# Incident Response Plan

## Revision

Version 15
1/5/24 1:31 PM

## SME

Charles Wilson
Garth Scheidemantel
Lucky Munro

## Abstract

This document describes the process to respond to security incidents.

## Group / Owner

Security / Partner Integration Planner

## Motivation

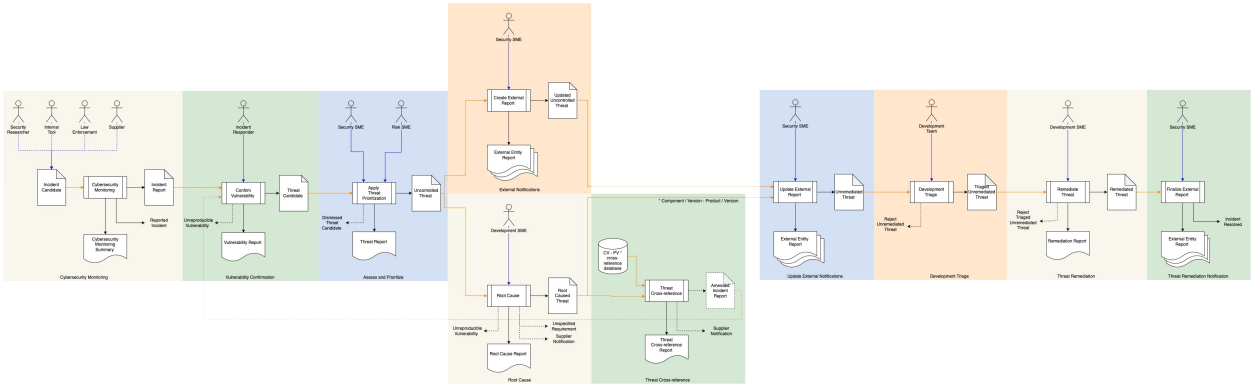
This document is motivated by the need to have formal processes in place for the management of incidents affecting safety-critical, cyber-physical systems in the field for certification of compliance to standards such as **ISO/SAE 21434** and **ISO 26262**.

## License

# Overview

The incident response process involves numerous steps and requires the involvement of multiple groups throughout the organization. Because of its broad reaching scope, it interlocks with several other processes within the **AVCDL**.

The following shows the incident response workflow from initial reporting through to resolution:

