OpenCRE and the art of performing SAMM assessments – Rob van der Veer

SAMM User day, Washington DC

November 1st 2023

Pleased to meet you

Rob van der Veer
Senior director AI, security & privacy
Software Improvement Group

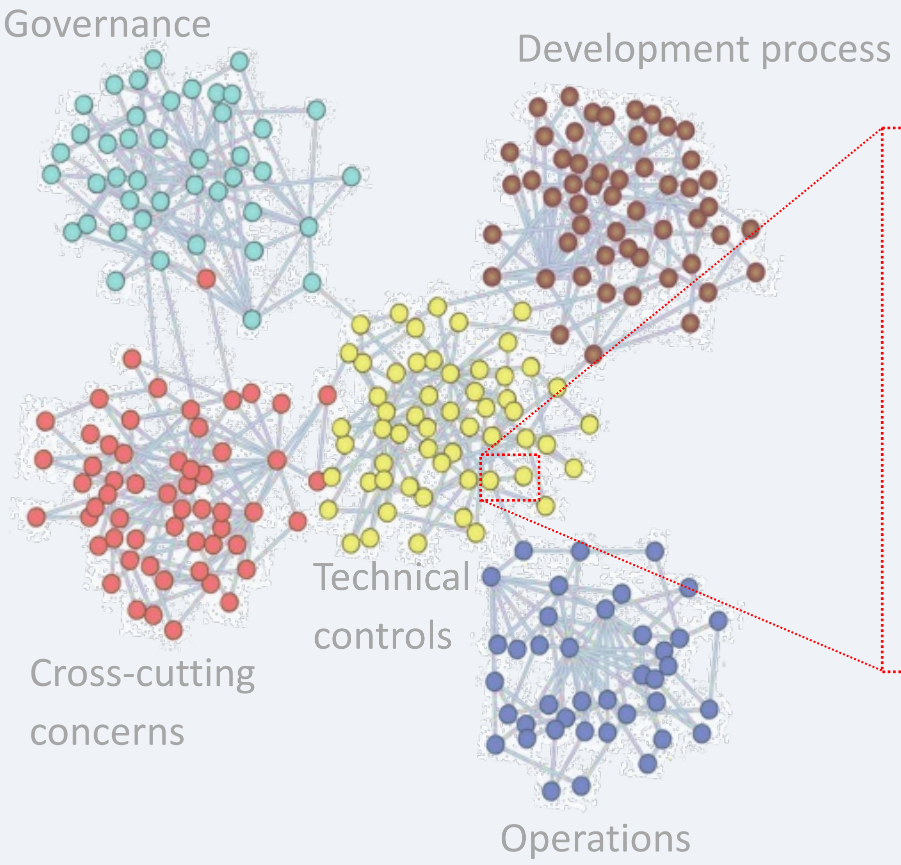
- 30 years experience AI, security & privacy
- Lead author ISO/IEC 5338 (AI lifecycle)
- Advisor ENISA, Dutch NCSC, CIP
- OWASP: SAMM, AI guide, ML top 10, AI Exchange, Integration standards
- OpenCRE.org
- ISO/IEC JTC1/SC42/WG4 (5338)
  ISO/IEC JTC1/SC42/WG4 AHG 4: liaison AI-Security
  ISO/IEC SC27/WG4(27090-AI security)
  ISO/IEC SC27/WG5(27091-AI privacy)
  CEN/CENELEC JTC13/WG 9 (CRA requirements)
  CEN/CENELEC JTC21/WG 1 TG (AI act cybersec requirements)

r.vanderveer@sig.eu
@robvanderveer
+31 6 20437187
www.linkedin.com/in/robvanderveer/

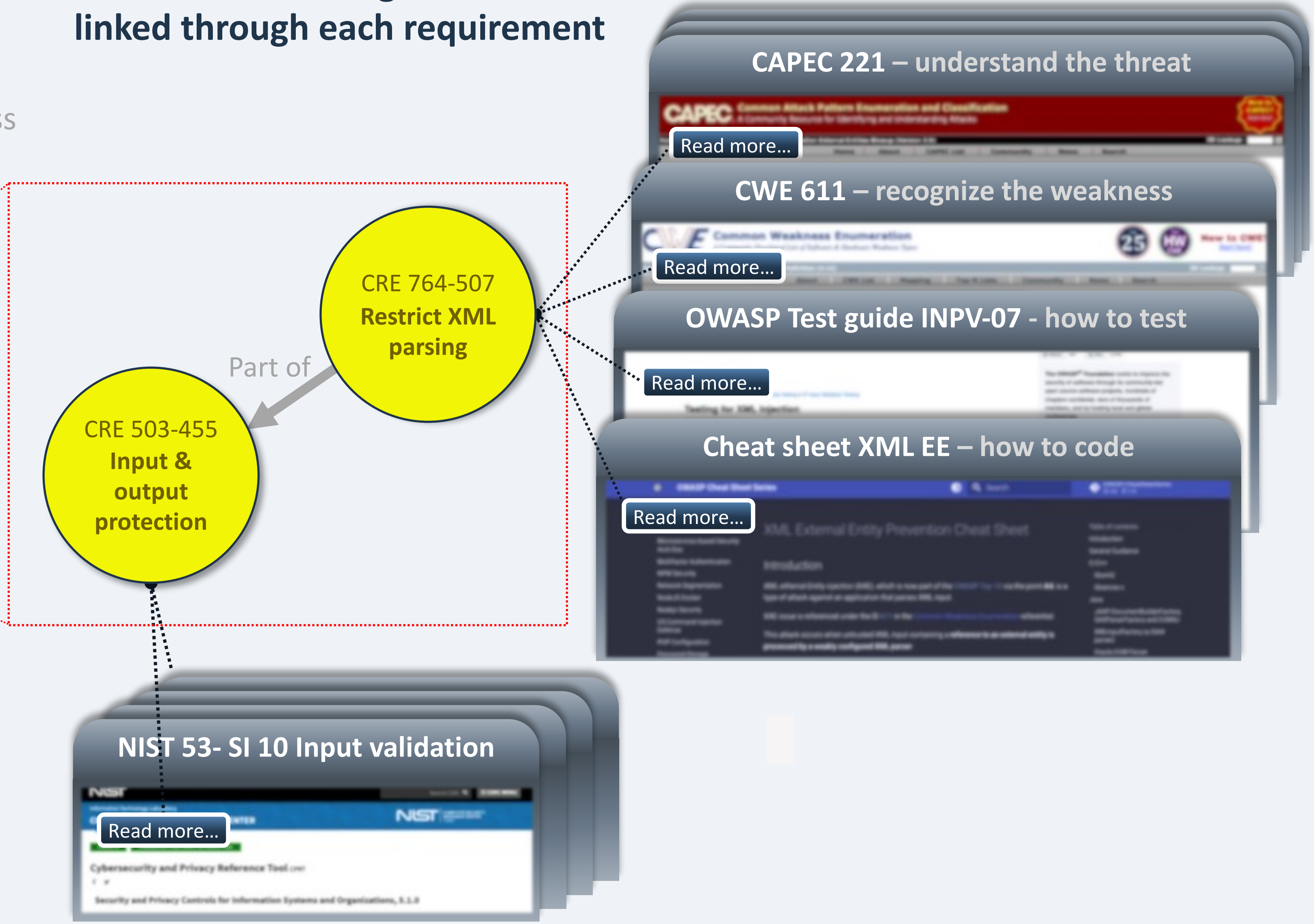
www.sig.eu/security

Common requirements are structured in the OpenCRE catalog

OpenCRE catalog of common requirements



Standards and guidelines linked through each requirement


CRE 764-507 **Restrict XML parsing**

Part of

CRE 503-455 **Input & output protection**

CAPEC 221 – understand the threat

Read more…

CWE 611 – recognize the weakness

Read more…

OWASP Test guide INPV-07 - how to test

Read more…

Cheat sheet XML EE – how to code

Read more…

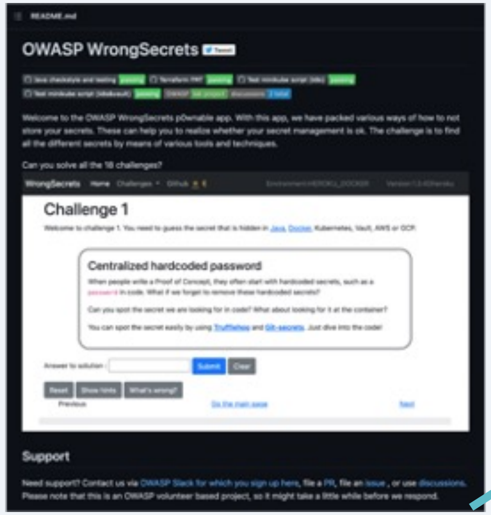
NIST 53- SI 10 Input validation

Read more…

Demo

How OpenCRE connects everything

WrongSecrets documentation



OWASP WrongSecrets

Welcome to the OWASP WrongSecrets p0wnable app. With this app, we have packed various ways of how to not store your secrets. These can help you to realize whether your secret management is ok. The challenge is to find all the different secrets by means of various tools and techniques.

Can you solve all the 18 challenges?

Challenge 1

Welcome to challenge 1. You need to guess the secret that is hidden in Java, Docker, Kubernetes, Vault, AWS or GCP.

Centralized hardcoded password

When people write a Proof of Concept, they often start with hardcoded secrets, such as a password in code. What if we forget to remove these hardcoded secrets?

Can you spot the secret we are looking for in code? What about looking for it at the container?

You can spot the secret easily by using Trufflehog and Git-secrets. Just dive into the code!

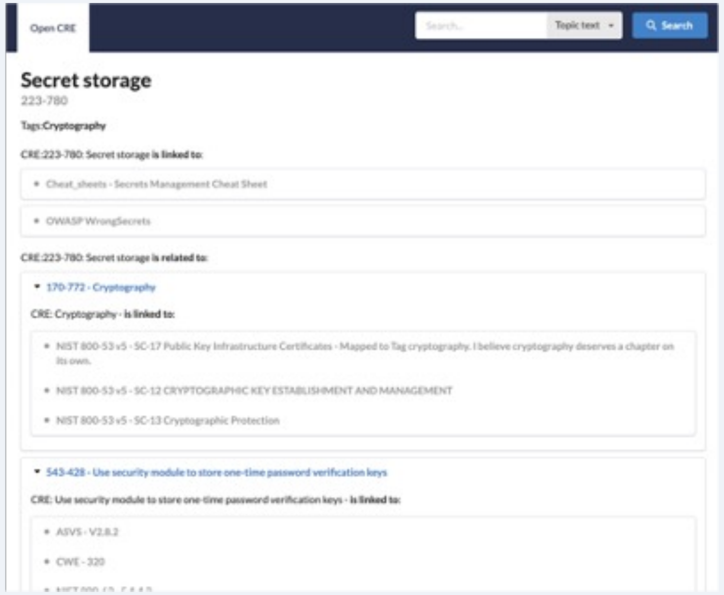
Answer to solution :

Support

Need support? Contact us via OWASP Slack for which you sign up here, file a PR, file an issue , or use discussions. Please note that this is an OWASP volunteer based project, so it might take a little while before we respond.

