



UNIVERSITÀ DI PARMA

# Viaggio al centro di un asset

da visibilità a consapevolezza

Marco Rottigni  
Chief Technical Security Officer EMEA  
Qualys

Ilaria Comelli  
Responsabile UO Sicurezza e Processi IT  
Università di Parma



UNIVERSITÀ DI PARMA

# Viaggio al centro di un asset

il percorso verso una soluzione

Parma, 14 novembre 2019

Ilaria Comelli

# 2016 Anno Zero



# GDPR art. 32 Sicurezza del trattamento

1. Tenendo conto dello **stato dell'arte** e dei **costi di attuazione**, nonché della **natura, dell'oggetto**, del **contesto** e delle **finalità del trattamento**, come anche del **rischio** di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire **un livello di sicurezza adeguato al rischio**, che comprendono, tra le altre, se del caso:

- a) la **pseudonimizzazione** e la **cifratura** dei dati personali;
- b) la capacità di assicurare su base permanente la **riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento**;
- c) la capacità di **ripristinare tempestivamente la disponibilità e l'accesso** dei dati personali in caso di incidente fisico o tecnico;
- d) una **procedura per testare, verificare e valutare** regolarmente **l'efficacia** delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla **distruzione**, dalla **perdita**, dalla **modifica**, dalla **divulgazione non autorizzata** o **dall'accesso, in modo accidentale o illegale, a dati personali** trasmessi, conservati o comunque trattati.

# Misure Minime AGID

5-5-2017

GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA

*Serie generale - n. 103*

## 1. GENERALITÀ.

### 1.1. SCOPO.

Il presente documento contiene le misure minime di sicurezza ICT per le pubbliche amministrazioni le quali costituiscono parte integrante delle linee guida per la sicurezza ICT delle pubbliche amministrazioni.

.....

La scelta di prendere le mosse dall'insieme di controlli noto come SANS 20, oggi pubblicato dal Center for Internet Security come CCSC «CIS Critical Security Controls for Effective Cyber Defense» nella versione 6.0 di ottobre 2015, trova giustificazione, oltre che nella larga diffusione ed utilizzo pratico, dal fatto che esso nasce con una particolare sensibilità per i costi di vario genere che l'implementazione di una misura di sicurezza richiede, ed i benefici che per contro è in grado di offrire. L'elenco dei venti controlli in cui esso si articola, normalmente riferiti come Critical Security Control (CSC), è ordinato sulla base dell'impatto sulla sicurezza dei sistemi; per cui ciascun controllo precede tutti quelli la cui implementazione innalza il livello di sicurezza in misura inferiore alla sua. È comune convinzione che i primi cinque controlli siano quelli indispensabili per assicurare il minimo livello di protezione nella maggior parte delle situazioni e da questi si è partiti per stabilire le misure minime di sicurezza per la pubblica amministrazione italiana, avendo ben presente le enormi differenze di dimensioni, mandato, tipologie di informazioni gestite, esposizione al rischio, e quant'altro caratterizza le oltre ventimila amministrazioni pubbliche.

# Misure Minime: da dove vengono

## Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

## Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

## Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises



# CIS: i primi 5 controlli

Inventory of Authorized and Unauthorized **Devices**

Inventory of Authorized and Unauthorized **Software**

**Secure Configurations** for Hardware and Software

**Continuous Vulnerability Assessment** and Remediation

**Controlled Use of Administrative Privileges**



Fonte: <https://www.cisecurity.org/controls/>

# Misure Minime AGID

- inventario dei dispositivi autorizzati e non autorizzati
- inventario del software autorizzato e non autorizzati
- configurazione sicura di hardware e software
- adozione di un processo di gestione continua delle vulnerabilità
- utilizzo controllato dei privilegi amministrativi
- adozione di difese contro i programmi malware
- capacità di recuperare l'operatività in caso di incidente, ovvero Business Continuity
- protezione dei dati attraverso l'adozione di idonee misure di sicurezza





Come definire  
le priorità?

# Da dove cominciare?



# Chi siamo? Qualche numero

27.709

Studenti



13

Sedi

35

Plessi



1,6 Gbps

Banda utilizzata

135

Subnet attive



854

Personale T.A.

7k circa

Dispositivi connessi

# Chi siamo? Categorie di utenti

## Docenti

- Professori Ordinari
- Professori Associati
- Ricercatori
- Docenti a contratto
- Professori emeriti
- Professori onorari

