CITTA' DI TORINO

Cybersecurity

Città di Torino

21 Febbraio 2022

Il Piano Triennale AgID 2022 – Focus Sicurezza

L' esigenza per la PA di contrastare le minacce informatiche è fondamentale in quanto garantisce non solo la disponibilità, l'integrità e la riservatezza delle informazioni proprie del Sistema informativo della Pubblica Amministrazione, ma è il presupposto per la protezione del dato che ha come conseguenza diretta l'aumento della fiducia nei servizi digitali erogati dalla PA.

OBIETTIVI DEL Cap. 6

1. Aumentare la **consapevolezza del rischio cyber** (Cyber Security Awareness) nelle PA

2. Aumentare il livello di **sicurezza informatica dei portali istituzionali** della Pubblica Amministrazione

RISULTATI ATTESI

- ❑ Incremento del livello di Cyber Security Awareness nella PA

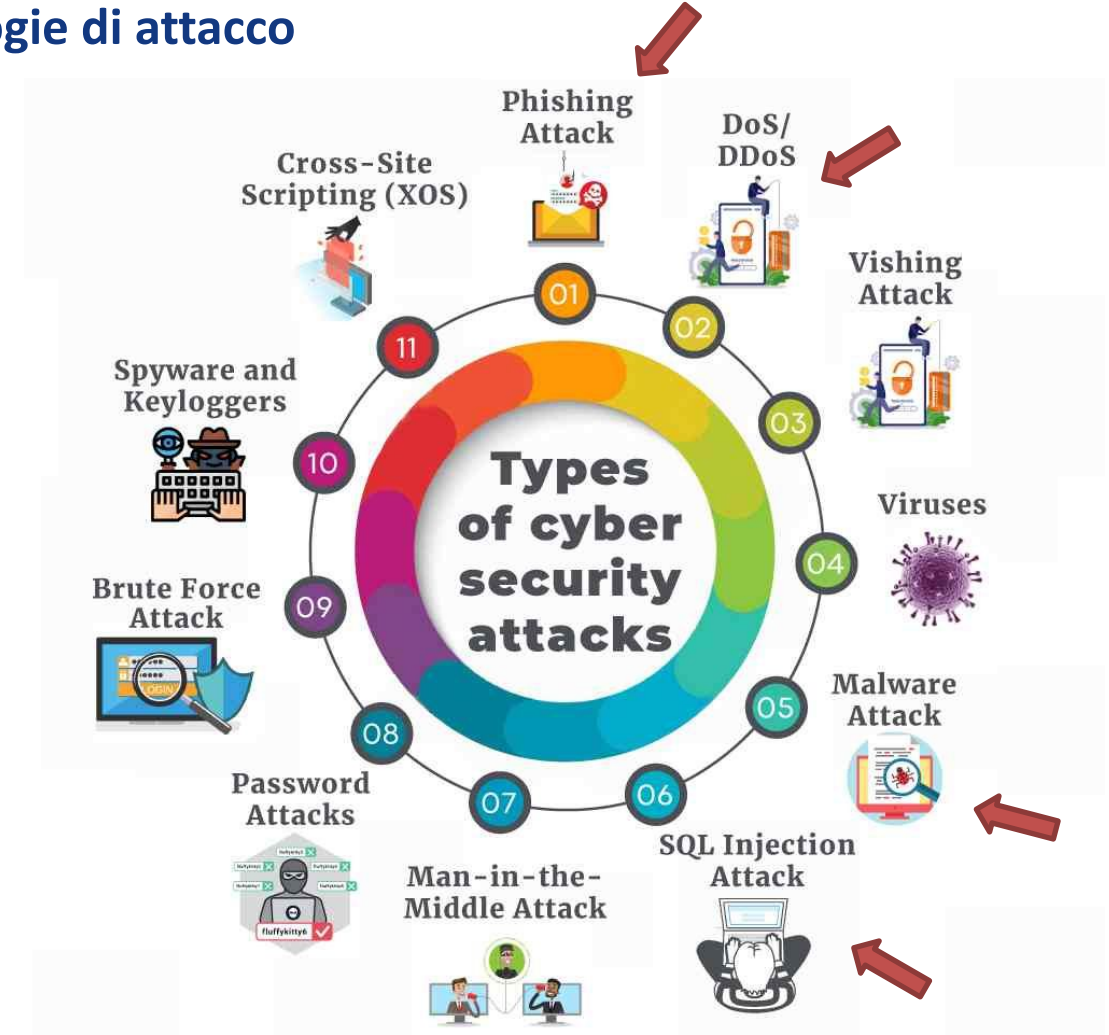
- ❑ Incremento del numero dei portali istituzionali che utilizzano il protocollo HTTPS only
- ❑ Massimizzazione del numero dei Content Management System (CMS) non vulnerabili utilizzati nei portali istituzionali delle PA

