The New Security Heroes

Alan Paller
apaller@sans.org

How they attack

- Spam with infected attachments
- Web sites that have infected content
- The most dangerous: targeted attacks
  - Fooling the victim into
  - Installing a program that
  - Calls the mother ship to get instructions telling it to
  - Connect with the servers inside the victim's organization to
  - Steal information,
  - Install back doors, and
  - Attack others

Increasing & Shifting

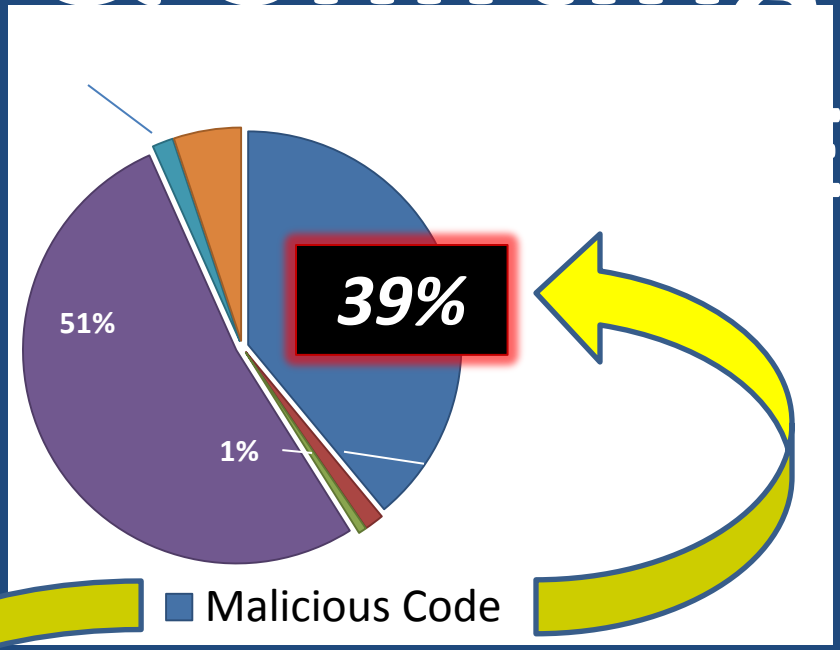
TICKETS

Years Compared	
FY 08	*FY 09*
2104	**3085**

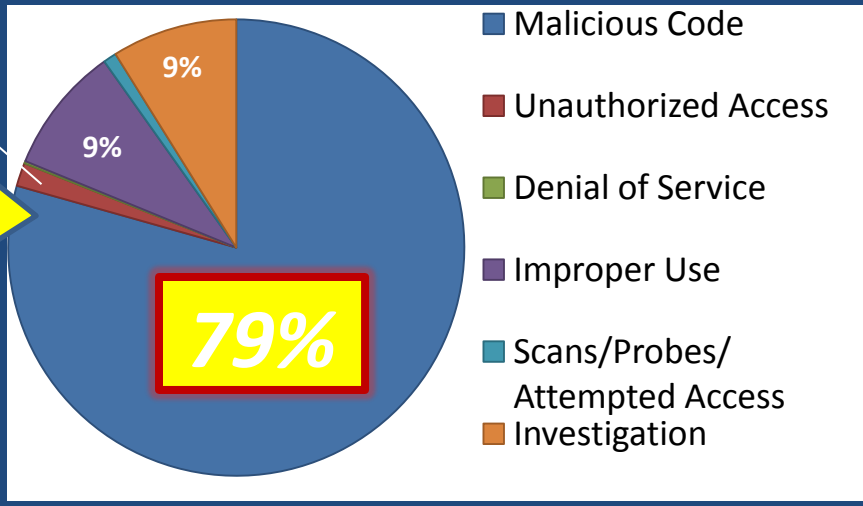
FY 09 Quarters	
Quarters	*Tickets*
Oct-Dec 08	560
Jan-Mar 09	555
Apr-Jun 09	639
July-Aug 09 *(Partial)*	805

Months Compared		
	2008 - Tickets	*2009- Tickets*
June	**154**	**300**
July	**183**	**352**
August	**250**	**453**

