

Request for Proposal (RFP)

Connected Asset Identification &
OT/ICS Asset Visibility Solution

For OT, ICS & IIoT Environments



THREAT
INTELLIGENCE



INDUSTRY
INSIGHTS



REGIONAL
ANALYSIS



CYBER RESILIENCE
STRATEGIES



Document Title	<i>RFP – Connected Asset Identification & OT Asset Visibility</i>
Version	<i>[Insert Version Number]</i>
Date of Issue	<i>[Insert Date]</i>
Issuing Organization	<i>[Insert Organization Name]</i>
Prepared By	<i>[Insert Department / Function]</i>
Document Classification	<i>[Insert Classification: e.g., Confidential / Internal Use Only]</i>
RFP Reference Number	<i>[Insert RFP Reference Number]</i>



Table of Contents

Table of Contents.....	3
1. Introduction	6
1.1 Purpose of This Document	6
1.2 Why Connected Asset Identification Matters in OT/ICS	6
1.3 Intended Audience.....	6
1.4 How Vendors Should Respond.....	7
2. Organization Background.....	8
2.1 Operational Environment Summary	8
2.2 Business Drivers for This Initiative	8
3. Project Overview	9
3.1 Project Goals	9
3.2 Security Objectives.....	9
3.3 Operational Objectives	9
3.4 Success Criteria	9
4. Environment Overview	11
4.1 Site Overview	11
4.2 Network Architecture	11
4.3 OT Asset Categories	11
4.4 Industrial Protocols in Use	12
4.5 Existing Monitoring and Security Capabilities	13
5. Current State Challenges	14
5.1 Visibility and Inventory Gaps.....	14
5.2 Operational Safety Constraints	14
5.3 Communication and Dependency Visibility	14
5.4 Compliance and Audit Readiness	14
5.5 Change Detection and Configuration Drift.....	15
6. Scope of Work	16
6.1 Passive Asset Discovery	16
6.2 Connected Asset Identification and Classification	16
6.3 Asset Metadata Enrichment.....	16
6.4 Communication and Dependency Mapping	16
6.5 Continuous Monitoring and Change Detection.....	16
6.6 Risk and Vulnerability Visibility	17
6.7 Inventory Normalization and Management.....	17
6.8 Multi-Site Visibility.....	17



6.9 Out of Scope	17
7. Functional Requirements	18
7.1 Passive and Agentless Discovery	18
7.2 OT Protocol Awareness and Deep Packet Inspection	18
7.3 Device Identification and Classification	19
7.4 Asset Metadata and Enrichment	20
7.5 Communication Monitoring and Flow Mapping	20
7.6 Change Detection and Alerting	21
7.7 Dashboards, Visualizations, and Reporting	21
7.8 Historical Visibility and Audit Trail	22
8. Technical Requirements	23
8.1 Deployment Architecture	23
8.2 Scalability and Performance	23
8.3 Data Management and Retention	24
8.4 Access Control and Authentication	24
8.5 Security of the Solution Itself	25
8.6 High Availability and Resilience	25
9. Security and Compliance Requirements	27
9.1 Framework Alignment	27
9.2 Operational Security Controls	27
10. Integration Requirements	29
11. Data and Reporting Requirements	31
12. Implementation and Deployment Requirements	32
12.1 Deployment Approach	32
12.2 Pilot Requirements	32
12.3 Training Requirements	33
12.4 Documentation Requirements	33
13. Vendor Experience and Qualifications	34
13.1 OT/ICS Cybersecurity Experience	34
13.2 Customer References	34
13.3 Certifications and Accreditations	35
14. Service and Support Requirements	36
14.1 Proposed SLA Summary	36
15. Evaluation Criteria	38
16. Pricing and Commercial Terms	39
16.1 Pricing Structure	39



16.2 Commercial Terms	39
17. Response Instructions for Vendors	41
17.1 Submission Deadline and Process	41
17.2 Required Response Format.....	41
17.3 Required Attachments	41
17.4 Clarification Process	42
17.5 General Conditions	42
18. Appendix.....	43
Appendix A - Glossary of Terms	43
Appendix B - Asset Inventory Template	44
Appendix C - Vendor Evaluation Scorecard	44
Appendix D - Site Questionnaire.....	45
Appendix E - Compliance Checklist Reference.....	46
Appendix F - Network Diagram Reference	46



1. Introduction

1.1 Purpose of This Document

This Request for Proposal (RFP) template has been developed to assist industrial organizations in evaluating, selecting, and procuring a Connected Asset Identification and OT/ICS Asset Visibility solution. The document provides a structured framework covering functional requirements, technical specifications, evaluation criteria, commercial expectations, and vendor qualification criteria relevant to operational technology (OT), industrial control system (ICS), and Industrial Internet of Things (IIoT) environments.

The issuing organization seeks to establish comprehensive visibility into all connected assets across its OT/ICS infrastructure - including devices, systems, communication flows, firmware versions, and network relationships - without disrupting operational continuity or compromising the safety of industrial processes.

1.2 Why Connected Asset Identification Matters in OT/ICS

Industrial environments increasingly comprise a complex and interconnected mix of legacy control systems, modern IIoT devices, engineering workstations, and IT-integrated OT networks. In this context, maintaining an accurate, continuous, and operationally safe asset inventory is a foundational cybersecurity requirement - and one of the most significant challenges facing industrial organizations today.

Without reliable connected asset identification, organizations face substantial blind spots including undetected unauthorized devices, undocumented communication paths, obsolete firmware running on critical controllers, and an inability to demonstrate asset-level compliance with frameworks such as IEC 62443, NIST SP 800-82, and sector-specific regulations.

Effective connected asset identification enables organizations to:

- Establish and continuously maintain a complete OT/ICS asset inventory.
- Identify unauthorized, rogue, or shadow OT devices across segmented networks.
- Map communication flows, dependencies, and trust relationships between assets.
- Detect changes to asset configurations, firmware, and network behavior.
- Support vulnerability assessments, risk prioritization, and incident response.
- Generate compliance evidence for audits and regulatory submissions.

1.3 Intended Audience

This RFP template is intended for use by:

- OT/ICS Security Teams and Industrial Control System Engineers responsible for defining technical requirements.



-
- Procurement and Sourcing Teams managing the vendor evaluation and commercial process.
 - IT/OT Convergence Teams overseeing network integration and cross-domain security governance.
 - Risk and Compliance Officers responsible for regulatory adherence and audit readiness.
 - Plant Managers and Operations Leadership with accountability for operational continuity.

1.4 How Vendors Should Respond

Prospective vendors are expected to respond to each section of this RFP in writing, providing clear, specific, and technically accurate information. Vendors should:

- Complete all requirement tables, clearly indicating support status (Fully Supported / Partially Supported / Not Supported / On Roadmap).
- Provide supplementary documentation, architecture diagrams, and product data sheets where applicable.
- Include relevant customer references from comparable industrial deployments.
- Clearly identify any assumptions, caveats, or conditions applicable to their responses.
- Submit responses in the format and by the deadline specified in Section 19 of this document.



2. Organization Background

Instructions: Complete the following fields to describe the issuing organization's operational profile and industrial environment. This context will enable vendors to propose appropriately scoped and calibrated solutions.

