monitoring. By referring to your list of classified sites, evaluate the following constraints: ○ Types of endpoints in your operational sites (IT-type endpoints, OT-type endpoints) ○ Key manufacturers and prevalent protocols of your OT-type endpoints ○ Ability to mirror traffic from the various levels of network switches (locally, remotely) ○ Willingness to upgrade your network infrastructure ○ Willingness to install network taps ○ Willingness to deploy agents / software on applicable endpoints ○ Willingness to use targeted active scanning ○ Availability of data sources to integrate with (SCADA system, OPC software, security tools, etc.) ○ Preference for the type of monitoring (network-based, host-based, integration-based, targeted active scanning) ○ Preference for the type of deployment (physical appliance, virtual appliance, agents / software) ○ Space availability in your operational sites ○ Power availability in your operational sites ○ Operating conditions in your operational sites ○ Ability to centralize the management of multiple sites ○ Preference for the type of centralized management (on-prem, in the cloud) ○ Preference for the type of licensing (on-prem, in the cloud) ○ Preference for the means of deployment (in-house resources, cybersecurity service provider / system integrator)	● Assessing your sites' constraints helps you narrow down the type(s) of OT monitoring you may want to evaluate. It can also help you define specific business and technical requirements, ensuring that the vendors you evaluate in the proof of concept are the most compatible to your needs ● Most of these constraints should be evaluated by the steering committee from a general perspective (i.e., at a high level). If certain site classifications have unique constraints, make sure that those are captured separately (e.g., different preference in the type of monitoring across business units, different operating conditions across high vs. low criticality sites, etc.). Additionally, the following constraints may require an examination on a site-by-site basis: ○ Types of endpoints in your operational sites (IT-type endpoints, OT-type endpoints) ○ Key manufacturers and prevalent protocols of your OT-type endpoints ○ Ability to mirror traffic from the various levels of network switches (locally, remotely) ● The types of endpoints in your operational sites should be categorized as follows: IT-type endpoints (e.g. workstations, servers, etc.), OT-type endpoints (e.g. PLCs, RTUs, etc.). Network devices and IIoT devices can each be placed as their separate categories or can be included under the IT-type endpoints and OT-type endpoints, respectively. It is important to note the prevalence of serial devices within your operational sites, as they typically require specialized hardware for detection (e.g., protocol gateways, serial data taps, etc.). Reflecting on the level of visibility you want to achieve and the cybersecurity domains you want to cover for each type of endpoint may help you develop a preference for specific type(s) of monitoring ● When examining your OT-type endpoints, identify the key manufacturers and prevalent protocols to verify their compatibility with your candidate tools (as well as to identify any unique integrations and / or capabilities offered by the OT monitoring vendors)

Phase #	Phase Title	Key Activity	Comments on Best Practices
2	Requirements Development	****Continued****	• As indicated in the previous phase, the prevalence of managed switches with port mirroring capabilities dictates the network infrastructure maturity of a site, which is one of the most important constraints for network-based monitoring. Your classification list of sites can help determine your ability to mirror traffic, both locally and remotely. If you observe that many of your sites have low network infrastructure maturity, the next logical constraint that you should examine is whether your organization is planning on upgrading its network infrastructure, and if not, whether it is willing to install network taps. It is important to note that both of these options need to be planned for from a time, resource, and procurement perspective, keeping in mind that the infrastructure upgrade can benefit beyond just OT monitoring. Some organizations may still prefer to install network taps (due to their reliable support of heavy network traffic), even if the sites' switches are capable of port mirroring. If you have a low maturity network infrastructure across your sites, and your organization is not willing to upgrade its infrastructure or install network taps, then network-based monitoring is not suitable for you • Your willingness to deploy agents / software as well as to use targeted active scanning can be dependent on the key functionalities you identified, the culture in your operations team (and their willingness to change any preconceived notions on those practices), the relationship between your cybersecurity and operations team, any restrictions in equipment warranties • Data sources, whether OT or security related, may not be available in every individual site; however, their availability in a centralized operational network (e.g., SCADA network, OT DMZ, etc.) is typically sufficient for integration-based monitoring • By understanding the strengths and limitations of the different market offerings, by developing a list of key functionalities, and by examining your sites' constraints, you can now develop a preference for the type(s) of OT monitoring you want to evaluate. You can also choose to not restrict your evaluation to one type of monitoring during the proof of concept, especially since many vendors combine different

Phase #	Phase Title	Key Activity	Comments on Best Practices
2	Requirements Development	****Continued****	methods as indicated earlier • If deciding on a physical deployment of appliances, the space and power availability in operational sites as well as the operating conditions are some of the most common parameters that organizations should examine, ensuring that the appropriate appliance models are evaluated during the proof of concept • Your organization's ability to centralize the management of multiple sites is dependent on the connectivity of your operational sites to a centralized network as well as on the type of the communication infrastructure, both of which are captured in the classification list from the previous phase. Typically, operational sites that share a common centralized network and a communication infrastructure are the easiest to aggregate in terms of management (if it makes sense to do so from a business perspective). If the operational sites share a common centralized network but not a communication infrastructure, it is still possible to aggregate them as long as the individual appliances in each site have been architected to communicate back to a central platform. As indicated in the previous phase, if your organization has multiple lines of business, each unit might have its own constraints, especially for the centralized management (e.g., on-prem using the corporate network, on-prem using an operational network, in the cloud, etc.) as well as for the licensing model (e.g., on-prem, in the cloud) • Reflecting on the means of deployment (i.e., in-house resources, cybersecurity service provider / system integrator) helps you identify if your organization requires a product offering from the vendors or a bundled offering of both product and professional / deployment services. It is important to note that many OT monitoring vendors are product-based companies only, without any types of services (a select few do); however, they can partner with cybersecurity service providers / system integrators to provide bundled offerings

Phase #	Phase Title	Key Activity	Comments on Best Practices
2	Requirements Development	● Determine the target state by which the OT monitoring tool will be operationalized: ○ In-house resources (dedicated analysts / high maturity) ○ In-house resources (ad hoc / low maturity) ○ Third party services (cybersecurity service provider / system integrator, OT monitoring vendor) ○ Hybrid of in-house and third party (shared responsibilities between in-house and third party resources)	● As discussed earlier in this phase, each type of monitoring requires a different level of effort to configure and / or operate. By reflecting on the target state of your OT cyber monitoring program, your preference for the type(s) of monitoring may also be influenced. For example, if your organization is considering a network-based monitoring approach (passive only) and intends to operate its tool in-house, without any dedicated analysts, you may need to consider how and if your organization can address the expected false positives (e.g., targeted active scanning and / or integrating with OT data sources can improve asset contextualization and reduce false positives). It is also possible, in this hypothetical example, to proceed with your initial approach (passive only), if network-level threat detection is a high priority, and you are not willing to leverage other types of monitoring - in that case, you can evaluate the extent of false positives for each candidate vendor during the proof of concept ● Additionally, this key activity ensures that the steering committee is identifying any resource and process limitations early on, which can be documented in the business case, therefore increasing the likelihood of a successful OT cyber monitoring program
		● Leverage your responses to the various key activities of this phase to develop a list of business requirements for OT monitoring: ○ ***Example (BR-1):*** tool must inventory network-connected assets ○ ***Example (BR-2):*** tool must alert on network-related threats ○ ***Example (BR-3):*** tool must have an on-prem centralized management platform that aggregates all individual monitored sites	● This key activity ensures that the steering committee is evaluating the role of OT monitoring with the context of its business needs. Additionally, well-defined business requirements ensure that only the most compatible vendors are evaluated in the proof of concept, thus increasing the likelihood of a suitable tool selection, with the optimal risk reduction and minimal amount of rework ● The list of business requirements can be as extensive as required but should have at least 10 items to ensure that your business needs are covered comprehensively. Since this list can be utilized as part of a RFP in the next phase, you can also leverage your organization's applicable procurement guidelines ● Below is an exemplification of how BR-1, BR-2, and BR-3 are developed by the hypothetical steering committee from the previous phase: ○ While compiling its classification list, the steering committee notes

