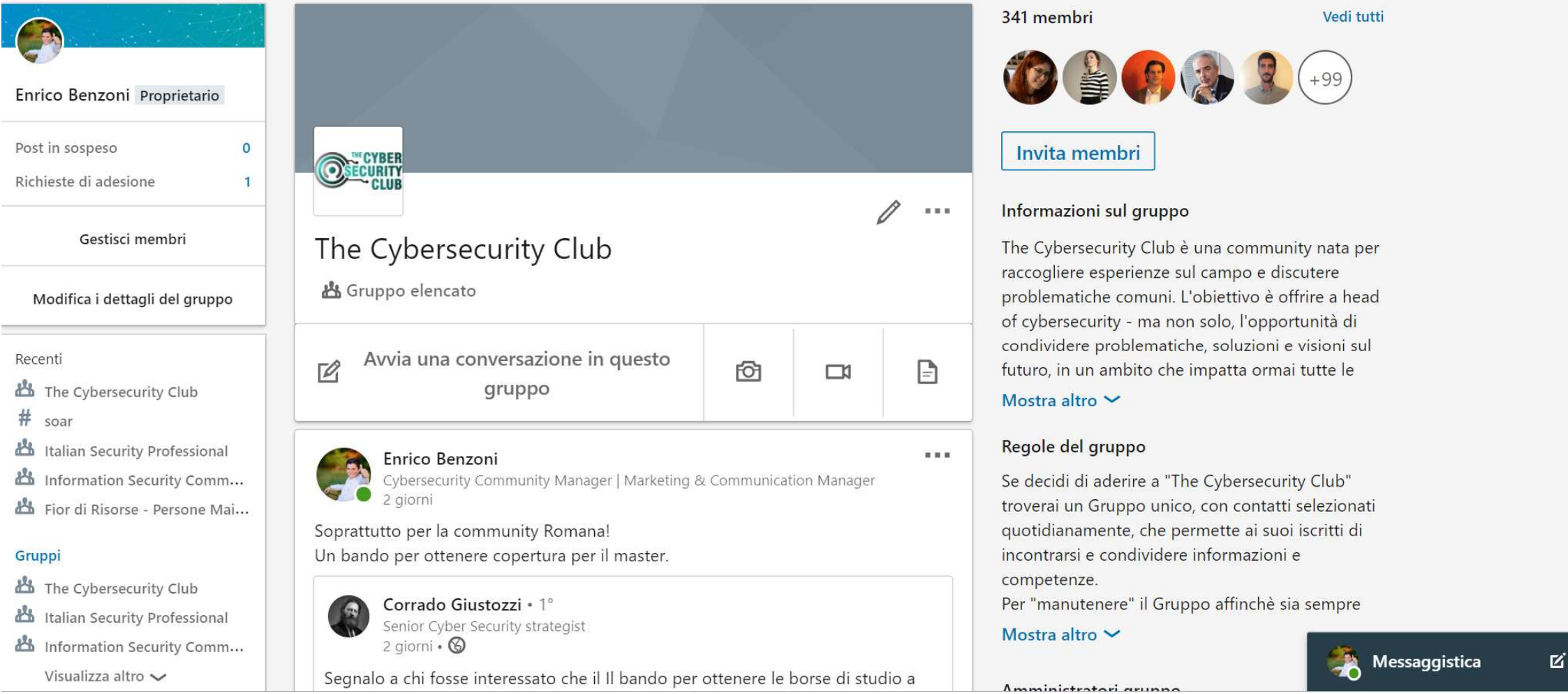
Una community per la Cybersecurity

Enrico Benzoni

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

The Cybersecurity Club su LinkedIn



CORRIERE DELLA SERA / SALUTE

REPORT CLUSIT 2019 SULLA SICUREZZA

Attacchi informatici: anche negli ospedali e nelle Asl è allarme

La sanità è uno dei settori più bersagliati dai pirati della Rete. Utilizzati software dannosi per realizzare estorsioni via internet, 17 le strutture hackerate in Italia

di Ruggiero Corcella

FEDERPRIVACY

Home Associazione Attività Informazione Strumenti Domande Frequenti

NEWS Collegio Garante Privacy, proroga fino al 31 dicembre e riapertura termini per la presentazione delle candidature

Online senza protezione 5 milioni di esami medici, indaga il Garante della Privacy

Flash News Giovedì, 10 Ottobre 2019 10:04

Oltre 5,8 milioni di radiografie, salvate con una serie di dati personali molto sensibili, come nome e cognome del paziente e motivo dell'esame, su server non protetti. E accessibili via internet anche a curiosi non autorizzati. È questa la scoperta fatta in Italia da Greenbone Networks, società tedesca di sicurezza informatica, che tra luglio e settembre ha analizzato le misure di protezione di 2.300 database medici, scoprendo che quasi uno su quattro, 590 per la precisione, è accessibile online. Offrendo a occhi indiscreti, o peggio, a malintenzionati, 24 milioni di dati relativi a pazienti da 52 Paesi nel mondo. Tra cui l'Italia, che spicca in Europa con il triste primato di immagini e data set

NEWS FOCUS PIÙ LETTI SPECIALI

Dalla privacy qualche diritto in più chi finisce in black-list ingiustamente
Lunedì, 14 Ottobre 2019 10:17

Romania, sanzionata la Raiffeisen Bank per violazione del Gdpr
Lunedì, 14 Ottobre 2019 09:53

Reputazione online, le tutele del Gdpr nel far west delle profilazioni
Lunedì, 14 Ottobre 2019 09:27

Cronaca Politica Economia Regioni + Mondo Cultura Tecnologia

PRIMOPIANO HI-TECH INTERNET & SOCIAL TELECOMUNICAZIONI SOFTWARE & APP STORIE DIGITAL

ANSA.it › Tecnologia › Internet & Social › Attacco hacker a ospedali nel mondo

Attacco hacker a ospedali nel mondo

Colpiti persino dispositivi per risonanza e raggi x

Redazione ANSA
ROMA
24 aprile 2018
19:05
NEWS

Suggerisci
Facebook
Twitter
Altri
Stampa
Scrivi alla redazione

Archiviato in
Informatica e Telecomunicazioni
Scienze informatiche
Crimini informatici

© ANSA/EPA CLICCA PER INGRANDIRE

(ANSA) - Un gruppo di hacker chiamato Orangeworm sta conducendo attacchi informatici diretti a ospedali e strutture sanitarie, arrivando a prendere il controllo dei computer per risonanze e macchine per i raggi X.