Organization Name	[Insert Organization Name]
Industry Sector	[e.g., Energy / Manufacturing / Oil & Gas / Chemicals / Pharmaceuticals / Mining / Utilities / Transportation]
Headquarters Location	[Insert Country / Region]
Number of Operational Sites	[Insert Number]
Geographic Distribution	[e.g., Single region / Multi-region / International / Global]
Approximate Total Employees	[Insert Number]
OT Security Maturity Level	[e.g., Initial / Developing / Defined / Managed / Optimizing - based on IEC 62443 or equivalent]
Applicable Regulations / Frameworks	[e.g., IEC 62443, NIST SP 800-82, NERC CIP, NIS2, CFATS, ISA/IEC, other]
Primary Contact for this RFP	[Insert Name, Role, Email, Phone]

2.1 Operational Environment Summary

[Insert a brief narrative description of the organization's OT/ICS environment. Describe the nature of operations (e.g., continuous process, batch manufacturing, discrete manufacturing), the criticality of systems involved, and any key operational constraints such as 24/7 uptime requirements, maintenance windows, or air-gapped networks.]

2.2 Business Drivers for This Initiative

Describe the primary factors driving the organization's need for a Connected Asset Identification solution. Select and customize applicable drivers below.

- Increasing regulatory and compliance requirements mandating documented OT asset inventories.
- Growing convergence between IT and OT networks increasing the attack surface.
- Incidents or near-misses attributed to unmanaged or unknown OT assets.
- Internal audit findings identifying gaps in asset visibility and tracking.
- Expansion of IIoT device deployments creating new unmanaged endpoints.
- Strategic initiative to implement a comprehensive OT security programme.

[Insert additional organization-specific business drivers as appropriate.]



3. Project Overview

3.1 Project Goals

The issuing organization seeks to procure a Connected Asset Identification and OT Asset Visibility solution that delivers the following overarching goals:

- Achieve complete, continuous, and accurate visibility into all connected assets across OT/ICS and IIoT environments.
- Identify, classify, and enrich asset records without introducing any operational risk or disruption.
- Map communication flows, network dependencies, and asset relationships across industrial network zones.
- Detect changes to asset inventory, configurations, firmware, and communication patterns in near-real-time.
- Support compliance with applicable regulatory frameworks and facilitate audit evidence generation.
- Integrate asset visibility data into broader security operations, risk management, and IT/OT governance workflows.

3.2 Security Objectives

- Eliminate unknown or unmanaged devices (shadow OT) from industrial networks.
- Identify assets running outdated, vulnerable, or unsupported firmware and software versions.
- Detect unauthorized network communications and anomalous device behavior.
- Support the development and maintenance of network segmentation policies.
- Enable risk-based prioritization of asset-level security activities.

3.3 Operational Objectives

- Maintain complete asset inventory with minimal manual effort or operational overhead.
- Ensure zero disruption to industrial processes during discovery and monitoring activities.
- Provide actionable, role-appropriate visibility for OT engineers, security analysts, and management.
- Reduce time-to-detection for asset changes, new device connections, and configuration drift.

3.4 Success Criteria



The following criteria will be used to assess the success of the deployed solution. [Issuing organization to validate and customize these criteria.]

#	Success Criterion	Target / Threshold
1	Asset discovery coverage across all in-scope OT network segments	[e.g., >95% of known assets identified within 30 days]
2	Time to establish initial baseline asset inventory	[e.g., Within [X] weeks of deployment]
3	False positive rate for newly detected / unknown assets	[e.g., <5% over a 90-day period]
4	Change detection latency for new device connections	[e.g., <[X] minutes from connection event]
5	Integration with existing SIEM / CMDB platforms	[e.g., Operational within [X] weeks of go-live]
6	Compliance report generation capability	[e.g., Automated reports aligned to IEC 62443 / NIST SP 800-82]
7	Platform uptime / availability	[e.g., >[X]% uptime per month]



4. Environment Overview

Instructions: Provide a detailed description of the OT/ICS environment to help vendors scope their solution accurately. Replace all placeholders with organization-specific information.

4.1 Site Overview

Site Name / ID	Location	Site Type	Approx. Asset Count	Criticality
[Site 1 Name]	[City, Country]	[e.g., Production Plant]	[e.g., 500-1,000]	[High / Med / Low]
[Site 2 Name]	[City, Country]	[e.g., Control Room]	[e.g., 100-500]	[High / Med / Low]
[Site 3 Name]	[City, Country]	[e.g., Substation]	[e.g., 50-200]	[High / Med / Low]
[Add rows]	[]	[]	[]	[]

4.2 Network Architecture

[Provide a high-level description of the OT network architecture, including zone and conduit topology, Purdue Model levels present (L0-L4), demilitarized zones (DMZ), IT/OT integration points, and any remote access infrastructure. Attach network architecture diagrams in the appendix where applicable.]

4.3 OT Asset Categories

The following asset categories are present within the in-scope environment. Vendors should confirm their solution's ability to identify, classify, and monitor each category.

Asset Category	Examples	Estimated Quantity	In Scope (Y/N)
Programmable Logic Controllers (PLCs)	Allen-Bradley, Siemens, Schneider, Mitsubishi	[Insert]	[Y/N]
Distributed Control Systems (DCS)	Honeywell, Emerson, ABB, Yokogawa	[Insert]	[Y/N]
Human Machine Interfaces (HMIs)	Wonderware, iFIX, WinCC, Ignition	[Insert]	[Y/N]
SCADA Systems	GE iFIX, Citect, Inductive Automation	[Insert]	[Y/N]



Asset Category	Examples	Estimated Quantity	In Scope (Y/N)
Remote Terminal Units (RTUs)	Various OEM vendors	[Insert]	[Y/N]
Industrial Historians	OSIsoft PI, AspenTech, GE Proficy	[Insert]	[Y/N]
Engineering Workstations (EWS)	Windows-based, vendor-specific	[Insert]	[Y/N]
Safety Instrumented Systems (SIS)	Triconex, Hima, Yokogawa ProSafe	[Insert]	[Y/N]
Industrial Network Switches	Cisco IE, Moxa, Hirschmann, Ruggedcom	[Insert]	[Y/N]
Industrial Firewalls / DMZ Devices	Fortinet, Palo Alto, Tofino, Cisco	[Insert]	[Y/N]
Remote Access Systems / Jump Servers	Vendor-branded VPN, Secure remote access	[Insert]	[Y/N]
IIoT Sensors and Smart Devices	Flow meters, pressure transmitters, smart sensors	[Insert]	[Y/N]
Industrial Servers	OPC servers, data concentrators, patch servers	[Insert]	[Y/N]
Field Devices (Drives, Actuators)	Variable speed drives, positioners, actuators	[Insert]	[Y/N]
IP-enabled Instruments	Analyzers, meters, cameras, access control	[Insert]	[Y/N]
IT Assets in OT Zones	Domain controllers, AV servers, patch servers	[Insert]	[Y/N]

4.4 Industrial Protocols in Use

Vendors must confirm native identification and parsing capability for all protocols relevant to the in-scope environment. Mark protocols present below.

Common industrial protocols that may be present include (select applicable):

- Modbus TCP / RTU
- EtherNet/IP (CIP)
- PROFINET
- PROFIBUS
- DNP3
- IEC 60870-5-101 / 104



-
- IEC 61850 (GOOSE, MMS, SV)
 - OPC-DA / OPC-UA
 - BACnet
 - HART-IP
 - FOUNDATION Fieldbus
 - CC-Link IE
 - DeviceNet
 - Sinec AP1
 - S7 / S7+

[Insert additional protocols relevant to the organization's environment.]

4.5 Existing Monitoring and Security Capabilities

Describe any existing OT security monitoring tools, SIEM platforms, vulnerability management tools, or asset management systems currently in use. This context enables vendors to identify integration opportunities.

[Insert description of existing tools and capabilities, including product names, vendor names, and integration points where known.]



5. Current State Challenges

The following challenges represent common OT/ICS asset visibility gaps experienced by industrial organizations. The issuing organization should annotate, expand, or remove items as appropriate to reflect its actual operational context.