Le minacce e le tipologie di attacco

…ma non solo:

Mail-bombing
Defacement
Truffe Informatiche
Scan Massivi Vulnerabilità
Penetration Test (veri o falsi!!)

Attacchi più frequenti



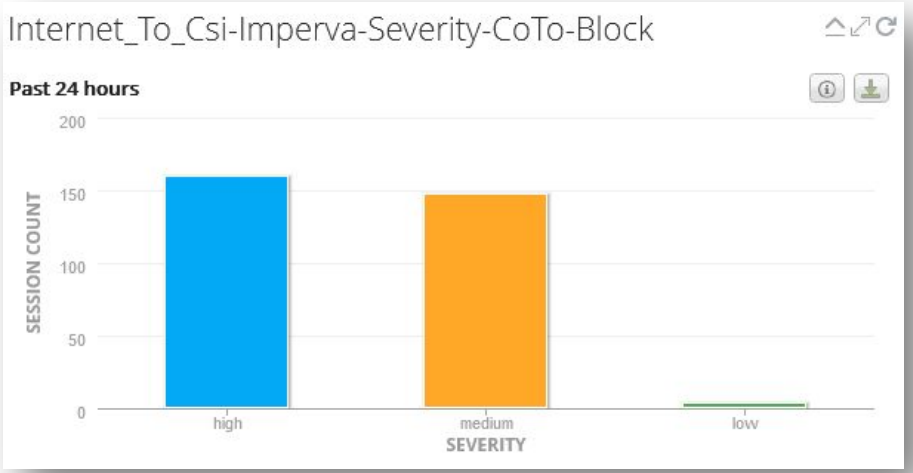
I numeri del 2021

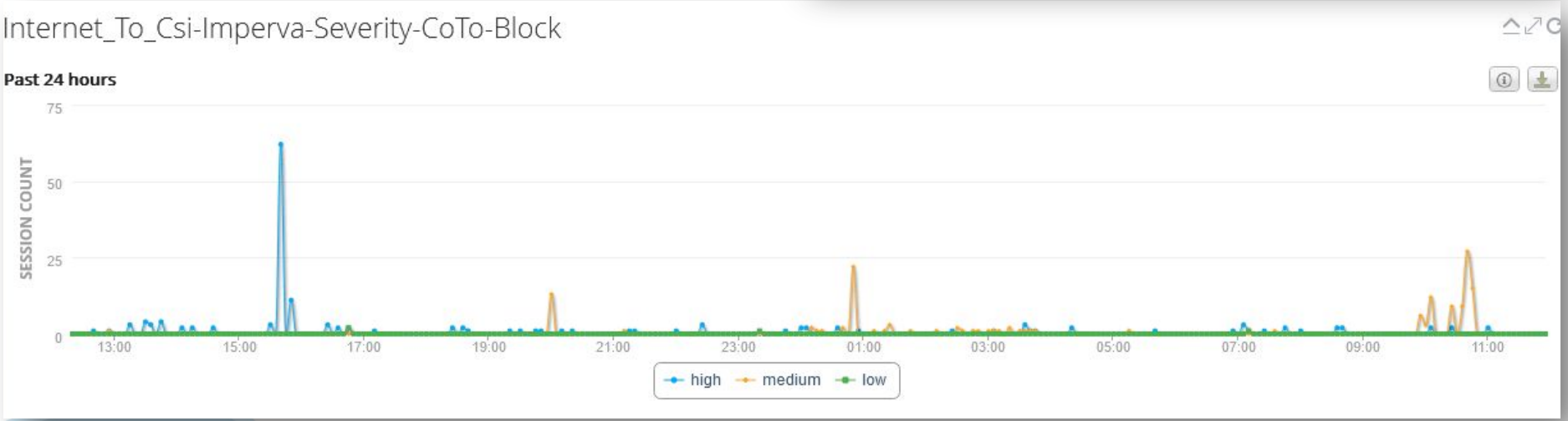
Numero di Server Protetti nel Data Center	**455**
Numero di URL dinamiche protette	317.334
Numero di Virtual Host protetti nel Data Center	922
Numero di eventi “malevoli” bloccati	Circa 14.500.000 (nella figura di dettaglio)

