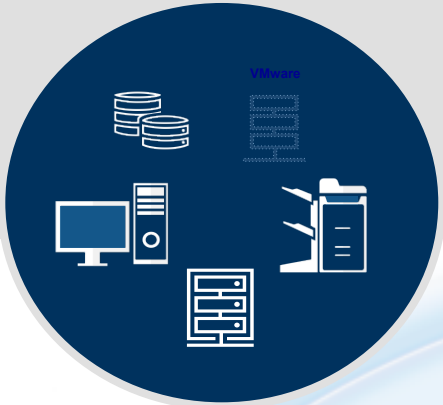
QUALYS®

How to manage evolving Cyber-Threats on evolving ICT infrastructure

Marek Skalicky, CISM, CRISC
MD for CEE Region

QUALYS®

ICT Assets and Apps are everywhere…



On Premise **Endpoints** **Cloud**

1 average ICT Asset = 20 Software components

1 average ICT Asset = 333 Security Datapoints for Risk & Compliance

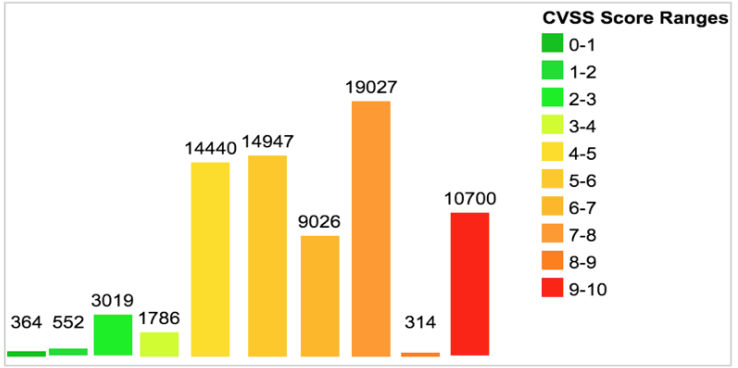
Vulnerabilities are growing and aging...

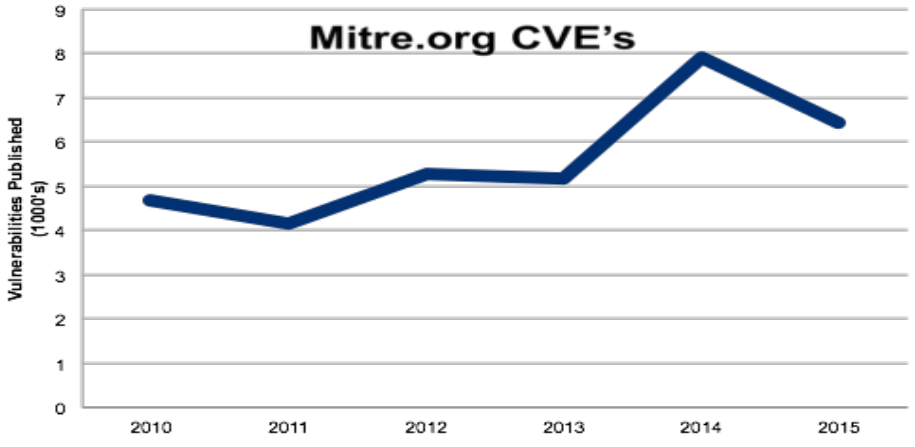
Distribution of all vulnerabilities by CVSS Scores

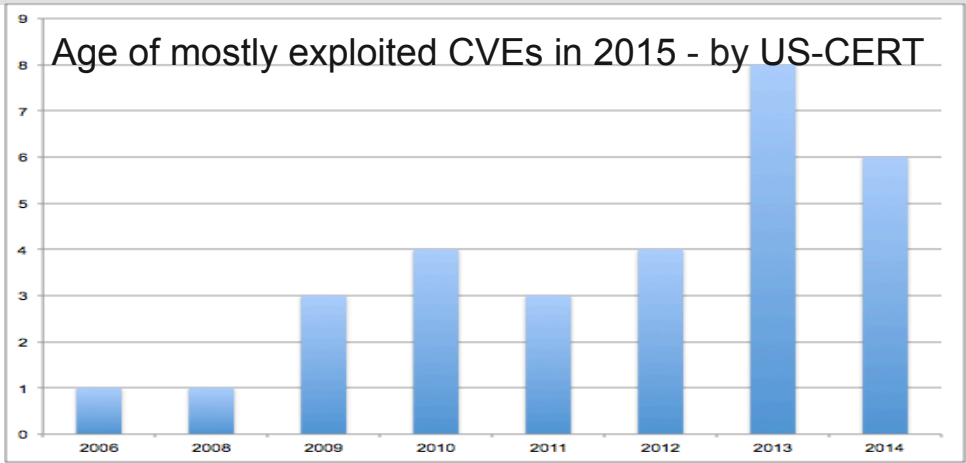
CVSS Score	Number Of Vulnerabilities	Percentage
0-1	364	0.50
1-2	552	0.70
2-3	3019	4.10
3-4	1786	2.40
4-5	14440	19.50
5-6	14947	20.20
6-7	9026	12.20
7-8	19027	25.70
8-9	314	0.40
9-10	10700	14.40
Total	74175	

