The Top 20 Critical Security Controls

from "best practice" to "common practice"

Tony Sager
Director, The SANS Institute
Director of Programs, the Council on CyberSecurity
October 2, 2013

Classic Risk Equation

$$\text{Risk} = f\left\{\frac{\text{Vulnerability, Threat, Consequence}}{\text{countermeasures}}\right\}$$

Overloaded terms in the (word) cloud!

The Top 20 Critical Security Controls
from "best practice" to "common practice"

Calabrese's Razor

"I've long held the opinion that the community of 'Information Security Experts' agree with each other 90% of the time…

…but waste 90% of their time arguing to the death with other InfoSec Experts about the remaining 10%."

Hal Pomeranz, Deer Run Associates
February 26, 2009

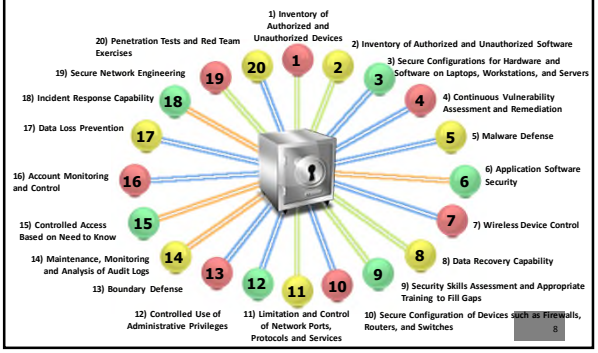
The Critical Security Controls

- Motivation: The "Fog of More"
  - SO much guidance, SO much help, SO many choices
  - *But where to begin?*
- Vulnerabilities are (relatively) well understood
  - *But translation to action was missing*
    - Getting to root causes
    - Establishing basic hygiene, baseline practice
    - the "80/20" of security

The Original Contributors

- Blue Team, Red Team members from DOD, NSA
- US-CERT and other non-military incident response teams, penetration testers
- The FBI and other LE organizations
- US DoE laboratories
- US Department of State
- US Department of Homeland Security
- DoD and private forensics experts, threat analysts
- The SANS Institute
- Federal CIOs and CISOs
- Plus over 100 other collaborators

What are the Critical Controls?



The "First Five"

1. software white listing
2. secure standard configurations
3. application security patching
4. system security patching
5. no administrative privileges while browsing the web or reading e-mail

The Principles

- A community approach
  - Open volunteer development
  - Create a support community (users, vendors, tools, mappings, linkages)
- Focused on attacks, priority
  - Simplify and Be Specific: an *action* focus
  - Bound the problem
- Automation, standards are essential

What's Next?

References

- Critical Security Controls
  - http://www.counciloncybersecurity.org
  - t.sager@counciloncybersecurity.org
- Verizon Data Breach Investigation Report
  - http://www.verizonenterprise.com/DBIR/2013/