Improving the chances of success in software security for your Software development

Daniela Soares Cruzes

CISO at VISMA

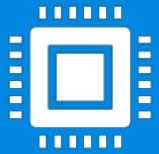
VISMA

About me

Daniela Cruzes

VISMA

Software Security Initiative



Engineering software so that it continues to function correctly under malicious attack.

Encompasses all the activities undertaken for the purpose of building secure software:

- Technical
- Business
- Social
- Organizational

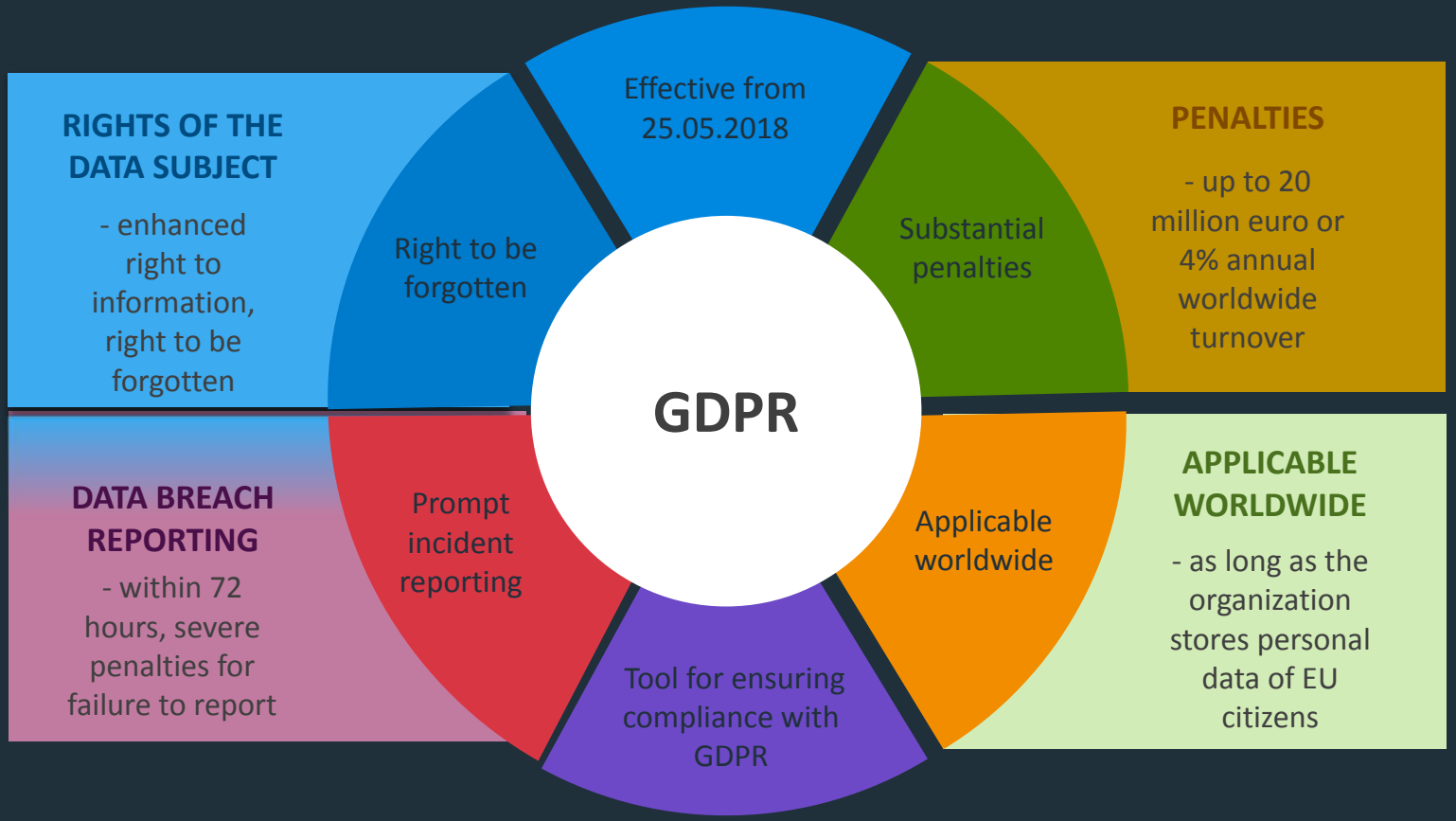
10

1

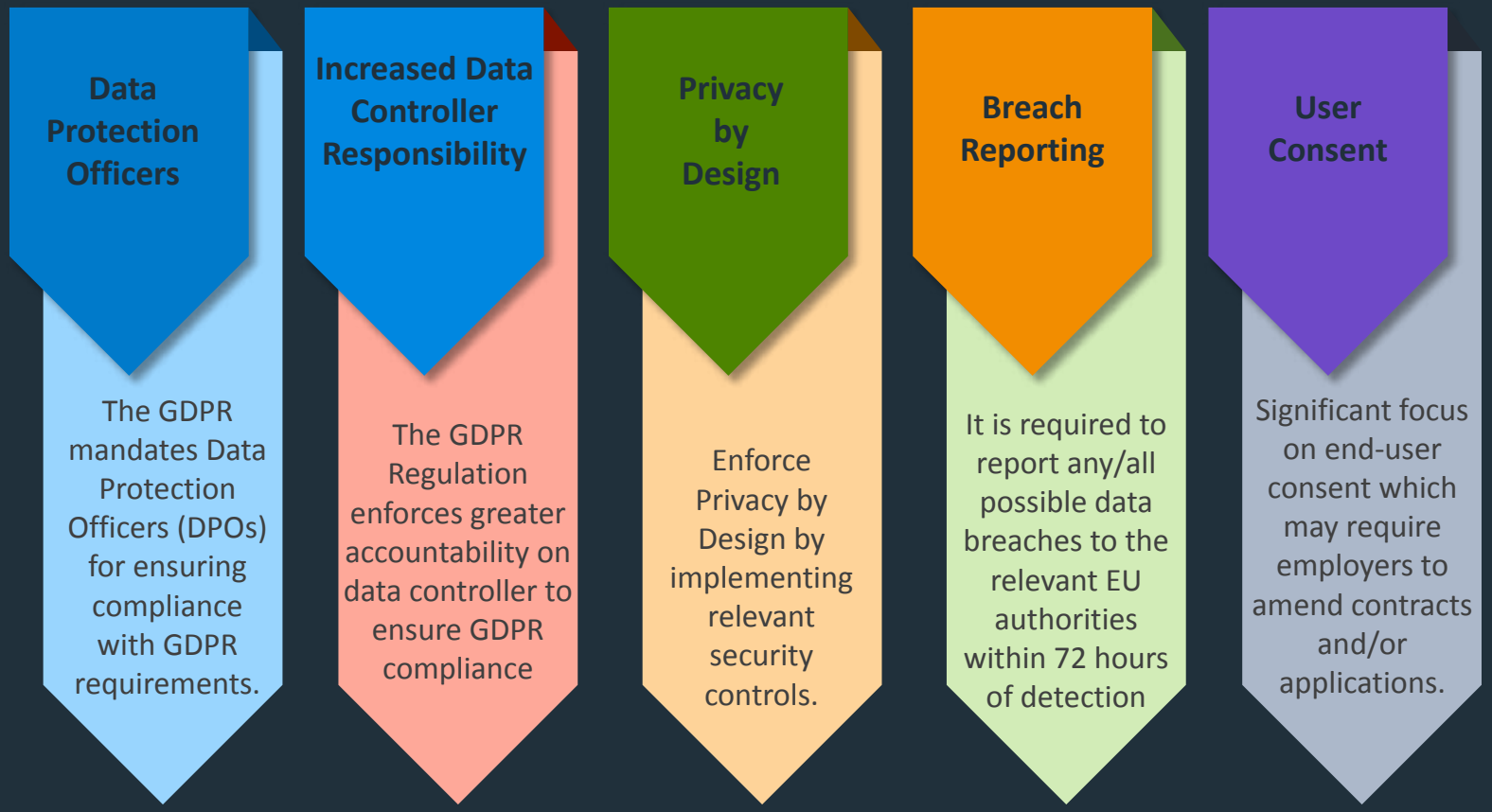
Define your own "adequate" level of security


FEDERAL RESERVE
SEC
REGULATIONS
BANK
JOB

GDPR


RIGHTS OF THE DATA SUBJECT
- enhanced right to information, right to be forgotten
Right to be forgotten
Effective from 25.05.2018
Substantial penalties
PENALTIES
- up to 20 million euro or 4% annual worldwide turnover
GDPR
DATA BREACH REPORTING
- within 72 hours, severe penalties for failure to report
Prompt incident reporting
Tool for ensuring compliance with GDPR
Applicable worldwide
APPLICABLE WORLDWIDE
- as long as the organization stores personal data of EU citizens

GDPR


Data Protection Officers
The GDPR mandates Data Protection Officers (DPOs) for ensuring compliance with GDPR requirements.
Increased Data Controller Responsibility
The GDPR Regulation enforces greater accountability on data controller to ensure GDPR compliance
Privacy by Design
Enforce Privacy by Design by implementing relevant security controls.
Breach Reporting
It is required to report any/all possible data breaches to the relevant EU authorities within 72 hours of detection
User Consent
Significant focus on end-user consent which may require employers to amend contracts and/or applications.

NIS2

Network and Information Systems Directive 2

https://www.linkedin.com/posts/andrejsavin_nis2-cybersecurity-in-practice-compliance-activity-7284902428146044929-Zlu0

Article 21

https://www.cyberday.ai/blog/nis2-overview-history-key-contents-and-significance-for-top-management

2

Assess your Software Security Practices

OpenSAMM

ISO/IEC 27001:2022

https://www.opensamm.org/

https://www.iso.org/standard/27001

OWASP OpenSAMM 2.0

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

https://owaspsamm.org/

SAMM ASSESSMENT

Analyze your security posture using our maturity measurement tool.

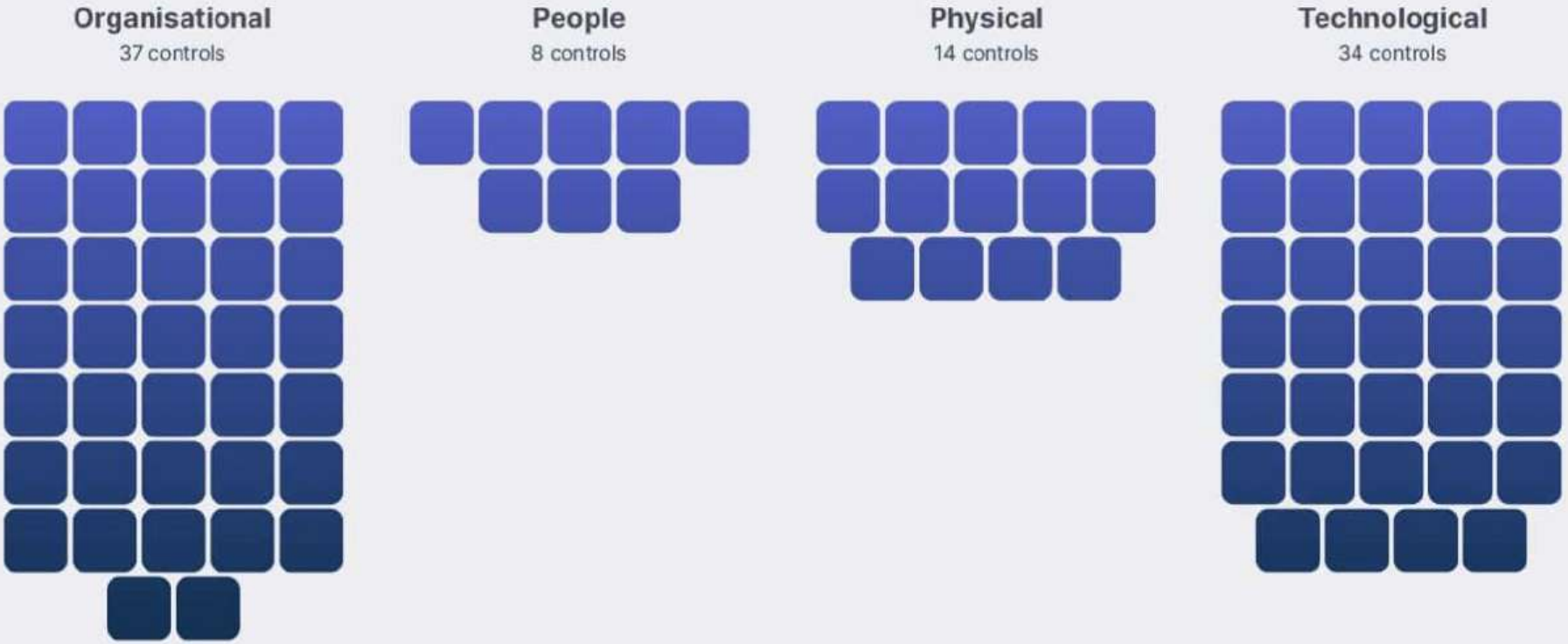
Attribution and License | Interview | Scorecard | Roadmap | Roadmap Chart | Lookups | imp-questions | imp-answers