Phase #	Phase Title	Key Activity	Comments on Best Practices
2	Requirements Development	****Continued****	that most of its sites have a high network infrastructure maturity, and while the remaining sites are of medium maturity, their network switches are scheduled for an upgrade in the upcoming 6 months. Additionally, all of the operational sites share a communication infrastructure that connects back to the OT DMZ ○ As mentioned in the first key activity of this phase, this steering committee has identified asset management as its highest cybersecurity priority, followed by threat detection, vulnerability management, configuration management, and incident response ○ While conducting its research and information gathering on the various functionalities in OT monitoring, the steering committee identifies its need for an asset inventory as well as for network-level threat detection, which are captured by BR-1 and BR-2, respectively. The remaining key functionalities should be similarly expressed through additional business requirements, not exemplified here for simplicity ○ While evaluating its sites' constraints, listed in the fourth key activity of this phase, the steering committee identifies its preference for on-prem centralized management, especially due to the sites' connectivity to the OT DMZ through a shared communication infrastructure - this is captured by BR-3. It is important to note that not every constraint needs to be addressed by a business requirement - just the ones that can be associated to a business need
		● Leverage your responses to the various key activities of this phase to develop a list of technical requirements for OT monitoring: ○ ***Example (TR-1):*** tool must use network-based monitoring to passively detect anomalous behavior as well as network-based attack signatures ○ ***Example (TR-2):*** tool must leverage deep packet inspection to identify the following attributes for the detected assets: asset class, asset type, vendor, model, operating system (OS) / firmware version, serial number, protocols used ○ ***Example (TR-3):*** tool must leverage native OT protocols to conduct targeted active scanning on the detected PLCs (specifically: SIMATIC S7-300, SIMATIC S7-1200, SIMATIC S7-1500)	● Well-defined technical requirements help identify which OT monitoring vendors can meet the functionalities you require, while adhering to your sites' constraints, and therefore minimizing the number of vendors that you need to evaluate with an on-site proof of concept ● The list of technical requirements can be as extensive as required but should have at least 15 items to ensure that you have enough technical specificity. Since this list can be utilized as part of an RFP to OT monitoring vendors, you can leverage your organization's relevant procurement guidelines ● Continuing with the example from the previous key activity, below is

Phase #	Phase Title	Key Activity	Comments on Best Practices
2	Requirements Development	****Continued****	an exemplification of how TR-1, TR-2, and TR-3 are developed by the hypothetical steering committee: ○ While examining its sites' constraints, the steering committee identifies its preference for a quick deployment which can provide a high coverage of its network. This, in addition to its compatible network infrastructure and need for network-level threat detection, consolidates its preference for network-based monitoring, captured by TR-1 ○ Despite the limited visibility it expects into individual endpoints, due to the inherent limitations of network-based monitoring (passive), the steering committee has a higher priority in identifying the attributes of its OT-type endpoints over its IT-type endpoints ○ In addition to the requirement for deep packet inspection, which allows for the identification of the desired attributes (captured by TR-2), the steering committee recognizes its need for targeted active scans that are compatible with its PLCs (SIMATIC S7 models) - this is captured by TR-3 ○ It is worth noting that a steering committee should ensure that all of its sites' constraints and required key functionalities are covered by technical requirements, not exemplified here for simplicity
3	Vendor Shortlisting	● Develop an initial list of OT monitoring vendors that the steering committee is interested in evaluating	● The following sources can be leveraged by the steering committee to identify OT monitoring vendors of interest: conferences, market research publications, white papers, peer groups, vendor showcases / demos, recommendations from cybersecurity service providers / system integrators; most of these sources may have already been examined in the previous phase, when identifying your required functionalities ● The initial list can be as extensive as required, although a reference to your business and technical requirements can help shorten it

Phase #	Phase Title	Key Activity	Comments on Best Practices
3	Vendor Shortlisting	● If warranted by the procurement process in your organization, or if the steering committee wishes to shortlist the list of vendors to 3 (recommended), issue an RFP. In addition to the standard sections of an RFP, as defined by your organization's procurement guidelines, ensure that the following items are included: ○ Business requirements (from the previous phase) ○ Technical requirements (from the previous phase) ○ List of classified sites (from the first phase) ○ Different variations in the network diagrams of your sites ○ Request for a pricing schedule, listing the specific line items that you require (product, licensing, annual support, training, professional / deployment services, etc.)	● For many organizations, issuing an RFP for product evaluations is mandatory. If that is the case for you, ensure that the requirements from the previous phase as well as your list of classified sites are incorporated into the RFP. Different variations in your network diagrams can also provide vendors with a better understanding of some of your site parameters (e.g., connectivity to centralized network, communication infrastructure, network topology, etc.) - if not available, it is suggested to construct these, even if at a high level ● It is worth noting that even if an RFP is issued, on-site proof of concepts are a must for every organization for a myriad of reasons. By evaluating OT monitoring vendors in your environment, you ensure that: ○ The value of OT monitoring is quantified ○ The value of OT monitoring is demonstrated to various stakeholders ○ Trust is built with operations, minimizing resistance to change during the deployment of the selected tool ○ Lessons learned are documented and incorporated into your deployment plan ○ You are selecting a tool that you know is actually compatible to your sites and needs ● It is up to your discretion as well as your organization's procurement guidelines on how to structure the RFP and its overall scoring. A suggested approach is to set up an RFP with multiple scoring rounds, with a pass / fail during the first round which focuses on the business and technical requirements, while the pricing and the proof of concept are evaluated for the shortlisted vendors only. However, since cost is typically a significant factor which may vary widely, it is also reasonable to score the pricing in conjunction with the business and technical requirements in the first round, as long as you shortlist no more than 3 vendors for the proof-of-concept evaluation ● Conducting proof of concepts with more than 3 vendors is still possible but not recommended, as it is usually excessive, especially if your business and technical requirements are well developed and representative of your needs. Typically, having 3 vendors for proof of

Phase #	Phase Title	Key Activity	Comments on Best Practices
3	Vendor Shortlisting	****Continued****	concepts ensures enough product diversity and competitiveness, without the added workload for managing additional vendors / products ● If the procurement process in your organization does not warrant an RFP, but you have identified more than 3 initial vendors, it may still be beneficial to issue an RFP to help shortlist the candidate vendors. You may also choose to informally score your initial list of vendors against your business and technical requirements, without issuing an RFP, as long as pricing is not a concern at that stage ● If an RFP is issued, evaluate the responses and determine the top candidate vendors with the highest overall scores, with which you can then proceed to the next phase
4	Site Identification	● From your list of classified sites, select one for the proof of concept while taking the following parameters into consideration: ○ Similarity in the constraints between the selected site and the rest of your operational sites ○ Type of environment (production, development, testing) ○ Scheduled downtime window (if applicable) ○ Relationship with the on-site operations team ○ Implementation prerequisites (change management approval, space availability, power availability, networking, etc.) ○ Level of support required from the on-site operations team during the technical evaluation phase ○ Presence of third party-managed equipment ○ Methods of access into the site (on-site physical access, remote access) ○ Availability of site documentation (asset inventory, network diagram)	● Although your operational sites may not share the exact same constraints, it is important for the steering committee to identify a site that represents the bulk of them ● If you noted major variations in your sites' constraints in the previous phase, you may need to conduct a proof of concept in more than one site, ensuring that the selected tool is compatible across your entire operations - variations in the following constraints may warrant that action: ○ Types of endpoints in your operational sites (IT-type endpoints, OT-type endpoints) ○ Key manufacturers and prevalent protocols of your OT-type endpoints ○ Preference for the type of monitoring (network-based, host-based, integration-based, targeted active scanning) ● For some organizations, conducting a proof of concept in a production site may not be possible. If that is the case for you, a development or testing environment can be selected instead, despite not being fully representative of your operational complexity and your sites' constraints. If possible, select an environment that is the most comparable to one of your production sites