FY08



FY09



Bringing about broad based change when no one works for you

The problem: CXOs are **accountable** for IT security

BUT

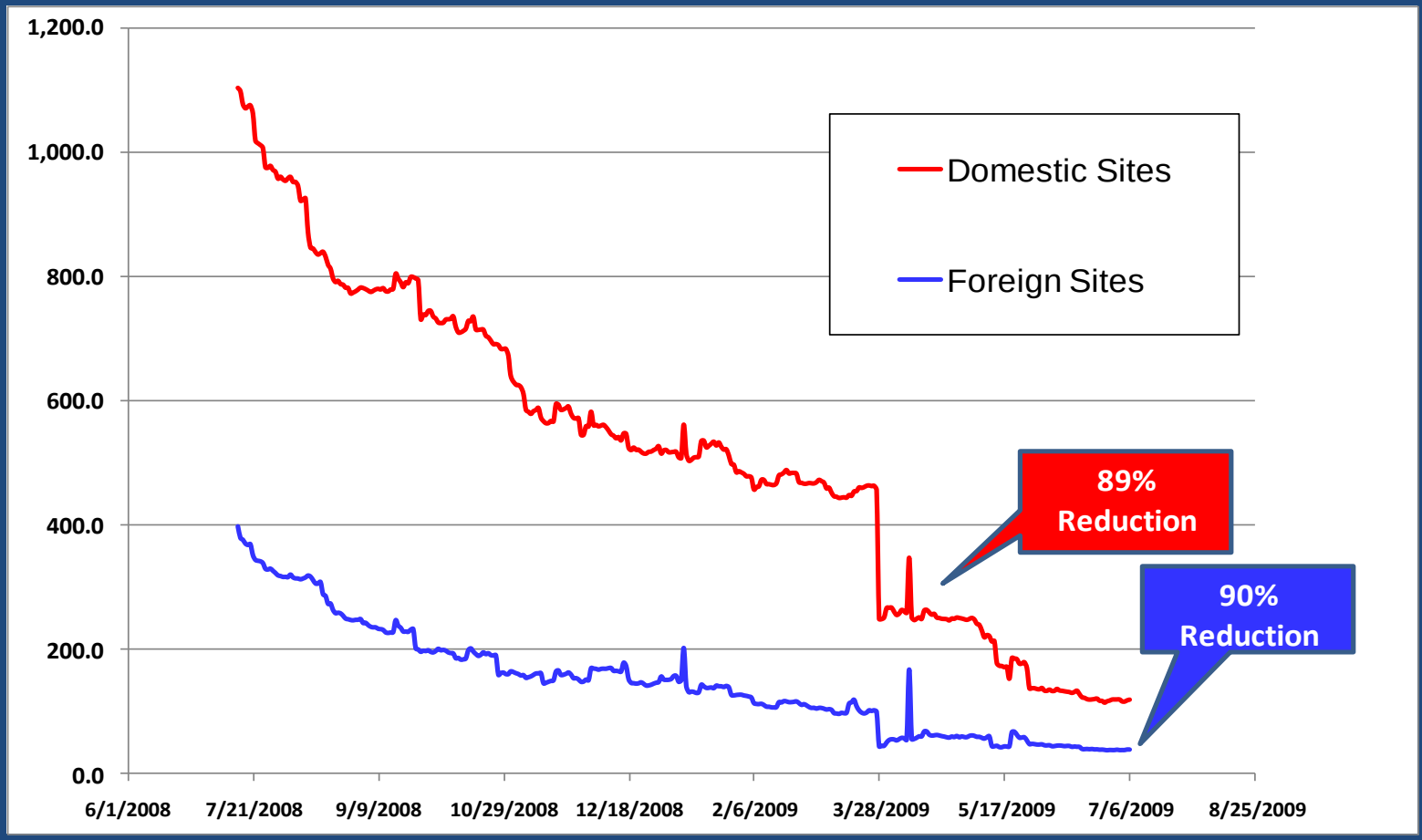
.

directly supervise only a small part of the systems actually in use.

What makes a security hero?