Design

		Threat Assessment		Answer		
Application Risk Profile	1	**Do you classify applications according to business risk based on a simple and predefined set of questions?**	0		0	0,000
		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?**	0		0	0,000
		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?**	0		0	0,000
		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				
Threat Modeling	1	**Do you identify and manage architectural design flaws with threat modeling?**	0		0	
		You perform threat modeling for high-risk applications You use simple threat checklists, such as STRIDE You persist the outcome of a threat model for later use				
	2	**Do you use a standard methodology, aligned on your application risk levels?**	0		0	
		You train your architects, security champions, and other stakeholders on how to do practical threat modeling Your threat modeling methodology includes at least diagramming, threat identification, design flaw mitigations, and how to validate your threat model artifacts Changes in the application or business context trigger a review of the relevant threat models You capture the threat modeling artifacts with tools that are used by your application teams				
	3	**Do you regularly review and update the threat modeling methodology for your applications?**	0		0	
		The threat model methodology considers historical feedback for improvement You regularly (e.g., yearly) review the existing threat models to verify that no new threats are relevant for your applications You automate parts of your threat modeling process with threat modeling tools				
		Security Requirements		**Answer**		
Software Requirements	1	**Do project teams specify security requirements during development?**	0		0	0,000
		Teams derive security requirements from functional requirements and customer or organization concerns Security requirements are specific, measurable, and reasonable Security requirements are in line with the organizational baseline				
	2	**Do you define, structure, and include prioritization in the artifacts of the security requirements gathering process?**	0		0	0,000
		Security requirements take into consideration domain specific knowledge when applying policies and guidance to product development Domain experts are involved in the requirements definition process You have an agreed upon structured notation for security requirements Development teams have a security champion dedicated to reviewing security requirements and outcomes				
	3	**Do you use a standard requirements framework to streamline the elicitation of security requirements?**	0		0	0,000
		A security requirements framework is available for project teams The framework is categorized by common requirements and standards-based requirements The framework gives clear guidance on the quality of requirements and how to describe them The framework is adaptable to specific business requirements				
Supplier	1	**Do stakeholders review vendor collaborations for security requirements and methodology?**	0		0	
		You consider including specific security requirements, activities, and processes when creating third-party agreements A vendor questionnaire is available and used to assess the strengths and weaknesses of your suppliers				
	2	**Do vendors meet the security responsibilities and quality measures of service level agreements defined by the organization?**	0		0	
		You discuss security requirements with the vendor when creating vendor agreements Vendor agreements provide specific guidance on security defect remediation within an agreed upon timeframe The organization has a templated agreement of responsibilities and service levels for key vendor security processes You measure key performance indicators				

Dicti

ANNEX A CONTROL CATEGORIES



https://www.isms.online/iso-27001/annex-a/

https://advisera.com/27001academy/explanation-of-11-new-iso-27001-2022-controls/

3

Formally Include Security Activities in your Development process

Software Engineering

Brian Randal definition (1968)

"Software engineering is the establishment and use of sound engineering principles in order to obtain economically software that is reliable and works efciently on real machines."

Chapter 27 Secure Systems Development - Security Engineering Book - Ross Anderson.

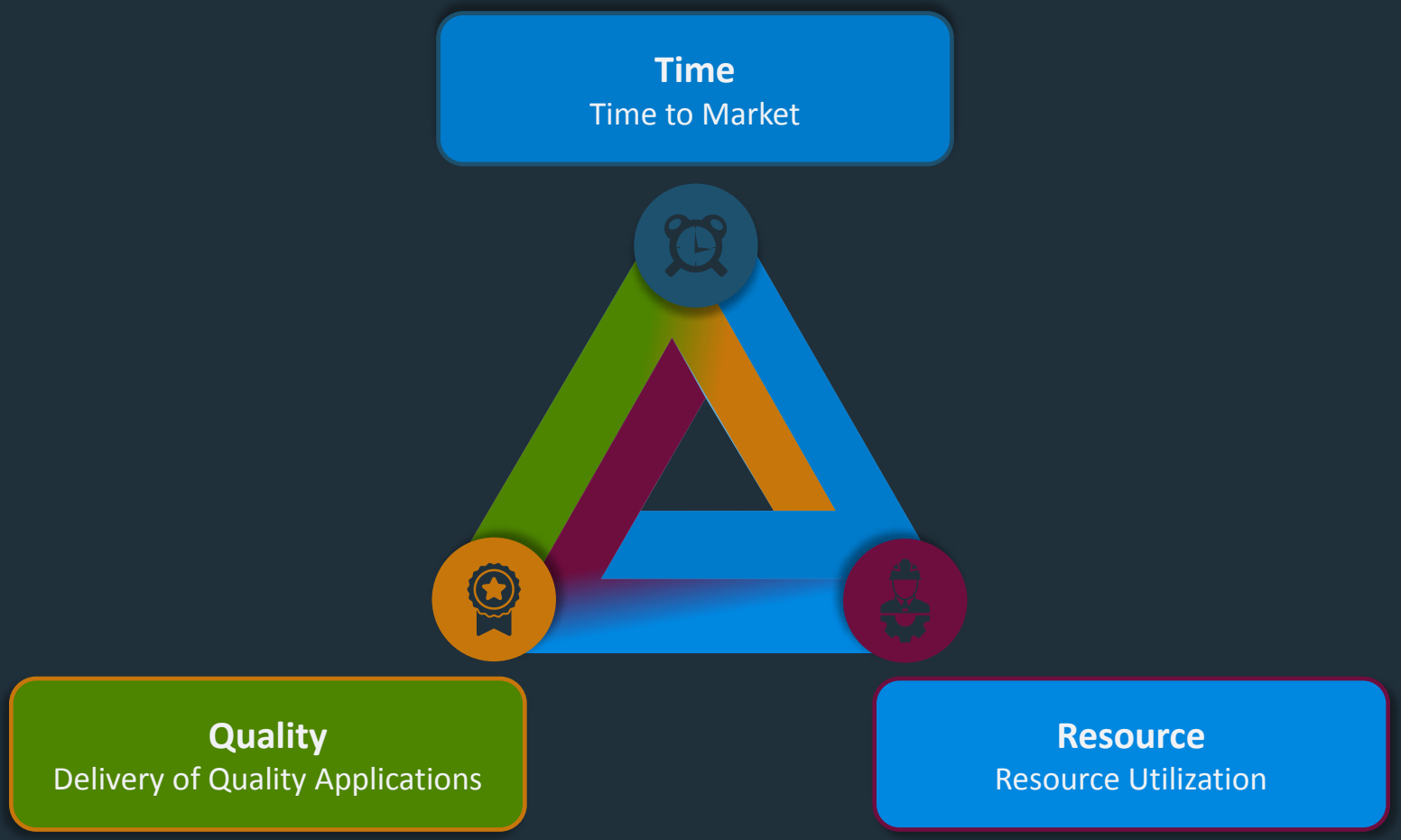
Two questions you have to ask are:

“Are we building the right system?”

and

“Are we building it right?”

SOFTWARE QUALITY CHALLENGES



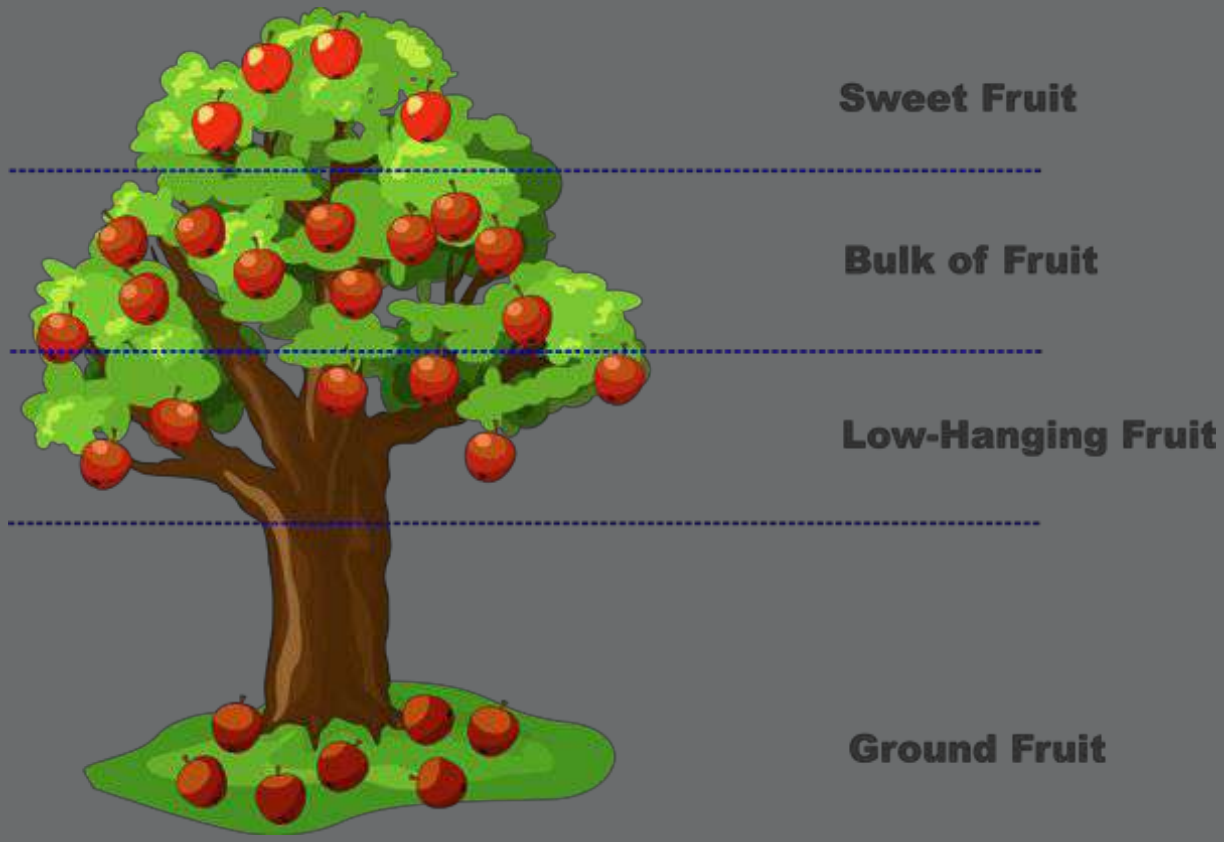
Sources: Segue

Prioritising protection goals

“At the heart of security engineering lie decisions about priorities: how much to spend on protection against what. Given that in business, profit is many times the reward for risks”

Risk Management - Security Engineering Book

What will you do to pick all fruits?



Waterfall way to managing risks...

Approvals and Gatecontrols...