Weighted Average CVSS Score: **6.8**

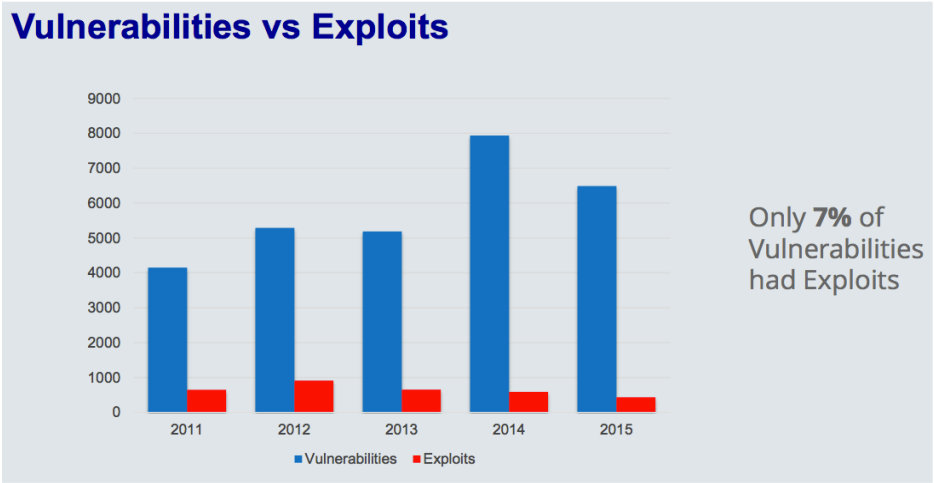
Vulnerability Distribution By CVSS Scores

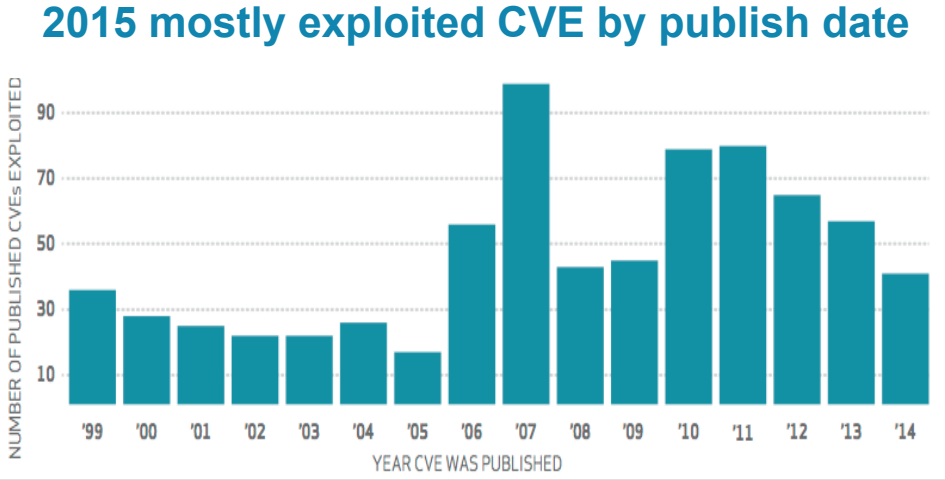


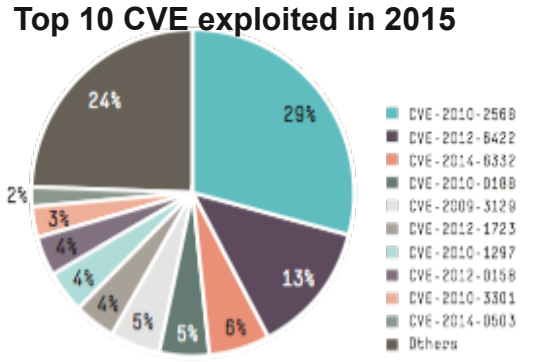




Cyber-threats are getting focused ...

