Incident Response Plan

Revision

Version 8
12/13/21 1:01 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

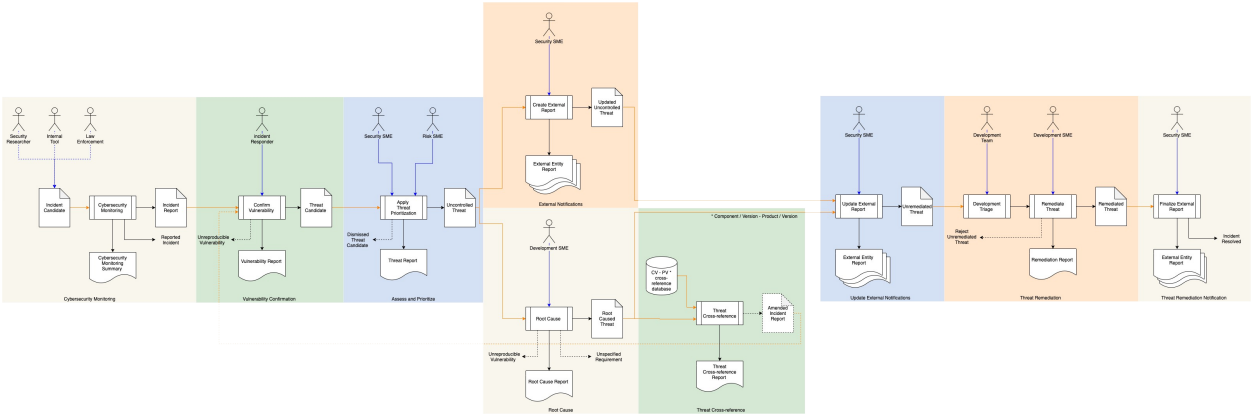
This document is motivated by the need to have formal processes in place for the management of incidents affecting safety-critical, cyber-physical systems in the field for certification of compliance to standards such as ISO 21434 and 26262.

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:

