Cybersecurity Incident Report

Revision

Version 1
1/27/22 2:54 PM

SME

Charles Wilson

Abstract

This document describes the process used to create a cybersecurity incident report.

Group / Owner

Security / Cyber Defense Incident Responder, Cyber Defense Forensics Analyst

Motivation

This document is motivated by the need to have formal processes in place to manage any security incidents which may have impact on safety-critical, cyber-physical systems for certification of compliance to standards such as ISO 21434 and 26262.

License

Overview

A cybersecurity incident report is the culmination of a series of activities. There will be times when the report is abbreviated as one or more of the possible activities may be determined as unnecessary. In its most expansive form, the following activities all take place:

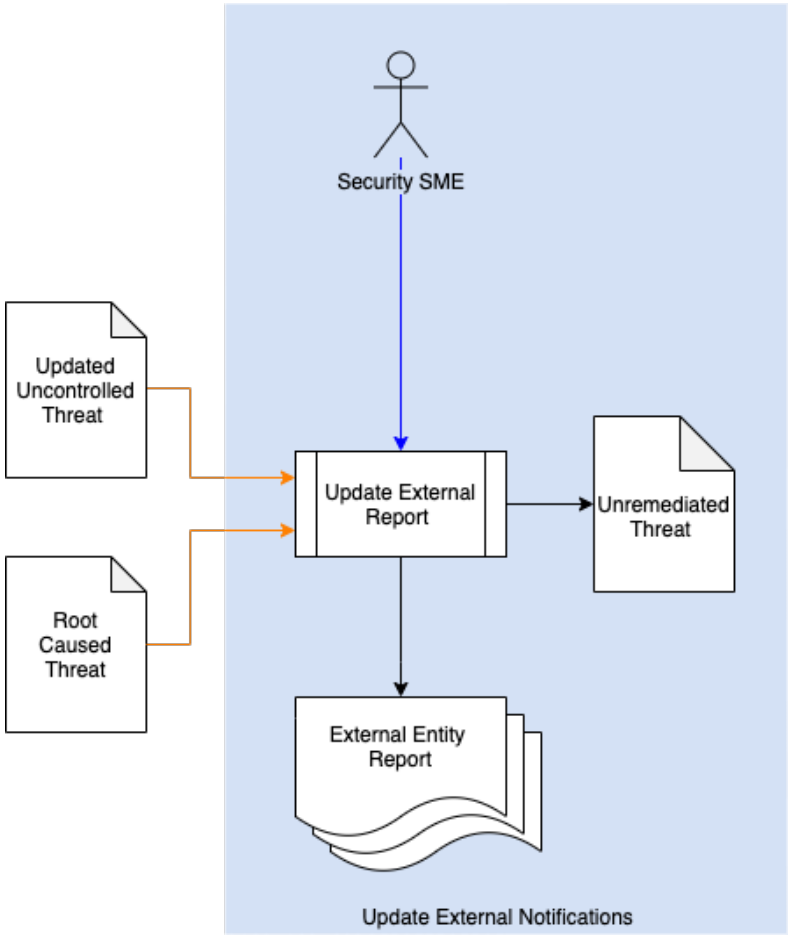
1. Identification and Confirmation
2. Assessment and Prioritization for Remediation
3. Determining the Root Cause
4. Information Sharing

These activities are typically performed sequentially, with the exception of information sharing.

Note: More details regarding the overall incident response process can be found in the **Incident Response Plan** [1].

Process

As shown in the **Incident Response Plan**, the cybersecurity incident report is an evolving document whose data manifests in multiple forms. The following workflow stage is taken from that document.



Here we see generation of one or more **External Entity Reports** based on the root causing of the identified uncontrolled threat.

Report Composition

The content of the cybersecurity incident report is fully documented in the NIST **Security Content Automation Protocol (SCAP)** [4, 5] documentation. This is the current standard for ingest by external entities. The more recent **Common Security Advisory Framework (CSAF)** [3] also provides a format which is easily exchanged. It has the advantage of being embodied as JSON rather than XML and providing validation code.

Note: In addition to machine-readable encoding, a human-readable format should strongly be considered.

References

1. **Incident Response Plan** (AVCDL secondary document)
2. NIST SP 800-150 ***Guide to Cyber Threat Information Sharing***
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
3. **Common Security Advisory Framework Version 2.0 draft 1 (CSAF)**
   https://docs.oasis-open.org/csaf/csaf/v2.0/csd01/csaf-v2.0-csd01.pdf
4. **The Technical Specification for the Security Content Automation Protocol (SCAP)**
   https://csrc.nist.gov/publications/detail/sp/800-126/rev-3/final
5. **Security Content Automation Protocol (SCAP) Version 1.2 Content Style Guide (Draft)**
   https://csrc.nist.gov/publications/detail/nistir/8058/draft