FISMA 2.0: Continuous Monitoring Case Study Update

John Streufert (DOSCISO@state.gov)
Deputy Chief Information Officer for Information Security
US Department of State

February 14, 2011

Nature of Attacks

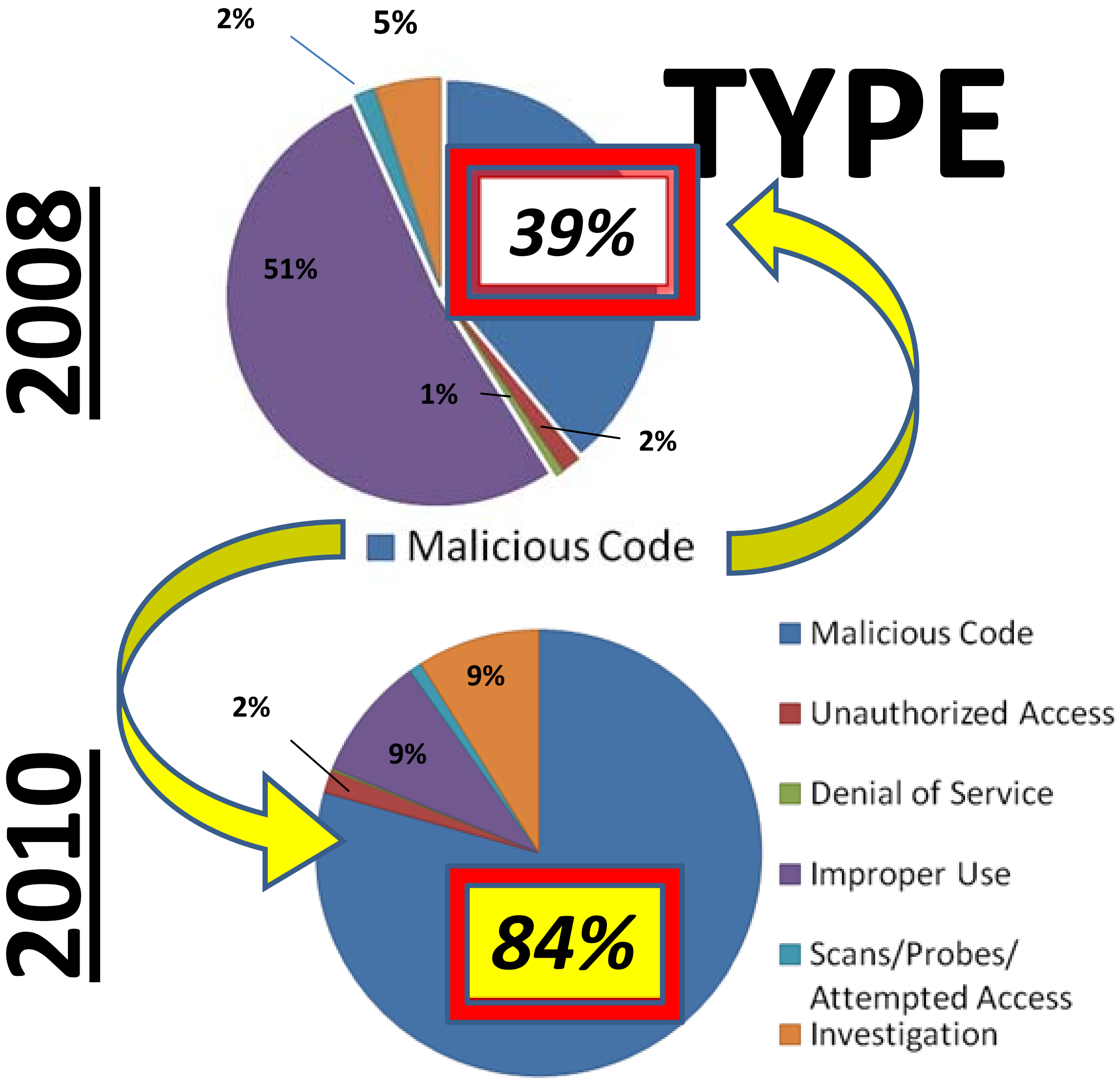
80% of attacks leverage known vulnerabilities and configuration management setting weaknesses