5.1 Visibility and Inventory Gaps

- No comprehensive, continuously updated inventory of OT assets exists across all sites and network zones.
- Asset records in existing CMDB or spreadsheet-based inventories are incomplete, outdated, or unreliable.
- Unknown or undocumented devices - including legacy equipment and shadow OT installations - are present on industrial networks.
- IIoT devices and smart field instruments are not systematically tracked or classified.

5.2 Operational Safety Constraints

- Active network scanning tools cannot be safely used in OT environments due to the risk of disrupting fragile control system communications.
- Many industrial devices (PLCs, RTUs, safety systems) are sensitive to unexpected network traffic and may fail or lock up when queried by conventional discovery tools.
- Maintenance windows for intrusive discovery activities are rare, limiting real-time inventory updates.

5.3 Communication and Dependency Visibility

- Communication flows between OT assets, between OT and IT zones, and with external entities are not systematically monitored or mapped.
- Asset dependencies critical to process continuity are not documented, hindering incident response and change management.
- Unauthorized or unexpected communication paths between network zones are difficult to detect without continuous monitoring.

5.4 Compliance and Audit Readiness

- The organization lacks the ability to generate automated, timestamped evidence of asset inventory completeness for regulatory audits.
 - Demonstrating compliance with frameworks such as IEC 62443 (SR 2.8, SR 7.8) or NIST SP 800-82 asset management controls requires significant manual effort.
-



-
- Asset change history is not systematically captured, making it impossible to reconstruct the state of the environment at a given point in time.

5.5 Change Detection and Configuration Drift

- There is no automated mechanism to detect when new devices are added to the OT network, or when existing device attributes (firmware, software, configuration) change.
- Configuration drift on PLCs, HMIs, and network equipment is not systematically identified or alerted.
- Unauthorized firmware or software changes on critical control assets may go undetected for extended periods.



6. Scope of Work

The prospective solution must deliver the following capabilities across all in-scope sites and network environments. Vendors should confirm compliance with each scope element in their proposal response.

6.1 Passive Asset Discovery

The solution must perform fully passive, agentless asset discovery through network traffic analysis - without transmitting any queries, probes, or packets that could impact OT device operation or network stability. Discovery must be continuous and automatic, not dependent on periodic scans or scheduled sweeps.

6.2 Connected Asset Identification and Classification

Identified assets must be classified by type, function, and role within the industrial environment. Classification must extend to OT-specific device categories including PLCs, DCS controllers, RTUs, HMIs, SCADA servers, historians, engineering workstations, safety systems, and IIoT devices. Vendor-proprietary and multi-vendor environments must be supported.

6.3 Asset Metadata Enrichment

The solution must automatically enrich asset records with detailed metadata, including (but not limited to): manufacturer, model, firmware version, software version, operating system, installed applications, hardware revision, serial number, MAC address, IP address, network zone, communication protocols in use, and known vulnerability associations.

6.4 Communication and Dependency Mapping

The solution must generate and continuously maintain communication flow maps showing which assets communicate with which other assets, using which protocols, across which network paths. Dependency maps must identify critical process dependencies between assets and between OT and IT zones.

6.5 Continuous Monitoring and Change Detection

The solution must operate continuously, detecting and alerting on changes to the asset inventory in near-real-time. This includes new device connections, device removals, firmware or software changes, new communication flows, and deviations from established asset baselines.



6.6 Risk and Vulnerability Visibility

The solution must correlate asset inventory data with known industrial vulnerability databases (e.g., ICS-CERT, NVD, vendor advisories) to surface asset-level risk indicators. Risk prioritization must account for asset criticality, exploitability, and OT-specific exposure context.

6.7 Inventory Normalization and Management

All discovered asset data must be normalized into a consistent, structured format suitable for export, integration, and long-term management. The asset inventory must support search, filter, grouping, and export capabilities.

6.8 Multi-Site Visibility

The solution must support centralized visibility across all in-scope sites while accommodating site-level segmentation, access controls, and reporting. A unified management interface should provide cross-site dashboards alongside site-specific views.

6.9 Out of Scope

[Define what is explicitly excluded from this engagement. Examples: IT endpoint management, cloud infrastructure monitoring, non-OT network zones, specific geographic regions, third-party managed environments, etc.]



7. Functional Requirements

Vendors must complete the Supported column for each requirement using: Y = Fully Supported | P = Partially Supported | N = Not Supported | R = On Roadmap (state expected release). All P and R responses must be accompanied by explanatory notes.

7.1 Passive and Agentless Discovery

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
FR-1.1	The solution must perform fully passive asset discovery through analysis of network traffic only, without sending any probes, queries, or packets to monitored assets.	[Vendor to complete]	[]	[Vendor to complete]
FR-1.2	The solution must operate in a completely agentless manner - no software agents, clients, or modifications may be installed on monitored OT/ICS devices.	[Vendor to complete]	[]	[Vendor to complete]
FR-1.3	Discovery must function via network TAP and/or SPAN/mirror port connection without any active interaction with the production network.	[Vendor to complete]	[]	[Vendor to complete]
FR-1.4	The solution must be certified or demonstrably safe for deployment in live industrial environments where device sensitivity to unexpected traffic is a critical concern.	[Vendor to complete]	[]	[Vendor to complete]
FR-1.5	The solution must support discovery across air-gapped, isolated, and multi-zone OT network environments.	[Vendor to complete]	[]	[Vendor to complete]

7.2 OT Protocol Awareness and Deep Packet Inspection

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
FR-2.1	The solution must natively parse and decode industrial protocols including: Modbus TCP, EtherNet/IP (CIP), PROFINET, PROFIBUS, DNP3, IEC 60870-5-104, IEC 61850, OPC-DA, OPC-UA, S7/S7+, BACnet, HART-IP, and others as specified.	[Vendor to complete]	[]	[Vendor to complete]



Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
FR-2.2	Deep packet inspection (DPI) of industrial protocols must extract device-identifying information such as device name, manufacturer, function code, memory addresses, and register data.	[Vendor to complete]	[]	[Vendor to complete]
FR-2.3	The solution must identify assets from proprietary and vendor-specific industrial protocols beyond common open standards.	[Vendor to complete]	[]	[Vendor to complete]
FR-2.4	The solution must maintain and regularly update its industrial protocol and device fingerprinting library.	[Vendor to complete]	[]	[Vendor to complete]
FR-2.5	Vendor must provide a full list of supported industrial protocols and the depth of inspection available for each.	[Vendor to complete]	[]	[Vendor to complete]

7.3 Device Identification and Classification

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
FR-3.1	The solution must automatically identify and classify assets by device type (e.g., PLC, HMI, RTU, SCADA server, historian, engineering workstation, IIoT device, switch, firewall).	[Vendor to complete]	[]	[Vendor to complete]
FR-3.2	Classification must include manufacturer, model, product family, and hardware generation where determinable from passive traffic analysis.	[Vendor to complete]	[]	[Vendor to complete]
FR-3.3	The solution must support multi-vendor environments including devices from all major OT/ICS vendors.	[Vendor to complete]	[]	[Vendor to complete]
FR-3.4	The solution must handle device types that present with limited or no identifying protocol traffic through inference and behavioral analysis.	[Vendor to complete]	[]	[Vendor to complete]
FR-3.5	The solution must allow operators to manually classify, enrich, or override auto-classified asset records.	[Vendor to complete]	[]	[Vendor to complete]
FR-3.6	Classification accuracy must be demonstrable and vendor must provide reference data on identification rates from comparable deployments.	[Vendor to complete]	[]	[Vendor to complete]