Phase #	Phase Title	Key Activity	Comments on Best Practices
4	Site Identification	****Continued****	• If a production site can be selected, identify the procedures for conducting changes / projects in the environment. For some organizations, a proof of concept may only be conducted during a downtime window (e.g., for maintenance, upgrades, production shutdown, etc.). If that is the case for you, consider a site that has a scheduled downtime window and plan your proof-of-concept schedule accordingly. As a best practice, avoid conducting proof of concepts during an unplanned downtime window to prevent any additional workload on the operations team (it can also be difficult to coordinate with the candidate vendors on short notice) • Although the relationship with the on-site operations team is often overlooked, it is an extremely important parameter to reflect on. Collaborating with operations ensures a solid understanding of the site, including its systems, processes, and network infrastructure, as well as the operators' day-to-day activities, desired use-cases, and concerns - all of which need to be considered to successfully secure operational sites. The proof of concept is a perfect opportunity to cultivate trust with operations and work towards the common goal of safe and reliable production, with minimal disruptions and incidents (cybersecurity related or otherwise). The business case document and the OT representation in the steering committee can facilitate your engagement with the on-site teams • By coordinating with the on-site operations team as well as the candidate vendors, the steering committee should identify any implementation prerequisites that need to be addressed before proceeding with the proof of concept. These prerequisites can vary based on your site's constraints, type(s) of monitoring being evaluated, and type of deployment being considered • Additionally, the steering committee should determine the level of support that is required from the on-site operations team during the technical evaluation, specifically for the following activities: ○ Setting up the candidate tools ○ Recurring check-ins on the performance of the candidate tools ○ Conducting controlled changes in the environment ○ Scoring the tools

Phase #	Phase Title	Key Activity	Comments on Best Practices
4	Site Identification	****Continued****	○ Uninstalling / removing the deployed tools upon completion of the proof of concept In some cases, the on-site team might take full ownership of some of these activities, but in most cases, it is only the controlled changes that may require their full ownership (with guidance from the steering committee). The level of support that can be provided by the on-site team also depends on their availability and working knowledge of networking ● It is important to identify any third party-managed equipment in the selected site, especially if that equipment needs to be configured or is expected to be affected in any way during the proof of concept. If that is the case, ensure that the relevant third parties are notified and involved ● Depending on the level of support that is identified for the on-site team, the steering committee should determine if other parties require on-site physical access and / or remote access. If, for example, a cybersecurity service provider / system integrator is assigned to set up the candidate tools, they need to be provided with the relevant training and other prerequisites to obtain on-site access. Remote access (in a secure way) can also be beneficial for providing relevant stakeholders (e.g., vendors, cybersecurity service providers, team members, etc.) with access to the candidate tools for the duration of the technical evaluation. It is up to the discretion of the steering committee to determine which methods of access into the site are preferred / required ● Before proceeding with the technical evaluation phase, verify if the selected site has an asset inventory and a network diagram. If an asset inventory is not available, work with your on-site operations team to develop one, by documenting all the known network-connected assets and the attributes you are interested in tracking. Without an asset inventory, you cannot validate the performance of the tools during the technical evaluation, since you do not have a source of truth for comparison. Constructing a high-level network diagram (if not available) can also help the vendors better understand the current state of your network

Phase #	Phase Title	Key Activity	Comments on Best Practices
4	Site Identification	• Engage the shortlisted vendors to obtain the relevant appliances or agents / software, providing them with the details of the identified site, including: ○ Any specific site constraints ○ Proof-of-concept schedule ○ Site documentation (asset inventory, network diagram)	• Depending on the type(s) of monitoring and the type of deployment being evaluated, a candidate vendor might require a few days up to a few weeks to provide you with the relevant appliance or agent / software (the upper end of this range is typically for physical appliances, which also need to be configured based on your network set-up). Provide the site details as early as possible to avoid any delays and / or conflict with your proof-of-concept schedule • To ensure a comprehensive technical evaluation of the shortlisted vendors, the duration of the proof of concept should be between 2 - 4 weeks, depending on the downtime window and availability of the on-site team. At a minimum, the first week of the proof of concept should be scheduled for the deployment of the tools and the discovery of the network-connected assets, while the final week should involve conducting controlled changes in the environment as well as the scoring of the tools. A longer duration for the proof of concept can provide the tools with more data, potentially improving their performance
5	Success Criteria Development	• Break down your technical requirements into technical areas, which are the most basic and quantifiable components of your technical evaluation: ○ ***Example:*** asset detection ○ ***Example:*** asset identification ○ ***Example:*** configuration change detection ○ ***Example:*** integrations ○ ***Example:*** targeted active scanning ○ ***Example:*** threat detection ○ ***Example:*** user experience ○ ***Example:*** vulnerability detection	• Technical areas are used to quantify and compare the performance of OT monitoring tools, enabling you to identify the vendor that is most compatible with your sites and needs. It is up to the discretion of the steering committee to determine the technical areas it wishes to evaluate • Key functionalities, previously identified, can also be used to derive technical areas; however, since they are less granular than technical requirements and do not incorporate your sites' constraints, they should mostly be used as a secondary source • The technical areas exemplified here are based on the technical requirements and the key functionalities of the hypothetical steering committee, presented earlier in this guide: ○ The first technical requirement (TR-1) is addressed by threat detection, while the second technical requirement (TR-2) is broken down into asset detection and asset identification. It is recommended to evaluate the detection of assets and the identification of attributes separately, as the latter is dependent on

Phase #	Phase Title	Key Activity	Comments on Best Practices
5	Success Criteria Development	****Continued****	the former and is also an indicator of how well an OT tool dissects protocols / data to extract attributes. The third technical requirement (TR-3) is addressed by targeted active scanning ○ The key functionality for configuration management is addressed by configuration change detection, while that for vulnerability management is addressed by vulnerability detection ○ As a reminder, this committee has a preference for network-based monitoring, to be augmented with targeted active scanning. Therefore, integrations in this case refers to the export of data from the OT monitoring tool into other third party platforms, and not vice versa (i.e., integration-based monitoring is not in scope) ○ Although user experience is not associated with a specific technical requirement or a key functionality, it should be used in every proof of concept to assess the usability of the candidate tools ○ The key functionality for incident response, which is the steering committee's lowest cybersecurity priority, can be addressed as a functional feature in user experience (exemplified later in this phase)
		● By referring to your technical requirements, set up the definition of each technical area: ○ ***Example:*** asset detection - tool must detect network-connected assets ○ ***Example:*** asset identification - tool must identify specific attributes of the detected assets ○ ***Example:*** configuration change detection - tool must detect configuration changes on the detected assets ○ ***Example:*** integrations - tool must integrate with specific third party tools ○ ***Example:*** targeted active scanning - tool must conduct targeted active scanning on the detected assets ○ ***Example:*** threat detection - tool must detect anomalous network behavior and attack signatures ○ ***Example:*** user experience - too must provide specific functional features ○ ***Example:*** vulnerability detection - tool must detect CVEs associated with the network-connected assets	● Technical areas should be defined in a clear and concise manner, highlighting a specific metric that needs to be evaluated during the proof of concept (e.g., network-connected assets, attributes, configuration changes, etc.)
		● Where applicable, segregate your technical areas into IT and OT: ○ ***Example:*** IT asset detection - tool must detect network-connected IT assets ○ ***Example:*** OT asset detection - tool must detect network-connected OT assets ○ ***Example:*** IT asset identification - tool must identify specific attributes of the detected IT assets ○ ***Example:*** OT asset identification - tool must identify specific attributes of the detected OT assets ○ ***Example:*** IT configuration change detection - tool must detect configuration changes on the detected IT assets ○ ***Example:*** OT configuration change detection - tool must detect configuration changes on the detected OT assets ○ ***Example:*** integrations - tool must integrate with specific third party tools	● By segregating technical areas into IT and OT, the steering committee can analyze the strengths and limitations of the tools with respect to each type of endpoints ● Additionally, if the steering committee has a higher priority in securing certain types of endpoints, it can assign higher weights to the relevant technical areas when calculating the overall score for each tool. For example, since this hypothetical committee has a higher priority in

