



Problem Statement

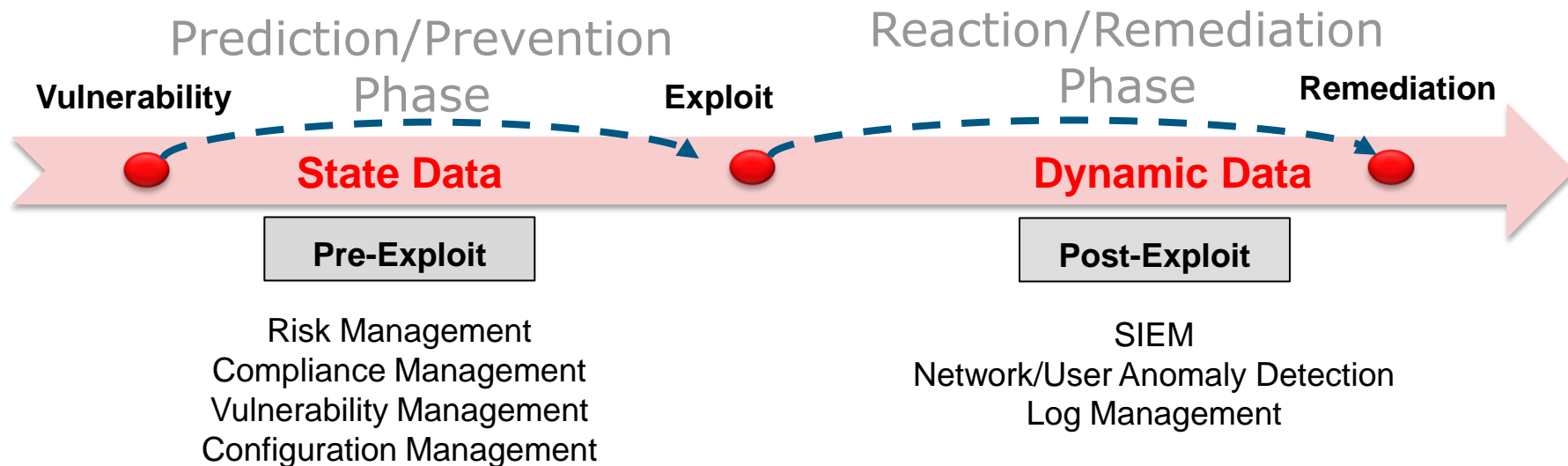
- Organizations are being targeted and threatened by sophisticated, automated and coordinated attacks (APT)
- Traditional efforts to address these cybersecurity threats and challenges have been narrow approaches with bolted-on technologies resulting in numerous pointed solutions .
- Getting complete, real-time security data gathered across the entire security spectrum: from vulnerability, to exploit, to threat intelligence is a major challenge
- Traditional security efforts are no longer effective. Desperate set of controls, vast volumes of data and information does not provide a clear actionable remediation

Cyber Situational Awareness

Situational Awareness is the ability to identify, process, monitor and report the critical elements of security across the entire security spectrum: from vulnerability, to exploit, to remediation

More simply, know what's coming, and be ready when it gets here

Cyber Situational Awareness



CSC Horizon (based on RSA Archer)

Situational Awareness dashboard that provides a holistic, near real-time status on your security posture.

- Knowing what is going on around you
 - Threat posture
 - Vulnerability posture
 - Compliance posture
 - Incidents
- Understand what normal is
 - Benchmarking/Baselining
- Know what (and who) your threats are
 - External intelligence feeds
 - Internal trend analysis
- Mature service that is available today
- Extension to our existing lines of service
- Empowers Analysts to focus on what is important and allow Executives to make quick, informed decisions
- Live demo available

The image shows a screenshot of a security dashboard grid. A red rectangular border highlights a central section of the grid. Within this section, a yellow rectangular highlight is placed over a tile labeled 'CSC Horizon'. The grid contains various security services categorized by color-coded headers.

	MANAGED SECURITY			
	CSC Enhance	CSC Extend	CSC Elevate	
Security Incident	Audit Log Assurance	SIEM	Data Loss Prevention	Business Assets
Assurance	Managed End Point	File Integrity Monitoring	Db Activity Monitoring	Im
Security App	Managed Vulnerability Scanning	Firewall Ruleset Assurance	Application FW	R
ing and Labs	Network IPS/ IDS	Managed Encryption Service	Password Storage	Business Plann
Incident Response	Dashboard Pulse	Technology Compliance	Advanced Threat Detection	Crisi
Education	Cloud MEP	Application Pentest	GRC	Disa Plann
Security	Cloud MVA	Managed Authentication Service	Global Threat Detection	BC
Force Multipliers	Cloud FIM	CSC Horizon	Cyber Analytics	
	Cloud vFW	Secure Mobility		
		Cloud Encryption		

