The Softer Side of Security
About Allison
Professionally

- [http://Linkedin.com/in/Allison-Shubert-msia-cissp-csllp-b47a403](http://Linkedin.com/in/Allison-Shubert-msia-cissp-csllp-b47a403)
- Over 19 years in IT
  - J2EE development
  - .net development
- Over 12 years in Information security
  - Focus on application security
  - Security architecture
  - Risk management
- CISSP and CSSLP certified
  - SME for ISC2 for Both the CISSP and CSSLP (I help write exam questions and determine the cut scores for passing the exams).
- Serve on the paper review selection committee for appsecEU and appsec Global (last 3 years)
Agenda

- Hard/Soft Skills
- Big picture thinking
  - Strategy
  - Roadmaps
- Communication
  - Planning
- Collaboration
Hard Skills

- Certifications
  - CEH
  - CISSP
  - CSSLP
  - GCIH
  - CISA
- OWASP top 10
- Threat Modelling
- Encryption/PKI
- SAML
- IDAM
- SIEM
- J2EE, .net, python, Git
Big Picture Thinking

• Not a technical skill
• Partially Based on experience
• Partially dependent on your temperament (you need to be open minded)
  • Can’t get bogged down in the weeds, but the weeds should influence the strategy
• Think about what the current strengths and weaknesses of the appsec program are today, including tools and people
  – Develop your vision
  • Ask yourself what works and what doesn’t
  • Ask yourself what would you change and why
  • Map out how you would change it
SWOT

S  Strengths
W  Weaknesses
O  Opportunities
T  Threats
Strengths

• What is it that the Software Security Group does well?
  • Do you automate well
  • Do you have good application coverage
  • Does your testing methodology produce good results
  • Are you able to provide security requirements repeatably
  • Do you have skilled and knowledgeable staff
  • Does the group hold any patents
Weaknesses

• What does the Software Security Group do poorly
  • Are processes documented or followed and repeatable
  • Do you have resource limitations
  • Are you reporting to many false positives
  • Are your metrics accurate
  • Do you have adequate budget
Opportunities

• What are the intangible opportunities that will impact the Software Security Group
  • Is there a new CISO/CIO/CTO who has a new found support for the security organization
  • Will there be a increase in budget
  • Increase in headcount
  • New training budget
Threats

• What Challenges will the Software Security Group encounter in the next several years?
  • Is there impending legislation/regulations that will hamper/impede/change the direction of the software security group
  • Has there been a recent SIRT that impacts the software security group
Putting It Altogether

Creating a Vision, Strategy, and Roadmap
Example SWOT

Strengths
- Documented repeatable process
- Skilled talented employees in the software security group

Weaknesses
- Resource limitations
- Slow response
- False positives
- Late involvement

Opportunities
- Increased budget
- Regulatory requirements for software security

Threats
- Employee turnover is high
• Organically create a culture of security by building security into our products by default
Roadmaps…

• Outlines several years activities
• Align to your vision and strategy
• Complement the SWOT analysis
# Roadmap

<table>
<thead>
<tr>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>• Establish mandatory training requirements and dates by which training must complete</td>
<td>• Measure completion rate against required date</td>
</tr>
<tr>
<td></td>
<td>• Measure completion rate against required date</td>
<td>• Mature Metrics</td>
</tr>
<tr>
<td>Training and Awareness</td>
<td>• Establish a training curriculum (all roles in the SSDLC)</td>
<td>• Review and update curriculum</td>
</tr>
<tr>
<td></td>
<td>• Roll out training</td>
<td>• Update required classes</td>
</tr>
<tr>
<td>Process</td>
<td>• Create security User Stories</td>
<td>• Introduce Threat Modelling</td>
</tr>
<tr>
<td></td>
<td>• Introduce security into the code reviews</td>
<td></td>
</tr>
<tr>
<td>Tools,</td>
<td>• Deploy and engineer SAST solution</td>
<td>• Engineer an integrate SCA into CI/CD pipeline</td>
</tr>
<tr>
<td>People</td>
<td>• Hire engineers to implement tools and engineer Integrations</td>
<td>• Cross train staff</td>
</tr>
</tbody>
</table>
Collaboration

- Arguably the most important
- We are dependent on others to get our jobs done
  - Requires buy in from others
  - Folks who won’t collaborate or compromise or always say No
    - Negative Nancy
- Lead by Example
Collaboration

• A little Psychology goes a long way
  • Buy in
    • work with your business partners to understand their goals and objectives.
    • Help them understand yours
    • Point out where you both can help each other
    • Ultimately people will be more willing to help if they feel they have been consulted and their feedback included
  • The person who always says no
    • If you still keep getting “no, go away”, then try to empathize with the person. We all have a boss and priorities
      • “Please help, my boss will string me up by my toenails if I don’t get this done” They know what you mean and how you feel.
      • Don’t shoot the messenger
      • Explain how this can be a win win situation. Explain how they can include this as a feather in their cap
      • If all else fails bake them some cookies 😊
Communication

• Not the same as collaboration
• Great so you have buy in, but now what?
• Communicate, communicate, communicate
  • There is nothing worse than just dropping a new standard, policy, process on the internal website
  • Announce new major initiatives on company communication channels
• Establish a communications plan
Communications Plan

• Define your process
  • Who has to approve any communications
  • Define what communication mediums you will use (email, collaboration channels, meetings/trainings, video, etc.)
    • Define your target audience
    • Define what you want to tell them (i.e. what is the problem)
    • Define why you are doing this
    • Define what actions, if any they will need to take
    • Define when it will happen
Questions?