Phase #	Phase Title	Key Activity	Comments on Best Practices
5	Success Criteria Development	○ ***Example:*** IT targeted active scanning - tool must conduct targeted active scanning on the detected IT assets ○ ***Example:*** OT targeted active scanning - tool must conduct targeted active scanning on the detected OT assets ○ ***Example:*** threat detection - tool must detect anomalous network behavior and attack signatures ○ ***Example:*** user experience - tool must provide specific product features ○ ***Example:*** IT vulnerability detection - tool must detect CVEs associated with the network-connected IT assets ○ ***Example:*** OT vulnerability detection - tool must detect CVEs associated with the network-connected OT assets	securing certain types of endpoints, it can assign higher weights to the relevant technical areas when calculating the overall score for each tool. For example, since this hypothetical committee has a higher priority in identifying the attributes of its OT-type endpoints over its IT-type endpoints, a higher weight can be assigned to both OT asset detection and identification (exemplified later in the phase)
		● Determine the evaluation methodology of each technical area: ○ ***Example:*** IT asset detection - use the site's asset inventory to validate which IT assets are detected by each tool ○ ***Example:*** OT asset detection - use the site's asset inventory to validate which OT assets are detected by each tool ○ ***Example:*** IT asset identification - use the site's asset inventory to validate which attributes of the detected IT assets are identified correctly by each tool ○ ***Example:*** OT asset identification - use the site's asset inventory to validate which attributes of the detected OT assets are identified correctly by each tool ○ ***Example:*** IT configuration change detection - conduct specific configuration changes on a sample of the detected IT assets; validate which changes are detected by each tool ○ ***Example:*** OT configuration change detection - conduct specific configuration changes on a sample of the detected OT assets; validate which changes are detected by each tool ○ ***Example:*** integrations - develop a list of third party tools with which you require out-of-the-box integrations; validate the list with each vendor ○ ***Example:*** IT targeted active scanning - using each tool, conduct targeted active scanning on a sample of the detected IT assets; validate what additional attributes are identified correctly ○ ***Example:*** OT targeted active scanning - using each tool, conduct targeted active scanning on a sample of the detected OT assets; validate what additional attributes are identified correctly ○ ***Example:*** threat detection - conduct specific network-related changes and / or specific attack simulations; validate which threat scenarios are detected by each tool; use a list of questions to determine the quality of threat detection ○ ***Example:*** user experience - use a list of questions to determine if the functional features you require are present in each tool ○ ***Example:*** IT vulnerability detection - use the site's asset inventory to research which IT assets have CVEs; validate if the CVEs are detected by each tool; use a list of questions to determine the quality of vulnerability detection ○ ***Example:*** OT vulnerability detection - use the site's asset inventory to research which OT assets have CVEs; validate if the CVEs are detected by each tool; use a list of questions to determine the quality of vulnerability detection	● It is up to the discretion of the steering committee to determine the evaluation methodology of each technical area, depending on the metric it has defined. The examples provided in this key activity detail the most common methodologies that can be utilized ● To accurately score asset detection, asset identification, and vulnerability detection, the site's asset inventory should be used as the source of truth. If a complete inventory is not available, ensure that you develop one beforehand. Although this might seem counterproductive, since OT monitoring tools are intended to generate an inventory, without a source of truth, you cannot have an accurate benchmark to evaluate the tools with ● Although asset detection is evaluated with respect to the site's entire asset inventory (i.e., known network-connected assets), asset identification should focus on the attributes of the detected assets only - this is because, if a tool does not detect an asset, you cannot deduce the tool's ability in dissecting and interpreting the protocols / data of that asset ● For vulnerability detection, leverage the OS, firmware version, or model of the known assets in your asset inventory to identify any CVEs beforehand. Validate your findings with the CVEs detected by the OT monitoring tools. It is important to note that if a tool does not detect an asset in general, and the OS, firmware version, or model in particular, it cannot detect its CVEs. However, it is recommended to evaluate this technical area with respect to every network-connected asset with known CVEs and not just the assets detected by the tools (this is because, vulnerability detection, compared to asset identification, should be more focused on minimizing potential risks in your environment)

Phase #	Phase Title	Key Activity	Comments on Best Practices
5	Success Criteria Development	****Continued****	• Configuration change detection, targeted active scanning, and threat detection involve controlled changes in the environment, which may require change management approval beforehand. To evaluate each of these technical areas, examine the net change in a tool's output by comparing what the tool detects before and after the controlled change • Since threat detection and vulnerability detection play an important role in threat remediation and threat prevention, respectively, they should be evaluated not just for detecting a threat / CVE but also for the quality of the detection and its usefulness - using a list of questions can help measure that • User experience can be measured through a variety of different methods; however, in this example, the evaluation methodology focuses on functional features only, presented through a list of questions
		• Elaborate the evaluation methodologies which require more details: ○ ***Example:*** IT asset identification - the following attributes are to be evaluated for each detected IT asset: ■ Asset class ■ Asset type ■ Vendor ■ OS ■ OS build version ■ Protocols used ○ ***Example:*** OT asset identification - the following attributes are to be evaluated for each detected OT asset: ■ Asset class ■ Asset type ■ Vendor ■ Model ■ Firmware version ■ Serial number ■ Protocols used ○ ***Example:*** IT configuration change detection - each of the following changes are to be conducted on a sample (3) of detected IT assets: ■ Enable AutoPlay of removable devices (Windows machine) ■ Enable Remote Registry service (Windows machine)	• For asset identification, evaluate the tools against the attributes that you defined in your technical requirements. Ensure that your site's asset inventory contains the most up-to-date attributes of your network-connected assets - without this, you cannot validate the accuracy of each candidate tool • Configuration changes, whether on IT-type endpoints or OT-type endpoints, should be conducted on a sample of assets (ideally 3), ensuring sufficient data collection. It is up to the discretion of the steering committee to determine what configuration changes to evaluate for. When conducting configuration changes in a production environment, leverage testing equipment if possible, otherwise, conduct any changes on non-critical assets only. Another strategy is to add testing equipment to the network, as long as it does not interfere with the existing network-connected assets. Any configuration changes should be conducted directly by the on-site operations team. In this hypothetical example, where the steering committee is evaluating network-based monitoring (passive mode), it is highly unlikely that the IT configuration changes will be detected, especially since they will be conducted locally on each individual