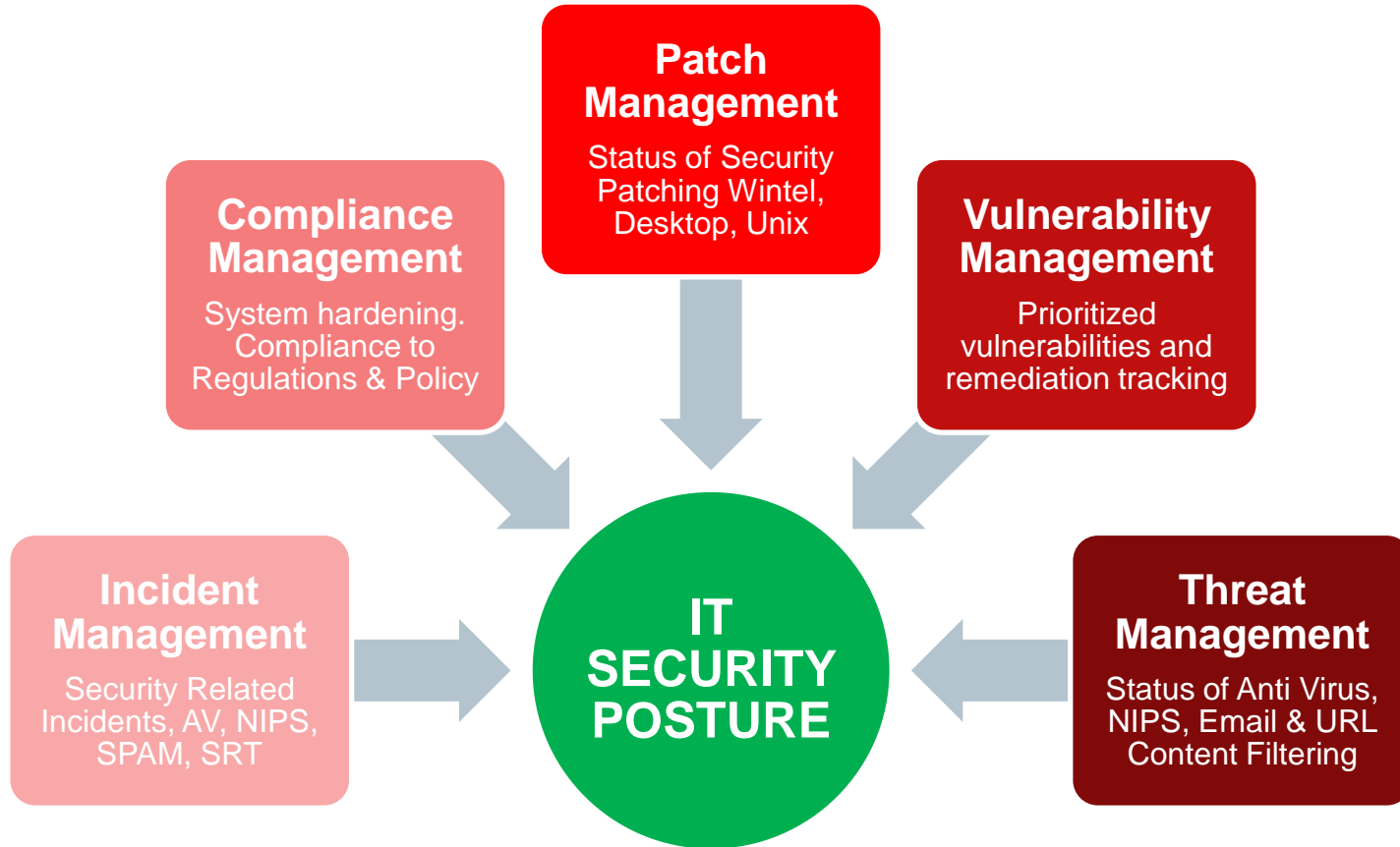
CSC Horizon at a Glance

- **Near Real-time data:** Enterprise dashboard integrates data from existing security controls into one easy-to-understand dashboard view
- **Highly customizable:** Allows you to customize your dashboard for specific job titles and roles
 - Executive Management, CISO, SOC Analysts, Auditors, etc.
- **Drill-down:** Start with a bird's eye view of your data, and drill down to the smallest of details
- **Perfect for Traditional & Cloud IT:** Works with traditional and CSC Trusted Cloud IT infrastructure
- **Non Intrusive** No infrastructure changes needed