Threats Further Escalate

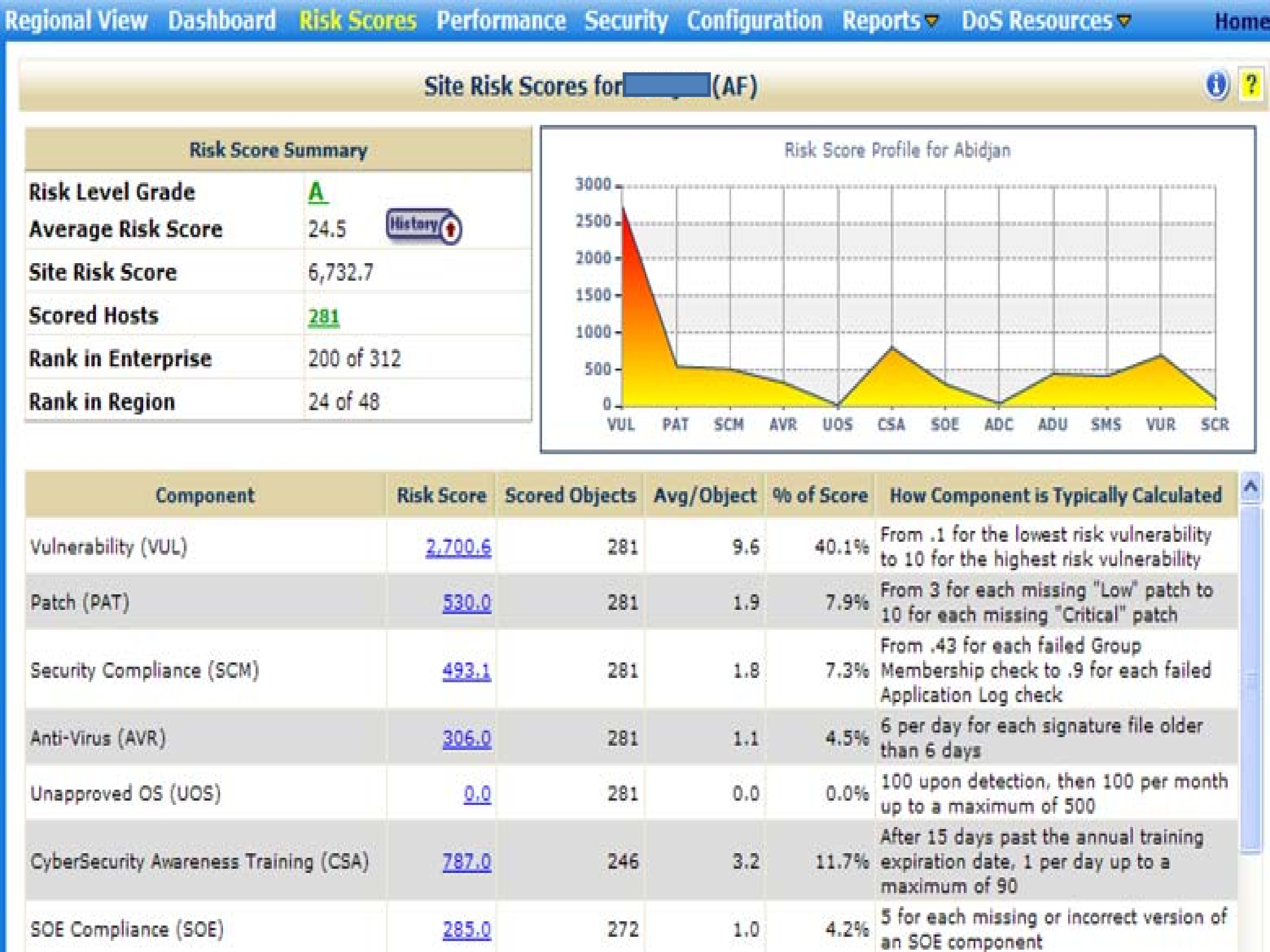
TICKET

Year	*Tickets*
2008	*2104*
2009	*3085*
2010	*7,998*

TYPE



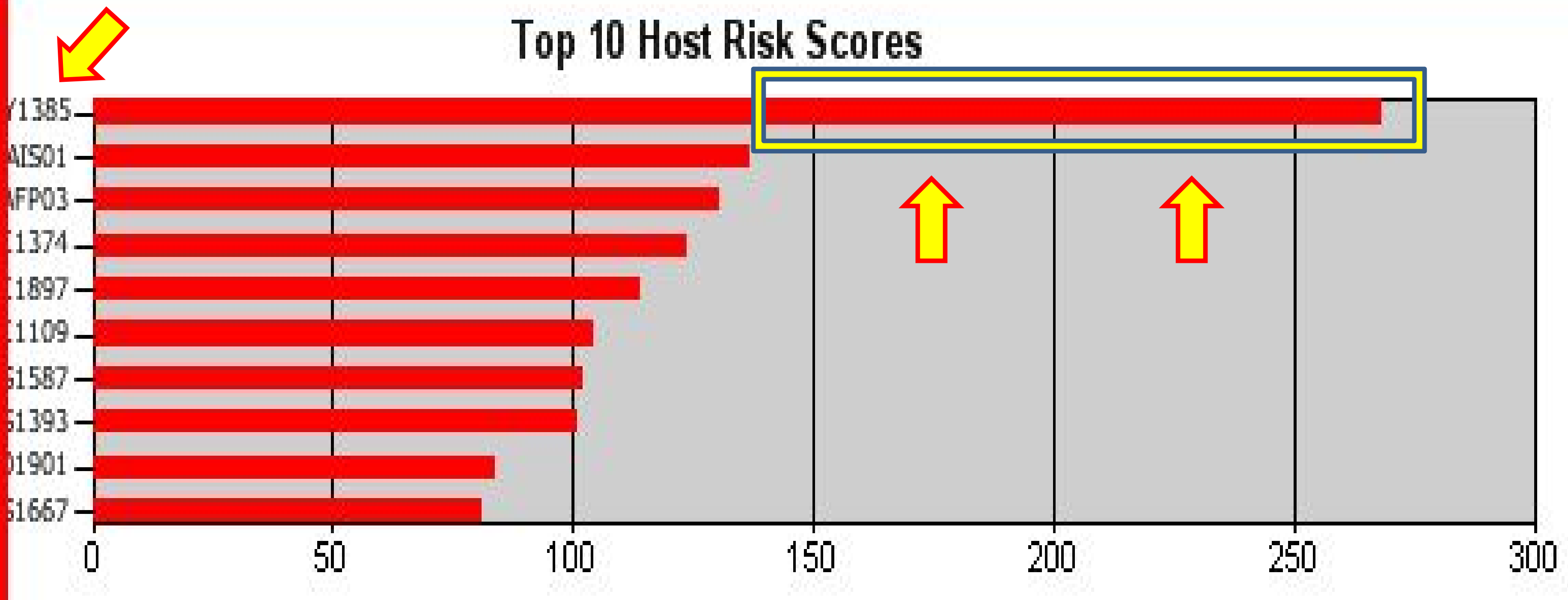
Continuous Monitoring

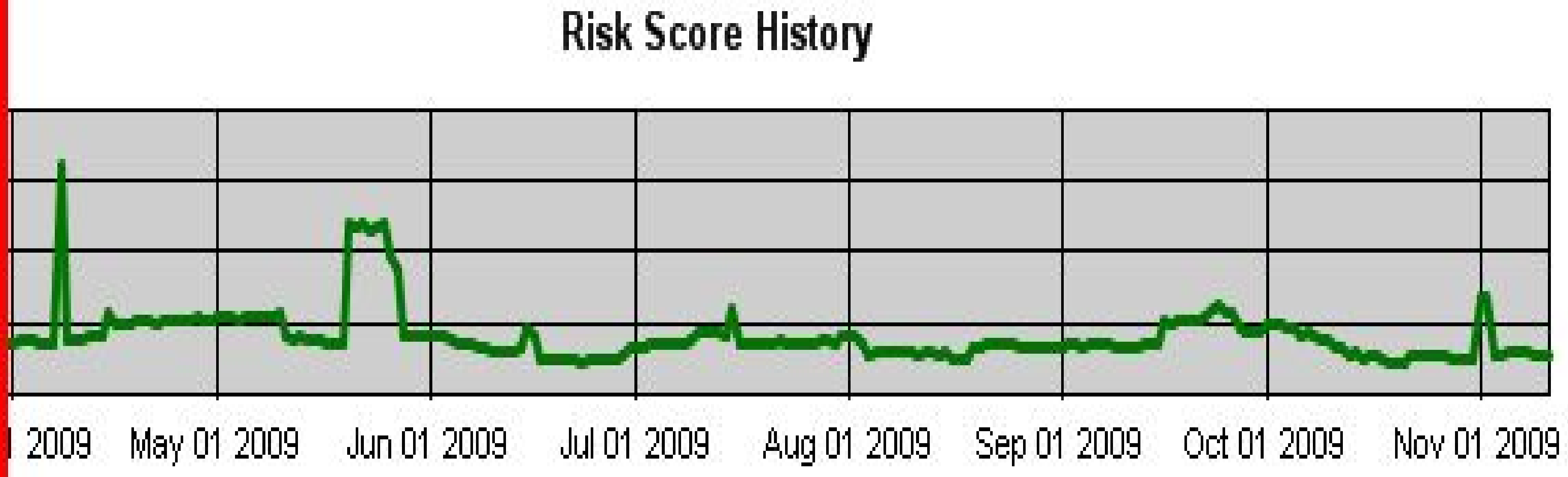


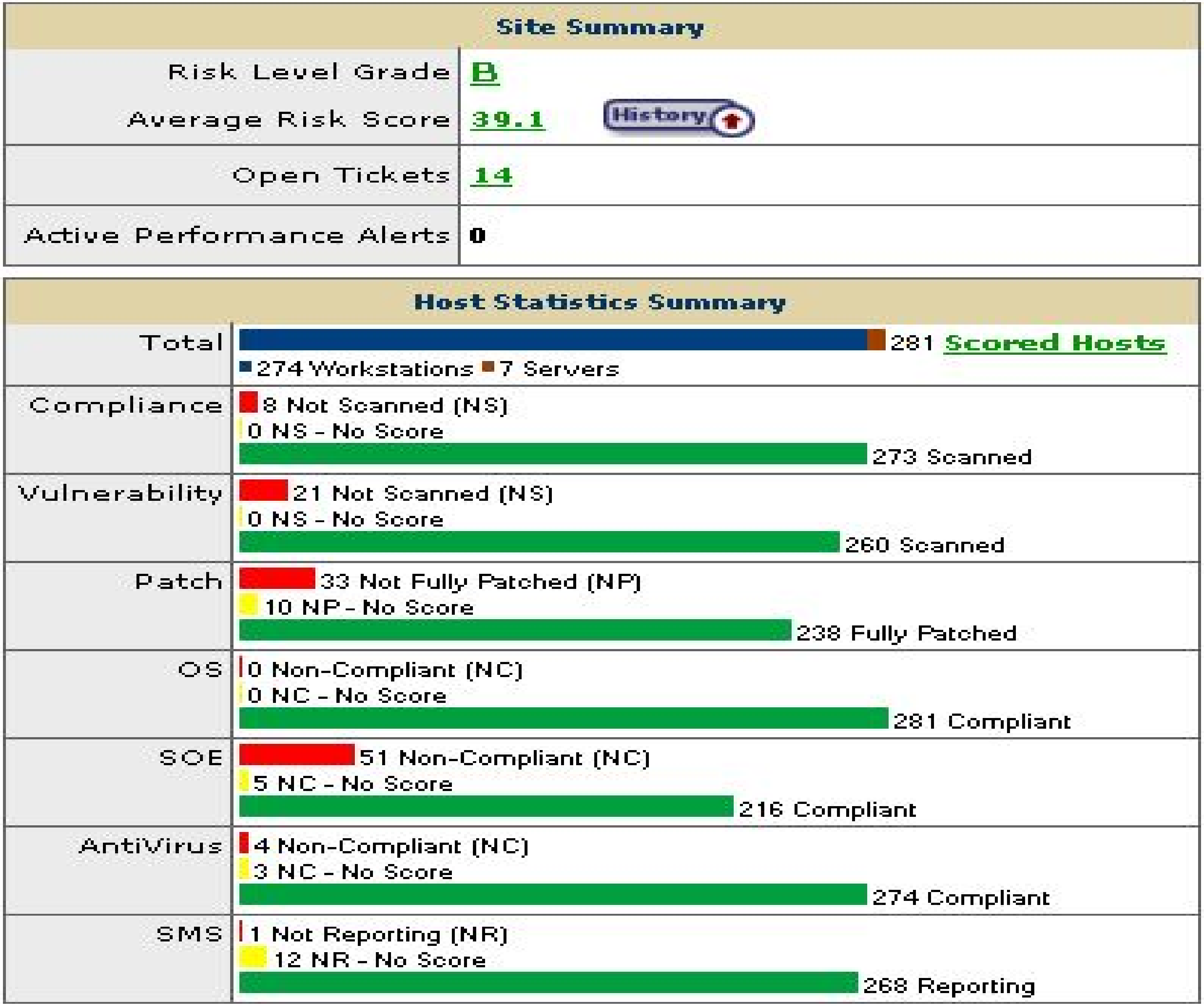
Site Risk Scores for [redacted] (AF)

Risk Score Summary		
Risk Level Grade	A	
Average Risk Score	24.5	History
Site Risk Score	6,732.7	
Scored Hosts	281	
Rank in Enterprise	200 of 312	
Rank in Region	24 of 48	

Component	Risk Score	Scored Objects	Avg/Object	% of Score	How Component is Typically Calculated
Vulnerability (VUL)	2,700.6	281	9.6	40.1%	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
Patch (PAT)	530.0	281	1.9	7.9%	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
Security Compliance (SCM)	493.1	281	1.8	7.3%	From .43 for each failed Group Membership check to .9 for each failed Application Log check
Anti-Virus (AVR)	306.0	281	1.1	4.5%	6 per day for each signature file older than 6 days
Unapproved OS (UOS)	0.0	281	0.0	0.0%	100 upon detection, then 100 per month up to a maximum of 500
