Understanding Workflow Graphs

Revision

Version 2
5/26/21 4:10 PM

Author

Charles Wilson

Abstract

This document describes the symbology and intent behind the AVCDL secondary document workflow graphs.

Document Status

Pending certification body review

License

Overview

The AVCDL secondary document workflow graphs are intended to concisely convey artifacts, actors, activities, reports, data stores, and notifications comprising various AVCDL phase requirement processes. It visualizes this through use of a forward dependency graph showing the relationship between the various elements. It also conveys a sense of the discrete steps, actors, inputs and outputs through color coding. Line-style allows for depiction of optional and mandatory flows. This visualization is implemented using ISO 5807 (flowchart) symbology [1, 3] with a few additions. This visualization also allows us to see the inherent parallelism present within the process.

Step Encapsulation

Each process workflow is broken into a series of steps. The activities and products of each step in the process are enclosed in tinted rectangles labeled with their activity name at the bottom center of the rectangle. Inputs coming from previous steps are show to the left of the tinted rectangle.

The following extract shows a stage entitled “deployment payload creation.”

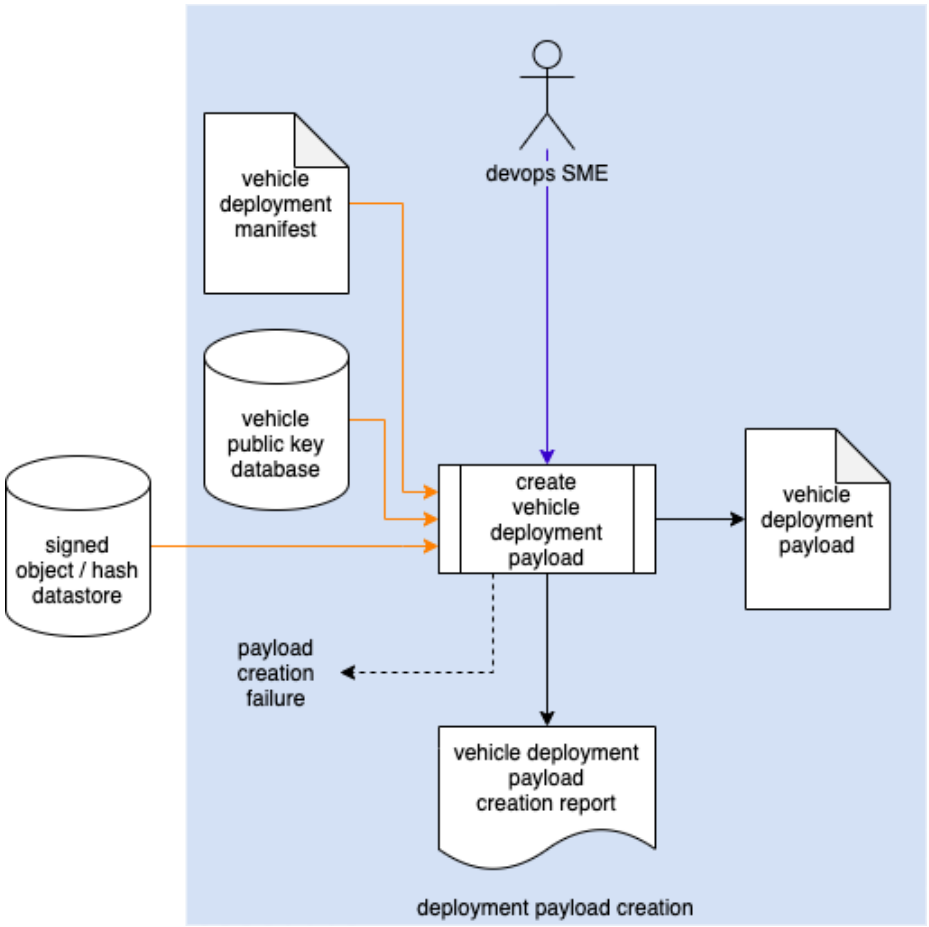

Figure 1 - Step Encapsulation

Symbology

The process workflow graph visualization uses a combination of ISO standard flowchart symbols with additional symbols denoting artifacts and actors to represent various elements. This section will elaborate on those.

Artifact

The **file icon** symbol is used to denote an artifact. This represents any artifact used as input to or produced as output from an activity. The line from the top indicates that it is produced by an activity within the step. The following extract shows that there is an activity report entitled “unremediated threat.” Note that the title is generic. The line from the left indicates that it is provided data from an activity within the step. The line from the right indicates that it is being used as the input to another step.