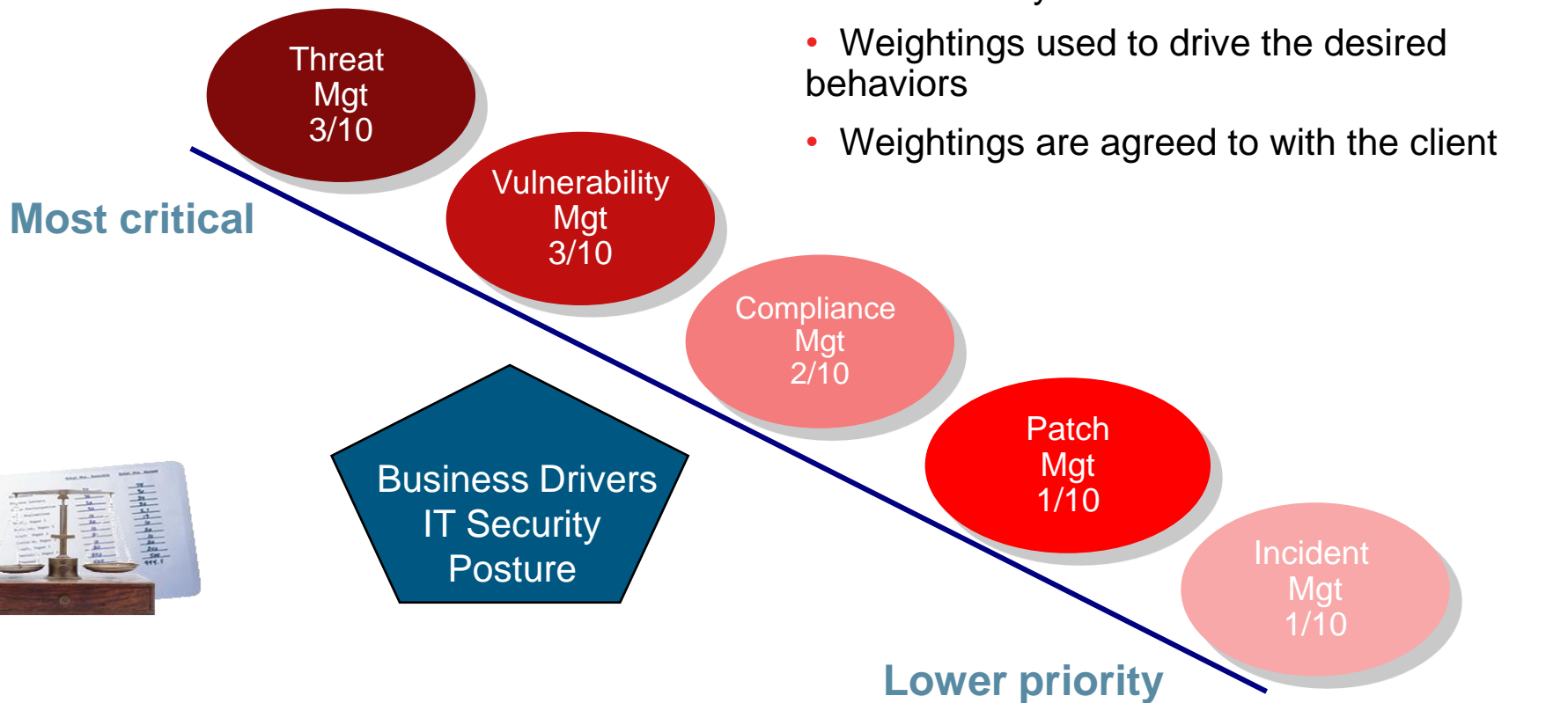
Security Category	Category Score	Target Category Score	Risk Rating - by Category	Category Weighting	Security Score and Risk Rating	Agreed Target
Threat Management	71	75	High	4	67 High	79 High
Vulnerability Management	84	75	Medium	3		
Compliance Management	78	60	High	1		
Incident Management	20	100	Extreme	1		
Change Management	40	100	Extreme	1		



HORIZON - Captures “IT controls based evidence”, security information, events, metric across security domains providing a holistic view of security and risk posture.



CSC HORIZON

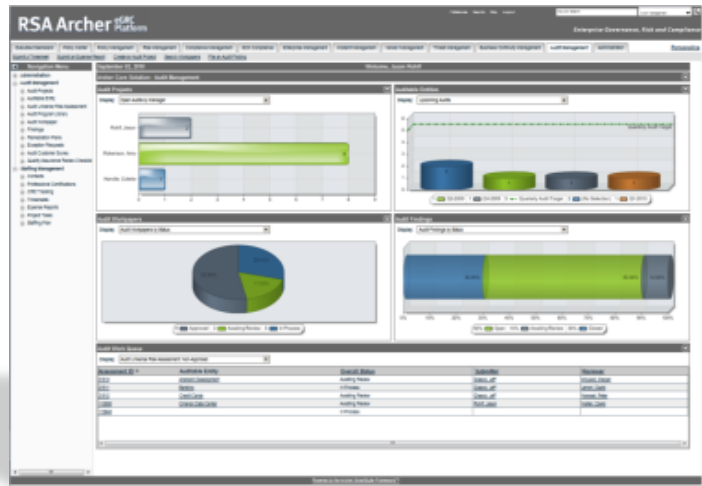


HORIZON - Technology Considerations

- Non-intrusive
- Technology agnostic
- Unique controls can be managed via custom connectors/scripts



- Compliance tools
- Antivirus
- Vulnerability Scanners
- Application Scanners
- Patch Management
- Databases CMDB's
- DLP
- Security Event and Information Management
- Applications *
- Business Process data *



* - HORIZONⁿ specific (GRC profile)