## Personale Tecnico Amministrativo

## Dottorandi

## Borsisti di ricerca

## Assegnisti di ricerca

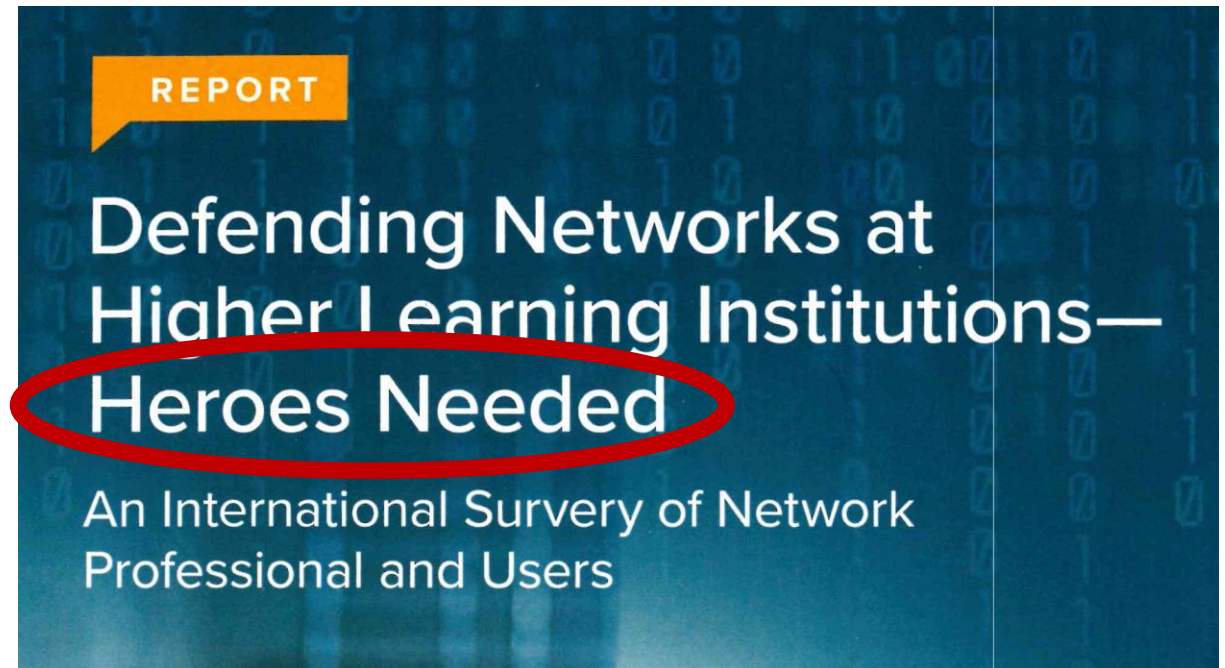
## Specializzandi

## Studenti

- Iscritti UniPR
- Erasmus
- interateneo

## Collaboratori

## Fornitori



# Criticità



# Equilibrio da trovare

Sicurezza  
dei dati

Libertà  
della ricerca



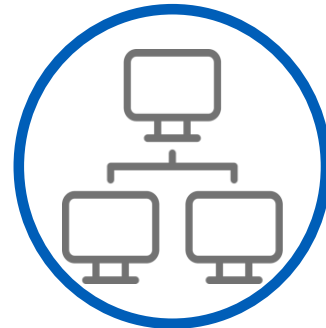
# Come scegliere le soluzioni



ambiti  
misure  
minime  
coperti



azioni su  
endpoint



azioni su  
infrastruttura



impatto  
esperienza  
utente

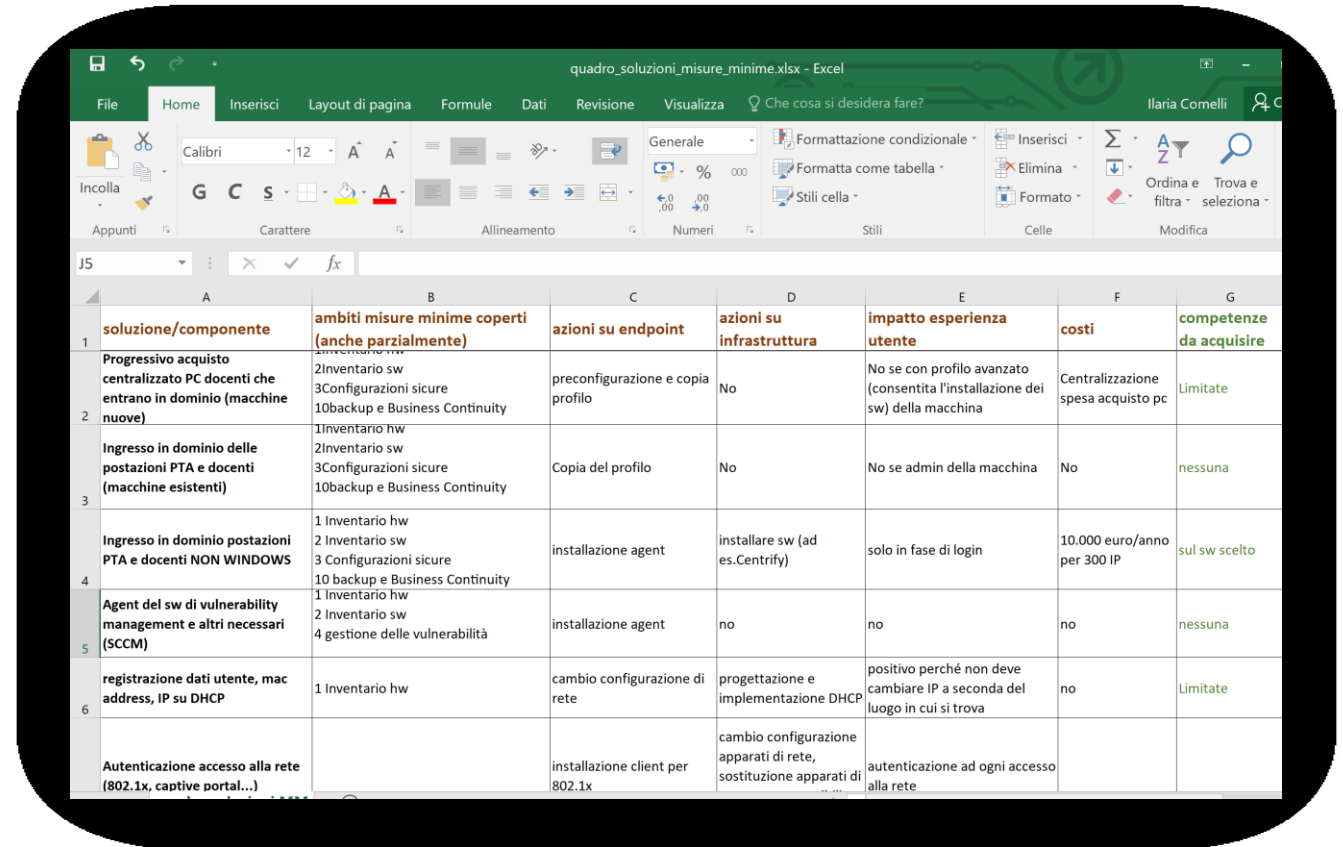


costi



competenze  
da acquisire

# Come scegliere le soluzioni



The screenshot shows an Excel spreadsheet titled "quadro\_soluzioni\_misure\_minime.xlsx". The table contains the following data:

	A	B	C	D	E	F	G
	<b>soluzione/componente</b>	<b>ambiti misure minime coperti (anche parzialmente)</b>	<b>azioni su endpoint</b>	<b>azioni su infrastruttura</b>	<b>impatto esperienza utente</b>	<b>costi</b>	<b>competenze da acquisire</b>
1	Progressivo acquisto centralizzato PC docenti che entrano in dominio (macchine nuove)	2Inventario sw 3Configurazioni sicure 10backup e Business Continuity	preconfigurazione e copia profilo	No	No se con profilo avanzato (consentita l'installazione dei sw) della macchina	Centralizzazione spesa acquisto pc	Limitate