- Radically improves security in ways that can be measured reliably, and replicated
- Ensures operational people are not asked to do the impossible. Ends the security wars with IT operations and with the audit staff.
- Teaches others organizations how to do the same thing or provides the catalyst to allow others to do even more

Results in 12 Months



Yet he never visited any of the 200+ foreign sites

So how did he do it?

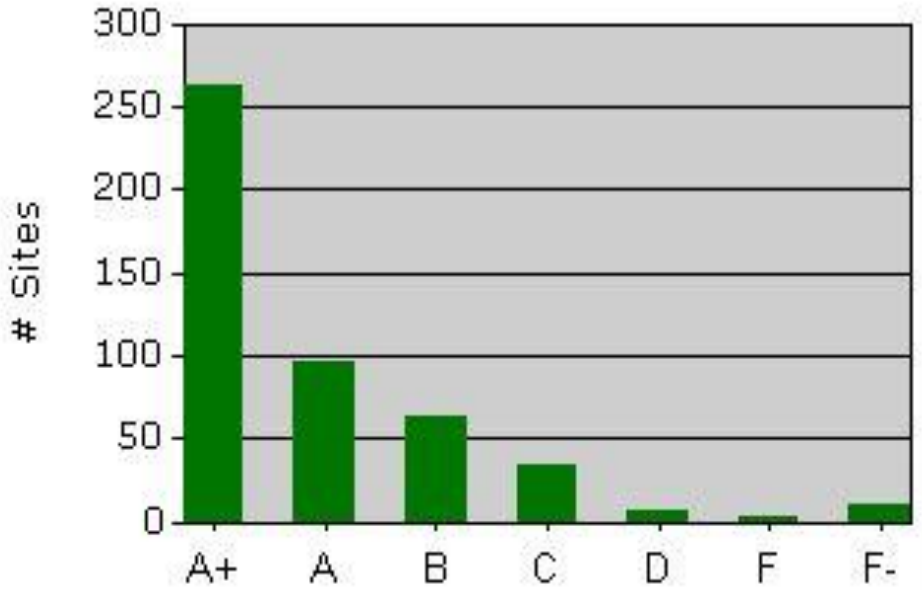
Risk Score Monitor Enterprise

Total Hosts	32,366	51,157
Average Risk Score per Host	101.7	33.2

Grading Scale

Average Risk Score		
At Least	Less Than	Grade
0.0	40.0	A+
40.0	75.0	A
75.0	110.0	B
110.0	180.0	C
180.0	280.0	D
280.0	400.0	F
400.0	-	F-

Grade Dis



Used the 20 critical controls

CAG ID	Consensus Audit Guidelines	NIST-800-53	CIRT Events 11 mo
1	Inventory of authorized and unauthorized hardware	CM-1, CM-2, CM-3, CM-4, CM-5, CM-8, CM-9	**Multiple Tools < 6% < 22%**
2	Inventory of authorized and unauthorized software	CM-1, CM-2, CM-3, CM-5, CM-7, CM-8, CM-9, SA-7	
3	Secure configurations for HW and SW, if available	CM-6, CM-7, CP-10, IA-5, SC-7	Nominal
4	Secure configurations for network devices such as firewalls and routers	AC-4, CM-6, CM-7, CP-10, IA-5, RA-5, SC-7	Nominal
5	Boundary Defense	AC-17, RA-5, SC-7, SI-4	< 7%
6	Maintenance/Analysis of complete security audit logs	AU-1, AU-2, AU-3, AU-4, AU-6, AU-7, AU-9, AU-11, AU-12, CM-3, CM-5, CM-6, SI-4	Nominal
7	Application software security	AC-4, CM-4, CM-7, RA-5, SA-3, SA-4, SA-8, SA-11, SI-3	Decentralized
8	Controlled use of Administrative Privileges	AC-6, AC-17, AT-2, AU-2	Nominal
9	Controlled access based on need to know	AC-1, AC-2, AC-3, AC-6, AC-13	< 1%
10	Continuous vulnerability testing and remediation	CA-2, CA-6, CA-7, RA-5, SI-2	Nominal
11	Dormant account monitoring and control	AC-2, PS-4, PS-5	Nominal
12	**Anti-malware defenses**	AC-3, AC-4, AC-6, AC-17, AC-19, AC-20, AT-2, AT-3, CM-5, MA-3, MA-4, MA-5, MP-2, MP-4, PE-3, PE-4, PL-4, PS-6, RA-5, SA-7, SA-12, SA-13, SC-3, SC-7, SC-11, SC-20, SC-21, SC-22, SC-23, SC-25, SC-26, SC-27, SC-29, SC-30, SC-31, SI-3, SI-8	< 60%
13	Limitation and control of ports, protocols and services	AC-4, CM-6, CM-7, SC-7	Not yet graded
14	Wireless device control	AC-17	Nominal
15	**Data leakage protection**	AC-2, AC-4, PL-4, SC-7, SC-31, SI-4	Pending

