SECURITY CULTURE AT SCALE

Building a Security Ambassadors Program
WHO ARE WE?

Cassie Clark, Sr. Security Community Strategist - Salesforce
Julia Knecht, Manager, Security and Privacy Architecture - Adobe
Jessica Chang, Security Culture Lead, Trust and Security - Dropbox
Christine Keung, Chief of Staff to the General Counsel - Dropbox
WHAT PROBLEM ARE WE TRYING TO SOLVE?

As companies grow…

• How do we keep security top of mind?
• How do we scale security effectively?
**Security Champions / Ambassadors Programs**

**Definition:** A network of volunteers embedded throughout your organization that help spread your message and provide information.

*(Hint: We may have heard this from Lance!)*

- Why is this important?
- Is this right for your company?
BRANDING YOUR CHAMPIONS PROGRAM

Brainstorm: Synonyms for people who might defend/secure...stuff

• Champions
• Ambassadors
• Sentinels
• Knights
NAMING EXERCISE

5 mins - What do we want people to think when they hear “security”?  
3 mins - What words / associations would we like to avoid?  
10 mins - Share ideas on the whiteboard  
10 mins - Whiteboard groupings based on common themes  
10 mins - Narrow down and decide!
COMPANY INTROS
Size: 1,700 FTEs

**Geographic spread:** Global, major offices in San Francisco & Dublin

**Org structure:** Legal → Trust & Security

**Program scope:**
- Security culture program launched in 2016
- Champions program in development

**Our program:** (wait for it…)
15,000 FTE’s
Major offices around the world
Size: 25,000+ FTEs
Geographic spread: Over 60 offices worldwide
Org structure: Tech & Products → Infrastructure → Security
Program scope: Mature for R&D/Product side, full rollout coming to Infrastructure and acquisitions
Program size: Over 250 developers/engineers and growing!
IDEATION TO PROGRAM

• Dropbox:
  • Security culture program
  • Champions program in development

• Adobe
  • SPLC + Champs

• Salesforce
  • Piloted in 2013, full launch in 2016
  • 50 Champions to 250 Champions...and more!
ENGAGING OUR CHAMPIONS
TRAINING + COMMUNITY

- Training + community = engaged Champions!
  - Training provides tools to do effective work
  - Community motivates Champions
- Champions scale security for you!
TRAINING

• Customized team-specific trainings
• Instituted and supported by our Champions
• Stories and anecdotes are powerful!
COMMUNITY

- Community is multifaceted
  - Relationship-building
  - Incentivization and engagement
- What we’ve done
  - Community mascot + branded swag
  - Champions-only internal channel
  - CTF Hackathon
  - Happy hours, scavenger hunts, etc.
EVENTS

- Champ Summit
- Hacker Village
- Product Security Summits
- CTF
- Hacktoberfest
METRICS
YOUR TURN!

Brainstorm: What are some possible metrics for your program?

Things to think about:
• Goals/objectives?
• Challenges?
• Problem(s)?
• Activities/training?
• How will you know participants are engaged?
IMPACT METRICS: ENGAGEMENT

- Attendance at events (in-person and streamed)
- Participation in activities
- Understanding of security issues
- Level of engagement
- Response to surveys
- Communication between Champions + Security team
IMPACT METRICS: TRAINING

• Number of trained Champions
• Results from quizzes/assessments
  • Baseline
  • Post-training

Yes (186)  No (84)
IMPACT METRICS: SECURE DEVELOPMENT LIFECYCLE

Training

<table>
<thead>
<tr>
<th>Training</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Pen Test

<table>
<thead>
<tr>
<th>Product</th>
<th>Planning</th>
<th>Execution</th>
<th>Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SCHEDULED</td>
<td>IN TEST</td>
<td>IN TEST</td>
</tr>
<tr>
<td>Overall Status</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

PSIRT Reported Issues

<table>
<thead>
<tr>
<th># of Issues</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Time to Resolution

<table>
<thead>
<tr>
<th>Status</th>
<th>TTR (in days)</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocker</td>
<td><strong>P1:0 DAYS</strong></td>
<td>&lt; 2D</td>
</tr>
<tr>
<td>Critical</td>
<td><strong>P2:0 DAYS</strong></td>
<td>&lt; 30D</td>
</tr>
<tr>
<td>Major</td>
<td><strong>P3:0 DAYS</strong></td>
<td>&lt; 40D</td>
</tr>
<tr>
<td>Status</td>
<td></td>
<td>⭐</td>
</tr>
</tbody>
</table>

Threat Model

<table>
<thead>
<tr>
<th>Last Quarterly Sync</th>
<th>Status</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>JAN 2017</strong></td>
<td>1 per quarter</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Architecture Review</th>
<th>Status</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>ON TRACK</strong></td>
<td>1 per year</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Overall Status</th>
<th>Status</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>ON TRACK</strong></td>
<td></td>
</tr>
</tbody>
</table>

Static Analysis

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Status</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>ONBOADING</strong></td>
<td>&gt;= Quarterly</td>
</tr>
</tbody>
</table>
CHALLENGES
CHALLENGES
LOGISTICS
LOGISTICS

What you’ll need:

• Program plan
• Leadership buy-in
• Roles and responsibilities
• Time
  • Staff time
  • Champion time
• Space and logistics
• Pilot program
TIME AND RESOURCES
BUDGET

Items to include:

• Training materials and curricula, especially if external
• Events/activities
• Incentives/swag
• Catering
• Logo/graphic design
• Staff time

No budget? Consider...

• Recognition is free!
• Build those relationships with Champions and Security
• Partnering with other teams/departments
HOW CAN I TAKE ACTION?
TAKEAWAYS

• Secure leadership buy-in
• Build program plan
• Identify a sponsor
• Define responsibilities
• Launch pilot = iterate!
• Evaluate
• And...launch!
QUESTIONS?
THANK YOU!

Cassie Clark: cassie.clark@salesforce.com
Julia Knecht: jknecht@adobe.com
Jessica Chang: findjess@dropbox.com
Christine Keung: ckeung@dropbox.com