il governo della sicurezza ICT:

l'esperienza del comune di Genova

23 novembre 2017

a cura: Direzione Sistemi Informativi

CYBER SECURITY

Il governo della sicurezza ICT: l'esperienza del comune di Genova

1

Inquadramento/descrizione dell'infrastruttura ICT

- reti
- sistemi
- workstation

2

Le infrastrutture di sicurezza attuali

- Fisica: il data center
- Logica: le principali tecnologie (software) di protezione e salvaguardia dati adottate e la loro efficacia "sul campo".

3

L'impatto delle nuove direttive

- la circolare AGID (aprile 2017)

a cura: Direzione Sistemi Informativi

GENOVA
MORE THAN THIS

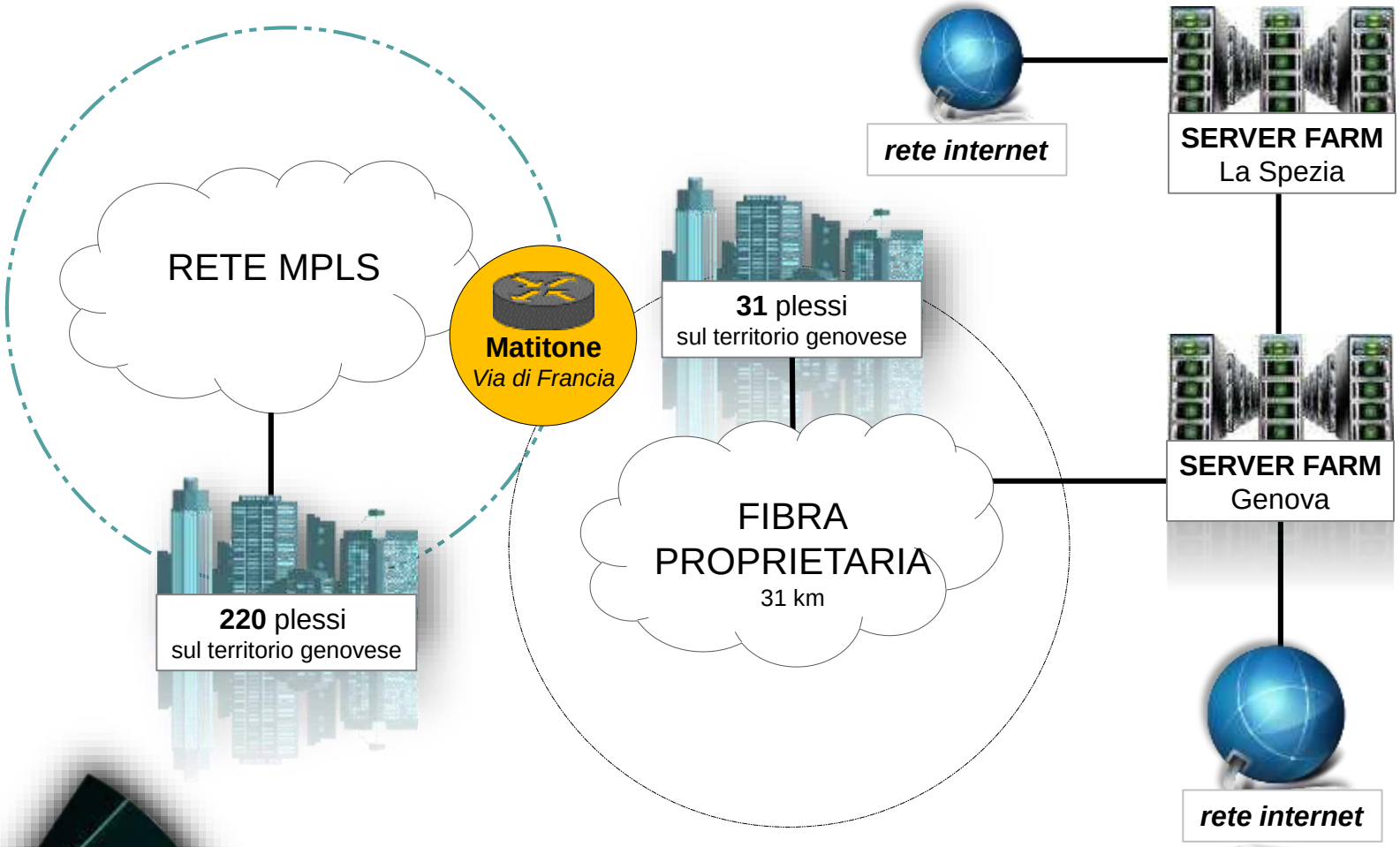
CYBER SECURITY

1

Inquadramento/descrizione dell'infrastruttura ICT

- reti
- sistemi
- workstation

Infrastrutture di rete



infrastrutture distribuita

attrezzatura

1.200 stampanti

5.150 pc / notebook

205 tablet

515 smartphone

102 telefoni voip

fonia

2023 sim — di cui

1108 servizi di fonia/dati

915 *servizi di:*
- → telecamere varchi
- → semafori
- → allarmi telecontrolli torrenti