'Learn more about storing secrets'

OpenCRE page on Storing secrets



Secret storage

223-780

Tags:Cryptography

CRE:223-780: Secret storage **is linked to:**

- Cheat_sheets - Secrets Management Cheat Sheet
- OWASP WrongSecrets

CRE:223-780: Secret storage **is related to:**

- 170-772 - Cryptography

CRE: Cryptography - **is linked to:**

- NIST 800-53 v5 - SC-17 Public Key Infrastructure Certificates - Mapped to Tag cryptography. I believe cryptography deserves a chapter on its own.
- NIST 800-53 v5 - SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
- NIST 800-53 v5 - SC-13 Cryptographic Protection

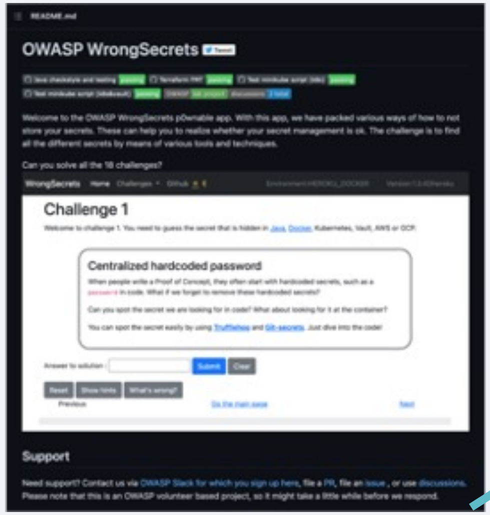
- 543-428 - Use security module to store one-time password verification keys

CRE: Use security module to store one-time password verification keys - **is linked to:**

- ASVS - V2.8.2
- CWE - 320

How OpenCRE connects everything - linking through

WrongSecrets documentation



README.md

OWASP WrongSecrets

Welcome to the OWASP WrongSecrets p0wnable app. With this app, we have packed various ways of how to not store your secrets. These can help you to realize whether your secret management is ok. The challenge is to find all the different secrets by means of various tools and techniques.

Can you solve all the 18 challenges?

Challenge 1

Welcome to challenge 1. You need to guess the secret that is hidden in Java, Docker, Kubernetes, Vault, AWS or GCP.

Centralized hardcoded password

When people write a Proof of Concept, they often start with hardcoded secrets, such as a password in code. What if we forget to remove these hardcoded secrets?

Can you spot the secret we are looking for in code? What about looking for it at the container?

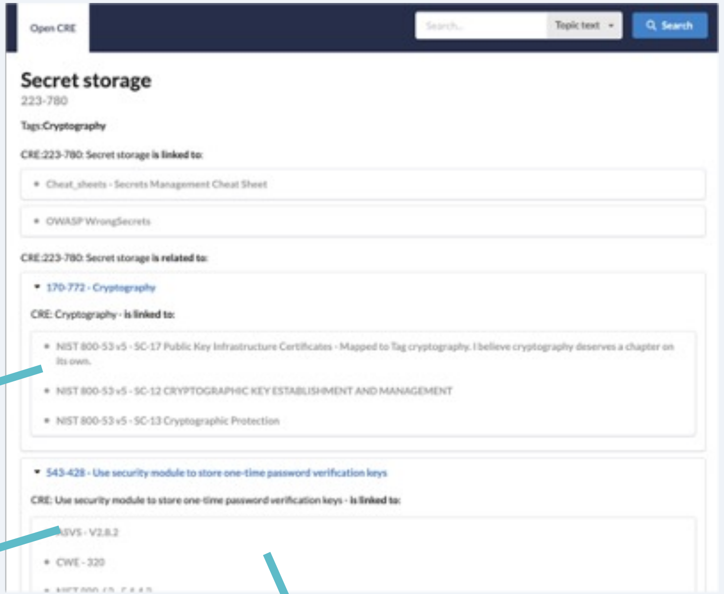
You can spot the secret easily by using Trufflehog and Git-secrets. Just dive into the code!

Support

Need support? Contact us via OWASP Slack for which you sign up here, file a PR, file an issue , or use discussions. Please note that this is an OWASP volunteer based project, so it might take a little while before we respond.

‘Learn more about storing secrets’

OpenCRE page on Secret Storage



Secret storage

223-780

Tags:Cryptography

CRE:223-780: Secret storage is linked to:

- Cheat_sheets - Secrets Management Cheat Sheet
- OWASP WrongSecrets

CRE:223-780: Secret storage is related to:

- 170-772 - Cryptography

CRE: Cryptography - is linked to:

- NIST 800-53 v5 - SC-17 Public Key Infrastructure Certificates - Mapped to Tag cryptography. I believe cryptography deserves a chapter on its own.
- NIST 800-53 v5 - SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
- NIST 800-53 v5 - SC-13 Cryptographic Protection

- 543-428 - Use security module to store one-time password verification keys

CRE: Use security module to store one-time password verification keys - is linked to:

- ASVS - V2.8.2
- CWE - 320

NIST 800-53 : SC-12 Crypto Key establishment & management

SP 800-53 Rev 5.1 and SP 800-53B Latest Versions

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

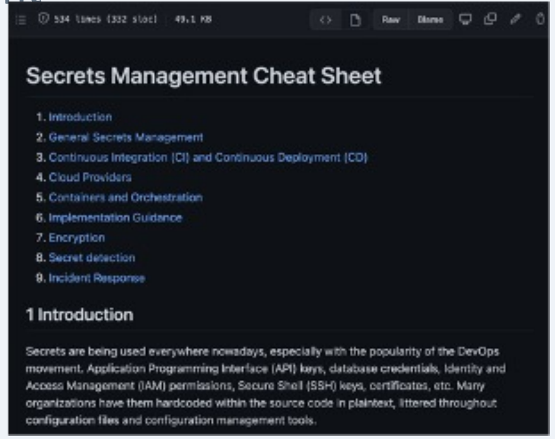
Jump To:

Control

Discussion

Control Enhancements

OWASP cheat sheet “Secrets management”



Secrets Management Cheat Sheet

1. Introduction
2. General Secrets Management
3. Continuous Integration (CI) and Continuous Deployment (CD)
4. Cloud Providers
5. Containers and Orchestration
6. Implementation Guidance
7. Encryption
8. Secret detection
9. Incident Response

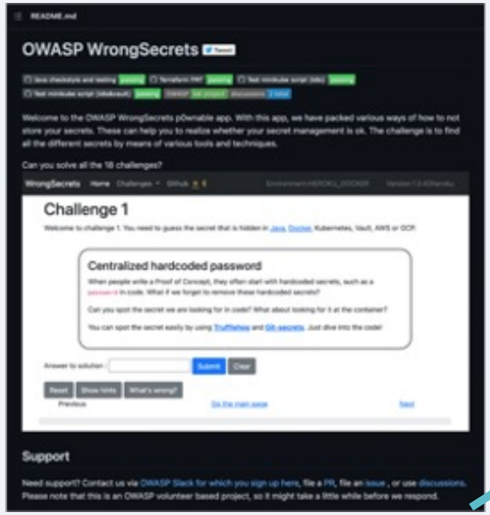
1 Introduction

Secrets are being used everywhere nowadays, especially with the popularity of the DevOps movement. Application Programming Interface (API) keys, database credentials, Identity and Access Management (IAM) permissions, Secure Shell (SSH) keys, certificates, etc. Many organizations have them hardcoded within the source code in plaintext, littered throughout configuration files and configuration management tools.

- ASVS
- TOP 10
- CAPEC threats
- CWE weaknesses
- Pro-active controls
- ZAP rules

How OpenCRE connects everything - linking through

WrongSecrets documentation



OWASP WrongSecrets

Welcome to the OWASP WrongSecrets p0wnable app. With this app, we have packed various ways of how to not store your secrets. These can help you to realize whether your secret management is ok. The challenge is to find all the different secrets by means of various tools and techniques.

Can you solve all the 18 challenges?

Challenge 1

Welcome to challenge 1. You need to guess the secret that is hidden in Java, Docker, Kubernetes, Vault, AWS or GCP.

Centralized hardcoded password

When people write a Proof of Concept, they often start with hardcoded secrets, such as a password in code. What if we forget to remove these hardcoded secrets?

Can you spot the secret we are looking for in code? What about looking for it at the container?

You can spot the secret easily by using Trufflehog and Git-secrets. Just dive into the code!

Answer to solution :

Previous

Go the main page

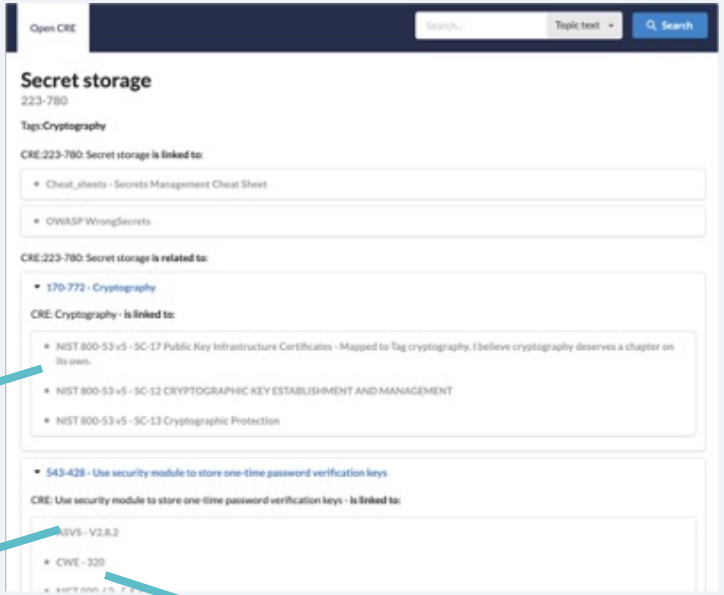
Next

Support

Need support? Contact us via OWASP Slack for which you sign up here, file a PR, file an issue , or use discussions. Please note that this is an OWASP volunteer based project, so it might take a little while before we respond.