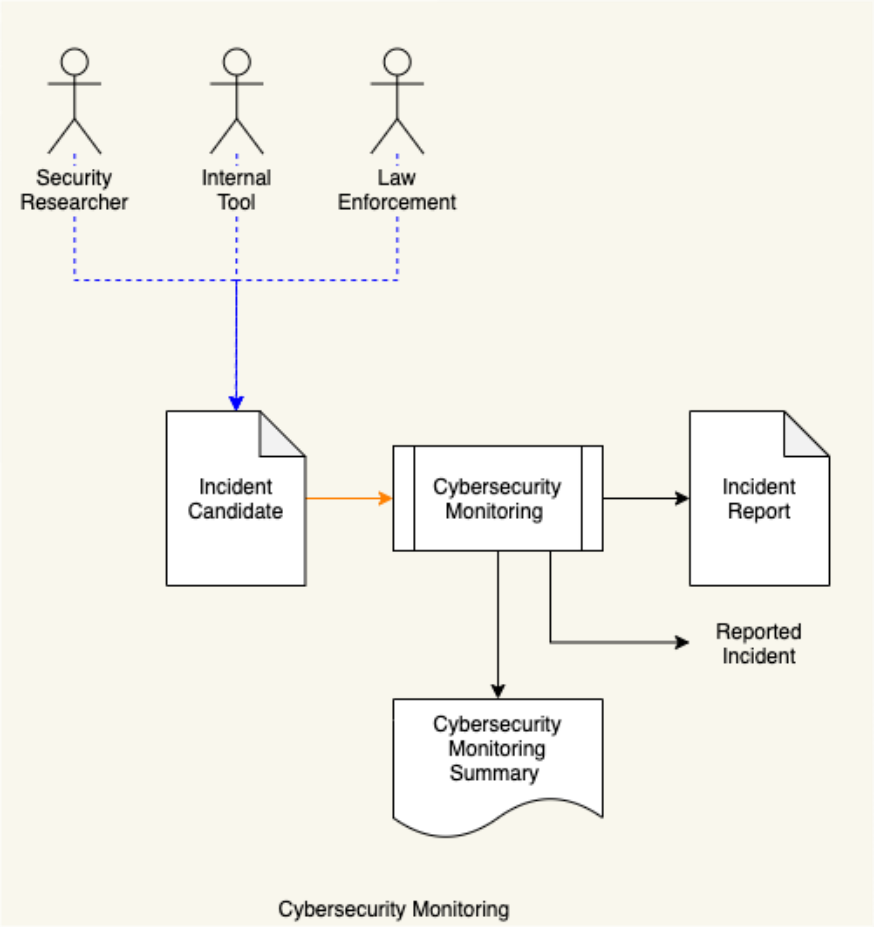


Note: Throughout this document threats shown as both inputs and outputs of various processes. These may be separate artifacts within the incident response system, but more commonly they represent different fields within the same issue response system database entry.

Process

Cybersecurity Monitoring

Inputs	Incident Candidate
Outputs	Incident Report Incident Monitoring Summary
Participants	Internal Tools (optional) Security Researcher (optional) Law Enforcement (optional)



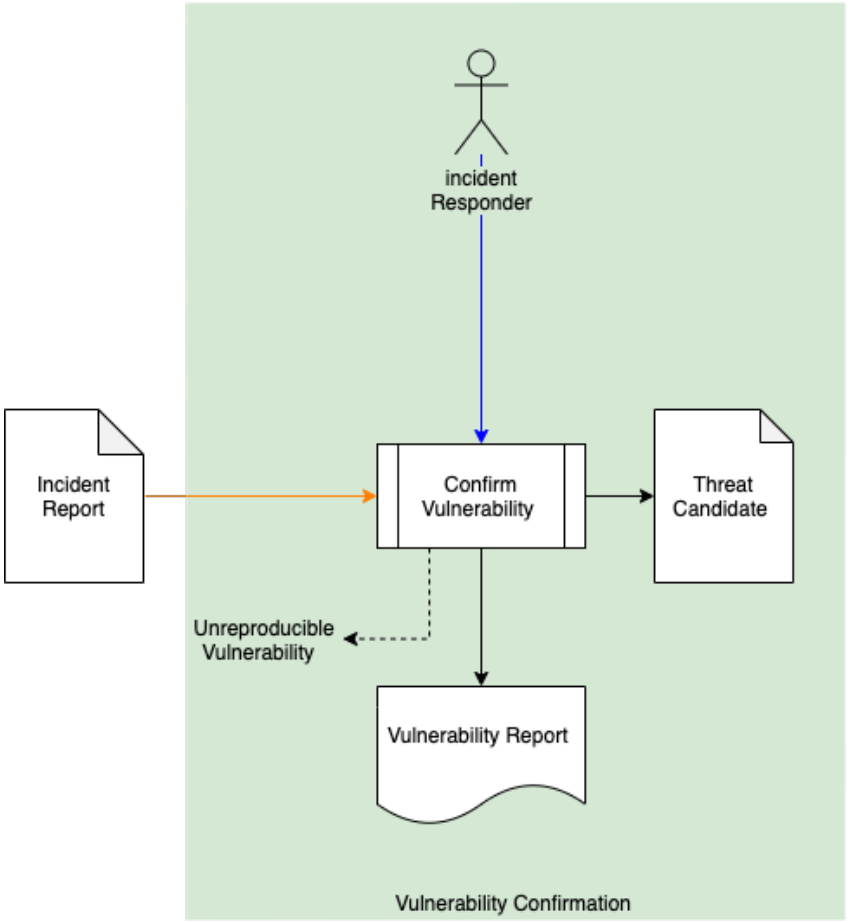
The incident monitoring process (see **Cybersecurity Monitoring Plan** [12]) detects a new **Incident Candidate** from internal tooling, law enforcement, or an independent researcher. The incident monitoring process then generates an **Incident Report** and a **Reported Incident** notification is sent.

