App Security? There is a metric for that!

by Yan Kravchenko
About Me

Yan Kravchenko, CSSLP, CISSP, CISA, CISM, QSA
Compliance Advisory Practice Lead

yan.kravchenko@netspi.com
612-455-8485

Twitter: @yanfosec
Contributor: https://www.netspi.com/blog/
AGENDA

• Background – Why is this necessary?
• Defining Risk:
  – Value / Potential Impact
  – Maturity / Susceptibility
• Why Open SAMM?
• Dashboards – Decision Support Systems
• Demo
Background – Why Apps?

- Data perimeter is no longer networks and firewalls
- Application Security has evolved to the keystone of organization’s security strategies
- Application security is complex and involves many aspects of security & technology
- Application security has been the cause of a significant percentage of security breaches
Alternatives

- BSIMM – expensive, cumbersome, proprietary
- Microsoft SDL - heavyweight, limited to MS
- Touchpoints - high-level, not enough details to execute
- CLASP - Large collection of activities, but no priority ordering
- All alternatives are based on a concept that all applications have the same threat and risk profile
Risk Measurement Challenges

• Applications can be developed with different SDLC methodologies
• Inconsistent maturity of the design and embedded security mechanisms
• Applications range in size, complexity, and perception of risk
• Application security / maturity is difficult to normalize, contrast, and compare
Defining Application Risks
Defining Risk

• Significance / Impact
  – What an application is
  – Does not change without significant changes to the nature of the application

• Maturity / Susceptibility
  – Maturity of the application
  – Can be changed by implementing additional security controls
  – Based on OWASP Software Assurance Maturity Model (SAMM)
Significance / Impact (Static)

- Customized for each organization
- Should not change unless the application or the organization undergoes big changes
- Focuses on application risk categories and attributes that are significant and meaningful
- Static risks can be used for risk calculation or presenting correlated risk scores as they relate to each static risk
- Static risks can be used to pivot data, highlighting internal initiatives
Maturity / Susceptibility (Dynamic)

- Based on OWASP Software Assurance Maturity Model (SAMM)
- Uses SAMM’s questionnaire for determining the maturity model
- Answers to questions help calculate numeric dynamic risk score as well as determine control maturity levels
- In addition to establishing the maturity level, SAMM provides detailed control implementation requirements
Why Open SAMM?
Software Assurance Maturity Model

Secure Development Lifecycle (SAMM)

proactive

security requirements / threat modeling

coding guidelines
   code reviews
   static test tools

Design

Build

test
   dynamic test tools

reactive

security testing
   dynamic test tools

Test

vulnerability scanning - WAF

Production

Secure Development Lifecycle (SAMM)
Secure Development Lifecycle (SAMM)
Governance

• **Strategy & Metrics** - Practice is focused on establishing the framework within an organization for a software security assurance program.

• **Policy & Compliance** - Practice is focused on understanding and meeting external legal and regulatory requirements.

• **Education & Guidance** - Practice is focused on arming personnel involved in the software life-cycle with knowledge and resources to design, develop, and deploy secure software.
Construction

- **Threat Assessment** - Practice is centered on identification and understanding the project-level risks based on software functionality and the runtime environment.

- **Security Requirements** - Practice is focused on proactively specifying the expected behavior of software with respect to security.

- **Secure Architecture** - Practice is focused on proactive steps for an organization to design and build secure software by default.
Verification

- **Design Review** - Practice is focused on assessment of software design and architecture for security-related problems.
- **Code Review** - Practice is focused on inspection of software at the source code level in order to find security vulnerabilities.
- **Security Testing** - Practice is focused on inspection of software in the runtime environment in order to find security problems.
Deployment

• **Vulnerability Management** - Practice is focused on handling vulnerability reports and operational incidents.

• **Environment Hardening** - Practice is focused on building assurance for the runtime environments hosting software.

• **Operational Enablement** - Practice is focused on gathering security critical information from the project teams building software and communicating it to the users and operators of the software.
• SAMM Maturity Levels:

  0 - Implicit starting point representing the activities in the Practice being unfulfilled

  1 - Initial understanding and ad hoc provision of Security Practice

  2 - Increase efficiency and/or effectiveness of the Security Practice

  3 - Comprehensive mastery of the Security Practice at scale
• Guidance for each level includes:
  – Objective
  – Activities
  – Results
  – Success Metrics
  – Costs
  – Personnel
  – Related Levels

See: http://www.opensamm.org/
SAMM Assessment Process

• Supports lightweight and detailed assessments
• Lightweight assessment can be complete in less than one hour per application
• Assessment worksheet is comprised of simple Yes / No questions
## Sample Dashboards – SAMM Scores