Figure 2 - Use of the file icon symbol to represent an artifact

Additionally, an artifact may be attributed to a specific entity. When this is the case, it is shown by an actor arrow coming into the symbol from the top. The following extract shows this.

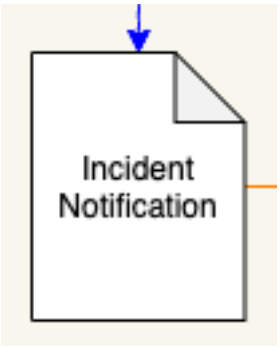

Figure 3 - Use of the file icon symbol to represent an artifact showing attribution

Activity

The ISO **predefined process** symbol is used to denote an activity. In traditional flowchart usage the predefined process would have one or more inputs and one or more outputs. For the purposes of this diagram, inputs will come from the left, outputs from the right, actors from the top, failure notifications from the bottom left, action notifications from the bottom right, and reports from the bottom center of the symbol. The title of the activity will be represented as text within the body of the symbol. The following extract shows that there is an activity which is a document entitled “create vehicle deployment payload.” It has three (3) inputs, one (1) output, is performed by one (1) actor, generates reports, and has a possible failure notification.

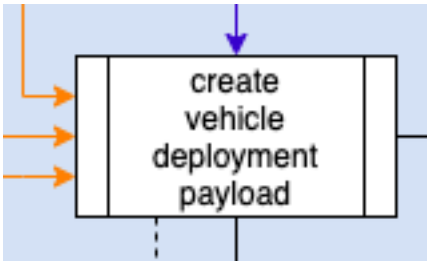

Figure 4 - Use of predefined process ISO flowchart symbol representing an activity

The following extract shows the exceptional case where the report cannot cleanly be shown coming from the bottom center of the activity. In that case, it may come from the bottom right.

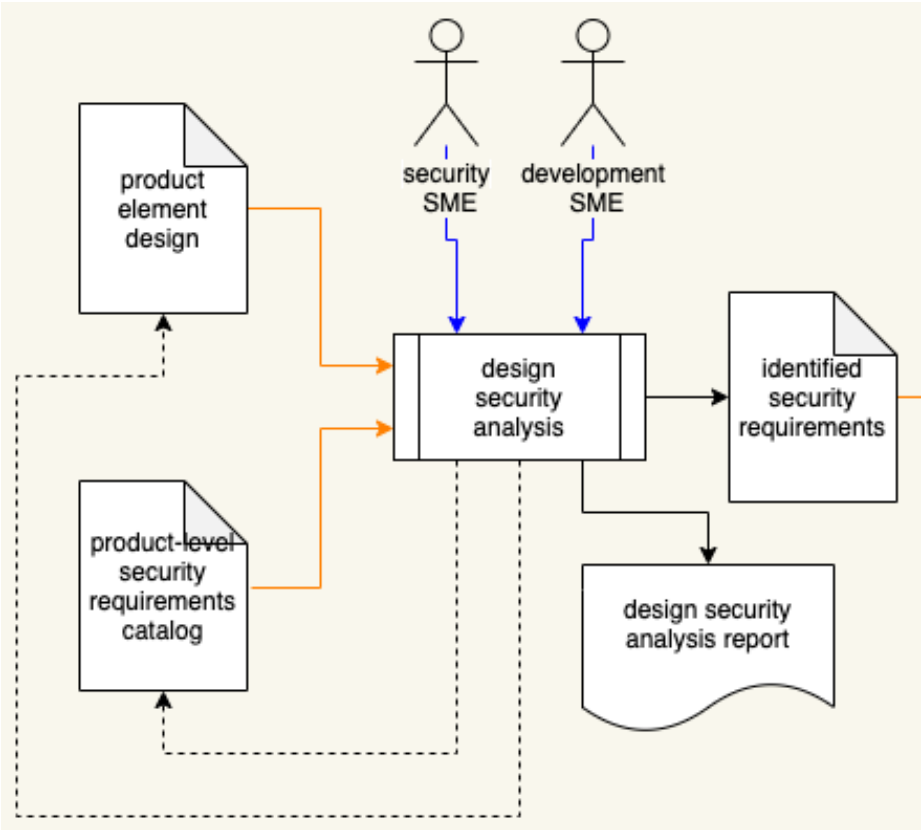

Figure 5 - Exception to report placement due to feedback

Report

The ISO **document** symbol is used to denote a report. This directly corresponds with the nature of the majority of AVCDL phase products. The line from the top indicates that it is produced by an activity within the step. The following extract shows that there is an activity report entitled “signed object ingest report.” Note that the title is generic.