Rilevazione dei dati su un campione di 30 giorni

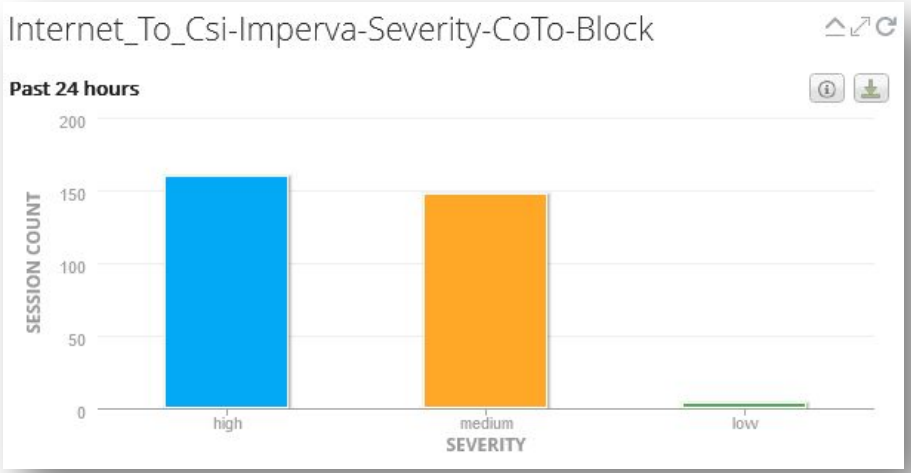
Alert Name	Severity	Num. of Events
Abnormally Long Header Line	High	31,023
Custom Violation	Low	34
Custom Violation	Medium	17,649
Custom Violation	High	54,847
Discrepancy between transfer-encoding and content-length	High	262
HTTP Signature Violation	Low	6,387
HTTP Signature Violation	High	418,963
Illegal Byte Code Character in Header Name	Medium	66,126
Illegal Byte Code Character in Header Value	Medium	8,660
Illegal Byte Code Character in Method	Medium	31,277
Illegal Byte Code Character in Parameter Name	Medium	524
Illegal Byte Code Character in Parameter Value	Medium	224
Illegal Byte Code Character in Query String	Medium	984
Illegal Byte Code Character in URL	Medium	22,600
Illegal HTTP Version	Medium	21,284
Illegal Host Name	Low	527
Illegal Parameter Encoding	Low	1,699
Illegal Response Code	Low	53
Illegal URL Path Encoding	Low	157,775
Malformed HTTP Header Line	High	38,704
Malformed URL	Low	36,506
NULL Character in Header Name	Low	54,211
NULL Character in Header Value	Low	7,708
NULL Character in Method	Low	27,935
NULL Character in Parameter Name	Low	694
NULL Character in Parameter Value	Low	8,392
NULL Character in Query String	Low	398
NULL Character in Url	Low	18,139
Redundant HTTP Headers	High	290
Redundant UTF-8 Encoding	Medium	3,729
SQL injection	High	13,381
Scraping Attack	Medium	13,550,803
Too Many Cookies in a Request	Low	9,968
Too Many Headers per Response	Medium	48,596
Too Many of the Same Response Code	Medium	38,396
Unauthorized Request Content Type	High	4,955
Unknown HTTP Request Method	Medium	35,526
Web Worm	High	8,284

