OpenSAMM & Maturity Programs

What's It All About?

Adrian Pastor

McAfee Confidential
The Foundstone Practice

Four logical teams

Risk Assessment
Policy
Governance
Compliance

Web App Pen Test
Code Review
Mobile Pen Test
Threat Model
SSMA (SDLC)

Strategy

Foundstone

Infrastructure

Net Pen Testing
Endpoint Config
Control Config
ICS/IoT
Host Configuration

Software Security

Foundstone

Incident Response

IR Program
EIR
Threat Intel
Tactical Approach

Security/Pen Testing
- Can my systems be hacked?
- Was my code written securely?
- Are my applications vulnerable?

Incident Response
- Have I been hacked?
- How’d they get in?
- What was stolen?
Strategic Approach

Compliance
- Am I in compliance with regulatory standards?
- How do I become compliant?
- Am I meeting reporting requirements?

Maturity Modeling
- How secure am I?
- What do I need to do to be more secure?
- How do I measure security in my environment?

Education/Training
- How do I assess the security of my company?
- How do I write secure code?
Software Security Maturity Assessment

Changing the game…

**Governance**
- Strategy & Metrics (SM)
- Policy & Compliance (PC)
- Education & Guidance (EG)

**Construction**
- Threat Assessment (TA)
- Secure Architecture (SA)
- Security Requirements (SR)

**Verification**
- Design Review (DR)
- Code Review (CR)
- Security Testing (ST)

**Deployment**
- Environment Hardening (EH)
- Vulnerability Management (VM)
- Operational Enablement (OE)

Application of Best Practice

<table>
<thead>
<tr>
<th>Maturity Levels</th>
<th>Largely Absent</th>
<th>Considered</th>
<th>Mostly Applied</th>
<th>Mastery</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

Between levels

https://www.opensamm.org/
# Improving Software Security Maturity

## Sample Roadmap

<table>
<thead>
<tr>
<th>Security Practices/Phase</th>
<th>Start</th>
<th>Phase I</th>
<th>Phase II</th>
<th>Phase III</th>
<th>Phase IV</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy &amp; Metrics</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Policy &amp; Compliance</td>
<td>0</td>
<td>0+</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Education &amp; Guidance</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Threat Assessment</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Security Requirements</td>
<td>0</td>
<td>0+</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Secure Architecture</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Design Review</td>
<td>0</td>
<td>0+</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Code Review</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Security Testing</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>0+</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Environment Hardening</td>
<td>0</td>
<td>0</td>
<td>0+</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Operational Enablement</td>
<td>0</td>
<td>0</td>
<td>0+</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>
Improving Software Security Maturity

What does maturity mean in this context?

Secure Architecture (SA)
- Maintain list of recommended software frameworks
- Apply security principles to design

Code Review (CR)
- Create review check list
- Integrate DAST & SAST tools into the dev process

Vulnerability Management (VM)
- Create/maintain application inventory
- Adopt a security issue disclosure process

Source: http://www.planet-bob.org/2015/11/crawl-before-you-walk/
The Good, the Bad, and the Ugly
Improving Software Security Maturity

Wrapping Up!

Source: trulia.com
Improving Software Security Maturity

Wrapping Up!

Source: trulia.com
Improving Software Security Maturity

Wrapping Up!

Source: trulia.com