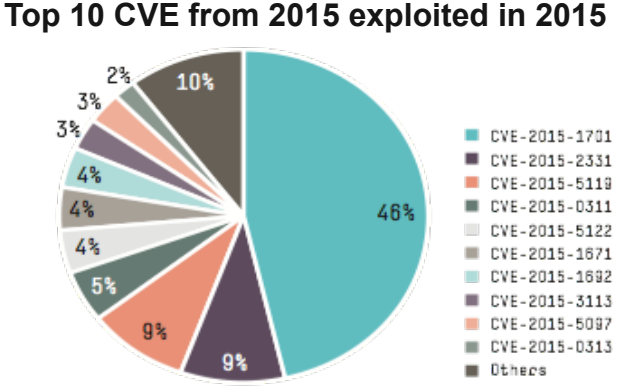






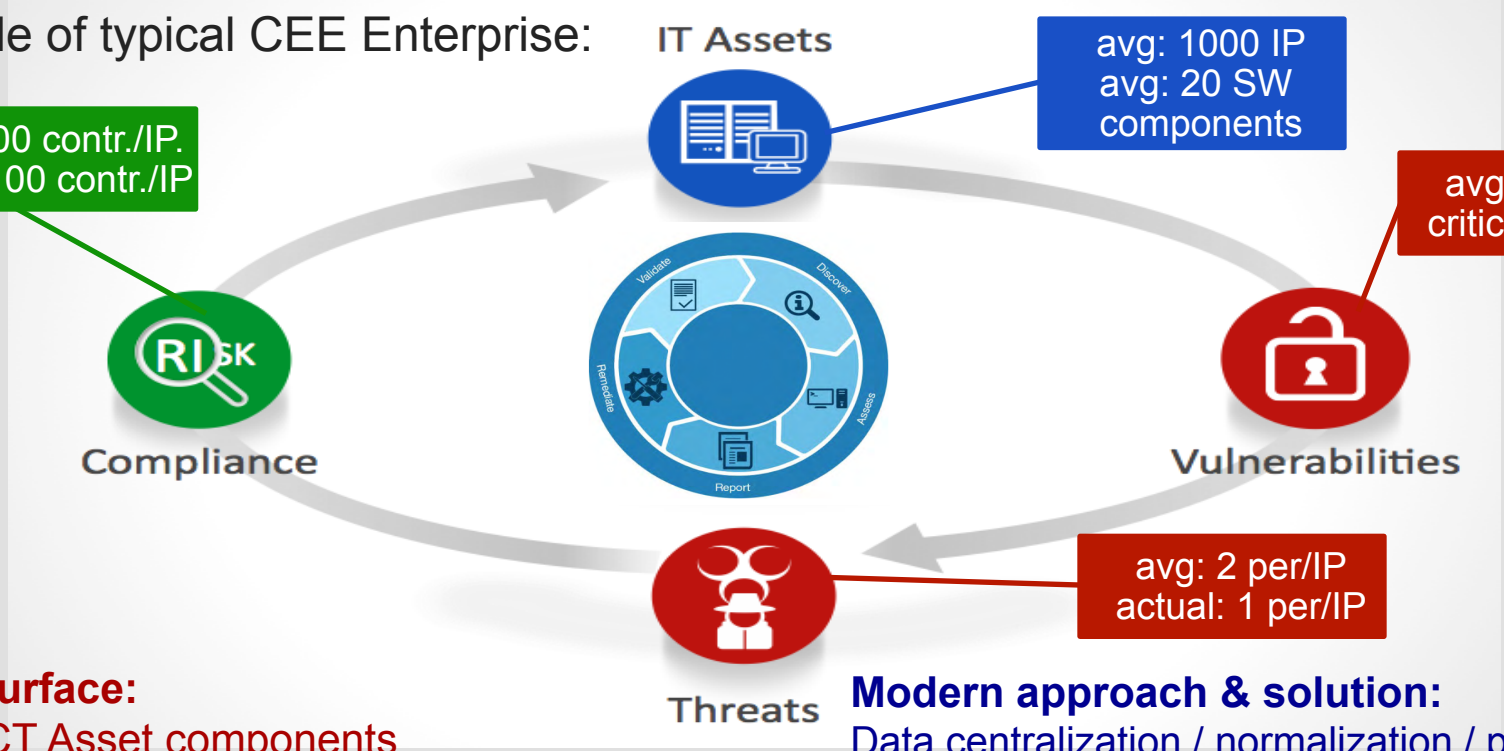
Based on real-breaches in 2015

Top exploited CVE by HPE'2016 Report



Where is the problem? In scope & time!