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
Outputs	Threat Candidate Vulnerability Report
Participants	Incident Responder



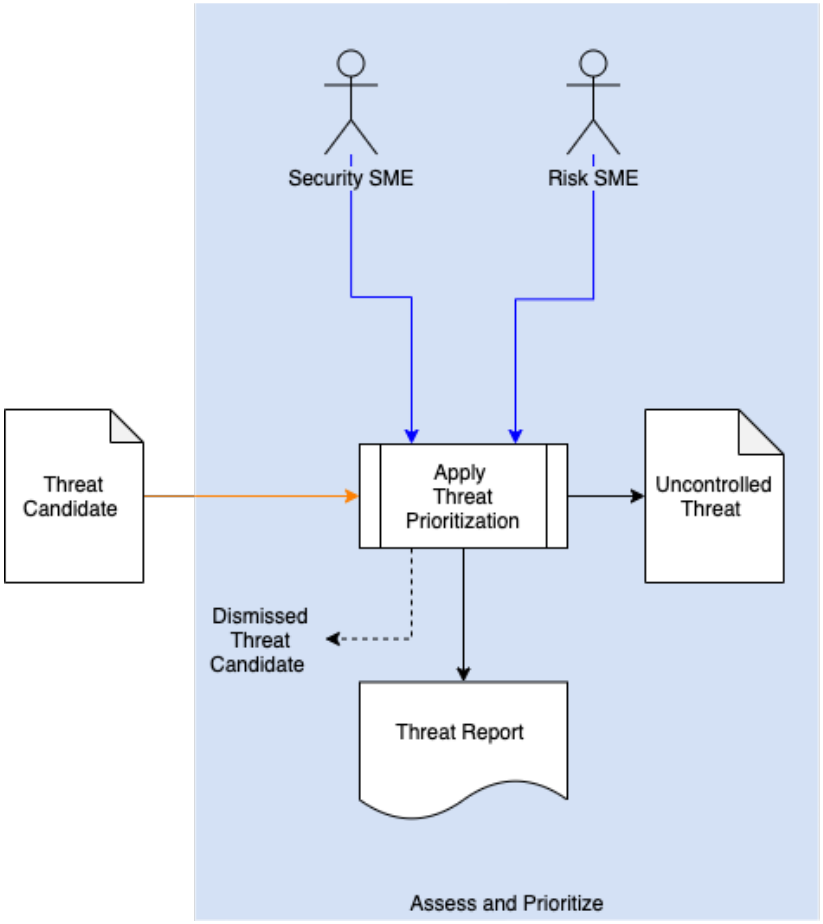
When an **Reported Incident** notification is received, an incident responder will attempt to confirm the vulnerability described in the **Incident Report** and will create a **Vulnerability Report** documenting their findings.

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 Threat Report
Participants	Security SME 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 with be generated.

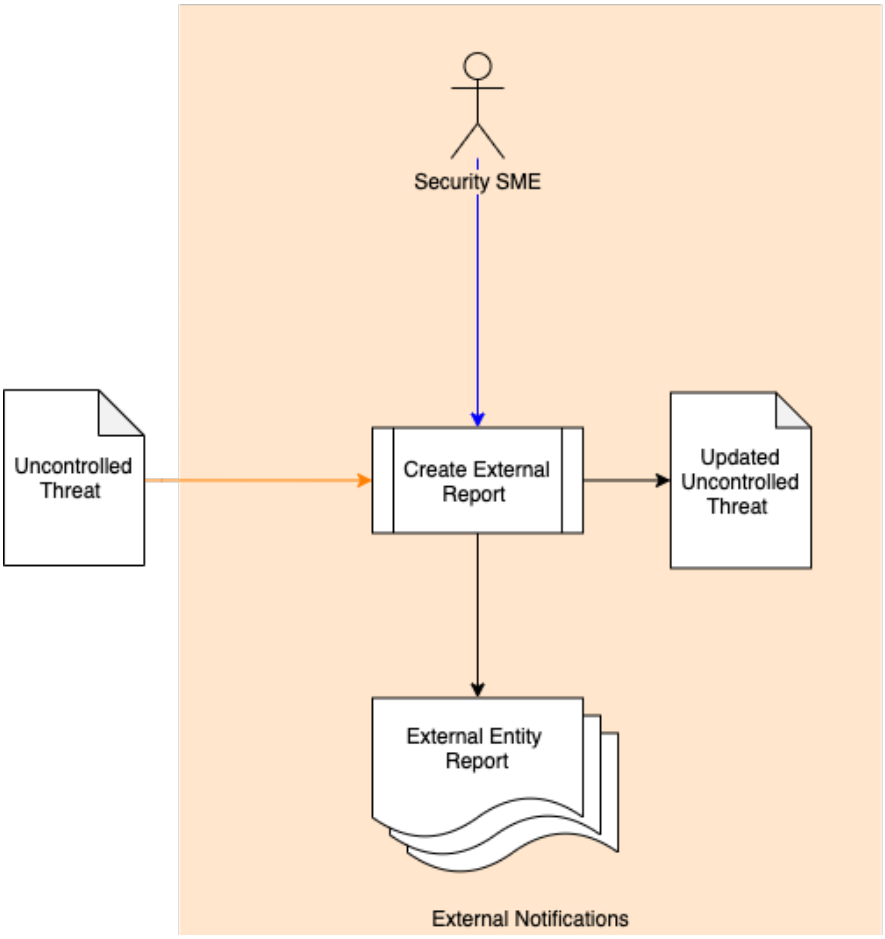
If the threat is determined to be controlled a **Dismissed Threat Candidate** notification will be generated.

