Security in Agile Development

Joakim
Who am I?

@JoakimTauren
Application Security Architect
@Visma Enterprise Development

“Hack all the things, drink all the booze”

Current scope:
~100 dev teams
~900+ developers
Governance model

- ~300 Dev teams
- 2000+ Developers
- 25+ Countries
- 70M+ lines of code

In SAST
Security at scale?
The Effective Leadership of Self-Managing Work Teams

- **Relating**
  - Social and Political Awareness
  - Building Team Trust
  - Caring for Team Members

- **Scouting**
  - Seeking Information from Managers, Peers, Specialists
  - Diagnosing Member Behavior
  - Investigating Problems Systematically

- **Persuading**
  - Obtaining External Support
  - Influencing Team

- **Empowering**
  - Delegating Authority
  - Flexibility Regarding Team Decisions
  - Coaching

---

Security as a service

- Central services for methodology, tooling and manual testing
- Main Goal: Assist teams
- Provide: Services for FREE for all teams

Transparency on all levels
Confluence and Jira
The Security Program

OWASP SAMM - Empower teams

- Security Training (ST)
- SSA, PSA, RA
- SPIP, PSOC, CTI
- SAST, DAST, MAVA, ATVS, Bug Bounty
The dev team

- Is responsible
- Knows the end users
- Aware of their context
- Receives support from us
- Own initiative

Security Engineer in each dev/app team
Service Owner accountable
Security Engineer

Role within each dev team
Evangelist/Champion of Security
Security culture promoter

Ensures Security is part of dev every day
Security Guild

A community of:

- Security Engineers
- Security Professionals
- Like-minded individuals

Gathers every other week online -> engagement

Has a chat channel
Target portfolio (Confluence)

Transparent list (current sec status) of ALL teams

Can be viewed by anyone in Visma
Security Self-Assessment

A number of questions for each team to answer

Core elements this serves

- Context based education
- Review process two-way learning
- Each item that needs attention -> Jira
Security Self-Assessment

Example questions:

- Client Side input validation?
- Input validation coverage and quality?
- Handling of passwords?
- Dynamic SQL?
Security Self-Assessment

The challenge and key to successful assessments:

Transparency
Security Maturity Index

- Transparent list (again!)
- Performance vs requirement
- Supports continuous improvement
- Numeric value between 0-XXXXX
- Tool for teams and mgmt
  - Required tier set by mgmt
<table>
<thead>
<tr>
<th>Service</th>
<th>Organization</th>
<th>Current Tier</th>
<th>Required Tier</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advisor Period &amp; Year-end Closing - Financial Statement and Reconciliation</td>
<td>PU</td>
<td>Platinum</td>
<td>Gold</td>
<td>✔</td>
</tr>
<tr>
<td>Advisor Period &amp; Year-end Closing - Transaction Analysis</td>
<td>PU</td>
<td>Platinum</td>
<td>Gold</td>
<td>✔</td>
</tr>
<tr>
<td>Advisor Period &amp; Year-end Closing - Taxation &amp; Annual Report</td>
<td>PU</td>
<td>Platinum</td>
<td>Gold</td>
<td>✔</td>
</tr>
<tr>
<td>Mobile Employee</td>
<td>Enterprise</td>
<td>Platinum</td>
<td>Platinum</td>
<td>✔</td>
</tr>
<tr>
<td>Cost Request Asset</td>
<td>PU</td>
<td>Platinum</td>
<td>Gold</td>
<td>✔</td>
</tr>
<tr>
<td>Integration Platform: IPProvisioning</td>
<td>PU</td>
<td>Platinum</td>
<td>Platinum</td>
<td>✔</td>
</tr>
<tr>
<td>Master Data Management</td>
<td>PU</td>
<td>Platinum</td>
<td>Platinum</td>
<td>✔</td>
</tr>
<tr>
<td>Component (hover to see description)</td>
<td>Data source</td>
<td># of occurrences</td>
<td>Penalty per</td>
<td>Penalty total</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------</td>
<td>------------------</td>
<td>-------------</td>
<td>---------------</td>
</tr>
<tr>
<td><strong>Security Self-Assessment &amp; Risk Assessment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1) SSA never performed/approved</td>
<td>Confluence</td>
<td>0</td>
<td>3000</td>
<td>0</td>
</tr>
<tr>
<td>2) RA never performed/approved</td>
<td>Confluence</td>
<td>0</td>
<td>500</td>
<td>0</td>
</tr>
<tr>
<td>3) SSA older than 12 months</td>
<td>Confluence</td>
<td>0</td>
<td>500</td>
<td>0</td>
</tr>
<tr>
<td>4) Unresolved issues from SSA older than 30 days</td>
<td>Jira</td>
<td>0</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td><strong>Static Application Security Test</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1) Not onboarded to SAST</td>
<td>Confluence</td>
<td>0</td>
<td>3000</td>
<td>0</td>
</tr>
<tr>
<td>2) Untriaged security defects</td>
<td>Coverity</td>
<td>0</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>3) High Impact Unresolved Security</td>
<td>Coverity</td>
<td>0</td>
<td>15</td>
<td>0</td>
</tr>
<tr>
<td><strong>Automated Third-party Vulnerability Service</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1) Not onboarded to ATVS</td>
<td>Confluence</td>
<td>0</td>
<td>2000</td>
<td>0</td>
</tr>
<tr>
<td>2) Unresolved third party vulnerabilities (frontend+backend)</td>
<td>Coverity</td>
<td>14</td>
<td>10</td>
<td>140</td>
</tr>
</tbody>
</table>
Security Maturity Index

Performance must be displayed to management

Tool for both management and team

Assists in evaluating needs
Transparency

From Security Maturity Index

Down to individual vulnerabilities
Product SOC

- Incidents
- Attribution
- Investigation
- Sherlock Holmes of Cyber
- Cyber Threat Intelligence
Product SOC

Successes 2019: 1 person behind bars (cannot disclose)

Ultimate goal:

- Police reports.
- More police reports..
- Even more police reports...
Cyber Threat Intelligence

Security analysts monitor and search for:

- Anyone distributing Visma accounts or secrets on black markets
- Mentionings of Visma brand names, employees, or services together with hostile language
- Chatter about pending attacks against Visma infrastructure
- Vulnerabilities and 0-day exploits impacting our technology stack
- and many other topics...

Any team in Visma can enroll to CTI as a Service, at no additional cost.
Responsible Disclosure

https://www.visma.com/trust-centre/security/

responsible-disclosure@visma.com

- Reproducible
- Coordinated disclosure
- Target only your own accounts, devices and information
- No phishing or social engineering
- Don’t disrupt the services
Bounty plz?
Bug Bounty

Teams can onboard for free!

Final steps towards true maturity

We do have prerequisites for onboarding

- 0 known vulnerabilities
Wrap-up, the tools

- Coverity (SAST)
- Detectify (DAST)
- Protecode + Retire.js (ATVS)
- “Internal” Hackers (6 persons) (MAVA)
- RecordedFuture (CTI)
So... Security as a Service?

The cool thing?

- All services are free-of-charge!!

Why?

- Money should not be the limiting factor
- Abstract the team away from money
Conclusions

Transparency and gamification works!

True maturity = police reports, Bug Bounties

Provide services for free!!

Each time you reuse a password..