App Security? There is a metric for that!

by Yan Kravchenko
About Me

Yan Kravchenko, QSA, CISSP, CISA, CISM, PCIP
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
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)
Static Risk

- 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
Dynamic Risk

• 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 they Open SAMM?
Secure Development Lifecycle (SAMM)
### 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>Governance: Strategy &amp; Metrics</td>
<td>0+</td>
<td>2+</td>
<td>0+</td>
<td>0+</td>
<td>0+</td>
<td>0+</td>
</tr>
<tr>
<td>Governance: Policy &amp; Compliance</td>
<td>0+</td>
<td>1+</td>
<td>0+</td>
<td>0+</td>
<td>0+</td>
<td>0+</td>
</tr>
<tr>
<td>Governance: Education &amp; Guidance</td>
<td>0+</td>
<td>2</td>
<td>2+</td>
<td>2+</td>
<td>2+</td>
<td>2+</td>
</tr>
<tr>
<td>Construction: Threat Assessment</td>
<td>0+</td>
<td>1+</td>
<td>1+</td>
<td>0+</td>
<td>1+</td>
<td>1+</td>
</tr>
<tr>
<td>Construction: Security Requirements</td>
<td>0</td>
<td>2+</td>
<td>0+</td>
<td>0+</td>
<td>1+</td>
<td>0+</td>
</tr>
<tr>
<td>Construction: Security Architecture</td>
<td>1+</td>
<td>2</td>
<td>1+</td>
<td>1+</td>
<td>1+</td>
<td>1+</td>
</tr>
<tr>
<td>Verification: Design Review</td>
<td>1+</td>
<td>0+</td>
<td>1+</td>
<td>0+</td>
<td>1</td>
<td>0+</td>
</tr>
<tr>
<td>Verification: Code Review</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1+</td>
<td>0+</td>
<td>3</td>
</tr>
<tr>
<td>Verification: Security Testing</td>
<td>1+</td>
<td>1+</td>
<td>1+</td>
<td>0+</td>
<td>1+</td>
<td>0+</td>
</tr>
<tr>
<td>Deployment: Vulnerability Management</td>
<td>1+</td>
<td>2+</td>
<td>1+</td>
<td>1+</td>
<td>1+</td>
<td>1+</td>
</tr>
<tr>
<td>Deployment: Environment Hardening</td>
<td>0</td>
<td>2</td>
<td>0+</td>
<td>0</td>
<td>0</td>
<td>0+</td>
</tr>
<tr>
<td>Deployment: Operational Enablement</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

Well need a risk analysis on this project before I can approve it.

Risk 1: Indecisiveness  
Risk 2: Overanalysis  
Risk 3: Cluelessness  
Risk 4: Micromanagement...

I don't understand these risks.  
That's number thirty-six.
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

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

Overall Maturity Categories

Governance  Construction  Verification  Deployment

Maturity Rating (10 point scale)
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

|-------|-------|-------|-------|-------|-------|-------|-------|-------|--------|--------|--------|--------|--------|--------|
Sample Dashboards

Average Revenue

SDLC Maturity Risk

Business Impact Risk

Very Large
Large
Moderate
Minimal
Sample Dashboards

Average Revenue Scores

- Very Large
- Large
- Moderate
- Minimal
Sample Dashboards

Materially Significant

Yes
Somewhat
No
Sample Dashboards

Average Number of Users per Client Risk Datagram

- Cumulative Risk Score
- Average Number of Users per Clients

Excessive Risk
Acceptable 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
App 13
App 14
App 15
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?
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!