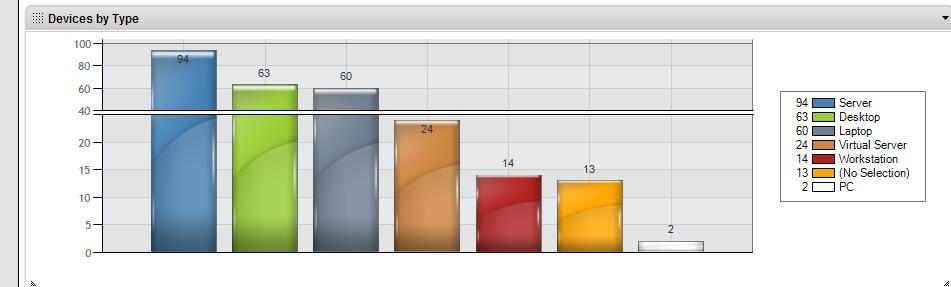
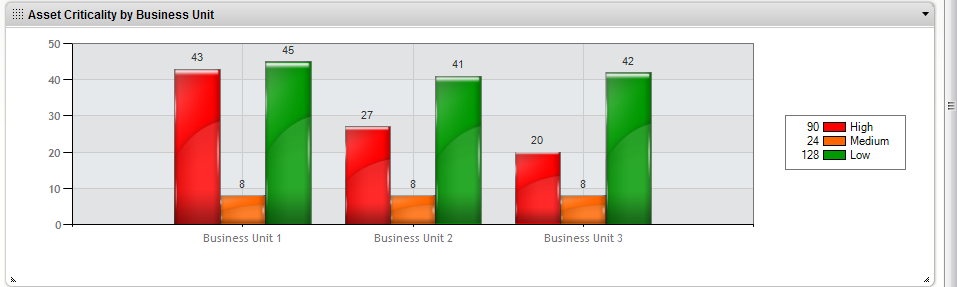
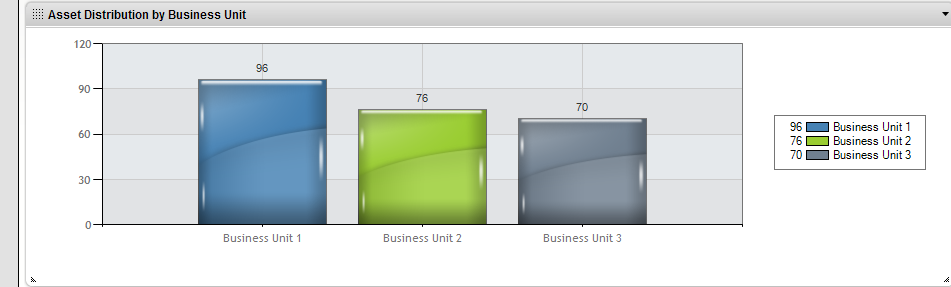
Customer Enterprise Security Status

Customer ▲	Overall Risk Rating	Vulnerability Scan Risk Rating	Threat Management Risk Rating	Configuration Risk Rating	Incident Risk Rating
Company A					
Company B					
Company C					
Company D					
Company E					

Business Unit Risk Ratings

Business Unit	Overall Risk Rating	Vulnerability Scan Risk Rating	Endpoint Protection Risk Rating	Patch Risk Rating	Configuration Risk Rating	Incident Risk Rating
Business Unit 1						
Business Unit 2						
Business Unit 3						

Page 1 of 1 (3 records)



Operating Systems Found

Operating System	Count of Operating System
Windows 7	53
Windows XP	45
Windows 2003 R2	37
Mac	21
Windows Vista	20
Windows Server 2008 R2	15
Windows Server 2008	14
Windows Server 2003	13

Critical Systems at High Overall Risk

Device Name	Criticality	Overall Risk Rating
USCWdms01	High	

New Devices in the Last 30 Days

No Records Found

Dashboard: Vulnerability Management

Welcome, James Byroads

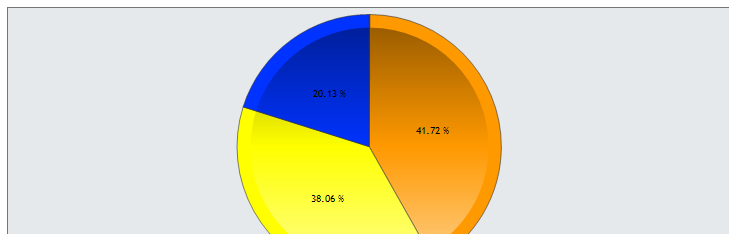
Options

CSC Top 10 Vulnerabilities

Scan ID	Device Name	Title	Severity	CVSS Base Score	Exploit Available	Criticality
Scan-12144	USCWapp05	MS09-071: Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)		8.3	Yes	
Scan-09278	testdevice1	BMC SNMP Agent Default Community Name (public)		7.5	Yes	
Scan-12140	USCWweb01	MS09-009: Vulnerabilities in Microsoft Office Excel Could Cause Remote Code Execution (968557)		6.8	Yes	
Scan-12139	USCWweb01	MS10-080: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)		6.8	Yes	
Scan-12138	USCWweb01	MS10-080: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)		6.8	Yes	
Scan-09398	testdevice1	MS10-080: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)		6.8	Yes	
Scan-09397	testdevice1	MS11-021: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2489279)		6.8	Yes	
Scan-09396	testdevice1	MS08-043: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (954066)		6.8	Yes	
Scan-09395	testdevice1	MS09-009: Vulnerabilities in Microsoft Office Excel Could Cause Remote Code Execution (968557)		6.8	Yes	
Scan-09394	testdevice1	Microsoft Office Service Pack Out of Date		6.8	Yes	

