Federal Continuous Monitoring Case Study: Department of State

Homeland Security

john.streufert@hq.dhs.gov

Director , National Cyber Security Division

Nature of Attacks

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

“Attack Readiness”

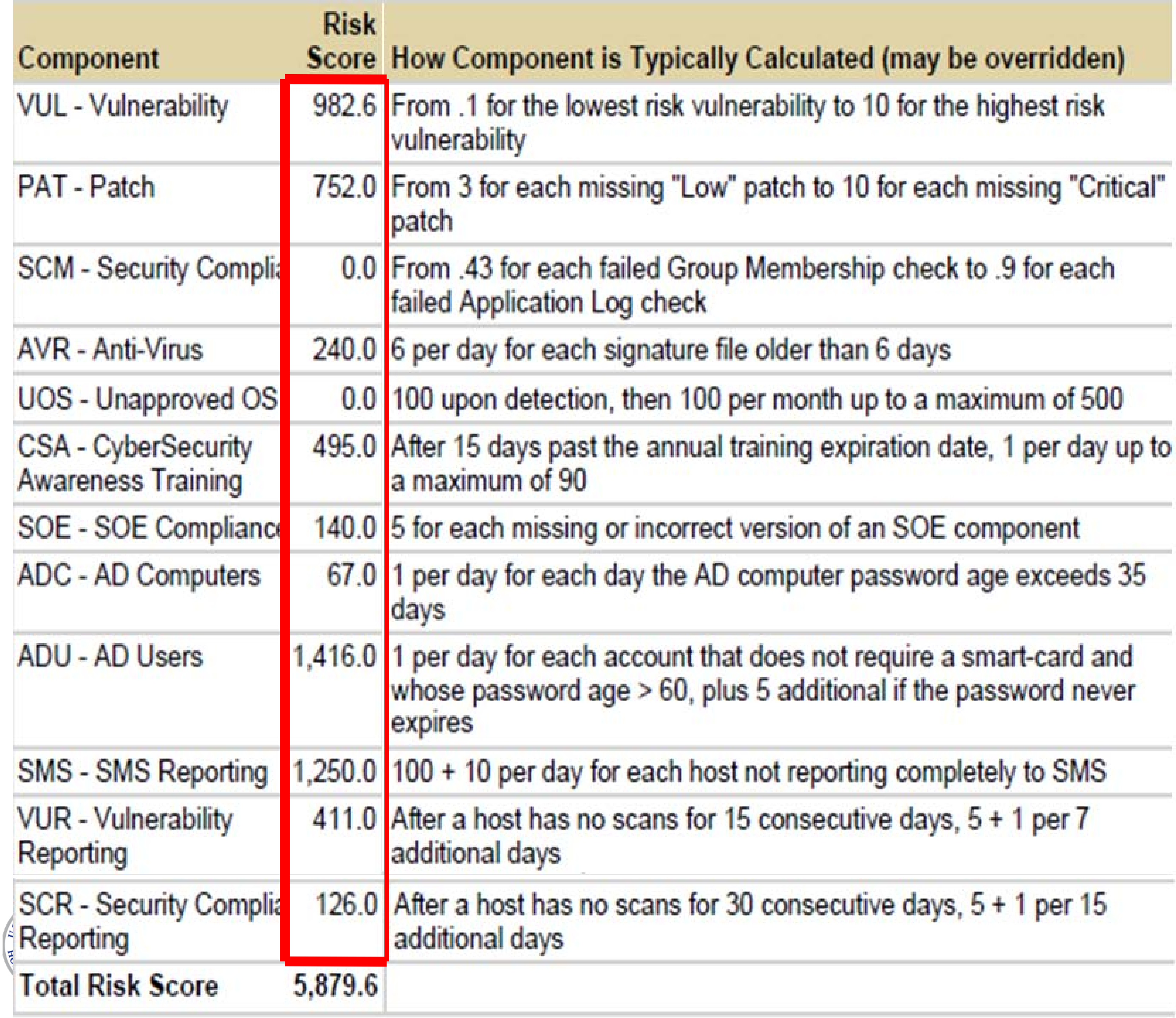
- What time is spent on
- Faster action =