Lo rivela un Istantanea schermo proprio sito da Symantec. "Il

ansa.it/canale_saluteebenessere/notizie/sanita/2018/11/09/attacchi-hacker-primo-pericolo-per-gli-ospedali_63b7b558-131b

Salute&Benessere

Attacchi hacker primo pericolo per gli ospedali

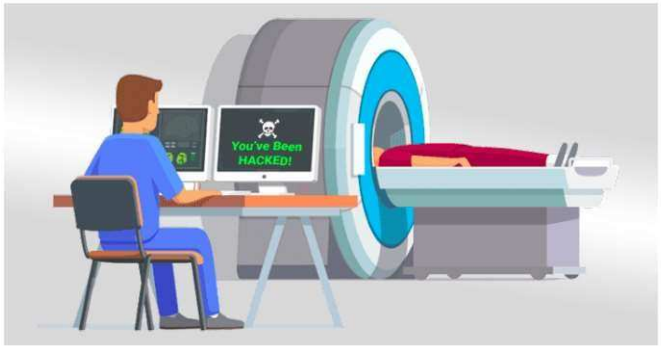
Non tutte le strutture attrezzate per sicurezza informatica

Redazione ANSA 09 novembre 2018 17:55

DALLA HOME SALUTE&BE

CYBERSECURITYITALIA

Orangeworm: nuovi at… informatici al settore sanitario degli USA, Europa e Asia

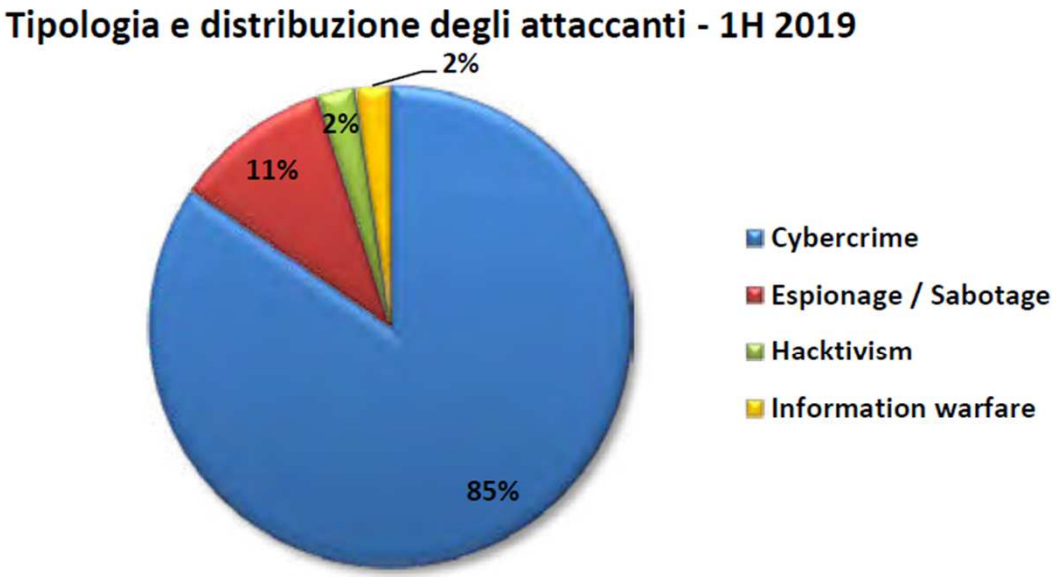


