Cybersecurity Monitoring Plan

Revision

Version 5
11/15/21 8:43 AM

SME

Garth Scheidemantel
Lucky Munro

Abstract

This document describes the process to monitor various sources for possible security-impacting activities and events.

Group / Owner

Security / Partner Integration Planner

Motivation

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

License

Overview

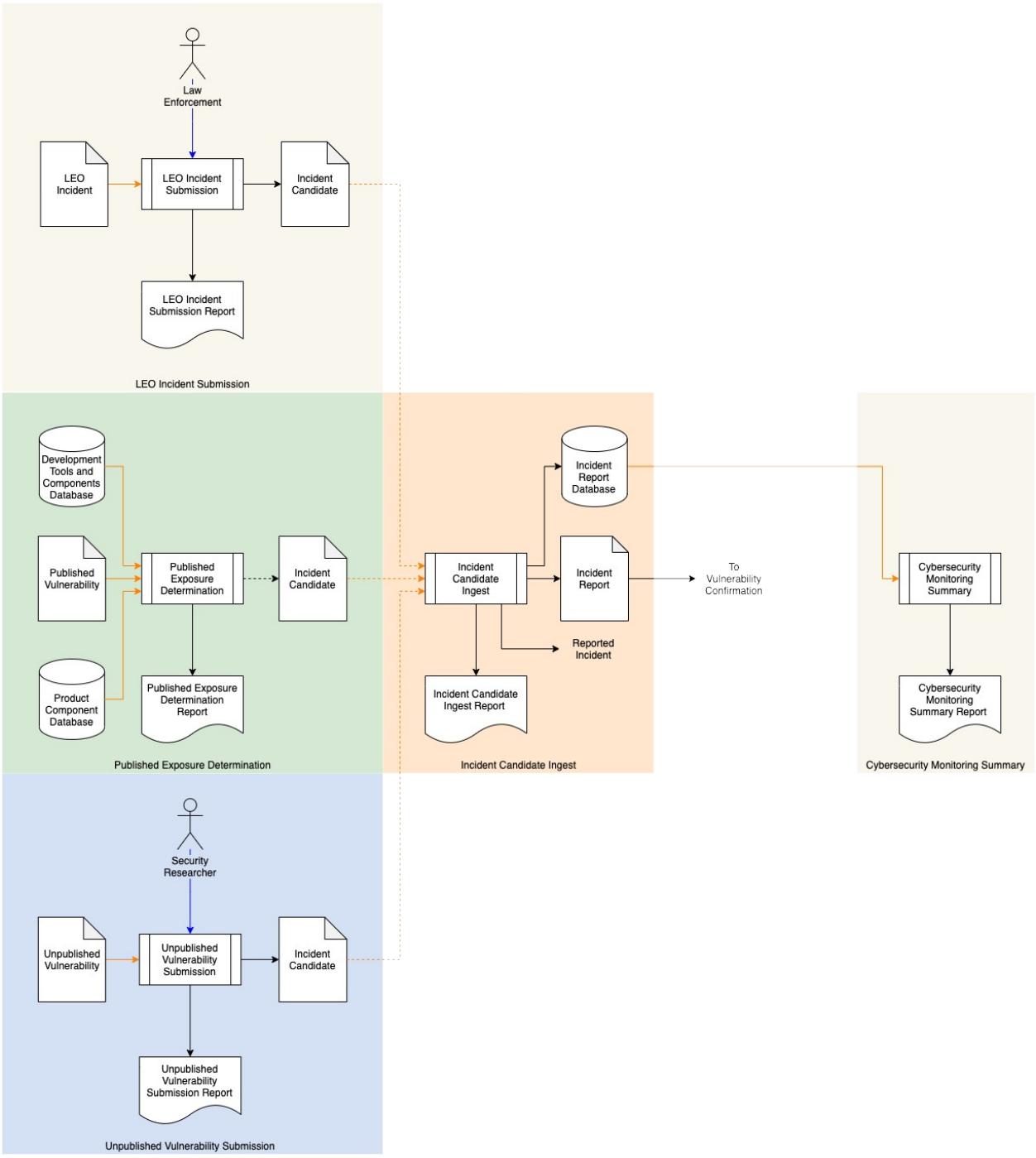
In order to reduce both the response and exposure time following a cybersecurity incident, there must be ongoing monitoring of various sources of cybersecurity intelligence. Information from those sources must be normalized, ingested, reviewed, and correlated with various tool and component information to allow for determination of the scope and criticality of the incident response needed to mitigate it.