CyberSecurity Awareness Training (CSA)	787.0	246	3.2	11.7%	After 15 days past the annual training expiration date, 1 per day up to a maximum of 90
SOE Compliance (SOE)	285.0	272	1.0	4.2%	5 for each missing or incorrect version of an SOE component


Top 10 Host Risk Scores
Y1385
AIS01
FP03
1374
1897
1109
1587
1393
1901
1667
0
50
100
150
200
250
300


Risk Score History
2009
May 01 2009
Jun 01 2009
Jul 01 2009
Aug 01 2009
Sep 01 2009
Oct 01 2009
Nov 01 2009



Site Summary	
Risk Level Grade	B
Average Risk Score	39.1 History
Open Tickets	14
Active Performance Alerts	0

Host Statistics Summary	
Total	281 Scored Hosts ■ 274 Workstations ■ 7 Servers
Compliance	🟥 8 Not Scanned (NS) 0 NS - No Score 273 Scanned
Vulnerability	🟥 21 Not Scanned (NS) 0 NS - No Score 260 Scanned
Patch	🟥 33 Not Fully Patched (NP) 🟨 10 NP - No Score 238 Fully Patched
OS	0 Non-Compliant (NC) 0 NC - No Score 281 Compliant
SOE	🟥 51 Non-Compliant (NC) 🟨 5 NC - No Score 216 Compliant
AntiVirus	🟥 4 Non-Compliant (NC) 🟨 3 NC - No Score 274 Compliant
SMS	1 Not Reporting (NR) 🟨 12 NR - No Score 268 Reporting

Continuous C&A 2.0

a. Once in 3 year study of 110 technical, managerial and operational controls (NIST 800-53)