Phase #	Phase Title	Key Activity	Comments on Best Practices
5	Success Criteria Development	■ Disable local firewall (Windows machine) ○ ***Example:*** OT configuration change detection - the following changes are to be conducted on a sample (3) of detected OT assets: ■ Switch PLC from Run to Program mode ■ Add a new contact to the PLC's program ○ ***Example:*** integrations - the following out-of-the-box integrations are to be evaluated: ■ Active Directory ■ IBM QRadar ■ Palo Alto Networks NGFW ■ ServiceNow ○ ***Example:*** IT targeted active scanning - each of the following targeted active scans are to be conducted on a sample (3) of detected IT assets: ■ SNMP poll (Windows machine) ■ WMI poll (Windows machine) ○ ***Example:*** OT targeted active scanning - each of the following targeted active scans are to be conducted on a sample (3) of detected OT assets: ■ S7Comm poll (SIMATIC S7-300 PLC) ■ S7CommPlus poll (SIMATIC S7-1200, SIMATIC S7-1500 PLCs) ○ ***Example:*** threat detection - the following threat scenarios are to be simulated in the network: ■ Add a new IT asset to the network ■ Force a new communication between the added IT asset and a PLC ■ Force a new activity between a PLC and an OT field asset ■ Set up a simulator testbed in the network, enabling pentesting activities on a soft PLC Additionally, the following questions are to be used to evaluate each threat scenario: ■ Does the tool detect the threat? ■ Does the tool classify the threat as a medium severity or above? ■ Does the tool provide an accurate description of the threat? ■ Does the tool provide an accurate network visualization of the threat? ■ Does the tool leverage relevant indicators of compromise to detect the threat (if applicable to the scenario)? ○ ***Example:*** user experience - the following questions are to be used to evaluate user experience: ■ Does the tool support home dashboard customization? ■ Does the tool present the asset database in a way that is easy to visualize and navigate? ■ Does the tool permit easy zone configuration? ■ Does the network graph provide a Purdue model mapping in addition to the network topology? ■ Does the tool support network graph customization? ■ Does the tool present vulnerabilities in a way that is easy to visualize and prioritize? ■ Does the tool logically group the types of alerts for easy visualization? ■ Does the tool support report customization?	endpoint. On the other hand, OT configuration changes are typically executed using programming software on a workstation; therefore, changes can be detected since the associated traffic will traverse the network. When conducting configuration changes on OT-type endpoints, ensure that there is no disruption to the site's operations. For instance, depending on the manufacturer and model of the PLC, switching from Run to Program mode as well as adding a new contact to the program (online if possible) may not pose a risk of disruption (i.e., PLC will not require to be stopped, existing program will not be affected). Therefore, it is important to collaborate with the on-site operations team to validate what types of changes they are comfortable in conducting on their testing / non-critical equipment ● The list of out-of-the-box integrations can be as extensive as required, depending on the steering committee's desired use-cases and current capabilities. Based on the examples provided for this hypothetical committee, the following use-cases can be set up: ○ Active Directory: import users / groups from your directory service, facilitating user management in the OT monitoring tool ○ IBM QRadar: forward alerts, associated with both assets and threats, from the OT monitoring tool to your SIEM platform, enabling centralized security monitoring and event correlation ○ Palo Alto Network NFGW: forward alerts and policies from the OT monitoring tool to your firewalls, enabling automated enforcement ○ ServiceNow: integrate the attributes of the detected assets into your configuration management database, providing a centralized view of your configuration items ● Similar to configuration changes, targeted active scans, whether on IT-type endpoints or OT-type endpoints, should be conducted on a sample of compatible assets (ideally 3). Targeted active scans are limited by the type of device and / or protocol that the OT monitoring vendor can support. In this case, two common examples are provided for the targeted active scanning of IT-type endpoints, specifically Windows machines (typically found in OT environments). For OT-type endpoints, specifically PLCs or other types of controllers, targeted active scans are usually based on the native protocol of the targeted endpoint, which in this hypothetical example is the S7Comm protocol

Phase #	Phase Title	Key Activity	Comments on Best Practices
5	Success Criteria Development	○ ***Example:*** IT vulnerability detection - the following questions are to be used to evaluate each IT asset with known CVEs: ■ Does the tool detect the known CVEs? ■ Does the tool augment the CVSS base score with temporal and / or environmental metrics? ■ Does the tool support custom scoring? ■ Does the tool present relevant remediation guidance? ○ ***Example:*** OT vulnerability detection - the following questions are to be used to evaluate each OT asset with known CVEs: ■ Does the tool detect the known CVEs? ■ Does the tool augment the CVSS base score with temporal and / or environmental metrics? ■ Does the tool support custom scoring? ■ Does the tool present relevant remediation guidance?	for the SIMATIC S7-300 PLCs and S7CommPlus protocol for the SIMATIC S7-1200 and S7-1500 PLCs. When conducting targeted active scans on OT-type endpoints, target non-legacy equipment only (to avoid any potential disruptions) ● Threat detection scenarios should be conducted in collaboration with, or on behalf of, the on-site operations team. The first two scenarios, exemplified here, should not pose any risk to the environment or its processes, if conducted correctly (the new communication between the added IT asset and the PLC can be something as simple as accessing the PLC's web server). The third scenario, which involves a new activity that has not yet been observed by the OT monitoring tool, should be conducted on non-critical PLCs only (e.g., resetting a sensor or an input to the PLC). Setting up a testbed, whether a physical or simulated one, enables you to conduct pentesting activities while assessing the tools' capabilities in detecting threats. In this case, a simulator testbed is suggested, which allows you to simulate a PLC / process that can be comparable to existing processes in your environment (refer to Appendix A for a possible set-up). The steering committee should determine the questions that best evaluate the usefulness of the detected alerts ● As previously mentioned, user experience is assessed through a series of questions that covers various functional features, required for the operations of the OT monitoring tool. It is up to the discretion of the steering committee to modify this list as it sees fit ● For vulnerability detection, in addition to comparing your findings with those of the OT monitoring tool, utilize a list of questions to evaluate the quality of the detection and its usefulness

Phase #	Phase Title	Key Activity	Comments on Best Practices
5	Success Criteria Development	● Determine the scoring methodology of each technical area: ○ ***Example:*** IT asset detection is scored for each tool using the following formula: $$\frac{\#\ of\ detected\ IT\ assets}{\#\ of\ known\ IT\ assets\ in\ the\ site} \times 100$$ ○ ***Example:*** OT asset detection is scored for each tool using the following formula: $$\frac{\#\ of\ detected\ OT\ assets}{\#\ of\ known\ OT\ assets\ in\ the\ site} \times 100$$ ○ ***Example:*** IT asset identification is scored for each tool using the following formula: $$\frac{\Sigma\left(\frac{\#\ of\ attributes\ identified\ correctly\ for\ each\ detected\ IT\ asset}{\#\ of\ attributes\ being\ evaluated\ for\ each\ detected\ IT\ asset}\right)}{\#\ of\ detected\ IT\ assets} \times 100$$ ○ ***Example:*** OT asset identification is scored for each tool using the following formula: $$\frac{\Sigma\left(\frac{\#\ of\ attributes\ identified\ correctly\ for\ each\ detected\ OT\ asset}{\#\ of\ attributes\ being\ evaluated\ for\ each\ detected\ OT\ asset}\right)}{\#\ of\ detected\ OT\ assets} \times 100$$ ○ ***Example:*** IT configuration change detection is scored for each tool using the following formula: $$\frac{\Sigma\left(\frac{\#\ of\ configuration\ changes\ detected\ on\ each\ sampled\ IT\ asset}{\#\ of\ configuration\ changes\ conducted\ on\ each\ \ sampled\ IT\ asset}\right)}{\#\ of\ sampled\ IT\ assets} \times 100$$	● The scoring methodology of each technical area should detail the formula that results in a metric, expressed as a percentage. It is up to the steering committee to devise its formulas based on the evaluation methodologies previously developed ● For asset detection, the output of the formula is the percentage of assets that are detected with respect to the total number of known network-connected assets ● For asset identification, the output of the formula is the percentage of attributes that are identified correctly across all detected assets ● For configuration change detection, the output of the formula is the percentage of configuration changes that are detected across all sampled assets