Example of typical CEE Enterprise:



Attack Surface:

20.000 ICT Asset components
20.000 Vulnerabilities (20% critical)
1.000 Actual Threats (Malware & Exploits)
100.000 Critical configuration security controls

Modern approach & solution:

Data centralization / normalization / prioritization
(Big)Data analytics / automation / workflow
Dashboards / Alerts / Tickets / Integrations
Cloud based architecture

QUALYS

So what to do – prioritization of controls ?

SANS / CIS Critical Security Controls - Version 6.1 – Aug. 2016

CIS CRITICAL SECURITY CONTROL	NIST 800-53 rev4*	NIST Core Framework	DHS CDM Program	ISO 27002:2013	ISO 27002:2005	NSA MNP	Au Top 35	NSA Top 10
1 Inventory of Authorized & Unauthorized Devices	CA-7 CM-8 IA-3: SA-4 SC-17 SI-4 PM-5	ID.AM-1 ID.AM-3 PR.DS-3	• HWAM: Hardware Asset Management	A.8.1.1 A.9.1.2 A.13.1.1	A.7.1.1 A.10.6.1 A.10.6.2 A.11.4.6	• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control • Log Management		
2 Inventory of Authorized & Unauthorized Software	CA-7 CM-2 CM-8 CM-10 CM-11 SA-4 SC-18 SC-34 SI-4 PM-5	ID.AM-2 PR.DS-6	• HWAM: Hardware Asset Managementt • SWAM: Software Asset Management	A.12.5.1 A.12.6.2		• Baseline Management • Executable Content Restrictions • Configuration and Change Management	1 14 17	• Application Whitelisting
3 Secure Configurations for Hardware & Software	CA-7 CM-2 CM-3 CM-5 CM-6 CM-7 CM-8 CM-9 CM-11 MA-4 RA-5 SA-4 SC-15 SC-34 SI-2 SI-4	PR.IP-1	• CSM: Configuration Settings Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	2-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements
4 Continuous Vulnerability Assessment & Remediation	CA-2 CA-7 RA-5 SC-34 SI-4 SI-7	ID.RA-1 ID.RA-2 PR.IP-12 DE.CM-8 RS.MI-3	• VUL: Vulnerability Management	A.12.6.1 A.14.2.8	A.12.6.1 A.13.1.2 A.15.2.2	• Patch Management • Log Management • Configuration and Change Management	2 3	• Take Advantage of Software Improvements
5 Controlled Use of Administrative Privileges	AC-2 AC-6 AC-17 AC-19 CA-7 IA-4 IA-5 SI-4	PR.AC-4 PR.AT-2 PR.MA-2 PR.PT-3		A.9.1.1 A.9.2.2 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.4	A.10.4.4 A.11.5.1 - A.11.5.3	• User Access • Baseline Management • Log Management	4 9 11 25	• Control Administrative Privileges