2	Ingresso in dominio delle postazioni PTA e docenti (macchine esistenti)	1Inventario hw 2Inventario sw 3Configurazioni sicure 10backup e Business Continuity	Copia del profilo	No	No se admin della macchina	No	nessuna
3	Ingresso in dominio postazioni PTA e docenti NON WINDOWS	1 Inventario hw 2 Inventario sw 3 Configurazioni sicure 10 backup e Business Continuity	installazione agent	installare sw (ad es.Centrify)	solo in fase di login	10.000 euro/anno per 300 IP	sul sw scelto
4	Agent del sw di vulnerability management e altri necessari (SCCM)	1 Inventario hw 2 Inventario sw 4 gestione delle vulnerabilità	installazione agent	no	no	no	nessuna
5	registrazione dati utente, mac address, IP su DHCP	1 Inventario hw	cambio configurazione di rete	progettazione e implementazione DHCP	positivo perché non deve cambiare IP a seconda del luogo in cui si trova	no	Limitate
6	Autenticazione accesso alla rete (802.1x, captive portal...)		installazione client per 802.1x	cambio configurazione apparati di rete, sostituzione apparati di rete	autenticazione ad ogni accesso alla rete		



# Inventario vs Gestione degli asset

Indirizzo IP

Localizzazione

Tipologia hardware

Elenco software

Vulnerabilità

Stato di salute

# Viaggio al centro di un asset

Dalla Visibilità alla Consapevolezza

Marco Rottigni  
Chief Technical Security Officer EMEA  
Qualys

Ilaria Comelli  
Responsabile UO Sicurezza, Processi IT  
Università di Parma

Cosa è stato realizzato?