  lower potential risk

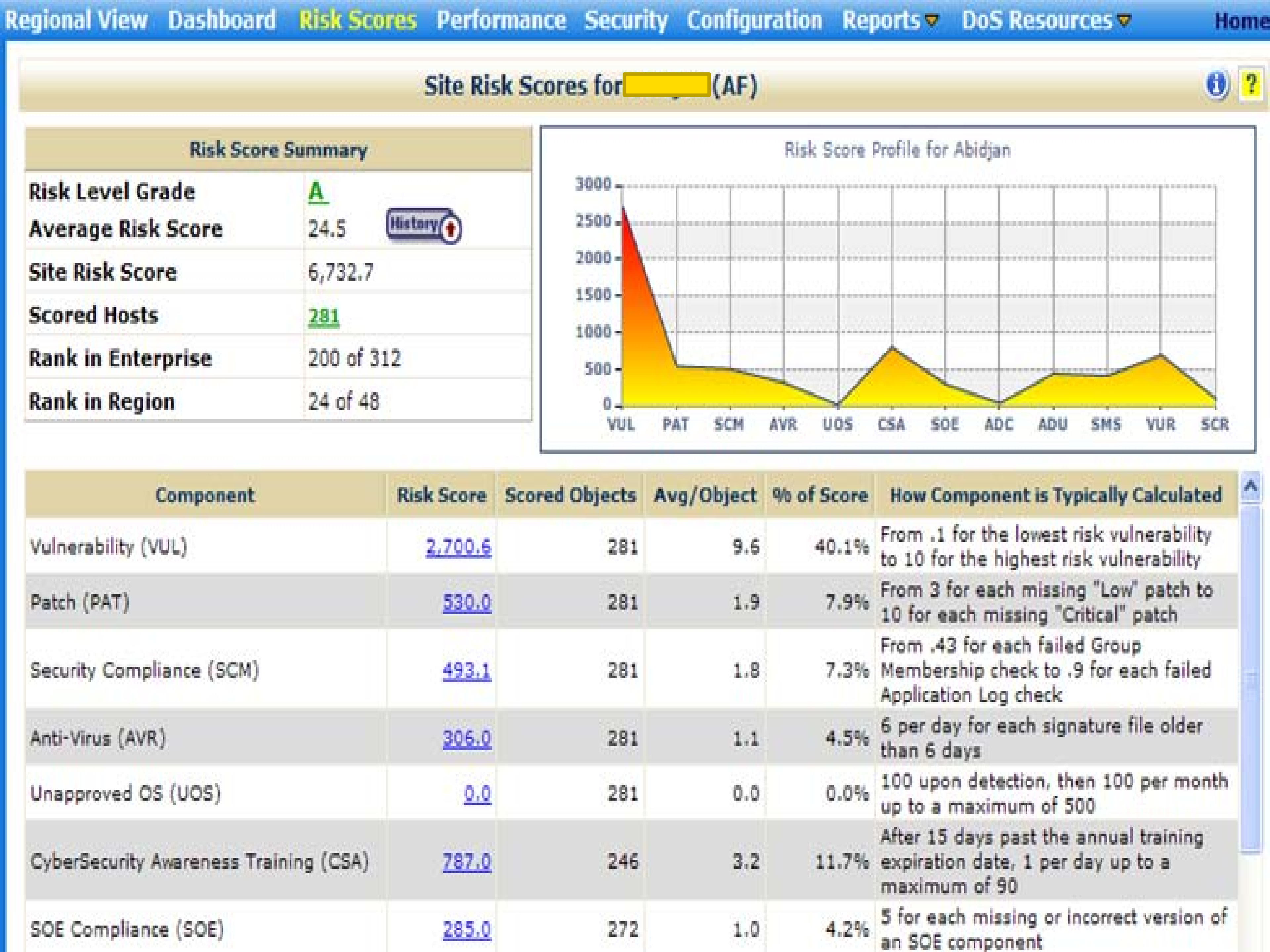
iPost creates 24 hour trading for ***risk market*** decisions.

