STORAGE DEVELOPER CONFERENCE
SDC 22
Fremont, CA
September 12-15, 2022
BY Developers FOR Developers

A SNIA Event

Product Security Certifications

Who, What, Where, and Why

Eric Hibbard, CISSP, CIPP/US, CISA
Samsung Semiconductor

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion, please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Background

- Formal security certification of products is not new
- Many governments require certification of products
  - Typically, those used in government systems
  - Occasionally, a market sector (e.g., HIPAA for healthcare in the US)

- For vendors, a certification can help meet minimum requirements or result in preferential treatment

Changing Landscape

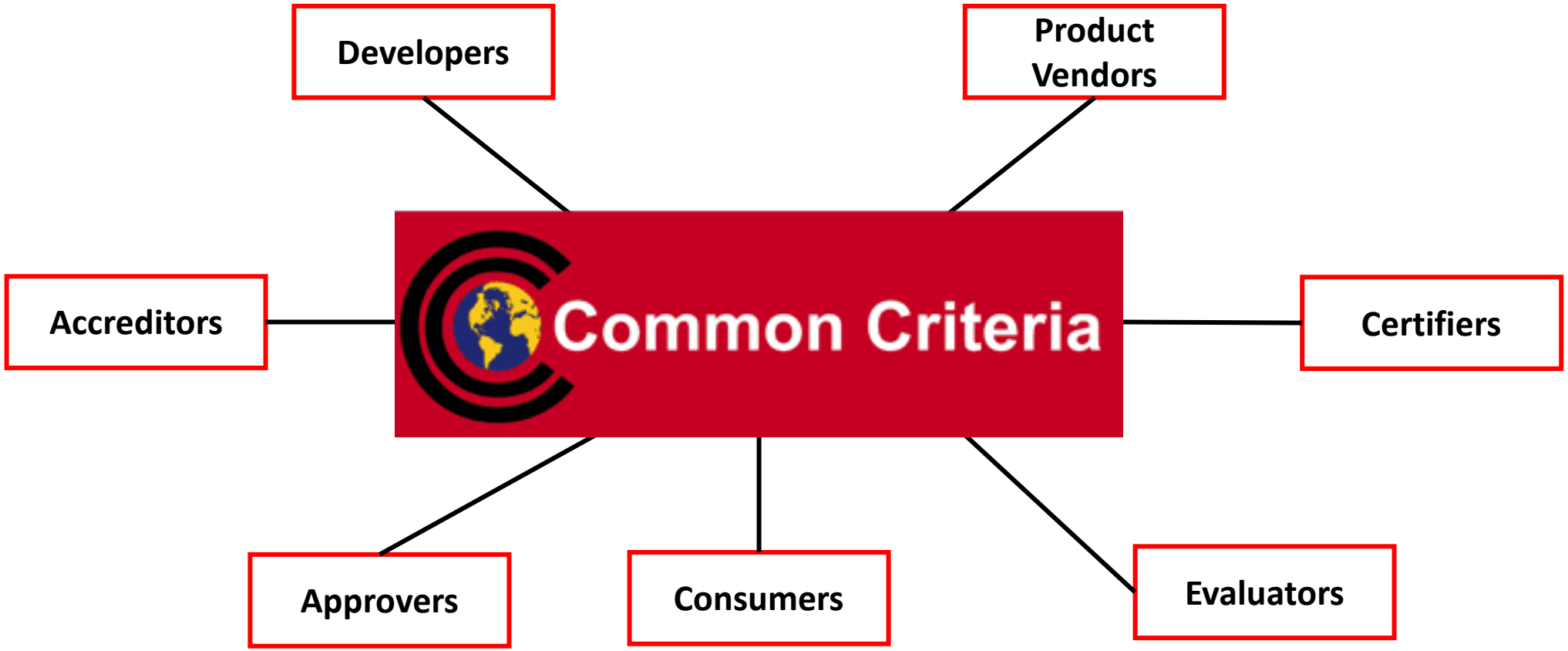
- The continued onslaught of data breaches and other attacks is raising the stakes for everyone
- Supply chain security issues are causing major headaches
- The legal community and regulators are holding suppliers accountable

- Two key certification programs have been updated:
  - Cryptographic Module Validation Program (CMVP) only accepting FIPS 140-3 submissions as of 2022-04-01
  - Common Criteria is being updated with the publication of the ISO/IEC 15408:2022 and ISO/IEC 18045:2022 standards