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 External Entity Report
Participants	Security SME



With the **Uncontrolled Threat** the Security SME generates **External Entity Reports** based on the findings. **SCAP** [10] is the preferred encoding for these reports.

Typical reports are:

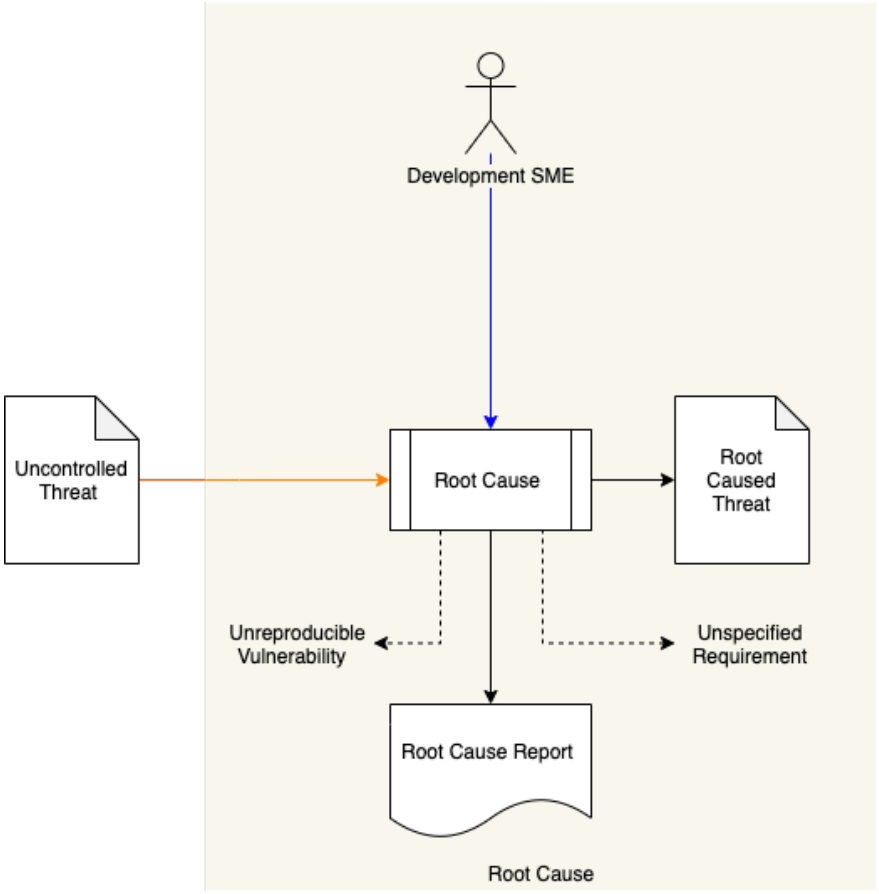
- Information Sharing and Analysis Center (ISAC) Report
- Common Vulnerability and Exposure (CVE) Report

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 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.