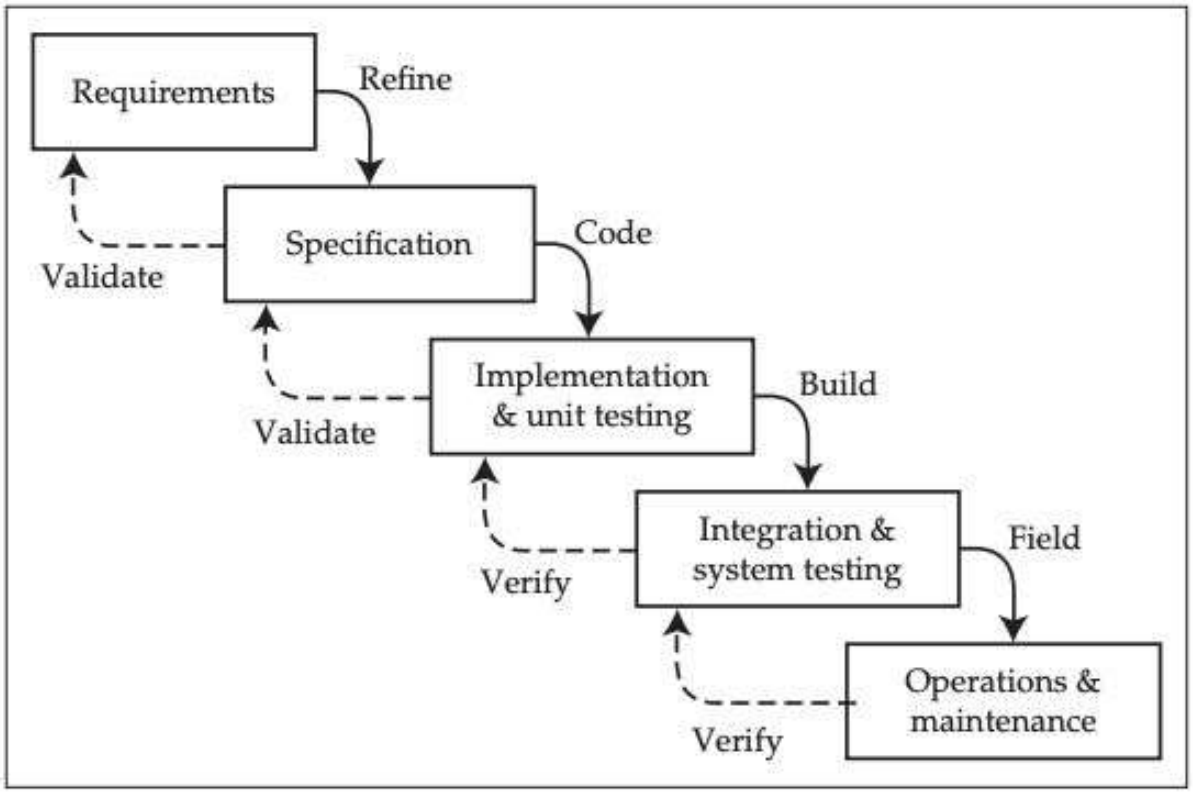


Figure 27.4: The waterfall model

Spiral model of managing risk…

The key is to solve the worst problem you're facing, so as to reduce the project risk as much as possible.

"Solve your worst problem. Repeat"

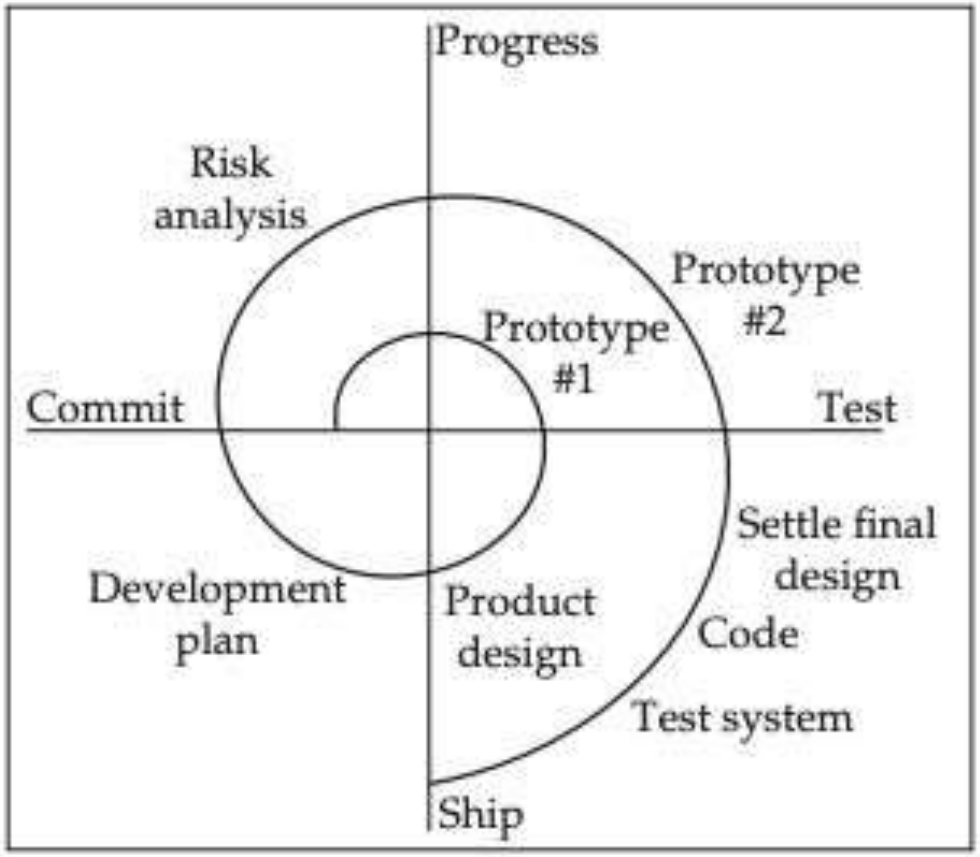


Figure 27.5: The spiral model

SaaS

Software as a Service

The key technical innovations behind SaaS are continuous integration and continuous deployment (CI/CD).

From DevOps to DevSecOps

Not just maintaining an existing security rating but responding to new threats, environmental changes, and surprising vulnerabilities.

The organising principles for DevSecOps is to ‘shift left’: the unifying theme is moving security, like software and infrastructure, into the codebase

When then to have security?
Why isnt security a phase?

Requirements ?
Design ?
Implementation?
Verification?
Release?

Microsoft Security Development Lifecycle

Start here

https://www.microsoft.com/en-us/securityengineering/sdl

microsoft.com/en-us/securityengineering/sdl/about

Ecosystem - Mana... CISO Ecosystems... 360° Business Insi... Risk Report - Adm... R12 Products - Go... TP: Room booking One Support - Ser... Addressable Mark...

Security Development Lifecycle (SDL) Timeline

- Growth of home PC's
- Rise of malicious software
- Increasing privacy concerns
- Internet use expansion

- Bill Gates' TwC memo
- Microsoft security push
- Microsoft SDL released
- SDL becomes mandatory policy at Microsoft
- Windows XP SP2 and Windows Server 2003 launched with security emphasis

- Windows Vista and Office 2007 fully integrate the SDL
- SDL released to public
- Data Execution Prevention (DEP) & Address Space Layout Randomization (ASLR) introduced as features
- Threat Modeling Tool

- Microsoft joins SAFECode & establishes SDL Pro Network
- DISA & NIST featured in the SDL
- Microsoft collaborates with Adobe and Cisco on SDL practices
- SDL revised under the Creative Commons License
- Microsoft declares Conformity to ISO 27034-1

- Additional resources dedicated to address projected growth in Mobile app downloads
- Industry-wide acceptance of practices aligned with SDL
- Adaption of SDL to new technologies and changes in the threat landscape
- Increased industry resources to enable global secure development adoption

- Log4shell (log4J), Solarwinds, XZ, and other vulnerabilities
- Executive Order 14028
- Microsoft acquires GitHub + GitHub acquires Semmle
- Microsoft contributes **Secure Supply Chain Consumption Framework (S2C2F)** to OpenSSF
- Microsoft Implements **CodeQL** as our single standard
- **Secure Future Initiative (SFI)** including Executive Accountability

4

Rethink roles and responsibilities towards security

Who does what?

Visma
Security Program

Roles at the Company

Asset Owner

(Product / Solution / Infrastructure / HR)

based in the specific Asset delivery team, responsible to manage and prioritize the asset delivery backlog, including the security requirements.

Security Contact/Coordinator

based in the Visma companies or segments and responsible for overseeing the overall security operations of the organization.

Security Engineer/Champion

based in the specific Product/ Solution Team with expert knowledge of the Visma Application/ Solutions Security Program and knowledge of the relevant security and privacy requirements.

Data Protection Manager

based in the Visma companies or segments and responsible for overseeing the existing processes related to privacy and for implementing necessary measures to ensure compliance.

The role of the Security Engineer/Champion

Visma Security Program

1. Seek for **Knowledge: technical and on processes.**
2. **Assist** with technical activities in Security: threat modelling, triage etc.
3. Help **adoption** of the security strategy for the product
4. Help on the process of **self-managing** security in the team.
5. **Not the ONE responsible for security in the team!**

VISMA

The role of the Developers

Visma
Security Program

1. Have knowledge for correct secure coding
2. Support the management with security knowledge for better prioritization of security
3. Identify and speak up when security threats are arising
4. Follow up with security tools and security work
5. Practice responsible security Every day

VISMA

The role of the Managers

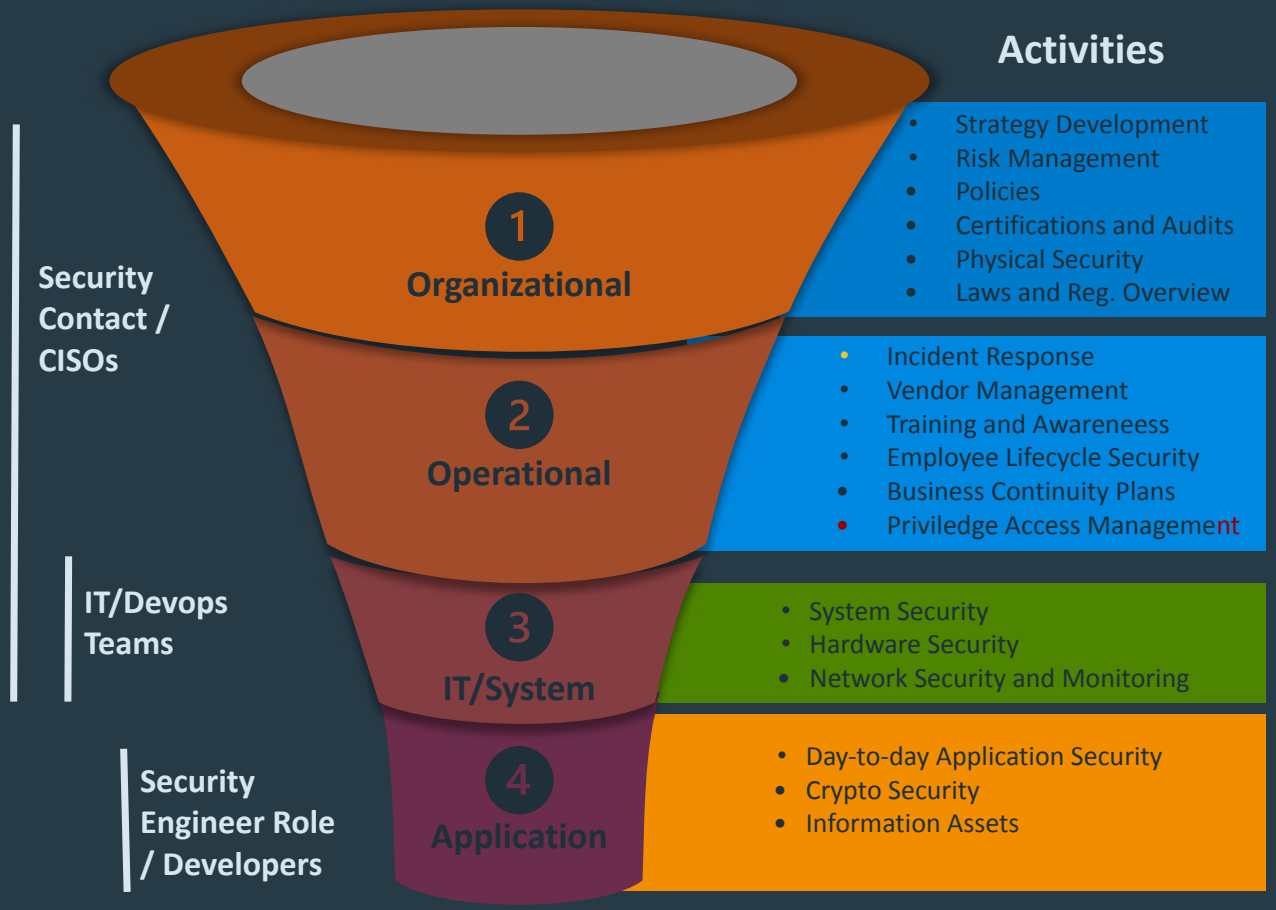
Visma
Security Program

1. Have enough security knowledge to make the right decision and prioritization of work.
2. Make sure that new features do not increase the attack surface of the products
3. Follow up with the Security Progress