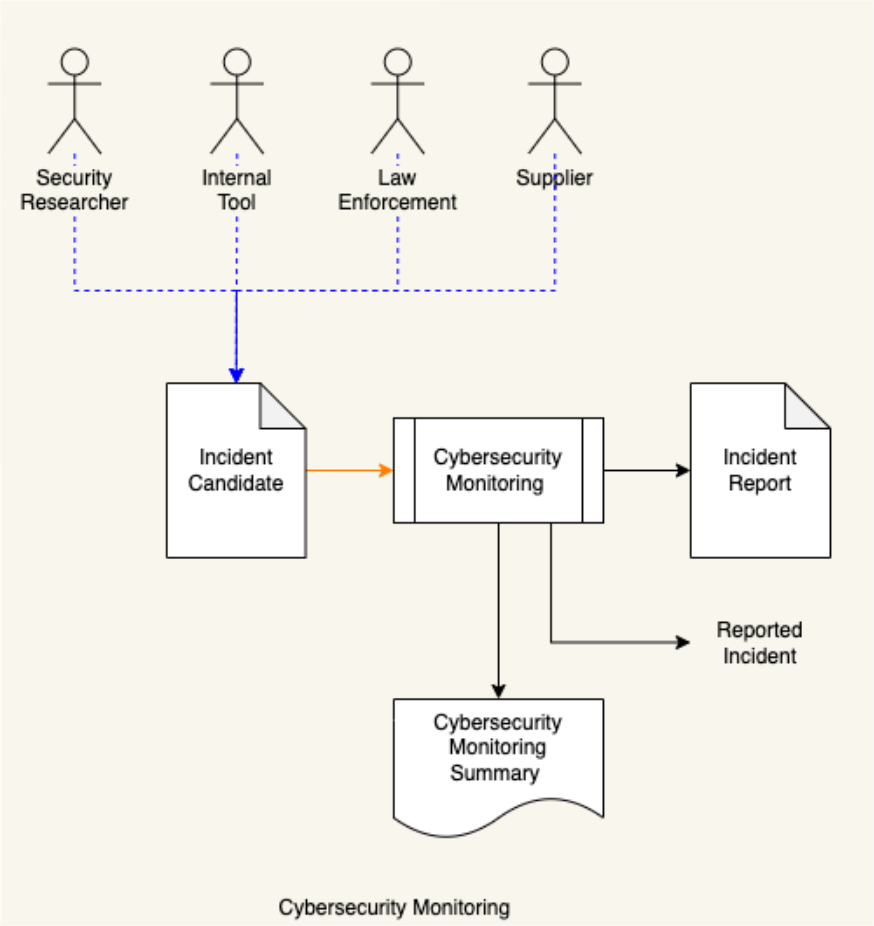


**Note:** Throughout this document threats shown as both inputs and outputs of various processes. These may be separate artifacts within the incident response system, but more commonly they represent different fields within the same issue response system database entry.

# Process

## Cybersecurity Monitoring

| | |
|---|---|
| **Inputs** | Incident Candidate |
| **Outputs** | Incident Report<br>Incident Monitoring Summary |
| **Participants** | Internal Tools (optional)<br>Security Researcher (optional)<br>Law Enforcement (optional) |



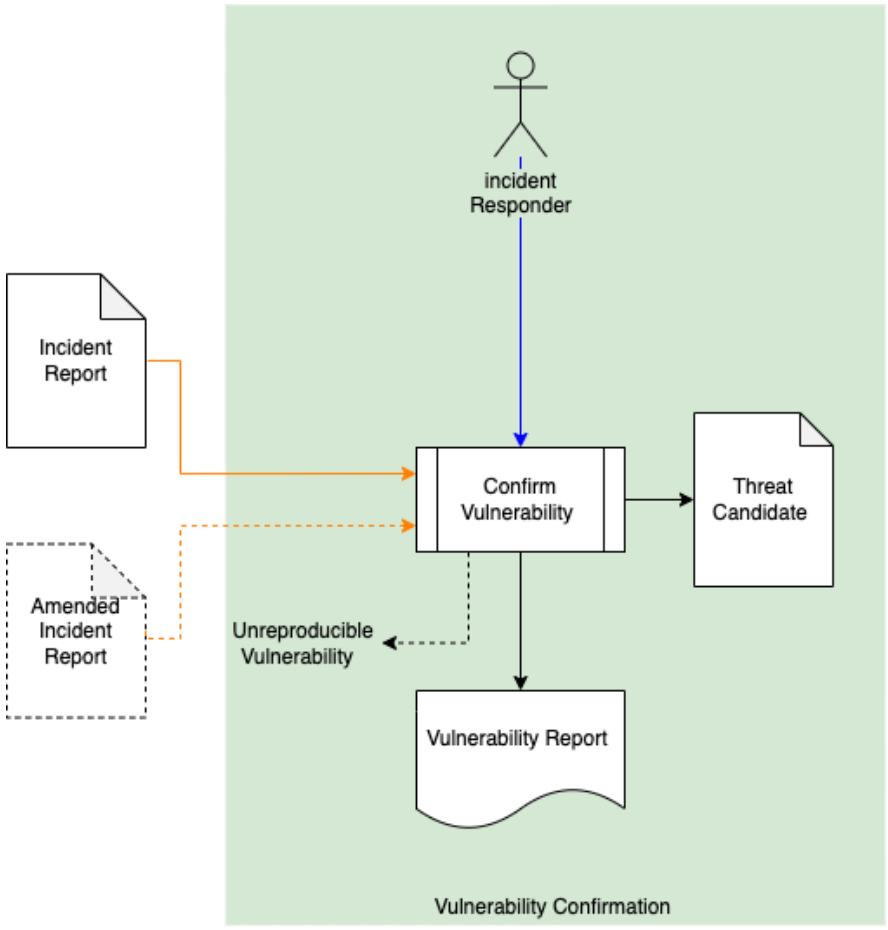

The incident monitoring process (see **Cybersecurity Monitoring Plan** [12]) detects a new **Incident Candidate** from internal tooling, law enforcement, an independent researcher or a supplier. The incident monitoring process then generates an **Incident Report** and a **Reported Incident** notification is sent.

A **Cybersecurity Monitoring Summary** is generated.

**Note:** Because of the asynchronous nature of the incident reporting, the Cybersecurity Monitoring Summary may be generated either on a per incident basis or periodically.

