Leading the Future of AI

OCP APAC SUMMIT | AUGUST 11–12, 2026
TAIPEI, TAIWAN

Navigating the OCP S.A.F.E.™ Process for Vendors

Rob Wood, Managing Partner
Rickey Wang, Security Consultant

Tetrel

Leading the Future of AI

ADOPTION STORIES

Navigating the OCP S.A.F.E.™ Process for Vendors

OCP S.A.F.E.™

OCP STARTUP Member™

Tetrel

Rob Wood
Managing Partner

Rickey Wang
Security Consultant

OCP APAC SUMMIT | AUGUST 11-12, 2026
TAIPEI, TAIWAN

Outline

What is OCP S.A.F.E.™

Preparing for Security Assessment

Engagement Process

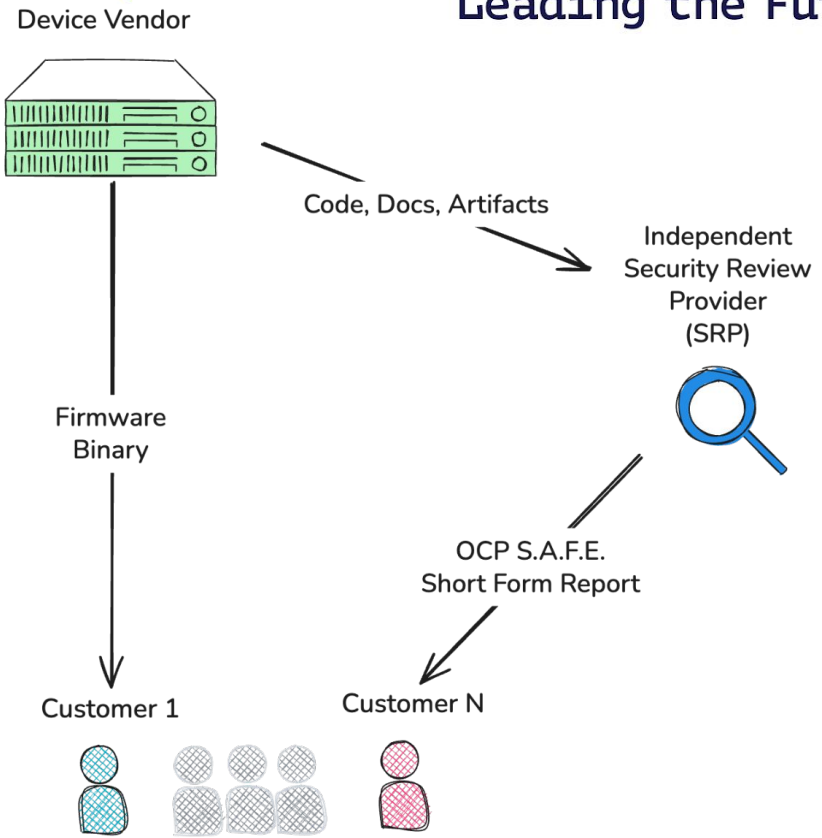
What is OCP S.O.L.I.D.

Caplitra Trademark Review

What is OCP S.A.F.E.™

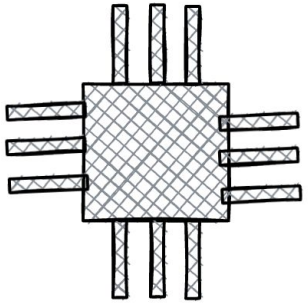
- Framework for reusable security assessments
- Produces evidence that a security review was performed
- Short-Form Report (SFR) is accepted and reusable across customers
- SFR is published to OCP S.A.F.E.™ GitHub repository

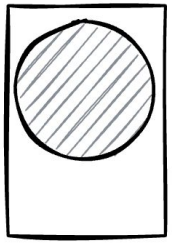
Common customer acceptance
Harmonized security standards
Transparent and verifiable



Who is OCP S.A.F.E.™ for?

- Device or firmware vendors:
  - Storage devices (SSD/HDD, NVMe, CXL, etc)
  - CPUs
  - GPUs and accelerators
  - Network devices
  - Power systems
  - Cooling systems
- UEFI vendor who requires Microsoft UEFI signing





" I have to **fix every vulnerability**,

have my flaws **published for everyone to see**,

with all the **review being done by AI**"

~~" I have to **fix every vulnerability**,~~

~~have my flaws **published for the world to see**,~~

~~with all the **review being done by AI**"~~

None of these are true!

Before you start...