linee telefoniche

37 centrali in rete
5.000 interni
1.000 linee di collegamento

Server farm

SISTEMI OPERATIVI

MICROSFT WINDOWS 2008 SERVER
MICROSFT WINDOWS 2012 SERVER
LINUX RED HAT
LINUX CENTOS
LINUX DEBIAN

224 TB — **SAN**

46 TB — **NAS**

Server fisici
80

Server virtuali
280

VIRTUALIZZAZIONE

VMWARE
VSPHERE

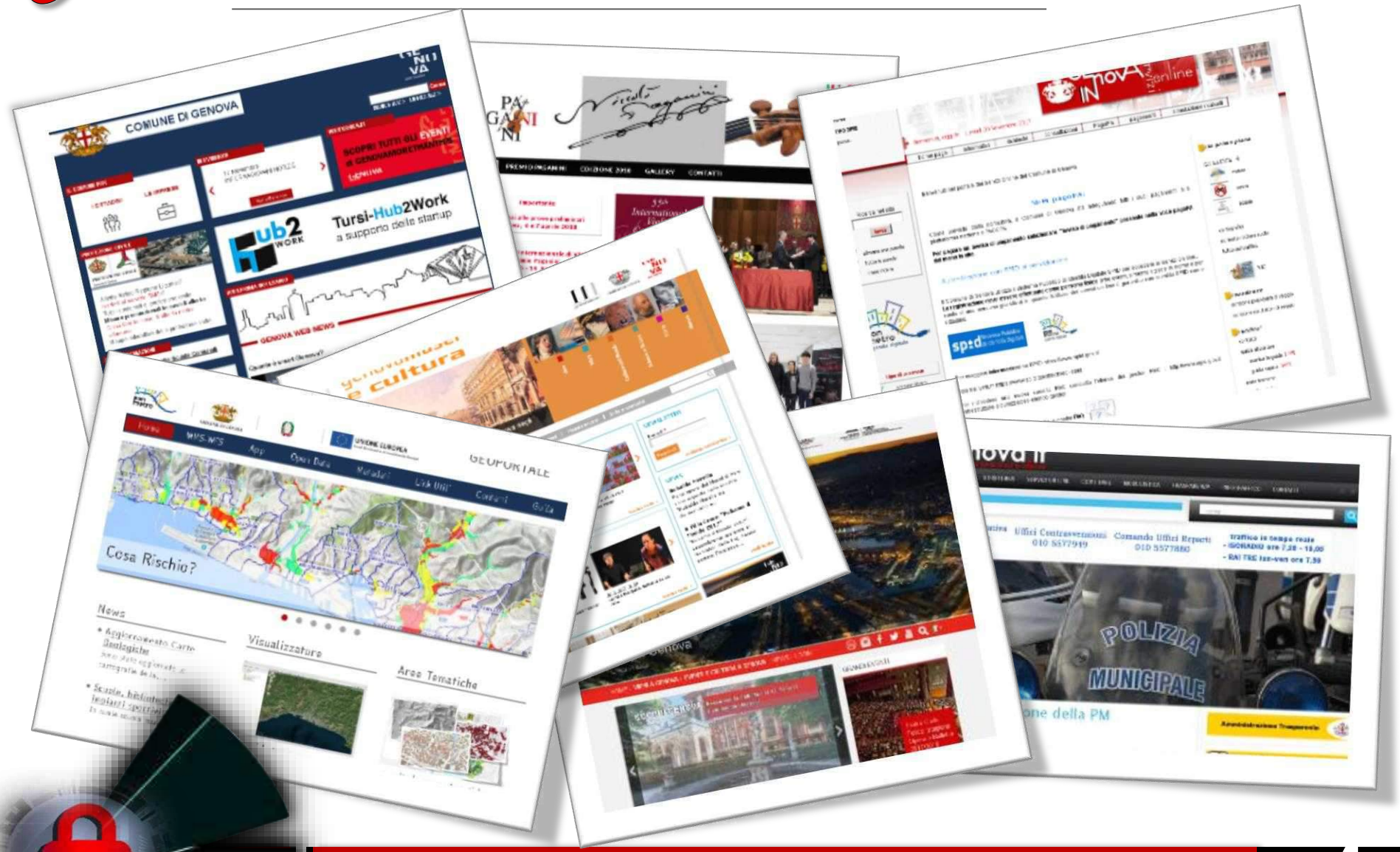
DBMS

MICROSFT SQL SERVER
ORACLE
MYSQL
POSTGRESQL

TECNOLOGIE

- BLADE SERVER
- TECNOLOGIE DI STORAGE AD ALTA AFFIDABILITÀ (RAID)
- INTERCONNESSIONI IN FIBRA OTTICA TRA SERVER E SAN
- RETE LOCALE 1 Gbps
- CONNETTIVITÀ INTERNET 1 Gbps
- CONNETTIVITÀ INTRANET 1 Gbps e 10 Gbps

Oltre 140 siti di informazione e servizi



270 access point installati

Il servizio FreeWiFiGenova non ha limiti di orario giornalieri
il singolo utente può navigare fino ad un massimo di 300 MB giornalieri.

In via di realizzazione l'integrazione con:

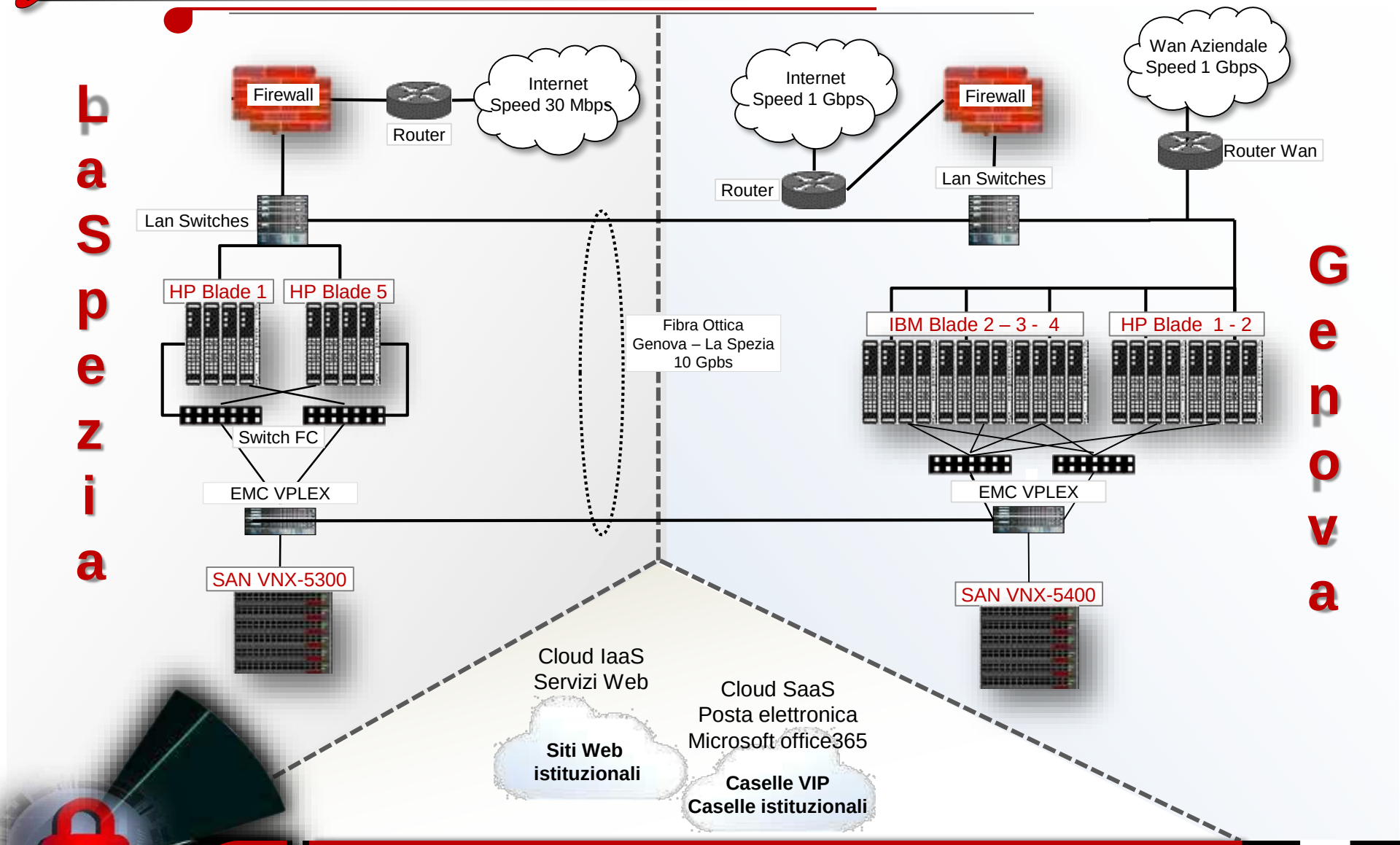
spid Sistema Pubblico di Identità Digitale