Recentemente sul blog Symantec, nella sezione di Cyber Threat

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

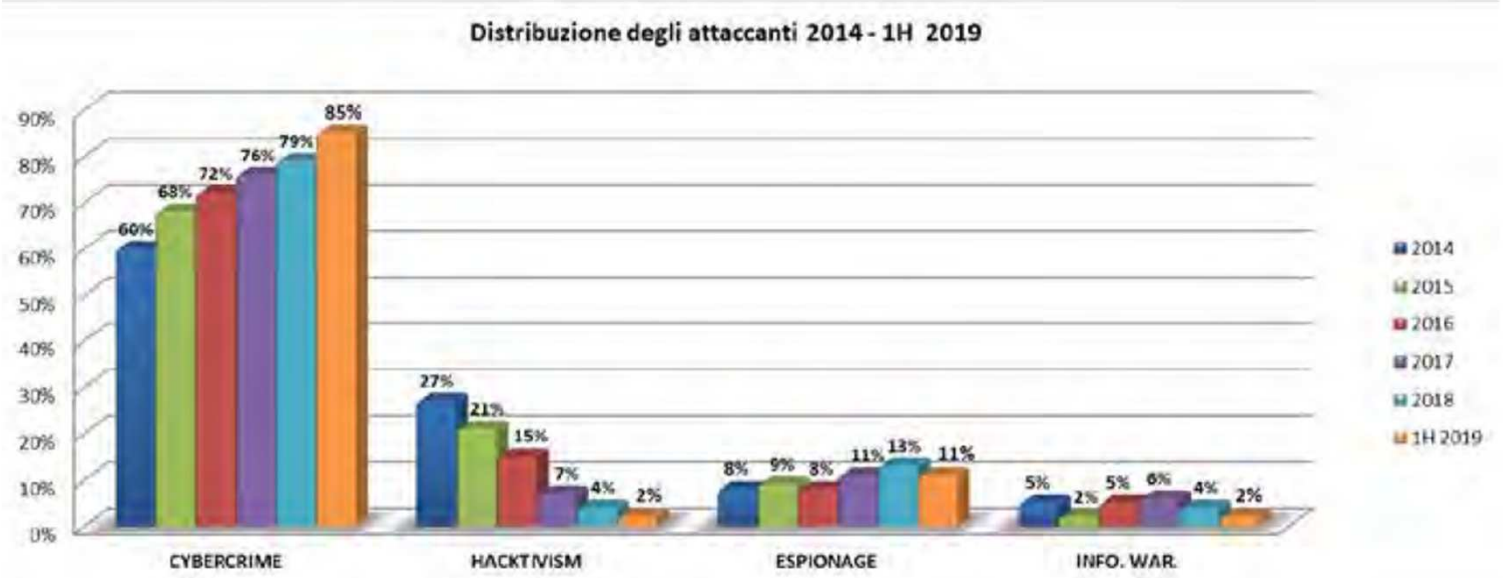
Fonte: Fortinet

Cybercrime ancora la principale fonte di incidenti



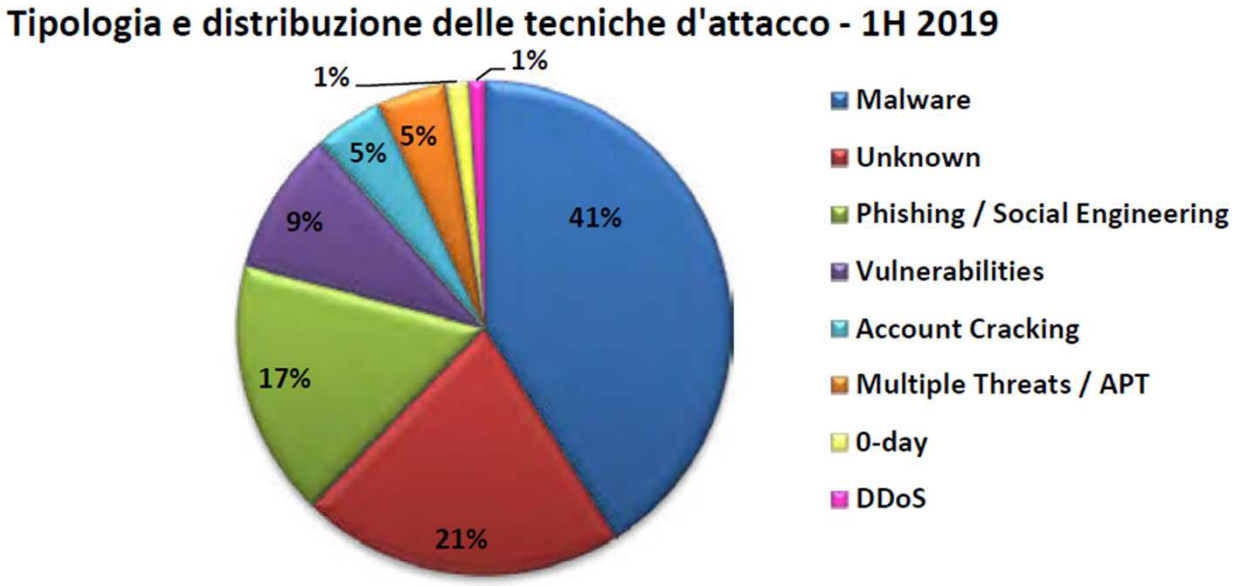
© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia - aggiornamento giugno 2019

Cyber Crime: un fenomeno in costante aumento



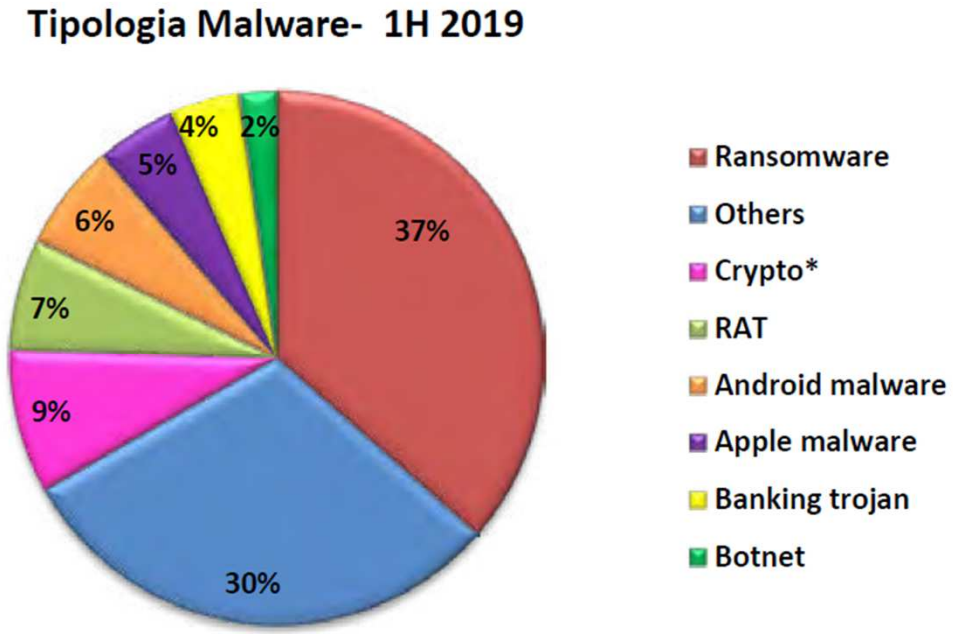
© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia - aggiornamento giugno 2019