# Vulnerability Confirmation

| | |
|---|---|
| **Inputs** | Incident Report<br>Amended Incident Report (optional) |
| **Outputs** | Threat Candidate<br>Vulnerability Report |
| **Participants** | Incident Responder |



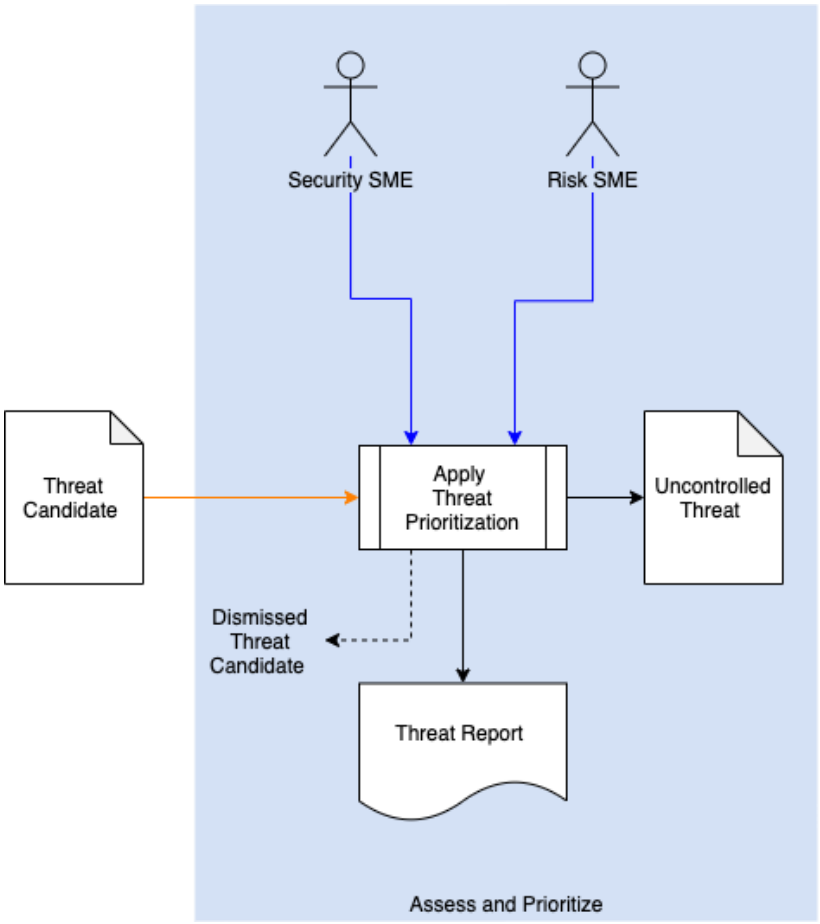

When a **Reported Incident** notification is received, an incident responder will attempt to confirm the vulnerability described in the **Incident Report** and will create a **Vulnerability Report** documenting their findings. Alternately, when an **Amended Incident Report** is generated by the same process is undertaken.

If the vulnerability is unreproducible, the incident responder will close the **Incident Report** and an **Unreproducible Vulnerability** notification will be sent to the reporter.

If the vulnerability is confirmed, the incident responder will generate a **Threat Candidate**.

# Assess and Prioritize

| | |
|---|---|
| **Inputs** | Threat Candidate |
| **Outputs** | Uncontrolled Threat<br>Threat Report |
| **Participants** | Security SME<br>Risk SME |




The Security SME will take the **Threat Candidate** and apply the **Threat Prioritization Plan**. The **Threat Candidate's** rank and risk will be assigned by the Security SME and Risk SME respectively. A **Threat Report** documenting the findings will be generated.