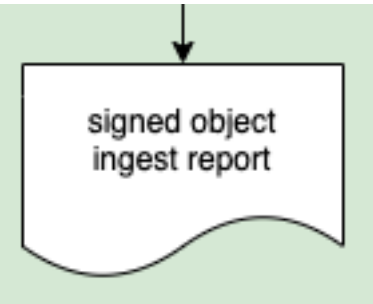

Figure 6 - Use of document ISO flowchart symbol representing a report

The following extract shows the representation of multiple reports of a type “External Entity Report” being created.

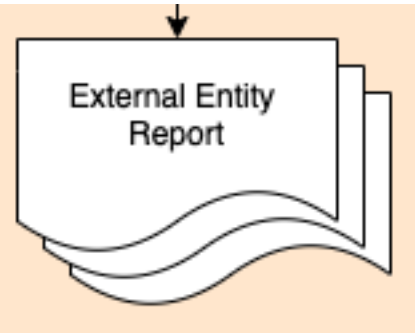

Figure 7 - Use of offset-layered document ISO flowchart symbols representing multiple reports

Data Store / Database

The ISO **data file** / **database** symbol is used to denote databases or other aggregate data stores. These are not intended to be reports, but rather data sources for other activities. The following extract shows that there is a phase product ("signed object / hash datastore") which is embodied as a database. The line from the left indicates that it is provided data from an activity within the step. The line from the right indicates that it is being used as the input to another step.

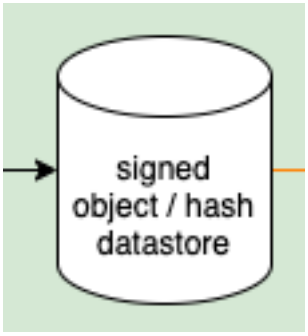

Figure 8 - Use of data file / database ISO flowchart symbol representing a data store / database

Actor

The **person** symbol is used to denote an actor. This symbol is used to show activity participant or artifact creator. An actor need not be a person, it may be a group or automated system. The following extract shows that the "Security SME" is an actor. Note that the title is generic.

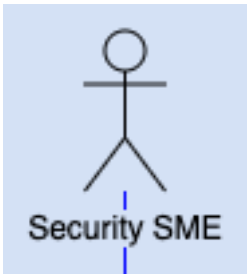

Figure 9 - Use of person symbol representing an actor

Notification

Free-floating **text** is used to denote a notification. This can either be a notification of activity failure or completion. The following extract shows that a “payload deployment failure” notification is generated by the “deploy payload” activity. Note that the titles are generic. The way the notification is handled, or the intended recipient is not specified. The dashed line is used here as a failure is not generated every time.

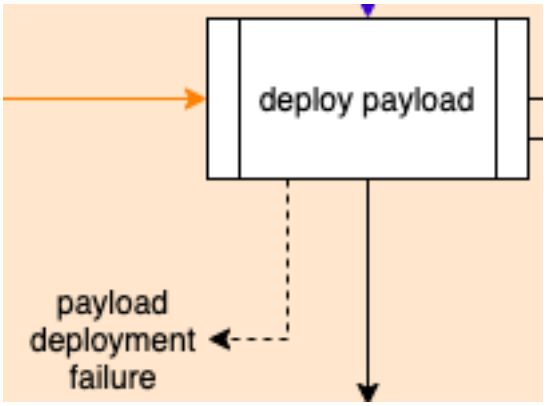

Figure 10 - Use of text representing a failure notification

The following extract shows that an “Incident Resolved” notification is generated by the “Finalize External Report” activity at its completion.

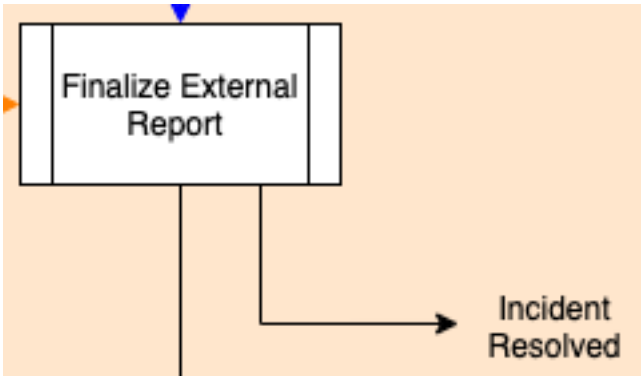

Figure 11 - Use of text representing an activity completion notification

Step Parallelism

Layout is used to denote the parallelism among steps. In the following extract we see the “External Notification” and “Root Cause” steps may be performed in parallel.