Malware e phishing sono ancora la principale minaccia



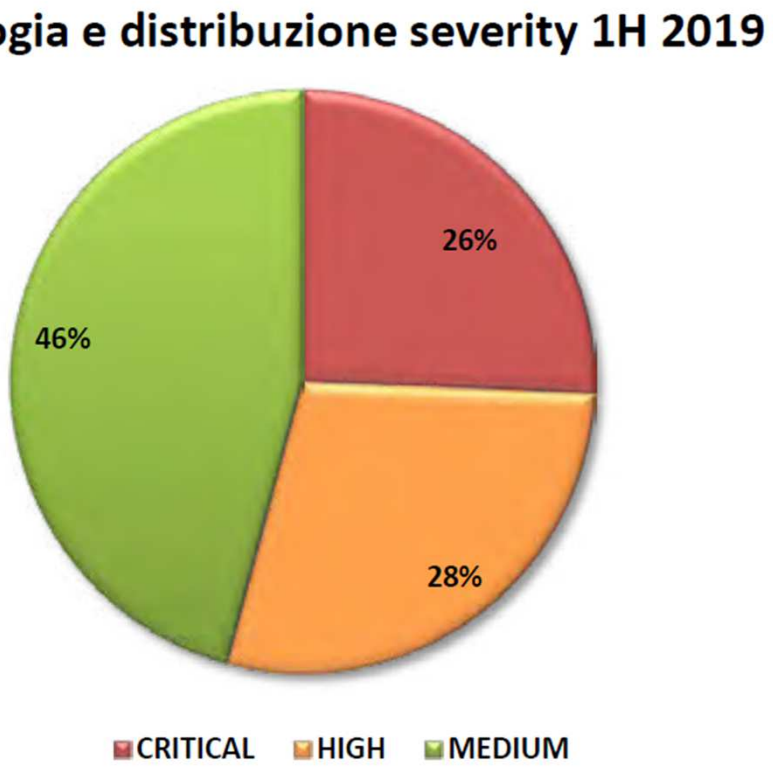
© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia - aggiornamento giugno 2019

I ransomware sono ancora una delle principali minacce



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia - aggiornamento giugno 2019

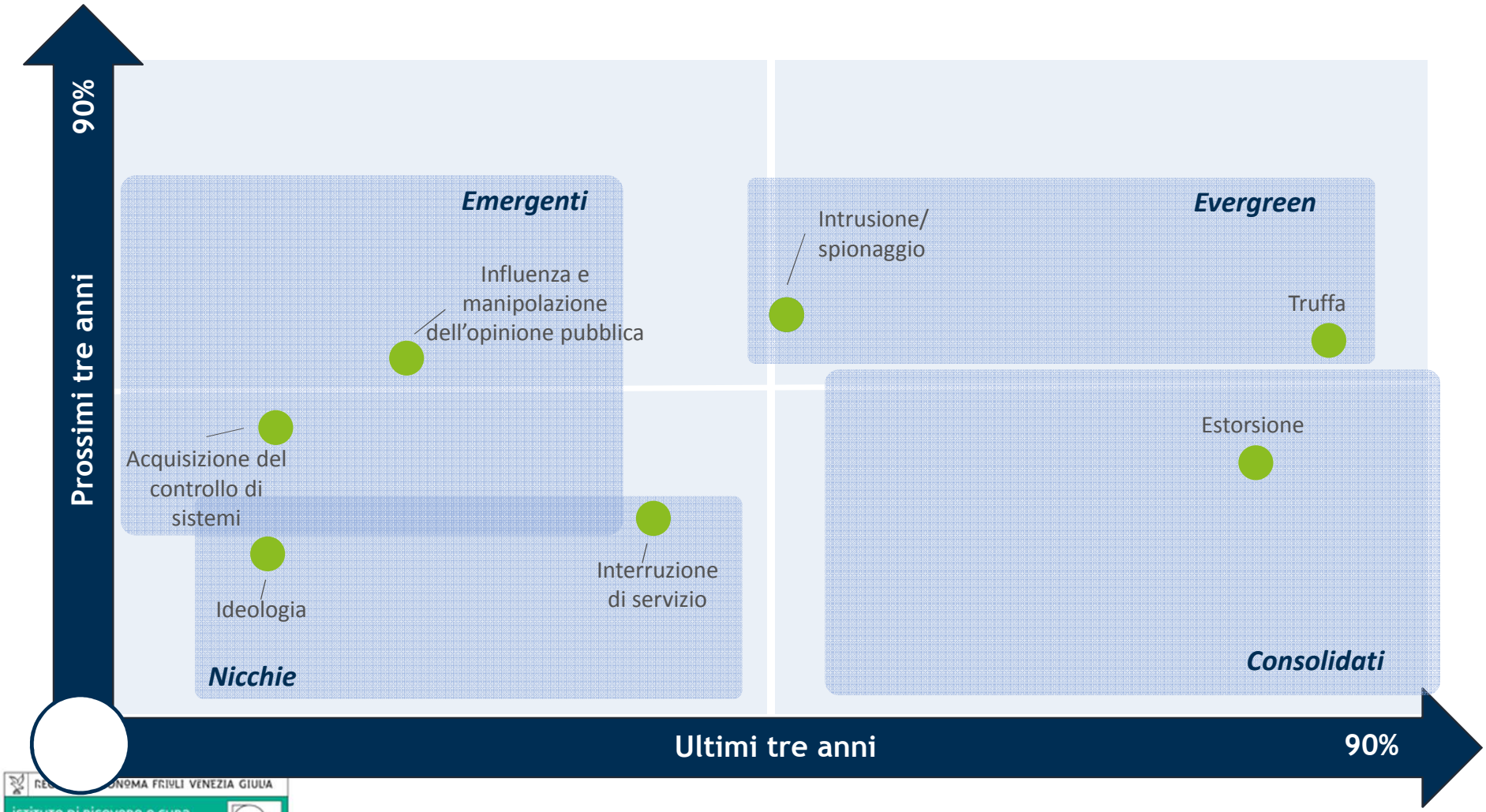
Continuiamo a gestire molti piccoli incidenti
(=molto denaro, poca consapevolezza)