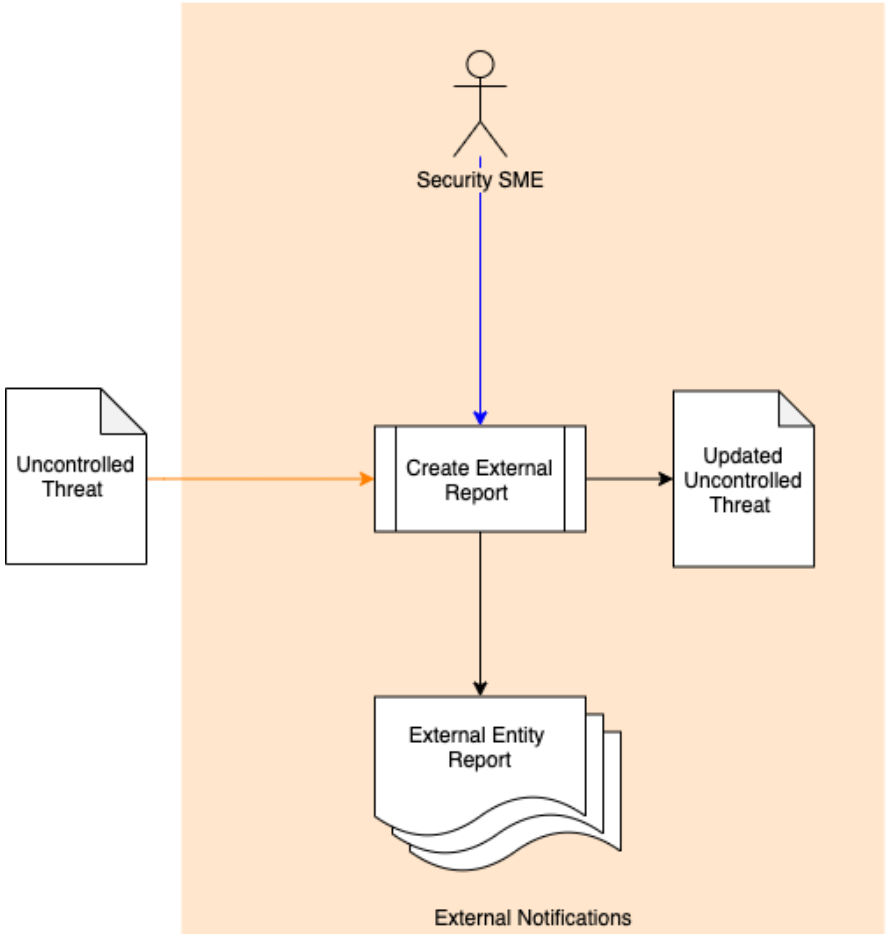
If the threat is determined to be controlled, a **Dismissed Threat Candidate** notification will be generated.

If the threat is determined to be uncontrolled, an **Uncontrolled Threat** will be generated.

**Note:** In practice, the **Threat Candidate** and **Uncontrolled Threat** are represented by different fields in the same issue response database entry.

## External Notification

| | |
|---|---|
| **Inputs** | Uncontrolled Threat |
| **Outputs** | Updated Accepted Threat<br>External Entity Report |
| **Participants** | Security SME |




With the **Uncontrolled Threat** the Security SME generates **External Entity Reports** based on the findings. The NIST **Security Content Automation Protocol (SCAP)** [10] is the current standard for ingest by external entities. The more recent **Common Security Advisory Framework (CSAF)** [15] also provides a format which is easily exchanged. It is preferred as it has the advantage of being embodied as JSON rather than XML and provides validation code for easier implementation.

Typical reports are:

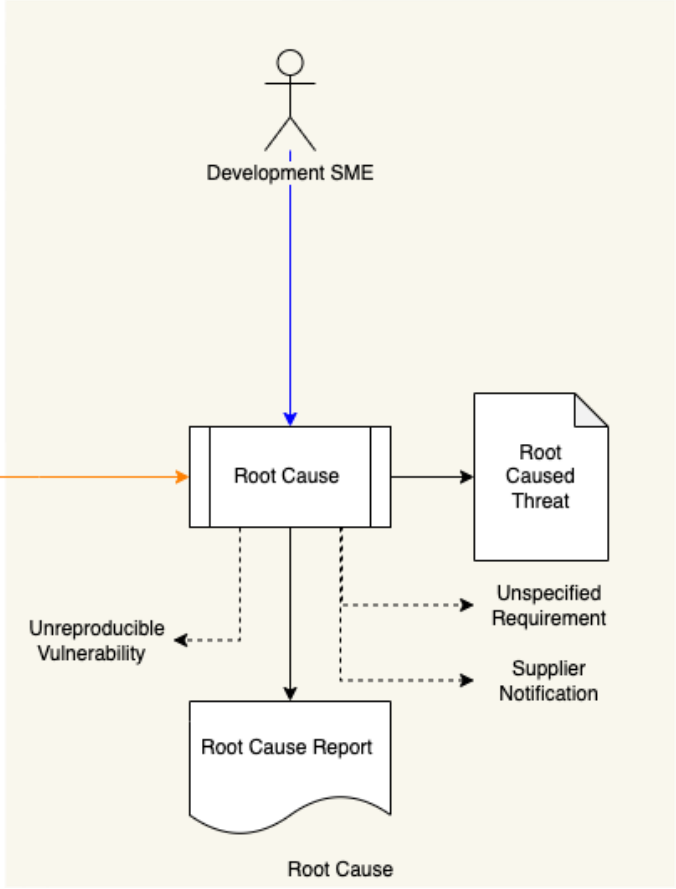
- Information Sharing and Analysis Center (ISAC) Report
- Common Vulnerability and Exposure (CVE) Report

The security SME will also generate an **Updated Accepted Threat**.