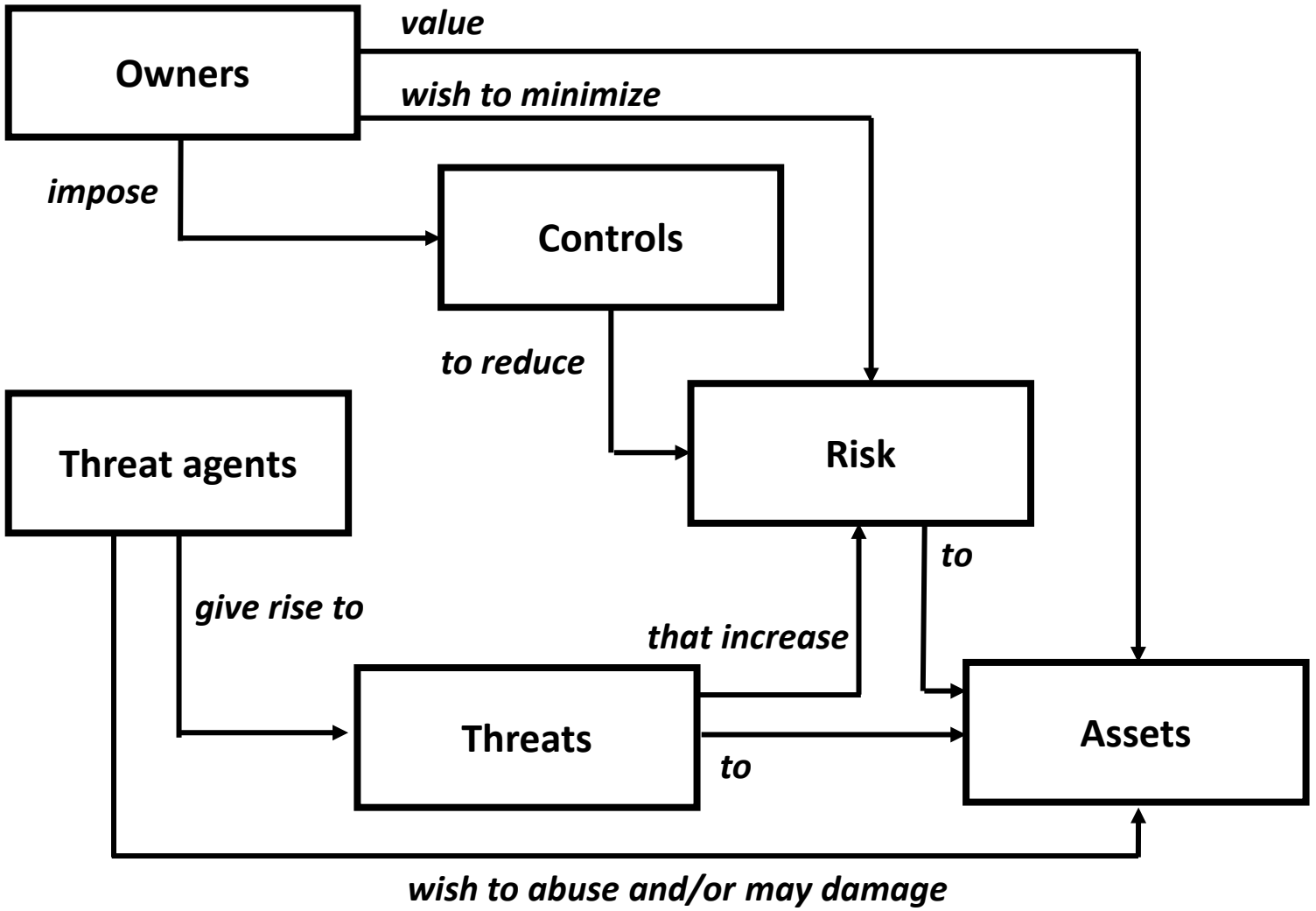
Common Criteria and FIPS 140-3

High-level Overview

Common Criteria (CC)