# CLOUD-BASED ARCHITECTURE



# Occhi e Cervello



### Global IT Resources

All Tags (12/12) | All Business Units | All Locations | Last 90 days



**ASSETS WITH ZERO-DAY VULNERABILITIES**

**200** vs. All Assets 2.5k (8%)  
▲ 5%

**ASSETS WITH MISSING CRITICAL PATCHES**

**20** vs. All Assets 2.5K (0.8%)  
▼ 52.38%

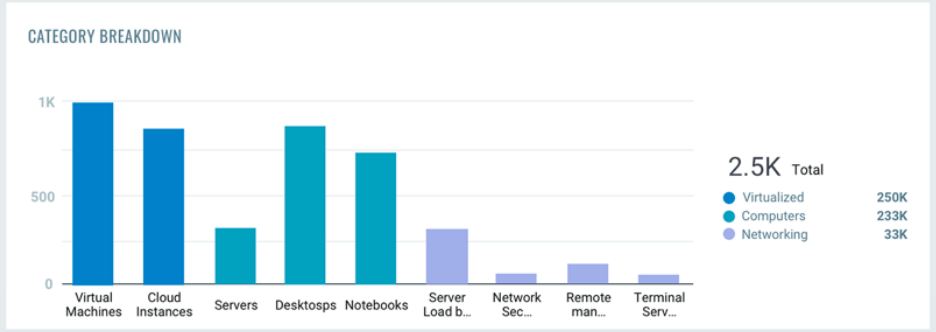
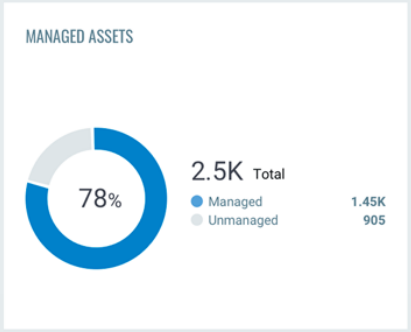
**INDICATION OF COMPROMISE ASSETS**

**58** vs. All Assets 2.5K (2.3%)  
▲ 20%

**CIS FAILED CONTROLS**

**92K** vs. All Assets 265K (35%)  
▲ 5%

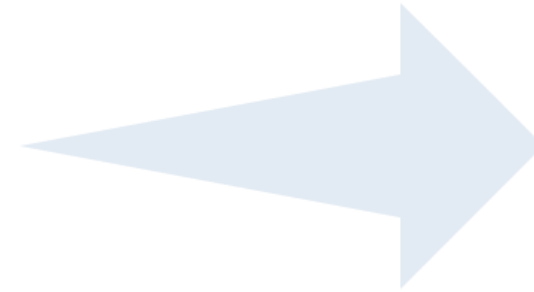
### Global IT Asset Inventory



# Il valore aggiunto di un Partner



Competenza




Agilità nella messa in opera



Supporto operativo

# L'Inventario «Multi-Prospettiva»...



The image displays several screenshots of the SMARTWORKING10 security management interface, illustrating a multi-perspective inventory of system components and vulnerabilities.

- Open Ports:** A table listing open ports with columns for Port, Protocol, Detected Service, and Service Description. For example, port 4880 is open on TCP for 'regina event di windows'.
- Installed Software:** A list of installed applications including '7-Zip 18.01', 'Acer Quick Access', 'Adobe Acrobat Professional', and 'Microsoft Office 2016'.
- Vulnerabilities:** A dashboard showing 'Confirmed Vulnerabilities' (53) and 'Potential Vulnerabilities' (1). It includes a 'Vulnerability Detection by Status' section with counts for Active (54), New (0), Resolved (0), and Fixed (0).
- Services:** A detailed list of system services such as 'ComEvo', 'CDPWin', 'ConProSvc', and 'ConSvc', along with their descriptions and current status (e.g., RUNNING).
- Asset Summary:** A summary view for the SMARTWORKING10 asset, showing system information like 'Microsoft Windows 10 Enterprise 10.0.17763.64' and a map of the last location.
- Threat Protection Summary:** A summary of 148 total RTIs for vulnerabilities, categorized by severity (Critical, Important, Moderate, Low, None) and status (Exploitable, Unexploitable, Active Attacks, Exploit Kit Available).
- Patch Management:** A view showing 'Missing Patches' (47) and 'Installed Patches' (248). It lists recent missing patches with details like patch title, bulletin, severity, and description.
- Indication of Compromise:** A view showing indicators of compromise, including a table with columns for Time, Object, Family, Category, and Score.

# L'Inventario «Multi-Prospettiva»...




### SMARTWORKING10

View Mode

- Asset Summary**
- System Information
- Agent Summary
- Network Information
- Open Ports
- Installed Software
- Vulnerabilities
- Threat Protection RTIs
- Indication of Compromise
- Patch Management

#### Asset Summary

 **SMARTWORKING10** [Rename](#)  
Microsoft Windows 10 Enterprise 10.0.17763 64 bit N/A Build 17763  
Acer

#### Identification

DNS Hostname: **SMARTWORKING10**  
FQDN: **SMARTWORKING10.**  
NetBIOS Name: **SMARTWORKING10**  
IPv4 Addresses: **160.78.**  
IPv6 Addresses: **fe80:0:0:0.**  
Asset ID: **4803686**  
Host ID: **3287466**

#### Last Location

Location unknown.  
Last Seen: 3 hours ago 8:50 AM  
Connected From: 160.78.