**Note:** This step can take place in parallel with **Root Cause** step.

# Root Cause

| | |
|---|---|
| **Inputs** | Uncontrolled Threat |
| **Outputs** | Root Caused Threat<br>Root Cause Report |
| **Participants** | Development SME |




The Development SME reviews the **Uncontrolled Threat** to determine the root cause. A **Root Cause Report** documenting the findings is generated.

If the vulnerability is unreproducible, an **Unreproducible Vulnerability** notification will be generated. If the vulnerability is reproducible, a **Root Caused Threat** is produced.

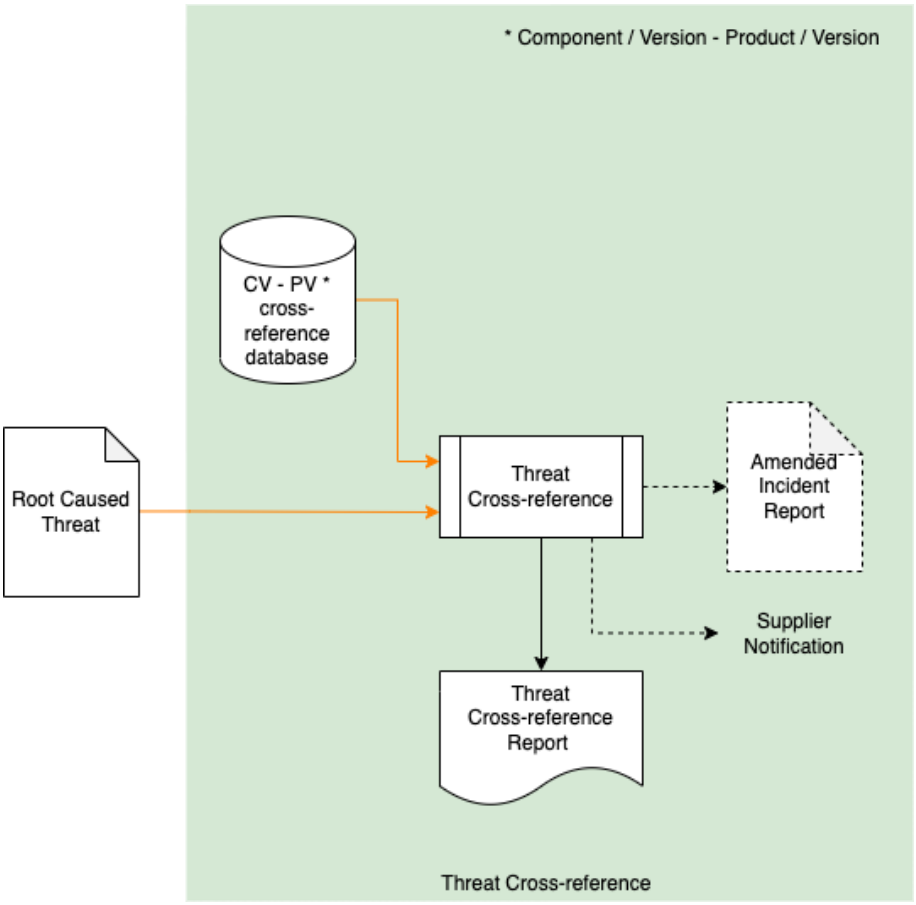
If it is determined that the threat is not covered by established requirements, an **Unspecified Requirement** notification will be generated. This will be taken up as input by either the **Design Showing Security Considerations** [13] (requirement exists) or **Product-level Security Requirements** [14] (requirement does not exist) process.

If it is determined that the threat is exploiting a deficiency in a supplier-provided element, a **Supplier Notification** is generated. This will be taken up by supply chain interaction processes.