VISMA

Security Tasks and Roles and Responsibilities

Visma
Security Program



5

Create your own Training Program

INSTRUCTOR LED TRAINING

E-LEARNING

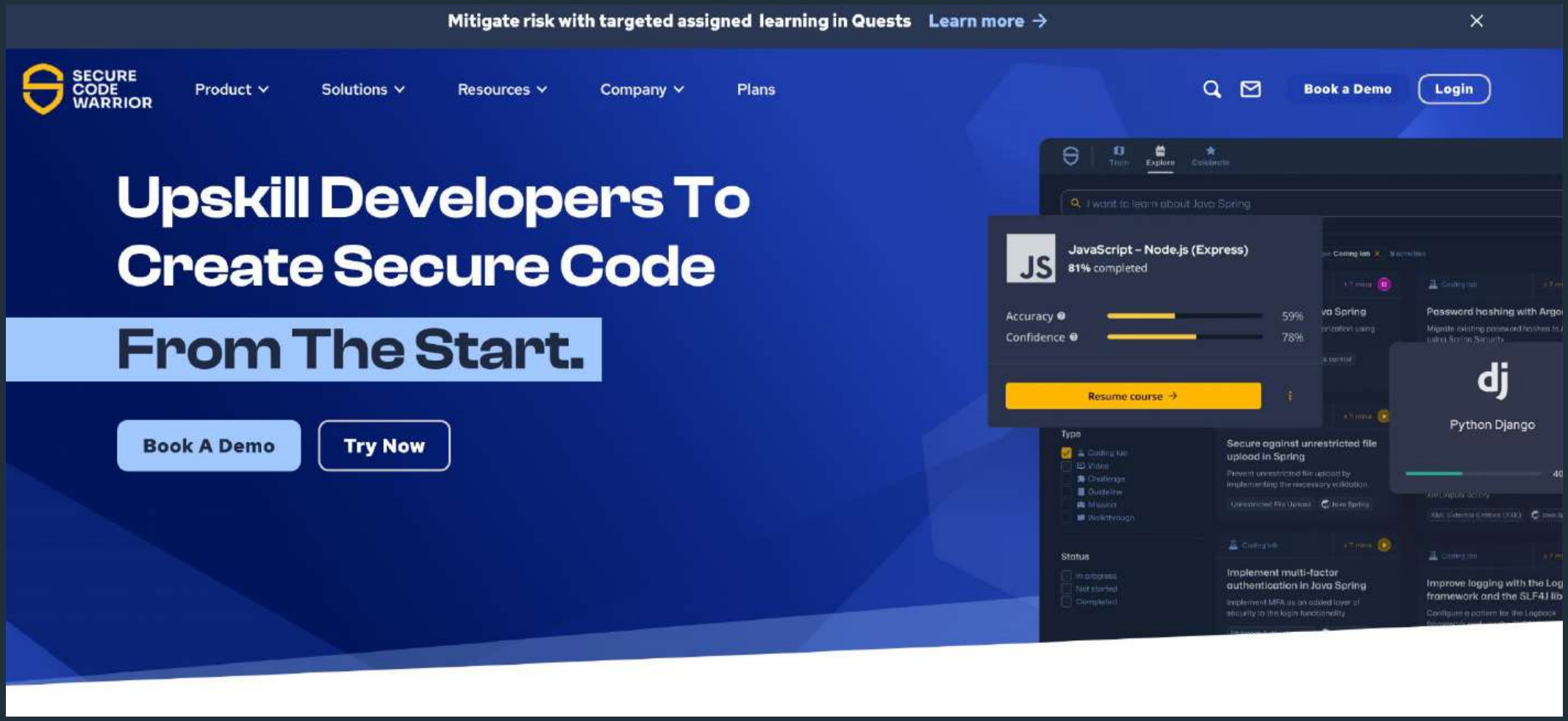
SIMULATION EMPLOYEE TRAINING

HANDS-ON TRAINING

COACHING OR MENTORING

GROUP DISCUSSSIONS

ROLE PLAYING


Mitigate risk with targeted assigned learning in Quests
Learn more
SECURE CODE WARRIOR
Product
Solutions
Resources
Company
Plans
Book a Demo
Login
Upskill Developers To Create Secure Code From The Start.
Book A Demo
Try Now
JavaScript – Node.js (Express)
81% completed
Accuracy
59%
Confidence
78%
Resume course
Python Django
Secure against unrestricted file upload in Spring
Implement multi-factor authentication in Java Spring
Password hashing with Argo
Improve logging with the Log framework and the SLF4J lib
Type
Status

cheatsheetseries.owasp.org

- Mana... | CISO Ecosystems... | 360° Business Insi... | Risk Report - Adm... | R12 Products - Go... | TP: Room booking | One Support - Ser... | Addressable Mark...

Introduction | Search | OWASP/CheatSheetSeries ☆29.4k ⑂4.1k

CHEAT SHEET SERIES PROJECT

Life is too short • AppSec is tough • Cheat!

The **OWASP Cheat Sheet Series** was created to provide a concise collection of high value information on specific application security topics. These cheat sheets were created by various application security professionals who have expertise in specific topics.

We hope that this project provides you with excellent security guidance in an easy to read format.

Channels Pages People

Search: phishing ⌘ + K

Bookmarks Launcher 25+ Notifications

Global Message Board

Discussion Drafts & Scheduled Folder Members Search

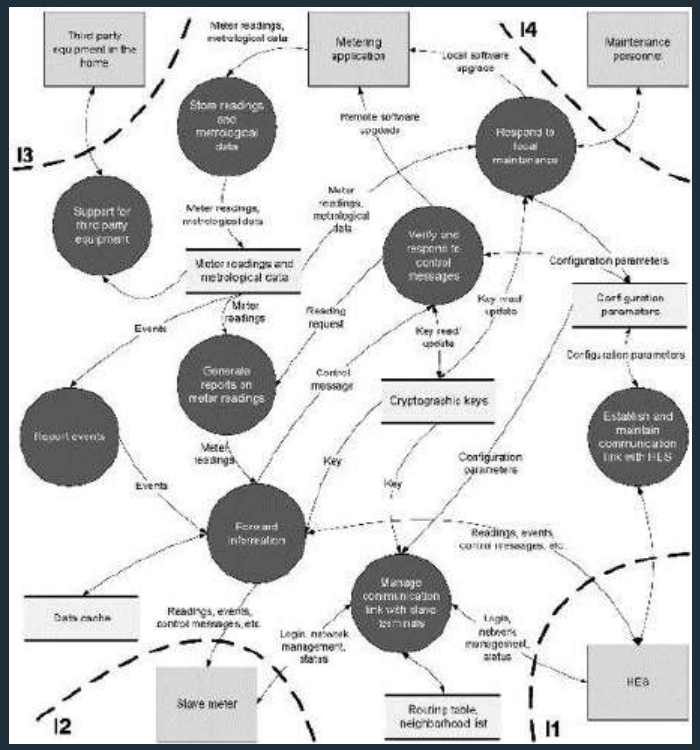
3 min read

Did you catch the phish...again? 🎣

Last Thursday, all Visma colleagues received an intriguing email that might have looked genuine.

6

Find ways that the team can start thinking like an attacker



S **Spoofing**
Can an attacker gain access using a false identity?

T **Tampering**
Can an attacker modify data as it flows through the application?

R **Repudiation**
If an attacker denies doing something, can we prove he did it?

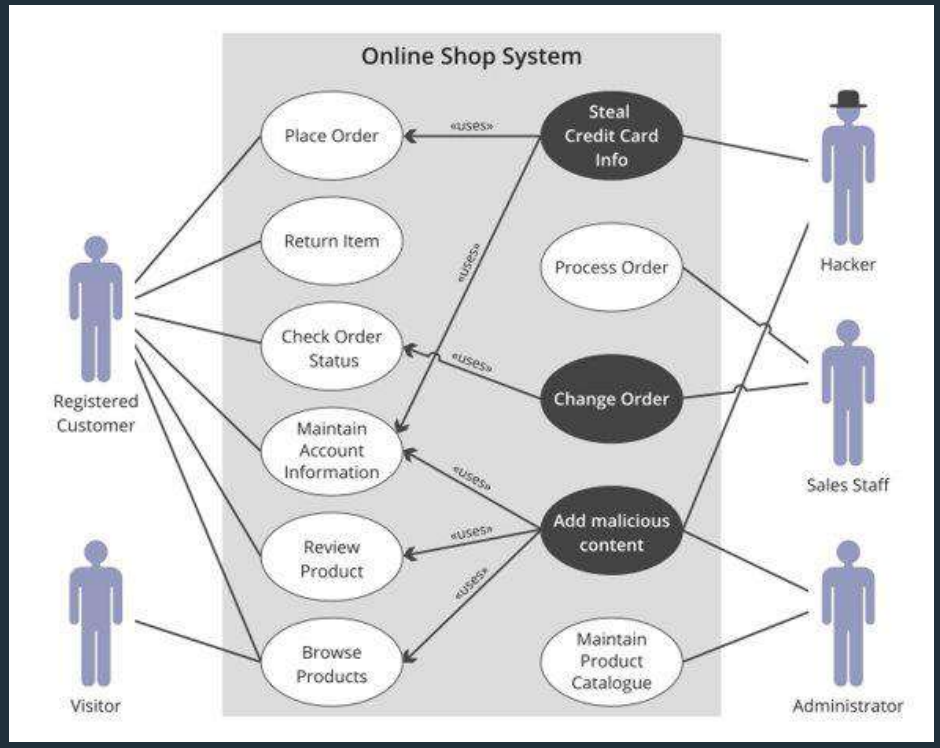
I **Information disclosure**
Can an attacker gain access to private or potentially injurious data?

D **Denial of service**
Can an attacker crash or reduce the availiability of the system?

E **Elevation of privilege**
Can an attacker assume the identity of a privileged user?

