6 Skills
# of Highly Effective
Security Professionals

By Sondra Schneider
CEO Security University
s0ndra@securityuniversity.net
203.357.7744

Basic Principles

- The Basic Principles of InfoSecurity are Universal and Timeless principles of processes and methodology.
- Values govern people's behavior and principles ultimately determine the consequences,
- **Processes and methodology used to educate and train our Cybersecurity professionals ensures the security work force is not just certifying but qualifing the workforce**.
- There are 6 Skills of Highly Effective & Validated InfoSec Professionals with simple steps to achieve that goal in a series of infosecurity skills certifications, manifesting as a progression from certified via validated via qualified.

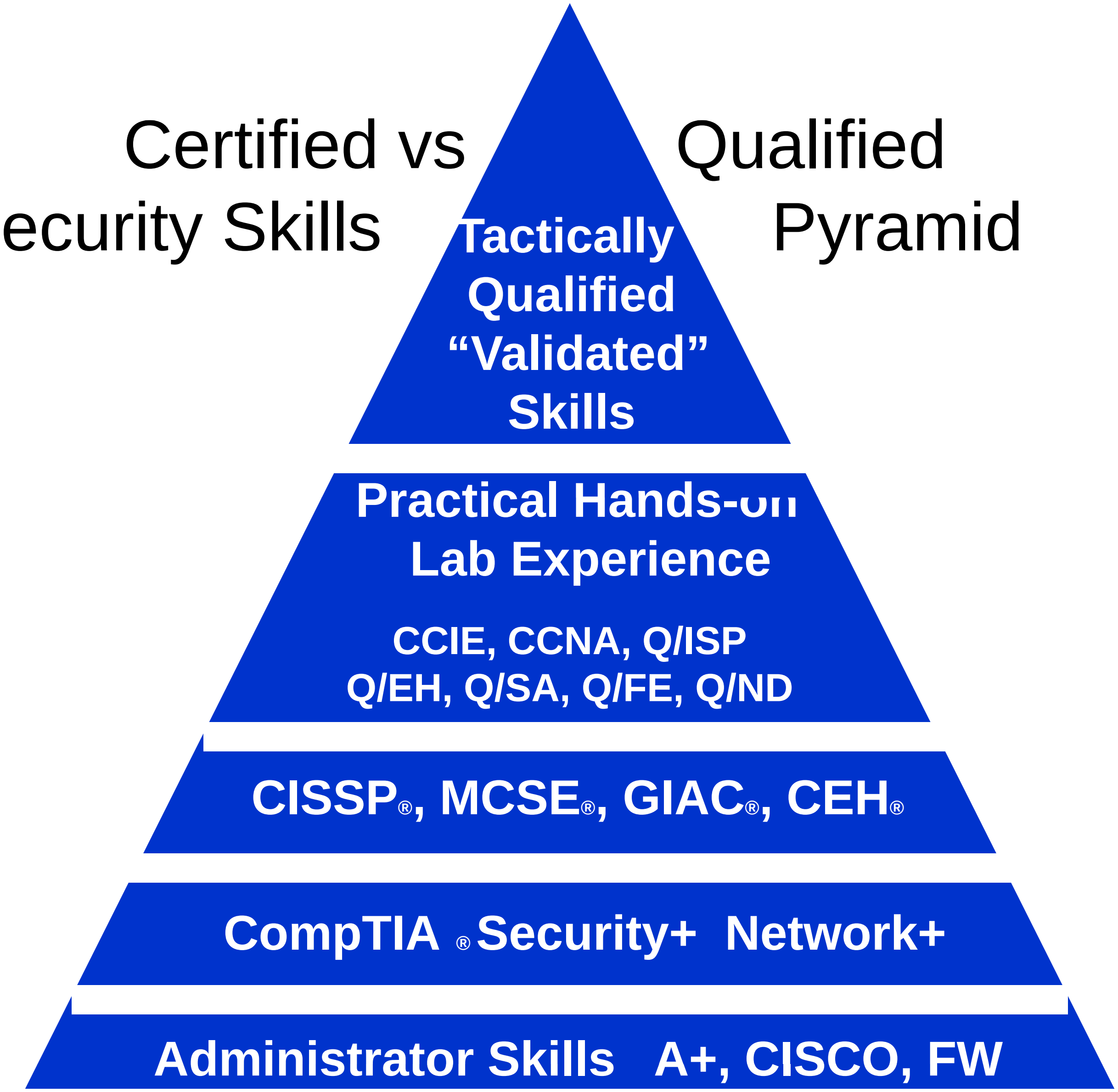
Today’s Cybersecurity Professionals

- 1,000 U.S. security specialists with the skills necessary to operate in cyberspace -- the country needs 10,000 to 30,000.
- CSIS' Commission on Cybersecurity condemned the credentials of today's federal cyber practitioners.