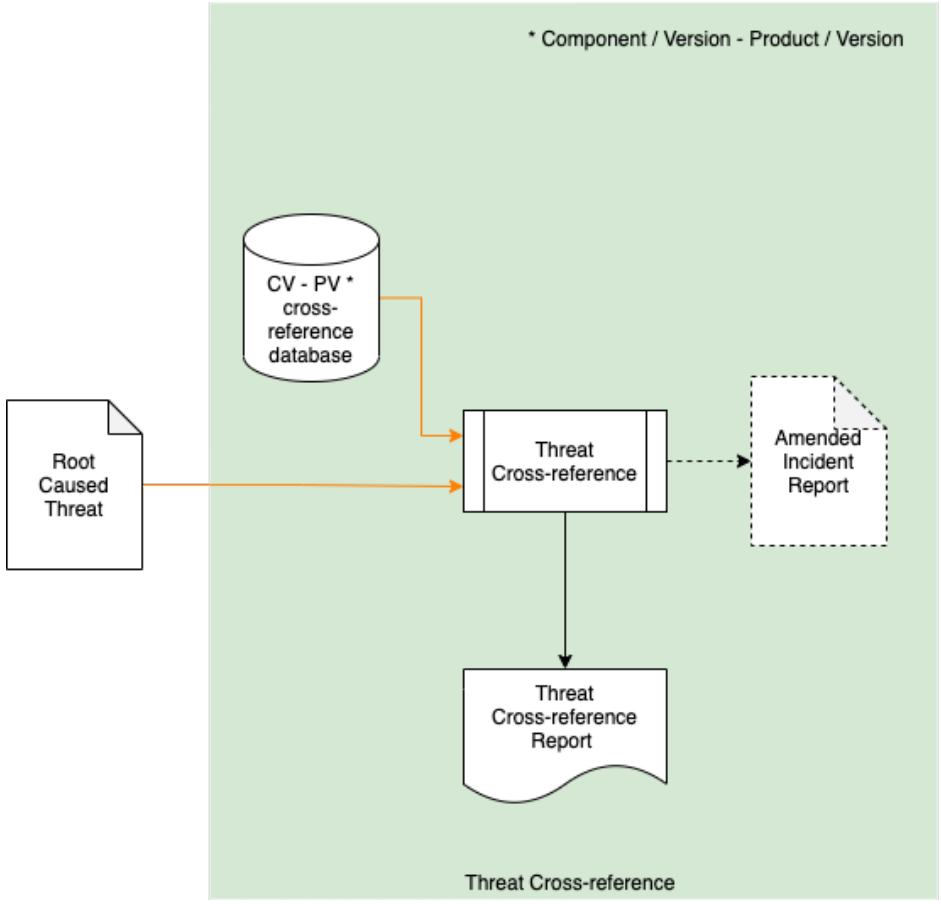
If the vulnerability is unreproducible, an **Unreproducible Vulnerability** notification will be generated. If the vulnerability is reproducible, a **Root Caused Threat** is produced.

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 to the by either the **Design Showing Security Considerations** [13] (requirement exists) or **Product-level Security Requirements** [14] (requirement does not exist) process.