The dashboard shows what are the hottest risks in local markets:

- organizations,
- systems,
- companies maintaining our systems;



Component	Risk Score	How Component is Typically Calculated (may be overridden)
VUL - Vulnerability	982.6	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
PAT - Patch	752.0	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
SCM - Security Complia	0.0	From .43 for each failed Group Membership check to .9 for each failed Application Log check
AVR - Anti-Virus	240.0	6 per day for each signature file older than 6 days
UOS - Unapproved OS	0.0	100 upon detection, then 100 per month up to a maximum of 500
CSA - CyberSecurity Awareness Training	495.0	After 15 days past the annual training expiration date, 1 per day up to a maximum of 90
SOE - SOE Complianc	140.0	5 for each missing or incorrect version of an SOE component
ADC - AD Computers	67.0	1 per day for each day the AD computer password age exceeds 35 days
ADU - AD Users	1,416.0	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	1,250.0	100 + 10 per day for each host not reporting completely to SMS
VUR - Vulnerability Reporting	411.0	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days
SCR - Security Complia Reporting	126.0	After a host has no scans for 30 consecutive days, 5 + 1 per 15 additional days
Total Risk Score	**5,879.6**	



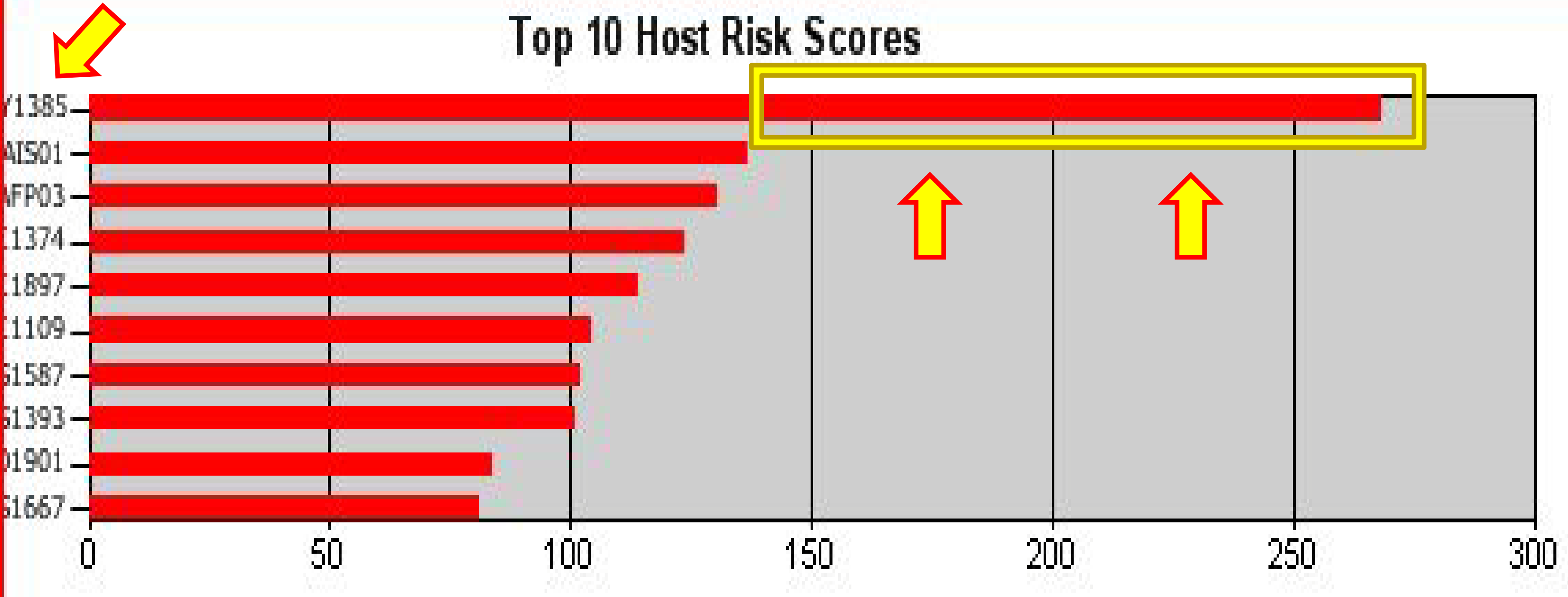
Site Risk Scores for [redacted] (AF)