- Select a Security Review Provider (SRP) from the OCP-approved list
  - Available on OCP S.A.F.E.™ Github Repo

- Engage **early** to avoid rewrites or re-spins
  - Architectural definition
  - Major milestones

- Development-phase review findings are **private**

1 - Determine Target and Scope

Joint discussion between Security Review Provider (SRP) and Vendor

(often input from Customer)

Target

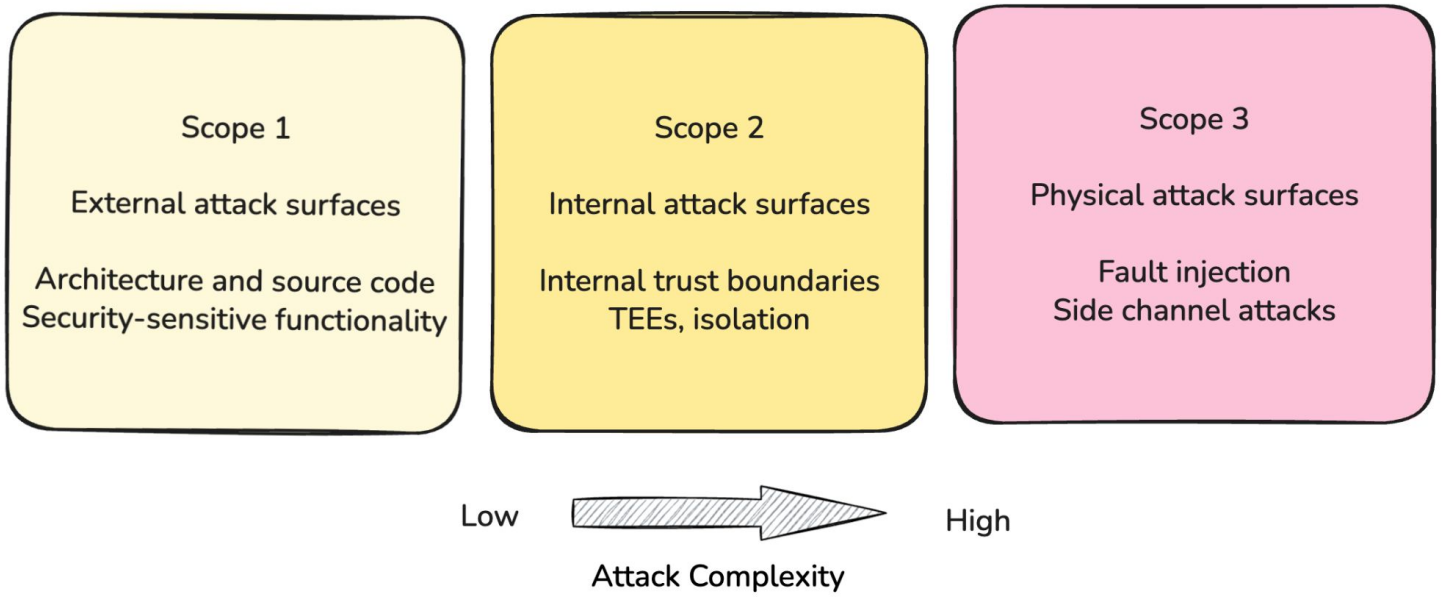
What is being tested

- What is the product, how is it used
- Hardware, ROM, Firmware?
- Third party components?

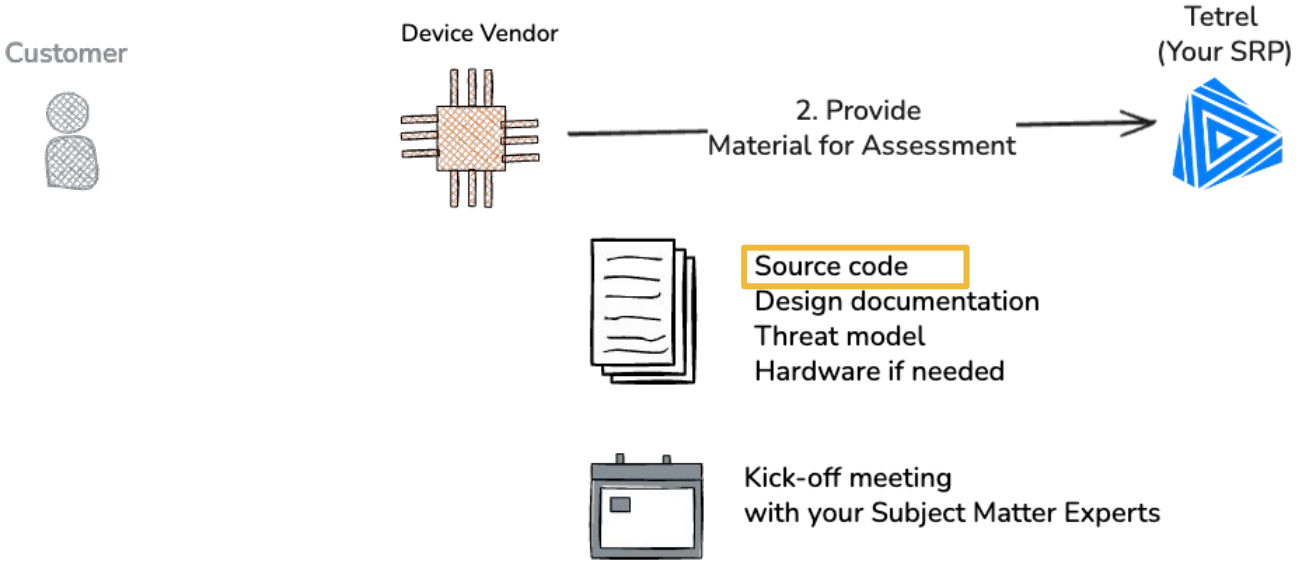
Scope

How deep is the Threat Model

OCP S.A.F.E.™ Review Scopes



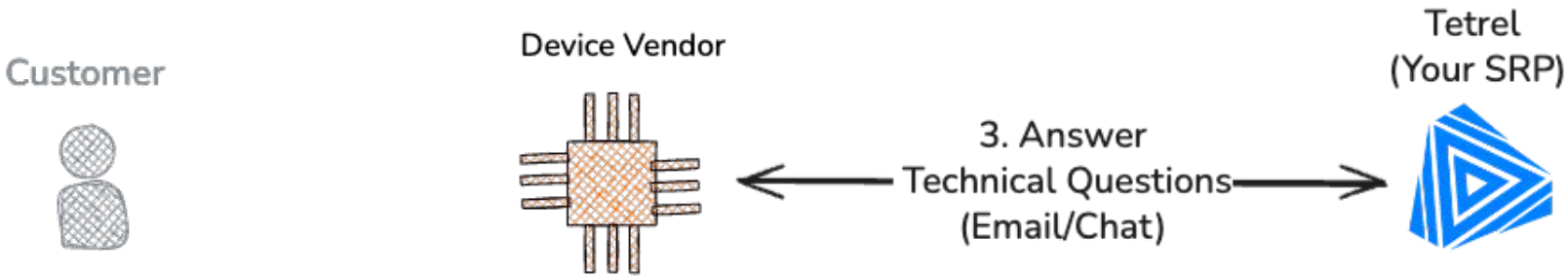
2 - Prepare Materials



SRP:
Security
Review
Provider

3 - Code Review

- Primarily manual review
- Additional LLM-assisted review (required by Jan 2027)



3 - Code Review

- Primarily manual review
- Additional LLM-assisted review (required by Jan 2027)

