SECURE CANBERRA 2017
Basic security

Not always exciting, but highly effective
Security as “fashion”

Bring out the Bling!

Silver Bullet
Just Ahead

ODAY CLOTHING
Where are we getting basics wrong?

- Mitigation
- Whitelisting
- Patching

Target

NHS

Equifax
Attacks still (mostly) start in “corporate” network

Booz Allen Hamilton “When the lights went out” 2016
Attack trends

Enterprise

Probe for weaknesses / long attacks / Investments in targets of opportunity

Social engineering / Clickjack / Phishing

Home/end user

Device recruitment / quick wins
Compliance tenants true

With some slight extra effort
Pick the framework

INFORMATION SECURITY ADVICE
FOR ALL LEVELS OF GOVERNMENT

NIST CYBERSECURITY FRAMEWORK

ISO 27001 Certified

SECURE CANBERRA 2017
INFORMATION SECURITY ADVICE
FOR ALL LEVELS OF GOVERNMENT

ESSENTIAL EIGHT MATURITY MODEL

Download ASD Protect Essential Eight Maturity Model (PDF), October 2017
First published June 2017; updated July, September and October 2017
ASD top 8 addresses each point

Booz Allen Hamilton “When the lights went out” 2016
How ASD helps in the real world

1. Phishing
2. MS Office
3. Malicious VBA
4. “Other weaponization”
5. Blackenergy
6. Other RAT
7. KillDisk
Enhance compliance
Patch Mitigate your environment

Automation & analysis
Home desktops more secure?
Embrace automation
Focus on what’s important

Base Metric Group
- Exploitability metrics
  - Attack Vector
  - Attack Complexity
  - Privileges Required
  - User Interaction

Impact metrics
- Confidentiality Impact
- Integrity Impact
- Availability Impact

Scope

Temporal Metric Group
- Exploit Code Maturity
- Remediation Level
- Report Confidence

Environmental Metric Group
- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement

Modified Base Metrics
Repeat offenders
Tougher on “unmanaged” devices
DevSecOps?

New initiatives....
Background - DevOps gains
The security afterthought
Better outcomes & less work

Days

Days/weeks

Days/weeks

Days/weeks

Dev → Build → Pre-prod → Production → Sec Testing
DevOps workflow “injection”
Interaction improvements

Figure 5. Application Development and Security Team Interaction

Which of the following statements reflect how your organization’s software development and security teams interact? (Percent of respondents, N=400, multiple responses accepted)

- Our software team and our security teams work collaboratively to prioritize which security-related defects are corrected based on their severity with respect to their likelihood of being exploited (58%)
- Our security team is part of a cross-functional development team that meets regularly both as part of daily scrums and in planning meetings (45%)
- Our security team provides guidelines and funding for application security (38%)
- None of the above (3%)

Source: Enterprise Strategy Group, 2017
Figure 6. SAST and DAST Adoption Impediments

<table>
<thead>
<tr>
<th>Reason</th>
<th>SAST (N=121)</th>
<th>DAST (N=177)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity of implementing the product/service</td>
<td>31%</td>
<td>32%</td>
</tr>
<tr>
<td>Current staff lacks specific technology knowledge and skills</td>
<td>27%</td>
<td>30%</td>
</tr>
<tr>
<td>Current code review processes we have in place works just as well</td>
<td>25%</td>
<td>29%</td>
</tr>
<tr>
<td>Price</td>
<td>24%</td>
<td>26%</td>
</tr>
<tr>
<td>Lack of integration with software development and delivery tools</td>
<td>22%</td>
<td>29%</td>
</tr>
<tr>
<td>We fear application security testing will slow down our development</td>
<td>17%</td>
<td>22%</td>
</tr>
<tr>
<td>process</td>
<td>22%</td>
<td>22%</td>
</tr>
<tr>
<td>We believe our software developers already know how to develop secure software</td>
<td>17%</td>
<td>20%</td>
</tr>
<tr>
<td>We rely on third-party consultants to assess the security of our</td>
<td>11%</td>
<td>16%</td>
</tr>
<tr>
<td>software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>We don’t believe that software developers should worry about security</td>
<td>11%</td>
<td>12%</td>
</tr>
<tr>
<td>We do not believe we have a software security problem</td>
<td>5%</td>
<td>8%</td>
</tr>
</tbody>
</table>

Source: Enterprise Strategy Group, 2017
Methodology as silver bullet?

- DevSevOps?
- Security sprints / SWAT
- Embrace a dev
Communicate security outcomes
And other winning strategies
Security: QA for IT?

Consider;

- Change from number of vulns to days since patch available “
- Cyber response
- Align metrics & data to new major projects
Challenges back to the vendors

• Choose vendors that well publicise found vulnerabilities e.g. to Mitre CVE, Bugtraq or VulnDB

• Too few organisations ask vendors about regular pen-testing

• IOT vendors, have they implemented hardening and/or whitelisting in their “device”? 

• IOT vendors, automated patching?

• IOT vendors, patches for how many years after product launch/end of sale?
Recommended reading:

• ASD essential 8 maturity model

• Mighty guide; communicating to the board
SECURE CANBERRA 2017

Thank You for Attending.