# Reverse Engineering, ATT&CK, ISA/IEC 62443 part 4-2 mapping

## Scope and Statement of Work

| Date | Services Performed By: | Services Performed For: |
|---|---|---|
| [Date] | USA | Customer<br>Customer Address |

# Reverse Engineering Approach

Through hardware, firmware and embedded device software testing and reverse engineering the discovery of both known vulnerabilities and zero days is not sufficient alone to enable supply chain improvements. Mapping vulnerabilities found to exploit ICS ATT&CK exploit tactics and techniques as well as ISA/IEC 62443 part 4-2 component and device security capability requirements helps to create a prioritized list of product improvements for component vendors and suppliers. Bill of materials, zero days and known CVEs become far more valuable to asset owners making product choices and to vendors making component and sub component supply chain decisions of each component and sub component was mapped to vulnerabilities, attacking techniques and tactics that could exploit vulnerabilities on components and subcomponents which were then mapped to product security capability requirements in part 4-2 that could defeat those tactics, techniques and vulnerabilities or at least make them no longer exploitable.

Many frameworks, standards, guidelines, and practices recommend and, in some cases, require that detailed technical security testing and supply chain verification, attack mapping and threat modeling occur in the product development lifecycle. Some examples include but are not limited to:

- **NIST SP 800-160 Systems Security Engineering** – System Security Requirements process and Verification and Validation Technical Process phases
- **ISA/IEC 62443 part 4-1 – Product Secure Development Lifecycle Maturity** – secure by design product development lifecycle practice requirements including secure by design, security requirement specification, attack mapping, threat modeling, independent security testing, continuous secure coding evaluation, considerations for third party components, handling and fixing vulnerabilities etcetera
- **ISA/IEC 62443 part 4-2 – Component Security Requirements** – security requirements for devices, firmware and software components and subcomponents
- **NIST Cybersecurity Framework (NIST CSF)** - Risk Assessment (ID.RA) - ID.RA-1: Asset vulnerabilities are identified and documented, Supply Chain Risk Management (ID.SC) - ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations
- **NIST SP 800-53rev5 & 82rev2** – CA-2 (Control Assessments), CA-8 (Penetration Testing), RA-3 (Risk Assessment), SA-11 (Developer Testing and Evaluation), SC-31 (Covert Channel Analysis), SR-6 (Supplier Assessments and Reviews), SR-10 (Inspection of Systems or Components)

Reverse Engineering with security mapping as a service can provide product improvements throughout the supply chain ecosystem. Some of the areas that will be tested and reviewed can include but are not limited to:

- Supply chain tracing and checking for counterfeit and defective components (e.g. chips on a circuit board)
- Checking firmware builds including bill of material subcomponents
- Checking hardware components and subcomponents to verify bill of material
- Sourcing of components
- Software components and subcomponents to generate bill of materials
- Checking coding repositories
- Documenting zero days as well as known vulnerabilities
- Determining which ATT&CK tactics and techniques could be used to exploit components
- Determining which part 4-2 requirements if built into components and or subcomponents could defeat which ATT&CK tactics and techniques that would make which vulnerabilities no longer exploitable
- Product comparison report cards between competitors and versions and families of products (including subcomponents that could be swapped out for more security subcomponents within products)
- Continuous testing throughout the product agile lifecycle and lifespan of the product

## Overview of Consultant

Consultant is a…..

## Scope of Work

The scope of work defines the systems, components, subcomponents, devices, equipment, suppliers, source code, repositories, binaries, software, firmware and hardware requested to be reverse engineered.

**Note: work with customer to call out specific products, suppliers, repositories, hardware, firmware, software, equipment, systems, locations etc in scope for reverse engineering. Deviations from this list will result in additional pricing for added scope.**

# Delivery Period

Scheduling of timelines to review engineer products and provide ATT&CK mapping, 62443 part 4-2 mapping and mitigation grading reports etc

**Note: once the dates and specifics products for reverse engineering have been provided list them here. Deviations from this may require additional charges (e.g. travel logistics changes, product changes etc).**

# Project Management & Communication

The lead point of contact for the customer product teams is expected to communicate regularly, at least weekly to support any issues, questions, billing and invoicing, access issues, travel issues etcetera.

