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

SAMM User day, Washington DC
November 1\textsuperscript{st} 2023
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)
Common requirements are structured in the OpenCRE catalog

OpenCRE catalog of common requirements

Standards and guidelines linked through each requirement

- CAPEC 221 – understand the threat
- CWE 611 – recognize the weakness
- OWASP Test guide INPV-07 - how to test
- Cheat sheet XML EE – how to code

Part of

CRE 503-455 Input & output protection

NIST 53- SI 10 Input validation

Governance

Development process

Technical controls

Operations

Cross-cutting concerns
Demo
How OpenCRE connects everything

WrongSecrets documentation

OpenCRE page on Storing secrets

‘Learn more about storing secrets’
How OpenCRE connects everything - linking through

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

WrongSecrets documentation

OpenCRE page on Secret Storage

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

OWASP cheat sheet “Secrets management”
How OpenCRE connects everything - linking through

WrongSecrets documentation

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

OWASP cheat sheet “Secrets management”

OpenCRE page on Secret Storage

OpenCRE page on Storing keys
How OpenCRE connects everything - linking back

WrongSecrets documentation

‘Learn more about storing secrets’

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

OWASP cheat sheet “Secrets management”

OpenCRE page on Secret Storage

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

Model | Implementation | Secure Deployment | Secret Management

Maturity Level 1 | Maturity Level 2 | Maturity Level 3

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 development environments may have a significantly lower security posture than configuration files stored in code repositories.

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

Core Team Guidance

I-SD-B
Implementation | Secure Deployment
Stream B - Secret Management

OWASP Projects and References
OpenCRE 223/380 for references and related topics

Secret storage
CRE: 223-780

Which contains CREs:
- CRE: 032-213: Use an isolated security environment
- CRE: 077-781: Use separately stored secrets
- CRE: 078-827: Set the highest feasible security level for the secret
- CRE: 082-530: Use unique random salt with each attempt
- CRE: 340-375: Use a dedicated secrets management
- CRE: 508-792: Use key vault
- CRE: 622-203: Store passwords salted and hashed
- CRE: 767-435: Set the highest feasible security level for the secret
- CRE: 774-888: Do not store secrets in the clear
- CRE: 783-255: Store cryptographic keys securely
- CRE: 821-832: Ensure keys and passwords are replaceable
- CRE: 881-321: Store credentials securely

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

OWASP Projects and References
OWASP 223/380 for references and related topics

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

Step 1: match using LLM

Step 2: construct prompt with the matched information

Step 3: the LLM answers the prompt

Trainset: The internet

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

Reference to OpenCRE
Reference to standard

OpenCRE Chat - how

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

..........................................................
..........................................................
..........................................................
..........................................................”
## Map analysis

### Cloud Controls Matrix: TVM: Threat & Vulnerability Management

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001:8.8</td>
<td>Management of technical vulnerabilities (Direct:0)</td>
</tr>
<tr>
<td>ISO 27001:5.26</td>
<td>Response to information security incidents (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:8.33</td>
<td>Test Information (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:5.28</td>
<td>Collection of evidence (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:5.37</td>
<td>Documented operating procedures (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:8.31</td>
<td>Separation of development, test and production environments (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:8.29</td>
<td>Security testing in development and acceptance (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:5.24</td>
<td>Information security incident management planning and preparation (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:6.8</td>
<td>Information security event reporting (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:5.23</td>
<td>Information security for use of cloud services (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:5.25</td>
<td>Assessment and decision on information security events (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:5.27</td>
<td>Learning from information security incidents (Strong:2)</td>
</tr>
</tbody>
</table>

### Cloud Controls Matrix: BCR: Business Continuity Management and Operational Resilience

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001:8.14</td>
<td>Redundancy of information processing facilities (Direct:0)</td>
</tr>
<tr>
<td>ISO 27001:5.29</td>
<td>Information security during disruption (Direct:0)</td>
</tr>
<tr>
<td>ISO 27001:3.30</td>
<td>ICT readiness for business continuity (Direct:0)</td>
</tr>
<tr>
<td>ISO 27001:8.13</td>
<td>Information backup (Strong:2)</td>
</tr>
</tbody>
</table>