<table>
<thead>
<tr>
<th>Category</th>
<th>Application 1</th>
<th>Application 2</th>
<th>Application 3</th>
<th>Application 4</th>
<th>Application 5</th>
<th>Application 6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Governance: Strategy &amp; Metrics</strong></td>
<td>0+</td>
<td>2+</td>
<td>0+</td>
<td>0+</td>
<td>0+</td>
<td>0+</td>
</tr>
<tr>
<td><strong>Governance: Policy &amp; Compliance</strong></td>
<td>0+</td>
<td>1+</td>
<td>0+</td>
<td>0+</td>
<td>0+</td>
<td>0+</td>
</tr>
<tr>
<td><strong>Governance: Education &amp; Guidance</strong></td>
<td>0+</td>
<td>2</td>
<td>2+</td>
<td>2+</td>
<td>2+</td>
<td>2+</td>
</tr>
<tr>
<td><strong>Construction: Threat Assessment</strong></td>
<td>0+</td>
<td>1+</td>
<td>1+</td>
<td>0+</td>
<td>1+</td>
<td>1+</td>
</tr>
<tr>
<td><strong>Construction: Security Requirements</strong></td>
<td>0</td>
<td>2+</td>
<td>0+</td>
<td>0+</td>
<td>1+</td>
<td>0+</td>
</tr>
<tr>
<td><strong>Construction: Security Architecture</strong></td>
<td>1+</td>
<td>2</td>
<td>1+</td>
<td>1+</td>
<td>1+</td>
<td>1+</td>
</tr>
<tr>
<td><strong>Verification: Design Review</strong></td>
<td>1+</td>
<td>0+</td>
<td>1+</td>
<td>0+</td>
<td>1</td>
<td>0+</td>
</tr>
<tr>
<td><strong>Verification: Code Review</strong></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1+</td>
<td>0+</td>
<td>3</td>
</tr>
<tr>
<td><strong>Verification: Security Testing</strong></td>
<td>1+</td>
<td>1+</td>
<td>1+</td>
<td>0+</td>
<td>1+</td>
<td>0+</td>
</tr>
<tr>
<td><strong>Deployment: Vulnerability Management</strong></td>
<td>1+</td>
<td>2+</td>
<td>1+</td>
<td>1+</td>
<td>1+</td>
<td>1+</td>
</tr>
<tr>
<td><strong>Deployment: Environment Hardening</strong></td>
<td>0</td>
<td>2</td>
<td>0+</td>
<td>0</td>
<td>0</td>
<td>0+</td>
</tr>
<tr>
<td><strong>Deployment: Operational Enablement</strong></td>
<td>0</td>
<td>2</td>
<td>0+</td>
<td>0</td>
<td>0</td>
<td>0+</td>
</tr>
</tbody>
</table>
Correlated Risk Analysis / Dashboards
Risk Correlation

Value * Maturity = Correlated Risk

- Value / Impact factors generate a numeric score, normalized against all applications
- SAMM activities generates a numeric score, based on answers provided as part of the SAMM assessment
- Provides a single measure of security for each application
- Can be applied uniformly across all applications
- Provides a “true” value, allowing a side-by-side comparison of all applications
Sample Dashboards

Correlated Application Security

SDLC Maturity Risk vs. Business Impact Risk

App 1
App 2
App 3
App 4
App 5
App 6
App 7
App 8
App 9
App 10
App 11
App 12
Sample Dashboards

**Governance**

- Strategy & Metrics
- Policy & Compliance
- Education & Guidance

**Construction**

- Threat Assessment
- Security Requirements
- Security Architecture

**Verification**

- Design Review
- Code Review
- Security Testing

**Deployment**

- Vulnerability Management
- Environment Hardening
- Operational Enablement
Sample Dashboards

Application Risk Scores

- App 1
- App 2
- App 3
- App 4
- App 5
- App 6
- App 7
- App 8
- App 9
- App 10
- App 11
- App 12
- App 13
- App 14
- App 15
Sample Dashboards

Average Revenue Chart:

- SDLC Maturity Risk
- Business Impact Risk
- Average Revenue

Legend:
- Very Large
- Large
- Moderate
- Minimal
Sample Dashboards

Average Revenue Scores

- Very Large
- Large
- Moderate
- Minimal
Sample Dashboards

Materially Significant

Yes

Somewhat

No
Sample Dashboards

Number of Clients Risk Datagram

- Excessive Risk
- Acceptable Risk

Cumulative Risk Score

Number of Clients

0 2000 4000 6000 8000 10000 12000

App 1
App 2
App 3
App 4
App 5
App 6
App 7
App 8
App 9
App 10
App 11
App 12
App 13
App 14
App 15
Sample Dashboards

Average Number of Users per Client Risk Datagram

Cumulative Risk Score vs. Average Number of Users per Clients

- Excessive Risk
- Acceptable Risk
Time for a quick demo...

THE TECHNOLOGY DEMO
THE SOFTWARE ISN'T 100% COMPLETE.

IF IT HAD A USER INTERFACE YOU WOULD SEE SOMETHING HERE... HERE...AND SOMETIMES HERE.

AND THEN YOU'D BE SAYING, "I GOTTA GET ME SOME OF THAT."
ANY QUESTIONS?
“Hands-On” Demo...

Tomorrow at 9:45am in Room 10
Summary

• Enhanced ability to manage the entire application security portfolio
• Normalizes risk scoring between different applications
• Allows application security optimization through efficient “what-if” calculations
• Helps identify insecure applications
• Metrics support ability to make application security decisions
• Measures accomplishments and highlights application risk reduction activities
Questions?

• Application Value / Potential Impact
• Maturity / Susceptibility
• Open SAMM
• Risk Correlation
• Dashboards

Yan Kravchenko – 612-455-8485
yan.kravchenko@netspi.com
Thank you!