  "It is the consensus that the current professional certification regime is not merely inadequate**, it creates a dangerously false sense of security" because the credentials do not improve employees' skills’**

- Current credentials focus too much on demonstrating expertise in **documenting security compliance** rather than expertise **in preventing and responding to attacks**

Certified vs Qualified IT Security Skills Pyramid



Tactically Qualified "Validated" Skills

Practical Hands-on Lab Experience

CCIE, CCNA, Q/ISP
Q/EH, Q/SA, Q/FE, Q/ND

CISSP®, MCSE®, GIAC®, CEH®

CompTIA ®Security+ Network+

Administrator Skills A+, CISCO, FW

Security University®

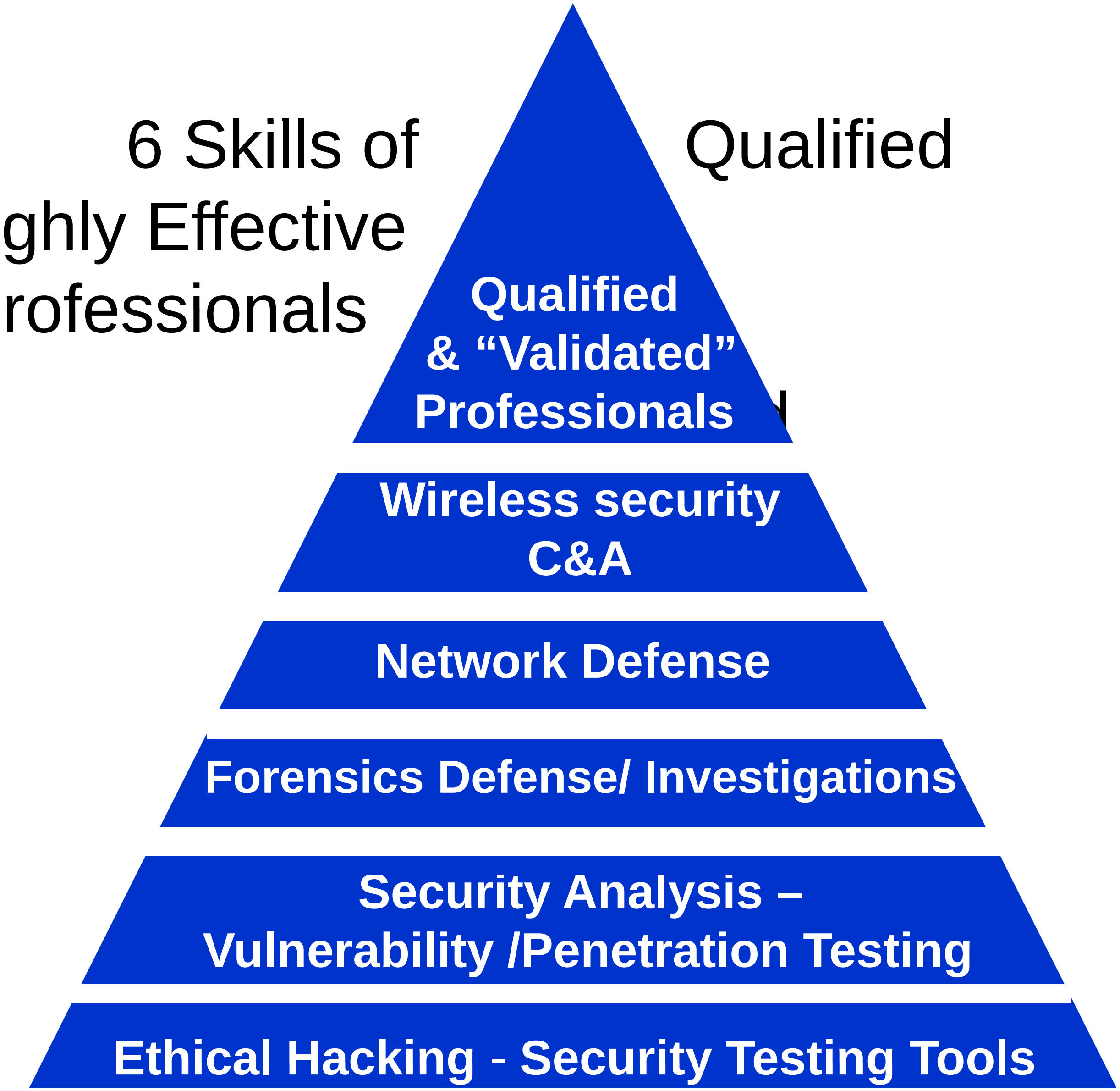
Job Analysis

- A ***job*** is a collection of tasks and responsibilities that an employee is responsible to conduct.
- A ***task*** is a typically defined as a unit of work, a set of activities needed to produce some result, e.g., assessing vulnerabilities, writing an assessment, threat management.
- Complex positions in your organization may include a large number of tasks, which were can refer to as ***functions***
- ***Job descriptions*** list the general tasks, or functions, and responsibilities of a position
- A ***job analysis*** examining the tasks and sequences of tasks necessary to perform the job.
- The analysis looks at the areas of knowledge and skills needed by the job
- Resulting in a ***role -*** the set of responsibilities with expected results associated with a job. (A job usually includes several roles)

Job analysis aims to answer questions such as:

- 1. Why does the job exist?
- 2. Who can do the job?
- 2. What tactical skills if any do you need to do the job?
- 3. How does the worker do the job?
- 4. **In a skills-based job, the skills are inferred from tasks and the skills are rated directly in terms of importance of frequency**.
- 5. How do you determine if they are qualified to perform the job?
- 6. What constitutes successful performance?

6 Skills of Qualified
Highly Effective
Security Professionals



Qualified
& “Validated”
Professionals

Wireless security
C&A

Network Defense

Forensics Defense/ Investigations

Security Analysis –
Vulnerability /Penetration Testing

Ethical Hacking - Security Testing Tools

Security University®

Competence or Confidence?

- Certification and Certificate are vastly different terms, yet the InfoSec industry uses them synonymously.