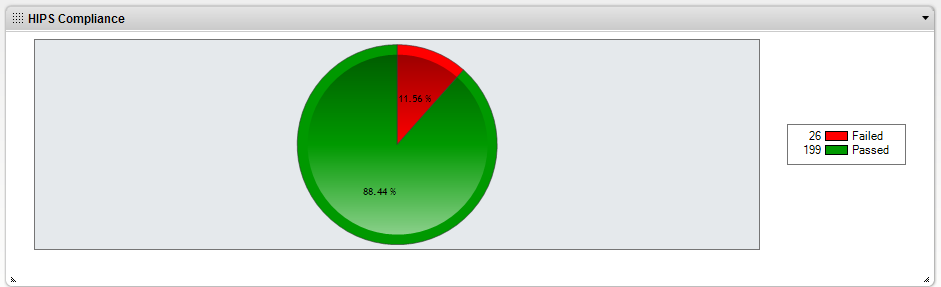
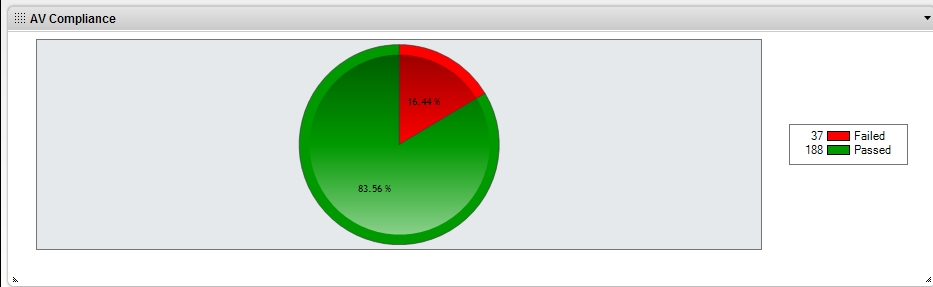
Page 1 of 1 (10 records)

Total Number of Vulnerabilities by Severity



Critical Systems at High Vulnerability Risk

Device Name	Criticality	Vulnerability Scan Risk Rating
uscwarcherwebap		
USCWftp04		
USCWdns02		
USCWweb01		
USCWftp05		
USCWweb08		
USCWfile06		



Critical Devices Failing AV Compliance

Device Name	Criticality	Type	AV Compliance
AJUGSSTS01	High	Server	Failed
AJUSNAS01	High	Server	Failed
AJUSRTRDHCP	High	Server	Failed
AJUSVCENTER	High	Server	Failed
DLPDEMODISCOVER	High	Server	Failed

Critical Devices Failing HIPS Compliance

Device Name	Criticality	Type	HIPS Compliance
AJUGSSTS01	High	Server	Failed
DLPDEMODISCOVER	High	Server	Failed
DLPDEMOMONITOR	High	Server	Failed
ENFORCEDEMO	High	Server	Failed
EPOAGENTHANDLER	High	Server	Failed

AV Top 10 Events

Subject	Count
Backdoor.Sykipotgen3	31
Backdoor.Breut	26
Infostealer.Shizlgen	22
Trojan.Activehijack	20
Backdoor.Cybotlgen10	17
W32.Pilleuzlgen31	16
W32.Waledac.C	11
Trojan.Zbotlgen30	9
W32.Begmian	7
Infostealer.Offsupload	7

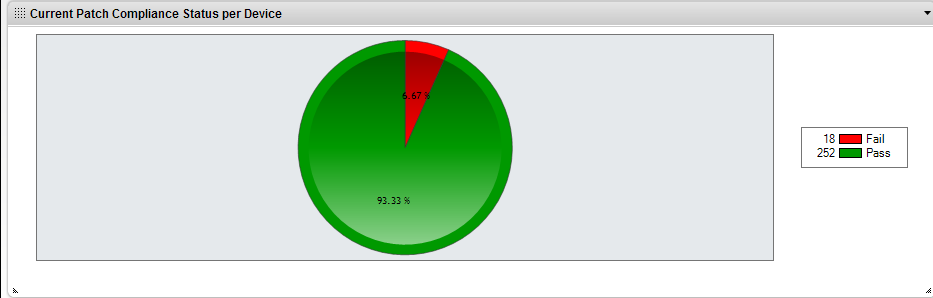
Page 1 of 1 (10 records)

HIPS Top 10 Events

Subject	Count
CMD Tool Access by a Network Aware Application	23,999
New Startup Program Creation	40
IIS6 Shielding - File Modification	30
MSSQL SQL Shutdown	20
Suspicious Function Invocation - Target Address Mismatch	16
Uninstall Registry Key Modification	15
MSSQL Core Envelope - File Execution by MSSQL	14
Event Log Registry Setting Modified	13
Adobe Reader Plug-in Cross-Site Scripting Vulnerability	10
MSSQL Aux. Envelope - File Execution by MSSQL	9