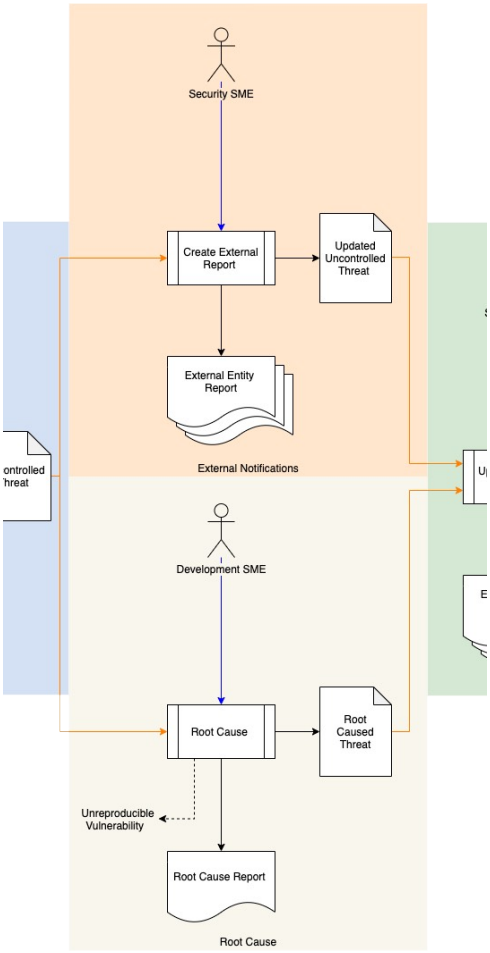

Figure 12 - Use of layout to denote parallelism in process steps

Use of Color / Style

Within the visualization there are several distinct uses of color.

Step Denotation

A primary use of color within the body of the workflow graph is to denote the individual steps. Four color are used [2]. In the following extract we see the use of these allowing us to clearly identify each step.

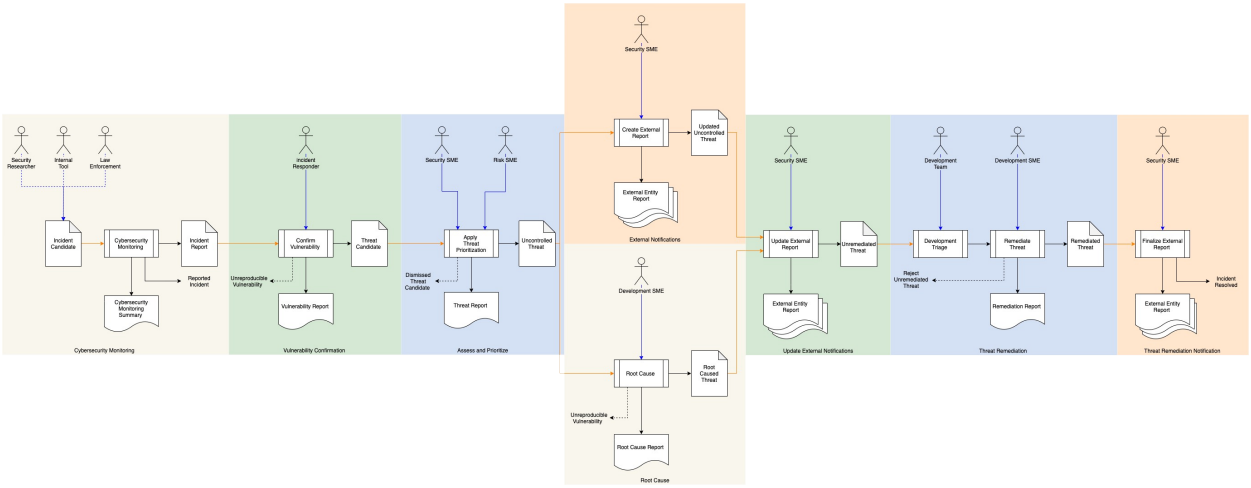

Figure 13 - Use of color to denote individual process steps

Line Color

A second use of color is to denote inputs and actors. This is shown as blue line for actors and orange lines for inputs, black for activity-generated things. The following extract shows the “Unremediated Threat” artifact as an input to the “Development Triage” activity.