Threat Modeling

https://www.microsoft.com/en-us/securityengineering/sdl/practices/secure-by-design

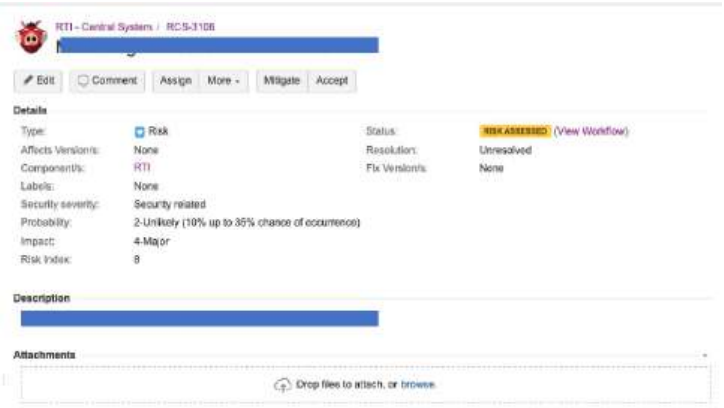


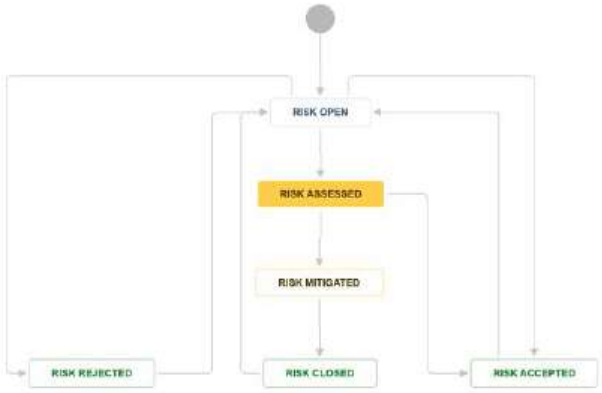
Type	Actors and actions
Use case	Insiders doing appropriate tasks
Abuse case	Outsiders trying to breach the system
Misuse case	Insiders doing inappropriate tasks intentionally
Confuse case	Insider doing inappropriate tasks unintentionally

Use Cases and Abuse Cases

7

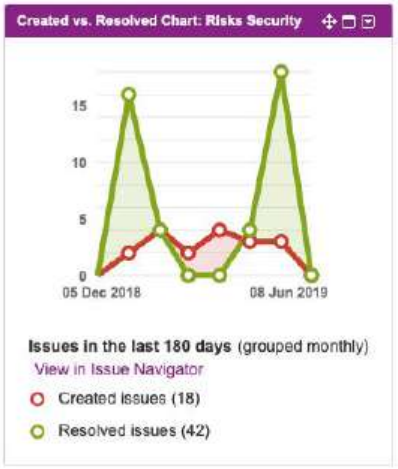
Systematically Assessing and Tracking Risks





Issue Statistics: Risks Security (Status)

Status	Count	Percentage
RISK OPEN	13	11%
RISK CLOSED	18	16%
RISK ASSESSED	32	28%
RISK MITIGATED	3	3%
RISK ACCEPTED	43	38%
RISK REJECTED	5	4%
Total	114	

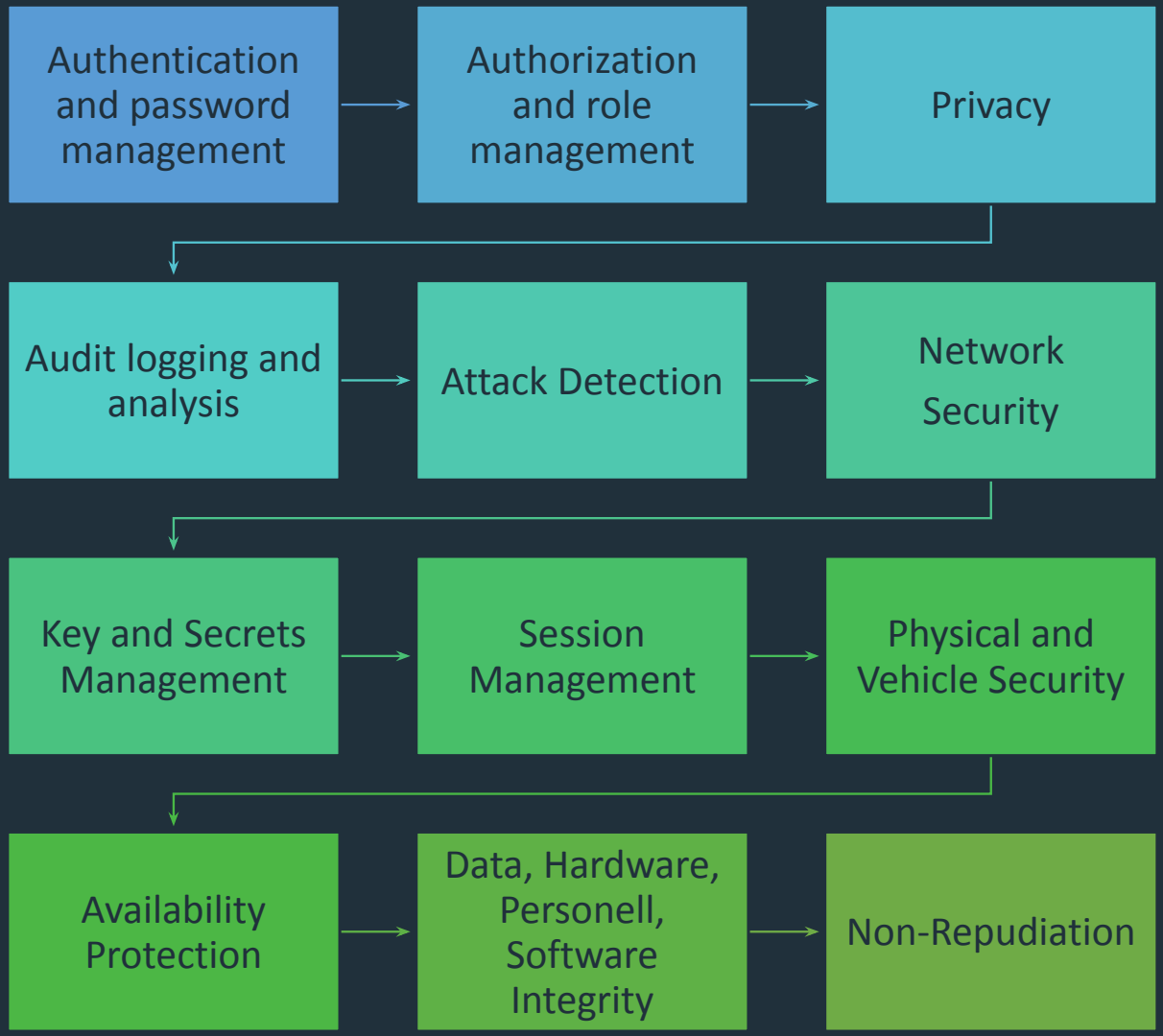


Security Risks in Jira

8

Eliciting and documenting security requirements

Analysis of the Project based on Security Factors



Font: Common Concepts Underlying Safety, Security, and Survivability Engineering - Acquisition Support Program - CMU/SEI-2003-TN-033

Data Oriented Design Requirements for Privacy and GDPR

MINIMISE AND LIMIT

HIDE AND PROTECT

SEPARATE

AGGREGATE

DATA PROTECTION BY DEFAULT.

https://www.datatilsynet.no/globalassets/global/english/guidelines/privacy-by-design/checklist-design.pdf

Process Oriented Design Requirements for Privacy and GDPR

INFORM

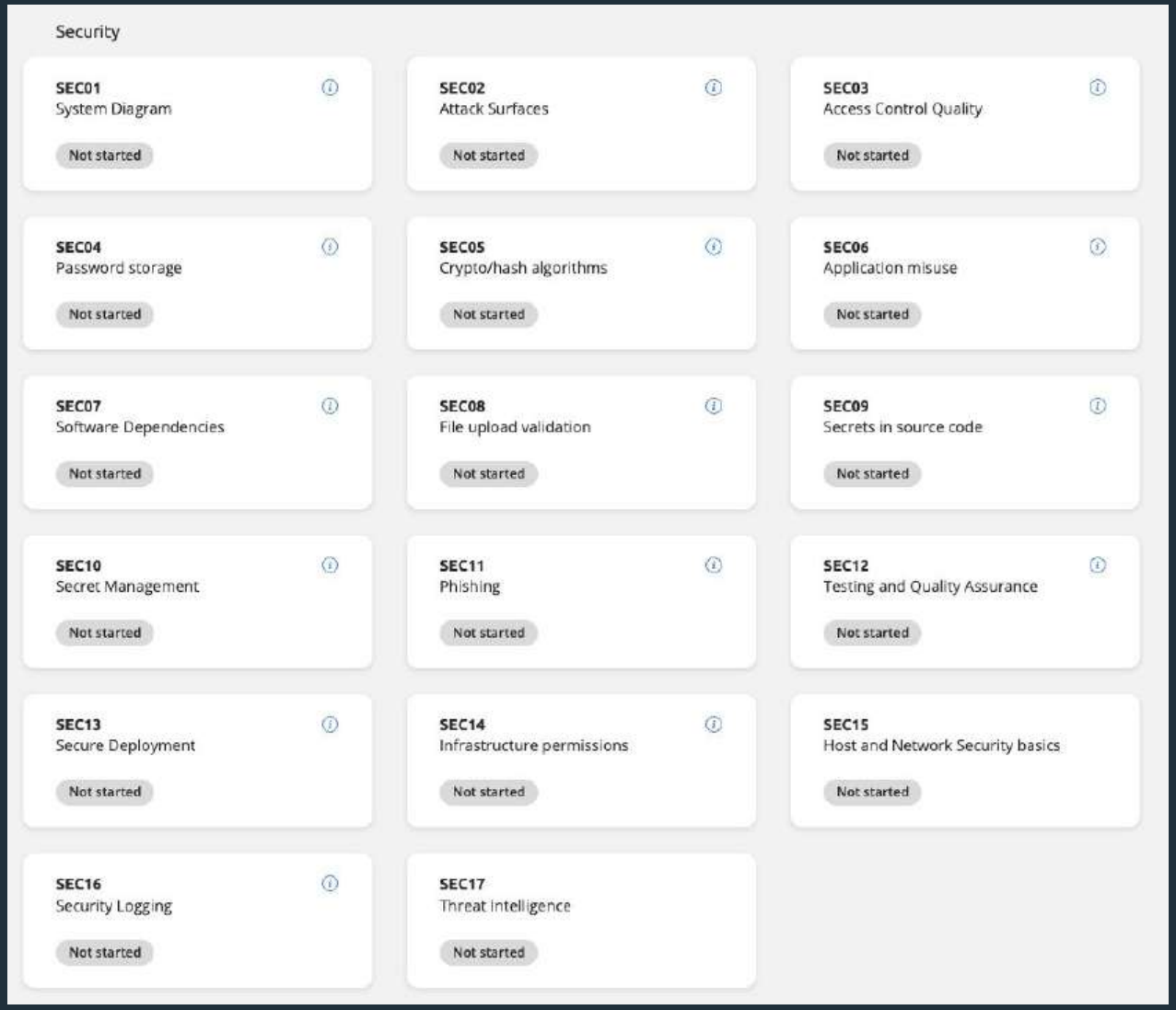
CONTROL

ENFORCE

DEMONSTRATE.

Visma
Security Program

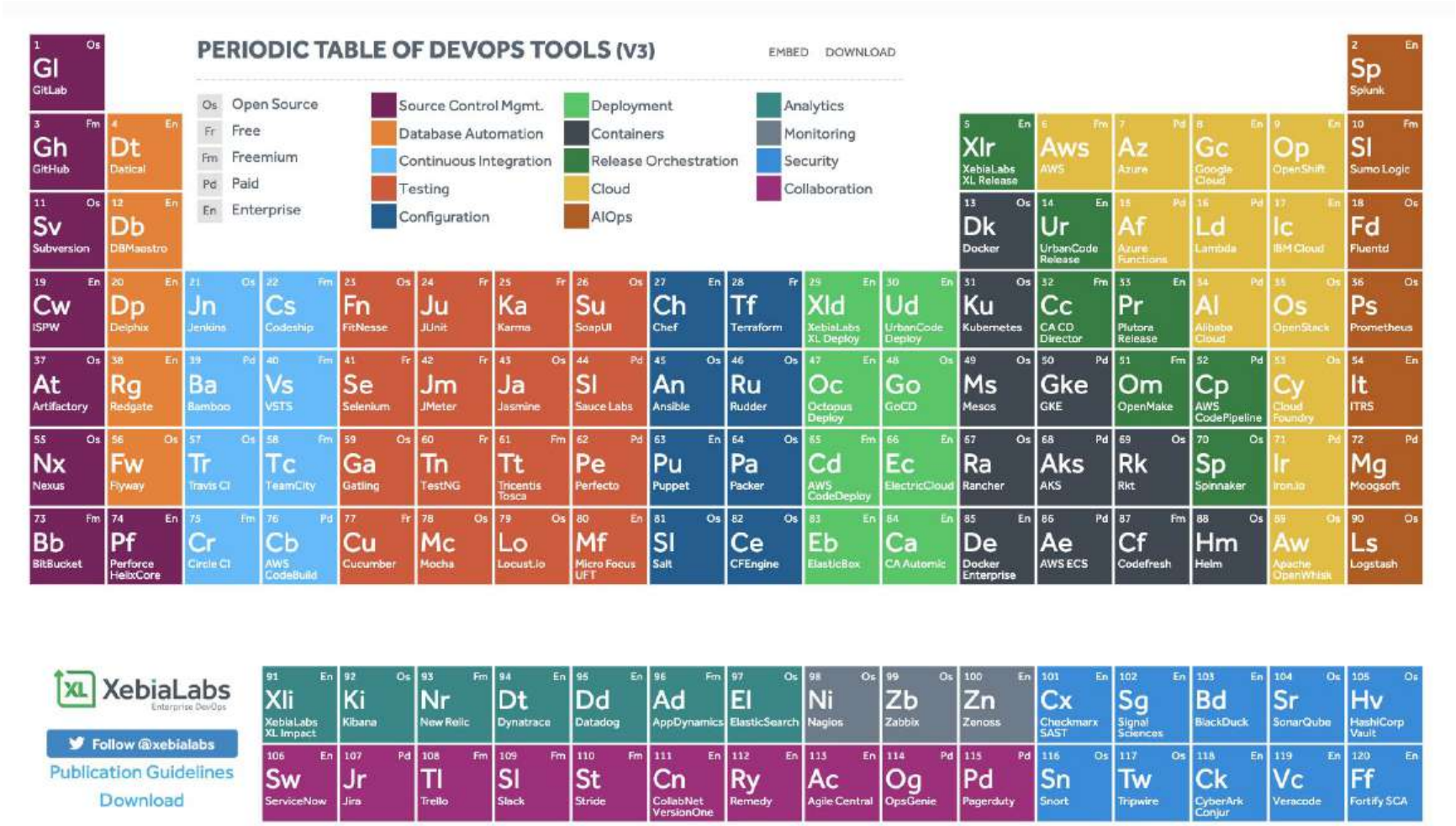
Security Self-Assessment



How often should a team discuss security?