#### Activity

Last User Login: **@unipr.it**  
Last System Boot: **October 17, 2019 7:20 AM**  
Created On: **April 9, 2019 8:03 AM**  
Last Checked-In: **3 hours ago 8:50 AM**  
Last Activity: **3 hours ago 8:50 AM**

#### Tags

UNIPR ALL (160.78.0.0/16)  
SEDE CENTRALE (160.78.) 01-01 Sede Centrale  
Cloud Agent Servizi

[Close](#)



# L'Inventario «Multi-Prospettiva»...



**SMARTWORKING10** [Close]

**View Mode**

- Asset Summary >
- System Information >**
- Agent Summary >
- Network Information >
- Open Ports >
- Installed Software >
- Vulnerabilities >
- Threat Protection RTIs >
- Indication of Compromise >
- Patch Management >

**System Information**

**Services**

Name	Description	Status
CcmExec	Host agenti di SMS	RUNNING
CDPSvc	Servizio piattaforma dispositivi connessi	RUNNING
CertPropSvc	Propagazione certificati	RUNNING
CmRcService	Controllo remoto di Configuration Manager	RUNNING
CoreMessagingRegistrar	CoreMessaging	RUNNING
DiagTrack	Esperienze utente connesse e telemetria	RUNNING
cphs	Intel(R) Content Protection HECI Service	RUNNING
cpispcon	Intel(R) Content Protection HDCP Service	RUNNING
CryptSvc	Servizi di crittografia	RUNNING
DcomLaunch	Utilit... di avvio processi server DCOM	RUNNING
DeviceAssociationService	Servizio associazione dispositivi	RUNNING
Dhcp	Client DHCP	RUNNING
AdobeARMSvc	Adobe Acrobat Update Service	RUNNING
Appinfo	Informazioni applicazioni	RUNNING
AppXSvc	Servizio di distribuzione AppX (AppXSVC)	RUNNING
AudioEndpointBuilder	Generatore endpoint audio Windows	RUNNING
Audiosrv	Audio di Windows	RUNNING
camsvc	Servizio di gestione dell'accesso alle funzionalit...	RUNNING
BFE	BFE (Base Filtering Engine)	RUNNING
BrokerInfrastructure	Servizio infrastruttura attivit... in background	RUNNING
Browser	Browser di computer	RUNNING

[Close]

# L'Inventario «Multi-Prospettiva»...



**SMARTWORKING10** [Close]

**View Mode**

- Asset Summary >
- System Information >
- Agent Summary >
- Network Information >
- Open Ports >**
- Installed Software >
- Vulnerabilities >
- Threat Protection RTIs >
- Indication of Compromise >
- Patch Management >

**Open Ports**

This list includes ports with listening services. [Download](#)

Port	Protocol	Detected Service	Service Description
49665	TCP	registro eventi di windows	-
49666	TCP	utilit	-
49667	TCP	configurazione desktop remoto	-
49668	TCP	spoolsv.exe	-
49669	TCP	lsass.exe	-
49670	TCP	impossibile ottenere informazioni sulla propriet...	-
49681	TCP	agente criteri ipsec	-
49692	TCP	lsass.exe	-
50185	UDP	wmiprvse.exe	-
51278	UDP	dike.exe	-
51279	UDP	dike.exe	-
51876	UDP	pubblicazione risorse per individuazione	-
51877	UDP	pubblicazione risorse per individuazione	-
51948	UDP	outlook.exe	-
53297	UDP	helper ip	-
54079	UDP	acrord32.exe	-

Page 2 of 3 | [Close](#) | [Refresh](#) | [Download](#)

Displaying open ports 21 - 40 of 49

[Close](#)

# L'Inventario «Multi-Prospettiva»...



**SMARTWORKING10** [Close]

**View Mode**

- Asset Summary >
- System Information >
- Agent Summary >
- Network Information >
- Open Ports >
- Installed Software** >
- Vulnerabilities >
- Threat Protection RTIs >
- Indication of Compromise >
- Patch Management >

**Installed Software**

Search... [Magnifying Glass] [Download](#)