- Certification assesses of an individual’s knowledge, skills, and abilities based on a body of knowledge. You can master the body of knowledge – confidently passing an exam.
- Certificate or Assessment Based Certification programs are performance based assessments of an individual’s knowledge, hands-on skills, and abilities based on practical assessment and validation of practical assessment.
- The recent CSIS report validates Certifications provide a false sense of security about the cyber workforce.
- If in 2005 validated hands-on security skills was required like a Cisco CCIE Certification is required by Cisco the 2001 workforce would be 40% closer to a 10,000 validated cybersecurity workforce standard.

https://www.ansica.org/wwwversion2/outside/PERfaq.asp?menuID=2

Workforce readiness

- How should companies verify or test to ensure the right people are in right place with the appropriate skill sets?
- There might be other choices for validating workforce readiness, but for this discussion, it comes down to hands-on skills qualification or certification.
- 6 Security Skills of Highly Effective Security Professionals
  Security testing tools, Ethical Hacking
  Security Analyst – Vulnerability Penetration Testing
  Forensic Defense & Investigations
  Network Defense
  Certification & Accreditation of ISMS
  Wireless Security

Overhaul cybersecurity certifications?

- Is there a debate to what is more important?
- 1) validate: an individual's conceptual knowledge,
- 2) assessment based performance associated with a tactical security skill?

- Who do you want on your six?
- Do you want a security SME who has practical security skills who competency has been validated with a certification, qualification and lastly a validation process
- or do you want a trained infosec person who has demonstrated expertise in documenting security compliance

Ownership

- Some day a combination of science, technology, education and discipline may produce an information infrastructure less sensitive to human foibles.
- But, unless and until then, these words by Thomas Jefferson that answer the question posed bythis essa y’s title.

“I know of no safe depository of the ultimate powers of society but the people themselves; and if we think them not enlightened enough to exercise their control with a wholesome discretion, the remedy is not to take it from them, but inform their discretion by education.“

6 Skills of Highly Effective Security Professionals

THANK YOU!

By Sondra Schneider
CEO Security University
s0ndra@securityuniversity.net
203.357.7744