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

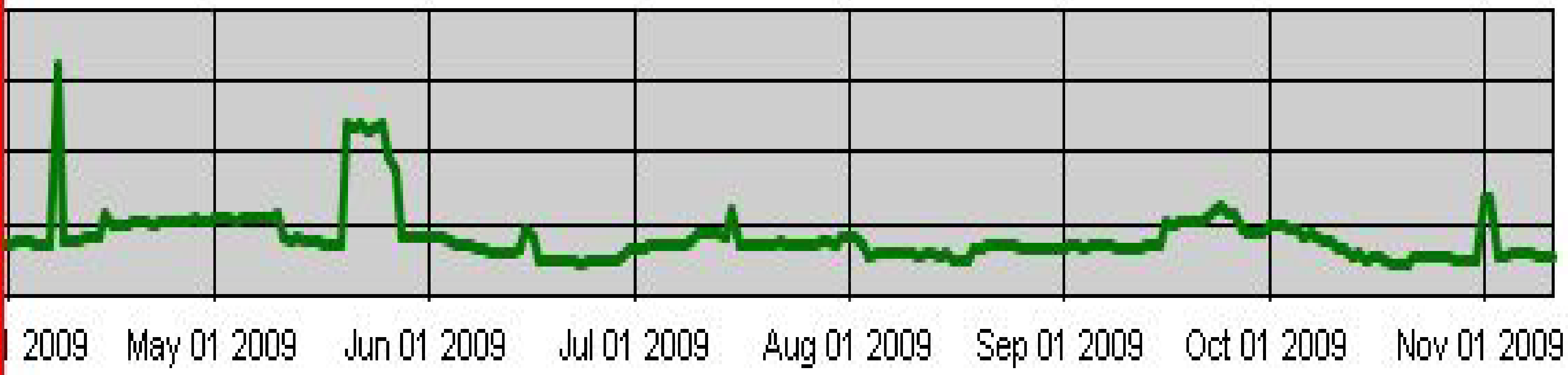
Risk Score Profile for Abidjan

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

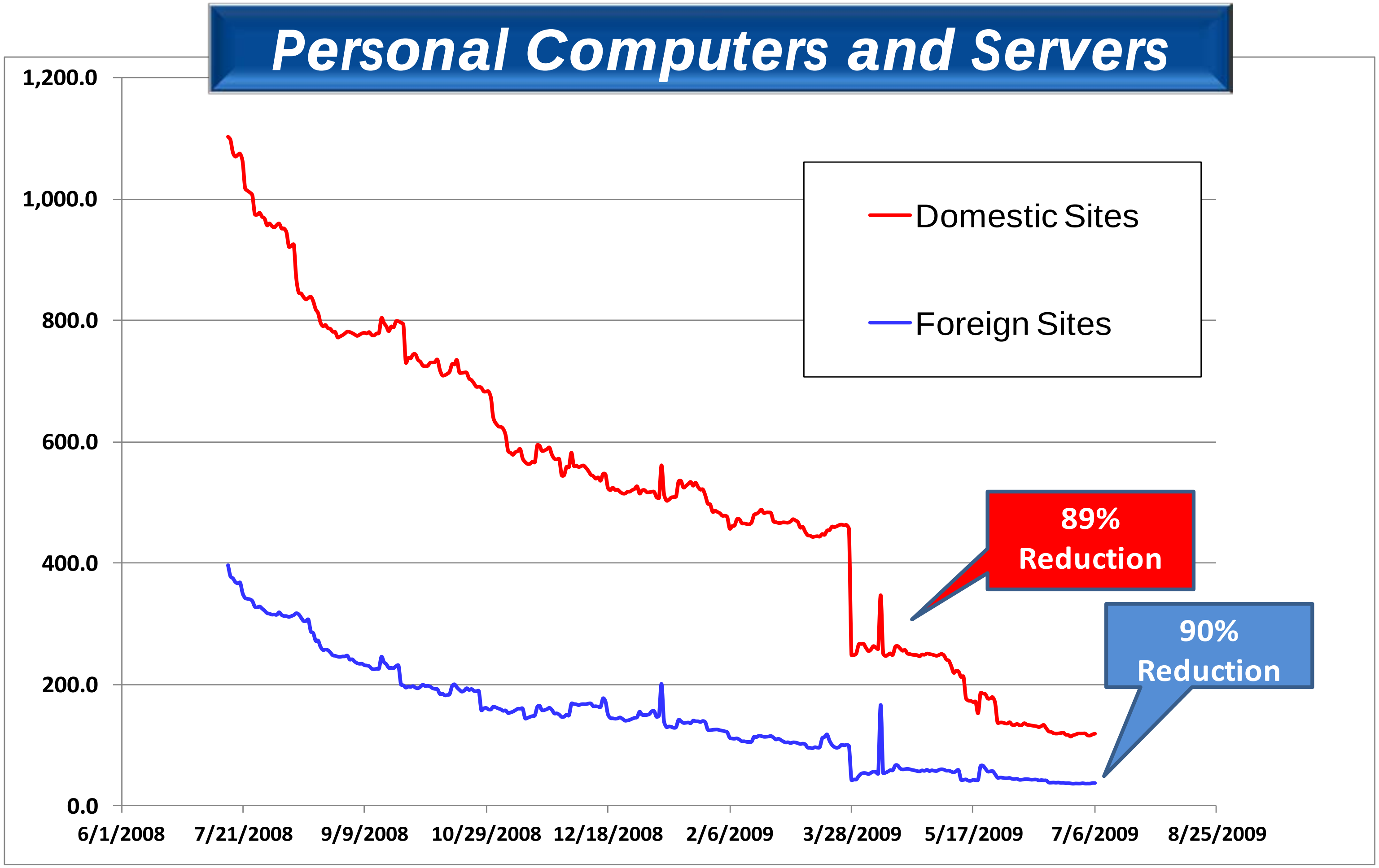
Top 10 Host Risk Scores



Risk Score History

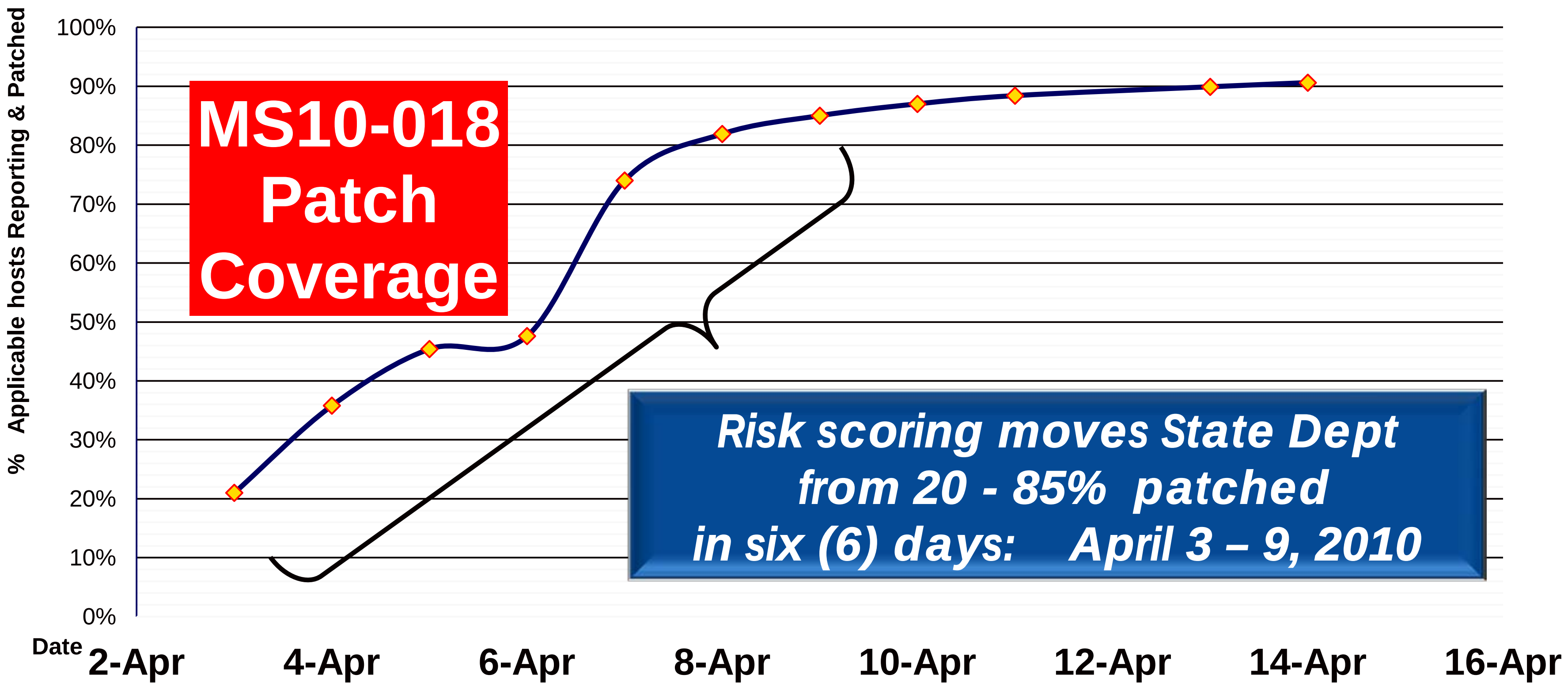