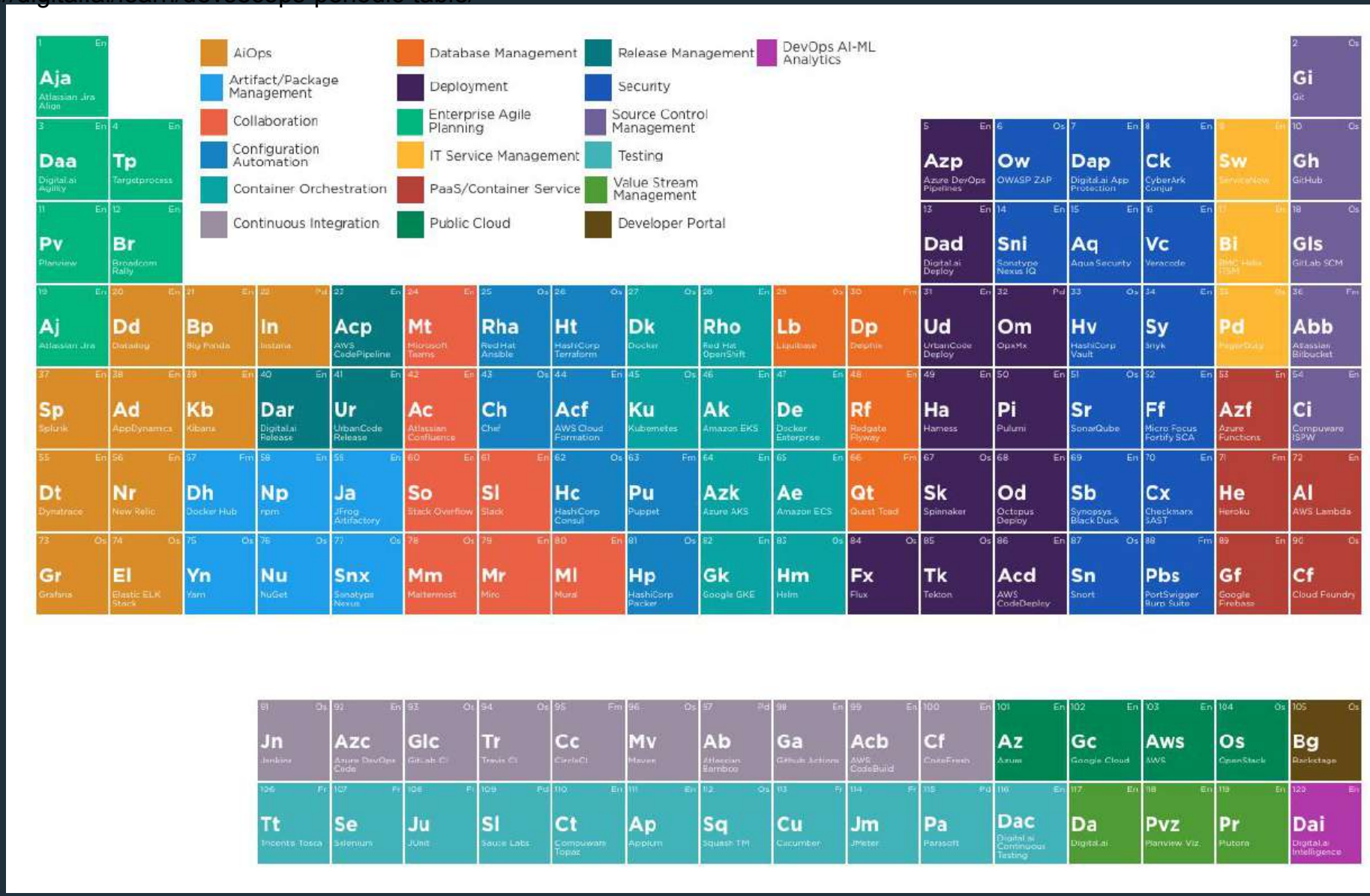
9

Introduce security tools in your pipeline



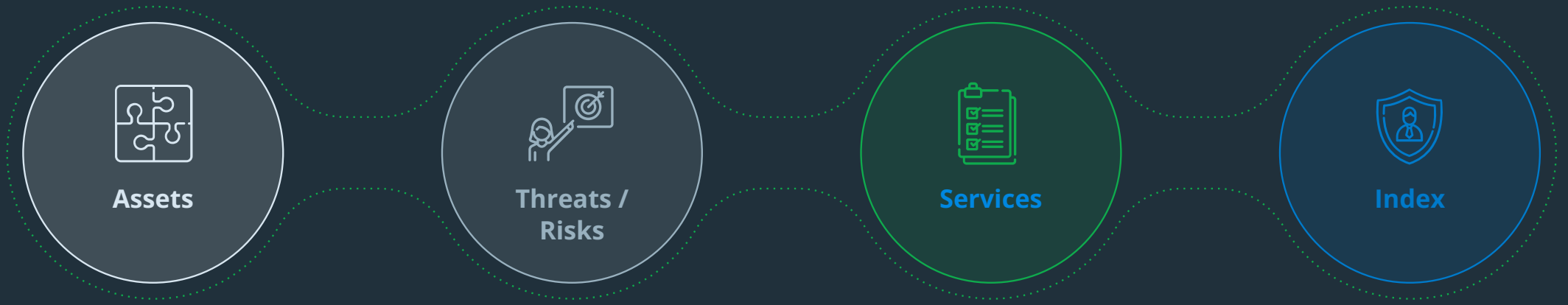
https://digital.ai/learn/devsecops-periodic-table/

https://digital.ai/learn/devsecops-periodic-table/



Application Security (VASP)

Visma
Security Program



Applications

Software application that we write and control

Risk of security incident due to potential code vulnerabilities

Three Annual Assessments
(SSA) Security Self-Assessment (1500)
(cSA) Compliance Self-Assessment (1500)
(PenTest) Pentest from Visma (3000)

Three Tools to be integrated in the Pipeline
(SAST) Static Application Security Test (3000)
(SCA) Software Composition Analysis (2000)
(CG) Cloud Guardian (1000 from Q2 2025)

Two monitoring Services
(CTI) Cyber Threat Intelligence (300)
(DAST) Dynamic Application Security Test (300)

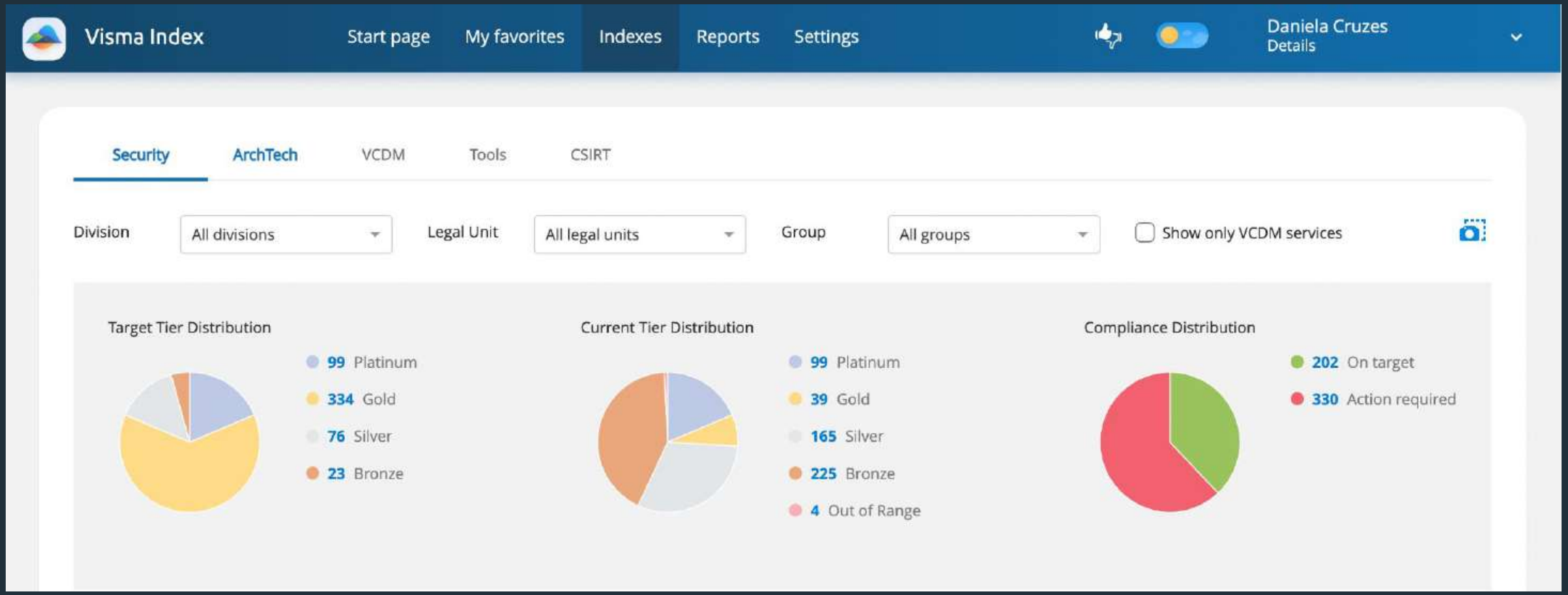
Two external ethical hacking services
(RD) Responsible Disclosure (Mandatory)
(BB) Bug Bounty (Optional)

What security tier should be in place? MD Defined.