Phase #	Phase Title	Key Activity	Comments on Best Practices
5	Success Criteria Development	○ ***Example:*** OT configuration change detection is scored for each tool using the following formula: $$\frac{\Sigma\left(\frac{\#\ of\ configuration\ changes\ detected\ on\ each\ sampled\ OT\ asset}{\#\ of\ configuration\ changes\ conducted\ on\ each\ sampled\ OT\ asset}\right)}{\#\ of\ sampled\ OT\ assets} \times 100$$ ○ ***Example:*** integrations is scored for each tool using the following formula: $$\frac{\#\ of\ out{-}of{-}the{-}box\ integrations\ supported}{\#\ of\ out{-}of{-}the{-}box\ integrations\ required} \times 100$$ ○ ***Example:*** IT targeted active scanning is scored for each tool using the following formula: $$\frac{\Sigma\left(\frac{\#\ of\ additional\ attributes\ identified\ correctly\ for\ each\ sampled\ IT\ asset}{\#\ of\ attributes\ previously\ missing\ for\ each\ sampled\ IT\ asset}\right)}{\#\ of\ sampled\ IT\ assets} \times 100$$ ○ ***Example:*** OT targeted active scanning is scored for each tool using the following formula: $$\frac{\Sigma\left(\frac{\#\ of\ additional\ attributes\ identified\ correctly\ for\ each\ sampled\ OT\ asset}{\#\ of\ attributes\ previously\ missing\ for\ each\ sampled\ OT\ asset}\right)}{\#\ of\ sampled\ OT\ assets} \times 100$$ ○ ***Example:*** threat detection is scored for each tool using the following formula: $$\frac{\Sigma\left(\frac{\#\ of\ questions\ answered\ correctly\ for\ each\ threat\ scenario}{\#\ of\ questions\ being\ evaluated\ for\ each\ threat\ scenario}\right)}{\#\ of\ threat\ scenarios} \times 100$$ ○ ***Example:*** user experience is scored for each tool using the following formula: $$\frac{\#\ of\ questions\ answered\ correctly}{\#\ of\ questions\ being\ evaluated\ for\ functional\ features} \times 100$$	• For integrations, the output of the formula is the percentage of out-of-the-box integrations that are supported with respect to the total number of integrations required • For targeted active scanning, the output of the formula is the percentage of additional attributes that are identified correctly across all sampled assets • For threat detection, the output of the formula is the percentage of questions that are answered correctly across all simulated threat scenarios • For user experience, the output of the formula is the percentage of questions that are answered correctly, corresponding to the functional features that are supported

Phase #	Phase Title	Key Activity	Comments on Best Practices
5	Success Criteria Development	○ ***Example:*** IT vulnerability detection is scored for each tool using the following formula: $$\frac{\Sigma\left(\frac{\#\ of\ questions\ answered\ correctly\ for\ each\ IT\ asset\ with\ known\ CVEs}{\#\ of\ questions\ being\ evaluated\ for\ each\ IT\ asset\ with\ known\ CVEs}\right)}{\#\ of\ IT\ assets\ with\ known\ CVEs} \times 100$$ ○ ***Example:*** OT vulnerability detection is scored for each tool using the following formula: $$\frac{\Sigma\left(\frac{\#\ of\ questions\ answered\ correctly\ for\ each\ OT\ asset\ with\ known\ CVEs}{\#\ of\ questions\ being\ evaluated\ for\ each\ OT\ asset\ with\ known\ CVEs}\right)}{\#\ of\ OT\ assets\ with\ known\ CVEs} \times 100$$	● For vulnerability detection, the output of the formula is the percentage of questions that are answered correctly across all assets with known CVEs
		● Determine the success range for evaluating the technical areas: ○ ***Example:*** does not meet expectations - any technical area with a score < 25% ○ ***Example:*** partially meets expectations - any technical area with a score >= 25% and <70% ○ ***Example:*** fully meets expectations - any technical area with a score >= 70%	● Based on its expectations, the steering committee should determine a success range and apply it across every technical area, ensuring consistency in the reporting of the results
		● Based on perceived priority, assign weights (out of 100%) to each technical area: ○ ***Example:*** IT asset detection - 10% ○ ***Example:*** OT asset detection - 15% ○ ***Example:*** IT asset identification - 10% ○ ***Example:*** OT asset identification - 15% ○ ***Example:*** IT configuration change detection - 5% ○ ***Example:*** OT configuration change detection - 5% ○ ***Example:*** integrations - 5% ○ ***Example:*** IT targeted active scanning - 5% ○ ***Example:*** OT targeted active scanning - 5% ○ ***Example:*** threat detection - 10% ○ ***Example:*** user experience - 5% ○ ***Example:*** IT vulnerability detection - 5% ○ ***Example:*** OT vulnerability detection - 5%	● When calculating the overall score of a candidate tool, each technical area should be assigned a weight (out of 100%) that represents your perceived priority. It is up to the discretion of the steering committee to set up the weight distribution as it sees fit ● In this hypothetical example, as a reminder, the steering committee has asset management as its highest cybersecurity priority, followed by threat detection, vulnerability management, configuration management, and incident response. Additionally, the committee prioritizes the attributes of its OT-type endpoints over its IT-type endpoints. Putting all of this together, the steering committee assigns the highest weights to OT asset detection and identification (each at 15%), followed by IT asset detection, IT asset identification, and threat detection (each at 10%), while the remaining technical areas are assigned the lowest weights (each at 5%)
		● Using your preferred spreadsheet software program, set up a separate sheet for each technical area based on its evaluation and scoring methodologies. Additionally, set up a separate sheet to calculate the overall score of each candidate tool, taking the weight distribution from the previous activity into account	● The spreadsheet for each technical area should be structured according to its evaluation methodology, defined earlier in this phase. Appendices B and C exemplify how to set up the technical areas for

Phase #	Phase Title	Key Activity	Comments on Best Practices
5	Success Criteria Development	****Continued****	IT asset identification and IT vulnerability detection, respectively, using a hypothetical tool A. At this stage, only the following information needs to be populated into the spreadsheets: ○ Source-of-truth information (e.g., known network-connected assets, required attributes for evaluation, assets with expected CVEs, etc.) ○ Planned controlled changes (e.g., configuration changes, targeted active scans, threat scenarios) ○ List of questions identified earlier ● Additionally, in each spreadsheet, set up the applicable formulas in the relevant cells, following the scoring methodology that you devised for each technical area ● The spreadsheet for the overall scores should reference the results of each technical area while taking the weight distribution into account. Appendix D exemplifies how this can be set up
6	Technical Evaluation	● Ensure that all the implementation prerequisites identified earlier are completed: ○ ***Example:*** change management approval is obtained ○ ***Example:*** rack space is made available ○ ***Example:*** power supply is made available ○ ***Example:*** core network switch is configured for port mirroring ○ ***Example:*** a field laptop is set up to manage the monitoring tools ○ ***Example:*** physical appliances are obtained from the vendors	● Implementation prerequisites, identified earlier in collaboration with the on-site operations team and the candidate vendors, should be completed before setting up the OT monitoring tools ● As previously mentioned, these prerequisites depend on your site's constraints, type(s) of monitoring being evaluated, and type of deployment being used ● In this hypothetical example, a few implementation prerequisites are listed for the installation of physical, network-based appliances
		● Provide the on-site operations team with an overview of the controlled changes that need to be conducted: ○ ***Example:*** configuration changes on a sample of detected IT assets ○ ***Example:*** configuration changes on a sample of detected OT assets ○ ***Example:*** targeted active scanning on a sample of detected IT assets ○ ***Example:*** targeted active scanning on a sample of detected OT assets ○ ***Example:*** simulation of threat scenarios	● All controlled changes that are required in the environment during the technical evaluation, including configuration changes, targeted active scans, and threat simulations, should be documented and socialized with the on-site operations team beforehand ● At this stage, since the monitoring tools are not yet deployed, it is impossible to know which assets will be detected by each tool, and therefore the samples for the controlled changes cannot yet be determined. The purpose of this key activity is to align with the operations team on the nature of the controlled changes and initiate