Source: https://www.cisecurity.org/critical-controls

How to do it on large scale?
1) Big Security Data Analytics around Assets

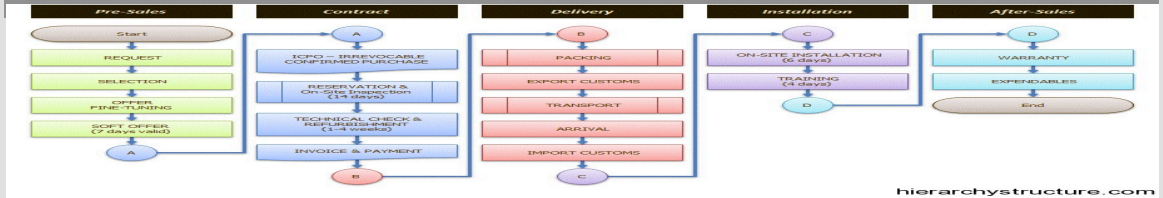
DASHBOARDS | ALERTS | TICKETS | WORKFLOWS | INTEGRATIONS

VULNERABILITY MANAGEMENT
+
THREAT ASSESSMENT
+
PATCH PRIORITIZATION

ASSET MANAGEMEMNT
+
HW & SW INVENTORY
+
CONTINUOUS VIEW & SEARCH

COMPLIANCE MANAGEMENT
+
SELF-AUDIT BENCHMARKING
+
CONFIGURATION HARDENING

MAPPING TO BUSINESS PROCESSES & BUSINESS APPLICATIONS



QUALYS

2) Continuous Asset Discovery, Centralization & Correlation