At least **GOLD**

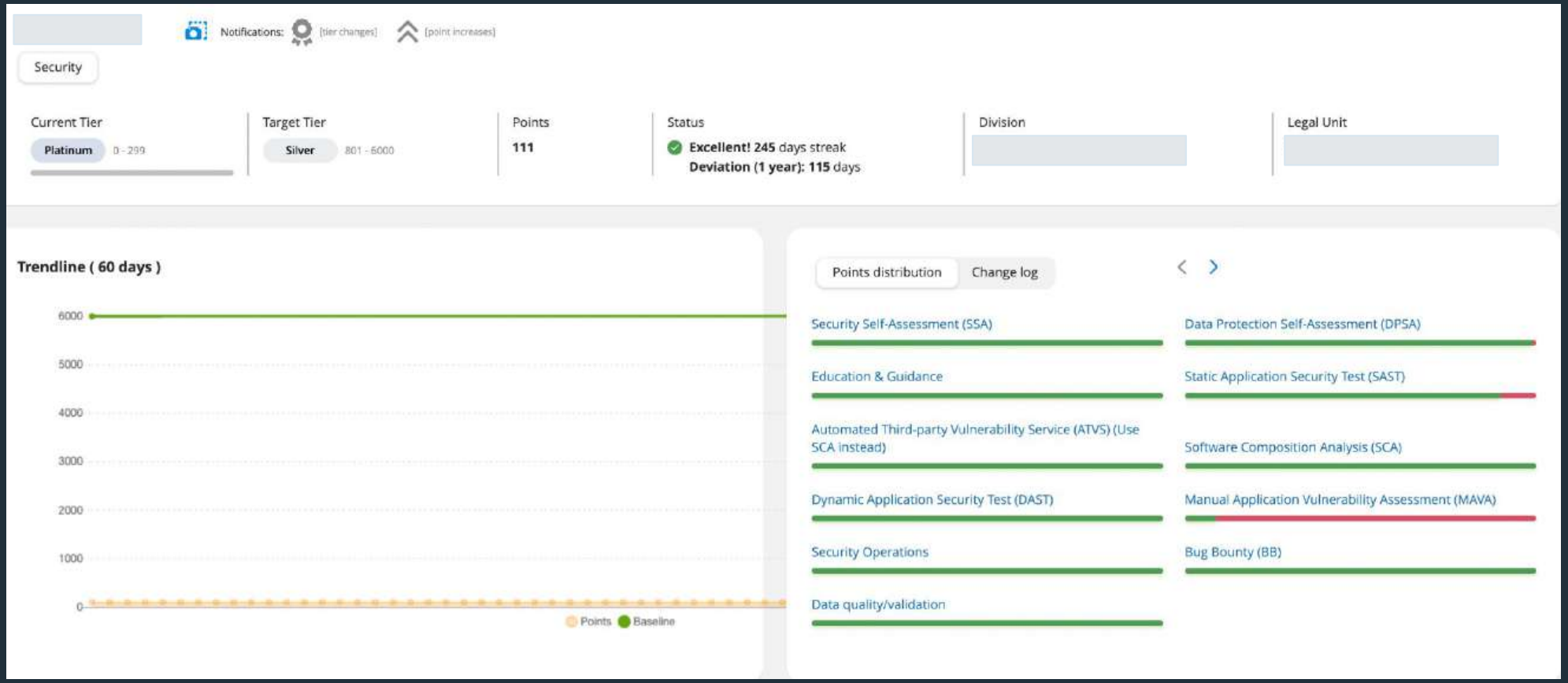
Visma
Security Program

Security Maturity Index



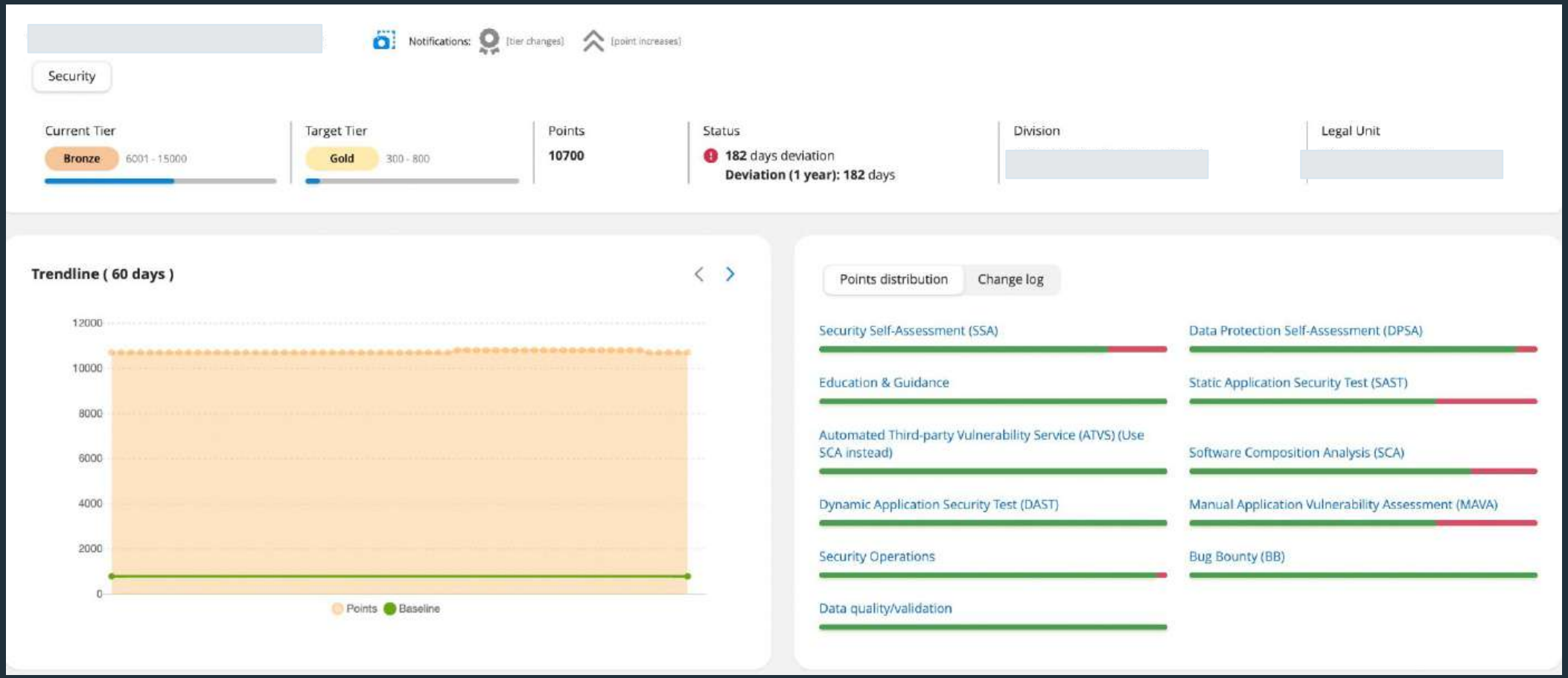
VISMA

Visma
Security Program



VISMA

Visma
Security Program



VISMA

Education & Guidance					
1 . Product Owner assigned	Confluence	0	1	0	
2 . Security Engineer assigned	Confluence	0	300	0	
				0	Well done!
Static Application Security Test (SAST)					
1 . Onboarded to SAST (VASP)	Hubble	1	3000	3000	
2 . Onboarded to SAST (Custom)	Hubble	0	100	0	
				3000	
Automated Third-party Vulnerability Service (ATVS) (Use SCA instead)					
1 . Onboarded to ATVS (VASP)	Confluence	1	0	0	
				0	Well done!
Software Composition Analysis (SCA)					
1 . Onboarded to SCA (VASP)	Snyk | Total: 0	1	2000	2000	
2 . Last analyzed older than 14 days	Snyk | Total: 0	0	0	0	
3 . Critical Impact Unresolved Security 30 days	Snyk | Total: 0	0	1	0	
4 . High Impact Unresolved Security 30 days	Snyk | Total: 0	0	0	0	
				2000	
Dynamic Application Security Test (DAST)					
1 . Onboarded to DAST (VASP managed)	Confluence	0	300	0	
				0	Well done!

VISMA

Manual Application Vulnerability Assessment (MAVA)

1 . MAVA never performed (VASP)	Confluence	1	3000	3000	
2 . Unresolved critical issues older than 30 days	Jira | Total: 0	0	3000	0	
3 . Unresolved severe issues older than 90 days	Jira | Total: 0	0	1000	0	
4 . Unresolved recommended issues older 180 days	Jira | Total: 0	0	100	0	
				3000	

Security Operations

1 . Onboarded to Cyber Threat Intelligence Service (CTI) (VASP)	Hubble	1	300	300	
2 . Onboarded to Infrastructure Security Log Management (SLM) - Non-VCDM	Confluence	1	0	0	
				300	

Bug Bounty (BB)

1 . Onboarded to Bug Bounty (VASP)	Hubble	0	1	0	
				0	Well done!

Data quality/validation

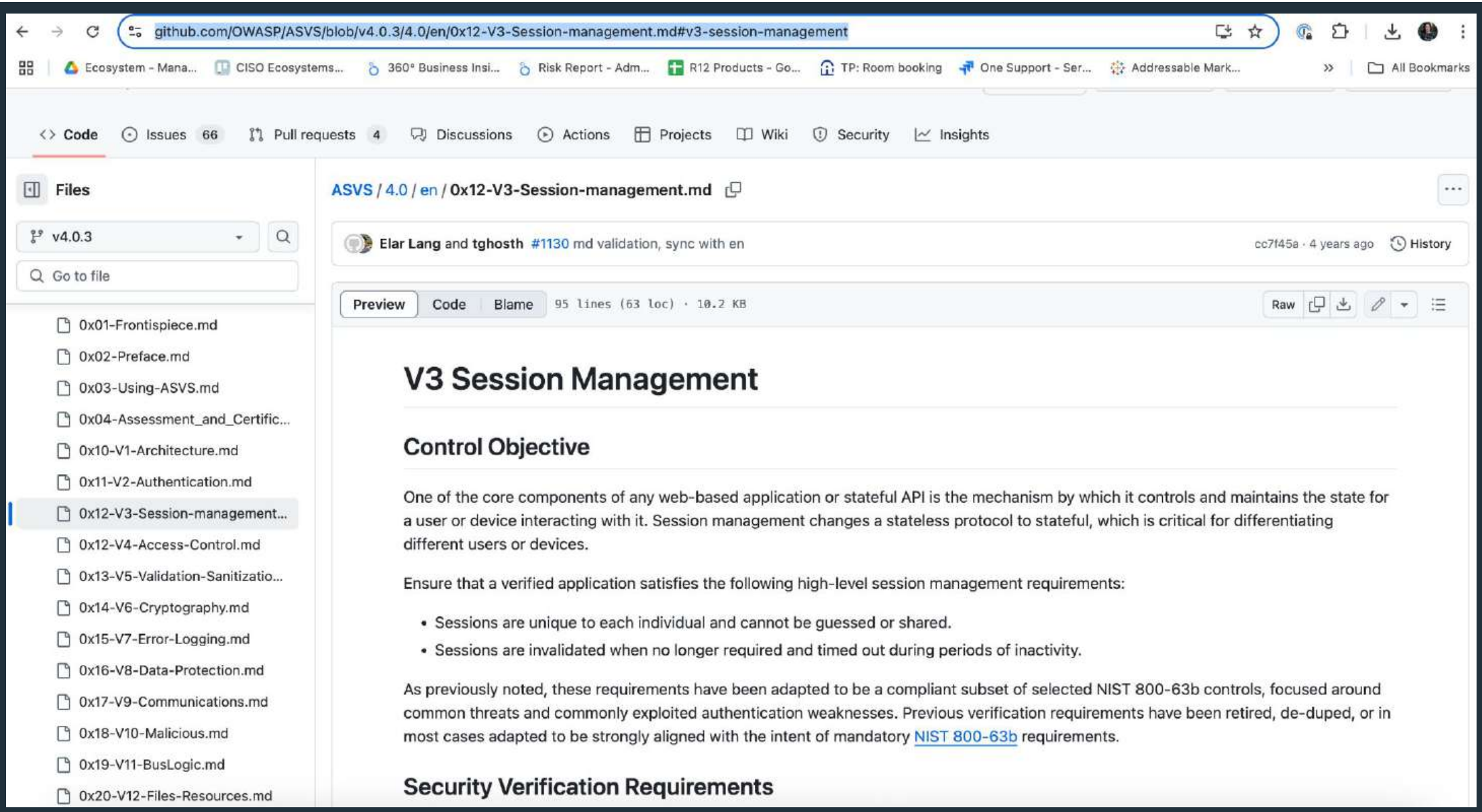
1 . PSC_ID missing	Confluence	0	1	0	
2 . Configuration required: Coverity project id not set in index	Confluence	0	1	0	
3 . Configuration required: Jira key mismatch	Confluence	0	1	0	
4 . Jira misconfigured	Jira	0	1	0	
				0	Well done!