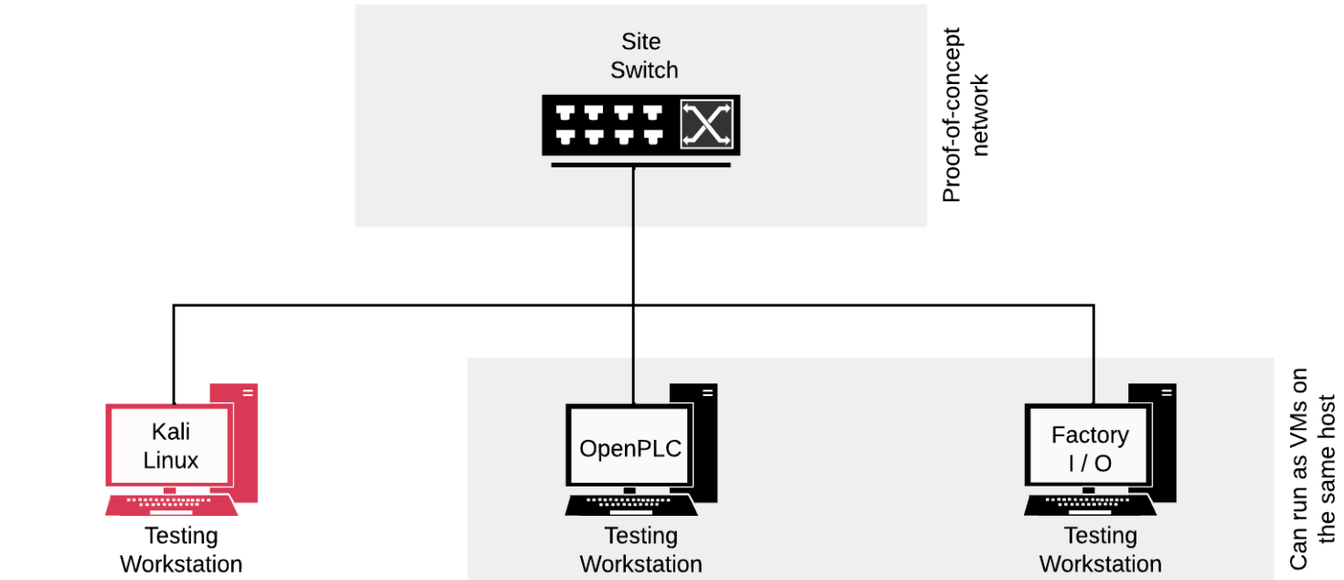
Phase #	Phase Title	Key Activity	Comments on Best Practices
6	Technical Evaluation	****Continued****	the required changement management approval process, if needed
		• Provide on-site physical access to the relevant parties, following your organization's safety policies and procedures (if applicable)	• As indicated earlier, if the steering committee has determined that a specific party (e.g., cybersecurity service provider / system integrator, cybersecurity team member, etc.) needs to be at the site for the duration of the technical evaluation, they need to be provided with access, following your organization's safety policies and procedures
		• Work with the on-site operations team as well as the vendors to set up the candidate tools (if applicable: tools should be set to learning mode)	• Whether on-site or remotely, the steering committee should collaborate with the operations team to set up the candidate tools. Depending on the type(s) of monitoring and the type of deployment being evaluated, this might require the installation of a physical appliance, the set-up of a virtual appliance, or the installation of an agent / software. Involve the candidate vendors during this key activity to ensure a smooth deployment process
		• Provision secure remote access to the relevant parties, following your organization's cybersecurity policies (if applicable)	• If the steering committee has determined that a specific party (e.g., cybersecurity service provider / system integrator, vendor, etc.) requires remote access to the tools for the duration of the technical evaluation, ensure that it is provisioned in a secure way, following your organization's cybersecurity policies
		• Update the site's network diagram with the proof-of-concept set-up	• An updated network diagram, with the details of the proof-of-concept set-up, provides a visual representation to the on-site operations team as well as to the vendors - this can be beneficial for troubleshooting, if needed
		• Conduct a recurring check-in on the performance of the candidate tools, ensuring that they are operating as intended	• As a reminder, the duration of the proof of concept should be set between 2 - 4 weeks, with the first week being dedicated for the deployment of the tools and the discovery of the network-connected assets, while the final week is for conducting controlled changes in the environment and for scoring the tools. Recurring check-ins, either on-site or remotely, should be conducted at least once a week during the technical evaluation, ensuring that the tools are ingesting data and operating as intended

Phase #	Phase Title	Key Activity	Comments on Best Practices
6	Technical Evaluation	• During the final week of the evaluation, conduct the controlled changes in the environment (if applicable: tools should be set to detection mode)	• At this stage, since the monitoring tools have had the opportunity to detect assets, you can determine which samples to conduct the controlled changes on • Controlled changes, developed in the earlier phase, should be conducted by, or in collaboration with, the on-site operations team. These changes may include: ○ Configuration changes ○ Targeted active scans ○ Simulation of threat scenarios • Depending on the type of monitoring being evaluated (network-based monitoring and / or host-based monitoring), ensure that the tools are set in detection mode to allow the appropriate alerting
		• Score each candidate tool, following the evaluation and scoring methodologies of each technical area	• During the final week of the technical evaluation, score the technical areas for each candidate tool, following your evaluation and scoring methodologies. It is recommended to score each controlled change immediately after conducting it. Appendices E and F exemplify the scoring of IT asset identification and IT vulnerability detection, respectively (based on the hypothetical example from the previous phase) • The spreadsheet for the overall scores should automatically calculate the final results of the candidate tools, given that each technical area is being referenced correctly. Appendix G exemplifies this for the hypothetical tool A
7	Financial Evaluation	• Ensure that the quotes provided by the candidate vendors cover the various line items that you require (e.g., product, licensing, annual support, training, professional / deployment services, etc.)	• It is important for the steering committee to determine if and how its requested line items are addressed in each quote. For instance, many vendors provide annual support as part of their licensing, while a few list it as a separate line item. Clarify any concerns with the vendors and ensure that the quotes are comparable in terms of what they cover. Classifying each line item under capital or operational expenditure can also facilitate the price scoring, especially if the committee has a preference for one type of expenditure over the other

Phase #	Phase Title	Key Activity	Comments on Best Practices
7	Financial Evaluation	• Ensure that the quoted products align with your business and technical requirements. Additionally, ensure that the designs put forward are comparable with one another, to the extent that is possible	• When evaluating quoted products, reference your business and technical requirements, ensuring that your needs and sites' constraints are addressed. Some vendors may provide add-ons, which may or may not align with your requirements • An important aspect of evaluating the vendors' proposed products and quotes is to understand the designs that are put forward. For example, a vendor might propose a design that may require fewer appliances and / or licenses, hence that vendor's pricing may be significantly lower - it is important to validate if the other vendors can propose a similar design, allowing for a fairer price comparison. In some instances, due to differences in the type(s) of monitoring being considered or in a vendor's unique offering, the proposed designs cannot be comparable • A suggested approach that can facilitate this key activity is to require the vendors to map their quoted products to your list of classified sites as well as to your network diagrams - this can provide a better understanding of the design and products that each vendor is proposing
		• Follow your organization's procurement guidelines to score the pricing from each candidate vendor	• Based on your organization's procurement guidelines, utilize a methodology for scoring the vendors' quotes (this is typically conducted by procurement)
8	Wrap-Up & Transition	• Uninstall / remove the deployed tools and coordinate their return to the vendors (if applicable)	• In collaboration with the on-site operations team, uninstall / remove the deployed tools, following the instructions provided by the vendors
		• Revert any changes that were conducted in your network in general, and on your network-connected assets in particular	• Any changes that were conducted in the proof-of-concept site should be reverted back, ensuring that no potential disruptors are left behind (whether in the network or on sampled assets). Documenting and tracking controlled changes in the technical evaluation phase can facilitate this key activity
		• If an RFP was issued, finalize the scoring of the shortlisted vendors using the technical and financial evaluations; identify the candidate vendor with the highest overall score. If an RFP was not issued, utilize the results of the technical and financial evaluations to score the candidate vendors	• Depending on the structure of the RFP and its overall scoring criteria, incorporate the results of the technical and financial evaluations to calculate the final score of each candidate vendor