Continuous Discovery

+

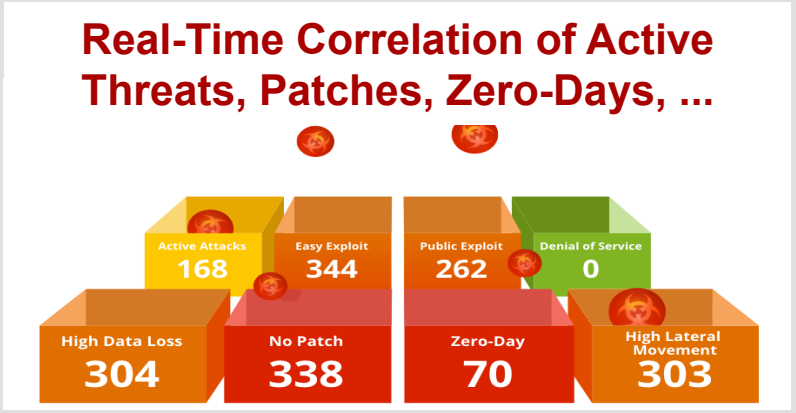
Real-time Distributed Data Collection

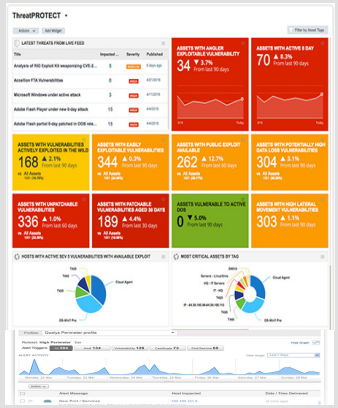
+

Data Analytics Correlation Backend

=

Continuous Security & Compliance

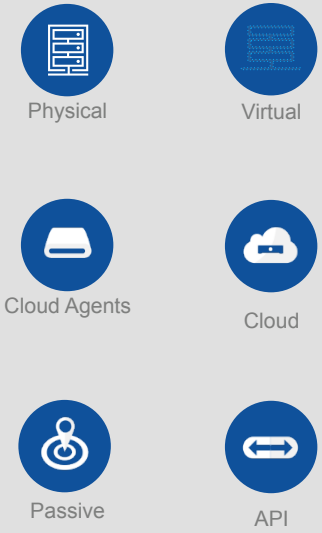




QUALYS

3) Via Multi-tenant & Elastic Cloud Architecture

Sensors

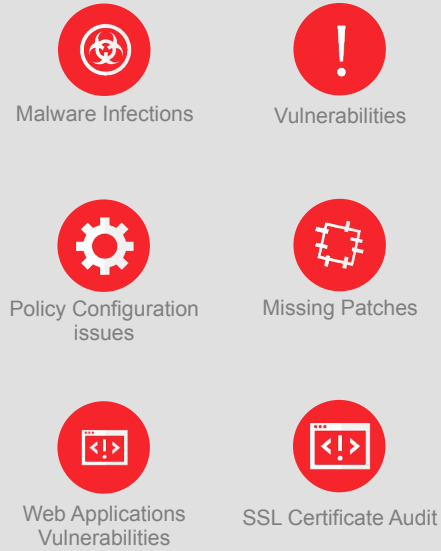


20 SW components / Asset
100 Critical Controls / Asset
333 Security datapoints / Asset

Data Analytics

20 Vulns detections / Asset
300 Real-time Threat correlations / Asset