La rete di telecamere per la sicurezza urbana

299 apparati video

- **38** per gestire il traffico
- **248** per la sicurezza del territorio
- **13** per controllare il livello dei torrenti

I percorso verso la Business continuity



CYBER SECURITY

2

Le infrastrutture di sicurezza attuali

- Fisica: il data center del Comune
- Logica: le principali tecnologie (software) di protezione e salvaguardia dati adottate e la loro efficacia "sul campo".

l'obiettivo: sicurezza ICT

proteggere il patrimonio informativo dell'Ente

Sicurezza Fisica

tutela delle infrastrutture ICT dell'Ente

Sicurezza Logica

tecniche di difesa dai Cyber attacchi, le soluzioni adottate

Sicurezza fisica

Il Datacenter di Liguria Digitale

CARATTERISTICHE

- Accesso ai locali del Data Center presidiato e videosorvegliato
- Partizionamento locali per funzione / azienda
- Impianto di Videosorveglianza
- Sistemi anti-intrusione anti-allagamento anti-incendio
- Tecniche di spegnimento incendi a gas inerte
- Gruppi di continuità statici a batterie e dinamici (moto-generatori Diesel)
- Backup dati su sistemi multipli localizzati in aree diverse distanti tra loro
- Presenza di armadi ignifughi per la protezione dei supporti di backup

Sicurezza logica

TECNOLOGIE UTILIZZATE

Sicurezza perimetrale:	Sicurezza email:	Sicurezza navigazione:	Sicurezza Endpoint:	Controllo vulnerabilità
firewall/IPS	**tecnologie antispam**	**web & content security**	**sistemi antivirus**	**vulnerability scanner**

Sicurezza logica

tecniche di difesa e prevenzione

IL Firewall perimetrale,
una tecnologia in costante evoluzione

I cardini per una difesa efficace

- Deep Packet Inspection
- Tecnologie IPS *(Intrusion Prevention system)*
- Log del traffico

Sicurezza logica

i logs del firewall

valutare l'efficacia delle regole

2535790	30Oct2017	12:27:23	192.168....	TCP	http	172.19.2...	192.168....	68	68-Standard	52859	inzone: Internal; outzone: Internal; service_id: http
2535791	30Oct2017	12:27:23	192.168....	UDP	domain-udp	172.19.6...	192.168....	5	5-Standard	44668	inzone: Internal; outzone: Internal; service_id: domain-udp
2535792	30Oct2017	12:27:23	192.168....	UDP	nbname	192.168....	192.168....	68	68-Standard	nbname	inzone: Internal; outzone: Local; service_id: nbname
2535793	30Oct2017	12:27:23	192.168....	UDP	snmp	172.19.4...	172.19.1...	68	68-Standard	3561	inzone: Internal; outzone: Internal; service_id: snmp
2535794	30Oct2017	12:27:23	192.168....	TCP	http	88.37.15...	93.62.17...	18	18-Standard	59856	inzone: External; outzone: Internal; service_id: http
2535795	30Oct2017	12:27:23	192.168....	UDP	nbname	192.168....	192.168....	68	68-Standard	nbname	inzone: Internal; outzone: Local; service_id: nbname
2535796	30Oct2017	12:27:23	192.168....	TCP	https	192.168....	192.168....	32	32-Standard	53006	inzone: Internal; outzone: Internal; service_id: https
2535797	30Oct2017	12:27:23	192.168....	TCP	https	192.168....	104.94.3...	68	68-Standard	49541	inzone: Internal; outzone: External; service_id: https
2535798	30Oct2017	12:27:23	192.168....	TCP	https	192.168....	192.168....	32	32-Standard	53008	inzone: Internal; outzone: Internal; service_id: https
2535799	30Oct2017	12:27:23	192.168....	UDP	snmp	172.19.4...	192.168....	68	68-Standard	3562	inzone: Internal; outzone: Internal; service_id: snmp
2535800	30Oct2017	12:27:23	192.168....	UDP	8116		192.168....	71	71-Standard	8116	inzone: Internal; outzone: Local
2535801	30Oct2017	12:27:23	192.168....	TCP	http	192.168....	192.168....	68	68-Standard	51238	inzone: Internal; outzone: Internal; service_id: http
2535802	30Oct2017	12:27:23	192.168....	TCP	9009	188.166....	93.62.17...	71	71-Standard	51150	inzone: External; outzone: Local