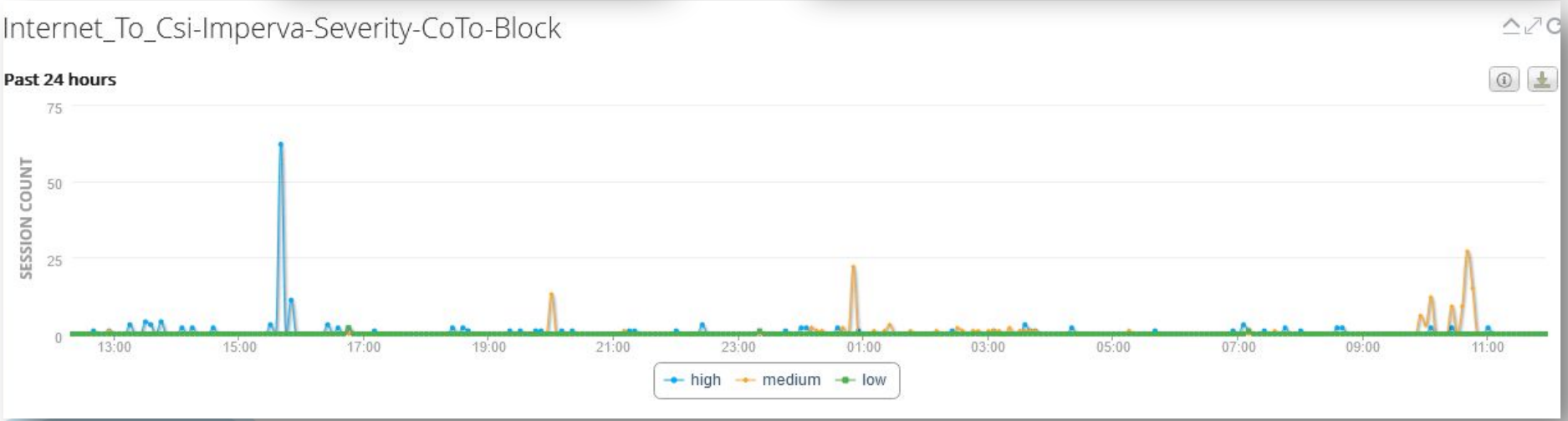
Tentativi di attacco su Città di Torino



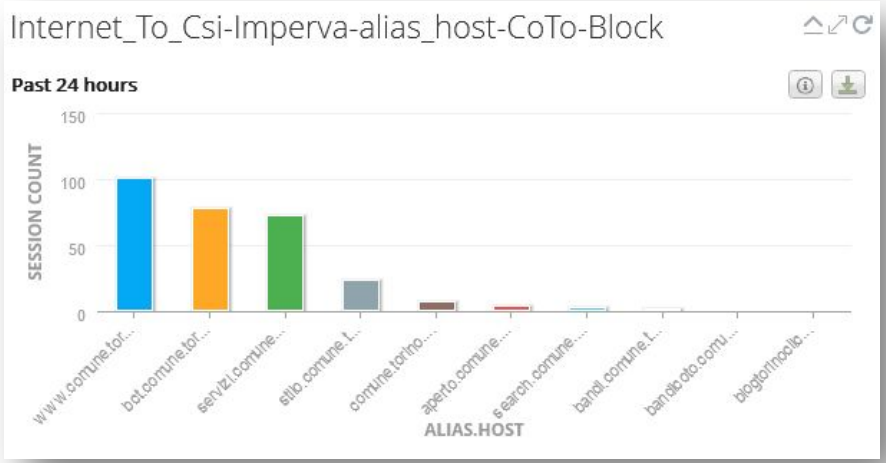


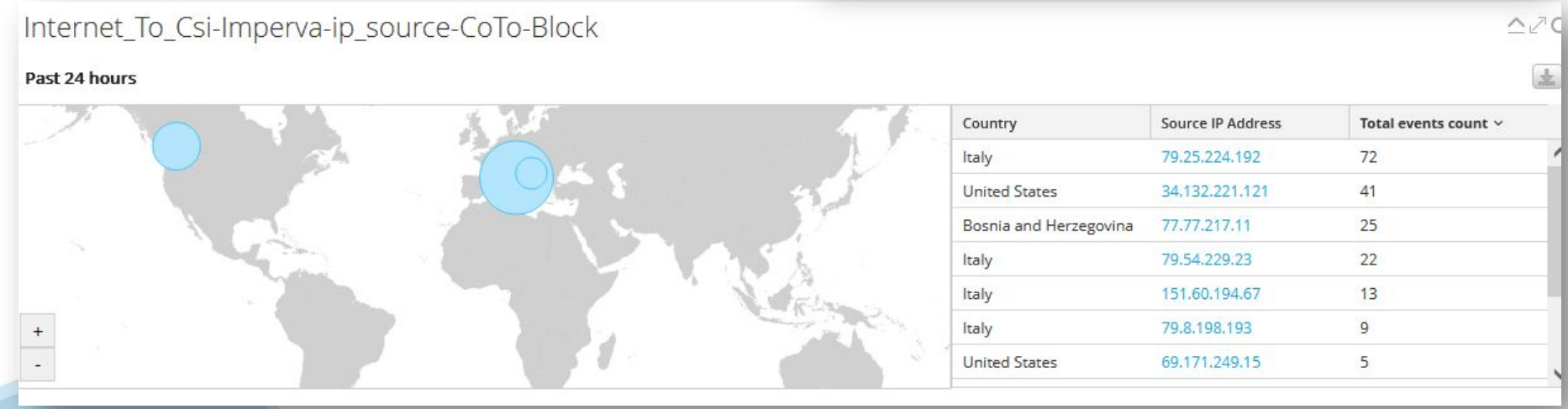
Tentativi di attacco su Città di Torino





Tentativi di attacco su Città di Torino





Country	Source IP Address	Total events count
Italy	79.25.224.192	72
United States	34.132.221.121	41
Bosnia and Herzegovina	77.77.217.11	25
Italy	79.54.229.23	22
Italy	151.60.194.67	13
Italy	79.8.198.193	9
United States	69.171.249.15	5

