Wasting Money on the Tools?
Automating the Most Critical Security Controls

Bonus: Gaining Support From Top Managers for Security Investments

Mason Brown

Director, The SANS Institute

About SANS

- Largest Security Training & Education Organization
  - 95,000 alumni
  - 60+ network security, app security and secure coding courses
  - 150+ events annually
  - 15,000 students per year
- Licensed, degree granting graduate education institution
- GIAC is an ANSI/ISO-accredited certification body
  - More than 26,000 certifications
- SANS Software Security Institute focuses on application layer attacks, defense and education
- Operates Internet Storm Center – the open source early warning system
- Consensus research projects including Top Cyber Security Threats and Top 25 Programming Errors

What is going on with the boss?
A CIO's Environment

- CIO mandates exceed time and resources available
- Cyber security is an enormously complex challenge—there are very few true experts
- Security is not the only thing on the plate
- So…
  - Compliance, Compliance, Compliance
  - Financial risk
  - Embarrassment (personal/brand) risk

It is time to focus on ways to make real improvements in security

Questions for Today

1. What is the landscape?
2. What should we automate?
3. Does automation work?
4. What tools do I need?
5. How do I get past the vendor sales pitch?
6. Won't it cost a lot?
7. What can I do right now?

Focus investments by letting cyber offense inform defense!

Analogy of Current Cybersecurity Approach

- An ambulance shows up at a hospital emergency room with a bleeding patient
- Hospital gives inoculations for flu, tetanus, shingles, and vaccination updates
- Hospital tests for communicable diseases, high blood pressure, sends blood sample for cholesterol check, gives eye exam and checks hearing
- At some point, doctors address the cause of the bleeding

OMB Policy Regarding FISMA Results in a Checklist Approach

Meanwhile, the patient is bleeding to death!!

We Need Triage--Not Comprehensive Medical Care
But how to prioritize?

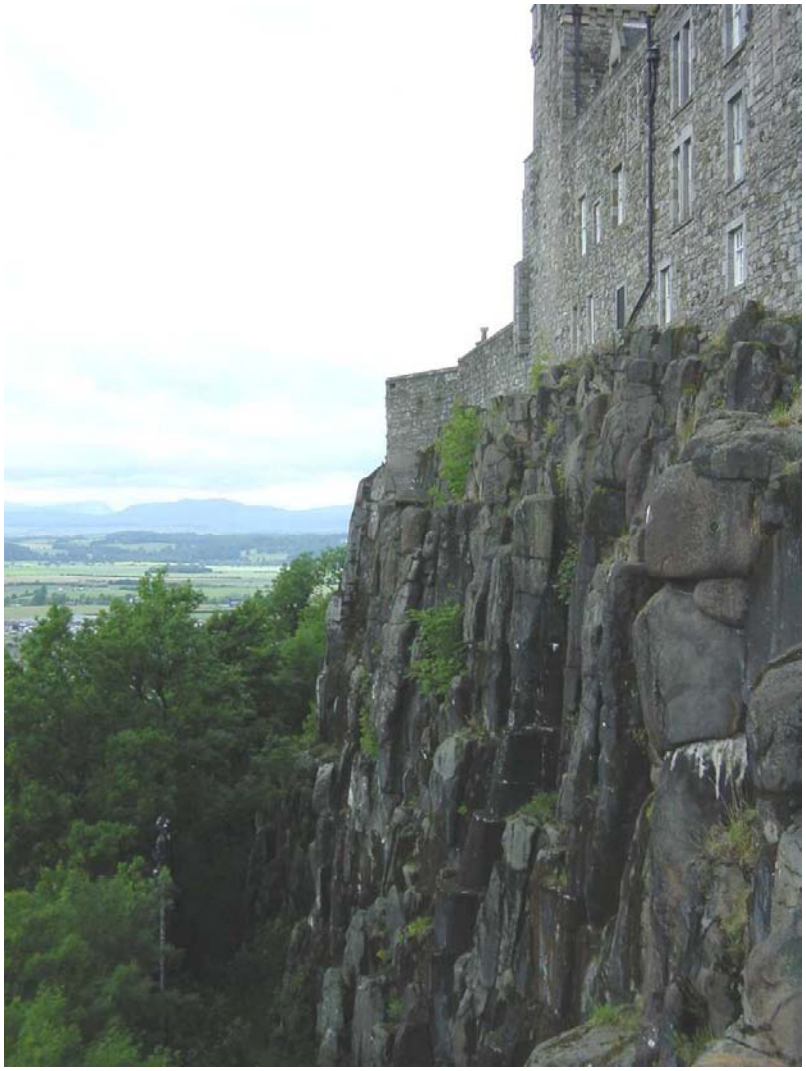
An "Aha" Moment!

