THE ART OF SECURING 100 PRODUCTS

Nir Valtman
@ValtmaNir
I work for NCR as the Application Security Head.

1st time speaking publicly, except at DEFCON, blackhat, and other conferences.

Mmmm…OH, AND

Neither of my previous startups succeeded!
But at least I invented few open source tools.

Lastly… I’m not a fan of the buzzword "Cyber"!

Cyber Cyber Cyber Arghhhh!!!!

The trademark specified above is a trademark or a registered trademark of its respective company. This slide is intended for informational purposes only and does not represent any endorsement by this company.
Why Does This Talk Matter?

- **Provides Practical Approaches To Secure 100 Products**
  - Why Does It Matter?
- **It's A Big Challenge To Secure 100 Products**
  - Why Does It Matter?
- **You May Need To Secure Many Products**
  - Why Does It Matter?
- **Someone Will Pay You Lots Of $$$ To Do It**
  - Why Does It Matter?
- **You Like Expensive Stuff!**
Agenda

Plan

Reality
Meet The Application Security Lead!

- Accountable for Product Security
  - Cloud-based, self-hosted or installed on customers’ premise
  - Part of the products are regulated
- Needs to keep the company out of the news
- Got executive leadership to support him

* Avatar generated on avatarmaker.com
The Daily Challenges

Need to secure a *single* high-risk product. Who’s involved?
## Mapping The Business Owners

<table>
<thead>
<tr>
<th>Product #1</th>
<th>Product #2</th>
<th>Product #100</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Software R&amp;D</td>
<td>✓ Software R&amp;D</td>
<td>✓ Software R&amp;D</td>
</tr>
<tr>
<td>✓ CISO</td>
<td>✓ CISO</td>
<td>✓ IT</td>
</tr>
<tr>
<td>✓ Legal</td>
<td>✓ Legal</td>
<td>✓ CISO</td>
</tr>
<tr>
<td>✓ Product Management</td>
<td>✓ Product Management</td>
<td>✓ Legal</td>
</tr>
<tr>
<td>✓ Internal Audit</td>
<td>✓ Solution Management</td>
<td>✓ Product Management</td>
</tr>
<tr>
<td></td>
<td>✓ Hardware Solutions</td>
<td>✓ Solution Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓ Hardware Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓ Professional Services</td>
</tr>
</tbody>
</table>
Will I Finish This Mapping Soon?

Start Date

Done!
SCOPING THE ACCOUNTABILITY

Cause someone will be blamed eventually
Core vs. Extensions

Core/Vanilla

Customer #1 Extensions

Customer #2 Extensions

... 

Customer #N Extensions
In theory, building a central security library is a best practice. In practice, theory sucks!

- Multiple code repositories
- Language/Framework specific
- Static Application Security Testing (SAST) should check violations
- Web vs. Native App
Difficult To Control All Engineering Parties

Application Security

APIs are documented!

Security requirements are documented!

Professional Services

Who cares? BYOAPI rocks!!

Software R&D
RESOURCE DIVERSITY & LIMITATIONS
The trademarks specified above are trademarks or registered trademarks of their respective owners. This slide is intended for informational purposes only and does not represent any endorsement.
## Diverse Application Security Tools

<table>
<thead>
<tr>
<th>Static Application Security Testing (SAST)</th>
<th>Checkmarx</th>
<th>Synopsys</th>
<th>V-Rayon</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IBM Security</td>
<td>Hewlett Packard Enterprise</td>
<td>Contrast Security</td>
</tr>
<tr>
<td>Dynamic Application Security Testing (DAST)</td>
<td>V-Rayon</td>
<td>Synopsys</td>
<td>Rapid7</td>
</tr>
<tr>
<td></td>
<td>Hewlett Packard Enterprise</td>
<td>IBM Security</td>
<td>Burp Suite Professional</td>
</tr>
<tr>
<td>Interactive Application Security Testing (IAST)</td>
<td>Synopsys</td>
<td>IBM Security</td>
<td>V-Rayon</td>
</tr>
<tr>
<td></td>
<td>Contrast Security</td>
<td>WhiteHat Security</td>
<td>V-Rayon</td>
</tr>
<tr>
<td>Software Composition Analysis</td>
<td>WhiteSource</td>
<td>BlackDuck</td>
<td>Synopsys</td>
</tr>
</tbody>
</table>

& More...  
- Mobile AST  
- Container Security  
- Code Obfuscation

The trademarks specified above are trademarks or registered trademarks of their respective owners. This slide is intended for informational purposes only and does not represent any endorsement.
What is the Application Security labor percentage of the engineering labor?