How one can recognize a “security “hero”

- The CISO of California “UN.BE.LIEV.ABLE”
- Jim Lewis “The only rock star in security”
- The Army General’s standing ovation

SOLUTION

Information & Tools

Timely – Targeted – Prioritized

"Metrics with the Most Meaning"

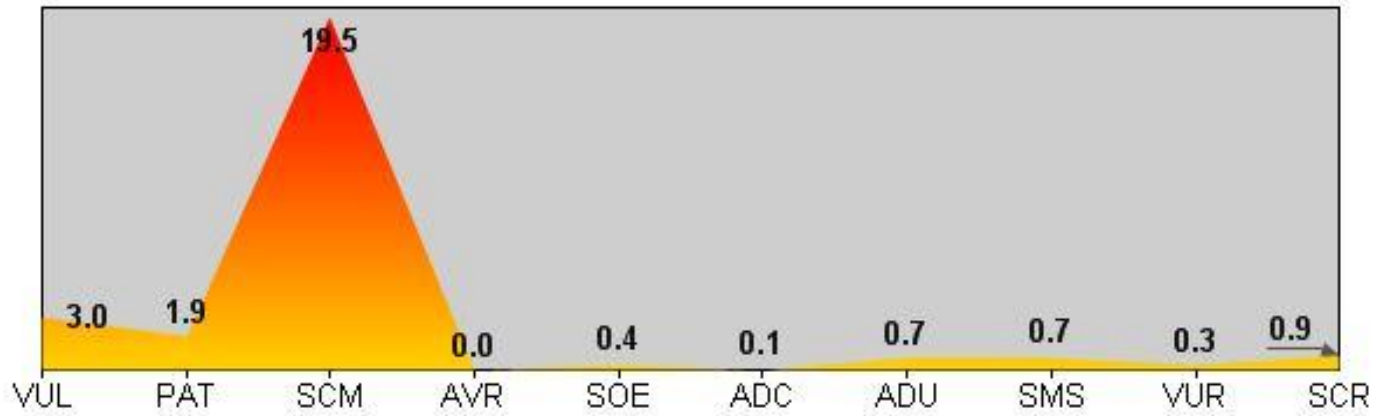
Risk Score Advisor

The following grading scale is provided by Information Assurance and may be revised periodically.

Site Risk Score	8,687.1
Hosts	317
Average Risk Score	27.4
Risk Level Grade	A+
Rank in Enterprise	163 of 438
Rank in Region	16 of 48

Average Risk Score		
At Least	Less Than	Grade
0.0	40.0	A+
40.0	75.0	A
75.0	110.0	B
110.0	180.0	C
180.0	280.0	D
280.0	400.0	F
400.0	-	F-