Monitoring sources may include:

- external
    - government sources
    - commercial or non-commercial sources
    - researchers
    - organization's supply chain
    - organization's customers
- internal
    - vulnerability analysis results
    - information from the field (vulnerability scanning reports, repair information, consumer usage information)
    - configuration information (hardware / software BOM)

Note: This is not an exhaustive list.

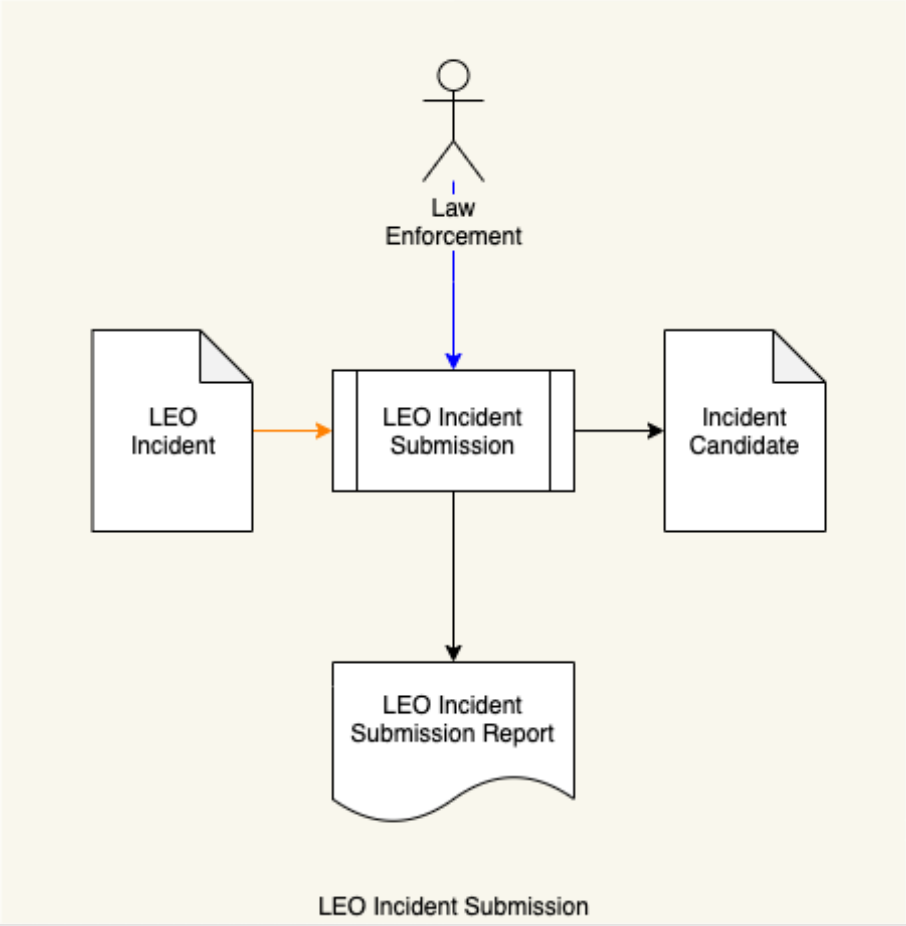
The following is the overview of the processes to ingest issues and to create cybersecurity monitoring summary reports.