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

Threat Cross-reference

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



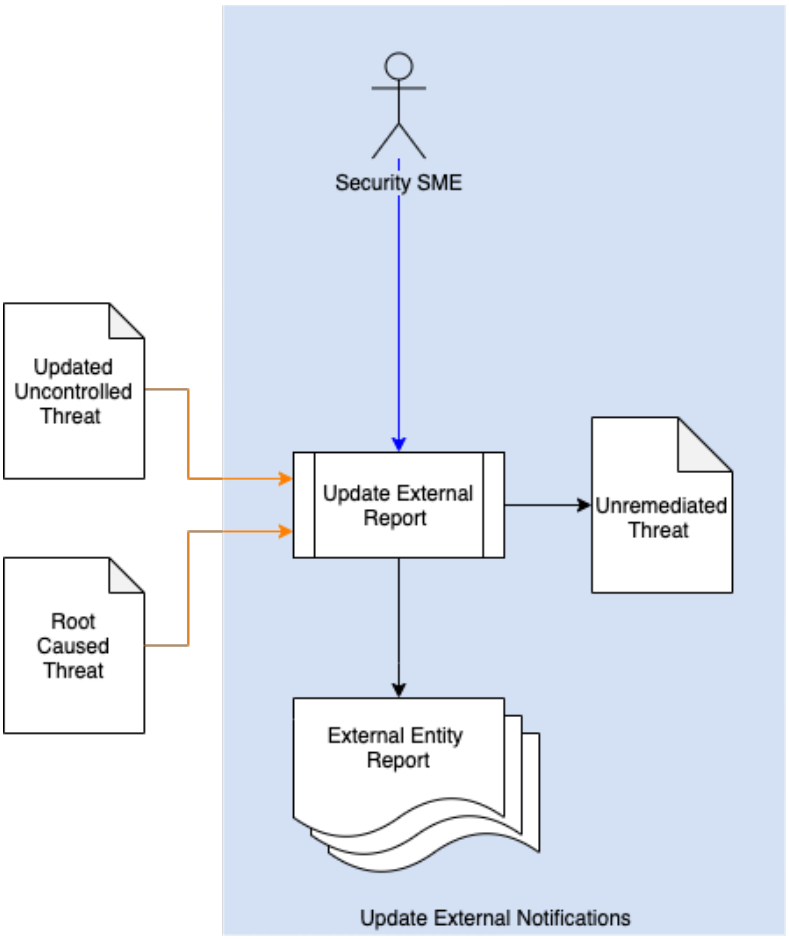
The **Root Caused Threat** is checked against the **Component / Version – Product / Version Cross-reference Database** (see **Component / Version – Product / Version Cross-reference Document** [11]). If any other elements are impacted, an **Amended Incident Report** including all impacted components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

A **Threat Cross-reference Report** will be generated.

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

Update External Notification

Inputs	Root Caused Threat Updated Uncontrolled Threat
Outputs	Unremediated Threat Updated External Entity Reports
Participants	Security SME