# Methodology and Approach

As defined in scope of work section. Below goes into a bit more details about what a customer should expect in the CONSULTANT's product reverse engineering approach.

## Reverse Engineering Set up

1. **Customer to secure source code, supplier access and subcomponents** – includes providing access to all suppliers, binaries, hardware, firmware, software, product documentation etcetera.
2. **Determine list of products in scope for reverse engineering and mapping -** work with customer and supplier product teams including technical points of contacts to get an general list of make, models, versions, any logistical issues etcetera to enable the CONSULTANT team to ensure the necessary tools needed for reverse engineering certain components is included.
3. **Acquire reverse engineering tools, products in scope for reverse engineering and set up testing workbench** – work with customer product teams and suppliers point of contact to ensure all product components in scope are received by reverse engineering and mapping team.

## Execute Reverse Engineering

1. Reverse engineer and document each product in scope including all hardware, firmware and software components, subcomponents, binaries, libraries, repositories etcetera
2. Document all zero days for each itemized component and subcomponent including make, versions, dependencies etcetera

3. Document all known vulnerabilities and their respective CVE, CWE numbers and scores itemized for each component and subcomponent including make, model, versions, dependencies etcetera
4. Map all zero day and known vulnerabilities on itemized lists to their respective ATT&CK tactics and techniques that could be used to exploit them
5. Map all complete itemized lists to part 4-2 component requirements that could defeat, disrupt, or render vulnerabilities, ATT&CK tactics and techniques no longer exploitable

### Post Reverse Engineering

1. Produce a recommended prioritized product improvement findings and mitigations report with a plan of actions and milestones (POA&M) roadmap towards implementing more ISA/IEC 62443 part 4-2 security capabilities in all components and subcomponents
2. Generate product, component, subcomponent comparison report cards including brands, versions, make, model dependencies etcetera
3. Ensure report and POA&M accepted and final invoices are paid.

## Deliverables

CONSULTANT will provide the following deliverables:

- **Itemized inventory list of all components, subcomponents including dependencies mapped to zero days and known vulnerabilities, ATT&CK tactics and techniques with corresponding ISA/IEC 62443 part 4-2 component requirements**
- **Prioritized recommended mitigations and findings report with POA&M roadmap for implementing product improvements using ISA/IEC 62443 part 4-2 component requirements**
- **Make, Model, Version, component, subcomponent, and dependencies comparison report cards**

## CONSULTANT Responsibilities

- CONSULTANT shall provide customer with ICS OT security expertise, services and deliverables defined in this SoW
- CONSULTANT shall provide as needed optional coaching of customer staff in areas where onsite travel is not possible within desired timelines due to post COVID19 travel bans and social distancing requirements or local laws and orders between countries and regions.
- CONSULTANT shall provide its own tools and request necessary information and products in scope for reverse engineering
- Reverse Engineering is limited to selected components, subcomponents, products, hardware, firmware, software, binaries, source code, repositories, suppliers etcetera and equipment, and systems in scope of this SoW.

- Implementation of recommendations to remediate discovered risks is not included in this engagement/SoW. Separate CONSULTANT services can be priced and purchased in a separate SoW for advisory and or systems security engineering related services to support remediation efforts.
- Additional modification of tasks or scope will result in the opportunity being considered a separate engagement offering that will require additional scoping, additional costs and/or change order.
- CONSULTANT will provide its own tools as necessary mentioned in this SoW
- CONSULTANT will collaborate with product vendor and government on responsible disclosures of zero days discovered during the Reverse Engineering projects