- 25-2000 pages; $30K - $+2.5M

Library cost: $130M in 6 years

- 95,000 pages @ $1400 per page

Changes: 150 - 200 a week,

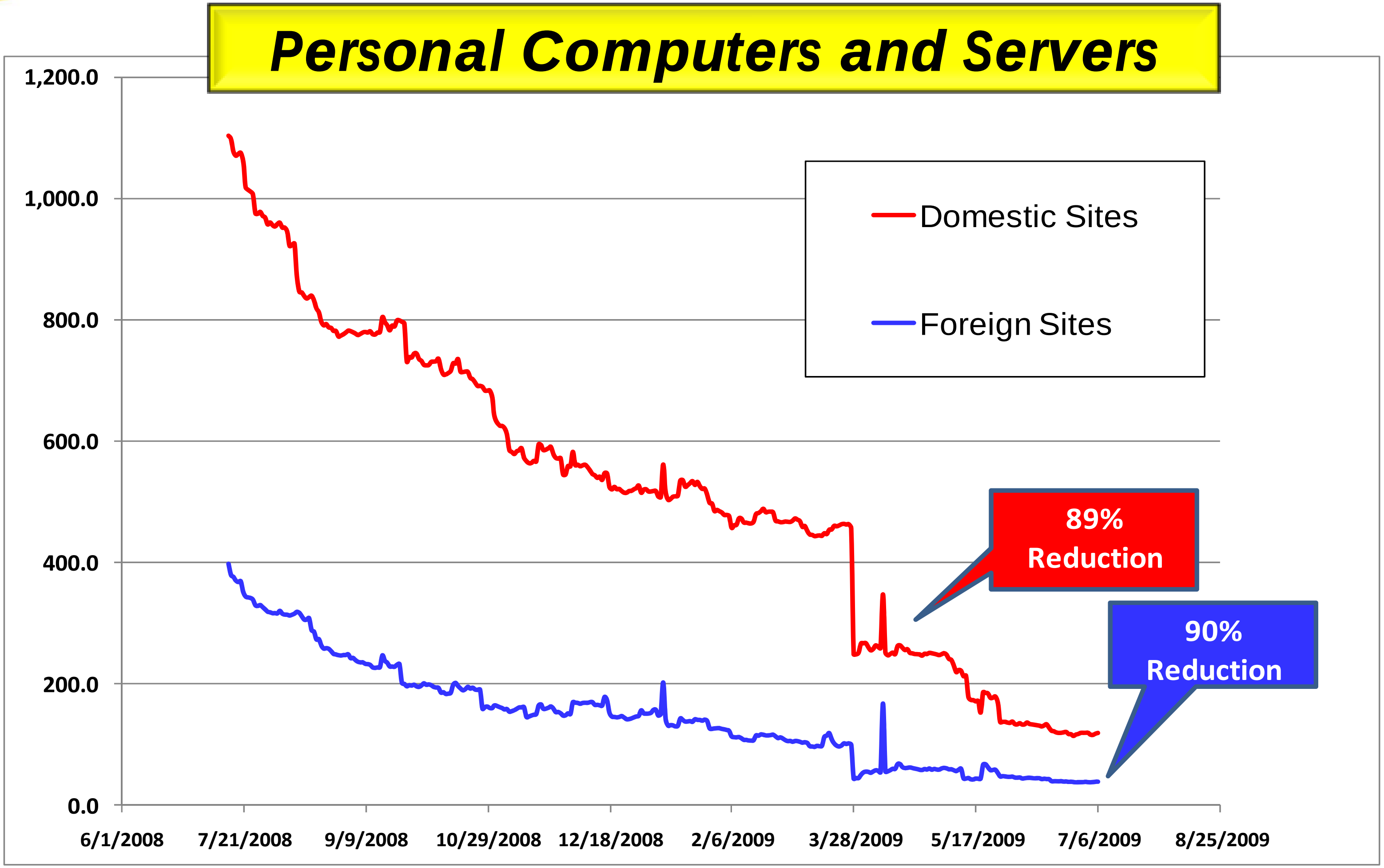
- 24,000 programs changed in 3 years

ROI?

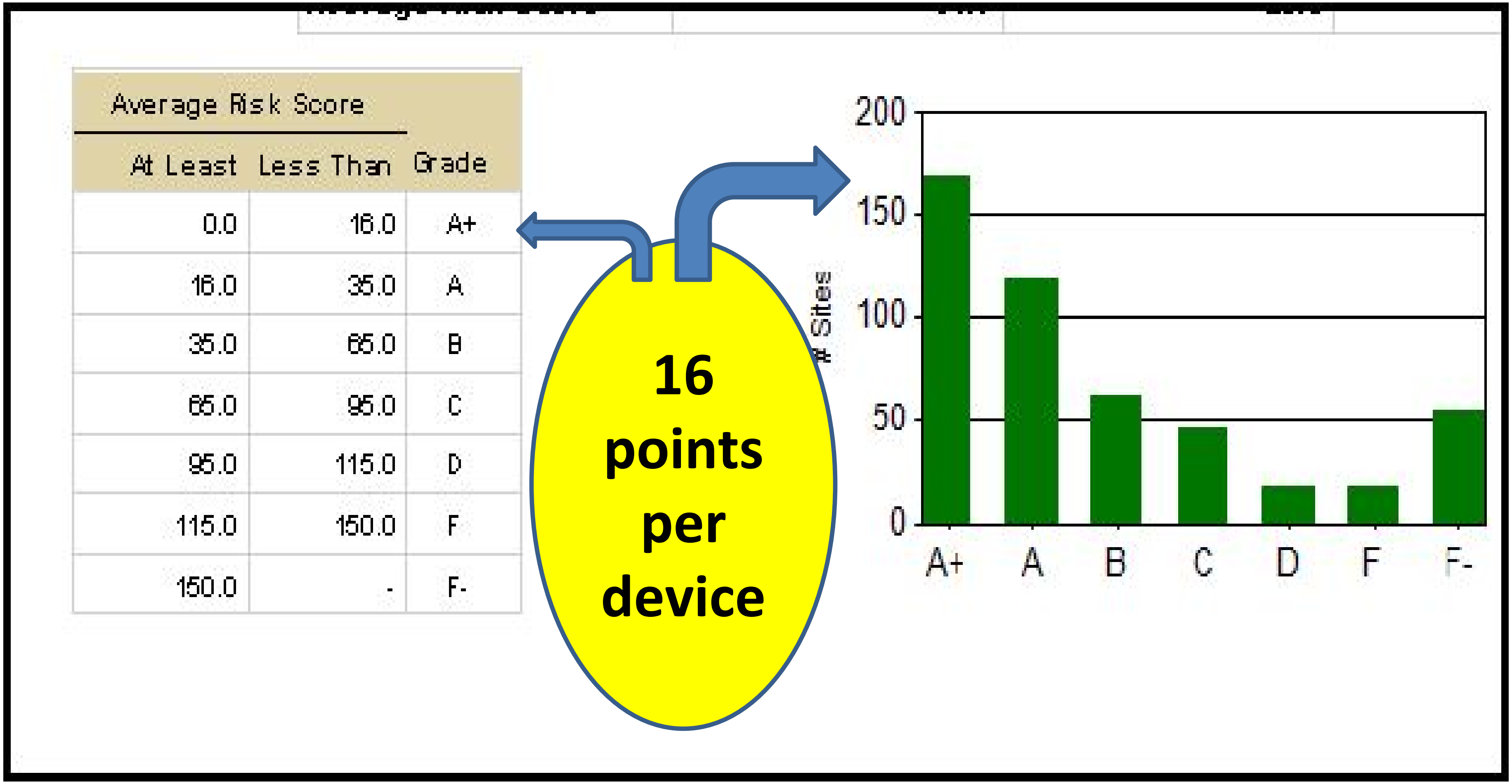
Objectives:

1. *Scan* every 36-72 hours
2. *Focus* on Attack Readiness
3. *Find* & Fix Top Issues Daily
4. *Personal* results graded
5. *Hold* managers responsible

