The Value of Security Benchmarks and Controls

Curt Dukes
Executive VP & General Manager,
Security Best Practices & Automation Group
March 21, 2017
Some Unfortunate Facts

• The vast majority of compromises are based on known problems that have known solutions

• 85% of the incidents managed by the US-CERT come down to the same five basic defenses

• Very few attackers use “stealth” techniques

• Very few defenders have automated workflow
68 incidents across 8 different countries responded to by Global Incident Response & Recovery Team

15,000 cases worked by the Cyber Defense Operations Center

85 – 90% of Incidents could have been prevented by:
1. Patching Critical Vulnerabilities
2. Removing Administrative Privileges
3. Using Strong Passwords / MFA

*Courtesy MSFT Security Research Center
“The Fog of More”

- anti-malware
- governance
- continuous monitoring
- baseline configuration
- SDL
- audit logs
- risk management framework
- encryption
- threat intelligence
- user awareness training
- two-factor authentication
- security controls
- need-to-know
- DLP
- certification
- penetration testing
- threat feed
- best practice
- SIEM
- virtualization
- sandbox
- compliance
- security bulletins
- incident response
- server isolation
- maturity model
- whitelisting
- anti-malware
- penetration testing
- threat intelligence
- user awareness training
- supply-chain security
- maturity model
- whitelisting
Even Foggier: Frameworks and Standards

ENISA Security Framework for Government Clouds
DHS Cybersecurity Framework
NISP DoD 5220.22-M
Bank of England CBEST
CISQ Automated Source Code Measures
COBIT
NATO CCD Cybersecurity Framework
NERC CIP
NIST 800-53
ISO 27001/27002
PCI DSS
Healthcare Common Security Framework
ISF Standard of Good Practice
The Defender’s Dilemma

1. What’s the right thing to do, and how much do I need to do?

2. How do I actually do it?

3. How can I demonstrate to others that I have done the right thing?
The CIS Critical Security Controls
Focus on the first 6 Controls

• Know what you are protecting
  ✓ CIS Control #1: Inventory of Authorized and Unauthorized Devices
  ✓ CIS Control #2: Inventory of Authorized and Unauthorized Software

• Define Secure Configuration Baseline
  ✓ CIS Control #3: Secure Configurations for Hardware and Software

• Continuously Monitor Vulnerability of Resources
  ✓ CIS Control #4: Continuous Vulnerability Assessment and Remediation

• Limit and Monitor Administrative Privileges
  ✓ CIS Control #5: Controlled Use of Administrative Privileges

• Continuous Monitoring/Situational Awareness
  ✓ CIS Control #6: Maintenance, Monitoring, and Analysis of Audit Logs
• Website:  [www.cisecurity.org](http://www.cisecurity.org)
• Email:  Controlsinfo@cisecurity.org
• Twitter:  @CISecurity
• Facebook:  Center for Internet Security
• LinkedIn Groups:
  • Center for Internet Security
  • 20 Critical Security Controls