7.4 Asset Metadata and Enrichment

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
FR-4.1	The solution must automatically populate asset records with: IP address, MAC address, hostname, manufacturer, device type, model, firmware version, software/OS version, and associated industrial protocols.	[Vendor to complete]	[]	[Vendor to complete]
FR-4.2	The solution must track hardware revisions, installed components, and detected application software where available from passive traffic.	[Vendor to complete]	[]	[Vendor to complete]
FR-4.3	Asset records must include network zone assignment, VLAN membership, and communication interface details.	[Vendor to complete]	[]	[Vendor to complete]
FR-4.4	The solution must support custom fields and tags to allow organization-specific enrichment of asset records.	[Vendor to complete]	[]	[Vendor to complete]
FR-4.5	The solution must correlate asset data with external vulnerability and threat intelligence sources (e.g., ICS-CERT, NVD) automatically.	[Vendor to complete]	[]	[Vendor to complete]

7.5 Communication Monitoring and Flow Mapping

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
FR-5.1	The solution must generate and maintain a live communication map showing all active communication flows between identified assets, including protocol, port, direction, and frequency.	[Vendor to complete]	[]	[Vendor to complete]
FR-5.2	Communication maps must distinguish between expected/authorized flows and newly detected or anomalous flows.	[Vendor to complete]	[]	[Vendor to complete]
FR-5.3	The solution must identify and visualize cross-zone communication flows (e.g., OT to IT, Level 2 to Level 3, DMZ traversal).	[Vendor to complete]	[]	[Vendor to complete]
FR-5.4	The solution must support the export of communication maps for use in network segmentation policy design and firewall rule review.	[Vendor to complete]	[]	[Vendor to complete]



Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
FR-5.5	Historical communication flow data must be retained and queryable to support incident investigation and change analysis.	[Vendor to complete]	[]	[Vendor to complete]

7.6 Change Detection and Alerting

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
FR-6.1	The solution must detect and alert on new devices connecting to the monitored network, including unauthorized or unknown assets.	[Vendor to complete]	[]	[Vendor to complete]
FR-6.2	The solution must detect changes to existing asset attributes, including firmware version, software version, IP address, and communication behavior.	[Vendor to complete]	[]	[Vendor to complete]
FR-6.3	The solution must detect new communication flows between assets that were not previously observed.	[Vendor to complete]	[]	[Vendor to complete]
FR-6.4	Alerts must be configurable by type, severity, asset category, network zone, and organizational unit.	[Vendor to complete]	[]	[Vendor to complete]
FR-6.5	The solution must support alert forwarding to external platforms (SIEM, email, ticketing systems) via configurable integration mechanisms.	[Vendor to complete]	[]	[Vendor to complete]

7.7 Dashboards, Visualizations, and Reporting

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
FR-7.1	The solution must provide role-based dashboards presenting asset inventory, communication maps, risk indicators, and change events in a clear visual format.	[Vendor to complete]	[]	[Vendor to complete]
FR-7.2	The solution must provide interactive asset search and filtering capabilities across all enriched metadata fields.	[Vendor to complete]	[]	[Vendor to complete]
FR-7.3	The solution must support multi-site dashboards providing enterprise-wide visibility alongside site-specific drilldown.	[Vendor to complete]	[]	[Vendor to complete]



Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
FR-7.4	The solution must generate structured reports including: asset inventory exports, risk reports, change reports, and compliance evidence reports.	[Vendor to complete]	[]	[Vendor to complete]
FR-7.5	Reports must be exportable in standard formats (e.g., PDF, CSV, JSON, XLSX) on a scheduled or on-demand basis.	[Vendor to complete]	[]	[Vendor to complete]
FR-7.6	The solution must provide visualization of asset relationship maps and network topology diagrams.	[Vendor to complete]	[]	[Vendor to complete]
FR-7.7	The solution must support customizable dashboards and report templates to meet organization-specific requirements.	[Vendor to complete]	[]	[Vendor to complete]

7.8 Historical Visibility and Audit Trail

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
FR-8.1	The solution must maintain a timestamped historical record of all asset states, enabling point-in-time reconstruction of the asset inventory.	[Vendor to complete]	[]	[Vendor to complete]
FR-8.2	All changes to asset records - including additions, modifications, and removals - must be logged with full audit trail metadata.	[Vendor to complete]	[]	[Vendor to complete]
FR-8.3	Historical communication flow data must be retained and queryable for a configurable retention period.	[Vendor to complete]	[]	[Vendor to complete]
FR-8.4	Audit logs must be tamper-evident and suitable for use as compliance and forensic evidence.	[Vendor to complete]	[]	[Vendor to complete]



8. Technical Requirements

8.1 Deployment Architecture

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
TR-1.1	The solution must support on-premises deployment within the organization's OT/ICS network environment, without requiring connectivity to external cloud services for core functionality.	[Vendor to complete]	[]	[Vendor to complete]
TR-1.2	The solution must support hybrid deployment models where centralized management is hosted externally (cloud or on-premises) while data collection sensors are located locally at each site.	[Vendor to complete]	[]	[Vendor to complete]
TR-1.3	The solution must support air-gapped or restricted-connectivity deployments where no outbound internet access is available from the OT network.	[Vendor to complete]	[]	[Vendor to complete]
TR-1.4	Network sensors / collectors must support deployment via standard network TAP or SPAN/mirror port configurations without requiring inline placement in the traffic path.	[Vendor to complete]	[]	[Vendor to complete]
TR-1.5	The solution must support both hardware appliance and virtual appliance sensor deployment options.	[Vendor to complete]	[]	[Vendor to complete]
TR-1.6	Vendor must provide detailed hardware specifications and sizing guidance for sensor and management platform deployment.	[Vendor to complete]	[]	[Vendor to complete]

8.2 Scalability and Performance

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
TR-2.1	The solution must scale to support [Insert number] assets across [Insert number] sites without degradation in discovery accuracy or platform performance.	[Vendor to complete]	[]	[Vendor to complete]
TR-2.2	The solution must handle peak network traffic volumes up to [Insert Mbps/Gbps] per sensor without packet loss or degraded analysis.	[Vendor to complete]	[]	[Vendor to complete]



Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
TR-2.3	The platform must support horizontal scaling of both sensor and management tiers to accommodate future growth.	[Vendor to complete]	[]	[Vendor to complete]
TR-2.4	Vendor must provide documented performance benchmarks and scalability limits for their proposed architecture.	[Vendor to complete]	[]	[Vendor to complete]

8.3 Data Management and Retention

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
TR-3.1	The solution must support configurable data retention periods for asset inventory data, communication flows, and event logs (minimum [Insert X] months).	[Vendor to complete]	[]	[Vendor to complete]
TR-3.2	All collected asset and network data must be stored in encrypted form at rest.	[Vendor to complete]	[]	[Vendor to complete]
TR-3.3	The solution must support data export in structured formats for long-term archiving and integration with external data management systems.	[Vendor to complete]	[]	[Vendor to complete]
TR-3.4	Vendor must describe data residency controls and options for organizations with data sovereignty requirements.	[Vendor to complete]	[]	[Vendor to complete]

8.4 Access Control and Authentication

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
TR-4.1	The platform must support Role-Based Access Control (RBAC) with configurable roles including read-only analyst, operator, site administrator, and global administrator.	[Vendor to complete]	[]	[Vendor to complete]
TR-4.2	The platform must support integration with enterprise identity providers (LDAP, Active Directory, SAML 2.0, OIDC) for centralized authentication.	[Vendor to complete]	[]	[Vendor to complete]
TR-4.3	Multi-factor authentication (MFA) must be supported for all administrative access.	[Vendor to complete]	[]	[Vendor to complete]
TR-4.4	All user actions within the platform must be logged in a tamper-evident audit log.	[Vendor to complete]	[]	[Vendor to complete]



Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
TR-4.5	Access to site-level data must be controllable at a per-site and per-zone granularity.	[Vendor to complete]	[]	[Vendor to complete]

8.5 Security of the Solution Itself

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
TR-5.1	All communications between sensors, management platform, and user interfaces must be encrypted using TLS 1.2 or higher.	[Vendor to complete]	[]	[Vendor to complete]
TR-5.2	The vendor must follow a documented secure software development lifecycle (SSDLC) for their product.	[Vendor to complete]	[]	[Vendor to complete]
TR-5.3	The vendor must provide a documented vulnerability disclosure and patch management process with defined SLAs for critical vulnerabilities.	[Vendor to complete]	[]	[Vendor to complete]
TR-5.4	The solution itself must not introduce any known vulnerabilities or unnecessary network services into the OT environment.	[Vendor to complete]	[]	[Vendor to complete]
TR-5.5	The vendor must provide software bill of materials (SBOM) for the solution upon request.	[Vendor to complete]	[]	[Vendor to complete]

8.6 High Availability and Resilience

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
TR-6.1	The management platform must support high availability (HA) configuration to eliminate single points of failure for the monitoring function.	[Vendor to complete]	[]	[Vendor to complete]
TR-6.2	Sensor appliances must continue local data capture and storage during periods of connectivity loss to the central management platform.	[Vendor to complete]	[]	[Vendor to complete]
TR-6.3	The solution must support automated failover and recovery mechanisms for core platform components.	[Vendor to complete]	[]	[Vendor to complete]



Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
TR-6.4	Vendor must specify recovery time objective (RTO) and recovery point objective (RPO) for the proposed platform architecture.	[Vendor to complete]	[]	[Vendor to complete]



9. Security and Compliance Requirements

9.1 Framework Alignment

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
CR-1.1	The solution must support alignment with IEC 62443 asset management requirements, including SR 2.8 (Auditable Events), SR 7.8 (Control System Component Inventory), and related security requirements.	[Vendor to complete]	[]	[Vendor to complete]
CR-1.2	The solution must support compliance evidence generation aligned to NIST SP 800-82 OT security guidelines, including asset inventory and access control documentation.	[Vendor to complete]	[]	[Vendor to complete]
CR-1.3	The solution must support organizations subject to sector-specific regulatory frameworks (e.g., NERC CIP, NIS2 Directive, CFATS, sector OT security regulations). Vendor must identify which frameworks their solution supports.	[Vendor to complete]	[]	[Vendor to complete]
CR-1.4	The solution must generate structured compliance reports that can be used as audit evidence for applicable regulatory frameworks.	[Vendor to complete]	[]	[Vendor to complete]

9.2 Operational Security Controls

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
CR-2.1	The solution must operate in a read-only, non-intrusive manner within OT networks, never transmitting unsolicited traffic to monitored devices.	[Vendor to complete]	[]	[Vendor to complete]
CR-2.2	The solution must support OT network segmentation visibility, identifying and reporting on communication flows that cross defined security zone boundaries.	[Vendor to complete]	[]	[Vendor to complete]
CR-2.3	The solution must detect and alert on devices communicating outside of their designated network zone without authorization.	[Vendor to complete]	[]	[Vendor to complete]



Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
CR-2.4	The solution must support configuration of authorized communication baselines against which deviations are detected and alerted.	[Vendor to complete]	[]	[Vendor to complete]
CR-2.5	Vendor must provide documentation confirming the solution has been tested and validated for safe operation in live industrial environments.	[Vendor to complete]	[]	[Vendor to complete]



10. Integration Requirements

Describe the organization's existing security and IT infrastructure with which the asset visibility solution must integrate. Vendors must confirm integration capability and describe the integration mechanism for each item.

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
IR-1.1	SIEM Integration: The solution must support forwarding of asset events, alerts, and inventory data to SIEM platforms via Syslog (CEF/LEEF) and/or REST API. [Specify SIEM platform: e.g., Splunk, Microsoft Sentinel, IBM QRadar, other].	[Vendor to complete]	[]	[Vendor to complete]
IR-1.2	CMDB Integration: The solution must support bi-directional or one-way synchronization of asset inventory data with CMDB platforms via API. [Specify CMDB: e.g., ServiceNow CMDB, BMC Helix, other].	[Vendor to complete]	[]	[Vendor to complete]
IR-1.3	Vulnerability Management Integration: The solution must provide asset context data (device type, firmware, OS, protocols) to vulnerability management platforms to enable OT-aware vulnerability assessment.	[Vendor to complete]	[]	[Vendor to complete]
IR-1.4	Ticketing / ITSM Integration: The solution must support automated ticket creation for configured alert types via integration with ITSM platforms. [Specify platform: e.g., ServiceNow, Jira, Remedy, other].	[Vendor to complete]	[]	[Vendor to complete]
IR-1.5	NAC Integration: The solution must support sharing of device identity and classification data with Network Access Control (NAC) platforms for automated enforcement decisions.	[Vendor to complete]	[]	[Vendor to complete]
IR-1.6	Firewall / Segmentation Integration: The solution must be able to share communication flow data with firewall management platforms to inform or automate rule updates.	[Vendor to complete]	[]	[Vendor to complete]
IR-1.7	API Availability: The solution must expose a fully documented RESTful API enabling programmatic access to all asset inventory, communication flow, alert, and reporting data.	[Vendor to complete]	[]	[Vendor to complete]
IR-1.8	OT Security Platform Integration: The solution must integrate or be compatible	[Vendor to complete]	[]	[Vendor to complete]



Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
	with other OT-specific security tools deployed in the environment. [Specify platforms where applicable].			
IR-1.9	Data Export: The solution must support export of all asset and event data in standard formats (JSON, CSV, STIX/TAXII for threat intelligence sharing).	[Vendor to complete]	[]	[Vendor to complete]



11. Data and Reporting Requirements

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
DR-1.1	Asset Inventory Report: The solution must generate a complete, exportable asset inventory report including all enriched metadata fields for every identified asset.	[Vendor to complete]	[]	[Vendor to complete]
DR-1.2	Communication Map Export: The solution must export communication flow data in a structured format showing source, destination, protocol, port, frequency, and zone classification.	[Vendor to complete]	[]	[Vendor to complete]
DR-1.3	Change Report: The solution must generate reports showing all asset inventory changes (additions, modifications, removals) over a specified time period.	[Vendor to complete]	[]	[Vendor to complete]
DR-1.4	Risk and Vulnerability Report: The solution must generate asset-level risk reports correlating device attributes with known vulnerability data.	[Vendor to complete]	[]	[Vendor to complete]
DR-1.5	Executive Summary Report: The solution must provide a high-level summary report suitable for presentation to non-technical stakeholders, covering asset counts, zone coverage, risk posture, and key metrics.	[Vendor to complete]	[]	[Vendor to complete]
DR-1.6	Compliance Evidence Report: The solution must generate reports specifically structured to serve as compliance evidence for applicable regulatory frameworks.	[Vendor to complete]	[]	[Vendor to complete]
DR-1.7	Site-Level Reports: The solution must support generation of both enterprise-wide and site-specific reports with appropriate access control.	[Vendor to complete]	[]	[Vendor to complete]
DR-1.8	Scheduled Reporting: Reports must be configurable to generate and distribute automatically on defined schedules.	[Vendor to complete]	[]	[Vendor to complete]
DR-1.9	Custom Reporting: The solution must support creation of custom reports using configurable filters, fields, and output formats.	[Vendor to complete]	[]	[Vendor to complete]



12. Implementation and Deployment Requirements

12.1 Deployment Approach

Vendors must provide a detailed deployment methodology including all phases, activities, dependencies, and resource requirements. The following elements are expected to be addressed in vendor proposals.