© Clusit - Rapporto 2019 sulla Sicurezza ICT in Italia - aggiornamento giugno 2019

Le finalità e i target di attacco informatico

OSSERVATORI.NET digital innovation

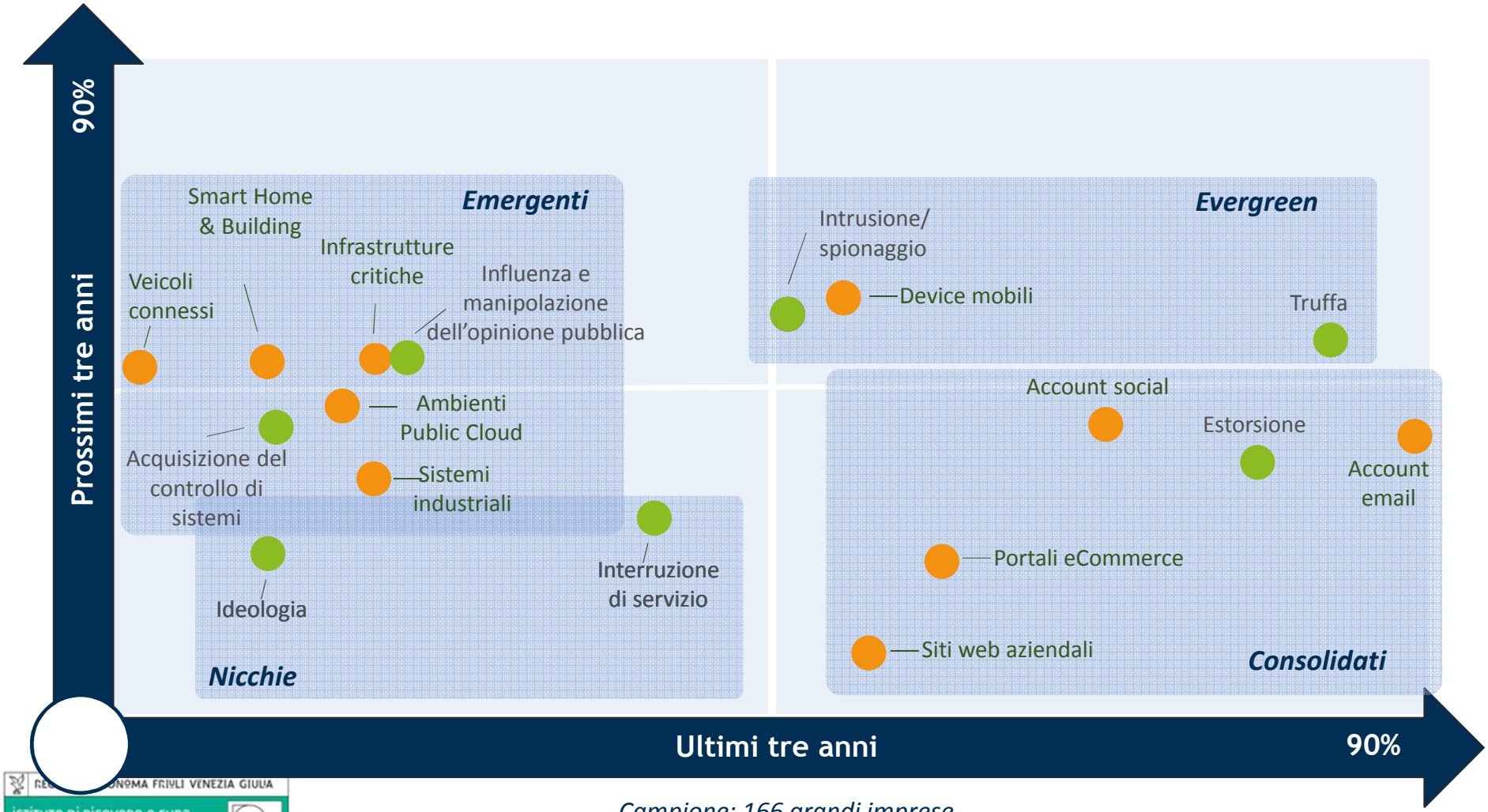


Finalità alla base di attacchi informatici

Campione: 166 grandi imprese

Le finalità e i target di attacco informatico

OSSERVATORI.NET digital innovation



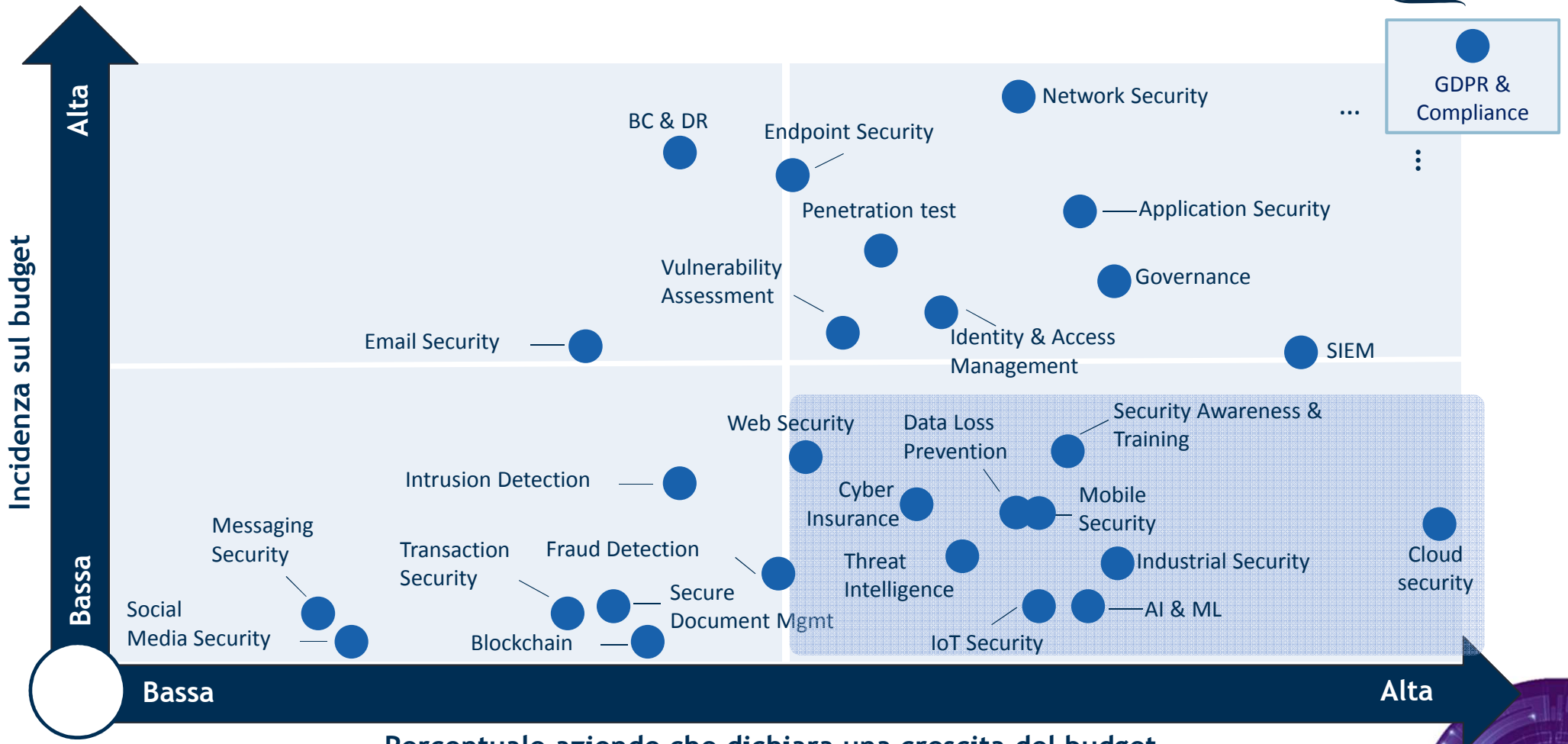
Finalità alla base di attacchi informatici

Target di attacco informatico

Campione: 166 grandi imprese

La scomposizione del mercato

OSSERVATORI.NET digital innovation