Risk Score Profile



Component	Risk Score	Avg / Host	% of Score	How Component is Calculated
VUL - Vulnerability	947.0	3.0	10.9 %	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
PAT - Patch	603.0	1.9	6.9 %	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
SCM - Security Compliance	6,181.2	19.5	71.2 %	From .9 for each failed Application Log check to .43 for each failed Group Membership check
AVR - Anti-Virus	0.0	0.0	0.0 %	6 per day for each signature file older than 6 days
SOE - SOE Compliance	115.0	0.4	1.3 %	5 for each missing or incorrect version of an SOE component
ADC - AD Computers	26.0	0.1	0.3 %	1 per day for each day the AD computer password age exceeds 35 days
ADU - AD Users	222.0	0.7	2.6 %	1 per day for each account that does not require a smart-card and whose password age > 60, plus 5 additional if the password never expires
SMS - SMS Reporting	230.0	0.7	2.6 %	100 + 10 per day for each host not reporting completely to SMS
VUR - Vulnerability Reporting	84.0	0.3	1.0 %	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days
SCR - Security Compliance Reporting	279.0	0.9	3.2 %	After a host has no scans for 30 consecutive days, 5 + 1 per 15 additional days
Total Risk Score	**8,687.1**	**27.4**	**100.0 %**	

For additional information on Risk Scoring, assistance with remediations, or to report suspected false positives, contact the IT Service Center to open a "Risk Score" ticket.