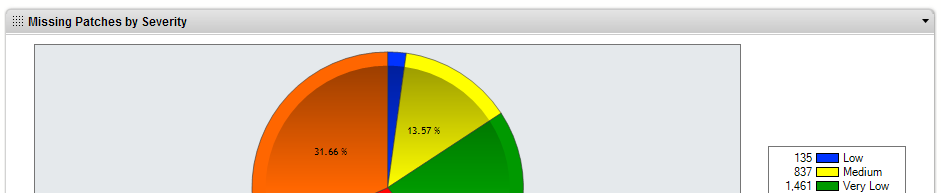
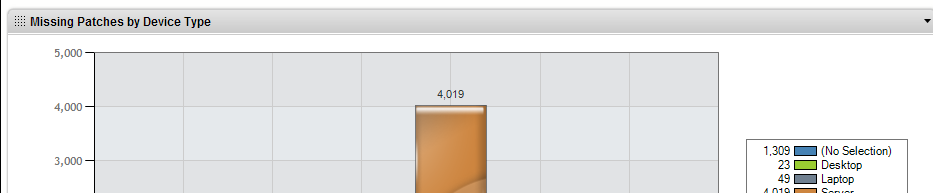
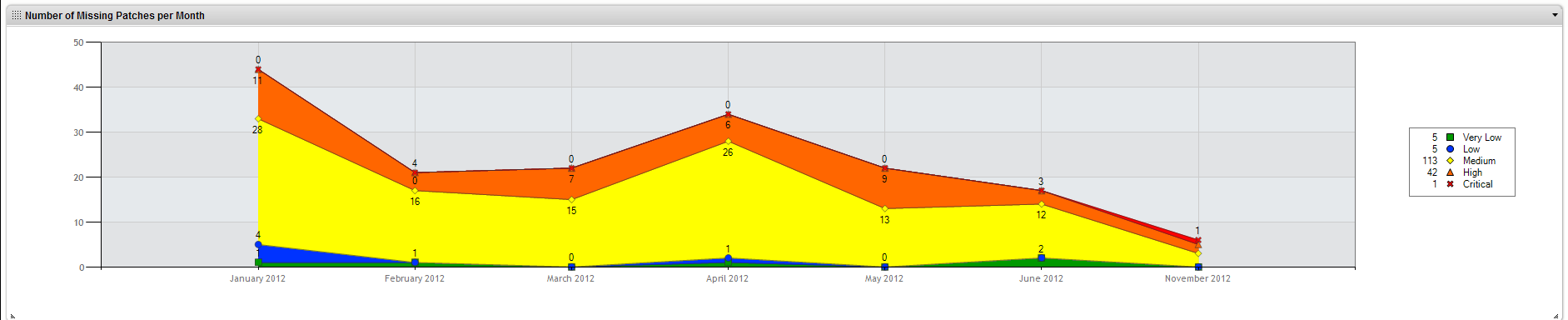
Page 1 of 1 (10 records)

Click to Expand the Navigation Menu



Critical Systems at High Patch Risk

Device Name	Criticality	Patch Risk Rating
USCWdns01	High	Very Low
AJUSVCENTER	High	Very Low
GPSMFSSVR	High	Very Low
AJUSNAS01	High	Very Low
USCWdb01	High	Very Low
uscwweb02	High	Very Low
USAJMVA1	High	Very Low



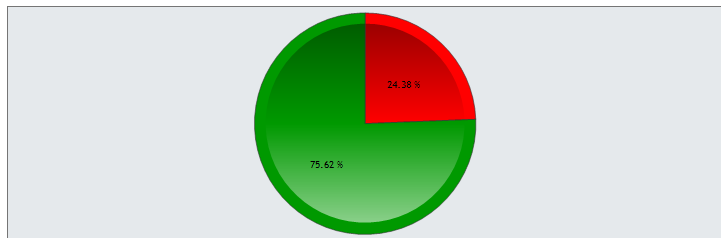
Click to Expand the Navigation Menu

Dashboard: Configuration Management

Welcome, James Byroads

Options

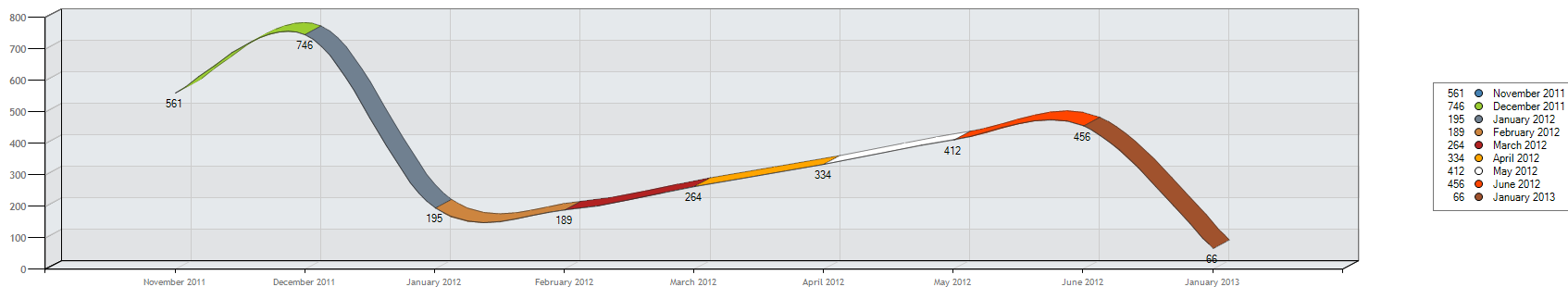
Configuration Check Results



Critical Systems at High Configuration Risk

Device Name	Criticality	Configuration Risk Rating
USCWdb02	High	High Risk
uscwarcherwebap	High	High Risk
USAJEPO45	High	High Risk
USCWfile04	High	High Risk
USCWapp01	High	High Risk
AJUSARCHER	High	High Risk
USCWftp01	High	High Risk
USC...	High	High Risk

Number of Failed Configuration Checks per Month



Top 10 Failed Configuration Checks

Configuration Check	Count of Test Result
Client Settings: Redirection: Drive	104
Client Settings: Redirection: Windows Printer	91
Interactive logon: Message title for users attempting to logon	91
Interactive logon: Number of previous logons to cache	91

Failed Configuration Checks for Critical Devices

Scan ID	Device	Configuration Check	Result	Criticality
Scan ID -244716	AJUSARCHER	Password must meet complexity requirement	Failed	High
Scan ID -244720	AJUSARCHER	Enforce Password History	Failed	High
Scan ID -244722	AJUSARCHER	Account Lockout Threshold	Failed	High
Scan ID -244724	AJUSARCHER	Reset Account Lockout counter after	Failed	High