Periodic Threat and Solution correlations

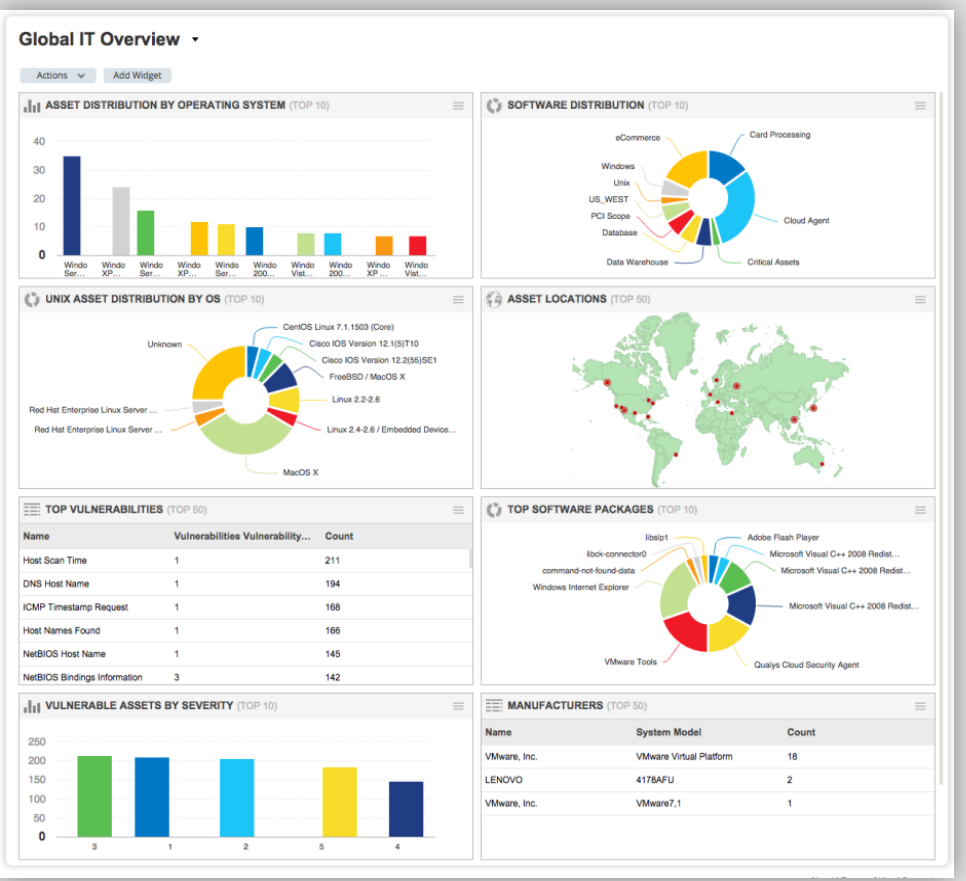
Incidence Response

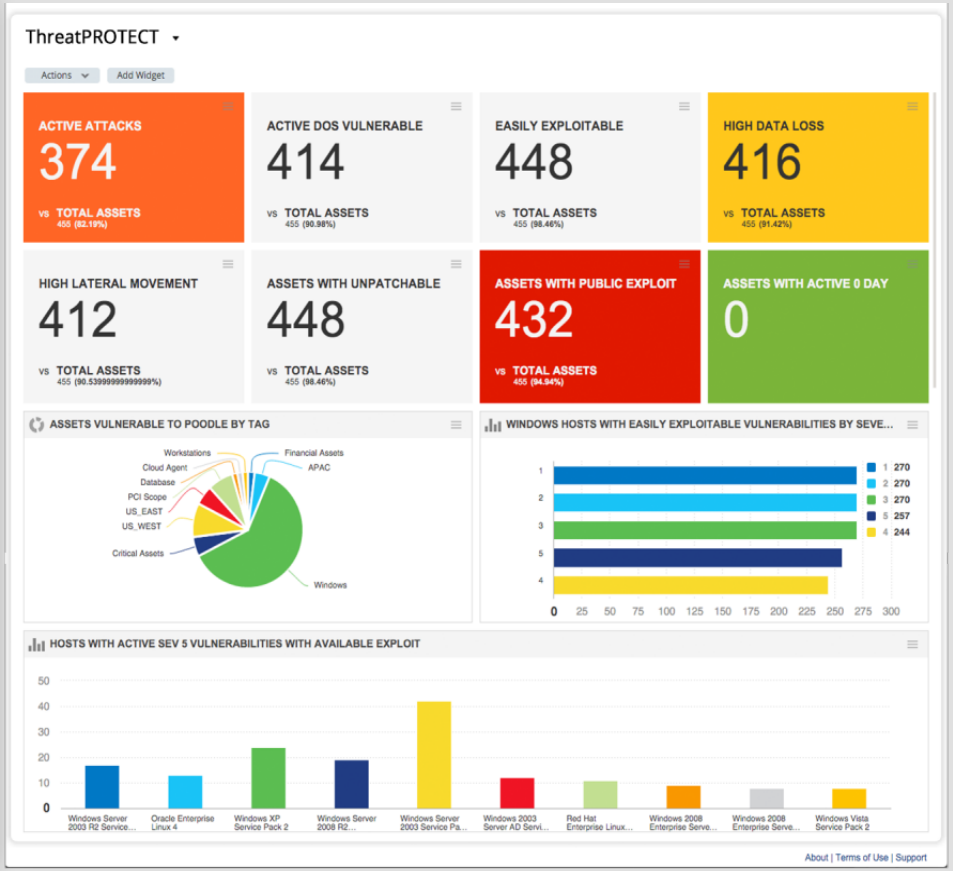


Real-time Asset dashboards
Real-time critical Vulns
Real-time Threats alerts

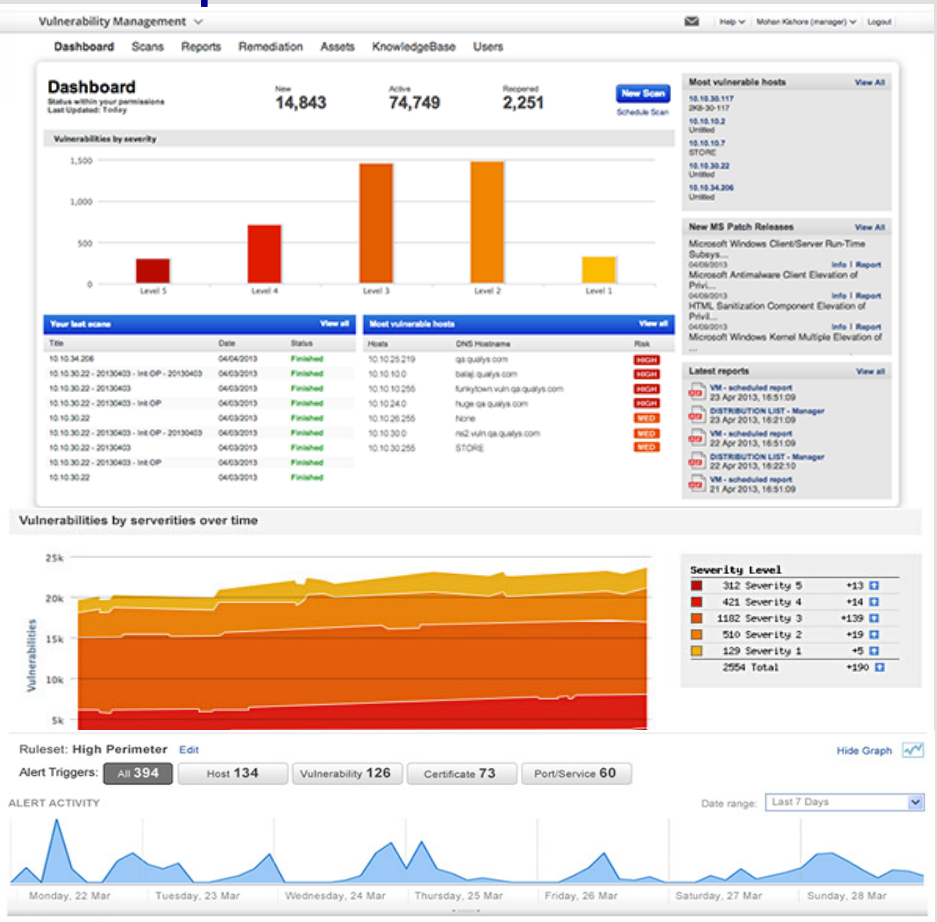
QUALYS

4) Moving from Reports to Dashboards & Alerts





5) Analyze trends and optimize workflows



6) Automate & Integrate for higher efficiency

CT Asset Management

servicenow

Remedy Corporation

IT Service Desks

QUALYSGUARD SMTP INTEGRATION

Risk

RedSeal

skybox security

Host Integrity Systems, Inc.