Process

LEO Incident Submission

Inputs	LEO Incident
Outputs	Incident candidate LEO incident submission report
Participants	Law Enforcement

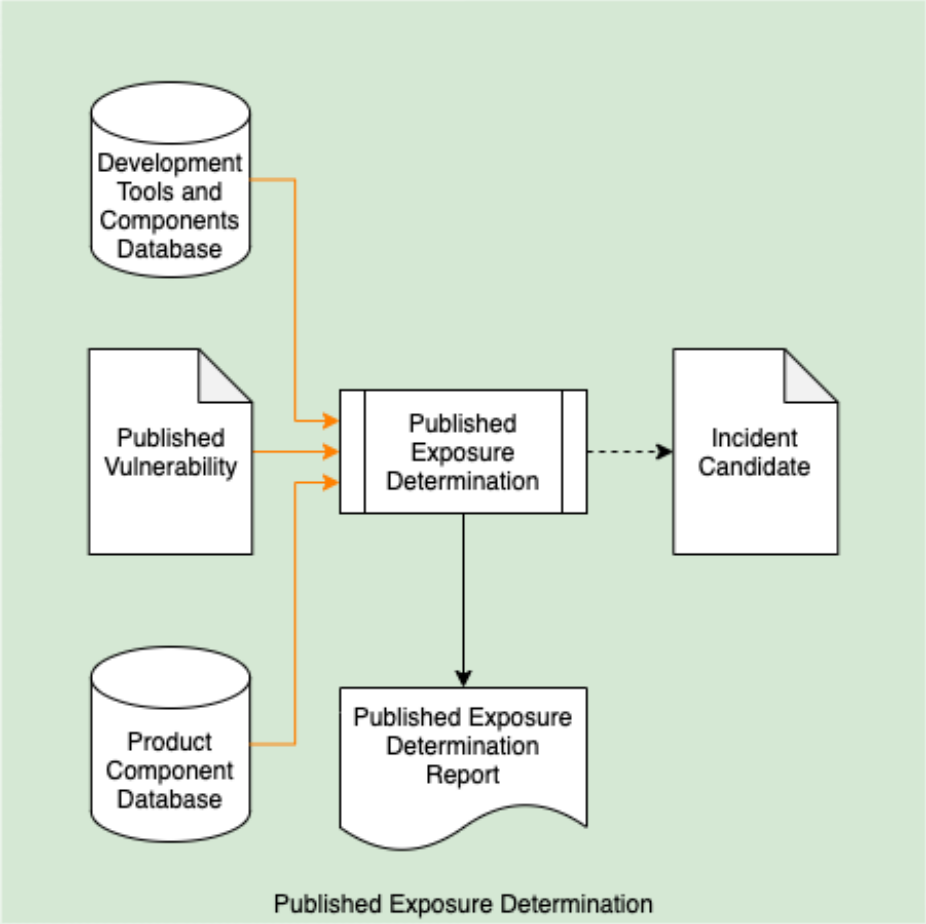


Law Enforcement submits a **LEO Incident**. The **LEO Incident** is normalized into an **Incident Candidate**. A **LEO Incident Submission Report** is generated.

Note: Details of the **Incident Candidate** are provided in the **Incident Candidate Ingest** step.

Published Exposure Determination

Inputs	Published vulnerability Development tools and components database Product component database
Outputs	Incident candidate Published exposure determination report
Participants	**none**