Results First 12 Months



Status today



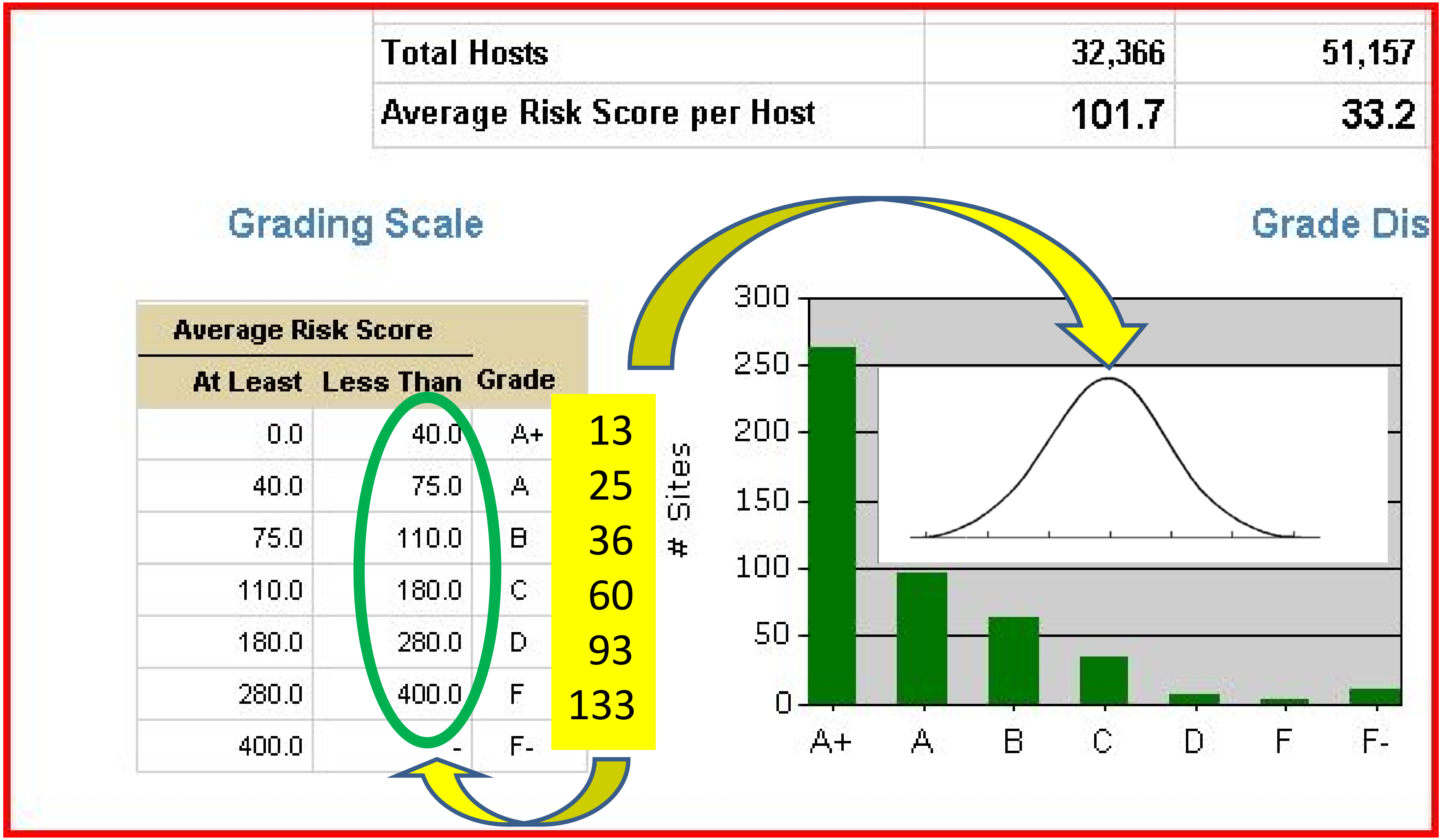
Average Risk Score		
At Least	Less Than	Grade
0.0	16.0	A+
16.0	35.0	A
35.0	65.0	B
65.0	95.0	C
95.0	115.0	D
115.0	150.0	F
150.0	-	F-

16 points per device

HOW ?

2nd Year by the Numbers

Risk Score Monitor Enterprise



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

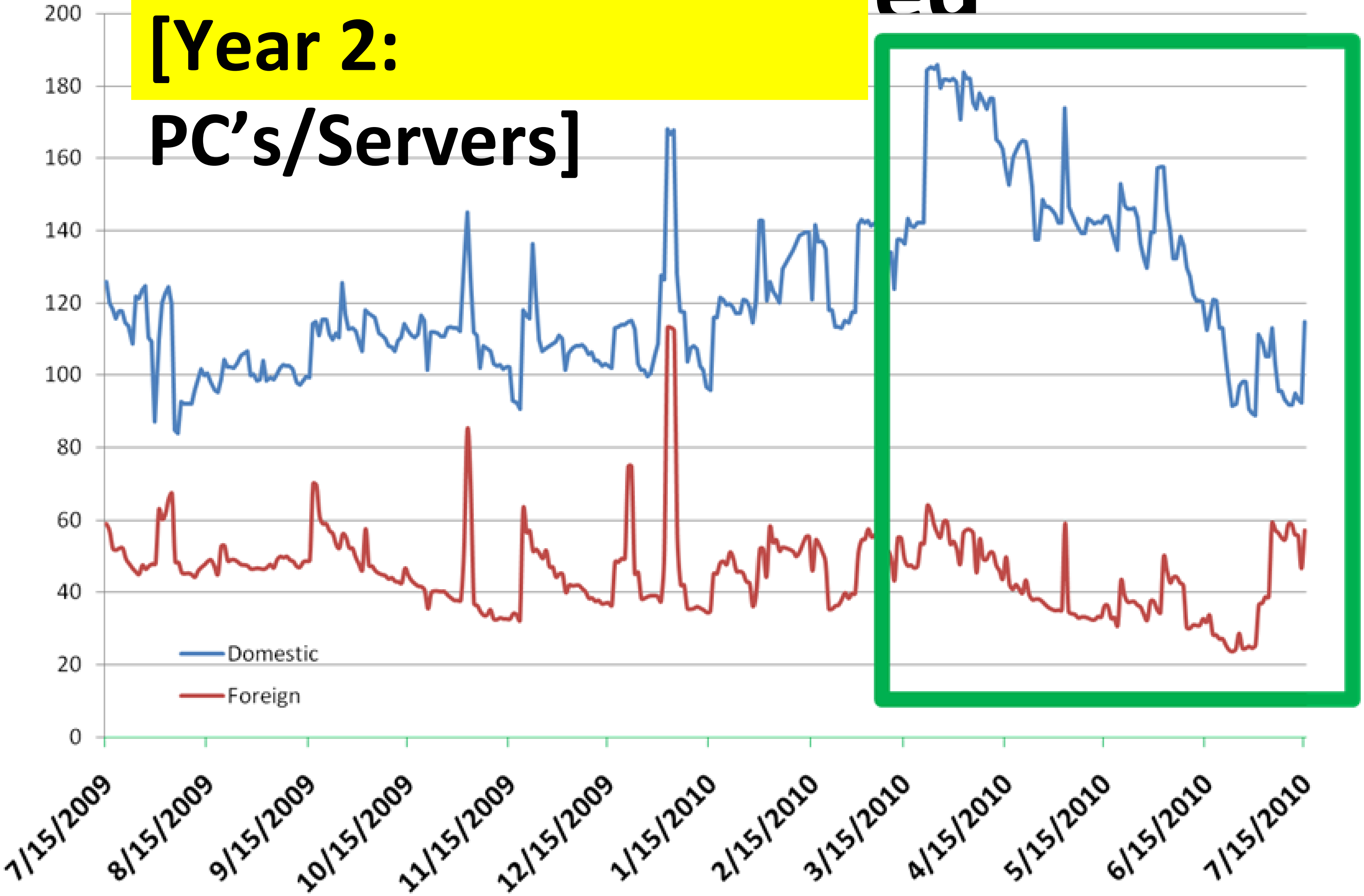
Grading Scale

Average Risk Score			
At Least	Less Than	Grade	
0.0	40.0	A+	13
40.0	75.0	A	25
75.0	110.0	B	36
110.0	180.0	C	60
180.0	280.0	D	93
280.0	400.0	F	133
400.0	-	F-	