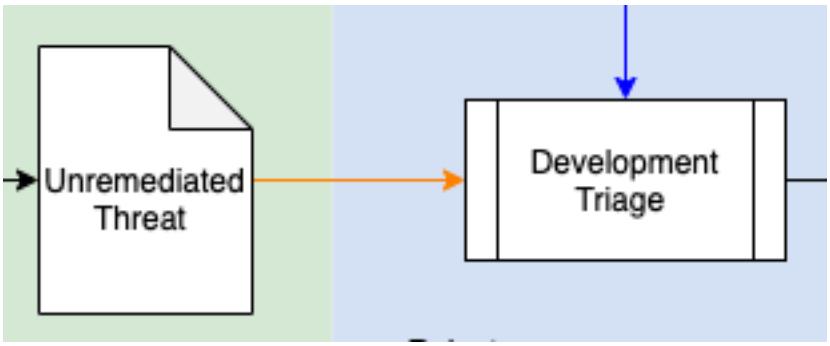

Figure 14 - Use of an orange line to activity input

The following extract shows the “Apply Threat Prioritization” activity generating the “Accepted Threat” artifact.

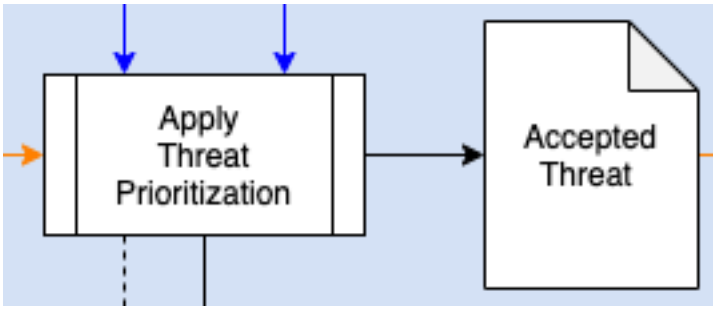

Figure 15 - Use of a black line to denote activity generated things

The following extract shows the “Development SME” actor performing the “Remediate Threat” activity.

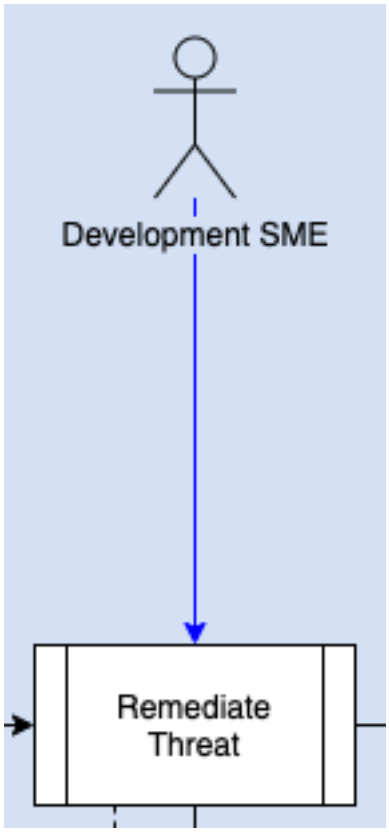

Figure 16 - Use of a blue line to denote an actor performing an activity

Line Style

Two line-styles are used. Solid lines are used for flows which are always involved. Dashed lines are used for flows which are either optional or conditional. The following extract shows a flow which always takes place between the “sign object” activity and the generated “signed object / hash archive” artifact.

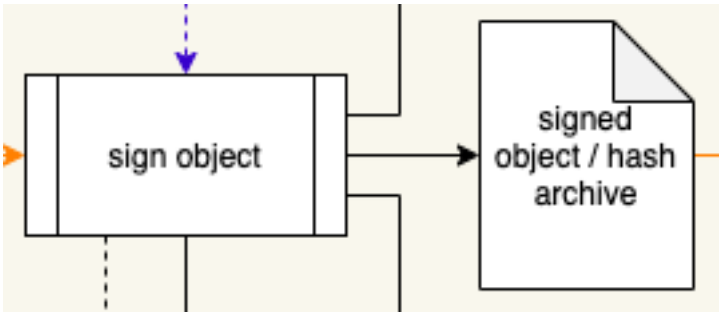

Figure 17 – Solid line use to denote an always involved flow

The following extract shows an optional flow between the “signed object ingest” activity and “ingest failure” failure notification.