'Learn more about storing secrets'

OpenCRE page on Secret Storage



Secret storage

223-780

Tags:Cryptography

CRE:223-780: Secret storage **is linked to:**

- Cheat_sheets - Secrets Management Cheat Sheet
- OWASP WrongSecrets

CRE:223-780: Secret storage **is related to:**

- 170-772 - Cryptography

CRE: Cryptography - **is linked to:**

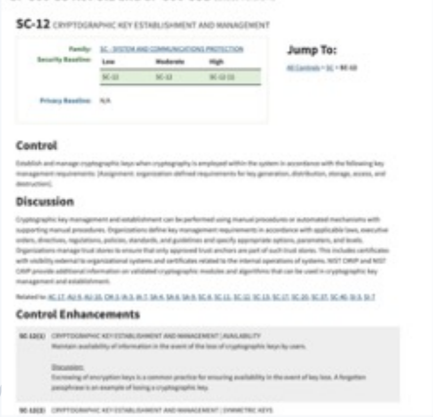
- NIST 800-53 v5 - SC-17 Public Key Infrastructure Certificates - Mapped to Tag cryptography. I believe cryptography deserves a chapter on its own.
- NIST 800-53 v5 - SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
- NIST 800-53 v5 - SC-13 Cryptographic Protection

- 543-428 - Use security module to store one-time password verification keys

CRE: Use security module to store one-time password verification keys - **is linked to:**

- ASVS - V2.8.2
- CWE - 320

NIST 800-53 : SC-12 Crypto
Key establishment & management



SP 800-53 Rev 5.1 and SP 800-53B Latest Versions

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Family: SC - SYSTEM AND COMMUNICATIONS PROTECTION

Security Baseline:

Low	Moderate	High
SC-12	SC-12	SC-12 (1)

Privacy Baseline: N/A

Jump To:

All Controls > SC > SC-12

Control

Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

Discussion

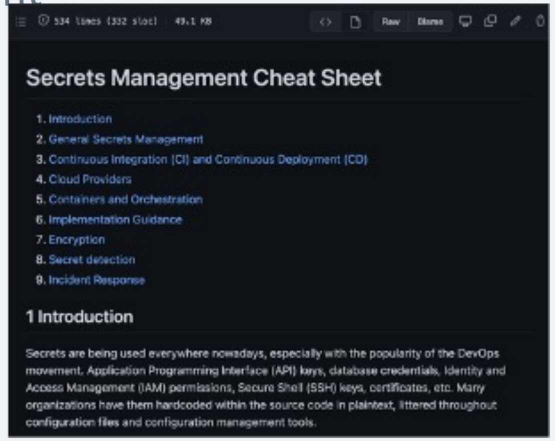
Control Enhancements

SC-12(1) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY
Maintain availability of information in the event of the loss of cryptographic keys by users.

Discussion:
Escrowing of encryption keys is a common practice for ensuring availability in the event of key loss. A forgotten passphrase is an example of losing a cryptographic key.

SC-12(2) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS

OWASP cheat sheet "Secrets management"



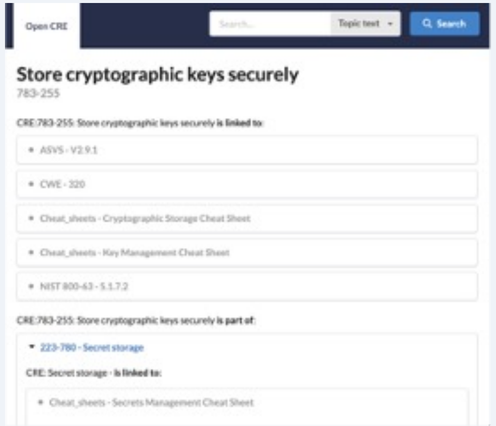
Secrets Management Cheat Sheet

1. Introduction
2. General Secrets Management
3. Continuous Integration (CI) and Continuous Deployment (CD)
4. Cloud Providers
5. Containers and Orchestration
6. Implementation Guidance
7. Encryption
8. Secret detection
9. Incident Response

1 Introduction

Secrets are being used everywhere nowadays, especially with the popularity of the DevOps movement. Application Programming Interface (API) keys, database credentials, Identity and Access Management (IAM) permissions, Secure Shell (SSH) keys, certificates, etc. Many organizations have them hardcoded within the source code in plaintext, littered throughout configuration files and configuration management tools.

OpenCRE page on Storing keys



Store cryptographic keys securely

783-255

CRE:783-255: Store cryptographic keys securely **is linked to:**

- ASVS - V2.9.1
- CWE - 320
- Cheat_sheets - Cryptographic Storage Cheat Sheet
- Cheat_sheets - Key Management Cheat Sheet
- NIST 800-63 - 5.1.7.2

CRE:783-255: Store cryptographic keys securely **is part of:**

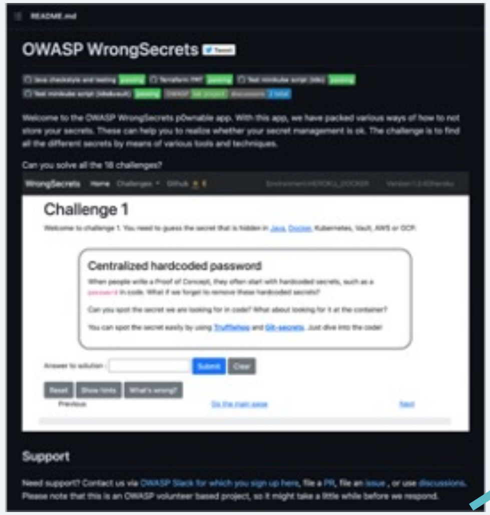
- 223-780 - Secret storage

CRE: Secret storage - **is linked to:**

- Cheat_sheets - Secrets Management Cheat Sheet

How OpenCRE connects everything - linking back

WrongSecrets documentation



README.md

OWASP WrongSecrets

Welcome to the OWASP WrongSecrets p0wnable app. With this app, we have packed various ways of how to not store your secrets. These can help you to realize whether your secret management is ok. The challenge is to find all the different secrets by means of various tools and techniques.

Can you solve all the 18 challenges?

Challenge 1

Welcome to challenge 1. You need to guess the secret that is hidden in Java, Docker, Kubernetes, Vault, AWS or GCP.

Centralized hardcoded password

When people write a Proof of Concept, they often start with hardcoded secrets, such as a password in code. What if we forget to remove these hardcoded secrets?

Can you spot the secret we are looking for in code? What about looking for it at the container?

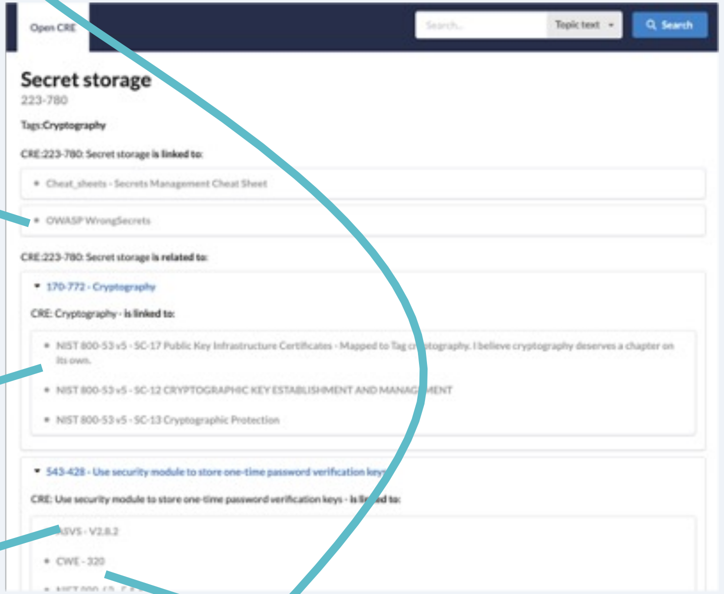
You can spot the secret easily by using Trufflehog and Git-secrets. Just dive into the code!

Answer to solution:

Support

Need support? Contact us via OWASP Slack for which you sign up here, file a PR, file an issue , or use discussions. Please note that this is an OWASP volunteer based project, so it might take a little while before we respond.

OpenCRE page on Secret Storage



Secret storage

223-780

Tags:Cryptography

CRE:223-780: Secret storage **is linked to:**

- Cheat_sheets - Secrets Management Cheat Sheet
- OWASP WrongSecrets

CRE:223-780: Secret storage **is related to:**

- 170-772 - Cryptography

  CRE: Cryptography - **is linked to:**

  - NIST 800-53 v5 - SC-17 Public Key Infrastructure Certificates - Mapped to Tag cryptography. I believe cryptography deserves a chapter on its own.
  - NIST 800-53 v5 - SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
  - NIST 800-53 v5 - SC-13 Cryptographic Protection

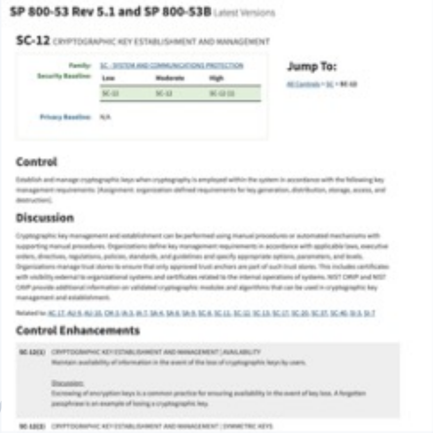
- 543-428 - Use security module to store one-time password verification keys

  CRE: Use security module to store one-time password verification keys - **is linked to:**

  - ASVS - V2.8.2
  - CWE - 320

'Learn more about storing secrets'

NIST 800-53 : SC-12 Crypto Key establishment & management



SP 800-53 Rev 5.1 and SP 800-53B Latest Versions

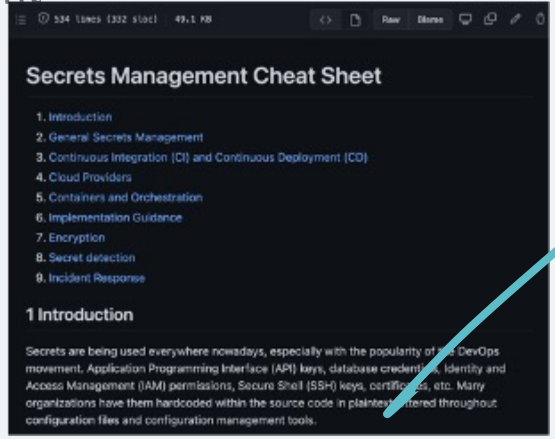
SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control

Discussion

Control Enhancements

OWASP cheat sheet "Secrets management"



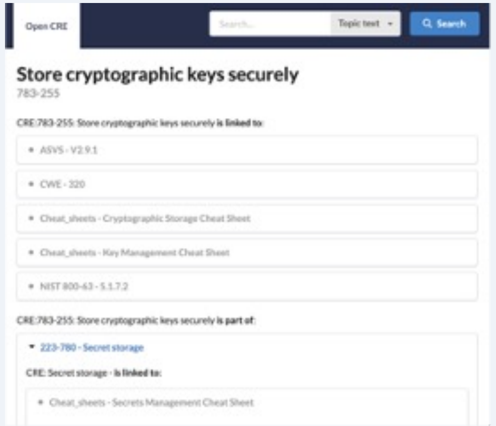
Secrets Management Cheat Sheet

1. Introduction
2. General Secrets Management
3. Continuous Integration (CI) and Continuous Deployment (CD)
4. Cloud Providers
5. Containers and Orchestration
6. Implementation Guidance
7. Encryption
8. Secret detection
9. Incident Response

1 Introduction

Secrets are being used everywhere nowadays, especially with the popularity of the DevOps movement. Application Programming Interface (API) keys, database credentials, Identity and Access Management (IAM) permissions, Secure Shell (SSH) keys, certificates, etc. Many organizations have them hardcoded within the source code in plaintext, littered throughout configuration files and configuration management tools.