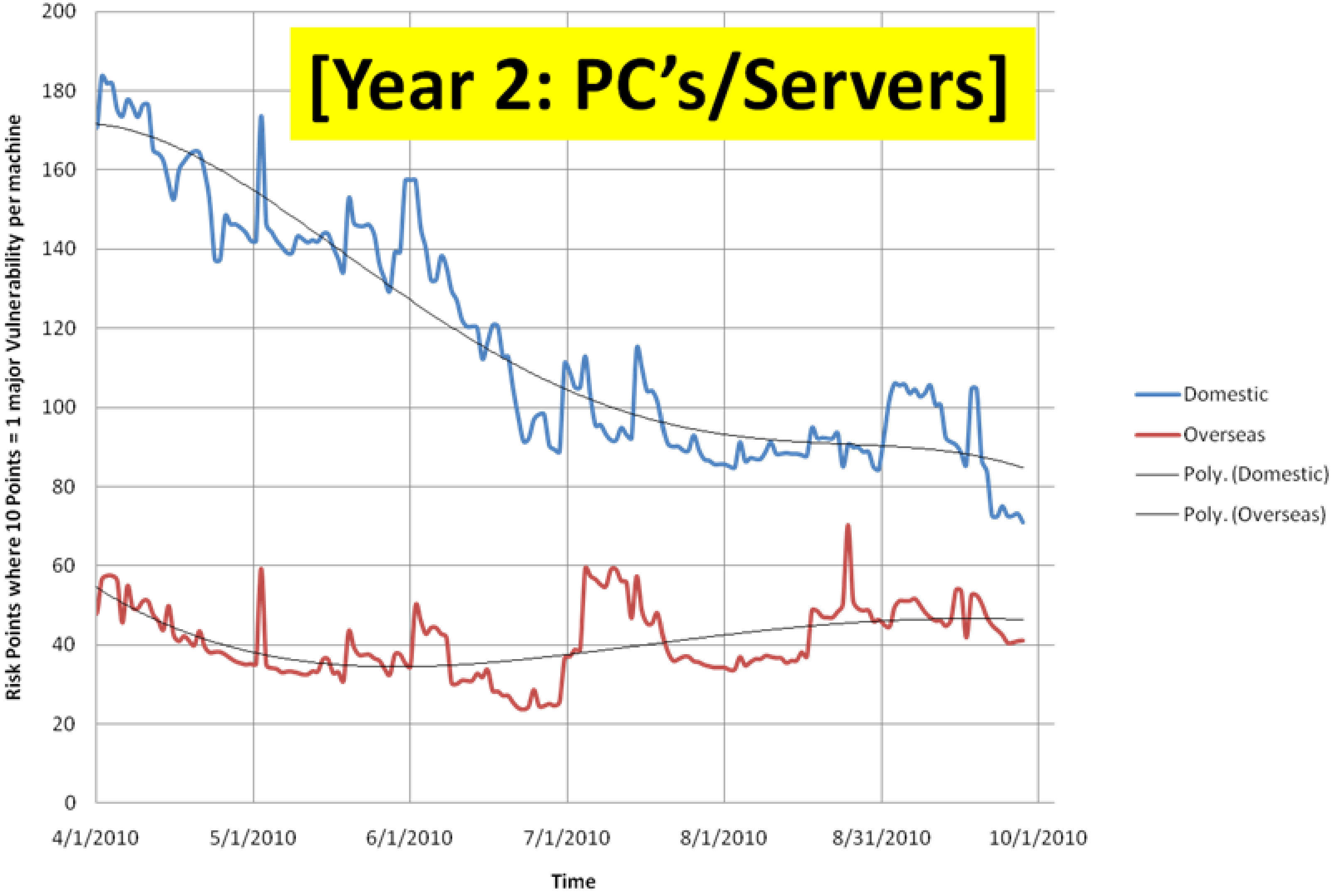
Grade Dis

1/3 of Remaining Risk Removed

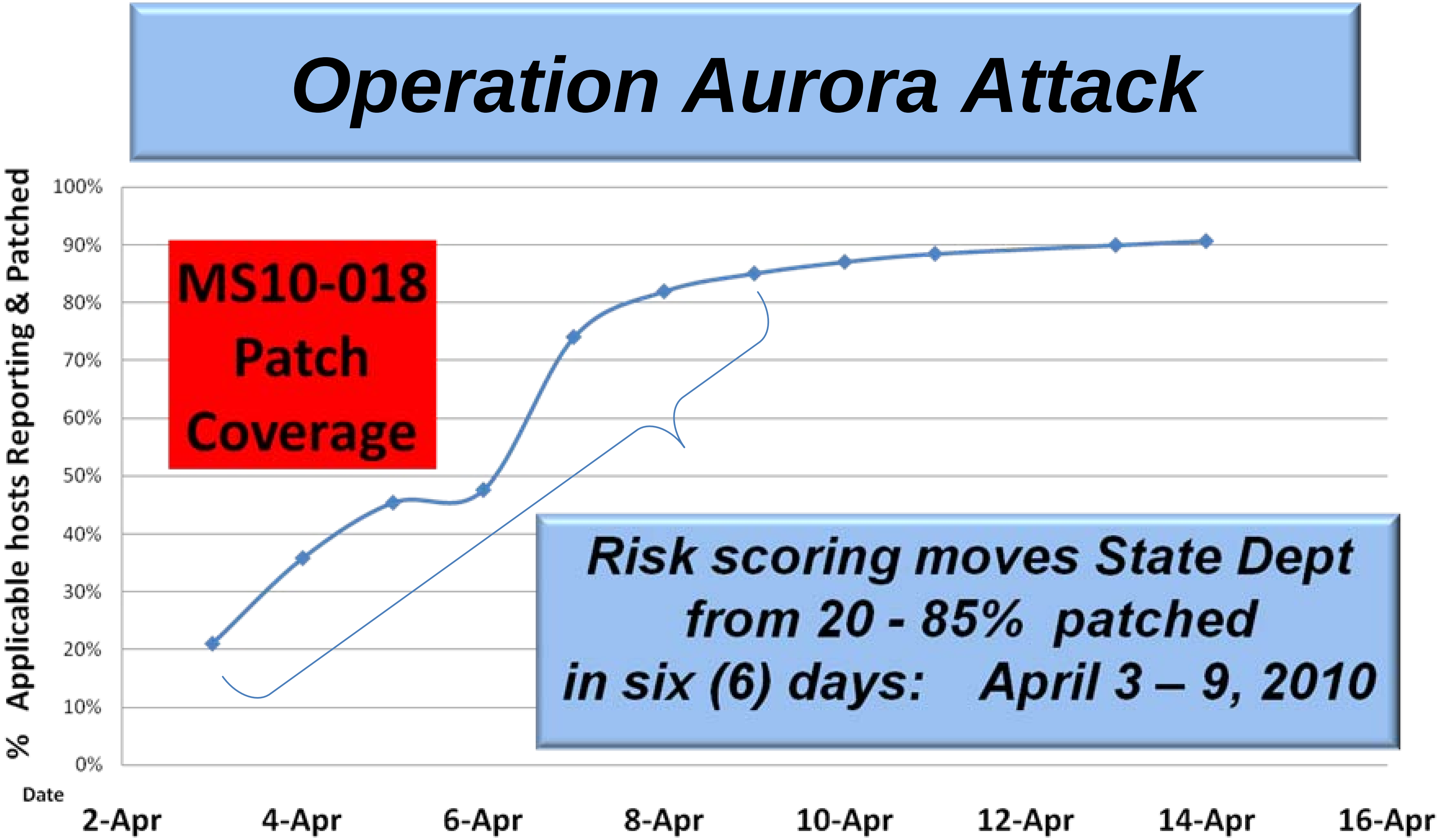
[Year 2: PC’s/Servers]