Deployment Element	Vendor Response / Approach
Initial environment assessment and pre-deployment planning	[Vendor to complete]
Pilot site deployment approach and success criteria	[Vendor to complete]
Full multi-site rollout phasing and schedule	[Vendor to complete]
Network TAP / SPAN configuration guidance and support	[Vendor to complete]
Management platform installation and configuration	[Vendor to complete]
Initial baseline establishment and tuning period	[Vendor to complete]
User acceptance testing (UAT) criteria and process	[Vendor to complete]
Parallel running and cutover approach	[Vendor to complete]
Post-deployment validation and acceptance	[Vendor to complete]

12.2 Pilot Requirements

The issuing organization requires a proof of concept / pilot deployment prior to full contract award. Vendors must confirm willingness to conduct a pilot and describe their pilot program offering.

Pilot Site(s)	[Insert proposed pilot site(s) and scope]
Pilot Duration	[Insert expected pilot duration, e.g., 30-90 days]
Pilot Objectives	[Insert specific outcomes to be demonstrated during the pilot]
Pilot Success Criteria	[Insert measurable criteria for pilot sign-off]



Pilot Cost	[Insert whether pilot is included in proposal cost or charged separately]
------------	---

12.3 Training Requirements

- Vendor must provide role-specific training for: OT Security Analysts, Platform Administrators, and OT Engineers.
- Training must include both initial deployment training and ongoing platform update training.
- Training materials must be provided in a documented, reusable format (e.g., user guides, video tutorials, online training portal).
- Vendor must specify training delivery options (on-site, virtual, self-paced) and associated costs.

12.4 Documentation Requirements

- Complete technical documentation including installation guides, configuration guides, and API reference.
- User and administrator operational guides for all platform components.
- Network architecture and deployment diagrams specific to the deployed configuration.
- Integration guides for all in-scope third-party platform integrations.
- Security hardening guide for the platform itself.



13. Vendor Experience and Qualifications

Vendors must provide detailed responses to each of the following qualification areas. Claims must be substantiated with verifiable evidence, references, and documentation.

13.1 OT/ICS Cybersecurity Experience

Information Requested	Vendor Response
Years of experience in OT/ICS cybersecurity	[Vendor to complete]
Number of OT/ICS asset visibility deployments completed globally	[Vendor to complete]
Number of active customers in comparable industrial sectors	[Vendor to complete]
Industrial sectors in which the vendor has delivered deployments	[Vendor to complete]
Largest deployment by asset count and site count	[Vendor to complete]
Geographic regions in which the vendor operates	[Vendor to complete]
Number of dedicated OT/ICS security engineers and researchers	[Vendor to complete]
Participation in ICS/OT industry groups (e.g., ISA, IIC, ISAGCA)	[Vendor to complete]

13.2 Customer References

Vendors must provide a minimum of [Insert number, e.g., three] customer references from organizations operating in comparable industrial sectors. References must be willing to discuss their deployment experience directly with the issuing organization.

Organization (or description)	Industry Sector	Deployment Scale	Years as Customer	Contact Available (Y/N)
[Reference 1]	[Sector]	[# assets / sites]	[Years]	[Y/N]
[Reference 2]	[Sector]	[# assets / sites]	[Years]	[Y/N]
[Reference 3]	[Sector]	[# assets / sites]	[Years]	[Y/N]



13.3 Certifications and Accreditations

- List all relevant product certifications (e.g., IEC 62443 product certification, Common Criteria, FIPS 140-2).
- List all relevant organizational certifications (e.g., ISO 27001, SOC 2 Type II).
- Identify any sector-specific certifications or qualifications (e.g., NERC CIP compliance validation, nuclear, defense).

[Vendor to list all applicable certifications with certification body, scope, and expiry date.]



14. Service and Support Requirements

Req. ID	Requirement Description	Vendor Response	Supported (Y/N/P)	Comments / Notes
SS-1.1	Vendor must offer 24/7/365 technical support coverage for Priority 1 (critical) incidents affecting platform availability or core functionality.	[Vendor to complete]	[]	[Vendor to complete]
SS-1.2	Vendor must define and commit to documented SLAs for each severity level including initial response time, status update frequency, and resolution time target.	[Vendor to complete]	[]	[Vendor to complete]
SS-1.3	A designated Customer Success Manager or Technical Account Manager must be assigned to the organization's account.	[Vendor to complete]	[]	[Vendor to complete]
SS-1.4	Vendor must provide a documented escalation path for technical support issues that cannot be resolved within defined SLA timeframes.	[Vendor to complete]	[]	[Vendor to complete]
SS-1.5	Software updates, security patches, and product releases must be provided within the support agreement at no additional licensing cost.	[Vendor to complete]	[]	[Vendor to complete]
SS-1.6	Vendor must provide advance notification of planned product changes, deprecations, or end-of-life timelines with a minimum [Insert, e.g., 12-month] notice period.	[Vendor to complete]	[]	[Vendor to complete]
SS-1.7	Vendor must provide access to a customer support portal, knowledge base, and ticketing system for case management and self-service troubleshooting.	[Vendor to complete]	[]	[Vendor to complete]
SS-1.8	Vendor must offer on-site support options for critical deployments and escalations where remote resolution is insufficient.	[Vendor to complete]	[]	[Vendor to complete]
SS-1.9	Vendor must provide a documented roadmap for product development and future capability releases, shared at minimum annually.	[Vendor to complete]	[]	[Vendor to complete]

14.1 Proposed SLA Summary



Severity Level	Description	Initial Response	Resolution Target	Escalation
P1 - Critical	Platform unavailable / core function failed	[Vendor]	[Vendor]	[Vendor]
P2 - High	Significant function impaired	[Vendor]	[Vendor]	[Vendor]
P3 - Medium	Non-critical issue / workaround available	[Vendor]	[Vendor]	[Vendor]
P4 - Low	General enquiry / enhancement request	[Vendor]	[Vendor]	[Vendor]



15. Evaluation Criteria

Proposals will be evaluated against the following criteria. Weightings are indicative and may be adjusted by the issuing organization to reflect specific priorities. A minimum qualifying score may be set at the organization's discretion.

Evaluation Criterion	Max Score	Weight (%)	Vendor Score	Evaluator Notes
1. Asset Visibility Accuracy and Coverage	20	20%	[/20]	[Notes]
2. Passive Discovery Safety and OT Operational Safety	15	15%	[/15]	[Notes]
3. OT Protocol Coverage and DPI Depth	15	15%	[/15]	[Notes]
4. Ease of Deployment and Operational Integration	10	10%	[/10]	[Notes]
5. Scalability and Multi-Site Architecture	10	10%	[/10]	[Notes]
6. Integration Capabilities (SIEM, CMDB, API)	10	10%	[/10]	[Notes]
7. Reporting Quality and Compliance Alignment	5	5%	[/5]	[Notes]
8. Vendor OT/ICS Experience and References	5	5%	[/5]	[Notes]
9. Support Quality and SLA Commitment	5	5%	[/5]	[Notes]
10. Total Cost of Ownership (3-year)	5	5%	[/5]	[Notes]
TOTAL	100	100%	[/100]	[Notes]

Note: The issuing organization reserves the right to conduct product demonstrations, proof-of-concept evaluations, and reference checks as part of the evaluation process, which may contribute to or modify scoring outcomes.



16. Pricing and Commercial Terms

Vendors must provide a comprehensive commercial proposal addressing all elements below. Pricing must be transparent, fully inclusive of all costs required for a production deployment, and structured to enable fair comparison across proposals.