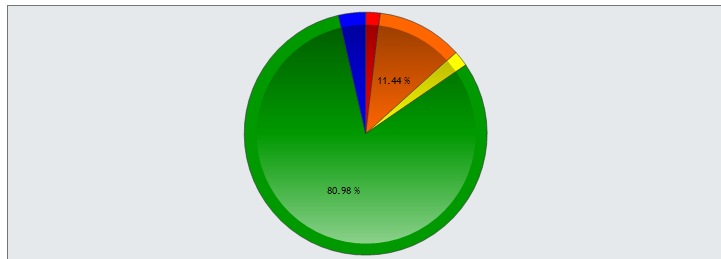
Click to Expand the Navigation Menu

Dashboard: Incident Management

Welcome, James Byroads

Options

Incidents by Priority



15 Critical
89 High
16 Medium
630 Low
28 Very Low

Critical Systems at High Incident Risk

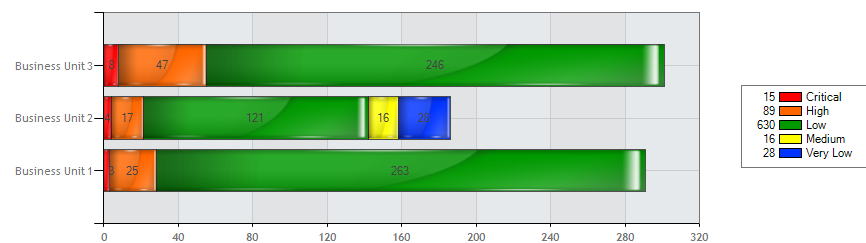
Device Name	Criticality	Incident Risk Rating
USCWdns01	⊖	
USCWweb01	⊖	
USCWweb03	⊖	

Page 1 of 1 (3 records)

Unassigned Incidents

Incident ID	Date/Time Occurred	Priority	Days Open
2	6/22/2012 6:00 PM		342
42	6/22/2012 6:00 PM		342
123	6/22/2012 6:15 PM		342
145	6/22/2012 6:20 PM		342
173	6/22/2012 6:25 PM		342
197	6/23/2012 8:00 AM		342
209	6/23/2012 8:00 AM		342
210	6/23/2012 8:00 AM		342

Business Unit Incidents by Priority

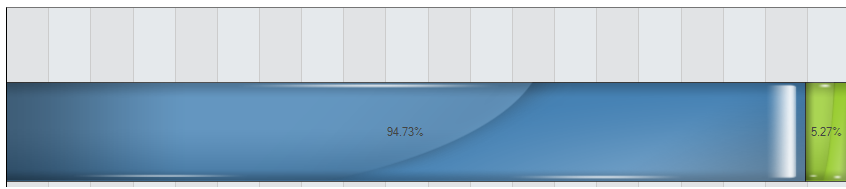


15 Critical
89 High
630 Low
16 Medium
28 Very Low

Top 10 Incidents by Frequency

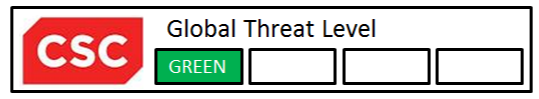
Incident Summary	Count of Incident Summary
Query/Viewer Query Succeeded	198
Monitor Event	110
Task successfully removed	73
Task successfully scheduled	70
ScheduledTask updated	70
Subsystem Status Changed to Error	39
Standard Assertion Events From Agents	39

Incidents by Status



Click to Expand the Navigation Menu

CSC Global Threat Level



CSC Global Threat Level

GREEN

NVD Recent Vulnerabilities

[National Vulnerability Database](#)
This feed contains the most recent CVE cyber vulnerabilities published within the National Vulnerability Database.

[CVE-2013-3641](#)
The Pizza Hut Japan Official Order application before 1.1.1.a for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.

[CVE-2013-3640](#)
Cross-site scripting (XSS) vulnerability in the Instant Web Publish function in FileMaker Pro before 12 and Pro Advanced before 12 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

[CVE-2013-2319](#)
FileMaker Pro before 12 and Pro Advanced before 12 does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.

[CVE-2013-1862](#)
mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.

Microsoft Vulnerabilities

[Microsoft Security Content: Comprehensive Edition](#)
Microsoft Security Content: Comprehensive Edition

[Advance Notification for June 2013 - Version: 1.0](#)

SecurityFocus News

[Infocus: Enterprise Intrusion Analysis, Part One](#)
Enterprise Intrusion Analysis, Part One

[Infocus: Responding to a Brute Force SSH Attack](#)
Responding to a Brute Force SSH Attack

[Infocus: Data Recovery on Linux and ext3](#)
Data Recovery on Linux and ext3

>> Advertisement <<
Can you answer the ERP quiz?
These 10 questions determine if your Enterprise RP rollout gets an A-.
<http://www.findtechinfo.com/as/acs?pl=781&ca=909>

[Infocus: WiMax: Just Another Security Challenge?](#)

SANS NewsBites

[SANSFIRE 2011](#)
SANSFIRE 2011

[PRISM Program Gives NSA Access to Data on Servers of Major US Internet Companies \(June 6, 2013\)](#)
It now appears that the National Security Agency's (NSA's) reach extends beyond just Verizon's call records.....

