When Application Security “The Wrong Way” Is the Right Thing for Your Organization

Jennifer Czaplewski
Director, Product Security
Target
350,000+ TEAM MEMBERS
$75B+ REVENUE
1,800+ STORES
39 DISTRIBUTION CENTERS

- order pickup
- drive up
- restock
- Shipt
- Introducing Wallet
- mobilePOS
✓ **Organize:** Product model, Agile, DevOps

✓ **Build:** Shift from packages to in-house engineering

✓ **Fail fast:** Innovation and continuous learning
Myth: There’s no single metric to measure application security
Product Intelligence

**Specific Actions to Take**

1. **Findings and Vulnerabilities (45%)**
   - On time closure (e.g. audit findings, pen test findings)

2. **Security Services (35%)**
   - Must use required services (e.g. penetration testing)

3. **Security Culture (10%)**
   - e.g. Security Ninja appointed and attending trainings

4. **Security Incidents (10%)**
   - e.g. Product has been root cause of a security incident
Product Intelligence

Security Findings

- 84% Last 12 Months

Security Endpoint Vulnerabilities

- 55% Critical and High Only

Security Services

- 88% of High Risk Apps Penetrated

Security Culture

- Gracie N. Mag

Security Incidents

- Events and Incidents Reported Dates:
  - 01/01/2018
  - 01/01/2019
Product Intelligence

Portfolio Security Summary

Select a Portfolio
- Portfolio Name
  - Synonymous Omission
  - Apply

Key Metrics
- Security Risk % Complete: 50%
- High-Risk Apps % Project Complete: 70%
- 12 Month % Findings Closed on Time: 90%
- % Endpoint Vulnerabilities Not Overdue: 80%
- SQL Injection (SQL) Findings: 0
- Cross-Site Scripting (XSS) Findings: 0
- Malware or Secrets Findings: 0

Product List
- Product Name | Score | Percentile | Security Risk | Comments
- Euphoriasaurus 564 | Ninja Needed
- Spermacetus 722 | Sue Lipton
- Fakeryazurus 751 | Grate N Keg
- Pteranodon Rax: The F5 team needs to do the work to address. Finding planned close date will push out to 1/15/19 to account for Peak, but the team is working with the F5 team to try and get that done by mid-October at the latest.
- Erroneousauras 780 | Chuck Norris
- Unicoodon 802 | Kira Lindahl

Portfolio Applications by Risk
- Number of Applications
  - High Risk
  - Low Risk
  - Medium Risk
  - Unrated

Findings and Endpoint Vulnerabilities - Trend
- % Closed vs % Finding vs EndPoint Vulner %
- Endpoint Vulner %
- Findings %

Security Services - Trend
- % Complete
- % Security Risk %

Secure Coding - Trend
- sleepy sessions
- XSS
- SQLI
- Secure Coding
- Findings

RSAC
RSA Conference 2020
What you need to build your own

**Technology**
- **Resources**: 2-3 for build and ongoing support
- **Technology**: Can be mostly done with Open Source
- **Integrations**: Most source systems have good APIs

**Prerequisites**
- **Asset Management**: Basic awareness of assets
- **Clear policy**: Requirements and risk rating structure
- **Top Down Commitment**: Not “just another metric”
Myth: Welcome any and all engineers to a security guild. Better still, mandate participation
Target’s *Exclusive* Security Ninja Program

**Participants are**
- Seasoned
- Influential
- Passionate

**Program is**
- Exclusive (<5% of tech population)
- Builds security awareness & excitement
- Accidental talent pipeline
Security Ninja Responsibilities

- Build and maintain security knowledge
- Guide teams in security best practices
- Maintain application inventory data
- Voice of customer for Info Security
Security Knowledge Development

Initial Onboarding
- Security Fundamentals
- Hands on Hacking

Quarterly Hands On Events
Interactive events for deeper learning

Monthly Information Sharing
- Topic deep dives
- Identify actions
- ChatOps

Elevated Belts
Opportunities to earn Purple or Black Belt
Organization-wide impact

“My team cares more about security; they’ve done better considering security earlier than they used to”

“Our ninja influences team culture towards a security aware mindset; she helps to articulate risk, prioritize resolution and educate the team”

“The way our team thinks about security today is different than before we had our Security Ninja; our security culture is more mature”

“It’s helped me get over my imposter syndrome and realize I am pretty good at security stuff, and I know what I’m talking about!”

Rate the effectiveness of your security ninja:

79% Effective or Very Effective
Myth: Scan ALL the things
Spotlight SAST

Objective

*Improve application security by integrating SAST into engineering practices*

Values

- Meet developers where they work
- Offer end to end solutions
- “Right way” = easiest way
**Spotlight SAST User Experience**

You can use this UI to configure how you would like to receive feedback for issues found in Spotlight SAST scans. You will ONLY be able to mark false-positives using Github issues or JIRA stories. We recommend that you DO NOT make Spotlight SAST a required check in your Github code review process.

<table>
<thead>
<tr>
<th>Owner</th>
<th>Repository</th>
<th>CI</th>
<th>Email Enabled</th>
<th>Email Upon Successful Scan</th>
<th>Github Issues Enabled</th>
<th>JIRA Stories Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>JenniferCzaplewski</td>
<td>cicl_workshop</td>
<td>Enter CI or application...</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>JenniferCzaplewski</td>
<td>Czaplewski_Team_Repo</td>
<td>Enter CI or application...</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>JenniferCzaplewski</td>
<td>Goals-and-Objectives</td>
<td>Enter CI or application...</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>JenniferCzaplewski</td>
<td>Ninjas</td>
<td>Enter CI or application...</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>JenniferCzaplewski</td>
<td>PSE-ToolsStrategy</td>
<td>Enter CI or application...</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>JenniferCzaplewski</td>
<td>security-portal</td>
<td>Enter CI or application...</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>JenniferCzaplewski</td>
<td>TestRepo.md</td>
<td>Enter CI or application...</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>JenniferCzaplewski</td>
<td>Training</td>
<td>Enter CI or application...</td>
<td>All</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Version 1</td>
<td>vs</td>
<td>Version 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide separate ticket/email for each issue in each branch</td>
<td>Reduce noise through consolidated tickets/emails</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unpredictable notifications</td>
<td>Customer-focused notifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users either fix or mark as false positive</td>
<td>More granular response beyond false-positive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Short description about how to resolve</td>
<td>Improved information about resolution guidance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Learnings
Lessons Learned

Iterate
Iterate

Focus on Behavior

Keep it Simple

Define your MVP and build from there

Our guiding principle: “what behavior do we want to drive”

Less is usually more
Apply What You Have Learned Today

- Next week you should:
  - Meet with your customers!
  - Identify 3 desired customer behaviors

- In three months:
  - Develop *objective* (not subjective) measurements
  - *Simplify* at least 3 metrics
  - Define *your* MVP...and build it
  - Meet with your customers (again)

- In six months:
  - Meet with your customers!
  - Iterate and improve your MVP based on measurements and behaviors
Thank you!

Questions??