Campione: 166 grandi imprese

La figura del CISO: presenza

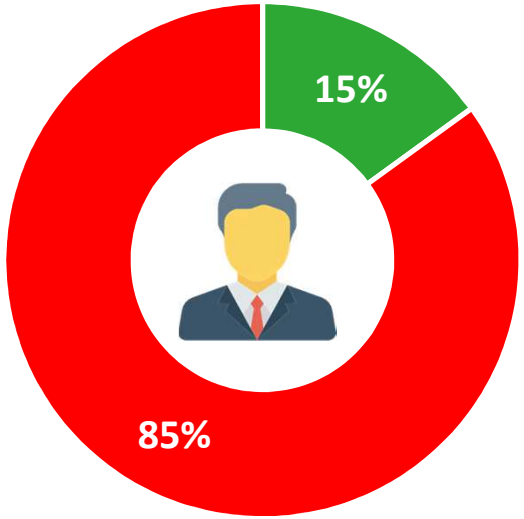
OSSERVATORI.NET digital innovation

Grandi imprese

- **47%** Presenza formale
- **12%** Presenza informale
- **30%** Responsabilità del CIO
- **7%** Responsabilità di altra funzione
- **2%** In introduzione
- **8%** Figura che si occupa sia di sicurezza fisica che logica

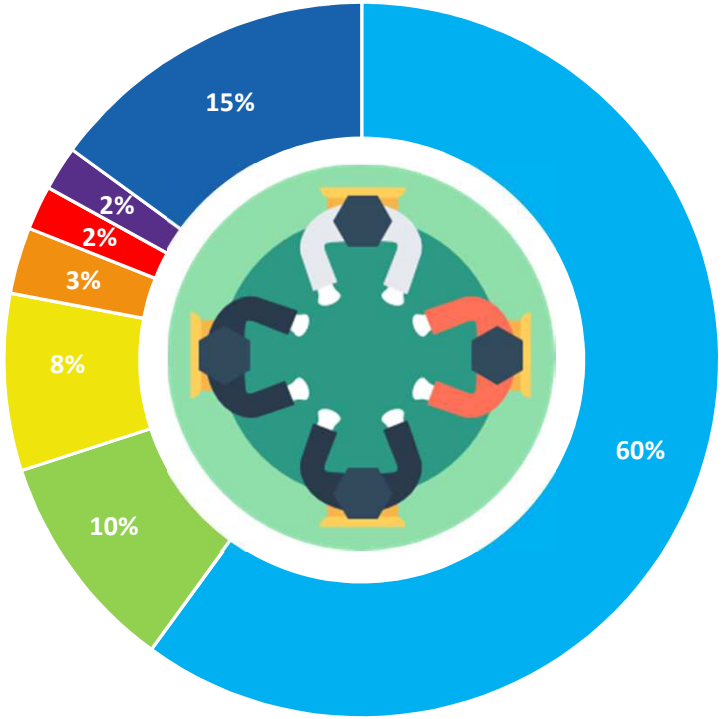
Campione: 166 grandi imprese

PMI



Dati ottenuti da un'elaborazione statistica di un campione di 501 piccole e medie imprese (addetti compresi tra 10 e 249)