[FISA Order Requires Verizon to Provide NSA With Metadata on All Calls \(June 5 & 6, 2013\)](#)
According to a document obtained by The Guardian, the US Foreign Intelligence Surveillance Court issued an order forcing Verizon to provide the NSA metadata on all calls made through its systems over the three-month period between April 25 and July 19 2013.....

[FBI and Microsoft take Down Citadel Botnet \(June 6, 2013\)](#)
Microsoft and the FBI worked together to take down the Citadel botnet, which is believed to have been instrumental in an estimated US \$500 million in thefts from online bank accounts.....

SecurityFocus Vulnerabilities

[Vuln: Novell ZENworks Configuration Management CVE-2013-1095 Cross-Site Scripting Vulnerability](#)
Novell ZENworks Configuration Management CVE-2013-1095 Cross-Site Scripting Vulnerability

[Vuln: Adobe Flash Player and AIR CVE-2013-3326 Remote Memory Corruption Vulnerability](#)
Adobe Flash Player and AIR CVE-2013-3326 Remote Memory Corruption Vulnerability

SANS @Risk

[SANSFIRE 2011](#)
SANSFIRE 2011

Dashboard: GTI

Welcome, James Byroads

Options

GTI Top Threats

Tracking ID	Title	Search Matching Quality	Record Link	Device Name	Device Criticality
4078944	Adobe Flash Player CVE-2012-0754 Remote Memory Corruption Vulnerability	100 %	Click to Open Report	USCWftp04	High
4078943	Adobe Flash Player CVE-2012-0754 Remote Memory Corruption Vulnerability	100 %	Click to Open Report	USCWdns02	High
4078942	Adobe Flash Player CVE-2012-0754 Remote Memory Corruption Vulnerability	100 %	Click to Open Report	USCWdns02	High
4078941	Adobe Flash Player CVE-2012-0754 Remote Memory Corruption Vulnerability	100 %	Click to Open Report	USCWweb08	High
4078939	Adobe Flash Player CVE-2012-0754 Remote Memory Corruption Vulnerability	100 %	Click to Open Report	USCWfile06	High
4078938	Adobe Flash Player CVE-2012-0754 Remote Memory Corruption Vulnerability	100 %	Click to Open Report	USCWdb03	High
4078937	Adobe Flash Player CVE-2012-0754 Remote Memory Corruption Vulnerability	100 %	Click to Open Report	USCWweb08	High
4078936	Adobe Flash Player CVE-2012-0754 Remote Memory Corruption Vulnerability	100 %	Click to Open Report	USCWweb01	High
4078935	Adobe Flash Player CVE-2012-0754 Remote Memory Corruption Vulnerability	100 %	Click to Open Report	USCWweb01	High
4078933	Adobe Flash Player CVE-2012-0754 Remote Memory Corruption Vulnerability	100 %	Click to Open Report	USCWftp05	High
4078932	Adobe Flash Player CVE-2012-0754 Remote Memory Corruption Vulnerability	100 %	Click to Open Report	USCWftp05	High
4078931	Adobe Flash Player CVE-2012-0754 Remote Memory Corruption Vulnerability	100 %	Click to Open Report	USCWftp04	High
4078900	Adobe Acrobat Reader Remote Code Execution Vulnerability	100 %	Click to Open Report	USCWftp04	High
4078899	Adobe Acrobat Reader Remote Code Execution Vulnerability	100 %	Click to Open Report	USCWdns02	High
4078898	Adobe Acrobat Reader Remote Code Execution Vulnerability	100 %	Click to Open Report	USCWdns02	High
4078897	Adobe Acrobat Reader Remote Code Execution Vulnerability	100 %	Click to Open Report	USCWweb08	High
4078893	Adobe Acrobat Reader Remote Code Execution Vulnerability	100 %	Click to Open Report	USCWftp04	High

Click to Expand the Navigation Menu

CSC Horizon – Recap

- Secure Web Portal - customize dashboard for specific job titles and roles
 - Executive Management, CISO, SOC Analysts, Auditors, etc
 - Real-time data: Enterprise dashboard integrates state and Dynamic data from existing security controls into one easy-to-understand dashboard
- A platform for today and tomorrow. A secure, flexible, extensible and scalable security architecture.
 - Cloud (CSC Trusted Cloud), traditional infrastructure, application
- Integration with a large number of disparate device types and the ability to support additional sources.
- Integrated incident, vulnerability, threat. compliance data to provide enterprise-wide “Situational Awareness”
- Integrated with advanced Threat Intelligence
- CSC Horizon based on RSA Archer – wedge to a GRC
- 24x7x365 visibility of security status via Internet

Why CSC ? – Current Position / Evolution

CSC is uniquely positioned to deliver a comprehensive end to end solution, and we can offer all of the following:

- ✓ Leveraging 1200 specialized staff, CSC is currently deploying RSA Archer across existing CSC customer base
- ✓ Demonstrable expertise in delivery of RSA Archer ITGRC and controls integration.
- ✓ Extensive library of standard and custom connectors to security anchors
- ✓ Consumable by customer within MSS tier model while providing high level of customization
- ✓ The ability to consult, design, deploy and manage Archer on a global enterprise level
- ✓ Account Security Lead – IT Security BAU delivery lead
- ✓ Risk & Compliance Executive - CIO/CSO/Director accountability



BUSINESS SOLUTIONS
TECHNOLOGY
OUTSOURCING