**Labor Limitations**

1%-2% of engineering org size
APPLICATION SECURITY
MATURITY PROGRAM

Maturity is knowing when and where to be immature
Governance – Easy To Say, Difficult To Control

Best Practice...

Develop an S-SDLC

Provide Technology-Specific Training

Define Risk Management & Risk Acceptance Process

Enforce the S-SDLC

Map, Track & Drive Towards Completion Of Trainings

Get Executives To Sign On A Security Risk
Construction – Relatively Difficult

Threat Assessment: Documenting risks in agile development lifecycle consumes much resources

Security Requirements: Should app security be involved in ALL requirements sessions?

Security Architecture: Providing best practices for various product types
Verification – Roadblocks Ahead!

**Design Review**
- Get a design diagram from engineering teams... *lots* of teams!!!
- Working with *many* smart engineering people – they know everything!

**Code Review**
- Utilizing automation is great if *ALL* bug tracking, code repo, and build systems are centralized
- Scaling automation for 100 products is nearly impossible (technology & labor wise)
- Building a central security library is a waste of time if technologies are vary!

**Security Testing**
- $$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
Deployment – Only Sounds Easy

"Shadow"-operated IRT
Work w/ every engineering team to QA hardening

Corporate IRT
If I define & It doesn't work, they're responsible
Perspective On 1 Of 100 Products

Application Security Maturity Overview
Additional Considerations

- Number of items per development lifecycle stage
  - E.g. pending QA, not started, in dev, etc.
- Average time to mitigate a vulnerability
- Prioritized list of outstanding Epics/US/Bugs
Perspective On 100 Products

Defects for Category: Multiple Categories and Multiple Products

Count

Backlog Defects

Backlog Year Month

All Measures / Defect Discovery
- New Defects - External
- New Defects - Internal
- Closed Defects - External
- Closed Defects - Internal
- Backlog Defects - External
- Backlog Defects - Internal
Perspective On 100 Products

Top 15 Product with Security Issues in past 3 months Category=Multiple Categories and Multiple Products

Product names are sanitized
DON’T REINVENT THE WHEEL, JUST REALIGN IT

(Anthony J. D’Angelo)
NCR’s App Sec Team’s Specialties

Application Security Architect

Application Security Engineer

Application Security Program Manager

Application Security Risk & Compliance Manager
## NCR’s App Sec Team’s Specialties Mapping

<table>
<thead>
<tr>
<th>OpenSAMM</th>
<th>Security Architecture</th>
<th>Program Management</th>
<th>Risk Management &amp; Compliance</th>
<th>Application Security Engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain</strong></td>
<td><strong>Activity</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governance</td>
<td>Strategy &amp; Metrics</td>
<td></td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td></td>
<td>Policy &amp; Compliance</td>
<td></td>
<td></td>
<td>V</td>
</tr>
<tr>
<td></td>
<td>Education &amp; Guidance</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>Construction</td>
<td>Threat Assessment</td>
<td>V</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Requirements</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td></td>
<td>Secure Architecture</td>
<td>V</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification</td>
<td>Design Review</td>
<td>V</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Code Review</td>
<td>V</td>
<td></td>
<td>V</td>
</tr>
<tr>
<td></td>
<td>Security Testing</td>
<td></td>
<td></td>
<td>V</td>
</tr>
<tr>
<td>Deployment</td>
<td>Vulnerability Mgmt</td>
<td>V</td>
<td>V</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Environment Hardening</td>
<td>V</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operational Enablement</td>
<td>V</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Prioritizing Security

Product Type

- Internal
- Regulated
- Internet-Facing
- Regulated

Strategy

- Investments & Commitments

Financial Impact

- <$500K
- $500K-$1M
- $1M-$5M
- >$5M
### Budgeting Labor Correctly – The Formula

<table>
<thead>
<tr>
<th>Product Type</th>
<th>% Of R&amp;D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet-Facing &amp; Regulated</td>
<td>2%</td>
</tr>
<tr>
<td>Internet-Facing</td>
<td>1%</td>
</tr>
<tr>
<td>Internal &amp; Regulated</td>
<td>1%</td>
</tr>
<tr>
<td>Internal</td>
<td>0.3%</td>
</tr>
</tbody>
</table>

**Example**

An *Internet-facing & regulated* product suite that is developed by an org size of **1000 employees** needs:

2% × 1000 = **20 App Sec Team Members**, consisting of 4 PM, 2 R&C, 4.6 Architects and 9.4 Engineers
A Lesson Learned

Even with an aggressive strategy, hiring app sec people is a **REAL** bottleneck!
A Satellite Program

Give a poor man a fish and you feed him for a day. Teach him to fish and you give him an occupation that will feed him for a lifetime.”