16.1 Pricing Structure

Cost Category	Description	Proposed Cost
Software Licensing	Perpetual / subscription license model - specify basis (per asset, per site, per sensor, other)	[Vendor to provide]
Subscription / Annual Fees	Annual subscription or maintenance fees including support	[Vendor to provide]
Implementation Services	Professional services for deployment, configuration, and integration	[Vendor to provide]
Training	Initial and ongoing training delivery for all required roles	[Vendor to provide]
Sensor Hardware	Network sensor / collector appliance hardware costs (if applicable)	[Vendor to provide]
Support Services	Annual technical support and customer success services	[Vendor to provide]
3-Year Total Cost of Ownership	Sum of all costs over a 3-year period including all renewals	[Vendor to provide]
Optional / Add-On Services	Any additional services, modules, or capabilities available at additional cost	[Vendor to itemize]

16.2 Commercial Terms

- Vendors must clearly state all assumptions underpinning their pricing (e.g., asset count thresholds, included sites, included support hours).
- Pricing must include all costs required for full production deployment - no undisclosed fees are acceptable.
- Vendors must specify contract term options and any volume or multi-year discount structures available.
- Vendors must specify renewal pricing mechanisms and any caps on price escalation at renewal.



-
- Vendors must specify terms for scaling pricing if the organization's asset count or site count increases.

[Insert any additional commercial requirements, preferred payment terms, or procurement constraints applicable to the issuing organization.]



17. Response Instructions for Vendors

17.1 Submission Deadline and Process

RFP Issue Date	[Insert Date]
Vendor Clarification Deadline	[Insert Date] - Questions must be submitted in writing to [Insert Contact Email]
Clarification Response Date	[Insert Date] - Responses to all questions will be distributed to all registered vendors
Proposal Submission Deadline	[Insert Date and Time] [Insert Time Zone]
Submission Method	[Insert submission method: e.g., secure email / procurement portal / physical delivery]
Submission Address / Portal	[Insert contact email address or portal URL]
Primary RFP Contact	[Insert Name, Role, Organization, Email, Phone]
Proposal Validity Period	[Insert duration, e.g., 90 days from submission deadline]

17.2 Required Response Format

Vendors must structure their proposal response to follow the same section numbering as this RFP document. Each section of this RFP must be addressed in the corresponding section of the vendor's response.

17.3 Required Attachments

1. Completed requirement tables (Sections 7-14) with all Vendor Response, Supported, and Comments fields completed.
2. Company profile and OT/ICS cybersecurity background.
3. Product overview documentation, data sheets, and architecture diagrams.
4. Customer reference list (minimum [Insert number] references in comparable sectors).
5. Sample asset inventory report, communication map, and compliance evidence report outputs.
6. Proposed implementation plan and project timeline.
7. Complete commercial proposal including itemized pricing as specified in Section 16.
8. List of all supported industrial protocols with depth of inspection detail.
9. Copies of relevant product and organizational certifications.
10. Any additional information the vendor believes is relevant to the evaluation.



17.4 Clarification Process

All questions regarding this RFP must be submitted in writing to [Insert RFP Contact Email] no later than [Insert Clarification Deadline]. Questions received after this date may not be answered. Responses to all questions received will be compiled and distributed to all registered vendors simultaneously to ensure a fair and equitable process. Vendors must not contact any other member of the issuing organization directly regarding this RFP.

17.5 General Conditions

- The issuing organization reserves the right to accept or reject any proposal, to waive irregularities, and to cancel this RFP at any time without obligation.
- Submission of a proposal does not guarantee award of a contract.
- All costs associated with proposal preparation are solely the responsibility of the vendor.
- Information submitted in response to this RFP will be treated as confidential and used solely for evaluation purposes.
- The issuing organization is not bound by any oral representations made during this process.



18. Appendix

Appendix A - Glossary of Terms

Term / Acronym	Definition
Asset	Any hardware or software component connected to the OT/ICS network, including devices, systems, and applications.
DCS	Distributed Control System - a process control system used in industrial and manufacturing environments.
DPI	Deep Packet Inspection - analysis of network packet content beyond headers to extract protocol-specific data.
EWS	Engineering Workstation - a computer used to configure, program, and maintain OT/ICS devices.
HMI	Human Machine Interface - an operator interface for monitoring and controlling industrial processes.
ICS	Industrial Control System - a general term encompassing all control systems used in industrial operations (SCADA, DCS, PLC-based systems).
IEC 62443	International series of standards for industrial cybersecurity, covering security requirements for OT/ICS systems and components.
IIoT	Industrial Internet of Things - networked sensors, instruments, and devices in industrial environments.
NIST SP 800-82	NIST Guide to OT Security - US National Institute of Standards and Technology guidance for securing industrial control systems.
OT	Operational Technology - hardware and software that monitors and controls physical processes, devices, and infrastructure.
OPC-UA	OPC Unified Architecture - a machine-to-machine communication protocol for industrial automation.
Passive Discovery	Asset discovery performed entirely through analysis of existing network traffic, without sending any queries or probes to monitored devices.
PLC	Programmable Logic Controller - a ruggedized industrial computer used to automate electromechanical processes.
RTU	Remote Terminal Unit - a field device used to interface physical objects with a SCADA system.
RBAC	Role-Based Access Control - a method of restricting access based on user roles within an organization.
SCADA	Supervisory Control and Data Acquisition - a system for remote monitoring and control of industrial processes.
Shadow OT	Unauthorized or undocumented OT devices connected to industrial networks without formal approval or inventory registration.



Term / Acronym	Definition
SIS	Safety Instrumented System - a system designed to bring an industrial process to a safe state in the event of a hazardous condition.
SIEM	Security Information and Event Management - a platform that collects, analyzes, and correlates security event data.
SPAN	Switched Port Analyzer - a switch feature that mirrors network traffic to a monitoring port without interrupting normal traffic flow.
TAP	Test Access Point - a hardware device used to passively copy network traffic for monitoring purposes without affecting the live traffic flow.
TLS	Transport Layer Security - a cryptographic protocol for securing communications over a network.
CMDB	Configuration Management Database - a repository for information about IT and OT assets and their relationships.
NAC	Network Access Control - a security approach that restricts network access based on device identity and policy compliance.
SBOM	Software Bill of Materials - a formal record of the components, libraries, and dependencies in a software product.

Appendix B - Asset Inventory Template

Organizations may use the following template as a starting point for documenting their pre-existing asset inventory or for validating solution outputs against known assets.

#	Asset Name / ID	IP Address	MAC Address	Device Type	Manufacturer	Model	Firmware	Network Zone
1	[]	[]	[]	[]	[]	[]	[]	[]
2	[]	[]	[]	[]	[]	[]	[]	[]
3	[]	[]	[]	[]	[]	[]	[]	[]
4	[]	[]	[]	[]	[]	[]	[]	[]
5	[]	[]	[]	[]	[]	[]	[]	[]

Appendix C - Vendor Evaluation Scorecard

Evaluators may use this scorecard to record structured scores for each vendor proposal during the review process.



Criterion	Weight	Vendor A Score	Vendor B Score	Vendor C Score	Evaluator Notes
Asset Visibility Accuracy	20%	[/20]	[/20]	[/20]	[Notes]
OT Safety (Passive Discovery)	15%	[/20]	[/20]	[/20]	[Notes]
Protocol Coverage	15%	[/20]	[/20]	[/20]	[Notes]
Deployment & Integration	10%	[/20]	[/20]	[/20]	[Notes]
Scalability	10%	[/20]	[/20]	[/20]	[Notes]
Integration Capability	10%	[/20]	[/20]	[/20]	[Notes]
Reporting & Compliance	5%	[/20]	[/20]	[/20]	[Notes]
Vendor Experience	5%	[/20]	[/20]	[/20]	[Notes]
Support Quality	5%	[/20]	[/20]	[/20]	[Notes]
Total Cost of Ownership	5%	[/20]	[/20]	[/20]	[Notes]
TOTAL	100%	[/20]	[/20]	[/20]	[Notes]

Appendix D - Site Questionnaire

Complete one copy of this questionnaire for each in-scope site and attach to this RFP or provide to vendors upon request.