**Note:** This step can take place in parallel with **External Notification** step.

# Threat Cross-reference

| | |
|---|---|
| **Inputs** | Root Caused Threat<br>Component / Version – Product / Version cross-reference database |
| **Outputs** | Amended Incident Report |
| **Participants** | **none** |



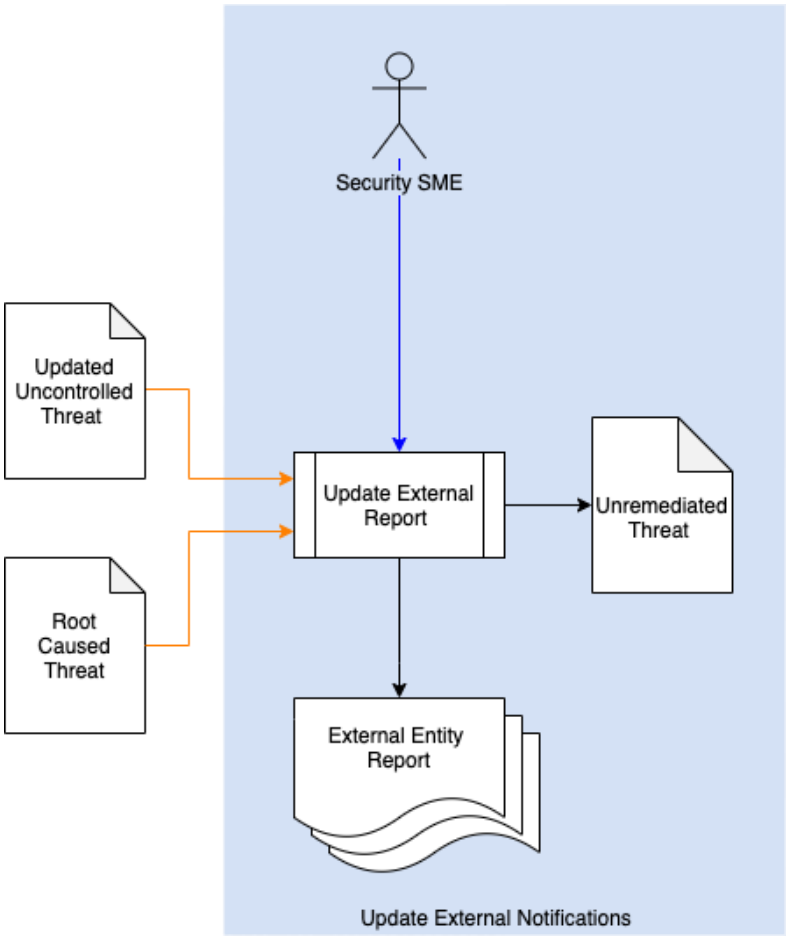

The **Root Caused Threat** is checked against the **Component / Version – Product / Version Cross-reference Database** (see **Component / Version – Product / Version Cross-reference Document** [11]). If any other elements are impacted, an **Amended Incident Report** including all impacted components and products will be created. A **Threat Cross-reference Report** will be generated.

If it is determined that the threat exists in supplier-provided elements, a **Supplier Notification** is generated. This will be taken up by supply chain interaction processes.

**Note:** The **Amended Incident Report** will be fed into the **Vulnerability Confirmation** stage for further consideration.

# Update External Notification

| | |
|---|---|
| **Inputs** | Root Caused Threat<br>Updated Uncontrolled Threat |
| **Outputs** | Unremediated Threat<br>Updated External Entity Reports |
| **Participants** | Security SME |