Human experts

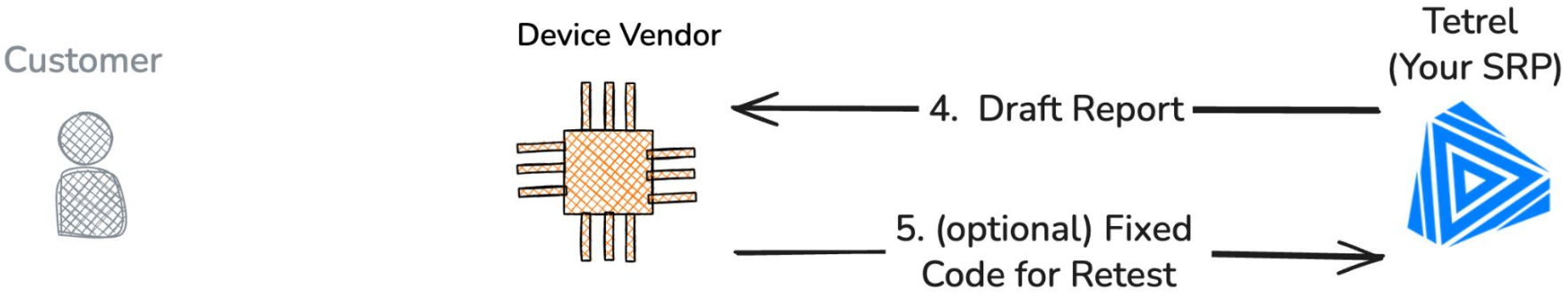
Main reviewer

LLM-assisted review

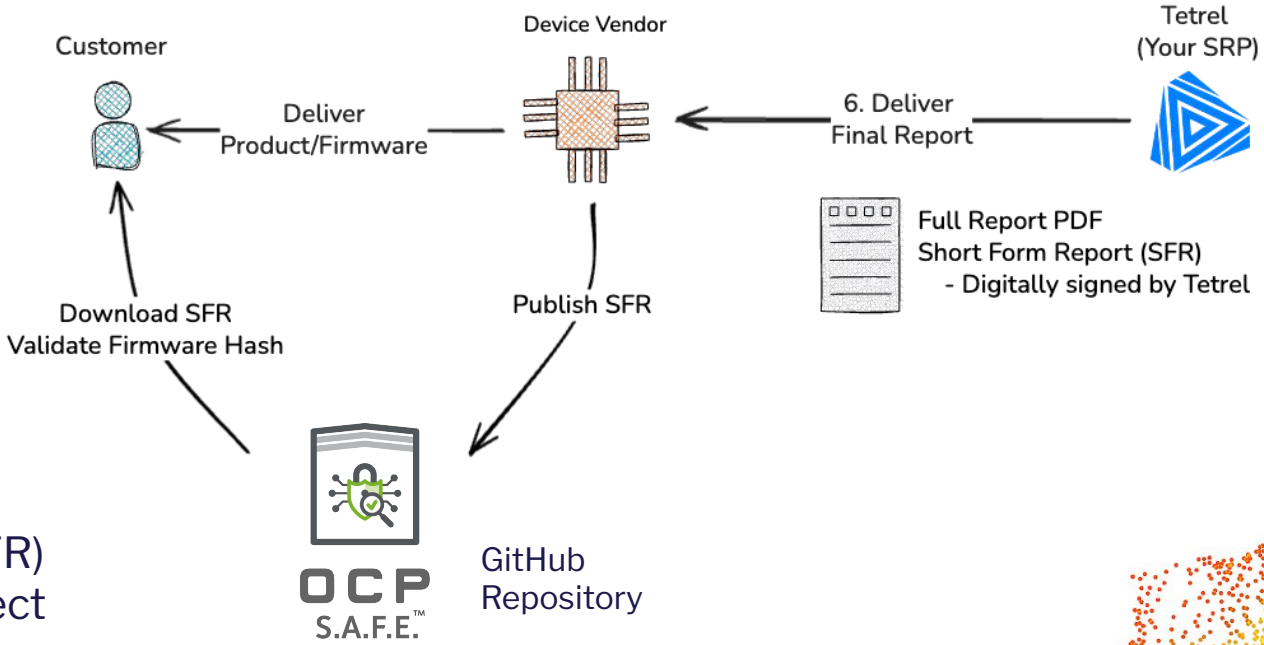
Finds different issues than humans
Match attackers' model capability

4 & 5 - Draft Report / Retest

- OCP S.A.F.E.™ has **no** minimum acceptance criteria
- SRP does not mandate fixes
- Mandatory for UEFI signing and OCP S.O.L.I.D. (more on that later)



6 - Publish



Vendor publishes
Short-form Report (SFR)
to OCP S.A.F.E.™ Project

6 - Publish

Submissions to OCP S.A.F.E.™ git repo must come **from the vendor**

Vendor controls timing and messaging

SRP does not publish anything

GitHub Repository

Common Timeline Risks

- Contract paperwork
  - Often slowest with large companies
- Kick-off delays
  - Access to code is necessary to start review
- Project size
  - Multiple reviewers are often assigned to help constrain timeline
- Remediation delays
  - Fixes can take time, and (occasionally) multiple iterations
  - Depends on Vendor development activities
- Final firmware hash generation
  - If SRP cannot build final binary, Vendor must provide the hash digest
  - This can delay if it requires post-tape-out testing, or final fuse configuration

Common Questions

- Multiple related product SKUs
- Fees
  - Depends on complexity
  - Typically $80k-$250k for a single component
  - Efficiencies for multiple related products
- Efficiencies with other security programs
  - Significant overlap with technical testing aspects of **IEC-62443, EU CRA/RED, EN 17927 SESIP**

OCP S.O.L.I.D.

- Defines minimum security features by product type
  - Included with OCP S.A.F.E.™ assessment by October 2026
- General requirements applicable to all products, plus class-specific for:
  - Server
  - Accelerator
  - NIC
  - Network appliance
  - Disk

Types of Assessment

- Firmware (Scope 1, 2)
- Hardware (Scope 3)
- Microsoft UEFI signing
  - OCP S.A.F.E.™ is a requirement for signing with these certs:
    - Microsoft Corporation UEFI CA 2011
    - Microsoft Corporation UEFI CA 2023
    - Microsoft Option ROM UEFI CA 2023
  - Requirement implemented as of Oct 2025

Caliptra Trademark

- Caliptra: open source Root-of-Trust
  - RTL, firmware, reference interface libraries
- Trademark usage is subject to integration review requirements.
  - i.e., integration must be correct!
- Trademark review uses the same set of trusted Security Review Providers as OCP S.A.F.E.™
- Review is largely documentation-based, but some RTL evidence is required

You do **NOT** have to fix everything

Findings do **NOT** have to be published

AI is **NOT** replacing human reviewers

Thank You!

tetrelsec.com/ocp

Links to OCP S.A.F.E.™ and OCP S.O.L.I.D.
Download this slide deck
Share with your colleagues