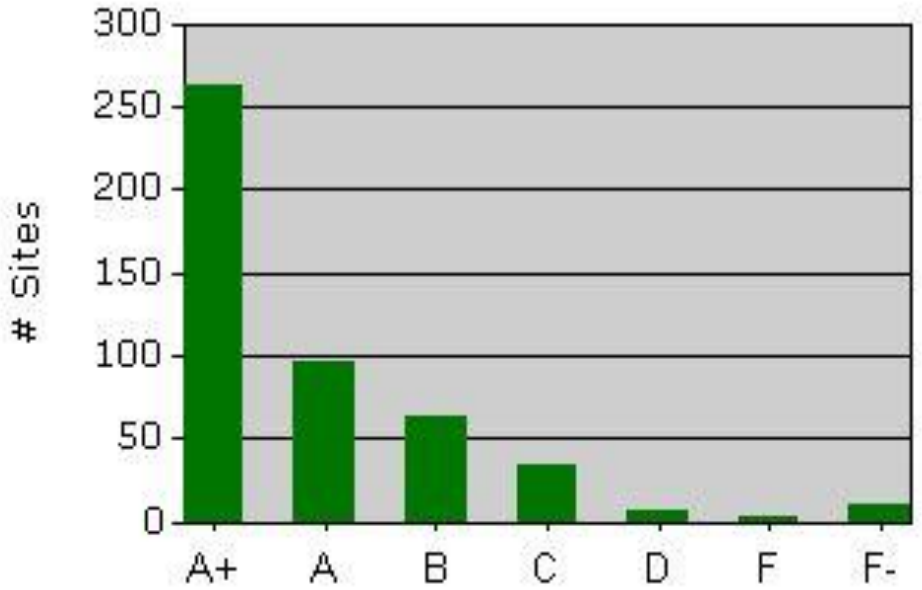
Risk Score Monitor Enterprise

Total Hosts	32,366	51,157
Average Risk Score per Host	101.7	33.2

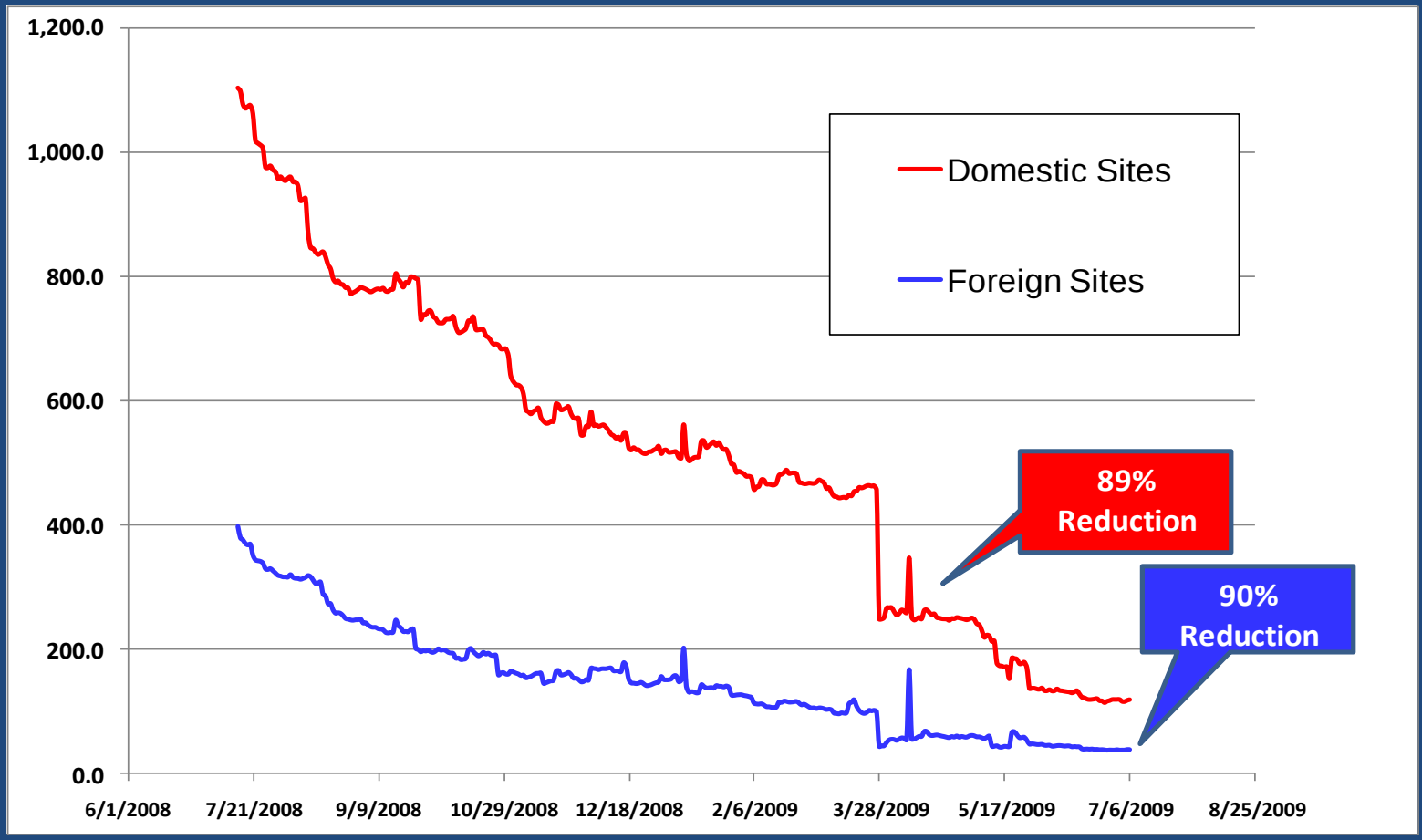
Grading Scale

Average Risk Score		
At Least	Less Than	Grade
0.0	40.0	A+
40.0	75.0	A
75.0	110.0	B
110.0	180.0	C
180.0	280.0	D
280.0	400.0	F
400.0	-	F-

Grade Dis



Results in 12 Months



Finding

Details empower technical managers

FOR TARGETED, DAILY ATTENTION TO REMEDIATION

Summaries empower executives

TO OVERSEE CORRECTION OF MOST SERIOUS PROBLEMS

Conclusions

- Huge improvements in a short time
- Scalable to large complex public and private sector organizations
- Higher ROI for continuous monitoring of technical controls as a substitute for paper reports

What allows continuous monitoring to work?

Because it combined:

- Reliability and fairness in the metrics
- Authoritative consensus on what needed to be measured

- But where did the consensus come from?
- And what else makes metrics effective?

Authoritative and Important
How can you prove you meet those criteria?

The big idea:

“Offense informs defense!”

Who understands offense?

- NSA Red Teams
- NSA Blue Teams
- 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
- State Dept.

Would they be willing to combine their knowledge of attacks and offense to define the most important defensive investments CIOs must make?

YES, UNDER THE DIRECTION OF JOHN GILLIGAN?