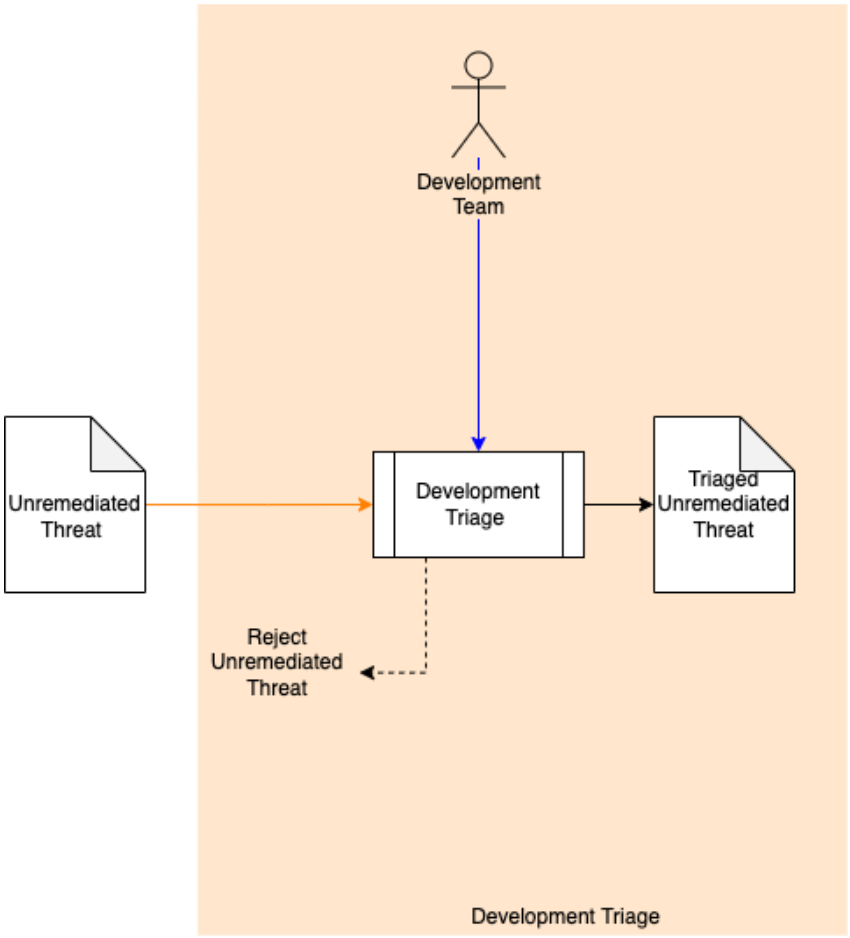



Using the information from the **Root Caused Threat** and **Updated Uncontrolled Threat** an updated set of **External Entity Reports** is generated.

An **Unremediated Threat** is generated.

# Development Triage

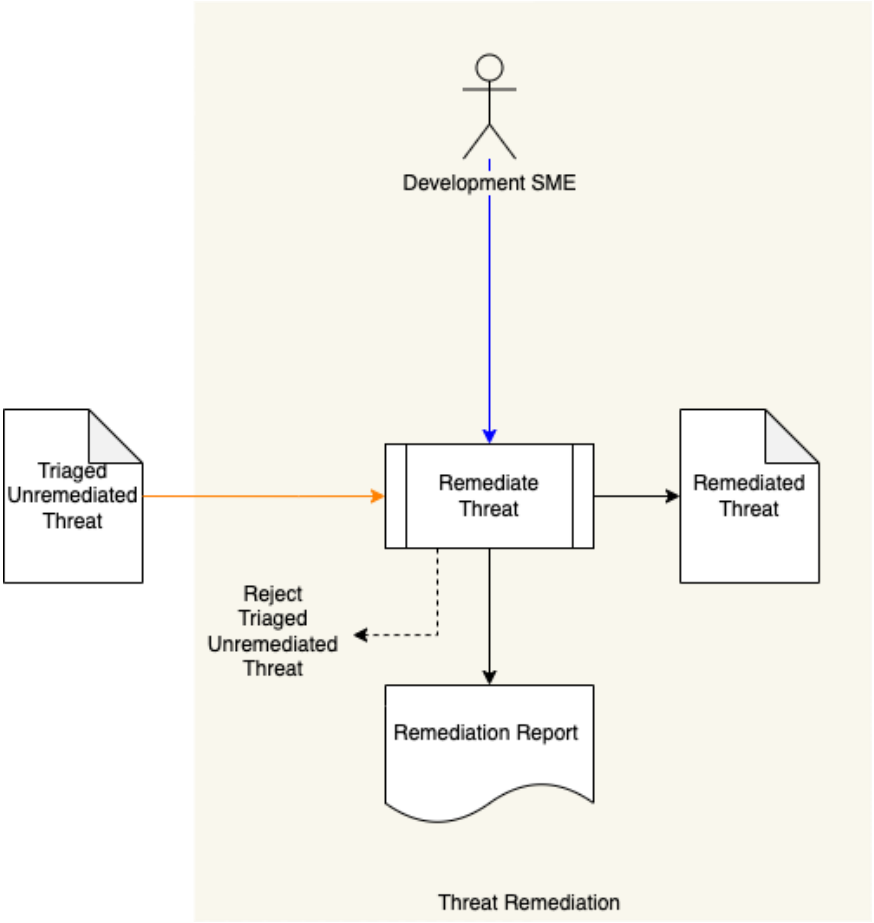
| | |
|---|---|
| **Inputs** | Unremediated Threat |
| **Outputs** | Triaged Unremediated Threat |
| **Participants** | Development Team |




The Development Team triages the **Unremediated Threat**. If the threat is determined to be non-impactful, a **Rejected Unremediated Threat** notification is sent. Otherwise, a **Triaged Unremediated Threat** is generated.