SIEM/Log

splunk>

LogRhythm

ArcSight

netForensics

Labs

StillSecure

TriGeo Network Security

RSA enVision

NetIQ

IDS/IPS

SOURCEfire

Pen Test

CORE SECURITY TECHNOLOGIES

Square Security

IMMUNITY

Access

Cyber-Ark

beyondtrust

IT GRC

R-sam

MODULO Solutions for IT GRC

bringa

LOCKPATH

MetricStream

RSA Archer eGRC Solutions

Allgress

Web App Firewall

BEE WARE Delivering Confidence in Web Applications

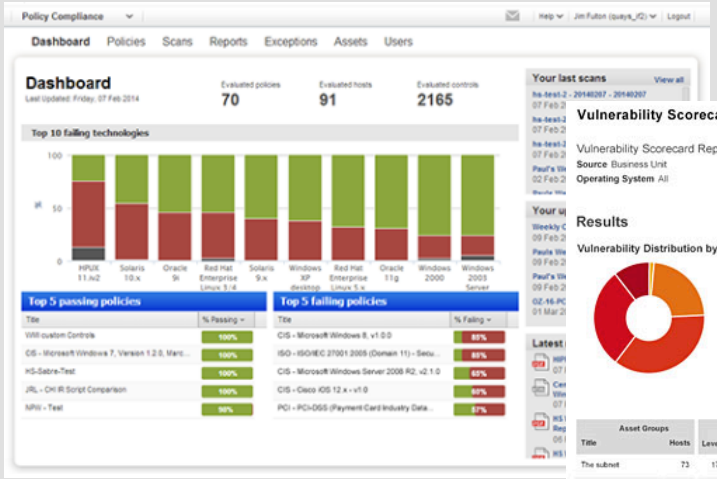
f5

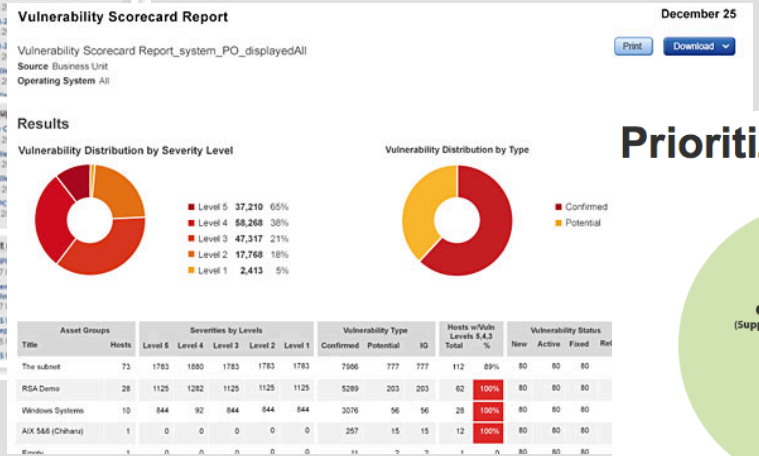
IMPERVA

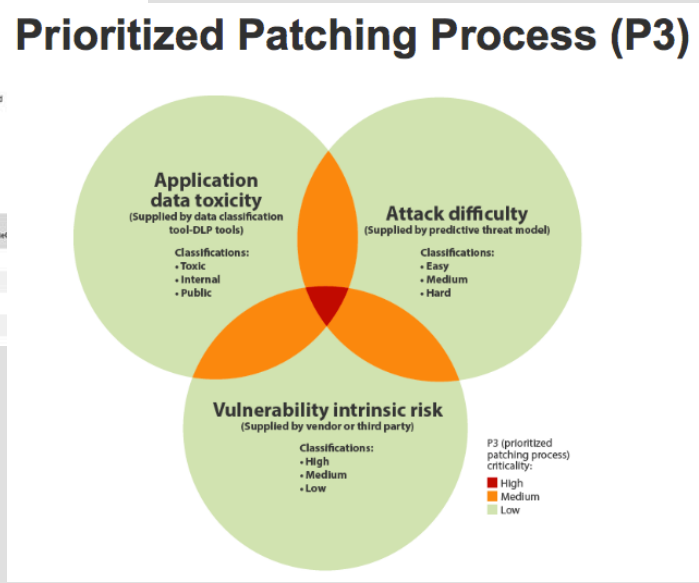
CITRIX

QUALYS

7) Deliver Visibility & Accountability & Prioritize again!







Because: No Visibility = No Security !!!

QUALYS

QUALYS®

Q&A

mskalicky@qualys.com