VISMA

10

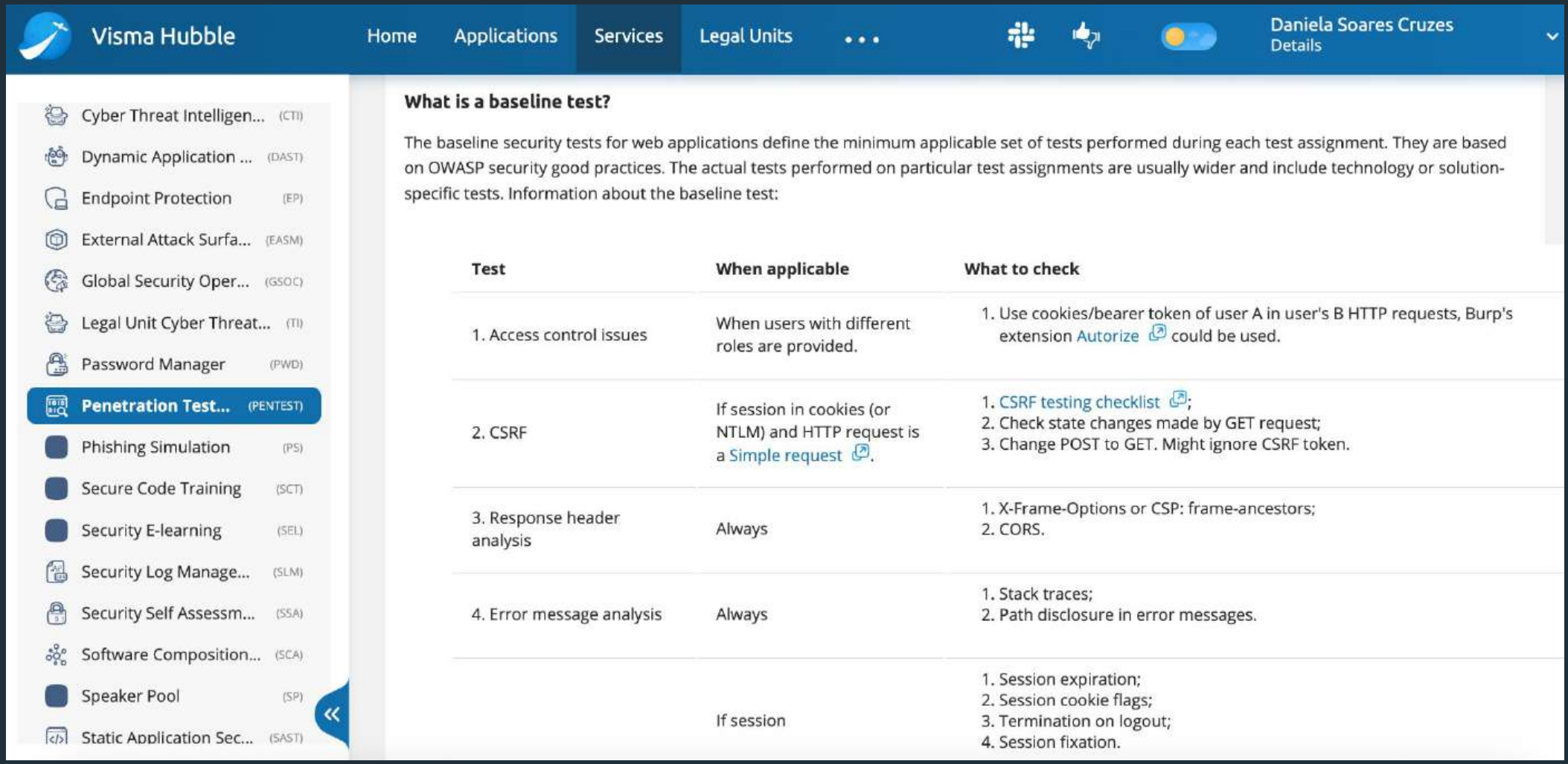
Define a systematic approach for Security Testing Penetration Testing Responsible Disclosure BugBounty

Security Testing



https://github.com/OWASP/ASVS/blob/v4.0.3/4.0/en/0x12-V3-Session-management.md#v3-session-management

Penetration Testing


Visma Hubble
Home
Applications
Services
Legal Units
Daniela Soares Cruzes
Details
Cyber Threat Intelligen... (CTI)
Dynamic Application ... (DAST)
Endpoint Protection (EP)
External Attack Surfa... (EASM)
Global Security Oper... (GSOC)
Legal Unit Cyber Threat... (TI)
Password Manager (PWD)
Penetration Test... (PENTEST)
Phishing Simulation (PS)
Secure Code Training (SCT)
Security E-learning (SEL)
Security Log Manage... (SLM)
Security Self Assessm... (SSA)
Software Composition... (SCA)
Speaker Pool (SP)
Static Application Sec... (SAST)
What is a baseline test?
The baseline security tests for web applications define the minimum applicable set of tests performed during each test assignment. They are based on OWASP security good practices. The actual tests performed on particular test assignments are usually wider and include technology or solution-specific tests. Information about the baseline test:
Test
When applicable
What to check
1. Access control issues
When users with different roles are provided.
1. Use cookies/bearer token of user A in user's B HTTP requests, Burp's extension Autorize could be used.
2. CSRF
If session in cookies (or NTLM) and HTTP request is a Simple request.
1. CSRF testing checklist;
2. Check state changes made by GET request;
3. Change POST to GET. Might ignore CSRF token.
3. Response header analysis
Always
1. X-Frame-Options or CSP: frame-ancestors;
2. CORS.
4. Error message analysis
Always
1. Stack traces;
2. Path disclosure in error messages.
If session
1. Session expiration;
2. Session cookie flags;
3. Termination on logout;
4. Session fixation.

RED TEAM

BLUE TEAM

Responsible Disclosure and Bug Bounty

visma.com/trust-centre/responsible-disclosure

Ecosystem - Mana... | CISO Ecosystems... | 360° Business Insi... | Risk Report - Adm... | R12 Products - Go...

Trust Centre | Security | Privacy

Security

Visma Responsible Disclosure

The information on this page is intended for security researchers interested in reporting security vulnerabilities to the Visma security team. If you are a customer and have a question about security or a password or account issue, please contact us through the support channels available for your product.

This policy sets out our definition of good faith in the context of finding and reporting vulnerabilities, as well as what you can expect from us in return.

Quick links:

- **Visma Responsible Disclosure program (Intigriti)**
- **Public Bug Bounty Program (Intigriti)**
- **Security Hall of Fame (HoF)**
- **Our PGP key**

https://www.visma.com/trust-centre/responsible-disclosure

What else we are doing in VISMA?

Forces Driving our Cybersecurity Program in 2025

https://laws.tds.company/

"Software Security is the practice of building software to be secure and to function properly under malicious attack"

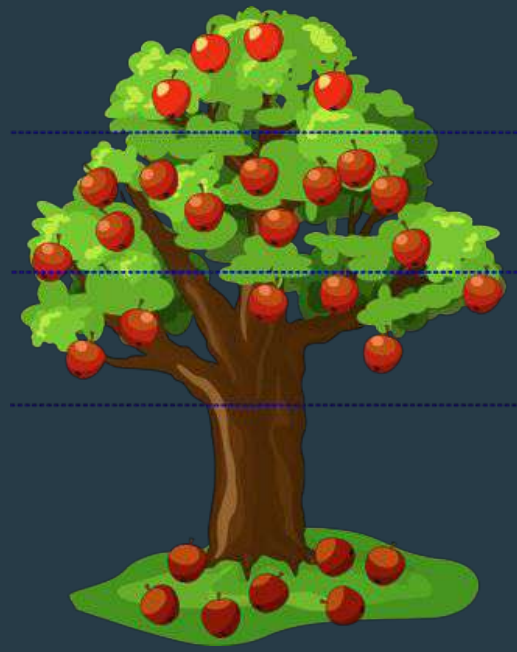
Gary Mc Graw

VISMA

RISK

People	• Roles and Responsibilities
Process	• Activities • Deliverables • Control Gates
Knowledge	• Standards & Guidelines • Compliance • Transfer Methods
Tools in the Pipeline	• Development and Support • Assessment Tools • Management Tools

Training and Cultural Embedding



Some Practical Links and Sources

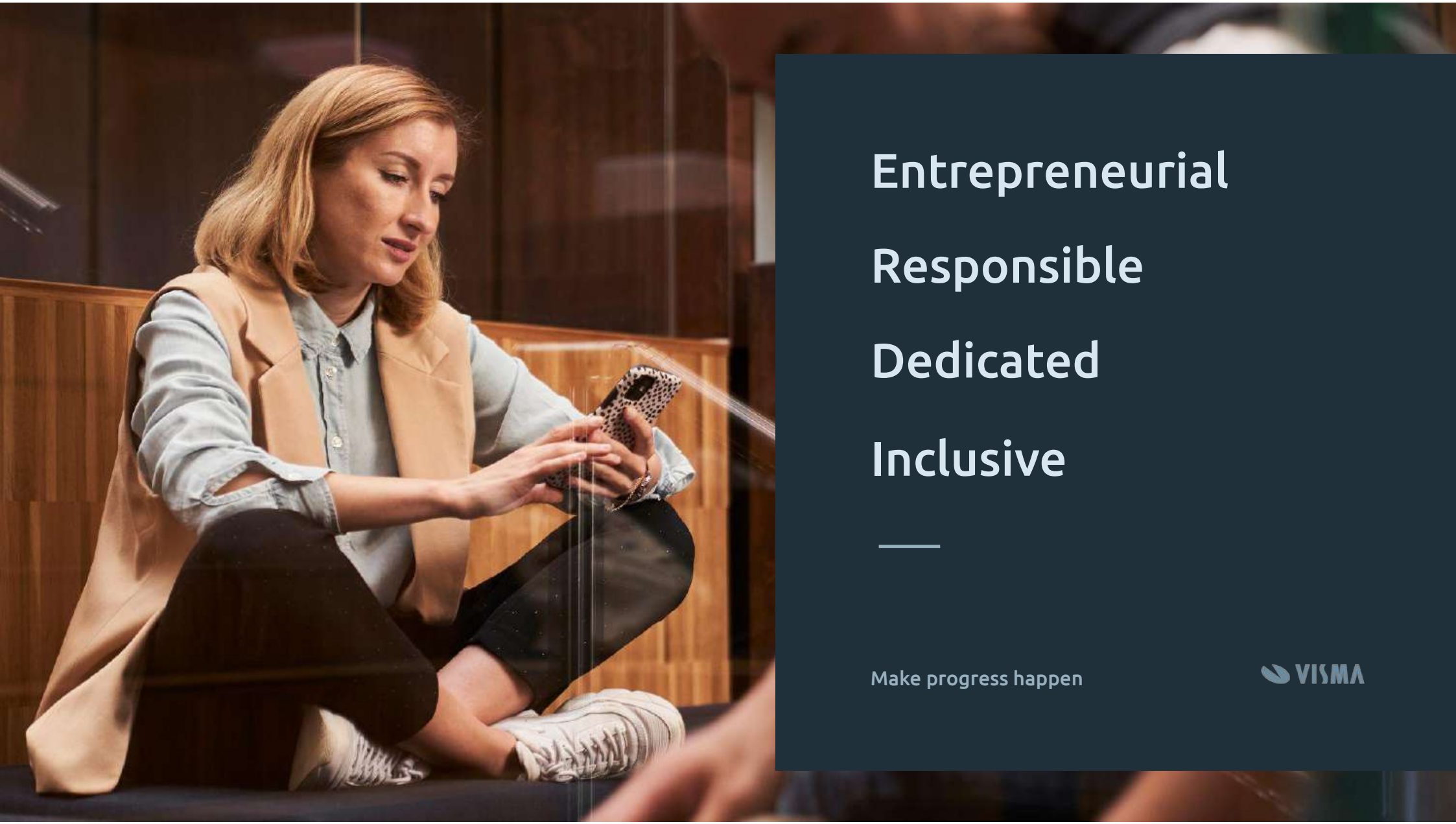
- Chapter 27 Secure Systems Development - Security Engineering Book - Ross Anderson.
- GDPR: https://gdpr.eu/tag/gdpr/
- OWASM SAMM: https://owaspsamm.org/model/
- Intention meetings:
  - https://www.sintef.no/en/publications/publication/1733965/
- Protection Poker:
  - https://www.sintef.no/en/digital/sos-agile-blog/protection-poker/
- Microsoft SDL:
  - https://www.microsoft.com/en-us/securityengineering/sdl
- Periodic Table of DevOps Tools:
  - https://digital.ai/periodic-table-of-devops-tools
- Secure Code Warrior:
  - https://www.securecodewarrior.com/

Improving the chances of success in software security for your Software development

Daniela Soares Cruzes

CISO at VISMA

VISMA



Entrepreneurial

Responsible

Dedicated

Inclusive

Make progress happen

VISMA