- Scene: Briefing by NSA regarding latest penetration assessment of DoD systems
- Objective: Embarrass DoD CIOs for failure to provide adequate security.
- Subplot: If CIOs patch/fix current avenues of penetration, NSA would likely find others
- Realization: Let's use NSA's offensive capabilities to guide security investments

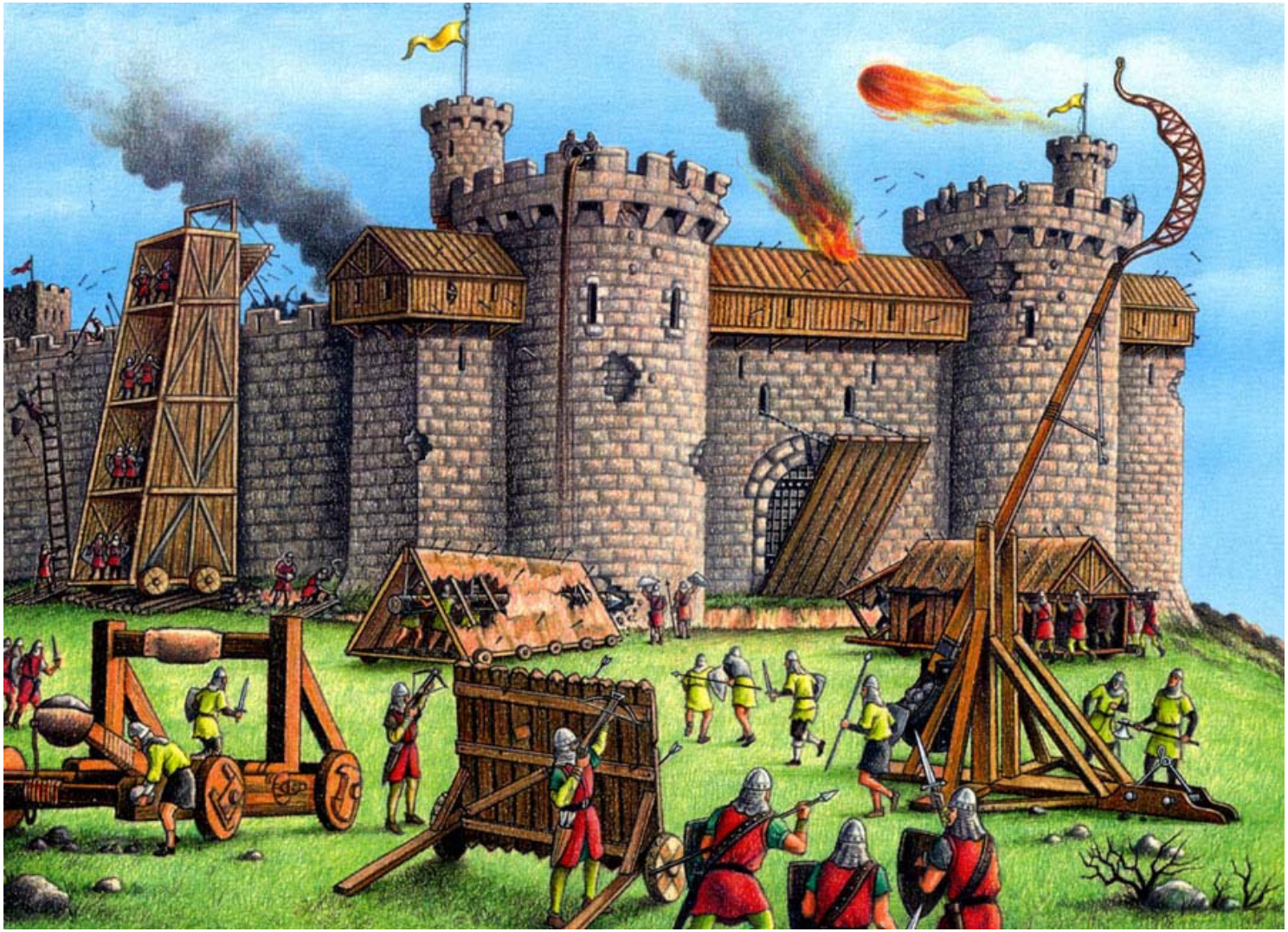
Let "Offense Inform Defense"!