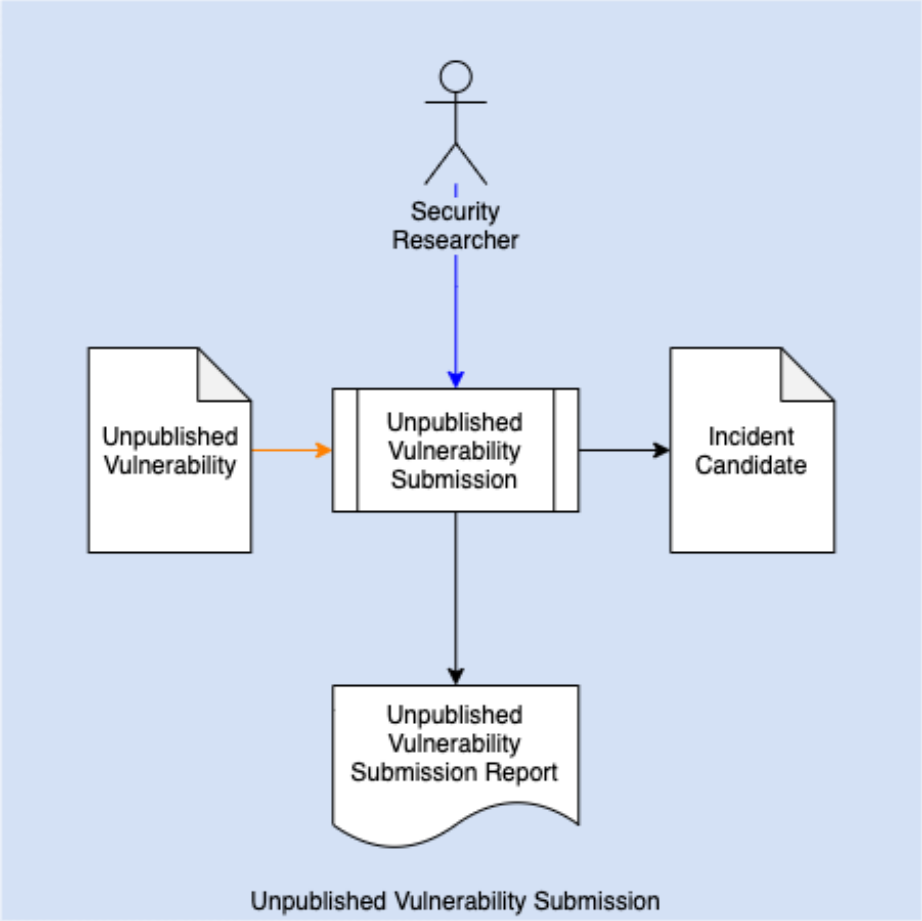
The **Published Vulnerability** is evaluated using the **Development Tools and Components Database** (see **List of Approved Tools** [10]) to determine if the vulnerability exists in any previously ingested tool or component. If the vulnerability is present there, the **Product Component Database** (see **Component / Version - Product / Version Cross-reference** [11]) is examined to determine whether it is present in any product. If a vulnerability is detected an **Incident Candidate** is generated. A **Published Exposure Determination Report** is generated.

Note: When the **Published Vulnerability** is sourced externally, the use of **SCAP** [1] encoding is recommended.

Note: Details of the **Incident Candidate** are provided in the **Incident Candidate Ingest** step.

Unpublished Vulnerability Submission

Inputs	Unpublished vulnerability
Outputs	Incident candidate Unpublished vulnerability submission report
Participants	Security researcher