(Chinese proverb.)
## A Satellite Program Example

<table>
<thead>
<tr>
<th></th>
<th>Yellow Belt</th>
<th>Green Belt</th>
<th>Brown Belt</th>
<th>Black Belt</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Online Training</strong></td>
<td>Foundation app sec classes</td>
<td>Advanced classes</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Instructor-led or conferences participation</strong></td>
<td></td>
<td></td>
<td>Various advanced topics</td>
<td></td>
</tr>
<tr>
<td><strong>Special Interest</strong></td>
<td></td>
<td>PII, GDPR, PCI, FFIEC</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Static/Dynamic/Interactive Security Analysis</strong></td>
<td>On-boarding</td>
<td>Tool/Process improvement</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td></td>
<td></td>
<td>Threat modeling</td>
<td>Standards review, reusable IP</td>
</tr>
</tbody>
</table>

- **Online Training**: Yellow Belt offers Foundation app sec classes, Green Belt offers Advanced classes, Brown Belt and Black Belt are not specified.
- **Instructor-led or conferences participation**: Green Belt offers Various advanced topics.
- **Special Interest**: Yellow Belt offers PII, GDPR, PCI, FFIEC, Green Belt offers Advanced classes, Brown Belt and Black Belt are not specified.
- **Static/Dynamic/Interactive Security Analysis**: Yellow Belt offers On-boarding, Green Belt offers Tool/Process improvement, Brown Belt and Black Belt are not specified.
- **Advanced**: Yellow Belt offers Threat modeling, Green Belt offers Standards review, reusable IP, Brown Belt and Black Belt are not specified.
Measuring Effectiveness!

Ongoing

- Escalations asking for security resources by the engineering teams are good!
- Status reports must be balanced
  - Neither too Green nor Red
Measuring Effectiveness!

Year Over Year

- Overall Application Security Maturity rank increases
- Decreased number of security vulnerability reporting per X (you to define) lines of code
  - Engineers will always make mistakes
  - Use 3rd parties to assess it
Scaling Out Team’s Capabilities

Security Questionnaire For Engaging An App Sec Architect

10 Yes/No Questions
# Scaling Out Team’s Capabilities

## Security Questionnaire For Engaging An App Sec Architect

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is Data Classified?</td>
<td></td>
</tr>
<tr>
<td>Do You Follow The S-SDLC?</td>
<td></td>
</tr>
<tr>
<td>Data Encryption?</td>
<td></td>
</tr>
<tr>
<td>Handle Sensitive Data Related To PII/PCI?</td>
<td></td>
</tr>
<tr>
<td>Security Automation Integrated Into Pipeline?</td>
<td></td>
</tr>
<tr>
<td>Consumer-Facing Mobile App?</td>
<td></td>
</tr>
</tbody>
</table>
Scaling Out Team’s Capabilities

Security Questionnaire For Engaging An App Sec Architect

Workflow
Collaboration Page
File

10 Yes/No Questions
Scaling Up Security

Application Security Must Fit Into Any Pipeline

DEV
- Plan
- Code
- Build
- Test

Continuous Delivery
- Continuous Integration
- Agile Development

OPS
- Release
- Deploy
- Operate
Scaling Up Security Using Release Automation

Static App Sec Testing
Interactive App Sec Testing (IAST)
Binary Signing
Code Obfuscation

Dynamic App Sec Testing (DAST)
Vulnerability Scanning
Runtime App Self Protection (RASP)
Scaling Up Security When Lacking Automation

Identify Quick Wins

Code Obfuscation
Static App Sec Testing
Penetration Tests
Manual Code Review
Dynamic App Sec Testing (DAST)
Binary Signing
Vulnerability Scanning

Even A Long-Term Plan Is A Viable Plan
Finding The Partnerships – Use Cases

- Customer Needs
- Industry Trends
- Regulations
- Security

Partnerships
Additional Tips

- Securing 100 products takes years.
  - Start by investing 80% of the resources in 20% of the products.

- Reflect your success!
  - Trending charts of app sec metrics
  - Integration of tools into the build process
  - Share product certifications completion
  - Speak at Black Hat 😊
Time To Take Notes
Apply What You Have Learned Today

- Next week you should:
  - Generate security engagement questionnaire (10 Yes/No Qs)
  - Identify security tool implementation quick wins
- In the first three months following this presentation you should:
  - Establish an application security maturity program
  - Develop a product security strategy based on
    - Company’s strategy
    - Development methodologies & pipelining tools
    - Product Types
- Within six months you should:
  - Hopefully map all products & owners 😊
  - Start executing the strategy
THANK YOU

Nir Valtman
@ValtmaNir