A Quiz

Should You Spend Money Here?



Or Here?



Finding the Most Common Attacks and Critical Controls

- Engage the best security experts:
  - NSA “Offensive Guys”
  - NSA “Defensive Guys”
  - DoD Cyber Crime Center (DC3)
  - US-CERT (plus 3 agencies that were hit hard)
  - Top Commercial Pen Testers
  - Top Commercial Forensics Teams
  - JTF-GNO
  - AFOSI
  - Army Research Laboratory
  - DoE National Laboratories
  - FBI and IC-JTF
- Prioritize controls to match successful attacks—mitigate critical risks
- Identify automation/verification methods and measures
- Engage CIOs, CISOs, Auditors, and Oversight organizations
- Coordinate with Congress regarding FISMA updates

Result: What is Actually Happening.
The Top Attack Patterns*

- **Attack boundary devices with damaged ACLs**
- **Attack without being detected and maintain long-term access due to weak audit logs**
- **Attack web sites exploiting programming errors**
- **Attack client software and other applications**
- **Gain administrator privileges to control target machines**
- **Gain access to sensitive data that is not adequately protected**
- **Exploit vulnerabilities on machines not being monitored and managed**
- **Exploit inactive user accounts**
- **Exploit poorly configured network services**
- **Exploit weak security of wireless devices**
- **Attack systems or organizations that have no or poor attack response**
- **Exploit poorly trained or poorly skilled employees**

* Developed as a part of developing 20 Critical Controls and not in priority order

20 Critical Controls for Effective Cyber Defense (1 of 2)

These are the controls that help defend against common attacks

Critical Controls Subject to Automated Collection, Measurement, and Validation:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance, Monitoring, and Analysis of Security Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based on Need to Know
10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention

20 Critical Controls for Effective Cyber Defense (2 of 2)

Additional Critical Controls (not directly supported by automated measurement and validation):

16. **Secure Network Engineering**
17. **Penetration Tests and Red Team Exercises**
18. **Incident Response Capability**
19. **Data Recovery Capability**
20. **Security Skills Assessment and Appropriate Training to Fill Gaps**

Example--Critical Control #3
Secure Configurations for Hardware and Software on Laptops, Workstations and Servers

- **Attacker Exploit**: Automated search for improperly configured systems
- **Control**:
  - QW: Define standard images that are hardened versions
  - QW: Negotiate contracts for secure images
  - Config/Hygiene: Monthly checks w/ executive metrics showing trends for systems meeting (and not) configuration guidelines
- **Associated NIST SP 800-53 Rev 3 Priority 1 Controls:**
  - CM-1, CM-2 (1, 2), CM-3 (b, c, d, e, 2, 3), CM-5 (2), CM-6 (1, 2, 4), CM-7 (1), SA-1 (a), SA-4 (5), SI-7 (3), PM-6
- **Automated Support**: Employ SCAP compliant tools to monitor/validate HW/SW/Network configurations
- **Evaluation**: Introduce improperly configured system to test response times/actions
- **BP:** Sandia National Labs takes the inventory a step further by requiring the name and contact information of a sysadmin responsible for each element in its inventory. Such information provides near instantaneous access to the people in a position to take action when a system at a given IP address is found to have been compromised.

Relevance of 20 Critical Controls to FISMA and NIST Guidelines

- FISMA
  - Security protections commensurate with risk
  - Implementation of minimum controls
  - Product selection by agencies
  - Periodic testing and evaluation of controls
- NIST Guidelines
  - Risk assessment is foundation
    - CAG based on government-wide risk assessment
  - Selection of controls based on risk
    - CAG controls address top cyber risks
    - 20 Critical Controls are subset of 800-53 controls