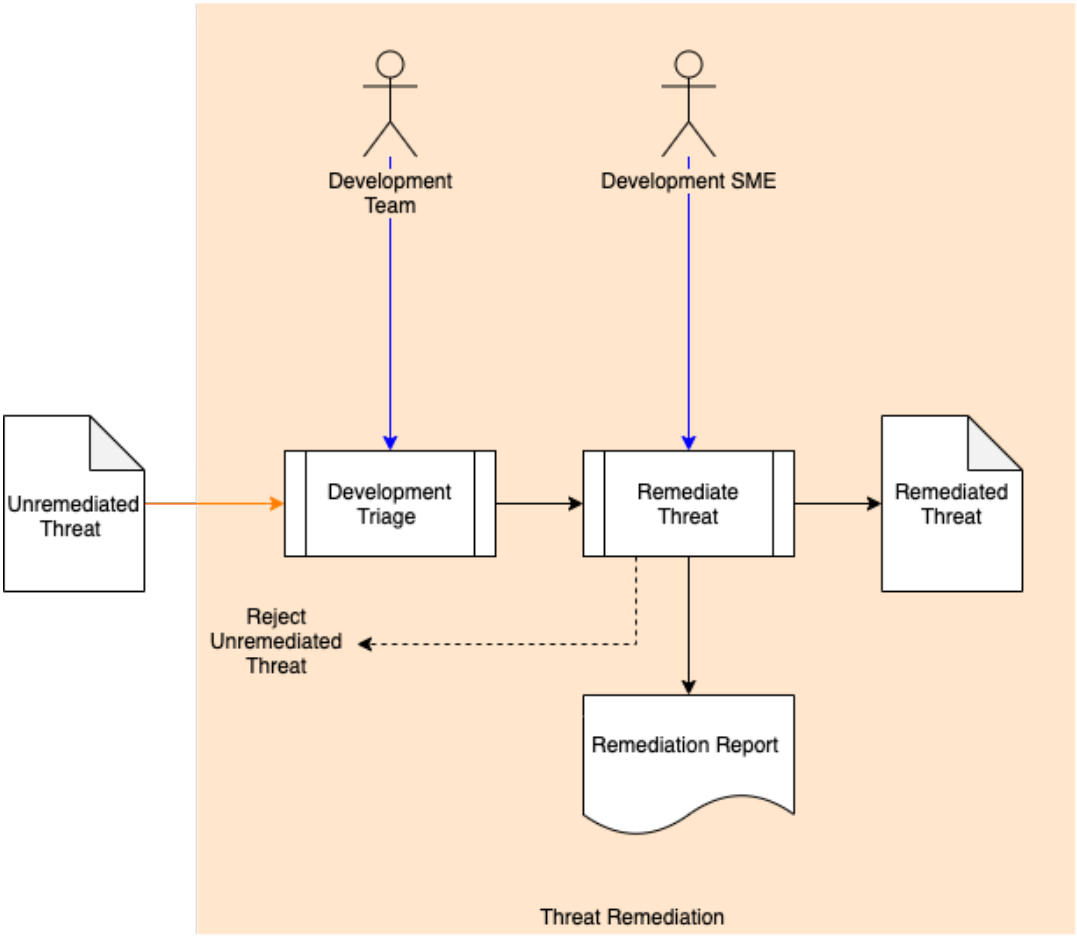


Using the information from the **Root Caused Threat** and **Updated Uncontrolled Threat** an updated set of **External Entity Reports** is generated.

An **Unremediated Threat** is generated.

Threat Remediation

Inputs	Unremediated Threat
Outputs	Remediated Threat Remediation Report
Participants	Development Team Development SME



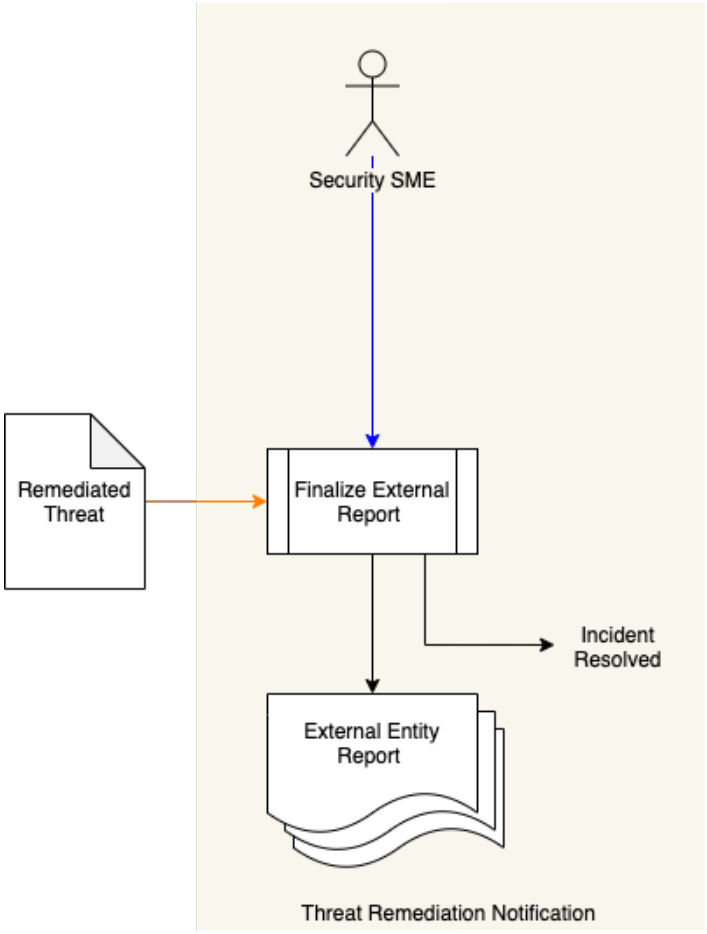
The Development Team triages the **Unremediated Threat**. The Development SME attempts to remediate the threat and a remediation report will be generated.

If the threat cannot be remediated a **Rejected Unremediated Threat** notification is sent.

If the threat can be remediated, a **Remediated Threat** is generated.

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)