Phase #	Phase Title	Key Activity	Comments on Best Practices
8	Wrap-Up & Transition	****Continued****	• If an RFP was not issued, utilize the results of the technical and financial evaluations to score each candidate vendor - it is up to the steering committee to determine the weight (out of 100%) of each of these evaluations based on the perceived priority (i.e., importance of functionality vs. price in the overall selection of the tool)
		• Update your business case document, describing your vendor selection process and highlighting the overall score of each candidate vendor. Additionally, document key findings, mapping them back to your risk management framework / threat model	• To demonstrate due diligence from a procurement / engineering perspective and to preserve evidence of the project, it is important for the steering committee to document its vendor selection process. Some of the important details that should be included are: ○ The various types of evaluations that were conducted (i.e., technical, financial, other scoring criteria if an RFP was issued) ○ A summary of the technical evaluation process, including the technical areas that were evaluated, the success range and weight distribution that were applied, and the final results of the proof of concept ○ The selected vendor based on the overall scores • Additionally, any key findings from the technical evaluation should be documented in the business case (e.g., number of unmanaged assets detected, number of end-of-life assets detected, number of critical vulnerabilities detected, major misconfigurations detected in the network and / or on assets, suspicious / unexpected communication in the network, etc.). To exhibit a stronger case for OT monitoring, map your key findings to your risk management framework / threat model. If, for example, your organization utilizes a cyber threat model that includes a threat event describing the exploitation of OS vulnerabilities, you can tie in the number of critical CVEs that were detected during the proof of concept (or perhaps the number of detected IT assets with an end-of-life OS)
		• Socialize your business case document with the relevant stakeholders	• Utilize the business case to onboard any additional stakeholders to your vision for an OT cyber monitoring program. As a reminder, OT cyber monitoring is a multi-departmental journey - selecting a suitable tool using a methodical yet collaborative way is its critical starting point

Appendix A: possible set-up of a simulator testbed, enabling you to conduct pentesting activities on a PLC / process that is relevant to your environment



This testing workstation can be used to simulate attacks on the simulator testbed, which comprises a soft PLC (simulated via OpenPLC or other products) and a virtual facility set-up (simulated via Factory I / O). Depending on the pentesting activities that your organization typically conducts, leverage the security tools that you see fit. Common Kali Linux tools (e.g., LOIC, Metasploit, Nmap) can provide enough flexibility to simulate threat scenarios on your simulator testbed (e.g., eavesdropping, injection attacks, DoS attacks, etc.)

OpenPLC is an open-source platform that can simulate a PLC, including its programming, internal processes, and network communication. It supports 5 different programming languages, adhering to IEC 61131-3. Despite its limited support of OT protocols (Modbus, DNP3), OpenPLC can be deployed on a variety of different hardware and is ideal to simulate threats on, without risking your production environment / equipment. Other platforms are also available in the market, some of which are offered by PLC manufacturers

Factory I / O is a software that can simulate industrial automation systems and processes, enabling users to set up and design virtual facilities. Using its built-in I / O drivers, the software can communicate with external PLCs (both physical and software-based) as well as broader, vendor-agnostic technologies. By integrating your OpenPLC program with a virtual set-up in Factory I / O, you can simulate the network communication and interaction between a PLC and field devices (although this may be limited to a Modbus / TCP simulation)

Appendix B: spreadsheet set-up for IT asset identification (for a hypothetical tool A). Since the technical evaluation has not yet commenced, the detected IT assets for tool A are unknown. The table below is only a partial representation; a separate table is required for each candidate tool in the same spreadsheet

Detected IT Assets			IT Asset Identification | Tool A						
Asset ID	Asset IP Address	Asset Function	Asset Class	Asset Type	Vendor	OS	OS Build Version	Protocols Used	Score

$$\text{Formula in each gray cell} = \frac{\#\ of\ attributes\ identified\ correctly\ for\ each\ detected\ IT\ asset}{6} \times 100$$

Appendix C: spreadsheet set-up for IT vulnerability detection (for a hypothetical tool A). Based on prior research, the committee identifies that the assets below are associated with multiple CVEs. The table below is only a partial representation; a separate table is required for each candidate tool in the same spreadsheet

IT Assets with Known CVEs			IT Vulnerability Detection | Tool A				
Asset ID	Asset IP Address	Asset Function	Does the tool detect the known CVEs?	Does the tool augment the CVSS base score with temporal and / or environmental metrics?	Does the tool support custom scoring?	Does the tool provide relevant remediation guidance?	Score
ID02	192.168.10.2	SCADA Client					
ID03	192.168.10.3	Workstation					

$$\text{Formula in each gray cell} = \frac{\#\ of\ questions\ answered\ correctly\ for\ each\ IT\ asset\ with\ known\ CVEs}{4} \times 100$$

Appendix D: spreadsheet set-up for the overall scores of 3 candidate vendors (hypothetical tools A, B, and C) while taking the weight distribution of the technical areas into account. The table below is only a partial representation; the remaining technical areas should be included as well

	10%	15%	10%	15%	5%	5%	
Vendor	**IT Asset Detection**	**OT Asset Detection**	**IT Asset Identification**	**OT Asset Identification**	**IT Vulnerability Detection**	**OT Vulnerability Detection**	**Overall Score**
Tool A							
Tool B							
Tool C							

Overall score (tool A) = [(*IT asset detection*) × 10%] + [(*OT asset detection*) × 15%] + [(*IT asset identification*) × 10%] + …

Appendix E: exemplification of the scoring of IT asset identification (for a hypothetical tool A). The assets below are the IT-type endpoints that were detected by tool A during the proof of concept. The table below is only a partial representation; each candidate tool needs to be scored in a similar manner based on its detected assets

Detected IT Assets			IT Asset Identification | Tool A						
Asset ID	Asset IP Address	Asset Function	Asset Class	Asset Type	Vendor	OS	OS Build Version	Protocols Used	Score
ID01	192.168.10.1	Network Switch	X	X	X			X	0.67
ID02	192.168.10.2	SCADA Client	X		X	X		X	0.67
ID03	192.168.10.3	Workstation	X	X	X	X		X	0.83

IT asset identification score (tool A) $= \frac{0.67+0.67+0.83}{3} \times 100 = 72\%$ (fully meets expectations)

Appendix F: exemplification of the scoring of IT vulnerability detection (for a hypothetical tool A).
The table below is only a partial representation; each candidate tools needs to be scored in a similar manner, using the same list of IT assets with known CVEs

IT Assets with Known CVEs			IT Vulnerability Detection | Tool A				
Asset ID	Asset IP Address	Asset Function	Does the tool detect the known CVEs?	Does the tool augment the CVSS base score with temporal and / or environmental metrics?	Does the tool support custom scoring?	Does the tool provide relevant remediation guidance?	Score
ID02	192.168.10.2	SCADA Client	X			X	0.5
ID03	192.168.10.3	Workstation	X				0.25

IT vulnerability detection score (for tool A) $= \frac{0.5+0.25}{2} \times 100 = 38\%$ (partially meets expectations)

Appendix G: exemplification of the overall scoring (for a hypothetical tool A), demonstrating the scores and weights for IT asset identification and IT vulnerability detection. The table below is only a partial representation; the remaining technical areas should be included and scored as well (to calculate the overall score for tool A)

	10%	15%	10%	15%	5%	5%	
Vendor	**IT Asset Detection**	**OT Asset Detection**	**IT Asset Identification**	**OT Asset Identification**	**IT Vulnerability Detection**	**OT Vulnerability Detection**	**Overall Score**
Tool A			**72%**		**38%**		
Tool B							
Tool C							

Overall score (tool A) = [(*IT asset detection*) × 10%] + [(*OT asset detection*) × 15%] + [72% × 10%] + …