App Security? There is a metric for that!

“Hands-On” Session

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

• Model Overview
• Developing Impact / Significance Factors
• Performing an Assessment
• Analyzing the Data
  – Configuring the Spreadsheet
  – Importing / entering data
  – Creating Dashboards
• Next steps
Model Overview

- Qualitative analysis of app-security
- Based on OpenSAMM
- Correlates two different types of risks
- Under Development
- Will be donated back to OWASP
Goals / Objectives

- Enhance the ability to manage the entire application security portfolio
- Normalize risk scoring between different applications
- Allow application security optimization through efficient “what-if” calculations
- Help identify insecure applications
- Metrics should support the ability to make application security decisions
- Measure accomplishments and highlights application risk reduction activities
Developing Static Risks

• Make each one count
• Relate each risk to business
• Focus on data easy to get
• Limit to no more than 12
• Focus on “permanent” risk factors
Performing Assessment

- Identify application owners
- Roll out a survey... or not...
- Meet with application owners and review gathered information
- If necessary, make changes quickly
Analyzing the Data

“"The Spreadsheet""
Next Steps

• Evaluate Baseline
• Find visualizations that matter
• Report back to application owners
• Identify your top own Top 10
• Increase scope / operationalize re-assessments
How you can help

• Provide feedback / ideas / criticisms
• Let the world know you are using OpenSAMM
• Consider contributing your SAMM data
• Participate / help organize local SIG
• Participate in local OWASP MSP chapter meetings
Questions?

• Model Overview
• Developing Impact / Significance Factors
• Performing an Assessment
• Analyzing the Data
• Next steps

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