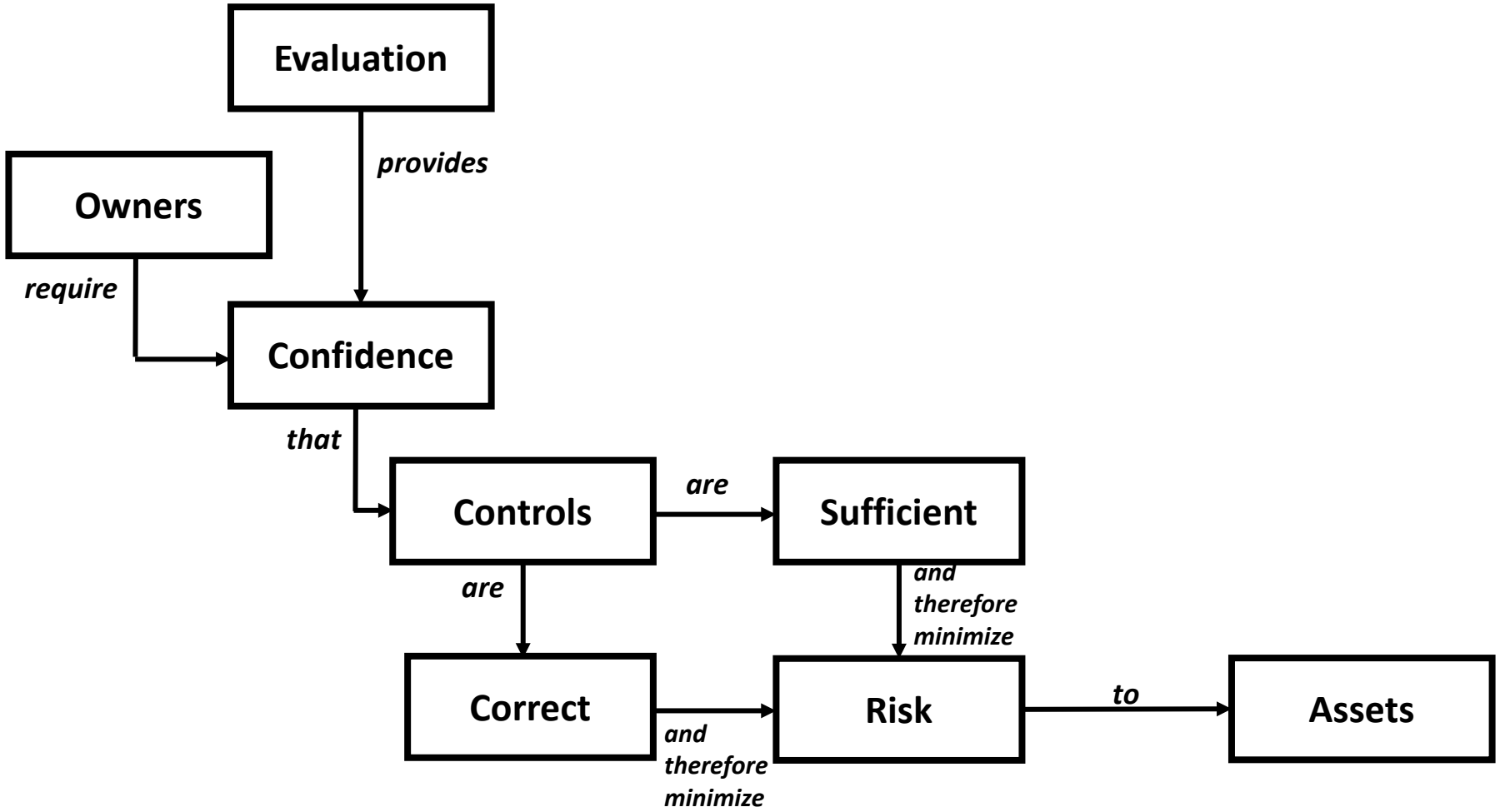


CC Security Concepts and Relationships



Source: ISO/IEC 5408-1:2022

CC Evaluation Concepts and Relationships

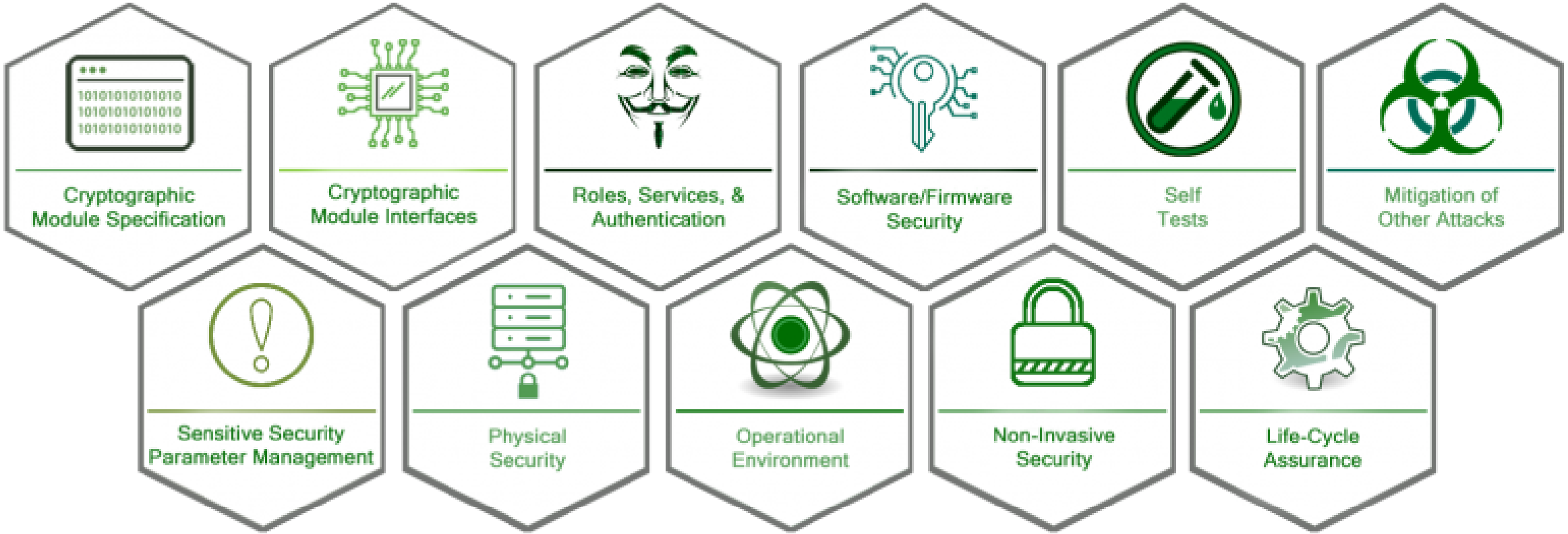


Source: ISO/IEC 5408-1:2022

CC Summary

- Certification is based on the entire product (target of evaluation)
  - Specific make and model as well as firmware
- Environment the product operates in can be a factor
- Vendors typically make their own security claims (basis of cert)
  - Evaluation assurance level (EAL) can impact requirements
- Protection Profiles (PP) and/or Collaborative Protection Profiles (cPP) may add an implementation-independent set of security requirements to also be considered
- Evaluation/testing performed by third-party (accredited lab)
- Results provided to CC scheme owner, which issues the cert
  - CC Mutual Recognition Agreement may help internationally
- Product changes can necessitate a recertification

FIPS 140-3 Elements



Source: Corsec Security, Inc.

FIPS 140-3 Summary

- Certification can be at the product level or limited to a subset (i.e., the cryptographic module)
- The security requirements are explicit
- Evaluation/testing performed by third-party (accredited lab)
- Results provided to scheme owner (NIST/CSEC), which issues the cert
- Product changes can necessitate a recertification

- Based on the ISO/IEC 19790:2012 requirements standard and ISO/IEC 24759:2017 derived test methods; US and CA use different criteria

Important Considerations

Product Development with an Eye to Certification

- System security engineering practices can be important
- Past vulnerability reports can be considered by the lab
- Documentation is important; CC and FIPS 140 are paper tigers
- Stated assumptions (e.g., the network is not a threat) have to pass the security giggle test
- Testing is critical to the third-party evaluation, so understand the testability of the security claims

Certification May Become Mandatory

- With the primary exception of encryption of sensitive US/CA Government data, certifications are currently optional for vendors