OpenCRE page on Storing keys



Store cryptographic keys securely

783-255

CRE:783-255: Store cryptographic keys securely **is linked to:**

- ASVS - V2.9.1
- CWE - 320
- Cheat_sheets - Cryptographic Storage Cheat Sheet
- Cheat_sheets - Key Management Cheat Sheet
- NIST 800-63 - 5.1.7.2

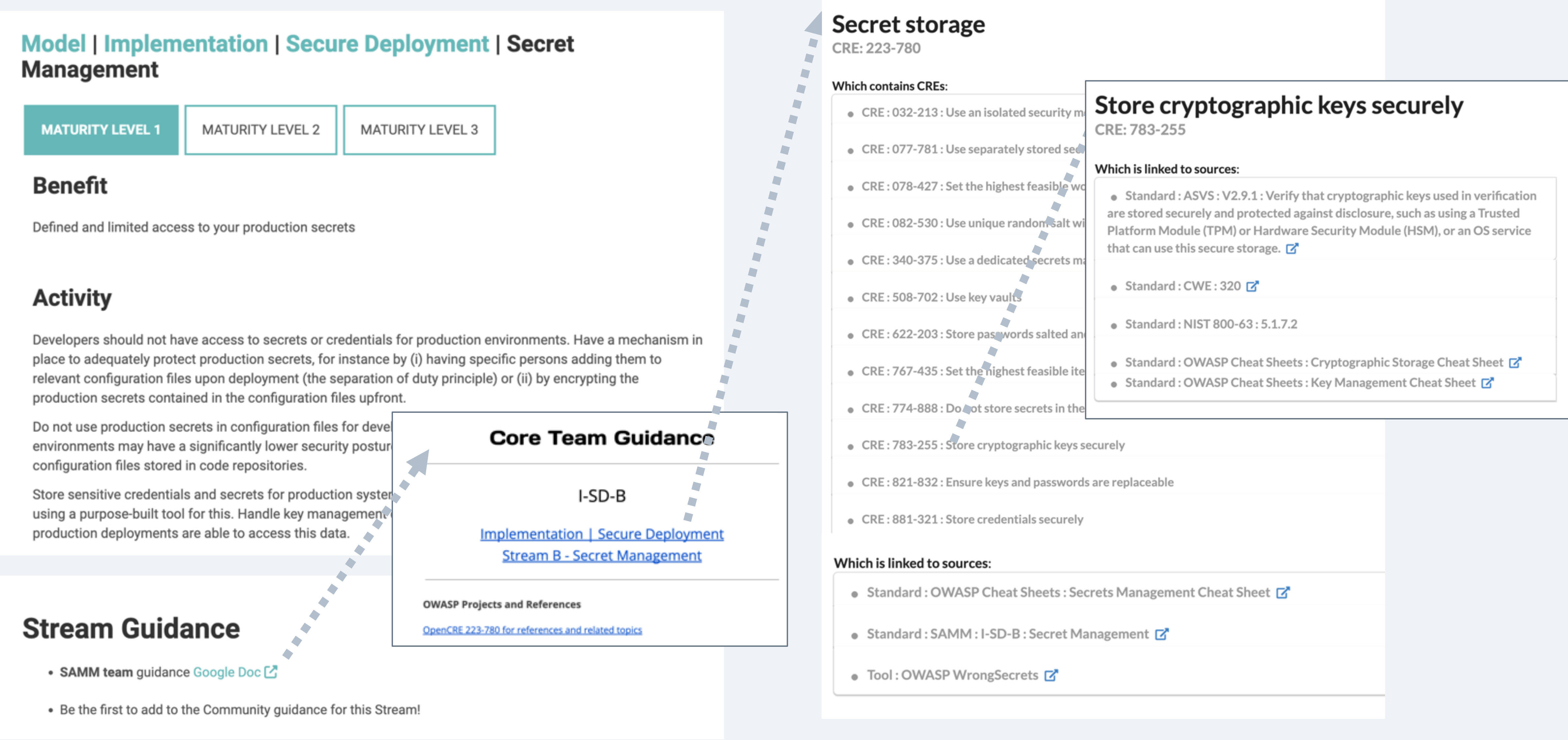
CRE:783-255: Store cryptographic keys securely **is part of:**

- 223-780 - Secret storage

  CRE: Secret storage - **is linked to:**

  - Cheat_sheets - Secrets Management Cheat Sheet

How OpenCRE connects SAMM: e.g. learn everything on Secret management



Model | Implementation | Secure Deployment | Secret Management

Benefit

Defined and limited access to your production secrets

Activity

Developers should not have access to secrets or credentials for production environments. Have a mechanism in place to adequately protect production secrets, for instance by (i) having specific persons adding them to relevant configuration files upon deployment (the separation of duty principle) or (ii) by encrypting the production secrets contained in the configuration files upfront.

Do not use production secrets in configuration files for devel
environments may have a significantly lower security postur
configuration files stored in code repositories.

Store sensitive credentials and secrets for production syster
using a purpose-built tool for this. Handle key management
production deployments are able to access this data.

Stream Guidance

- **SAMM team** guidance Google Doc
- Be the first to add to the Community guidance for this Stream!

Core Team Guidance

I-SD-B

Implementation | Secure Deployment
Stream B - Secret Management

OWASP Projects and References

OpenCRE 223-780 for references and related topics

Secret storage

CRE: 223-780

Which contains CREs:

- CRE : 032-213 : Use an isolated security m
- CRE : 077-781 : Use separately stored sec
- CRE : 078-427 : Set the highest feasible wo
- CRE : 082-530 : Use unique random salt wi
- CRE : 340-375 : Use a dedicated secrets ma
- CRE : 508-702 : Use key vaults
- CRE : 622-203 : Store passwords salted an
- CRE : 767-435 : Set the highest feasible ite
- CRE : 774-888 : Do not store secrets in the
- CRE : 783-255 : Store cryptographic keys securely
- CRE : 821-832 : Ensure keys and passwords are replaceable
- CRE : 881-321 : Store credentials securely

Which is linked to sources:

- Standard : OWASP Cheat Sheets : Secrets Management Cheat Sheet
- Standard : SAMM : I-SD-B : Secret Management
- Tool : OWASP WrongSecrets

Store cryptographic keys securely

CRE: 783-255

Which is linked to sources:

- Standard : ASVS : V2.9.1 : Verify that cryptographic keys used in verification are stored securely and protected against disclosure, such as using a Trusted Platform Module (TPM) or Hardware Security Module (HSM), or an OS service that can use this secure storage.
- Standard : CWE : 320
- Standard : NIST 800-63 : 5.1.7.2
- Standard : OWASP Cheat Sheets : Cryptographic Storage Cheat Sheet
- Standard : OWASP Cheat Sheets : Key Management Cheat Sheet

What is OpenCRE?

www.opencre.org

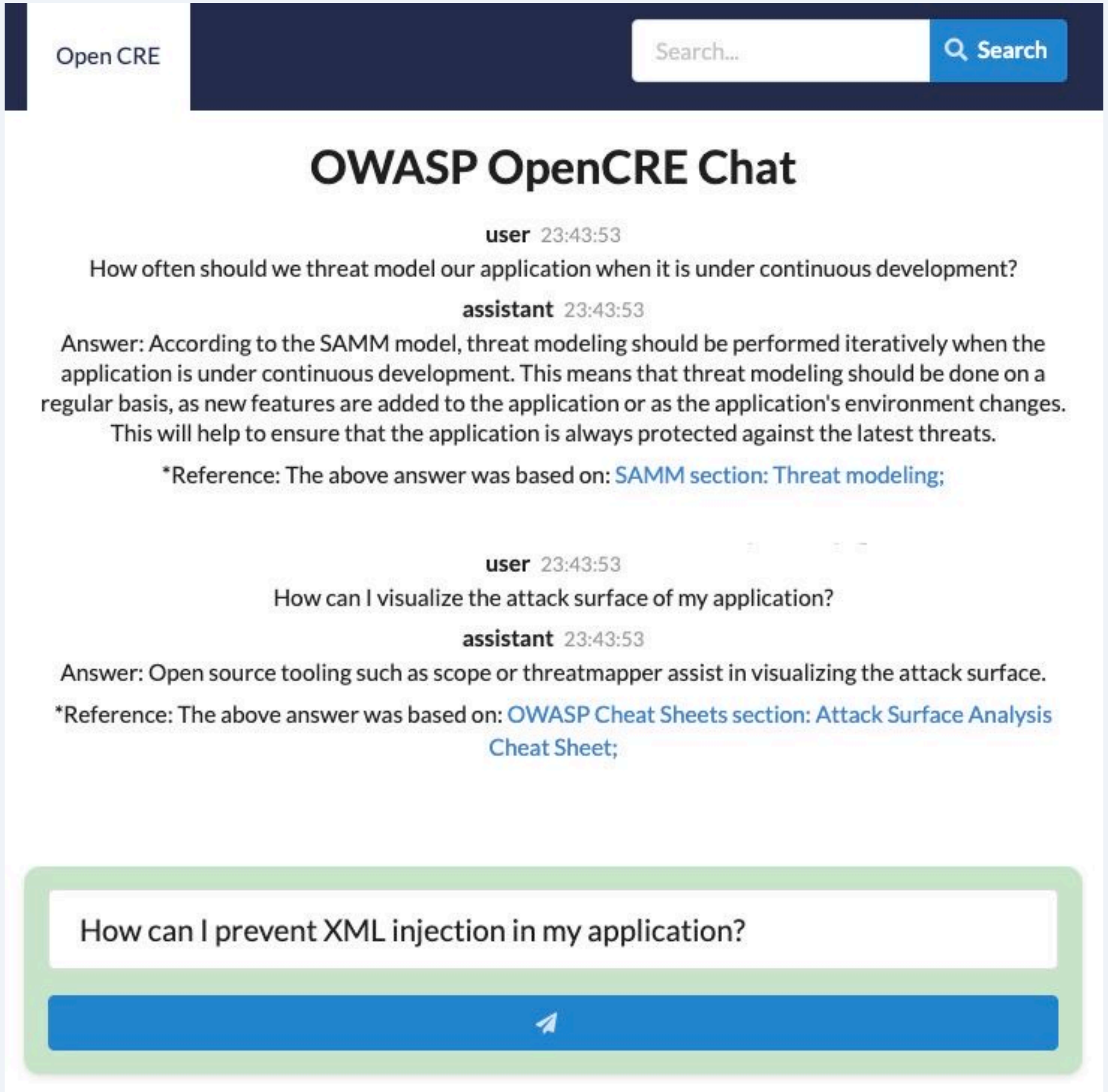
By the **Integration standards project** at OWASP:
Led by Spyros Gasteratos and Rob van der Veer
Through many collaborations, e.g. SKF, Owasp top 10, ASVS, OSSF, CSA

“**CRE is** an interactive database for smart access to security standards and guidelines when designing, developing, auditing, testing and procuring for cyber security. It links and unlocks these resources into one unified overview, allowing easy referencing, searching, browsing, and asking questions.”

Mapping: ISO27001, ASVS, Top10, NIST 800-63, NIST 800-53, Pro-active controls, Cheat sheets, Testing guide, CWE, Capec, Zap, Juice shop, NIST SSDF, OWASP SAMM, CCM

Because we have all those standards we can do a bunch of great things: search, browse, chat and map. For which we built features.

OpenCRE Chat



OWASP OpenCRE Chat

user 23:43:53

How often should we threat model our application when it is under continuous development?

assistant 23:43:53

Answer: According to the SAMM model, threat modeling should be performed iteratively when the application is under continuous development. This means that threat modeling should be done on a regular basis, as new features are added to the application or as the application's environment changes. This will help to ensure that the application is always protected against the latest threats.

*Reference: The above answer was based on: SAMM section: Threat modeling;

user 23:43:53

How can I visualize the attack surface of my application?

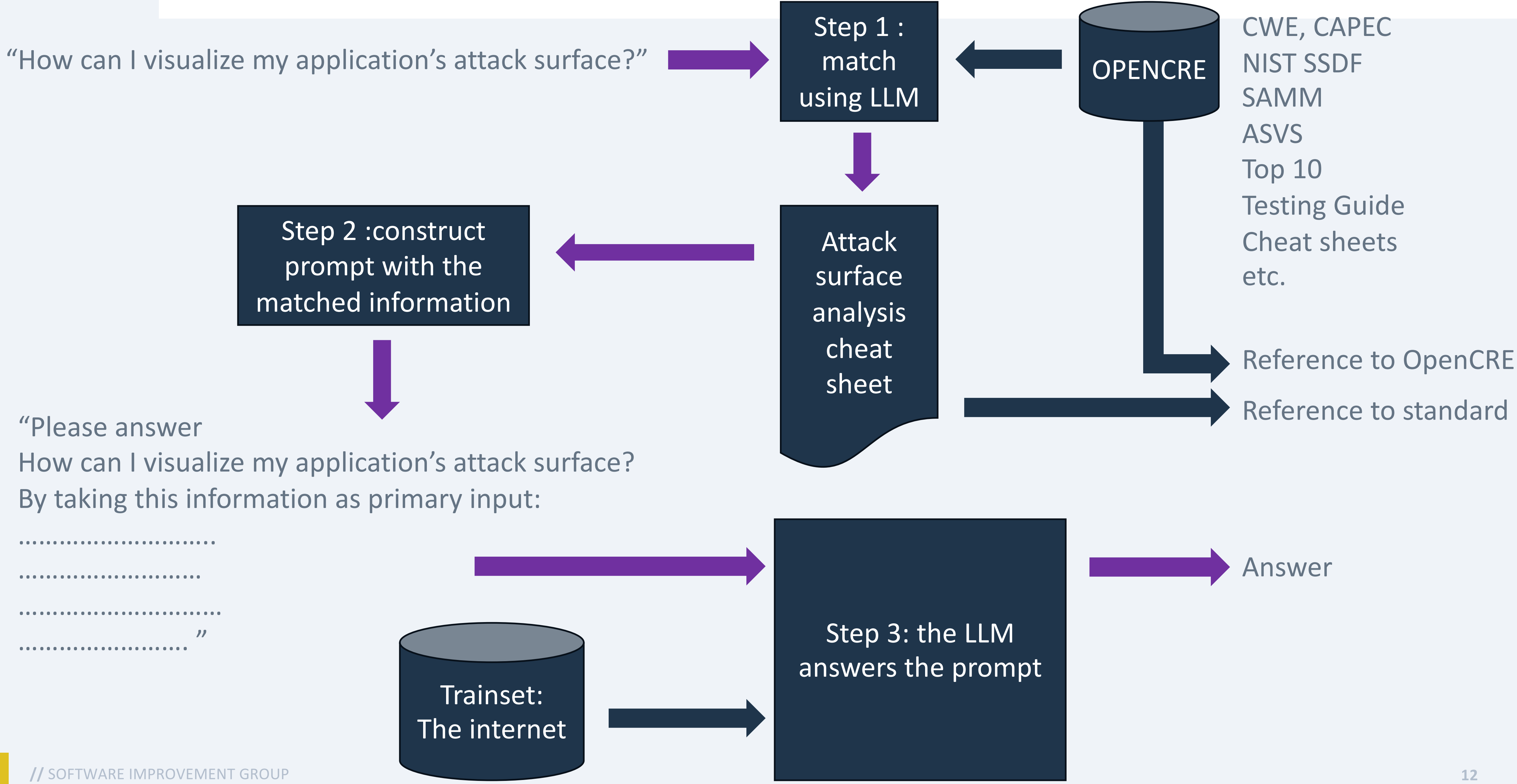
assistant 23:43:53

Answer: Open source tooling such as scope or threatmapper assist in visualizing the attack surface.

*Reference: The above answer was based on: OWASP Cheat Sheets section: Attack Surface Analysis Cheat Sheet;

How can I prevent XML injection in my application?

OpenCRE Chat - how



“How can I visualize my application’s attack surface?”

Step 1 : match using LLM

OPENCRE

ISO27001
NIST 800-53
CWE, CAPEC
NIST SSDF
SAMM
ASVS
Top 10
Testing Guide
Cheat sheets
etc.

Attack surface analysis cheat sheet

Step 2 :construct prompt with the matched information

Reference to OpenCRE

Reference to standard

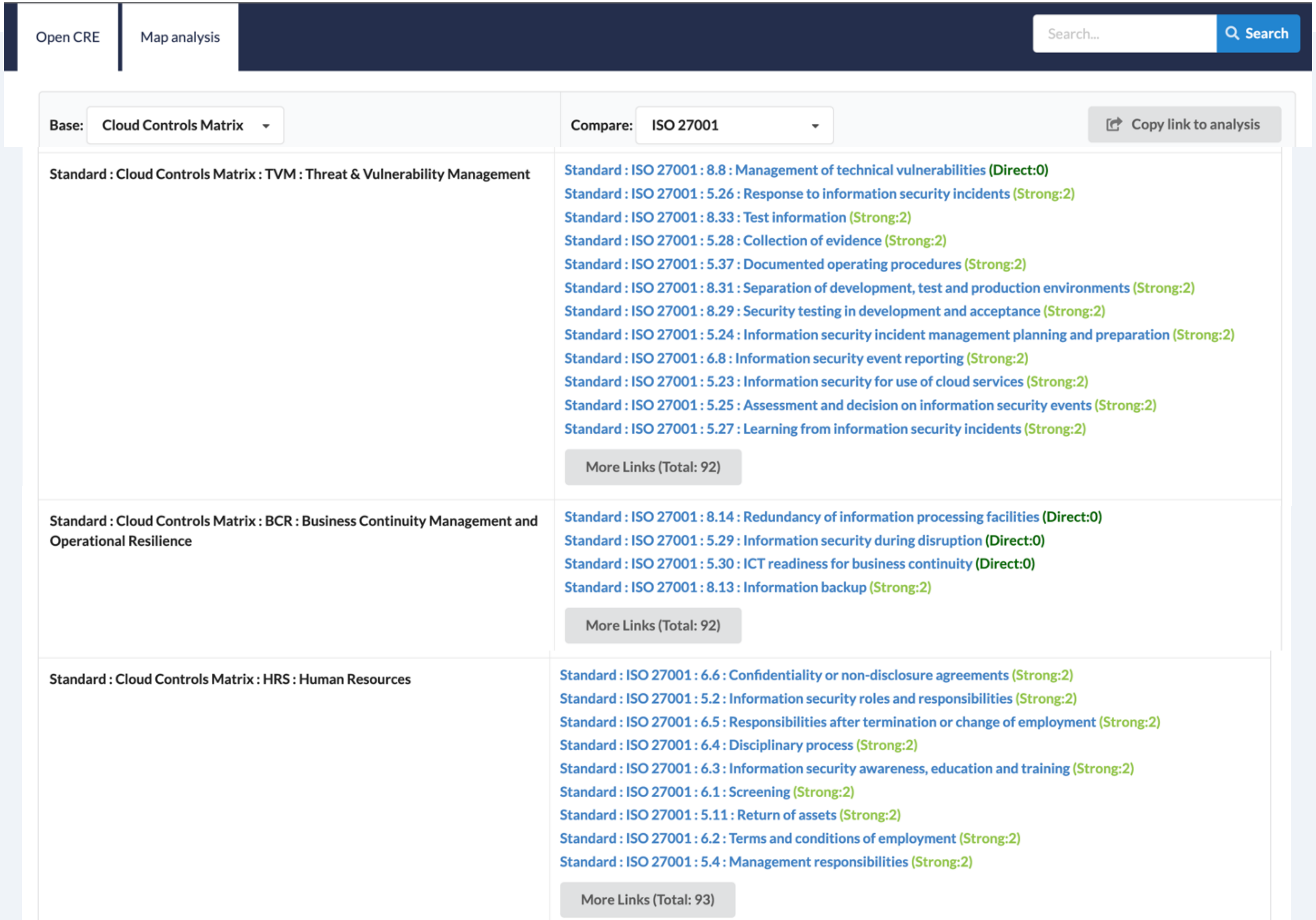
“Please answer
How can I visualize my application’s attack surface?
By taking this information as primary input:
…………………………..
………………………
…………………………..
…………………….. ”

Trainset: The internet

Step 3: the LLM answers the prompt

Answer

Map analysis



Base: Cloud Controls Matrix

Compare: ISO 27001

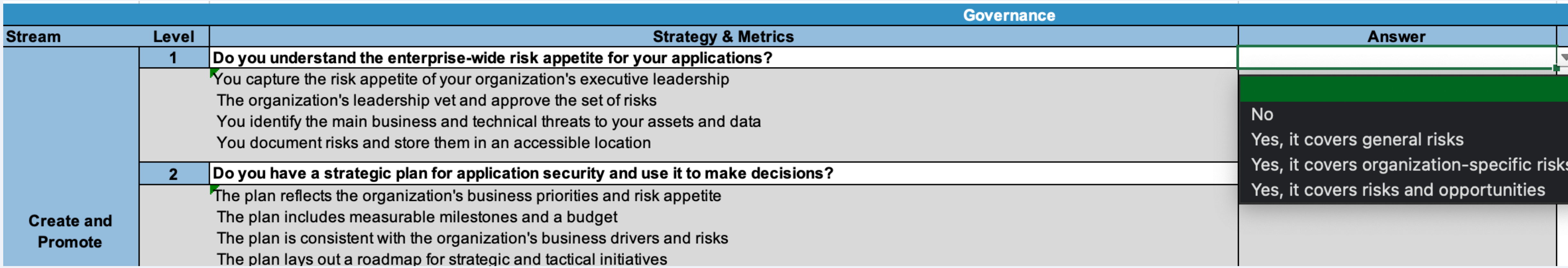
Standard : Cloud Controls Matrix : TVM : Threat & Vulnerability Management	Standard : ISO 27001 : 8.8 : Management of technical vulnerabilities (Direct:0) Standard : ISO 27001 : 5.26 : Response to information security incidents (Strong:2) Standard : ISO 27001 : 8.33 : Test information (Strong:2) Standard : ISO 27001 : 5.28 : Collection of evidence (Strong:2) Standard : ISO 27001 : 5.37 : Documented operating procedures (Strong:2) Standard : ISO 27001 : 8.31 : Separation of development, test and production environments (Strong:2) Standard : ISO 27001 : 8.29 : Security testing in development and acceptance (Strong:2) Standard : ISO 27001 : 5.24 : Information security incident management planning and preparation (Strong:2) Standard : ISO 27001 : 6.8 : Information security event reporting (Strong:2) Standard : ISO 27001 : 5.23 : Information security for use of cloud services (Strong:2) Standard : ISO 27001 : 5.25 : Assessment and decision on information security events (Strong:2) Standard : ISO 27001 : 5.27 : Learning from information security incidents (Strong:2) More Links (Total: 92)
Standard : Cloud Controls Matrix : BCR : Business Continuity Management and Operational Resilience	Standard : ISO 27001 : 8.14 : Redundancy of information processing facilities (Direct:0) Standard : ISO 27001 : 5.29 : Information security during disruption (Direct:0) Standard : ISO 27001 : 5.30 : ICT readiness for business continuity (Direct:0) Standard : ISO 27001 : 8.13 : Information backup (Strong:2) More Links (Total: 92)
Standard : Cloud Controls Matrix : HRS : Human Resources	Standard : ISO 27001 : 6.6 : Confidentiality or non-disclosure agreements (Strong:2) Standard : ISO 27001 : 5.2 : Information security roles and responsibilities (Strong:2) Standard : ISO 27001 : 6.5 : Responsibilities after termination or change of employment (Strong:2) Standard : ISO 27001 : 6.4 : Disciplinary process (Strong:2) Standard : ISO 27001 : 6.3 : Information security awareness, education and training (Strong:2) Standard : ISO 27001 : 6.1 : Screening (Strong:2) Standard : ISO 27001 : 5.11 : Return of assets (Strong:2) Standard : ISO 27001 : 6.2 : Terms and conditions of employment (Strong:2) Standard : ISO 27001 : 5.4 : Management responsibilities (Strong:2) More Links (Total: 93)

Software
Improvement
Group

Selected lessons from SAMM assessments by SIG

Rob van der Veer

Self-assessment pitfall 1: Thinking the quality criteria are not mandatory

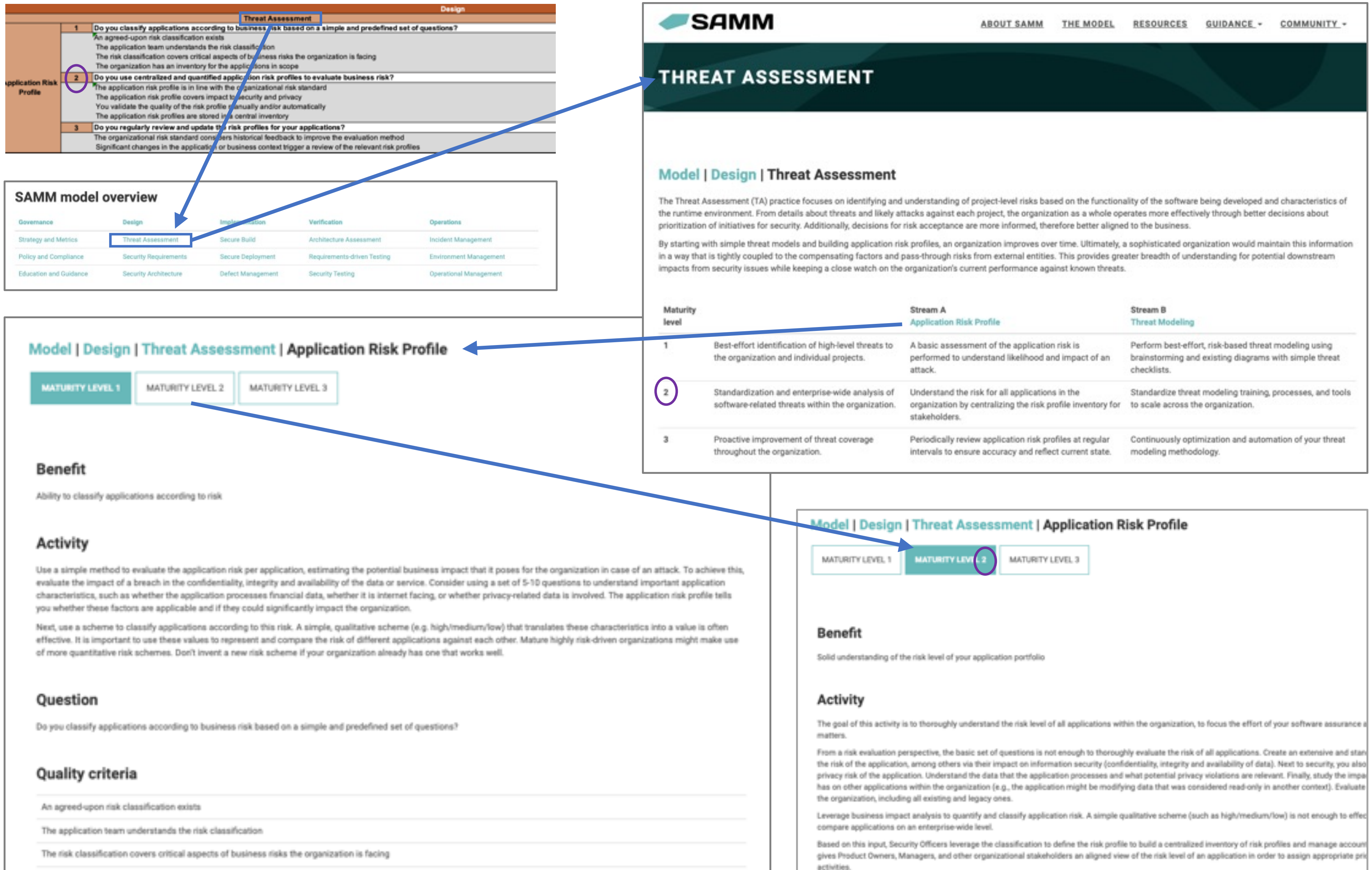


Governance			
Stream	**Level**	**Strategy & Metrics**	**Answer**
Create and Promote	**1**	**Do you understand the enterprise-wide risk appetite for your applications?**	
		You capture the risk appetite of your organization's executive leadership The organization's leadership vet and approve the set of risks You identify the main business and technical threats to your assets and data You document risks and store them in an accessible location	
	2	**Do you have a strategic plan for application security and use it to make decisions?**	
		The plan reflects the organization's business priorities and risk appetite The plan includes measurable milestones and a budget The plan is consistent with the organization's business drivers and risks The plan lays out a roadmap for strategic and tactical initiatives	

No
Yes, it covers general risks
Yes, it covers organization-specific risk
Yes, it covers risks and opportunities

// SELF-ASSESSMENT PITFALLS

Self-assessment pitfall 2 - Not looking up information beyond the sheet



Design		
		Threat Assessment
pplication Risk Profile	1	**Do you classify applications according to business risk based on a simple and predefined set of questions?**
		An agreed-upon risk classification exists The application team understands the risk classification The risk classification covers critical aspects of business risks the organization is facing The organization has an inventory for the applications in scope
	2	**Do you use centralized and quantified application risk profiles to evaluate business risk?**
		The application risk profile is in line with the organizational risk standard The application risk profile covers impact to security and privacy You validate the quality of the risk profile manually and/or automatically The application risk profiles are stored in a central inventory
	3	**Do you regularly review and update the risk profiles for your applications?**
		The organizational risk standard considers historical feedback to improve the evaluation method Significant changes in the application or business context trigger a review of the relevant risk profiles

SAMM model overview

Governance	Design	Implementation	Verification	Operations
Strategy and Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Policy and Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Education and Guidance	Security Architecture	Defect Management	Security Testing	Operational Management

Model | Design | Threat Assessment

The Threat Assessment (TA) practice focuses on identifying and understanding of project-level risks based on the functionality of the software being developed and characteristics of the runtime environment. From details about threats and likely attacks against each project, the organization as a whole operates more effectively through better decisions about prioritization of initiatives for security. Additionally, decisions for risk acceptance are more informed, therefore better aligned to the business.

By starting with simple threat models and building application risk profiles, an organization improves over time. Ultimately, a sophisticated organization would maintain this information in a way that is tightly coupled to the compensating factors and pass-through risks from external entities. This provides greater breadth of understanding for potential downstream impacts from security issues while keeping a close watch on the organization's current performance against known threats.

Maturity level		Stream A Application Risk Profile	Stream B Threat Modeling
1	Best-effort identification of high-level threats to the organization and individual projects.	A basic assessment of the application risk is performed to understand likelihood and impact of an attack.	Perform best-effort, risk-based threat modeling using brainstorming and existing diagrams with simple threat checklists.
2	Standardization and enterprise-wide analysis of software-related threats within the organization.	Understand the risk for all applications in the organization by centralizing the risk profile inventory for stakeholders.	Standardize threat modeling training, processes, and tools to scale across the organization.
3	Proactive improvement of threat coverage throughout the organization.	Periodically review application risk profiles at regular intervals to ensure accuracy and reflect current state.	Continuously optimization and automation of your threat modeling methodology.

Model | Design | Threat Assessment | Application Risk Profile

Benefit

Ability to classify applications according to risk

Activity

Use a simple method to evaluate the application risk per application, estimating the potential business impact that it poses for the organization in case of an attack. To achieve this, evaluate the impact of a breach in the confidentiality, integrity and availability of the data or service. Consider using a set of 5-10 questions to understand important application characteristics, such as whether the application processes financial data, whether it is internet facing, or whether privacy-related data is involved. The application risk profile tells you whether these factors are applicable and if they could significantly impact the organization.

Next, use a scheme to classify applications according to this risk. A simple, qualitative scheme (e.g. high/medium/low) that translates these characteristics into a value is often effective. It is important to use these values to represent and compare the risk of different applications against each other. Mature highly risk-driven organizations might make use of more quantitative risk schemes. Don't invent a new risk scheme if your organization already has one that works well.

Question

Do you classify applications according to business risk based on a simple and predefined set of questions?

Quality criteria

An agreed-upon risk classification exists

The application team understands the risk classification

The risk classification covers critical aspects of business risks the organization is facing

Model | Design | Threat Assessment | Application Risk Profile

Benefit

Solid understanding of the risk level of your application portfolio

Activity

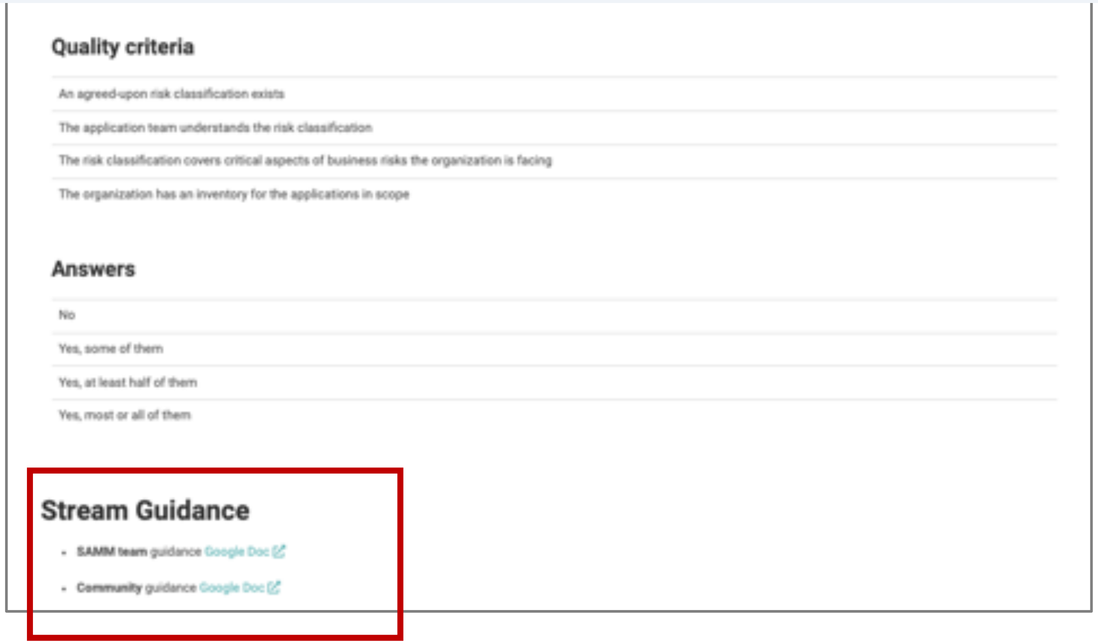
The goal of this activity is to thoroughly understand the risk level of all applications within the organization, to focus the effort of your software assurance
matters.

From a risk evaluation perspective, the basic set of questions is not enough to thoroughly evaluate the risk of all applications. Create an extensive and stan
the risk of the application, among others via their impact on information security (confidentiality, integrity and availability of data). Next to security, you also
privacy risk of the application. Understand the data that the application processes and what potential privacy violations are relevant. Finally, study the impa
has on other applications within the organization (e.g., the application might be modifying data that was considered read-only in another context). Evaluate
the organization, including all existing and legacy ones.

Leverage business impact analysis to quantify and classify application risk. A simple qualitative scheme (such as high/medium/low) is not enough to effec
compare applications on an enterprise-wide level.

Based on this input, Security Officers leverage the classification to define the risk profile to build a centralized inventory of risk profiles and manage accoun
gives Product Owners, Managers, and other organizational stakeholders an aligned view of the risk level of an application in order to assign appropriate pri
activities.

Self-assessment pitfall 2 - Not looking up information beyond the sheet



Quality criteria

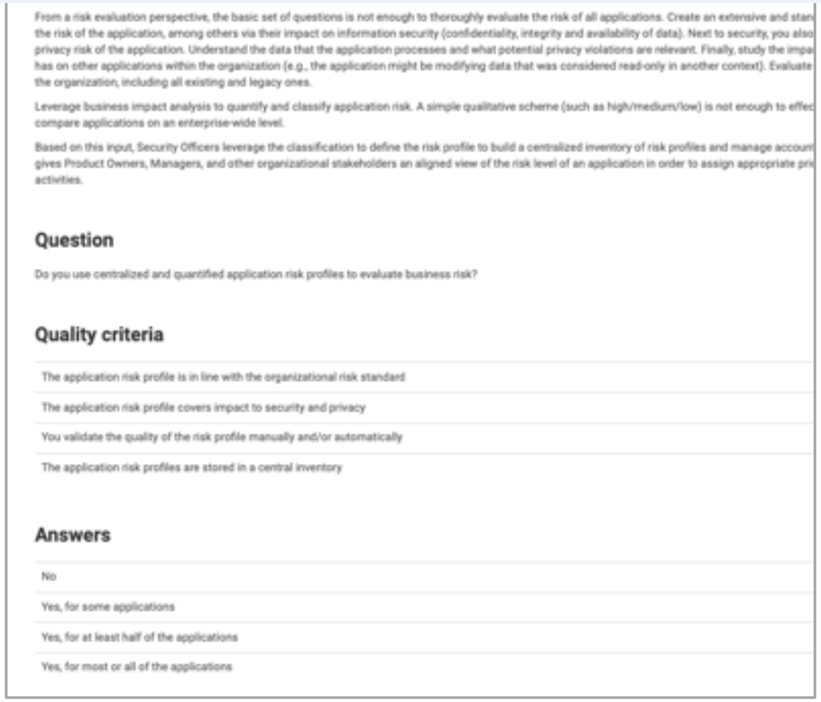
- An agreed-upon risk classification exists
- The application team understands the risk classification
- The risk classification covers critical aspects of business risks the organization is facing
- The organization has an inventory for the applications in scope

Answers

- No
- Yes, some of them
- Yes, at least half of them
- Yes, most or all of them

Stream Guidance

- **SAMM team** guidance Google Doc
- **Community** guidance Google Doc



From a risk evaluation perspective, the basic set of questions is not enough to thoroughly evaluate the risk of all applications. Create an extensive and stan
the risk of the application, among others via their impact on information security (confidentiality, integrity and availability of data). Next to security, you also
privacy risk of the application. Understand the data that the application processes and what potential privacy violations are relevant. Finally, study the impa
has on other applications within the organization (e.g., the application might be modifying data that was considered read-only in another context). Evaluate
the organization, including all existing and legacy ones.

Leverage business impact analysis to quantify and classify application risk. A simple qualitative scheme (such as high/medium/low) is not enough to effec
compare applications on an enterprise-wide level.

Based on this input, Security Officers leverage the classification to define the risk profile to build a centralized inventory of risk profiles and manage account
gives Product Owners, Managers, and other organizational stakeholders an aligned view of the risk level of an application in order to assign appropriate pri
activities.

Question

Do you use centralized and quantified application risk profiles to evaluate business risk?

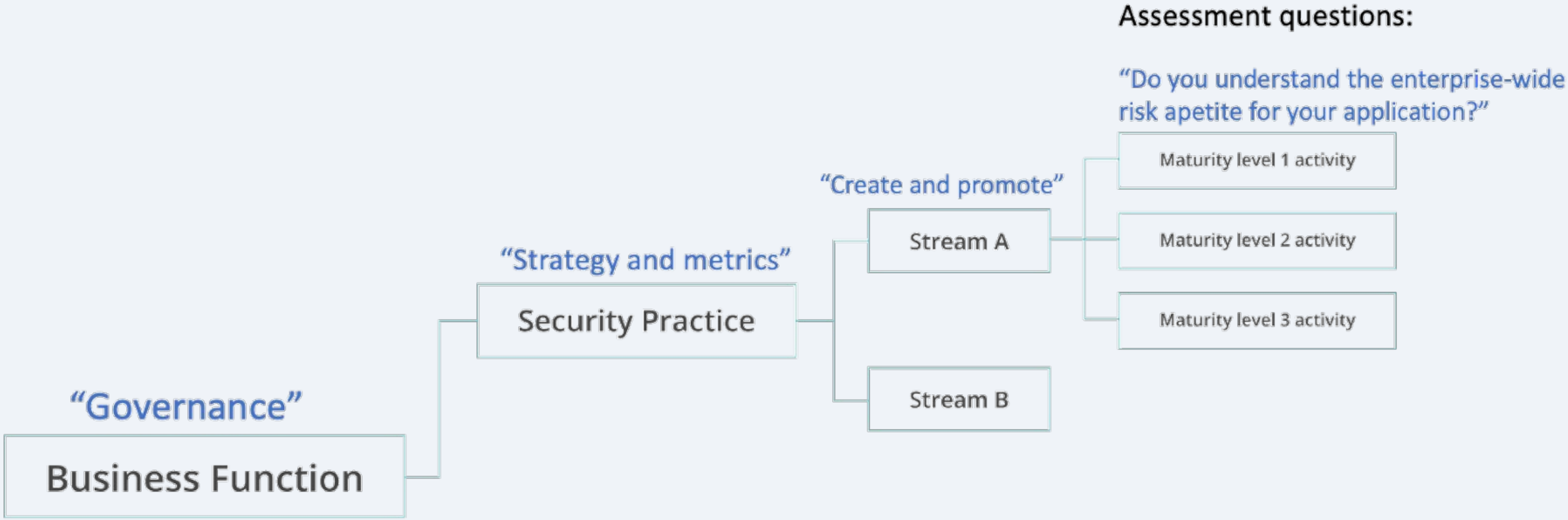
Quality criteria

- The application risk profile is in line with the organizational risk standard
- The application risk profile covers impact to security and privacy
- You validate the quality of the risk profile manually and/or automatically
- The application risk profiles are stored in a central inventory

Answers

- No
- Yes, for some applications
- Yes, for at least half of the applications
- Yes, for most or all of the applications

Sidestep – the SAMM model structure



Assessment questions:

“Do you understand the enterprise-wide risk apetite for your application?”

“Governance”

Business Function

“Strategy and metrics”

Security Practice

“Create and promote”

Stream A

Stream B

Maturity level 1 activity

Maturity level 2 activity

Maturity level 3 activity

Self-assessment pitfall 3: assessing too literally - positively

- **Purpose of assessment**: judge whether the goal behind the requirement (SAMM question, Quality criteria) is met sufficiently, by a sufficient application of the controls
- **Example**: “Developers need to follow a training”
  - Let’s say people watch a training video every year of about an hour
  - Let’s say it satisfies all Quality criteria
  - The self-assessor may take the criteria too literally: “Great, they follow training”: Positive
- Assessment requires judging and that **requires deep expertise** about secure software development (e.g. what types of training are effective)
- Self-assessors typically don’t have that deep expertise
- Result:
  - Self-assessors will lean to more positive assessment
  - If self-assessment is the only way of assessment, this may lead to shallow implementation, or even *Cargo cult*

Self-assessment pitfall 4: assessing too literally - negatively

- **Example**: “The organization needs a TMS tool (Training Management System)”
  - Let’s say that somebody tracks progress using a shared Google sheet
  - The self-assessor takes the criteria too literally: “That’s not a TMS tool”: Negative
- The spirit of the requirement is to have systematic and shared administration of training
- Result:
  - If self-assessment is the only way of assessment, this may lead to implementation with unnecessarily complex or costly meausures – gold plating

Pros and cons of self-assessment

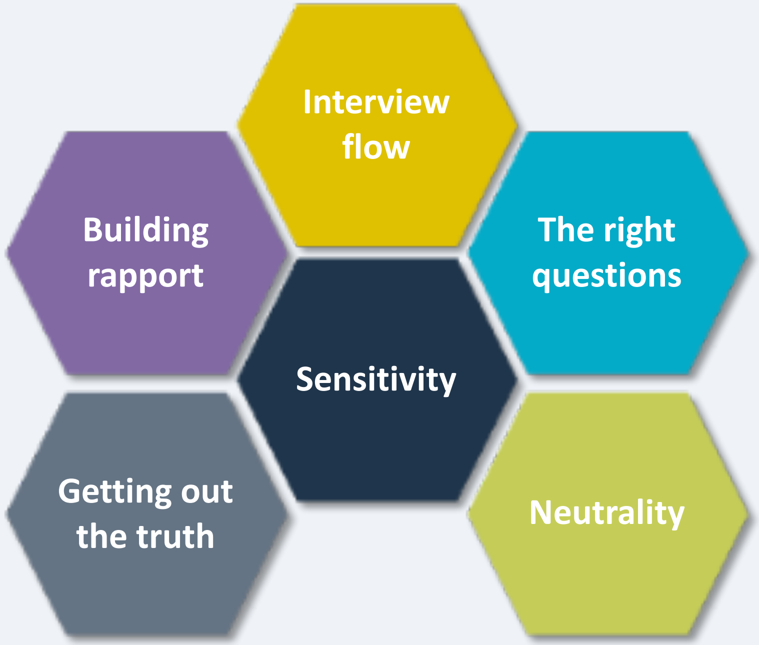
PRO	CON
Cheaper & quicker to arrange	Less accurate and typically too positive
Faster – typically no interviews and studying	Misinterpretations can lead to wrong assessment
Positive learning effect	May lead to cargo cult, or gold plating
	May be biased - personally and socially
	No recommendations about the how

The best practice is for an organization to have a good mix of self-assessment and independent expert assessment.

The art of expert assessment

*

- **Interview**:
  - Necessary to assess, unless everything is perfectly documented (never)
  - Provides insights into a world; opinions, thougths, issues and feelings***
  - Helps to clarify questions ****
  - Allows doublechecking of answers or follow-up questions on the spot *****
  - Helps reduce question-fatigue ******


Interview flow

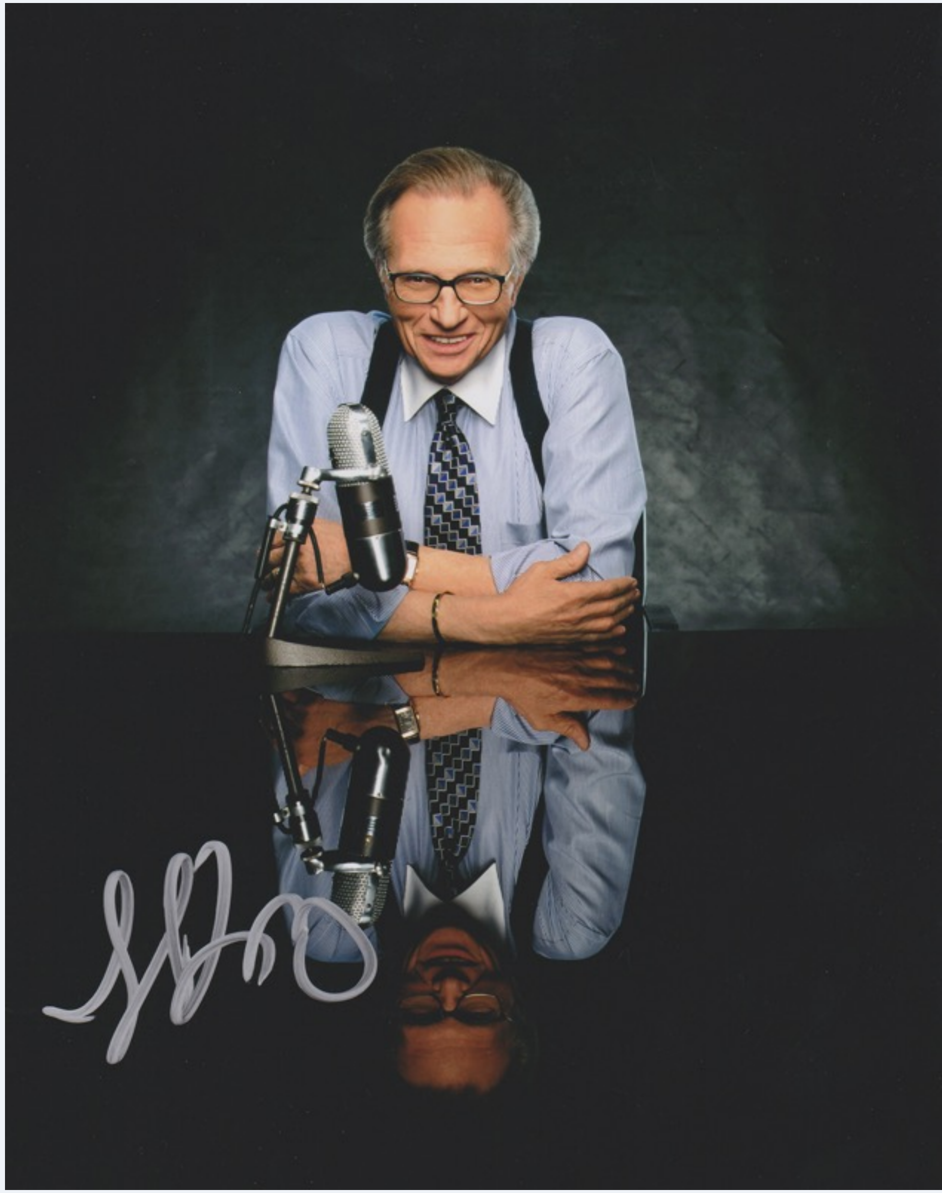
Building rapport

The right questions

Sensitivity

Getting out the truth

Neutrality



The art of building rapport*

Building rapport

- **Be likeable**
  - Be courteous
  - Even more: Be friendly (warm, approachable and easy to relate with in character)
  - Respectful
  - Humble – you need help
  - Be fun – a bit of humour. Be careful wih humour in an international setting that you're not familiar with**.
- **Connect**
  - Be relevant – find connection points. Know the client's context. Talk about food,travel, sports, children or things important to you.
- **Authentic** - Be yourself
- **Credible** - Demonstrate it***
- Create **harmony**
  - Mirror their energy level
  - Uncover insights together: collaborate NOT interrogate
  - Have a natural conversation, not a robotic one ****

The art of sensitivity

Sensitivity

- Understand that the person may feel **threatened** – be careful with being too direct.
- Ask about **facts before controversial** matters
- **Avoid remembering people that what is said is being noted**
  - Keep keyboard noise down*
  - Put your pencil down at sensitive moments (only works face to face)
  - See if you can avoid having the laptop become a wall between you and the group

The art of interview flow

- Turn it into **a natural conversation**
  Don't follow a strict order. You'll get more information.*
- Steer
  - Ask **one question** at a time
  - **Direct** your question at someone. To avoid a group hesitating. Not the most dominant person per se. Motivate others to join, esp the silent people. "How do YOU see this?" **
  - Give interviewees a **sense of structure** - provide transition between major topics.
  - **Gentle but clear** steering. Don't lose control. Find a balance between pushing your questions and letting the interviewee digress a bit.
- React
  - **Encourage** responses with enthusiasm
  - **Listen**. Confirm with "yes, uh-huh, and I see". **Paraphrase.**
  - Ask **follow-up** questions. "How often does that happen" Be really curious****
  - Give **the feeling you listened** instead of stormed in and have them answer 20 questions.
    You may need their support later.

The art of the right questions

- Ask **open-ended** questions
- Follow your prepared **interview guide**, applying the art of minimizing questions and skipping questions
- **Deviate** from the prepared orderwhere necessary to allow flow

The right questions

The art of minimizing questions

Prepare questions for which the answers are likely to cover as many things on your checklist as possible.

Example checklist of things to find out:

Do you understand the enterprise-wide risk appetite for your applications ?

"You capture the risk appetite of your organization's executive leadership
The organization's leadership vet and approve the set of risks
You identify the main business and technical threats to your assets and data
You document risks and store them in an accessible location"

Do you have a strategic plan for application security and use it to make decisions?

"The plan reflects the organization's business priorities and risk appetite
The plan includes measurable milestones and a budget
The plan is consistent with the organization's business drivers and risks
The plan lays out a roadmap for strategic and tactical initiatives
You have buy-in from stakeholders, including development teams"

Do you regularly review and update the Strategic Plan for Application Security?

"You review and update the plan in response to significant changes in the business environment, the organization, or its risk appetite
Plan update steps include reviewing the plan with all the stakeholders and updating the business drivers and strategies
You adjust the plan and roadmap based on lessons learned from completed roadmap activities
You publish progress information on roadmap activities, making sure they are available to all stakeholders"

Do you have and apply a common set of policies and standards throughout your organization?

"You have adapted existing standards appropriate for the organization’s industry to account for domain-specific considerations
Your standards are aligned with your policies and incorporate technology-specific implementation guidance"

Do you have a complete picture of your external compliance obligations?

"You have identified all sources of external compliance obligations
You have captured and reconciled compliance obligations from all sources"

Guide with interview questions:

Question:
What do you get as input in documentation or instruction from the organisation regarding security?

Notes:

For example: risks, threats, assets specifications, security plan, business priorities, metrics, KPIs, policies, standards, compliance obligations, requirements

Can we see it? How is it accessible? Does everybody know about it?

Ask what they are missing.

In case of a security plan: is it regularly reviewed and updated? Is progress communicated?

The art of being neutral

Neutrality

- Be aware: **Interviewers are known to bias results**
- Various **studies** found that:
  - Attitudes and opinions reported by interviewers are positively correlated with the interviewers’ own attitudes and opinions
  - When responses are vague the interviewer, through projection, tends to classify them in the direction of their own bias
- When answers are ambigious, **ask for clarification**
- Also: **Do not ask leading questions**.

The art of getting out the truth

Getting out the truth

- Ask **how things really happened recently**, not how they should happen
- Be aware that **interviewee's may lie**

  - e.g. Due diligence
  - e.g. Shame
  - e.g. Protect colleagues and the individual
- **Ask for artefacts**

  - sample –based
  - early in the interview
- Delicate? **Rephrase** the question to hide the goal :
  "Do you have access to the internet in the factory"
  ->
  "What internet browser are you using on factory machines"