Grade	Now	April	May	June	July	Aug	Sep
A+	40	36	31	27	22	18	13

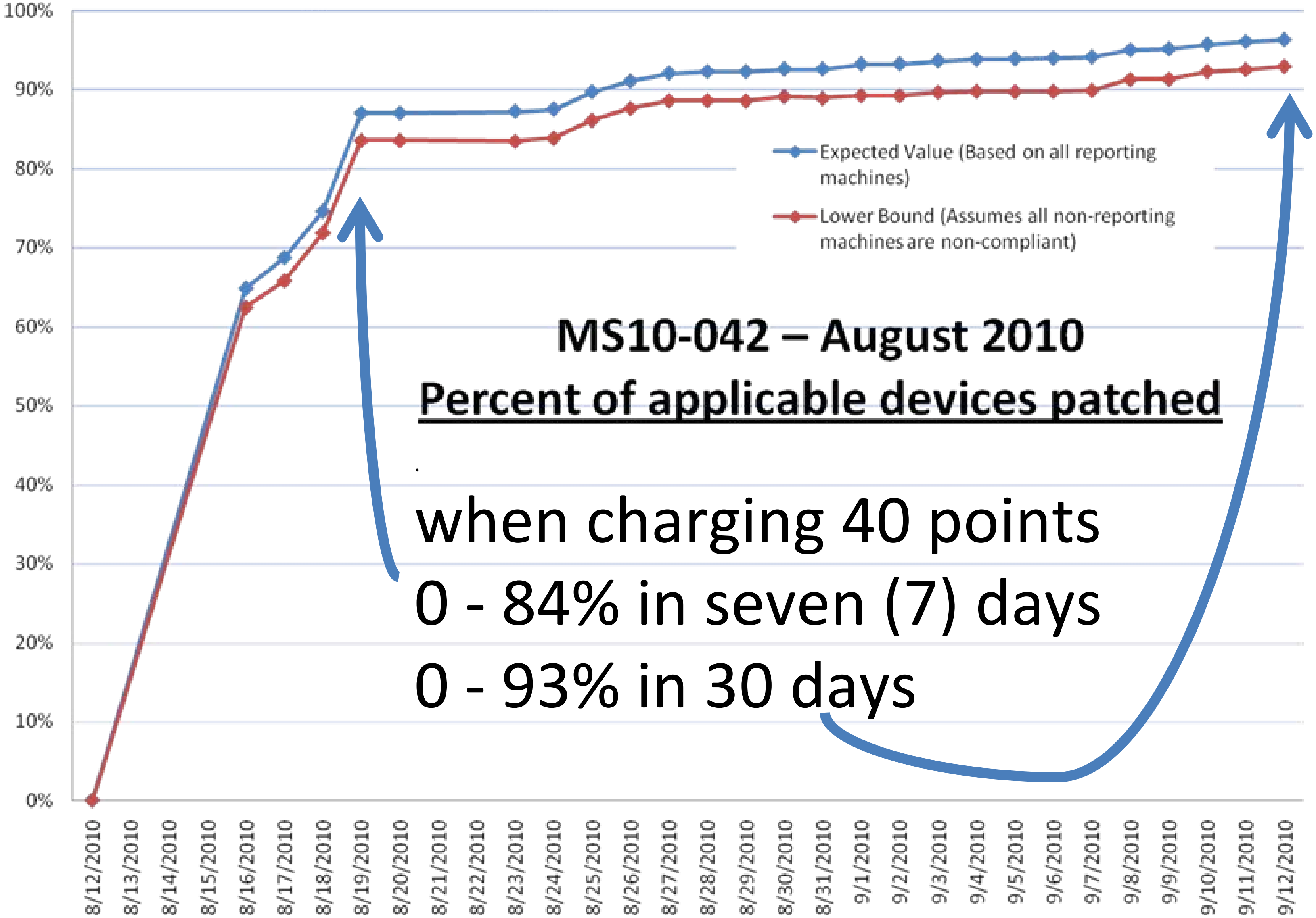


Call a Problem 40x Worse



Risk scoring moves State Dept from 20 - 85% patched in six (6) days: April 3 – 9, 2010

Efficiency is Repeatable & Sustained



MS10-042 – August 2010

Percent of applicable devices patched

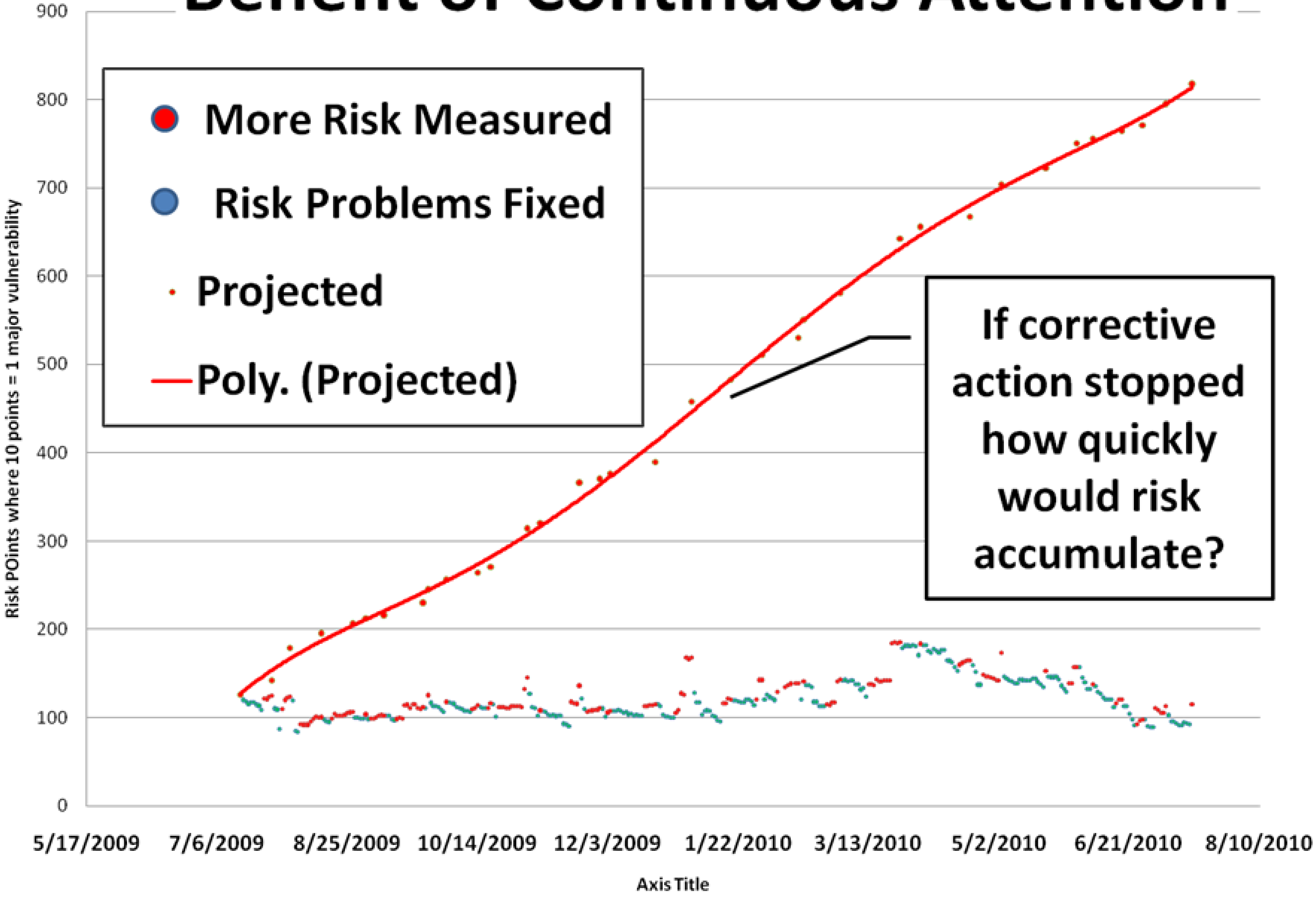
.

