SCALING AN APPLICATION SECURITY PROGRAM AT THE IMF: A CASE STUDY

Jason Li
Senior Manager
Aspect Security (now part of EY)
@InnocuousInfo

Majid Malaika
Application Security Specialist
International Monetary Fund
@MajidMalaika
THE VIEWS EXPRESSED HEREIN ARE THOSE OF THE SPEAKERS AND SHOULD NOT BE ATTRIBUTED TO THE IMF, ITS EXECUTIVE BOARD, OR ITS MANAGEMENT.
How did we get here?
What does your application security (AppSec) program look like?

- Just Starting
- Still Young
- Mature
- Wait, what?? Where am I?!?
Application security is hard
Application security is hard

- New field
- Rapidly changing environment
- Competing priorities
- Industry still behind
Why are you doing this?
Prerequisites for success

- Management
- Accurate and up-to-date asset inventory
- Baseline and a plan
- Deep technical knowledge of software development
Approach

- Develop current state or “as-is” security capabilities and maturity assessment
- Develop strategy or “to-be” security capabilities
- Perform gap analysis
- Develop transition plan from current state to target state
AppSec programs have to be tailored
Plan

- Application risk profiling
- Secure Software Development Lifecycle (SDLC) integration services
- Tailored application security training and guidance
- Application security automation
- Vulnerability management
Application Security Risk Level (ASRL)
Model calibration

- Representative sampling of applications
- Scoring calculation
- Sanity check

Application Security Risk Levels

<table>
<thead>
<tr>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Very Low</td>
</tr>
</tbody>
</table>
Benefits of ASRL

Activity Scope
- Targeted
- Broad

Activity Rigor
- Min
- Max

Personnel
- Div
- ISG

Very Low | Low | Medium | High | Very High
---|---|---|---|---
Targeted | Broad | Targeted | Broad | Targeted | Broad | Targeted | Broad
Min | Max | Min | Max | Min | Max | Min | Max
Div | ISG | Div | ISG | Div | ISG | Div | ISG
SDLC integration
SDLC integration

1. Ideation
   - Security Requirements
   - Threat Modeling

2. Elaboration
   - Risk Analysis
   - Abuse Cases & Acceptance Criteria

3. Execution
   - Static Code Analysis (Manual/Automated)
   - Dynamic Testing (Manual/Automated)

4. Deployment/Release
   - Vulnerability Management
   - Continues Monitoring
CASE STUDY

Actual results and lessons learned
Case study: ASRL process

Challenges we faced

- Lack of continuity hurt efficiency
- Teams found questions confusing
- Same owner for many applications
- Legacy apps with new owners
- Discrepancy between collected fields and asset inventory fields

Lessons learned

- Use a dedicated resource
- Update based on experiences
- Short meetings across multiple weeks
- Provide questions in advance
- Work with asset inventory team to update
ASRL results

Expected results

Actual results
Case study: targeted training

Challenges we faced

- Roles need different training
- Outsourced development results in staff that comes and goes
- Developers geographically dispersed
- Off-the-shelf trainings insufficiently tailored

Lessons learned

- Ensure role-based curriculum
- Include security training requirements in contract agreements
- Favor e-learning/recorded modules
- Mix commodity training with custom developed modules
Training results

- Three main series
  - Security awareness
  - Secure processes/activities
  - Technical application security
- Nine roles identified
- 28 e-learning modules
Case study: application security guidance

Challenges we faced
- Teams don’t have time to read docs
- Teams need relevant guidance
- Organization moving toward cloud

Lessons learned
- Streamline as two-page reference
- Tailor to most common architectures
- Highlight standard control equivalents
Case study: Application Security Knowledge Domains (ASKDs)
Case study: road map status

- Part of a multiyear program build-out
  - Still progress to be made

- What does the future look like?
  - New testing methods
  - New development paradigms
  - Emerging trend toward security champions
How can you start applying?

Next week you should:
- Get buy-in from management

In the first three months following this presentation you should:
- Identify your set of profiling questions
- Model an initial sample set of applications to calibrate
- Align appropriate security activities based on risk level

Within six months you should:
- Complete the profiling of your application portfolio
- Identify program activities based on portfolio trends
- Begin assessing your highest risk applications
Takeaways

- Find your crown jewels
- Buy-in from management
- Don’t do the same thing for every application
- A stitch in time saves nine ...
QUESTIONS?

Jason Li (@InnocuousInfo)
Majid Malaika (@MajidMalaika)
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2018 Ernst & Young LLP.
All Rights Reserved.

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com