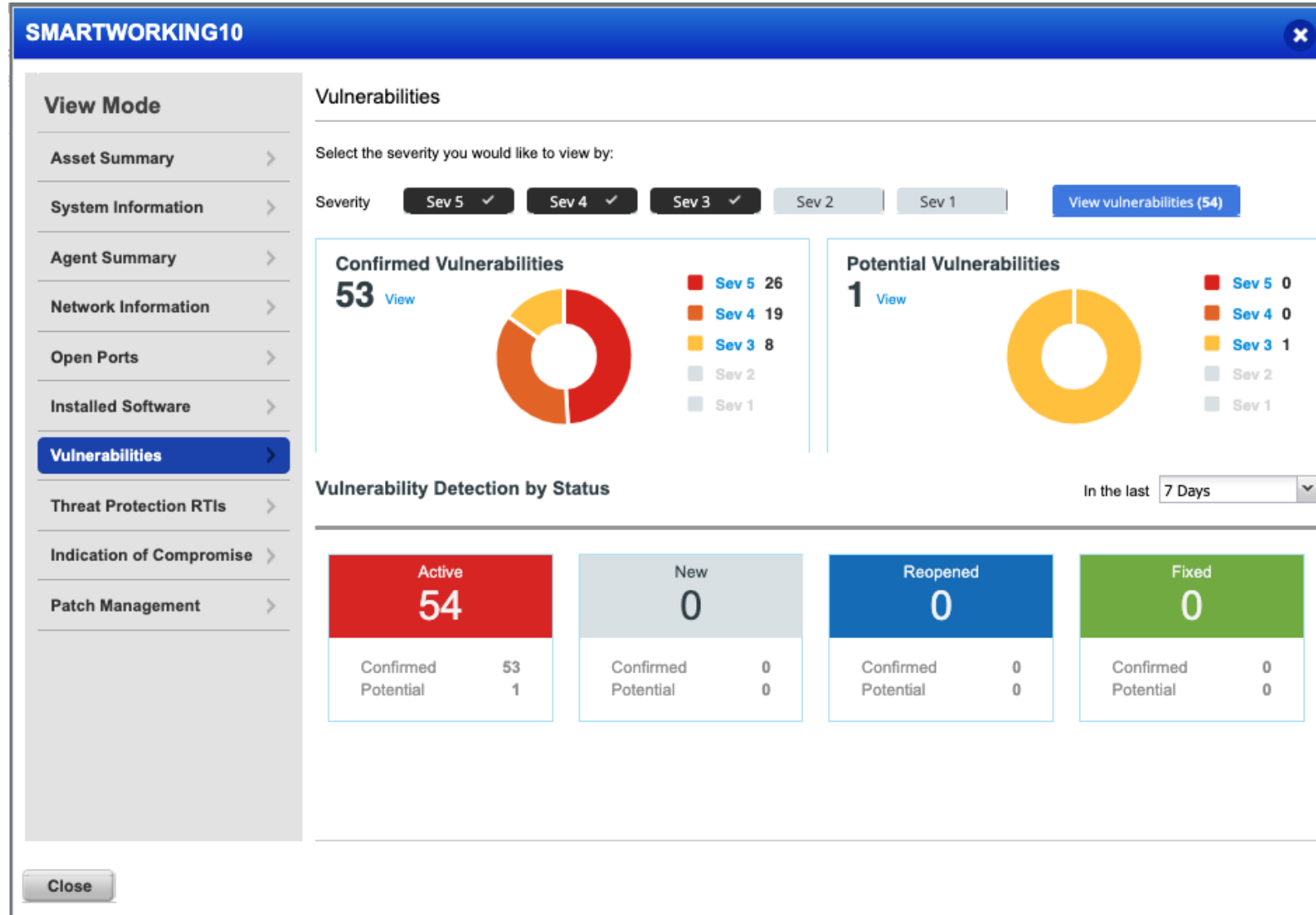
Name	Version
7-Zip 18.01	18.01.00.0
Acer Quick Access	2.01.3025
Adobe AIR	32.0.0.89
Adobe Acrobat 8 Professional - Italiano, Español, Ned...	8.3.1
Adobe Acrobat Reader DC - Italiano	15.007.20033
Adobe Digital Editions 4.5	4.5.7
Adobe Flash Player 24 NPAPI	24.0.0.186
Adobe Refresh Manager	1.8.0
Conexant HD Audio	8.66.16.52
ConfigMgr Wake-up Proxy	5.00.8716.1000
Configuration Manager Client	5.00.8790.1000
Definition Update for Microsoft Office 2016 (KB31154...	
Dike GoSign	7.0.2
DisplayLink Graphics Driver	9.0.1651.0
File version of Microsoft XML parser (MSXML) v3 :	8.110.17763.437

Page 1 of 7 [Refresh] Clear

Displaying installed software 1 - 20 of 139

**Close**

# L'Inventario «Multi-Prospettiva»...



# L'Inventario «Multi-Prospettiva»...



### SMARTWORKING10

View Mode

- Asset Summary >
- System Information >
- Agent Summary >
- Network Information >
- Open Ports >
- Installed Software >
- Vulnerabilities >
- Threat Protection RTIs >**
- Indication of Compromise >
- Patch Management >

#### Threat Protection Summary

Total RTIs for Vulnerabilities **148**

Zero Day	1	High Lateral Movement	25
Easily Exploitable	44	High Data Loss	25
Unpatchable	9	Vulnerable to DOS	24
Active Attacks	3	Malware	1
Exploit Kit Available	1	Public Exploit	15

#### LATEST THREATS FROM LIVE FEED

Last refreshed less than a minute ago

Title	Severity	Published
No threats pertaining to this asset were found in the past 30 days.		