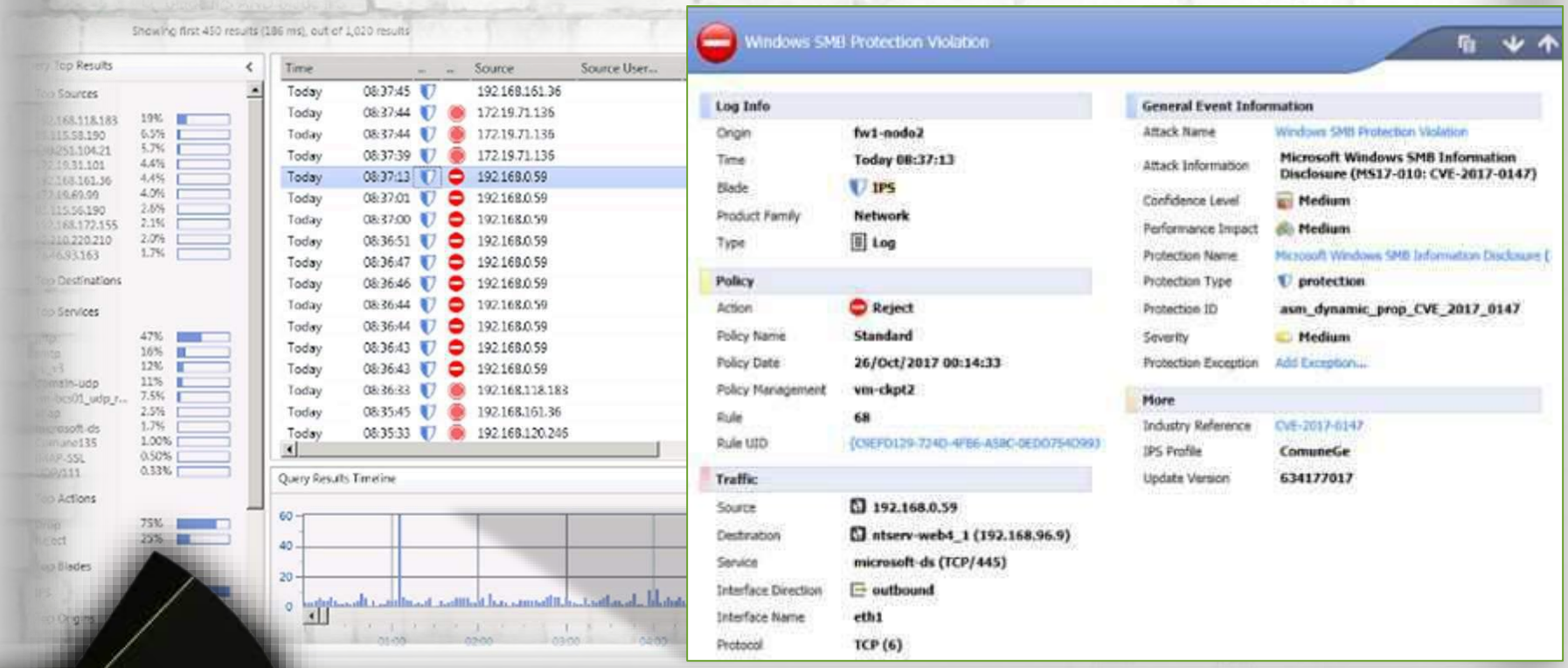
IMAP-SSL 172.19.7... 17.133.2... 65233 TCP packet out of state: First packet isn't SYN; tcp_flags:FIN-PUSH

2535807	30Oct2017	12:27:23	192.168....	TCP	http	5.170.31....	93.62.17...	18	18-Standard	2993	inzone: External; outzone: Internal; service_id: http
2535808	30Oct2017	12:27:23	192.168....	TCP	http	192.168....	192.168....	68	68-Standard	59698	inzone: Internal; outzone: Internal; service_id: http
2535809	30Oct2017	12:27:23	192.168....	TCP	http	95.251.1...	93.62.17...	18	18-Standard	56696	inzone: External; outzone: Internal; service_id: http
2535810	30Oct2017	12:27:23	192.168....	TCP	IMAP-SSL	172.19.7...	17.133.2...			65232	TCP packet out of state: First packet isn't SYN; tcp_flags: FIN-PUSH
2535811	30Oct2017	12:27:23	192.168....	TCP	http	5.170.31....	93.62.17...	18	18-Standard	2329	inzone: External; outzone: Internal; service_id: http
2535812	30Oct2017	12:27:23	192.168....	TCP	IMAP-SSL	172.19.7...	17.133.2...			65233	TCP packet out of state: First packet isn't SYN; tcp_flags: FIN-PUSH
2535813	30Oct2017	12:27:23	192.168....	TCP	9009	188.166....	93.62.17...	71	71-Standard	51248	inzone: External; outzone: Local
2535814	30Oct2017	12:27:23	192.168....	UDP	domain-udp	172.19.7...	8.8.8.8	5	5-Standard	54833	inzone: Internal; outzone: External; service_id: domain-udp
2535815	30Oct2017	12:27:23	192.168....	TCP	https	5.170.31....	93.62.17...	20	20-Standard	44604	inzone: External; outzone: Internal; service_id: https
2535816	30Oct2017	12:27:23	192.168....	UDP	nbname	192.168....	192.168....	68	68-Standard	nbname	inzone: Internal; service_id: nbname
2535817	30Oct2017	12:27:23	192.168....	UDP	snmp	172.19.4...	192.168....	68	68-Standard	3563	inzone: Internal; outzone: Internal; service_id: snmp
2535818	30Oct2017	12:27:23	192.168....	UDP	snmp	172.19.4...	172.19.2...	68	68-Standard	3564	inzone: Internal; outzone: Internal; service_id: snmp
2535819	30Oct2017	12:27:23	192.168....	TCP	http	95.242.6...	93.62.17...	18	18-Standard	50160	inzone: External; outzone: Internal; service_id: http
2535820	30Oct2017	12:27:23	192.168....	TCP	https	192.168....	52.164.2...	68	68-Standard	41851	inzone: Internal; outzone: External; service_id: https
2535821	30Oct2017	12:27:23	192.168....	TCP	http	5.170.31....	93.62.17...	18	18-Standard	2084	inzone: External; outzone: Internal; service_id: http
2535822	30Oct2017	12:27:23	192.168....	TCP	http	95.251.1...	93.62.17...	18	18-Standard	60540	inzone: External; outzone: Internal; service_id: http

Sicurezza logica

i logs del firewall

i filtri IPS e Wannacry

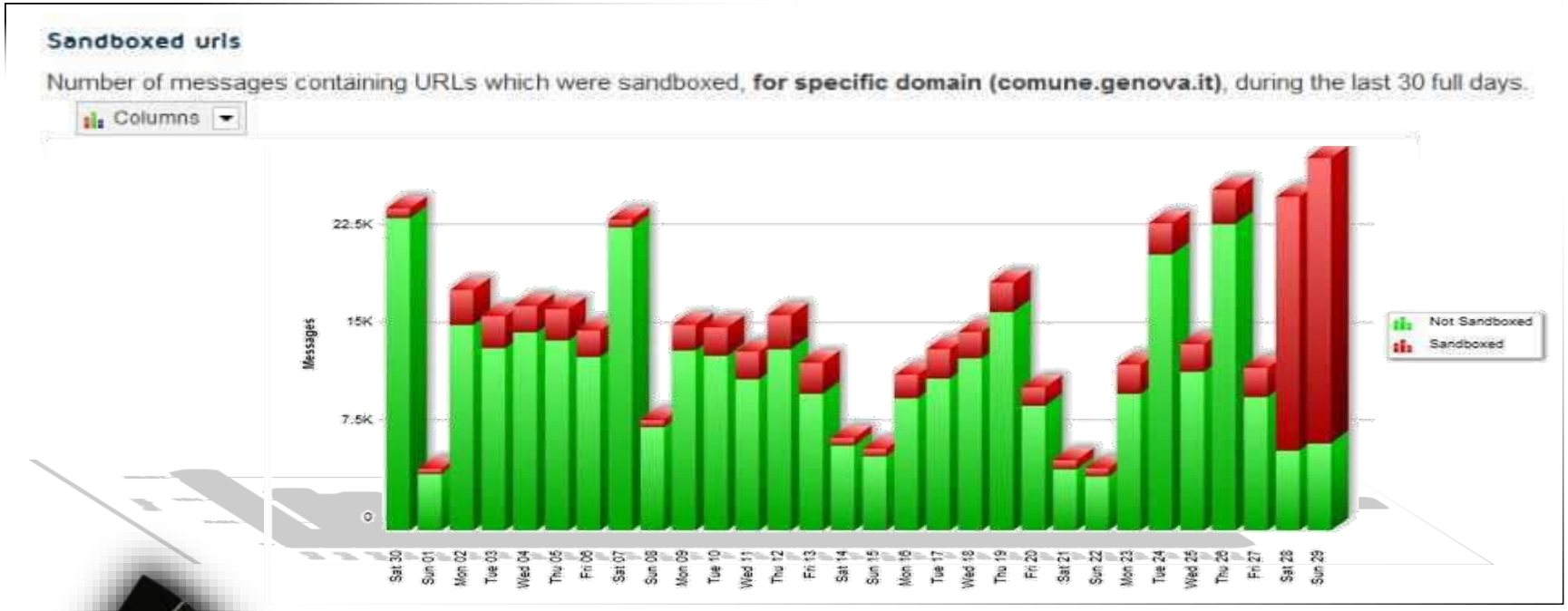


tecniche antispam

Email come veicolo della minaccia cibernetica	la soluzione Forcepoint Email Security Cloud: le sue peculiarità
÷ Phishing ÷ Virus ÷ Spam	÷ Possibilita' di individuare e bloccare allegati potenzialmente pericolosi ÷ Efficace nell'individuazione di spam & phishing ÷ Url Sandboxing ÷ Web Security integration

Forcepoint Email Security Cloud

URL SANDBOXING

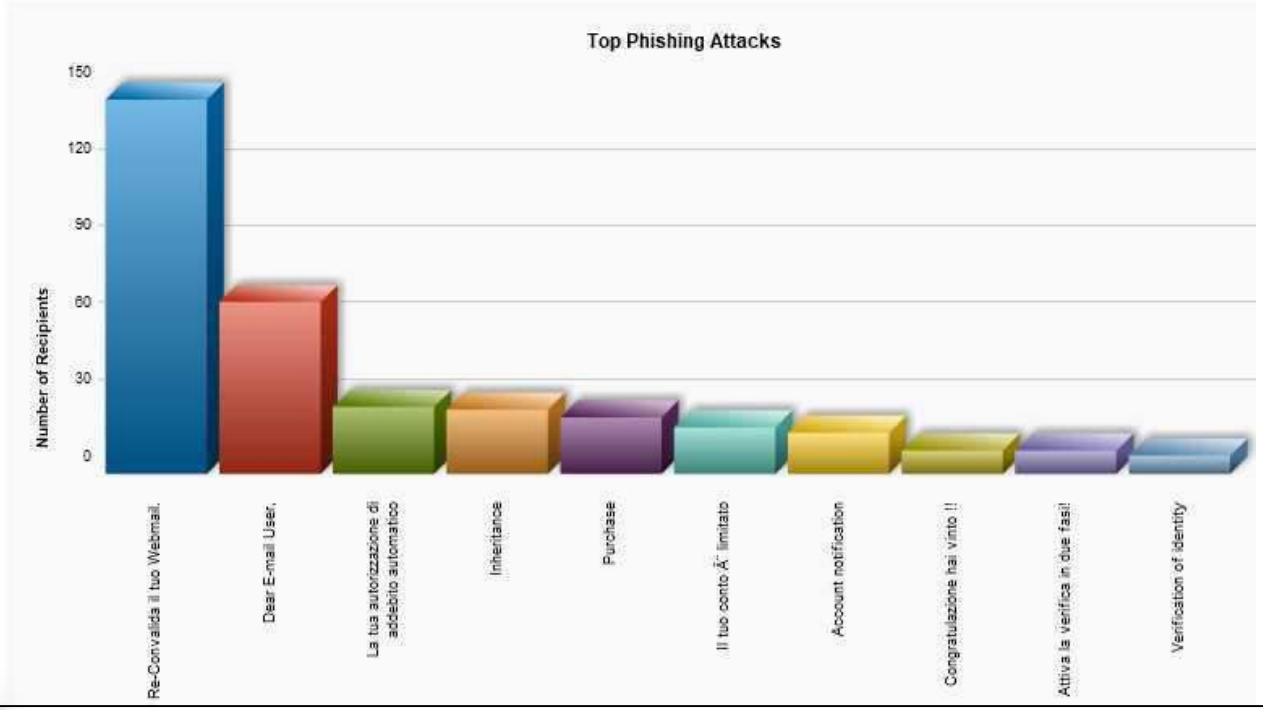


Forcepoint Email Security Cloud

tentativi di phishing

Top Phishing Attacks

Top phishing topics by number of recipients, **for specific domain (comune.genova.it)**, during the last 30 full days.
Click on a message subject to view actions performed by users on that email



Sicurezza logica

usare internet in sicurezza

Tecnologie web di content filtering

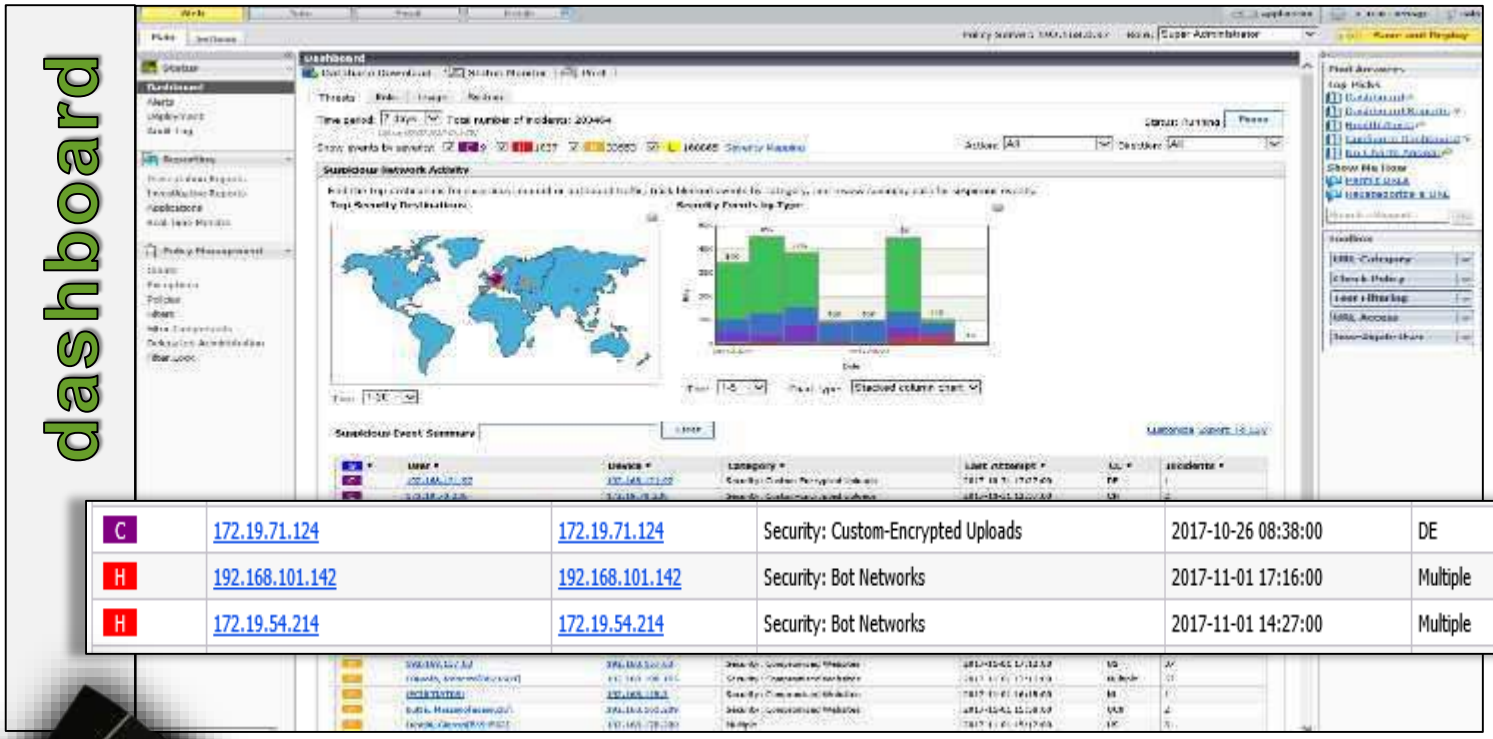
- ✓ Advanced Classification Engine (ACE)
- ✓ Analisi in tempo reale delle potenziali minacce
- ✓ Ampia categorizzazione dei siti web *(circa 120 categorie)*

- ✓ Classificazione della sicurezza in tempo reale
- ✓ Classificazione dei contenuti in tempo reale

Sicurezza logica

Forcepoint Triton APX

dashboard



C	172.19.71.124	172.19.71.124	Security: Custom-Encrypted Uploads	2017-10-26 08:38:00	DE	3
H	192.168.101.142	192.168.101.142	Security: Bot Networks	2017-11-01 17:16:00	Multiple	836
H	172.19.54.214	172.19.54.214	Security: Bot Networks	2017-11-01 14:27:00	Multiple	174

Sicurezza logica

antivirus aziendale

il presidio sugli ENDPOINT

TrendMicro Officescan XG – caratteristiche:

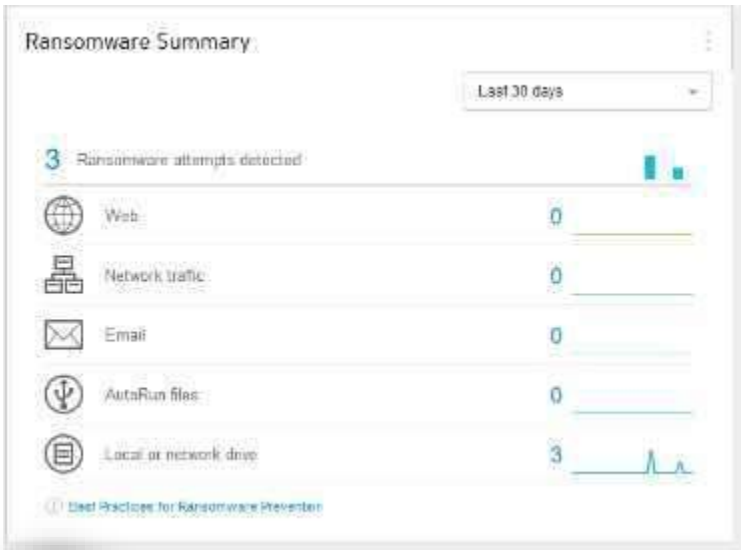
- Tecniche di Machine learning
- Analisi del comportamento *(contro script, injection, ransomware, attacchia memoria e browser)*
- Reputazione dei siti Web
- Reputazione dei file

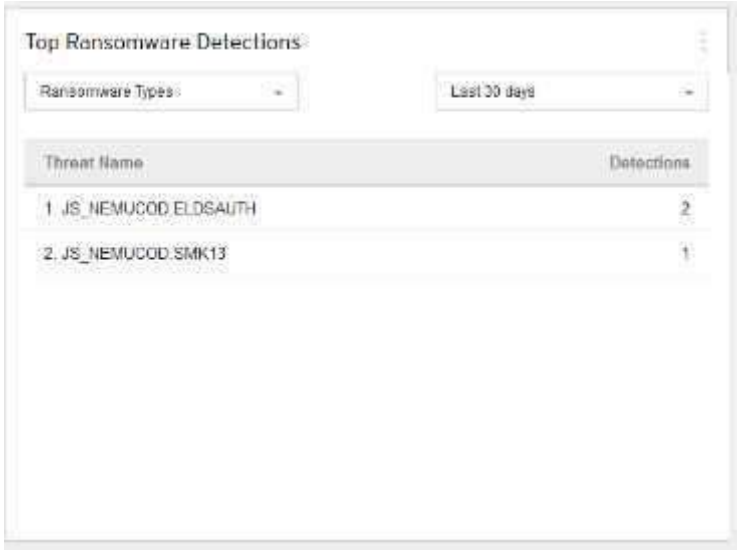
Gartner Group

Sicurezza logica

TrendMicro Officescan XG

I Widget specializzati sulla minaccia Ransonware:
Efficacia dei meccanismi di rilevazione





I test periodici di vulnerabilità

Il tool utilizzato:
NESSUS vulnerability scanner

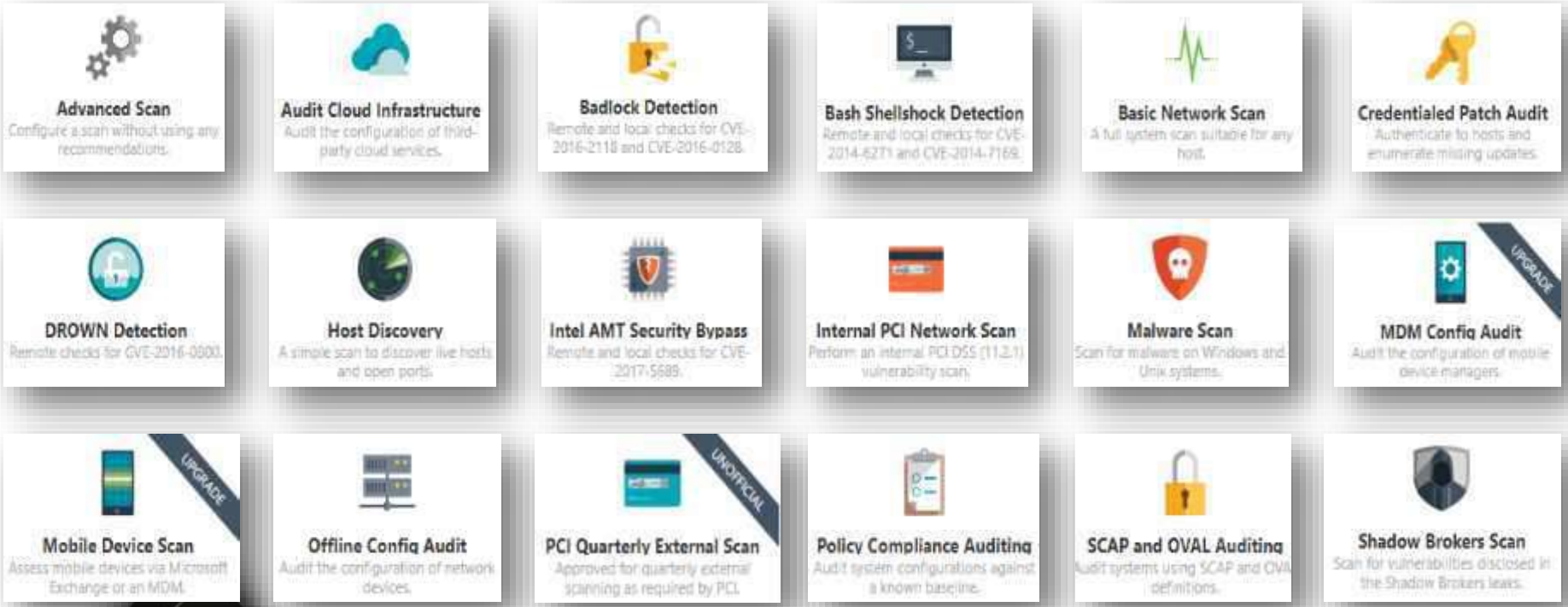
caratteristiche

- Database delle vulnerabilità costantemente aggiornato
- Riconoscimento avanzato dei servizi
- Indicazione delle risoluzioni piu' adatte in funzione della vulnerabilità rilevate
- Reporting dettagliato
- Scheduler automatizzato delle scansioni
- Console di gestione Web-based