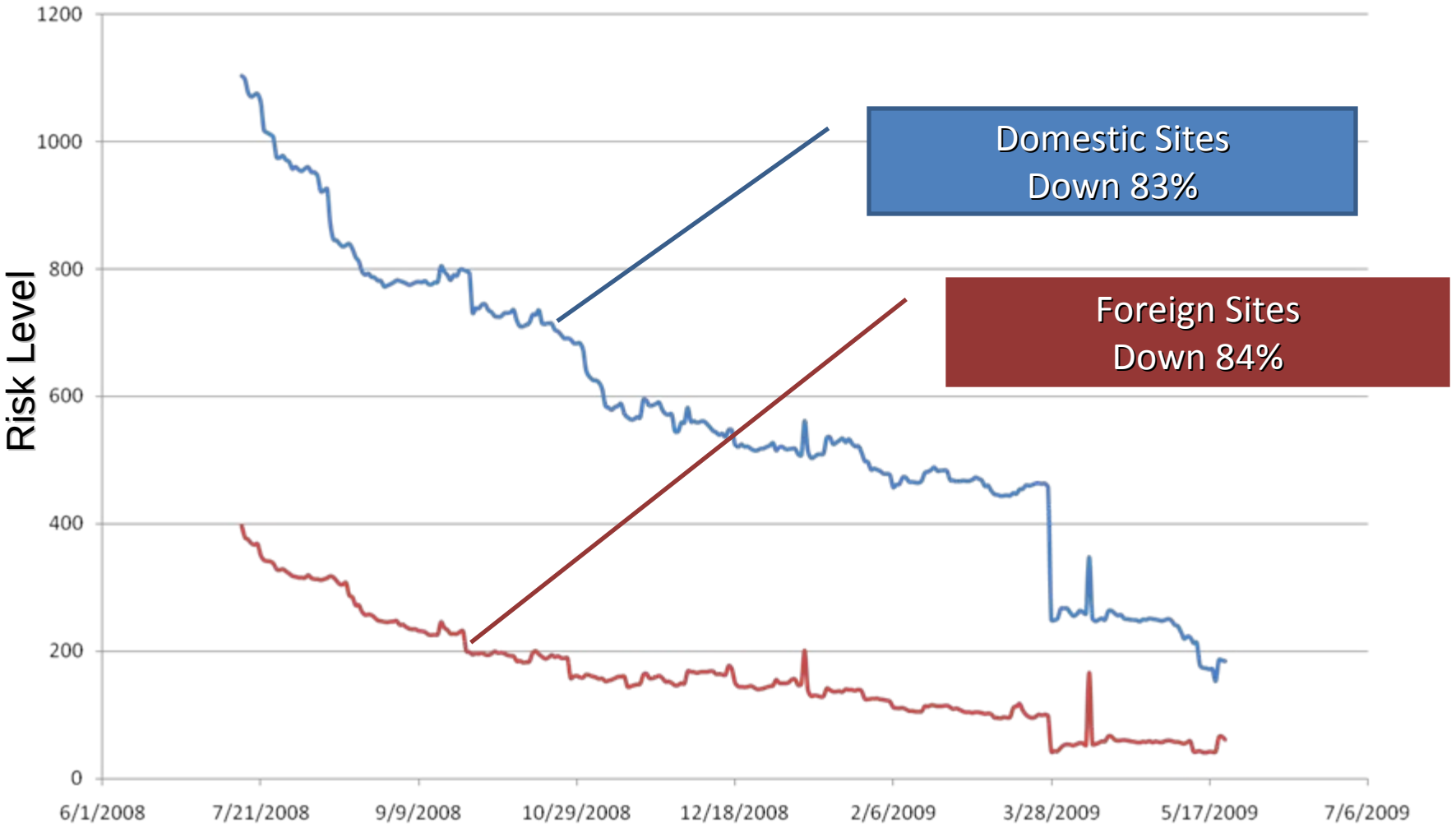
20 Critical Controls helps agencies to comply with FISMA!

Questions for Today

1. What is the landscape?
2. What should we automate?
3. Does automation work?
4. What tools do I need?
5. How do I get past the vendor sales pitch?
6. Won't it cost a lot?
7. What can I do right now?

Focus investments by letting cyber offense inform defense!

Site Scoring Progress
Configurations using SMS, Vulnerability Testing



Questions for Today

1. What is the landscape?
2. What should we automate?
3. Does automation work?
4. What tools do I need?
5. How do I get past the vendor sales pitch?
6. Won't it cost a lot?
7. What can I do right now?

Focus investments by letting cyber offense inform defense!