Site Name	[Insert Site Name]
Site Location	[Insert Physical Address / Region]
Site Type / Function	[e.g., Production plant, Control room, Substation, Refinery, etc.]
Estimated OT Asset Count	[Insert range or estimate]
Network Zones Present	[e.g., Level 0-Level 4, DMZ, Safety network]
Industrial Protocols in Use	[List applicable protocols]
SPAN/TAP Points Available	[Insert Y/N and describe available monitoring points]
Connectivity to Central Site	[Insert bandwidth and connectivity type: e.g., MPLS, VPN, isolated]
Maintenance Window	[Insert available maintenance windows for deployment activities]
Special Access Requirements	[e.g., escort required, HSE induction, security clearance]
Existing Security Tools	[List any OT security tools already deployed at this site]
Known Operational Constraints	[Insert any constraints relevant to deployment planning]



Appendix E - Compliance Checklist Reference

This checklist provides reference guidance for aligning asset visibility solution requirements to key control frameworks. Organizations should verify applicability to their specific regulatory context.

Framework / Control	Control Description	Mapped Requirement	Compliance Status
IEC 62443 SR 2.8	Auditable events - system must log all relevant security-related events	FR-8.2, TR-4.4	[Compliant / Gap / N/A]
IEC 62443 SR 7.8	Control system component inventory - complete documented asset inventory	FR-3.1 - FR-4.5	[Compliant / Gap / N/A]
NIST SP 800-82 §6.2	OT asset management - identifying, documenting, and managing OT assets	Section 6, 7	[Compliant / Gap / N/A]
NIST SP 800-82 §6.7	Network monitoring - continuous monitoring of OT network activity	FR-5.1 - FR-6.5	[Compliant / Gap / N/A]
NERC CIP-002	BES Cyber System identification and categorization	FR-3.1 - FR-3.6	[Compliant / Gap / N/A]
NIS2 Art. 21(2)(a)	Risk management - asset inventory as part of cybersecurity risk measures	Section 7, 9	[Compliant / Gap / N/A]
[Insert Framework]	[Insert Control Description]	[Insert Req. ID]	[Compliant / Gap / N/A]

Appendix F - Network Diagram Reference

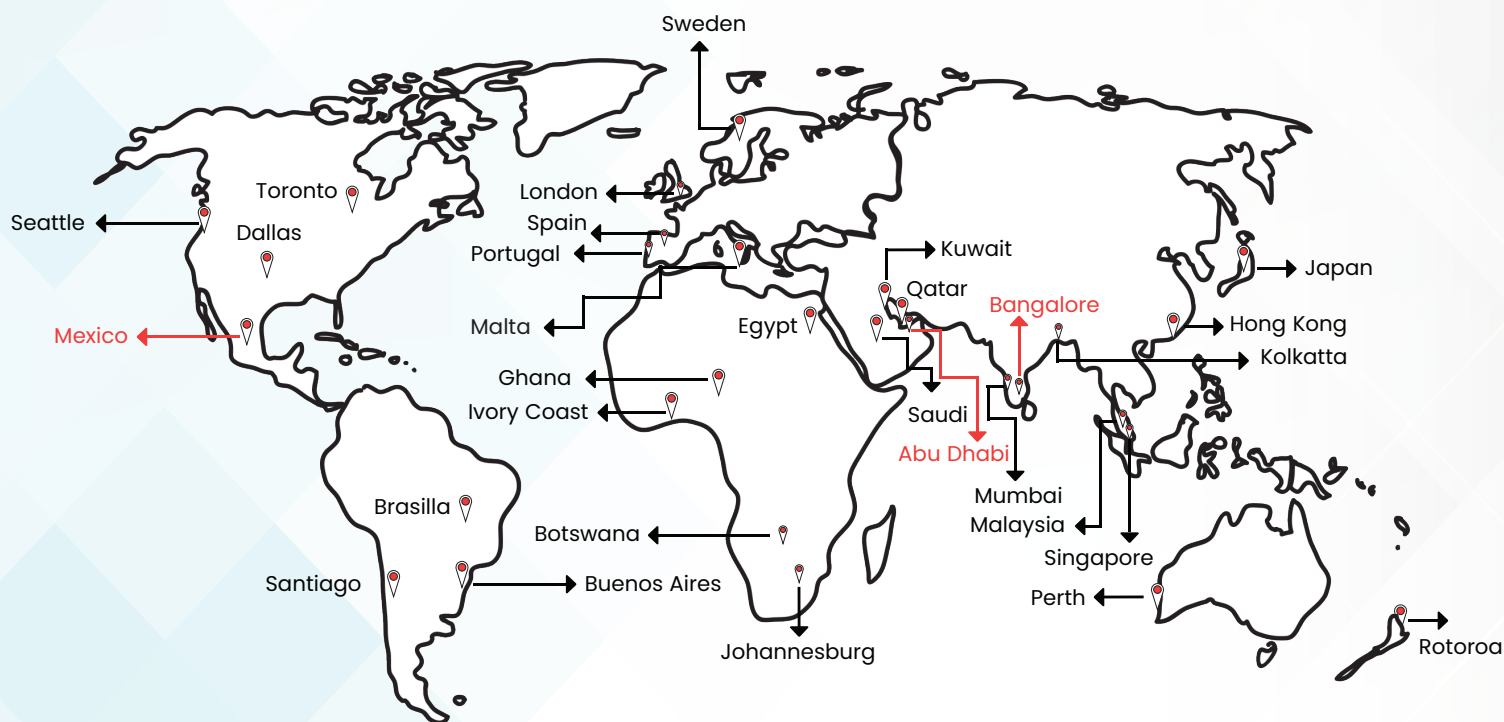
Attach or reference the organization's OT/ICS network architecture diagrams here. Diagrams should illustrate the Purdue Model zone structure, key network segments, IT/OT integration points, and proposed monitoring tap/span locations for vendor reference during solution scoping.

[Attach network architecture diagrams or reference document identifiers here. Mark any CONFIDENTIAL diagrams as restricted distribution.]





About Shieldworkz



ISOC and Honeypot Locations

Honeypot Locations



Security Operations Center



Shieldworkz is a global OT security company founded by top industry experts to protect critical infrastructure using proprietary technology and a leading consulting platform, we partner with businesses to secure assets, networks, and programs across industries. Our services are tailored to each client's cyber risks and backed by the world's largest OT and IoT threat intelligence facility and a global research team.

47

Secure Your Industrial Future

Talk to us today!



From OT security assessments covering NIS2, IEC 62443, NERC CIP and other regional requirements to an OT security platform, Shieldworkz covers all compliance and industrial cybersecurity enhancement needs. Talk to us to learn how you can enhance your security posture in 7 easy steps.

CONTACT US



📍 Fritz-Schäffer-Street 1,
4th floor
Bonn, 53113, Germany
☎ +49 (0) 228 / 929 39210
✉ europe@shieldworkz.com



📍 Tenth floor,
FAB BUSINESS CENTER
Abu Dhabi,
United Arab Emirates
☎ +971 56 660 5200
✉ middleeast@shieldworkz.com



📍 Gopalan Signature Tower,
No 6, 2nd Floor, Old Madras
Road, Benniganahalli
Bengaluru,
Karnataka 560093
☎ +91 9059620557
✉ apac@shieldworkz.com