La Service Control Room

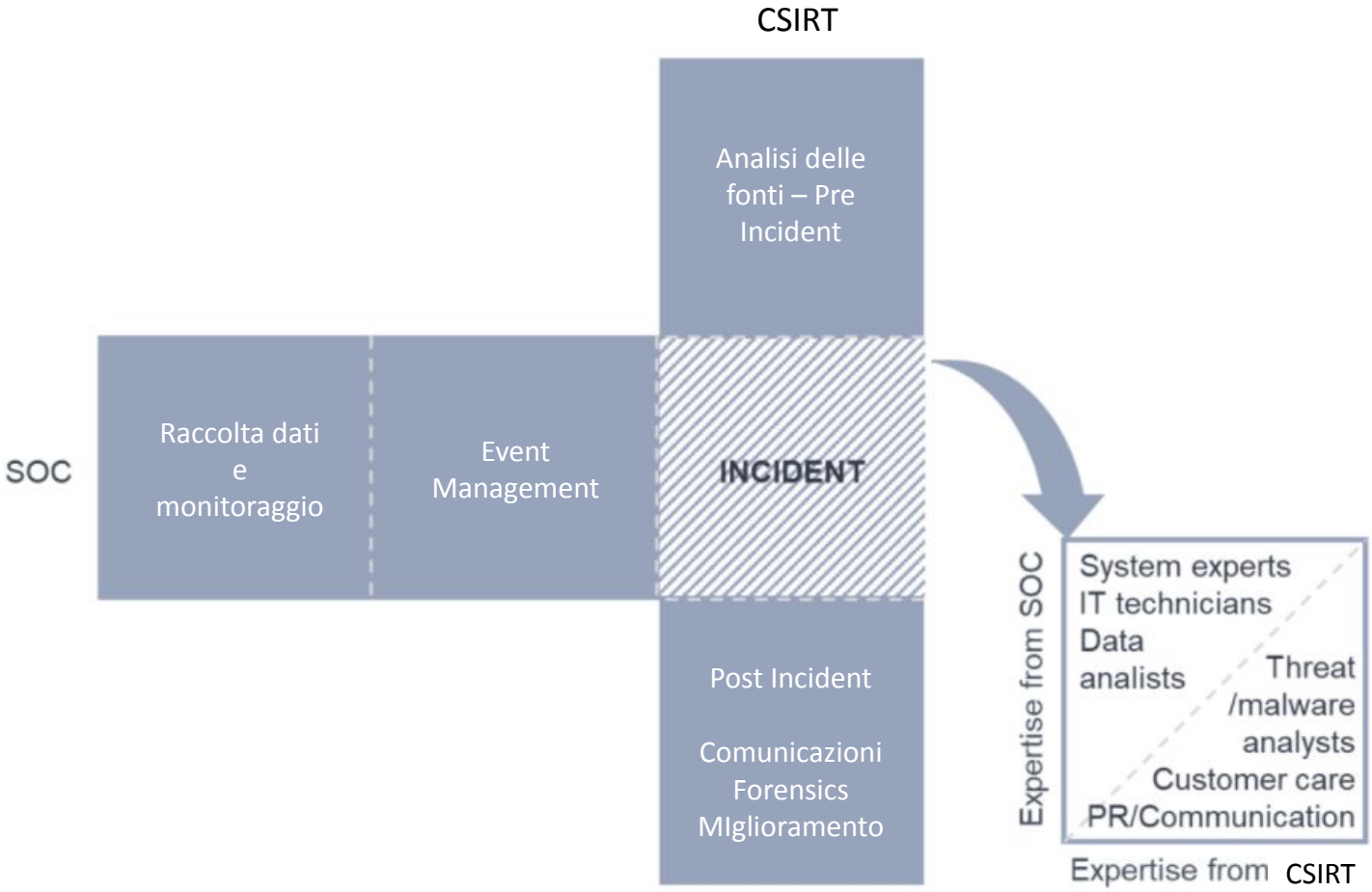
- 350 mq
- Due aree operative «gemelle»
- 55 tecnici specializzati
- Servizi di monitoraggio e conduzione operativa H24
- Circa 2.000 servizi monitorati
- Area riservata al Security Operation Center
- Area «War Room» per gestione delle crisi

CSIRT e D-SOC, Approfondimento Tematico

Il **Security Operation Center (SOC)** è in una certa misura la torre di controllo per gli attacchi informatici. Responsabile del monitoraggio dell'infrastruttura tramite processi standardizzati, coordina le contromisure da adottare per la difesa in caso di incidenti informatici. Nella gestione delle allerte, gli specialisti della sicurezza decidono se occuparsi direttamente di un incidente nel SOC o se passarlo alla competenza dello CSIRT.