- Several governments and regions (EU) are considering mandatory security certifications as a condition of sales/use in their jurisdictions
- States are requiring “reasonable” security and considering ways to validate product security

Other Security Certifications

ISO/IEC 27001

- Organizational certification that focuses on information security management systems (ISMS)
- ISO/IEC 27002 controls are often used during the audits
- Vendors that have an ISO/IEC 27001 certification often get relief when being established as a qualified vendor (risk questionnaires)
- Products cannot be ISO/IEC 27001 certified

Payment Card Industry

- PCI Data Security Standard (PCI DSS) forms the basic requirements
- Required of organizations processing/handling credit card data
- Applies to the ICT involved with credit card data
- Products cannot be PCI DSS, but their inclusion or absence of security features can have an impact
- PCI DSS 4.0 was released early in 2022

Summary

Conclusions

- If security certifications are likely for a product, it is important to identify the strategy early in the product development
- The product security certification requirements could change significantly
  - New editions of standards and requirements
  - Possible mandatory certifications
- Because of the make/model nature of certifications, the timing should be carefully considered
- There may be opportunities for vendors to participate in the development of requirements (e.g., cPPs)

Recommendations Before Signing a Lab

- Vet the accredited lab prior to engaging
  - Do you need to develop test harness or use your own resources?
- Check the pricing contingency the lab is building into their testing model
  - If retesting is necessary, this presents risk to the lab
- Determine how the lab does its gap analysis
  - Paper-based approaches can miss granular details
- Confirm with the lab how long the entire process takes
- Determine ownership of the project deliverables

Thank You!

Please take a moment to rate this session.

Your feedback is important to us.