What Works For Automating the Critical Controls

1. Vendors assert that their tool “automates a specific control”
2. Vendor supplies federal or financial user who can verify they are using it to automate that control (and it works)
3. Results to be published November 12 in Government Computer News and FCW Summit on the Critical Controls
4. Labs can validate SCAP and ARF support

100+ Tools Being Validated

Vendor	Product (Tool)	Critical Controls Addressed	End-User Testimonial
Foundstone (by McAfee)	Foundscan	3	
Qualys	QualysGuard	3,10	
PedSeal	PedSeal Vulnerability Advisor	4	
Secure Bytes	Secure Bytes Secure Cisco Auditor	4	
Algosec	Algosec Firewall Analyzer	4,10	
Lumension	PatchLink Scanner	1,2,10	
Solarwinds	LANSurveyor/Engineer Toolset	1(LanSurveyor)/4(Engineer Toolset)	
Lumeta	IP Sonar	1	
Insightix	BSA Visibility	1	
Tenable	Nessus	3,10	
Trusted Computer Solutions	Security Blanket	4,8,13 and user doing the?	
IPSwitch	WhatsUpGold	1	
ESACO	Network Inventory	1,2	
BMC	Remedy Asset Manager	1	
Cyber Operations	ACL Compliance Director	4	
LANDesk	Asset Manager	1	
IBM	ISS/Tivoli/AppScan	1/Tivoli	
BIX	Parity	2	
Komodo Laboratories	NEWT Professional		
Shavlik	Hotchik	2	
eEye	End Point Solution/Retina	2(endpoint Systems)	
Symantec	End Point Solution	2	
Sophos	End Point Solution	2	
nCircle	Suite 360		
AirMagnet	WiFiAnalyzer PRO		
Archer Technologies	SmartSuite		
CACE Technologies	CACE AirPCap Tx/Pilot		
Citrix	ONE		
[illegible]	Canvas Professional		
ESA	ESA Defend		
Kaspersky Lab	Administration Kit		
Manage Engine	ADAudit Plus/Firewall Analyzer	4(firewallanalyzer),11(ADaudit plus)	
MaxPowerSoft	Active Directory Reports		
McAfee	ePolicy Orchestrator		
Microsoft	Forefront & System Center		
Motorola Inc.	AirDefense Mobile		
NetScout	NetScout nGenius Performance Manager & Visualizer		
Network Instruments	NIObserver		
Quest	Enterprise Security Reporter	11	
Rapid 7	Nexpose	1-7, 10-11, 13-15?	
Relational Security	RSAM		
Skybox Security	Security Products	4,10	
Trend Micro	Control Manager		
Fortify	Fortify 360		
Ounce Labs/IBM	Core	7	

Cool Discovery 1

Network device configuration

1. Has your organization ever changed the access control list (ACL) on firewalls and/or routers to allow traffic for specific applications or events? Did you remember to change them all back? Are you sure?
2. Validating a full rule set on a major router takes 2-3 days of an extraordinary technology expert.
3. We found a tool that automates it fully.

Cool Discovery 2

Hardware Inventory (it is hard to protect systems that you don't know you own)

1. Most inventory tools use an active 'ping' and miss a substantial portion of the assets…and usually cannot tell you (real time) when a rogue machine is installed
2. We found two that can find almost all and alert you – using passive discovery, router logs, and more, in addition to active pinging.
3. Huge time savings.

Final Thoughts

- We can’t do everything
- We know where to focus
- We know what can be automated
- We can validate the tools that work
- Procurement can be leveraged to make it affordable

We Need to Stop the Bleeding—Now!

Bonus: Career Move

What you can do right now.

- No one knows yet if this will replace FISMA
- Do the gap analysis
- Show it to your executives. They are thinking about compliance, risk and embarrassment.
- Show them you are too.
- It's not too hard and you need to do it anyway – the Controls just save you time figuring out priorities
- Then when it comes, you are the 'expert'

More on Controls and Tools

- Critical Controls URLs:
  www.sans.org/critical-security-controls/
  http://csis.org/files/publication/Twenty_Critical_Controls_for_Effective_Cyber_Defense_CAG.pdf

- FCW Critical Controls Tools Event
  http://1105govinfoevents.com/EventOverview.aspx?Event=CSC09

Contact Information

Mason Brown

mbrown@sans.org

www.sans.org