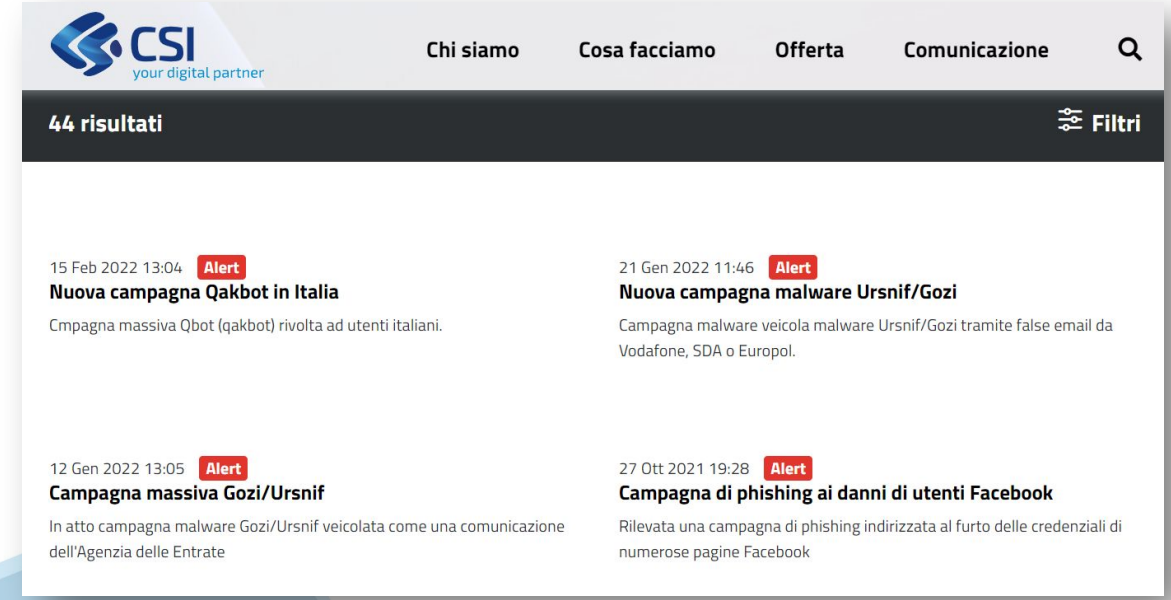
Nel **Computer Security Incident Response Team - CSIRT**, gli specialisti della sicurezza IT mettono in atto le misure di difesa e di ripristino che necessitano di un'analisi più approfondita, tra cui attività di threat hunting e analisi forensi per la ricerca attiva di incidenti nella sicurezza. Lo CSIRT supporta gli Enti nella comunicazione di tali episodi agli interessati dagli incidenti e alle forze dell'ordine. Lo CSIRT amplia così i compiti del SOC.

CSIRT e D-SOC, Approfondimento Tematico



CSIRT, il percorso

- CSI è stato accreditato alla community europea a luglio 2021
  - Acronym used (short name): **CSI-RT**
  - Official team name: **CSIRT CSI Piemonte**
  - **csirt.csipiemonte.it**



CSIRT – Constituency e Piano dei Servizi

- **CSIRT con modello organizzativo "Indipendente" (ENISA):** agisce come organizzazione indipendente, con una propria direzione e proprie risorse, pur essendo collocato all'interno di un ente/organizzazione che potrà essere a sua volta parte della constituency. Questo modello è basato su un CSIRT dedicato e centralizzato con piena responsabilità e autorità sulle attività di analisi, gestione e risposta agli incidenti.

- **Livello di autorità: Assente, Condiviso e Completo:** a seconda dell'Ente e dei servizi erogati dal DC. Es. REGP, Città (Completo); ASL (Condiviso, in questo momento)

Es. Applicazione di Patch di Sicurezza:

- **Livello di autorità completo**: Lo CSIRT può richiedere alle organizzazioni di scollegarsi dalla rete fino a quando non avranno installato la patch, intervenendo manualmente per scollegare i componenti non conformi.
- **Livello di autorità condiviso**: Il CSIRT potrebbe consigliare agli Enti di scollegarsi dalla rete fino a quando la patch è stata installata e può assistere fornendo il proprio supporto nel coordinamento e nel fornire indicazioni utili alla soluzione.
- **Livello di autorità assente**: Lo CSIRT può diffondere l'informazione alla è può cercare di motivare la necessità del patching ma non può forzarne l'installazione.

CSIRT– Constituency e Piano dei Servizi

- **SERVIZI REATTIVI**, sono concepiti per rispondere alle richieste di assistenza, ai rapporti sugli incidenti e a qualunque rischio o attacco nei confronti della constituency.