Results First 12 Months



Call a Problem 40x Worse

Operation Aurora Attack

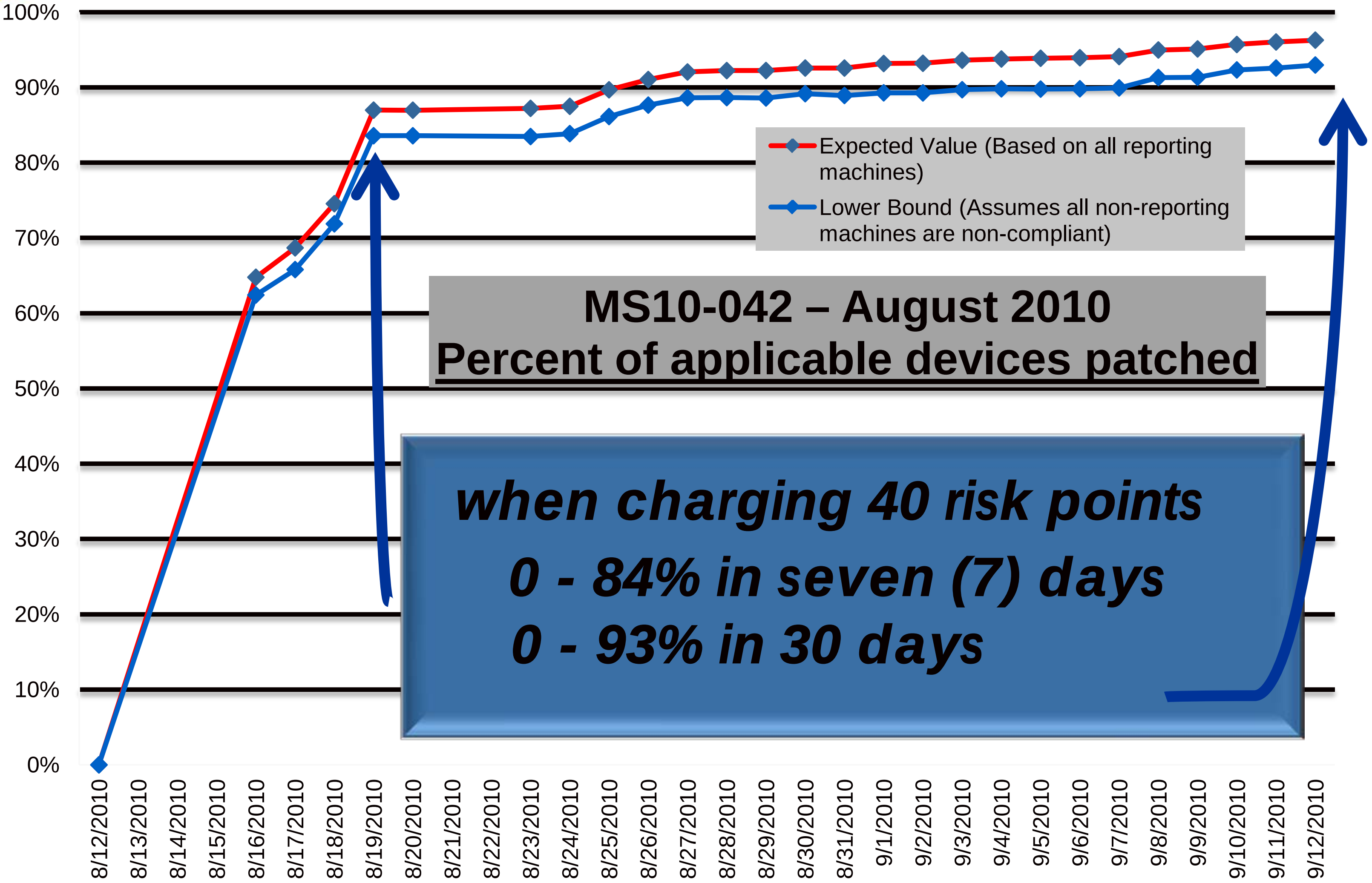


MS10-018 Patch Coverage

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

Homeland Security

Efficiency is Repeatable & Sustained



MS10-042 – August 2010

Percent of applicable devices patched

when charging 40 risk points

0 - 84% in seven (7) days

0 - 93% in 30 days

Homeland Security

Intrusion Detection – What and How

Incident Management – Who and Where

Risk Scoring Targeted Remediation

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland
Security