La figura del CISO: posizionamento



- CIO
- Sicurezza
- Board
- Compliance e Legal
- Risk Management
- Operations
- Altro

Campione: 166 grandi imprese


CiSO
Pentester

THE TOP (WORST) PASSWORDS

RANK	PASSWORD	RANK	PASSWORD
1	123456	11	1234567
2	PASSWORD	12	MONKEY
3	12345	13	LETMEIN
4	12345678	14	ABC123
5	QWERTY	15	111111
6	123456789	16	MUSTANG
7	1234	17	ACCESS
8	BASEBALL	18	SHADOW
9	DRAGON	19	MASTER
10	FOOTBALL	20	MICHAEL

I principali fattori di rischio: l'importanza del fattore umano

OSSERVATORI.NET digital innovation

82%

Distrazione o scarsa consapevolezza dei dipendenti

41%

Obsolescenza ed eterogeneità dei sistemi IT

39%

Software update e/o patching non effettuato con regolarità

31%

Accesso in mobilità delle informazioni e dati aziendali

Campione: 166 grandi imprese

Ho chiesto a un collega…

CIS CONTROL: Un esempio di approccio pragmatico

Da https://www.cisecurity.org/controls/:

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

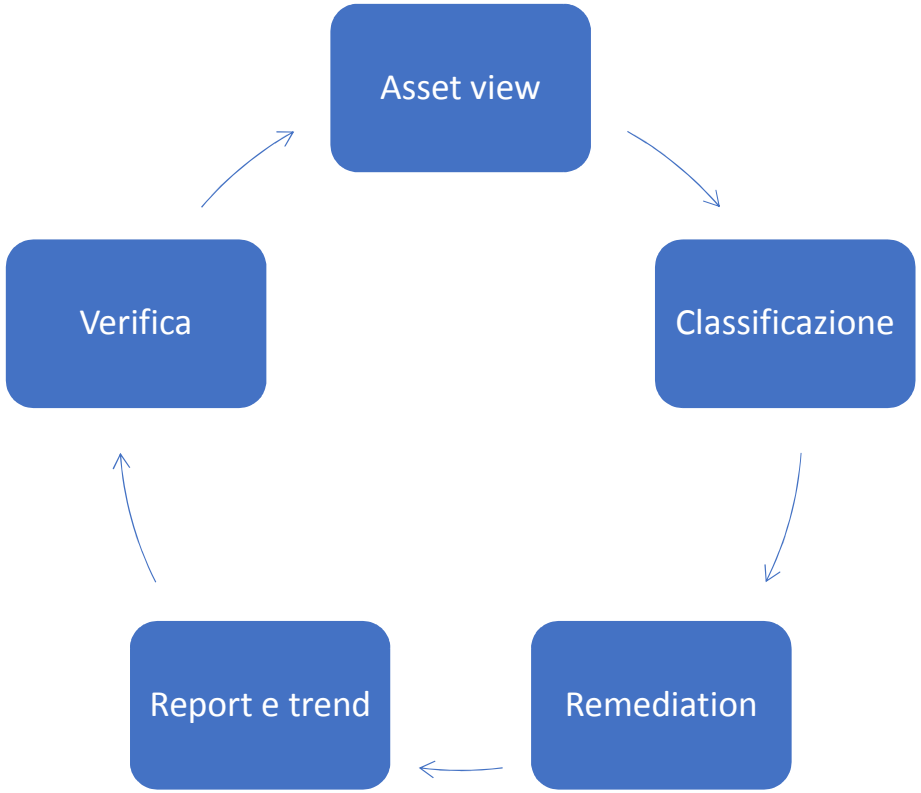
6: Maintenance, Monitoring and Analysis of Audit Logs

CONOSCERE LE VULNERABILITÀ È FONDAMENTALE

VA VS VM

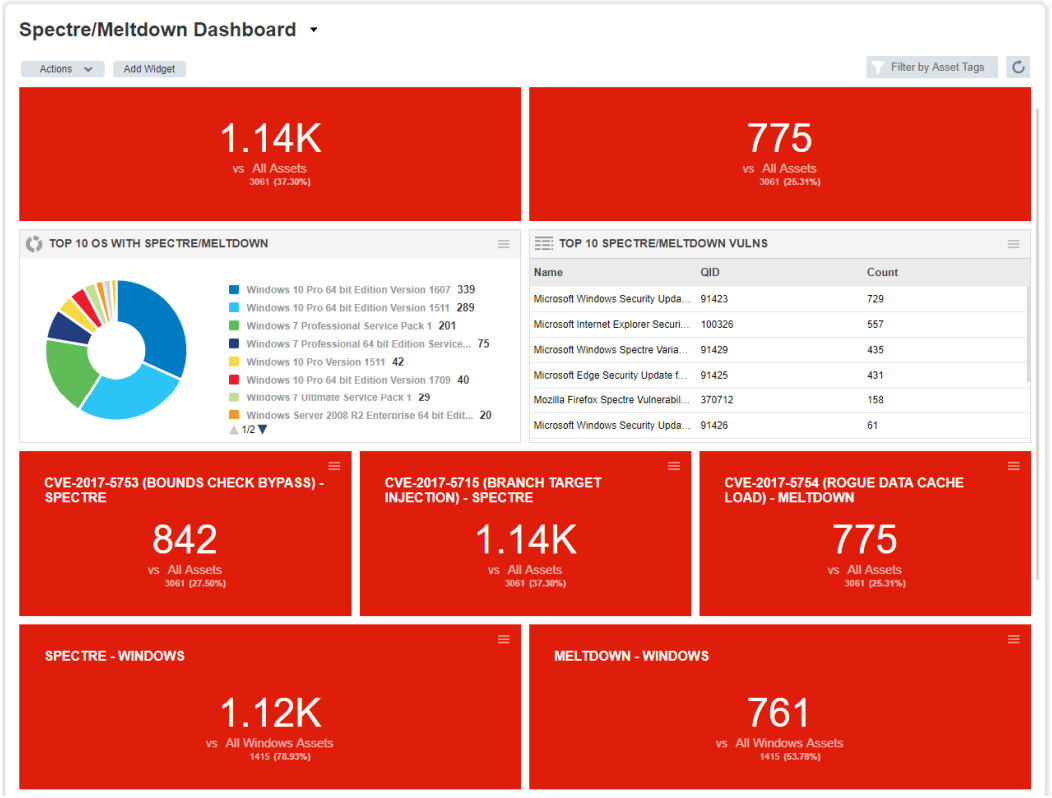
MA NON TUTTI I PROBLEMI SONO UGUALI..