- **ALLARMI E AVVISI**, la divulgazione di informazioni che descrivono un attacco, una vulnerabilità, tentativi di intrusione, virus o hoax e nel raccomandare azioni a breve termine per la risoluzione del relativo problema.

- **GESTIONE DEGLI INCIDENTI**, che comprende il ricevimento, il triage (o categorizzazione) e la risposta a richieste e rapporti nonché l'analisi di incidenti ed eventi.

- **GESTIONE DELLE VULNERABILITA'** ovvero l'attività che consiste nel ricevere informazioni e rapporti sulle vulnerabilità hardware e software, analizzarne la natura, la meccanica, gli effetti e sviluppare strategie di risposta per la loro mitigazione.

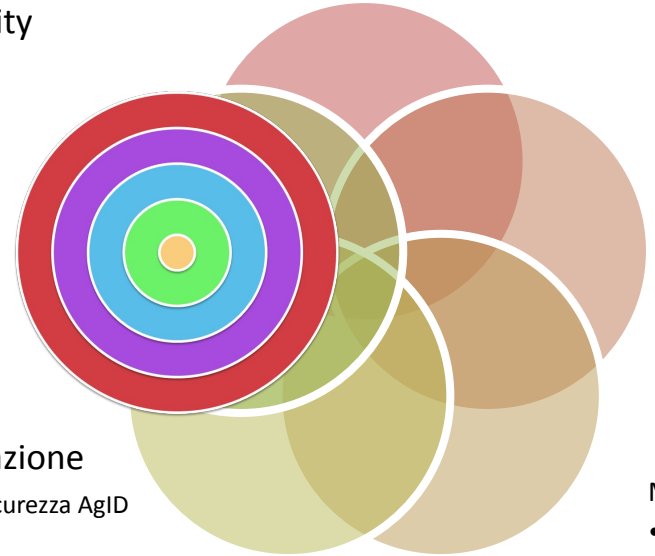
Gli strumenti ed i servizi Cyber del CSI Piemonte

Device Security

- Posti di lavoro
- Device mobili
- Crittografia
- Content Filter

Servizi di Cybersecurity

- Vulnerability Assessment
- SOC
- Remediation Plan
- Indagini Forensi



Protezione della Rete

- Sicurezza Perimetrale
- Sistemi anti DDoS
- Sicurezza delle reti interne
- Virtual Private Network
- Sicurezza dei servizi Cloud (Nivola)

Awareness – Formazione

- Verifica misure minime sicurezza AgID
- Risk Assessment
- Formazione end user
- Formazione a Referenti IT/Security
- Simulazione Incident

Monitoraggio della sicurezza

- Raccolta, analisi e correlazione Log
- Alerting su fenomeni anomali
- Audit sistemi e Amministratori

Cybersecurity e Piano Triennale ICT della Città

E' in fase di finalizzazione il Piano triennale ICT 2022-2024 della Città di Torino, che prevede al suo interno un ampio focus sulla Cybersecurity e in particolare sugli interventi previsti per incrementare il livello di sicurezza e resilienza del Sistema Informativo della Città:

- Incremento dei livelli di segmentazione della rete comunale (visibilità tra aree e sedi)
- Rafforzamento dei sistemi di autenticazione per l'accesso da remoto
- Interventi per il superamento dell'obsolescenza applicativa
- Ammodernamento e razionalizzazione delle postazioni di lavoro (in logica portatile+VPN)
- Interventi di formazione del personale e simulazione di attacchi
- Predisposizione di un Piano di gestione della crisi (emergenza informatica)
- Rafforzamento della rete dei Master informatici
- Aggiornamento del Disciplinare interno per l'uso degli strumenti informatici
- Ampliamento dei sistemi di controllo e monitoraggio
- Assessment esterno per individuare il rischio residuo e azioni conseguenti
- Definizione di un piano di audit periodico sui sistemi e servizi della Città

Grazie