# Threat Remediation

| | |
|---|---|
| **Inputs** | Triaged Unremediated Threat |
| **Outputs** | Remediated Threat<br>Remediation Report |
| **Participants** | Development SME |

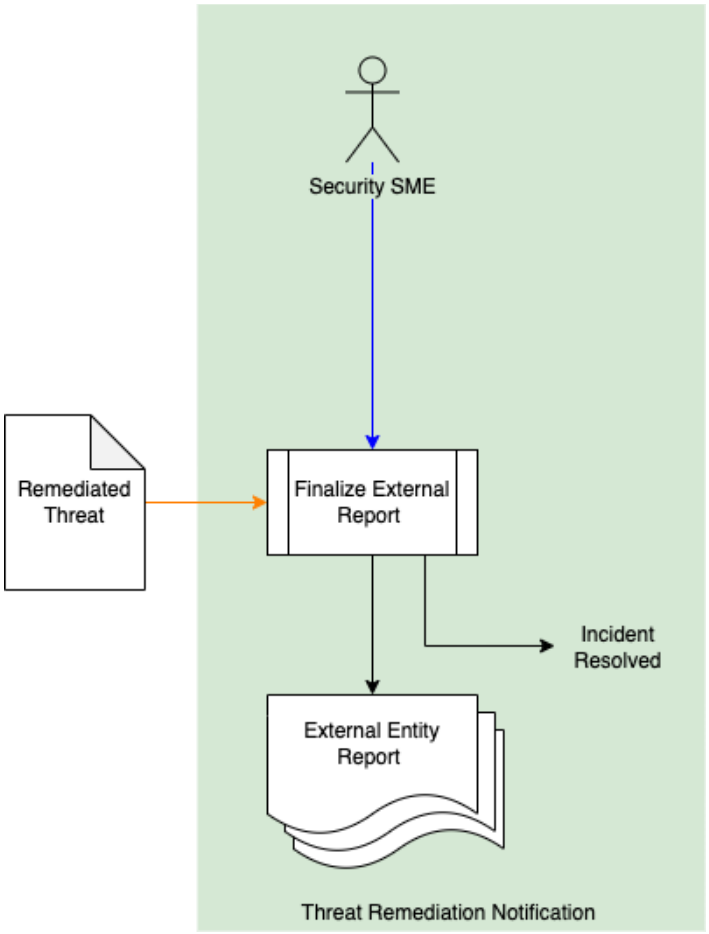



The Development SME attempts to remediate the threat and a **Remediation Report** will be generated. If the threat cannot be remediated a **Rejected Unremediated Threat** notification is sent. Otherwise, a **Remediated Threat** is generated.

**Note:** If the threat has been determined to stem from a supplier-provided element deficiency, the Development SME shown is assumed to represent resources of the supplier.

# Threat Remediation Notification

| | |
|---|---|
| **Inputs** | Remediated Threat |
| **Outputs** | External Entity Report |
| **Participants** | Security SME |




Using the **Remediated Threat**, the Security SME generates the final **External Entity Reports**. An **Incident Resolution** notification is generated and sent to the original incident reporter.

# References


1. **Incident Monitoring Summary (**AVCDL tertiary document**)**
2. **Vulnerability Report (**AVCDL tertiary document**)**
3. **Threat Prioritization Plan (**AVCDL secondary document)
4. **Computer Security Incident Handling Guide**
   **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf**
5. **Incident Handler's Handbook**
   **https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901**
6. **Threat Report (**AVCDL secondary document**)**
7. **ISAC Report**
   **https://www.cisecurity.org/isac/report-an-incident/**
8. **CVE Report**
   **https://cve.mitre.org/cve/request_id.html#cna_participants**
9. **Root Cause Report (**AVCDL tertiary document**)**
10. **NIST SP800-126r3 The Technical Specification for the Security Content Automation Protocol (SCAP) v1.3**
    **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf**
11. **Component / Version – Product / Version Cross-reference Document (**AVCDL secondary document)
12. **Cybersecurity Monitoring Plan (**AVCDL secondary document)
13. **Design Showing Security Considerations (**AVCDL secondary document)
14. **Product-level Security Requirements (**AVCDL secondary document)
15. **OASIS Common Security Advisory Framework (CSAF)**
    **https://oasis-open.github.io/csaf-documentation/**