DEVO DARE PRIORITÀ.. MA COME?



Importanza Asset

Facilità di Exploit


Spectre/Meltdown Dashboard
Actions
Add Widget
Filter by Asset Tags
1.14K
vs All Assets
3061 (37.30%)
775
vs All Assets
3061 (25.31%)
TOP 10 OS WITH SPECTRE/MELTDOWN
Windows 10 Pro 64 bit Edition Version 1607 339
Windows 10 Pro 64 bit Edition Version 1511 289
Windows 7 Professional Service Pack 1 201
Windows 7 Professional 64 bit Edition Service... 75
Windows 10 Pro Version 1511 42
Windows 10 Pro 64 bit Edition Version 1709 40
Windows 7 Ultimate Service Pack 1 29
Windows Server 2008 R2 Enterprise 64 bit Edit... 20
1/2
TOP 10 SPECTRE/MELTDOWN VULNS
Name QID Count
Microsoft Windows Security Upda... 91423 729
Microsoft Internet Explorer Securi... 100326 557
Microsoft Windows Spectre Varia... 91429 435
Microsoft Edge Security Update f... 91425 431
Mozilla Firefox Spectre Vulnerabil... 370712 158
Microsoft Windows Security Upda... 91426 61
CVE-2017-5753 (BOUNDS CHECK BYPASS) - SPECTRE
842
vs All Assets
3061 (27.50%)
CVE-2017-5715 (BRANCH TARGET INJECTION) - SPECTRE
1.14K
vs All Assets
3061 (37.30%)
CVE-2017-5754 (ROGUE DATA CACHE LOAD) - MELTDOWN
775
vs All Assets
3061 (25.31%)
SPECTRE - WINDOWS
1.12K
vs All Windows Assets
1415 (78.93%)
MELTDOWN - WINDOWS
761
vs All Windows Assets
1415 (53.78%)


WannaCry
Actions
Add Widget
Filter by Asset Tags
MISSING MS17-010 PATCH
292
vs All Windows Systems
1415 (20.63%)
WANNACRY RANSOMWARE DETECTED - AUTH ONLY
0
vs All Windows Systems
1415 (0.00%)
DOUBLEPULSAR BACKDOORS
0
vs All Windows Systems
1415 (0.00%)
WINDOWS HOSTS PENDING REBOOT - AUTH ONLY
121
vs All Windows Systems
1415 (8.55%)
TOP 5 OS MISSING MS17-010 PATCH
80
60
40
20
0
Windows 7 Professional Service Pack 1 67
Windows 10 Pro 64 bit Edition Version 1511 48
Windows 10 Pro 64 bit Edition Version 1607 34
Windows 7 Service Pack 1 25
Windows XP 20
Windows 7 Professio...
Windows 10 Pr...
Windows 10 Pr...
Windows 7...
Windows XP
TOP 5 EOL/OBSOLETE OPERATING SYSTEMS
Windows 10 Pro 64 bit Edition Version 1511 293
Cisco IOS 12.1 / Cisco IOS 12.2 / Cisco IOS 1... 112
Windows XP Service Pack 3 51
Windows 10 Pro Version 1511 44
Windows 7 Professional 42
SMB VERSION 1 NOT DISABLED - AUTH ONLY
1.37K
vs All Windows Systems
1415 (97.03%)
ETERNALCHAMPION - AUTH ONLY
222
vs All Windows Systems
1415 (15.68%)
ETERNALROMANCE - AUTH ONLY
222
vs All Windows Systems
1415 (15.68%)
ETERNALSYNERGY - AUTH ONLY
208
vs All Windows Systems
1415 (14.69%)
EXPLODINGCAN
2
vs All Windows Systems
1415 (0.14%)
WEBDAV NOT DISABLED [EXPLODINGCAN]
10
vs All Windows 2003 Systems
31 (32.25%)
ESTEEMAUDIT
0
vs All Windows Systems
1415 (0.00%)
ENGLISHMANDENTIST - AUTH ONLY
0
vs All Windows Systems
1415 (0.00%)

Il vulnerability management è:

- uno strumento che permette di avere visibilità in maniera continuativa di tutte le vulnerabilità presenti

- protegge da tutte le vulnerabilità
- effettua dei penetration test sulla propria infrastruttura
- impedisce il proliferarsi di un attacco che sfrutta una vulnerabilità

Grazie

enrico.benzoni@axians.it

335.6413135

Axians.it

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO