ICS OT IoT Threat Modeling

Scope and Statement of Work

Date	Services Performed By:	Services Performed For:
[Date]		Customer
	USA	Customer Address

Threat Modeling Approach

Threat Modeling enables product vendors, systems integrators, security consultants, regulators, asset owners and operators and other interested stakeholders the ability to map out and model potential risks within devices, components, applications, and systems. Threat Modeling does not replace formal security assessments or testing, but it can help illuminate or discover areas of focus for design, testing, assessments, and continuous improvement. Defining what a component is, what its interfaces are, how it should or is expected to interact with other components and environments is a good place to start. Further detailing all interfaces, communications, conduits, parts, and components allows for complex modeling and analysis prior to more resource intensive and intrusive steps such as formal security testing, reverse engineering, product development, and security assessments.

Furthermore, mapping leveraging industry modeling tools, practices and techniques enables consistency in threat modeling of components, devices, applications, and systems. Using industry standards, practices and guidelines allows for quickly determining what potential mitigations could be used to decrease or eliminate attack surfaces.

Many frameworks, standards, guidelines, and practices recommend and, in some cases, require detailed technical security testing and supply chain verification, attack mapping and threat modeling occur throughout an asset's 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)

Threat Modeling can provide improvements in product design, product selection, systems integration choices and practices, management of limited testing resources and prioritized test cases to include verification and validation of potential design weaknesses.

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 threat modeled.

Example high level steps of the threat model approach are as follows:

- **Step 1: Define Asset Scope** – This allows the consultant to document details about each component, device, protocol, conduit, application, system, and network in scope for the threat model.
- **Step 2**: **Asset Description** – This allows the consultant to create a general description of each in scope component, device, application, protocol, conduit, system, and network. The description also includes the assets' role or purpose, their interdependencies, their user functions, and roles etcetera.
- **Step 3**: **Threat Model Diagram** – This allows the consultant to leverage diagraming tools to create a visual model of the in scope components, subcomponents, interfaces, protocols, communication conduits, applications, devices, networks, and systems.
- **Step 4**: **Define Possible Attack Test Cases** – This allows the consultant to create a list of attack scenarios that could occur if the in scope assets were to be used. These attack scenarios could then be tested in a future or parallel penetration test, acceptance test or reverse engineering and exploitation engagement.
- **Step 5**: **Attack Mapping Threat Model Matrix** – This allows the consultant to document and list out critical threat modeling details for each in scope device, component, subcomponent, interface, protocol, conduit, systems, network, and application. This matrix will capture asset properties, asset types, asset make and model, relevant common weaknesses, application attack tactics, and techniques etcetera. This Matrix will also capture any known

asset related CVEs and provide specific mitigation control recommendations from industry standards, regulations, practices, and guidelines.

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

Delivery Period

Scheduling of timelines to review products, components, devices, protocols, applications, networks, systems, and conduits that should be included in the threat model.

Note: once the dates and specific assets for threat modeling 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 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.

Threat Model Set up

1. **Determine in scope assets** – consultant works with customer to determine what assets are in scope for the threat model.
2. **Collect asset information** - includes customers providing access to all suppliers, binaries, hardware, firmware, software, product documentation etcetera. Also include the consultant conducting OSINT research to collect datasheets, spec sheets, research papers, product manuals etcetera.
3. **Gather tools and prepare Threat Modeling environment** – consultant sets up, purchases and prepares tools that will be used to conduct the threat model. Some of the tools that will be used include but is not limited to:
    a. Consultant ICS OT IoT Attack Mapping Threat Modeling Matrix Tool
    b. IriusRisk Threat Modeling Tool

c. Mind mapping and System Modeling and Diagraming tools (e.g., Lucidchart, Draw.io, Visio, Mindmapper etc.)
d. MITRE EMB3D
e. MITRE ATT&CK
f. MITRE CWE
g. CVE (e.g., NIST NVD, MITRE CVE, CISA KEV list)
h. OWASP
i. ISA/IEC 62443 parts 4-2 and 3-3
j. Asset product documentation (e.g., manuals, datasheets, spec sheets, P&ID, UML, SysML, process flow diagrams, network diagrams etc.)
k. Consultant Generative AI Threat Modeling Agent Tool

Execute Threat Modeling

1. Analyze all collected documentation, features, interfaces etcetera collected for in scope components.
2. Document make, model, versions, asset functional details descriptions etcetera.
3. Build visual Threat Modeling Diagram showing all subcomponents, components, interfaces, protocols, conduits, features, interdependencies etc.
4. Document MITRE EMB3D properties
5. Document CWE ID
6. Document associated MITRE EMB3D threat types and associated MITRE ATT&CK Tactics and Techniques
7. Document associated known product CVEs
8. Document associated MITRE EMB3D mitigations, OWASP practices, ISA/IEC 62443 part 4-2 & 3-3 requirements, NIST SP 800-82 controls etcetera.
9. Create applicable Attack Test Case Scenarios
10. Complete Attack Mapping Threat Modeling Matrix
11. Create Threat Modeling Analysis summary report including summary and detailed recommended mitigations.

Post Threat Modeling Execution

1. Finalize verification of all collected and analyzed information.
2. Finalize updates to Threat Model Diagram.
3. Finalize updates to Attack Mapping Threat Model Matrix
4. Finalize Threat Model Analysis report including recommended mitigations and high level POA&M implementation roadmap
5. Deliver all artifacts to the customer
6. Conduct customer out brief and answer any customer questions for potential follow up work listed on POA&M mitigation and implementation roadmap.

Deliverables

CONSULTANT will provide the following deliverables:

1. Copies of all collected and discovered documentation and artifacts.
2. Final Threat Model Diagrams.
3. Final Attack Mapping Threat Model Matrix.
4. Final Threat Model Analysis Report including an appendix POA&M mitigation implementation roadmap.
5. Optional post deliverable end of engagement out brief or Q&A follow up next steps with customer team.

CONSULTANT Responsibilities

- CONSULTANT shall provide customer with ICS OT security expertise, services and deliverables defined in this SoW
- CONSULTANT shall provide its own tools and request necessary information and products in scope for threat modeling
- Threat Modeling 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 separate SoW for advisory and 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.

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 threat model and answer questions. Customer inability to provide this staff may affect the completion of tasks and/or deliverables.

Fee Schedule, Terms & Conditions

This engagement will be conducted as a fixed cost plus contract 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 they are payable immediately upon submission from CONSULTANT to customer.

Item Description	Estimated Project Total
CONSULTANT threat modeling services and deliverables	**$**

Note: 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
- 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 cover the fees, pricing, and scope of requested changes.