when charging 40 points

0 - 84% in seven (7) days

0 - 93% in 30 days

Benefit of Continuous Attention



If corrective action stopped how quickly would risk accumulate?

Brody’s Best 5

1. Know boundaries of the enterprise
2. Devices on the network
3. Configurations Settings

Are:

Checked every 36-72 hours (PC’s and Servers)

Assigned to 1 of 400+ teams for remediation

Patching coverage 0-84% in 7 days

Brody’s Best 5

4. Who is accessing the systems;
5. What those individuals are doing when accessing those systems

System users or incidents are:

- Recorded in logs and access control lists
- Continuously assessed for intrusions
- Watched for data exfiltration
- Penalized for violations
- Trained annually and tested daily for rules in 6 mo
- Monitored for elevated privileges (improved in 6 months)

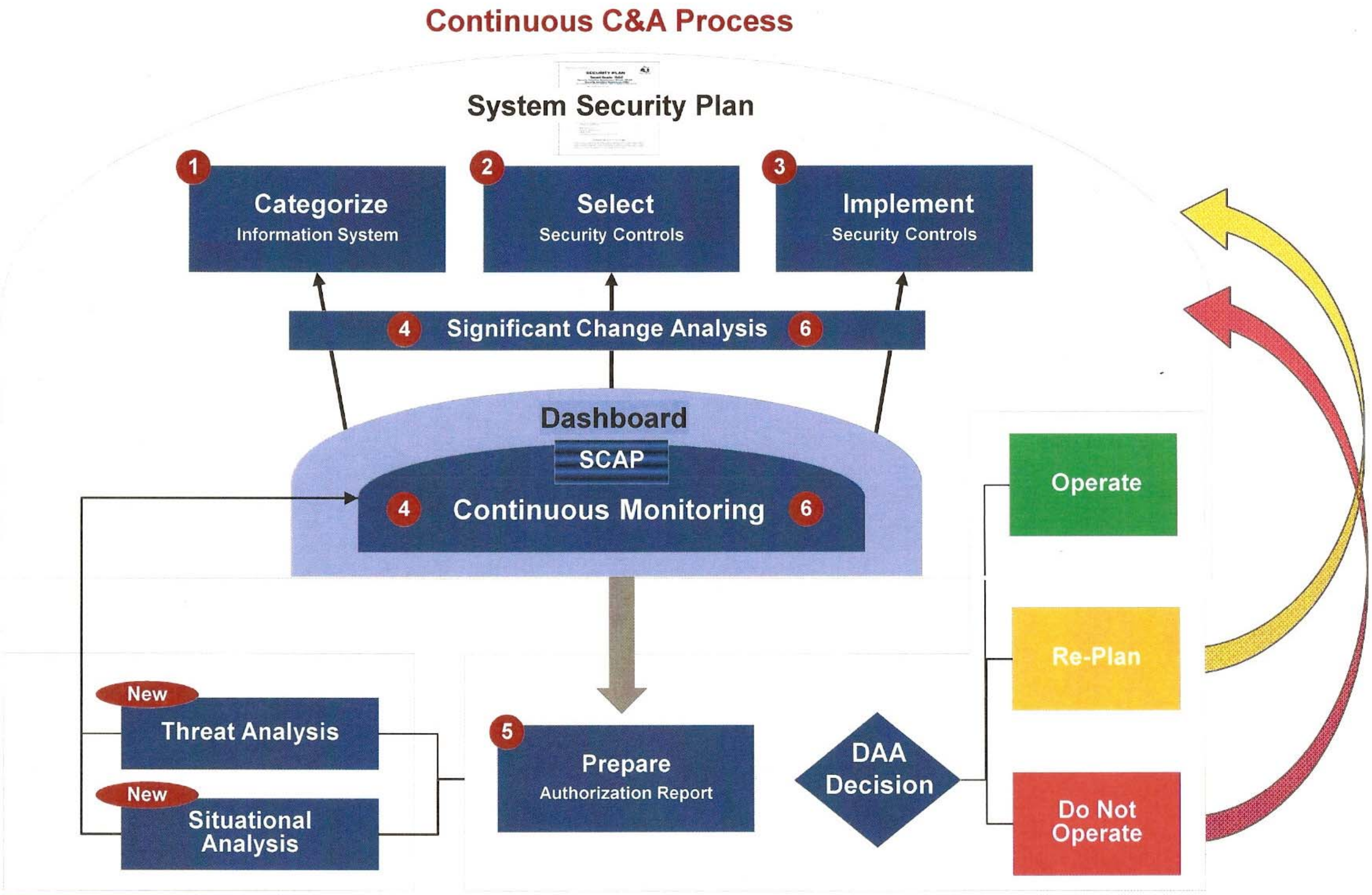
Insider threat

“The Department has continued to work on the deployment of an automated tool that will continuously monitor the classified network to detect anomalies that would not otherwise be apparent.”

20 Year old commercial said

"The quality goes in, before the name goes on"

Continuous C&A Process will provide more effective real-time security – not just a snapshot in time


Continuous C&A Process
System Security Plan
1 Categorize Information System
2 Select Security Controls
3 Implement Security Controls
4 Significant Change Analysis 6
Dashboard
SCAP
4 Continuous Monitoring 6
Operate
Re-Plan
Do Not Operate
New Threat Analysis
New Situational Analysis
5 Prepare Authorization Report
DAA Decision

Conclusions

- **Risk Scoring and Continuous Monitoring is scalable to large complex public and private sector organizations**
- **Higher ROI for continuous monitoring of technical controls as a substitute for paper reports**
- **Summarized risk estimates could be fed to enterprise level reporting**