Close

# L'Inventario «Multi-Prospettiva»...



**SMARTWORKING10**

**View Mode**

- Asset Summary >
- System Information >
- Agent Summary >
- Network Information >
- Open Ports >
- Installed Software >
- Vulnerabilities >
- Indication of Compromise >**
- Patch Management >

**Indication of Compromise**

indicator.score:"8" Active View

**Telemetry Type**

file 4

**Score**

8 4

**Malware Category**

puu 4

Time	Object	Family	Category	Score
October 29, 2019 12:41:15 PM	<b>WizardPages.dll</b> C:\Users\Administrator\AppData\Local\Temp\7zS8783...	Webcompanion	PUA	8
October 29, 2019 12:41:14 PM	<b>installer.exe</b> C:\Users\Administrator\AppData\Local\Temp\7zS8783...	Webcompanion	PUA	8
October 29, 2019 12:41:13 PM	<b>DevLib.dll</b> C:\Users\Administrator\AppData\Local\Temp\7zS8783...	Webcompanion	PUA	8
October 29, 2019 12:41:13 PM	<b>GenericSetup.exe</b> C:\Users\Administrator\AppData\Local\Temp\7zS8783...	Webcompanion	PUA	8

Close

# L'Inventario «Multi-Prospettiva»...



## SMARTWORKING10

**View Mode**

- Asset Summary >
- System Information >
- Agent Summary >
- Network Information >
- Open Ports >
- Installed Software >
- Vulnerabilities >
- Threat Protection RTIs >
- Indication of Compromise >
- Patch Management >**

### Patch Management

Select the severity you would like to view by:

Severity **Critical** ✓ **Important** ✓ **Moderate** ✓ Low None [View List \(295\)](#)

#### Missing Patches

**47** [View](#)

Critical	38
Important	8
Moderate	1
Low	
None	

#### Installed Patches

**248** [View](#)

Critical	193
Important	55
Moderate	0
Low	
None	

#### Top 5 Recent Missing Patches

Patch Title	Bulletin	Severity
Firefox 70.0	FF19-023	Critical
Java 8 Update 231	JAVA8-231	Important
Security updates ava...	APSB19-49	Critical
VLC Media Player 3...	VLC-308	Moderate
Security updates ava...	APSB19-41	Important

#### Top 5 Deployed Patches

Patch Title	Bulletin	Severity
Description of the se...	MS19-10-OFF-4475...	Important
Servicing stack upda...	MS19-10-SSU-4521...	Critical
Security Cumulative ...	MS19-10-W10-4519...	Critical
Description of the se...	MS19-10-OFF-4484...	Important
October 1, 2019, upd...	MSNS19-10-4484116	Critical

[Close](#)

# ... e la visione di insieme

**Global IT Asset Inventory**

Global IT Asset Inventory TRIAL

HOME DASHBOARD INVENTORY

Last 30 Days

**OPERATING SYSTEM DISTRIBUTION**

Total: 364

- Windows: 147
- Linux: 94
- Firmware: 85
- Unidentified: 19
- Network O.: 14

**CATEGORY BREAKDOWN**

- Computers
- Networking Device

**Malware Family Detection**

Indication of Compromise

Current State

**MALWARE CATEGORIES**

- backdoor
- exploit
- trojan
- adware
- malware
- pus...
- adw...
- troja...
- spy...

**MALWARE FAMILIES**

- backdoor
- sq2
- conduit
- generic
- mywebsearch
- can
- lobit...
- myw...
- gene...
- pokk...

**Vulnerability Management**

DASHBOARD VULNERABILITIES SCANS REPORTS REMEDIATION ASSETS KNOWLEDGEBASE USERS

**ACTIVE**

46.2K vs All vulnerabilities 51.5K (90%) ▼ 89.69%

**NEW**

5.03K vs All vulnerabilities 51.5K (1%) ▼ 9.76%

**REOPENED**

276 vs All vulnerabilities 51.5K (1%) ▼ 0.53%

**VULNERABILITIES BY SEVERITY**

Severity	Count
3	26.4K
2	14.0K
4	11.4K
5	4.09K
1	2.37K

**VULNERABILITIES BY TYPE**

- Confirmed: 32968
- Potential: 25199

**Threat Protection**

Dashboard Feed Assets Configuration

**Live Feed** Last updated a few seconds ago

Saved Searches

Search for threat news feeds

**HIGH RATED FEED 211** **MEDIUM / LOW RATED FEED 21,899**

**HIGH** 2 days ago

**Google Chrome Exploit in wild**

Live Threat Intelligence Feed Trick or Treat! Treat it is xD Rather than live in dread of Trick, Google chrome decided to treat its user with the Latest Chrome Update on Halloween Eve. But this...

Google Chrome CVE-2019-13720 10 Impacted Assets

**MEDIUM** October 29, 2019

**PoC Exploit available for CVE-2015-0008**

An exploit for CVE-2015-0008 is now available from The Exploit-DB. Qualys has added QID(s) 91129, 91017 to detect this issue in your environment. Please check your ThreatPROTECT dashboard for...

