Professional Security Certifications

Wesley H. Higaki
ACSAC - December 2009
Role of Professional Certifications

**Individuals:**
- Why do we pursue certifications?
- What do we hope to gain?

**Companies:**
- Why do they want certified professionals?
- What do they hope to gain?

**Consumers:**
- Why should they care?
Who Do You Trust?

Why?
Confidence Hierarchy

- Do the Right Things
  - Secure practices
- Third Party Validation
  - Independent confirmation
- Standard Criteria
  - Using open standards
- Evolving Criteria
  - Evolving standards
Job Listings

Out of over 60,000 jobs listings with “security” and “engineer”

10% included “certified”
  6% CISSP
  1% CISA
  1% SANS
Differences

UNIVERSITY DEGREE

VS.

PROFESSIONAL CERTIFICATION
## Differences and Similarities

<table>
<thead>
<tr>
<th>University Degree</th>
<th>Professional Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education</td>
<td>Training</td>
</tr>
<tr>
<td>Theoretical</td>
<td>Commercial</td>
</tr>
<tr>
<td>Broad</td>
<td>Focused</td>
</tr>
</tbody>
</table>

### Similarities

- Non-standard curricula
- Variety of options
- Constantly updated
Value of Certifications

\[
\text{VALUE} = \text{RELEVANCE} + \text{RECOGNITION}
\]
Relevance and Recognition

• Relevant to current needs
• Differentiator
• Vetting and validation
• Only one criteria of many
Security Lifecycle Certifications

• Support secure development practices
  – Promoted by SAFECode
• Support internal training activities