Sicurezza logica

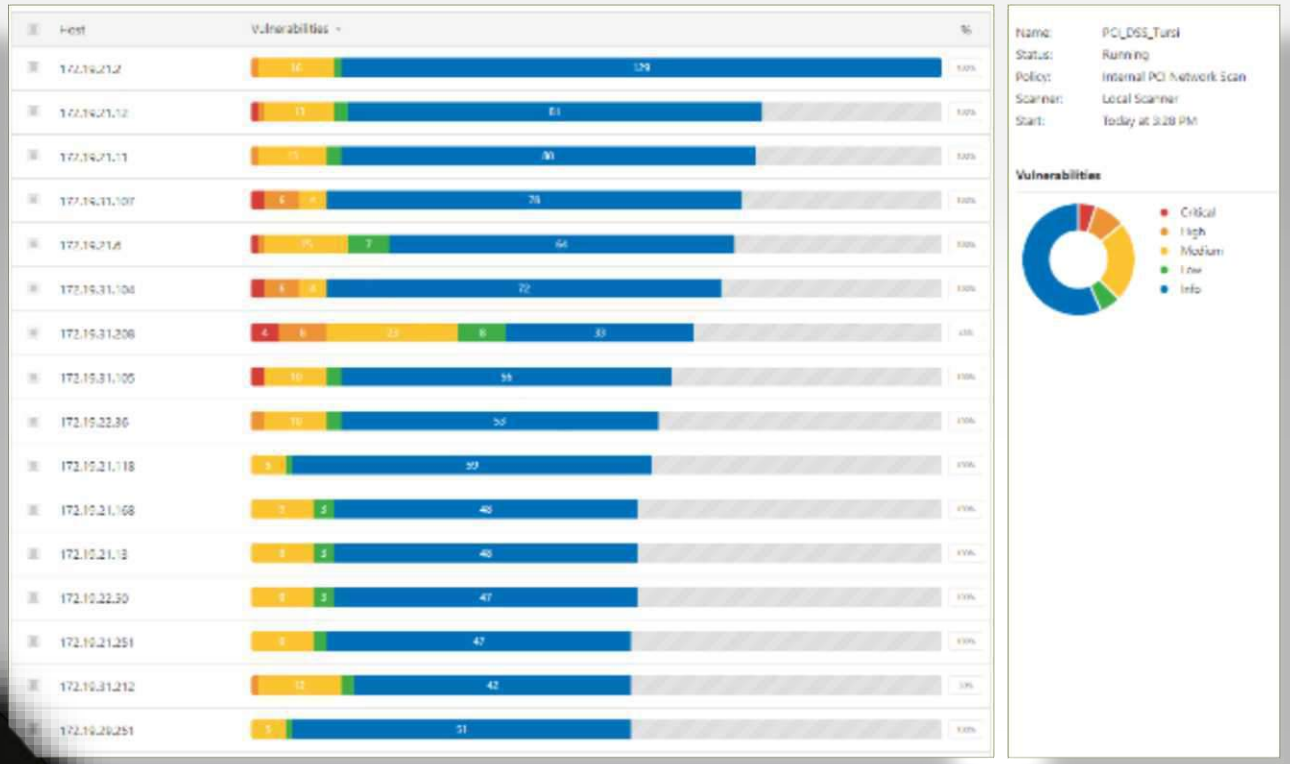
Nessus vulnerability scanner

Scan templates



Nessus vulnerability scanner

Scansione PCI DSS: i risultati



CYBER SECURITY

3

L'impatto delle nuove direttive

- la circolare AGID (aprile 2017)

percorso attuativo

→ **agosto 2015**

Direttiva del Presidente del Consiglio dei Ministri che emana disposizioni finalizzate a consolidare lo stato della sicurezza informatica nazionale, alla luce dei crescenti rischi cibernetici che minacciano anche il nostro Paese; La direttiva assegna all'Agenzia per l'Italia Digitale il compito di sviluppare e rendere disponibili "indicatori degli standard di riferimento" che mettano le amministrazioni in grado di dotarsi degli standard minimi di prevenzione e reazione ad eventi cibernetici.

→ **settembre 2016**

pubblicazione documento con le Misure minime reso disponibile da AgID e dal CERT-PA.

→ **18 aprile 2017**

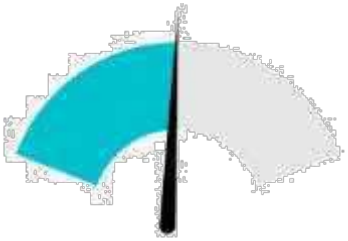
pubblicazione in Gazzetta Ufficiale circolare n. 2/2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni.

le categorie

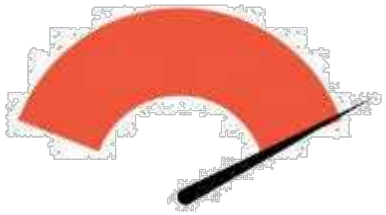
- Inventario dei dispositivi autorizzati e non autorizzati
- Inventario del software autorizzato e non autorizzato
- Configurazione sicura di hardware e software
- Adozione di un processo di gestione delle vulnerabilità
- Capacità di recuperare l'operatività in caso di incidente (ovvero Business Continuity)
- Adozione di difese contro i programmi malware
- Utilizzo controllato dei privilegi amministrativi
- Protezione dei dati

i livelli di adeguamento previsti

minimo
ovvero il livello al di sotto del quale il rischio è ritenuto inaccettabile



standard
ovvero il livello ottimale verso cui tutta la PA dovrebbe tendere



alto
livello di pertinenza degli Enti coinvolti nel processo di gestione della sicurezza nazionale.

ricadute organizzative

ABSC_ID			Livello	Descrizione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica

Grazie per l'attenzione

«Poiché il sistema sicuro non esiste, bisogna sempre diffidare di colui che afferma che i suoi sistemi sono assolutamente sicuri, perché non conosce la sicurezza oppure è semplicemente un folle».

Eugene "Spaf" Spafford
Professore di Informatica alla Purdue University
ed esperto di sicurezza informatica

a cura: Direzione Sistemi Informativi

GENOVA
MORE THAN THIS