### Cloud Controls Matrix: HRS: Human Resources

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001:6.6</td>
<td>Confidentiality or non-disclosure agreements (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:5.2</td>
<td>Information security roles and responsibilities (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:6.5</td>
<td>Responsibilities after termination or change of employment (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:6.4</td>
<td>Disciplinary process (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:6.3</td>
<td>Information security awareness, education and training (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:6.1</td>
<td>Screening (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:5.11</td>
<td>Return of assets (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:6.2</td>
<td>Terms and conditions of employment (Strong:2)</td>
</tr>
<tr>
<td>ISO 27001:5.4</td>
<td>Management responsibilities (Strong:2)</td>
</tr>
</tbody>
</table>
Selected lessons from SAMM assessments by SIG

Rob van der Veer
# Self-Assessment Pitfall 1: Thinking the Quality Criteria are Not Mandatory

<table>
<thead>
<tr>
<th>Stream</th>
<th>Level</th>
<th>Strategy &amp; Metrics</th>
<th>Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td><em>Do you understand the enterprise-wide risk appetite for your applications?</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- You capture the risk appetite of your organization’s executive leadership</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The organization’s leadership vet and approve the set of risks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- You identify the main business and technical threats to your assets and data</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- You document risks and store them in an accessible location</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td><em>Do you have a strategic plan for application security and use it to make decisions?</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The plan reflects the organization’s business priorities and risk appetite</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The plan includes measurable milestones and a budget</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The plan is consistent with the organization’s business drivers and risks</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The plan lays out a roadmap for strategic and tactical initiatives</td>
<td></td>
</tr>
</tbody>
</table>
Self-assessment pitfall 2 - Not looking up information beyond the sheet
Self-assessment pitfall 2 - Not looking up information beyond the sheet

Stream Guidance
- SARIM team guidance [Google Doc]
- Community guidance [Google Doc]
Sidestep – the SAMM model structure

Assessment questions:

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

Maturity level 1 activity

Maturity level 2 activity

Maturity level 3 activity

“Strategy and metrics”

Security Practice

“Create and promote”

Stream A

Stream B

“Governance”

Business Function
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 measures – gold plating
# SELF-ASSESSMENT PITFALLS

## Pros and cons of self-assessment

<table>
<thead>
<tr>
<th>PRO</th>
<th>CON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cheaper &amp; quicker to arrange</td>
<td>Less accurate and typically too positive</td>
</tr>
<tr>
<td>Faster – typically no interviews and studying</td>
<td>Misinterpretations can lead to wrong assessment</td>
</tr>
<tr>
<td>Positive learning effect</td>
<td>May lead to cargo cult, or gold plating</td>
</tr>
<tr>
<td></td>
<td>May be biased - personally and socially</td>
</tr>
<tr>
<td></td>
<td>No recommendations about the how</td>
</tr>
</tbody>
</table>

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, thoughts, issues and feelings
  - Helps to clarify questions
  - Allows double-checking of answers or follow-up questions on the spot
  - Helps reduce question-fatigue

Diagram showing:
- Interview flow
- Building rapport
- Sensitivity
- Getting out the truth
- The right questions
- Neutrality
The art of 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 with 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

- 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 order where necessary to allow flow
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:

<table>
<thead>
<tr>
<th>Question</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>What do you get as input in documentation or instruction from the organisation regarding security?</td>
<td>For example: risks, threats, assets specifications, security plan, business priorities, metrics, KPIs, policies, standards, compliance obligations, requirements</td>
</tr>
<tr>
<td>Can we see it? How is it accessible? Does everybody know about it?</td>
<td>Ask what they are missing.</td>
</tr>
<tr>
<td>In case of a security plan: is it regularly reviewed and updated? Is progress communicated?</td>
<td></td>
</tr>
</tbody>
</table>

Example checklist of things to find out:
The art of being neutral

- 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 ambiguous, **ask for clarification**
- Also: **Do not ask leading questions.**
The art of 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”