1. CIO OF US DEPARTMENT OF ENERGY
2. CIO OF US AIR FORCE
3. CO-CHAIR OF THE FEDERAL CIO COUNCIL SECURITY COMMITTEE
4. KEY MEMBER OF THE COMMISSION ON CYBERSECURITY FOR THE 44TH PRESIDENCY
5. PRES. OBAMA'S TRANSITION TEAM LEAD FOR IT AND INFORMATION SECURITY FOR BOTH DOD AND THE INTELLIGENCE COMMUNITY

Consensus Audit Guidelines (CAG) Steps to broad implementation

1. ***Start with attacks (offense informs defense)***
2. ***Agree on the controls that would stop or quickly recover from the known attacks.***
3. Agree how to automate and measure effectiveness
4. Public review period (Feb -March 2009) and revision
5. Pilot program in two agencies and tuning
6. Establish tests that repeatably evaluate effectiveness
7. Find the tools that automate each control
8. Gain OMB, CIO and IG agreement to adopt the CAG.
9. ***Buy it together to keep costs down.***
10. Commercial adoption as “minimum standard of due care.”
11. Keep controls current through multi-agency governance

Result: Twenty Critical Controls

Consensus Audit Guidelines (CAG)

- The twenty key controls
  1. 15 subject to automation: examples
     1. Inventory
     2. Wireless
     3. Configuration
  2. 5 that are important but cannot be easily automated

15 critical controls can be automated

CAG ID	Consensus Audit Guidelines	NIST-800-53	CIRT Events 11 mo
1	Inventory of authorized and unauthorized hardware	CM-1, CM-2, CM-3, CM-4, CM-5, CM-8, CM-9	**Multiple Tools < 6% < 22%**
2	Inventory of authorized and unauthorized software	CM-1, CM-2, CM-3, CM-5, CM-7, CM-8, CM-9, SA-7	
3	Secure configurations for HW and SW, if available	CM-6, CM-7, CP-10, IA-5, SC-7	Nominal
4	Secure configurations for network devices such as firewalls and routers	AC-4, CM-6, CM-7, CP-10, IA-5, RA-5, SC-7	Nominal
5	Boundary Defense	AC-17, RA-5, SC-7, SI-4	< 7%
6	Maintenance/Analysis of complete security audit logs	AU-1, AU-2, AU-3, AU-4, AU-6, AU-7, AU-9, AU-11, AU-12, CM-3, CM-5, CM-6, SI-4	Nominal
7	Application software security	AC-4, CM-4, CM-7, RA-5, SA-3, SA-4, SA-8, SA-11, SI-3	Decentralized
8	Controlled use of Administrative Privileges	AC-6, AC-17, AT-2, AU-2	Nominal
9	Controlled access based on need to know	AC-1, AC-2, AC-3, AC-6, AC-13	< 1%
10	Continuous vulnerability testing and remediation	CA-2, CA-6, CA-7, RA-5, SI-2	Nominal
11	Dormant account monitoring and control	AC-2, PS-4, PS-5	Nominal
12	**Anti-malware defenses**	AC-3, AC-4, AC-6, AC-17, AC-19, AC-20, AT-2, AT-3, CM-5, MA-3, MA-4, MA-5, MP-2, MP-4, PE-3, PE-4, PL-4, PS-6, RA-5, SA-7, SA-12, SA-13, SC-3, SC-7, SC-11, SC-20, SC-21, SC-22, SC-23, SC-25, SC-26, SC-27, SC-29, SC-30, SC-31, SI-3, SI-8	< 60%
13	Limitation and control of ports, protocols and services	AC-4, CM-6, CM-7, SC-7	Not yet graded
14	Wireless device control	AC-17	Nominal
15	**Data leakage protection**	AC-2, AC-4, PL-4, SC-7, SC-31, SI-4	Pending

How one can recognize a “security “hero”

- The CISO of California “UN.BE.LIEV.ABLE”
- Jim Lewis “The only rock star in security”
- The Army General’s standing ovation

John Gilligan's answer to: "We don't have a lot of money; how can we get started doing what State did ?"

- You already have most (70%) of the tools you need to automate security risk measurement.
- The State Dept. will give you the software they use to measure and display risk.
- This isn't a money issue or a technology issue. It's a leadership issue. You don't have to wait for someone to tell you to do it.
- There is no other path available to CIOs and security managers to escape from the "compliance morass" and make a measureable difference in security.