## Customer Responsibilities

- Customer will designate one (1) employee to serve as a primary authoritative point of contact (POC) at the organizational level for the project. The POC will be responsible for enabling CONSULTANT to schedule customer resources for required meetings, travel, logistics, billing, access needs, and other needs deemed necessary to complete the project work as scoped. The POC will participate in status meetings as required and will serve as the first point of escalation for any project-related requests or issues.
- Customer will provide access to all proprietary information, source code, repositories, suppliers, hardware, firmware, software, applications, site locations, assets, systems, devices and third parties necessary to complete the Scope of Work.
- Customer and customer resources will execute all data and product gathering activities in an efficient manner. All products and data requested will be promptly submitted to CONSULTANT within the requested timeframe to stay on schedule with the scope, delivery, methodology and approach timelines outlined in this SoW. Any delays incurred in acquiring this information or access may result in the need for a Change Order and rescheduling of the project, at the discretion of CONSULTANT.
- Customer will provide the necessary staff availability to complete reverse engineering and answer questions. Customer’s inability to provide this staff may affect the completion of tasks and/or deliverables.
- Customer will provide access to any necessary facility, tools, systems, information, devices, accounts, and work areas to complete the project. This includes vendor products and software such as calibration tools, PLC programming tools for equipment in scope etcetera.

## Fee Schedule, Terms & Conditions

This engagement will be conducted as a fixed cost in addition to reimbursable travel expenses for flights, uber, rental cars, hotel, meals, baggage fees etcetera. The total value for the Services pursuant to this SoW shall not exceed the cost listed below unless otherwise agreed to by both parties via the project change control procedure, as outlined within. A Project Change Request (PCR) will be issued specifying the amended value.

This figure is based on the Scope of services and deliverables in this SoW. The fixed cost does not include the reimbursable travel expenses. Travel expenses will be submitted as expense invoice after each site visit and the are payable immediately upon submission from CONSULTANT to customer.

| Item Description | Estimated Project Total |
|---|---|
| CONSULTANT reverse engineering services and deliverables | **$** |

**Note: Average pricing for reverse engineering projects depending on scope of equipment and duration of projects. 30% of estimate is due upon acceptance of SoW to begin security FAT or SAT event. Remaining balance should be paid in full within 72 hours of receipt of deliverables.** If additional products are added or requested, then full payment of completed projects must be received before scheduling additional product projects. All invoicing and payments are processed as ACH and or credit both partial and full lump sum payments accepted and billed via automated electronic invoices from accounting system. **An automatic 5% late fee will be added per 10 days late payment upon all submitted invoices. All invoices are due upon submission by CONSULTANT. Late fees apply to separate reimbursable expenses invoices as well.**

## Out-of-Pocket Expenses / Invoice Procedures

Covers reimbursable travel and supplies such as baggage fees, airfare, hotel, uber and rental vehicles etcetera.

## Assumptions

The following assumptions are observed throughout this engagement:

- CONSULTANT assumes no responsibility of liability for actions of customer staff during engagements either by their own actions or their understanding of recommendations, requests, questions or coaching from CONSULTANT
- CONSULTANT expects customer to collaborate on responsible disclosures of any zero days that CONSULTANT team discovers as well as updates to existing CVEs where adjustments need to be

made to existing public disclosures. This includes giving CONSULTANT team member public credit for both discovery and mappings to ICS ATT&CK and ISA/IEC 62443 part 4-2

- A Change Order may be required for any additional equipment or durations beyond the agreed scope in this SoW for the quoted fixed price.
- CONSULTANT assumes that the final deliverable report will be consistent with the items identified in the Deliverables section within this SoW. A Change Order fee will be applied to any additional deliverables that are required and are not included within this SoW.

# Project Change Control Procedure

The following process will be followed if a change to this scope of work (SOW) is required:

- A Project Change Request (PCR) will be the vehicle for communicating change. The PCR must describe the change, the rationale for the change, and the effect the change will have on the project SoW.
- The designated Project Manager of the requesting party (CONSULTANT or Customer) will review the proposed change and determine whether to submit the request to the other party.
- Both Project Managers will review the proposed change and approve it for further investigation or reject it. CONSULTANT and Customer will mutually agree upon any charges for such investigation, if any. If the investigation is authorized, the Customer Project Managers will sign the PCR, which will constitute approval for the investigation charges. CONSULTANT will invoice Customer for any such charges, if any. The investigation will determine the effect that the implementation of the PCR will have on SOW price, schedule and other terms and conditions of the Agreement.
- Upon completion of the investigation, both parties will review the impact of the proposed change and, if mutually agreed, a Change Authorization will be executed.
- A written Change Authorization and/or PCR must be signed by both parties to authorize implementation of the investigated changes. The PCR will contain the fees, pricing and scope of requested changes.