12 Impacted Assets

**HIGH** October 27, 2019

**Nginx + PHP 7 Remote Code Execution Vulnerability**

Live Threat Intelligence Feed On October 24 th 2019, PHP released updates to fix a remote code execution vulnerability. The vulnerability allows an attacker to run arbitrary commands on a vulnerable serv...

php Nginx CVE-2019-11043 0 Impacted Assets

**MEDIUM** October 29, 2019

**PoC Exploit available for CVE-2015-0009**

An exploit for CVE-2015-0009 is now available from The Exploit-DB. Qualys has added QID(s) 91020 to detect this issue in your environment. Please check your ThreatPROTECT dashboard for...

0 Impacted Assets

**HIGH** October 16, 2019

**SUDO Security Policy Bypass Vulnerability**

Live Threat Intelligence Feed Sudo is one of the most important and widely used core command that allows a permitted user to execute a command as the superuser or with other user privileges. It is...

CVE-2019-14287 root Sudo sudo security policy /sudoers 1 Impacted Assets

**MEDIUM** October 28, 2019

**PoC Exploit available for CVE-2019-11043**

An exploit for CVE-2019-11043 is now available from The Exploit-DB. Qualys has added QID(s) 150270, 177444, 177445, 197678, 87400, 177426 to detect this issue in your environment. Please...

0 Impacted Assets

**HIGH** October 10, 2019

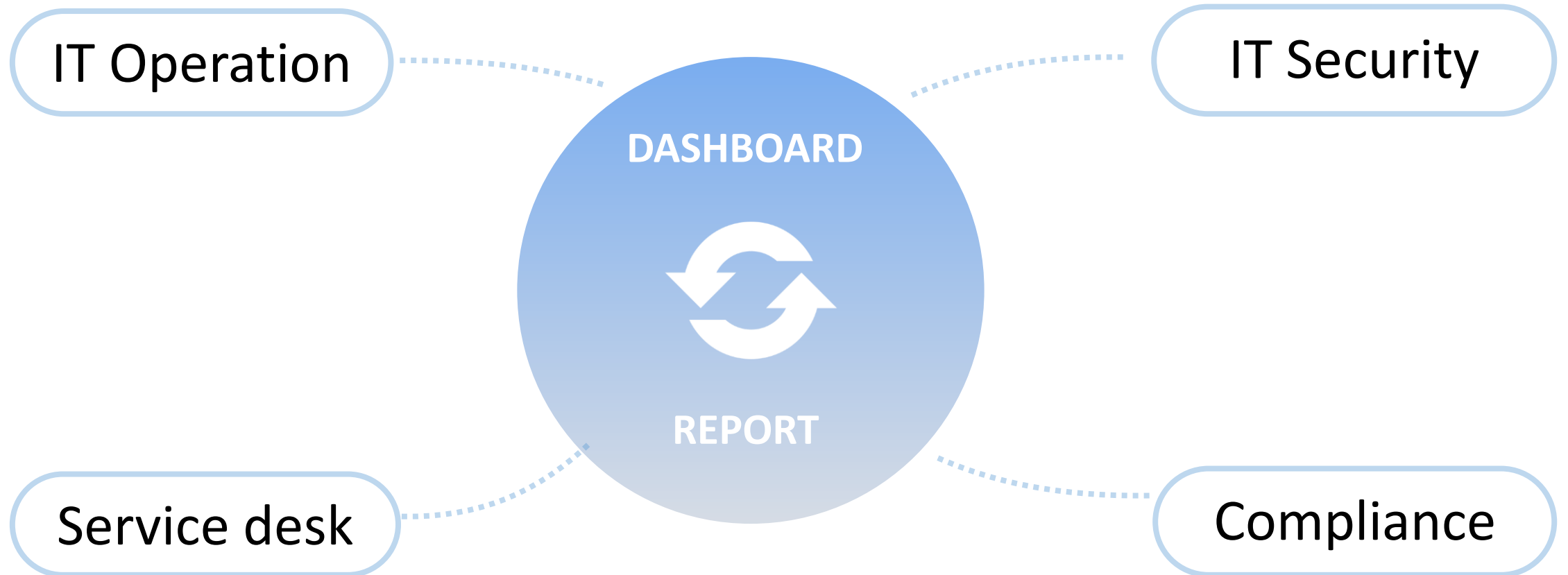
**vBulletin remote code execution vulnerability**

Live Threat Intelligence Feed Summary: A critical remote code execution (RCE) bug affecting default 5.x versions of vBulletin (CVE-2019-16759) is being actively exploited in the wild, allowing...

0 Impacted Assets



# Dati consumabili da più utenti



# Take home messages

- Single Pane of Glass, Single Source of Truth
- Futura integrazione con altre piattaforme (es. CMDB)
- Creare utenti differenziati che abbiano visibilità su ambienti di competenza → condivisione strutturata delle informazioni

Certo, avremmo potuto noleggiare un servizio...  
ma non senza rinunciare ad una crescita delle  
competenze interne che riteniamo fondamentale!

Ilaria Comelli

Grazie!

[ilaria.comelli@unipr.it](mailto:ilaria.comelli@unipr.it)

[marco@qualys.com](mailto:marco@qualys.com)