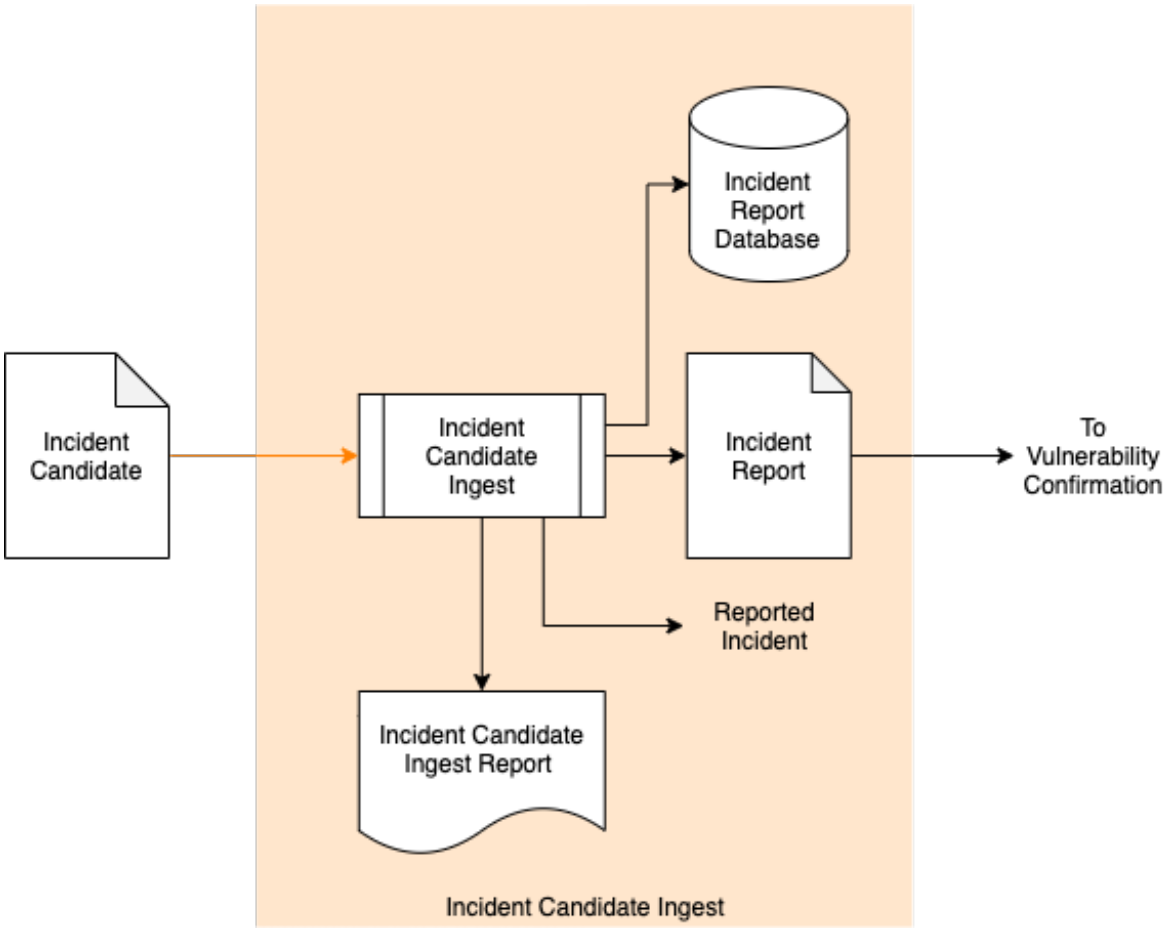


A security researcher communicates an **Unpublished Vulnerability** to the organization via a secured, well-established mechanism (encrypted email [`security@company.com`], secure file sharing site, secure web portal, …). The **Unpublished Vulnerability** is normalized into an **Incident Candidate** and **Unpublished Vulnerability Submission Report** is generated.

Note: Details of the **Incident Candidate** are provided in the **Incident Candidate Ingest** step.

Incident Candidate Ingest

Inputs	Incident candidate
Outputs	Threat candidate Incident report database Incident candidate ingest report
Participants	**none**



The **Incident Candidate** is ingested creating an **Incident Report** and an entry in the **Incident Report Database**. An **Incident Candidate Ingest Report** is generated.

A **Reported Incident** notification is generated.

Note: The **Incident Report** feeds into the **Vulnerability Confirmation** step of the **Incident Repose Plan** [3].

Incident Candidate

The **Incident Candidate** produced by any of the three input mechanisms share a single format. It is recommended that the report be encoded as a JSON file. The file should be organized into a summary and a source-specific information section.