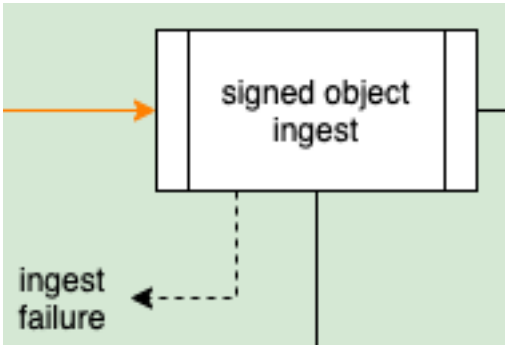

Figure 18 - Dashed line use to denote a conditional failure notification

The following extract shows an optional flow between the “design security analysis” activity and the “product-level security requirements catalog” artifact denoting an optional update.

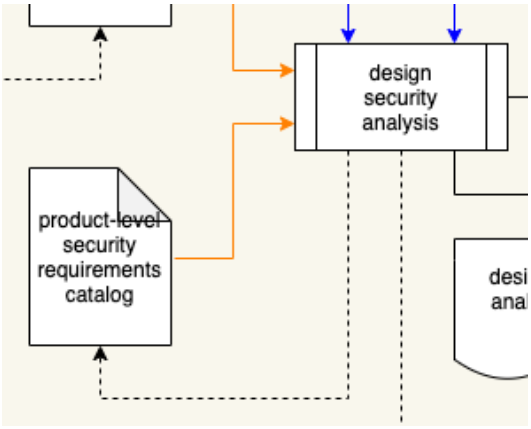

Figure 19 - Dashed line use to denote feedback from activity to artifact

The following extract shows an optional flow (attribution) between three (3) actors and the “Incident Notification” artifact. Note that the apparent solid line segment is a visual artifact.

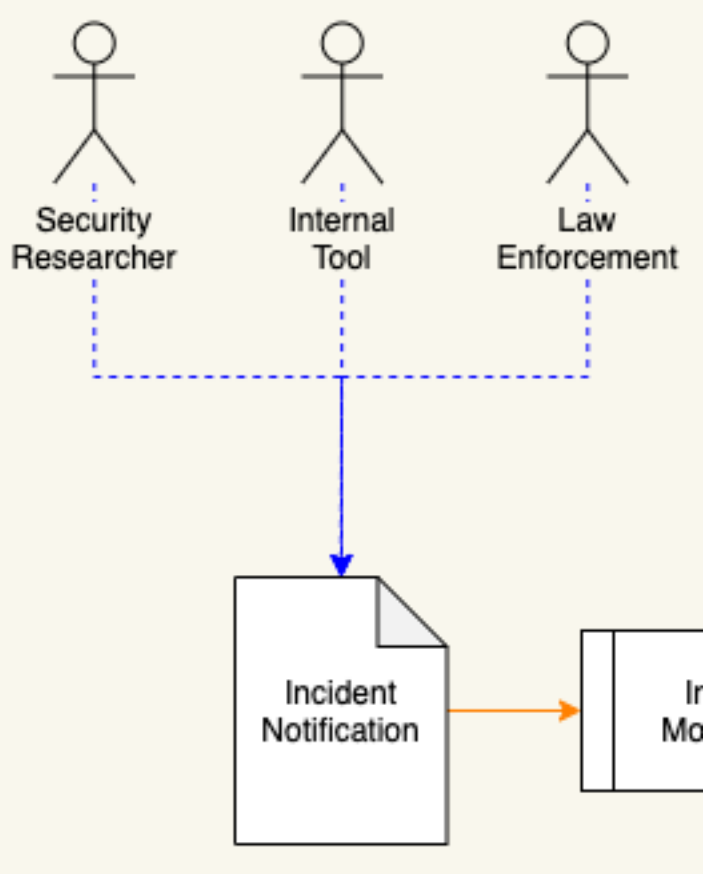

Figure 20 - Dashed line use to denote optional attribution

References

1. **Flowchart**
   https://en.wikipedia.org/wiki/Flowchart
2. **Four Color Theorem**
   https://en.wikipedia.org/wiki/Four_color_theorem
3. **ISO 5807:1985 Information processing – Documentation symbols and conventions for data, program and system flowcharts, program network charts and system resource charts**
   https://www.iso.org/standard/11955.html