The summary includes:

- Date / Time (ISO 8601 [9])
- Summary of incident candidate
- Reporter
  - Name (tool name where appropriate)
  - Contact information
- Incident candidate's source [**security researcher**, **internal tool**, **law enforcement**]
- Source-specific information

Law enforcement-specific information includes:

- Law enforcement case reference number
- Technical Details
- Migrations (optional)
- Resources (optional)

Internal tool-specific information includes:

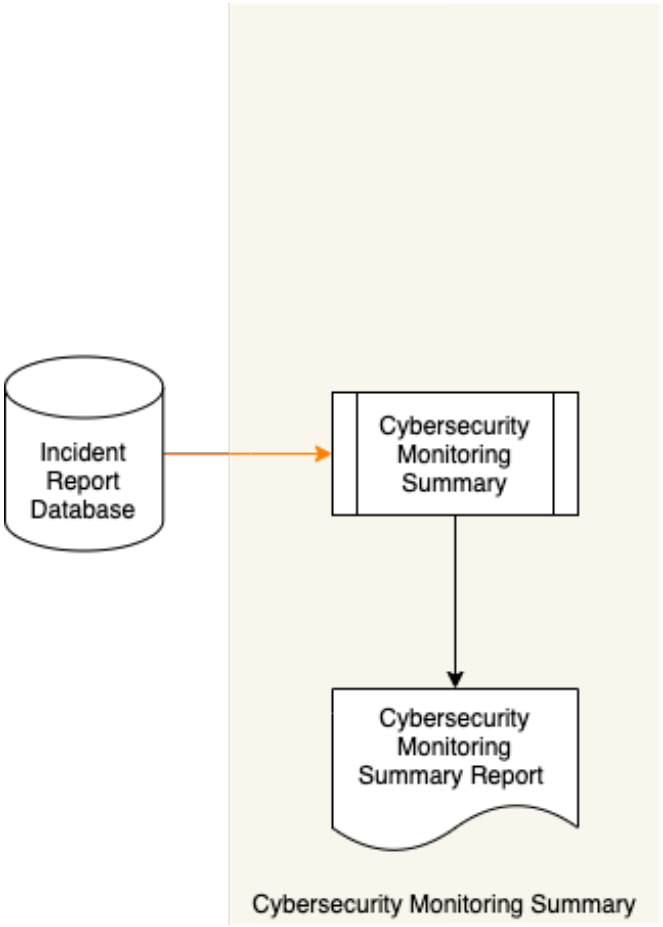
- Affected element name
- Affected element version
- Affected element URI
- URI to affected products
- Description of tool used
- Tool setting (optional)
- Tool results

Security researcher-specific information includes:

- Product name
- Vulnerability type [**spoofing**, **tampering**, **information disclosure**, **denial-of-service**, **replay attack**, …]
- Scope of exposure (optional)
- Detailed explanation of the reported vulnerability
- Instructions that demonstrate the reported vulnerability

Cybersecurity Monitoring Summary

Inputs	Incident report database
Outputs	Cybersecurity monitoring summary report
Participants	**none**



On a periodic basis, the **Incident Report Database** is queried, and a **Cybersecurity Monitoring Summary Report** is generated.

Note: The generation of a summary is typically an auditing-related activity.

References

1. **The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3**
   https://csrc.nist.gov/publications/detail/sp/800-126/rev-3/final
2. **NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations**
   https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf
3. **Incident Response Plan** (AVCDL secondary document)
4. **LEO Incident Submission Report** (AVCDL tertiary document)
5. **Published Exposure Determination Report** (AVCDL tertiary document)
6. **Unpublished Vulnerability Submission Report** (AVCDL tertiary document)
7. **Incident Candidate Ingest Report** (AVCDL tertiary document)
8. **Cybersecurity Monitoring Summary Report** (AVCDL tertiary document)
9. **ISO 8601: Data elements and interchange formats – Information interchange – Representation of dates and times**
   https://en.wikipedia.org/wiki/ISO_8601
10. **List of Approved Tools** (AVCDL secondary document)
11. **Component / Version - Product / Version Cross-reference** (AVCDL secondary document)
12. **Starting A Vulnerability Disclosure Program**
    https://developers.google.com/android/play-protect/starting-a-vdp