IMPETUS
Strumenti & Piattaforma

Practitioners Guides
Condividono quanto appreso nell'esperienza di IMPETUS con un pubblico più ampio

Firearm Detector
Monitora costantemente i feed delle telecamere di sorveglianza e invia un allarme se viene rilevata un'arma da fuoco in un luogo pubblico

Bacteria Detector
Monitora costantemente l'aria per rilevare concentrazioni di batteri insolitamente elevate

Urban Anomaly Detector
Monitora costantemente i dati raccolti da più sensori urbani e rileva casi che si discostano dalla norma, indicando possibili situazioni pericolose

Social Media Detection
Esegue la scansione di grandi volumi di testo sui social media e altri siti online pubblici, alla ricerca di argomenti/parole chiave che potrebbero indicare potenziali problemi o minacce

Workload Monitoring System
Misura il carico di lavoro mentale e lo stress degli operatori utilizzando un'interfaccia cervello-computer e genera allarmi in caso di anomalie

Evacuation Optimiser
Fornisce indicazioni su come gestire efficacemente un'evacuazione, basandosi su diverse simulazioni di possibili scenari di evacuazione

Cyber Threat Intelligence
Rileva e classifica le minacce del cyberspazio, aiuta gli operatori IT di un'organizzazione a mitigarne gli effetti

Cyber threat Detection and Response
Rileva le vulnerabilità informatiche nei sistemi IT: genera allarmi e suggerisce contromisure

La Piattaforma IMPETUS
Integra più strumenti in un'unica interfaccia

Practitioners Guides

Condividono quanto appreso nell'esperienza di IMPETUS con un pubblico più ampio

QUALE PROBLEMA AFFRONTANO LE GUIDE?

Avanzate soluzioni tecnologiche atte a raccogliere, analizzare e utilizzare dati possono potenzialmente contribuire molto a migliorare la sicurezza nelle città. Ma non possono essere usate semplicemente "tirandole fuori dalla scatola": vanno infatti svolte diverse considerazioni relative all'uso etico della tecnologia, alla protezione dei dati e della privacy dei cittadini, alla sicurezza informatica e alle possibili nuove/diverse modalità operative per generare valore aggiunto e un impatto positivo nel lungo termine.

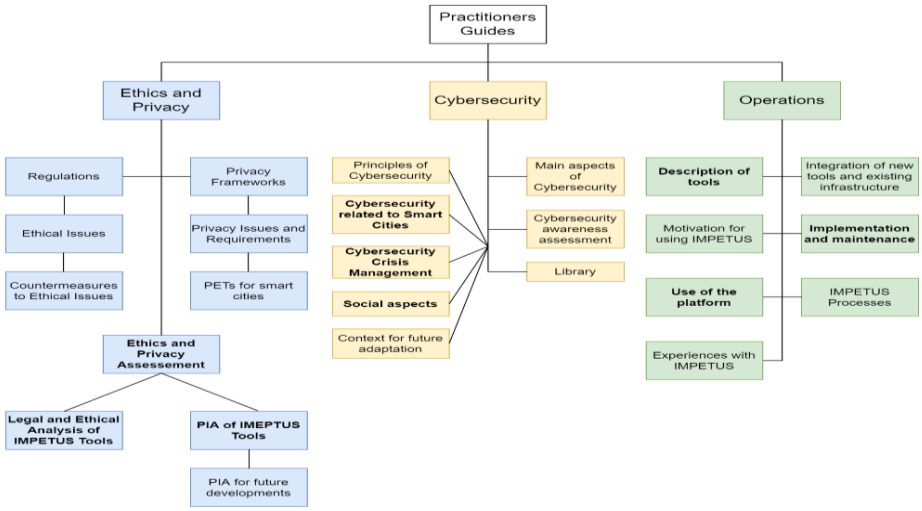
Per affrontare queste tematiche sono stati pensati diversi approcci e molte sono state le "lezioni apprese" lungo il percorso. Le *Practitioners Guides* vogliono aumentare la consapevolezza sui temi affrontati e condividere quanto visto in IMPETUS a un pubblico più ampio. Raccolgono linee guida, tutorial, *check list*, riferimenti normativi e alla letteratura specializzata e altro materiale che si riferisce a tre aree:

- *Ethics:* come integrare principi e procedure per tutelare privacy e dati utilizzati a livello operativo.
- *Cybersecurity*: come proteggersi da rischi informatici, rilevandoli e risolvendoli, nelle smart cities.
- *Operations*: come integrare nuove tecnologie con le attuali modalità operative per migliorarle.

Sebbene le guide si riferiscano all'esperienza in IMPETUS, sono applicabili anche in altri contesti legati ad approcci tecnologici simili, alla gestione e alla sicurezza di smart cities.

COME VENGONO UTILIZZATE LE GUIDE?

- **A chi si rivolgono?** A chiunque abbia responsabilità nel garantire la sicurezza degli spazi pubblici e/o sia coinvolto in aspetti operativi, etici, legali o di cybersecurity relativi all'utilizzo di soluzioni tecnologiche avanzate in ambito sicurezza.
- **Quali benefici per i lettori?** approcciando in modo integrato questioni tecniche e non tecniche, si può massimizzare l'apporto delle soluzioni tecnologie che si intendono adottare.



COME FUNZIONANO?

Le *Practitioners Guides* sono implementate come pagina Wiki (con il framework e i tool di Confluence) con un'interfaccia interattiva che facilita la consultazione dei contenuti. Si vuole infatti permettere a lettori con background e ruoli diversi una facile navigazione verso i moduli di loro interesse.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Firearm Detector

Monitora costantemente i feed delle telecamere di sorveglianza e invia un allarme se viene rilevata un'arma da fuoco in un luogo pubblico

QUALE PROBLEMA RISOLVE QUESTO STRUMENTO?

Situazioni pericolose ed eventi estremi che coinvolgono l'uso di armi, purtroppo, si verificano sempre più spesso nelle nostre città. Lo scopo di questo strumento è utilizzare le telecamere di sorveglianza per rilevare in tempo reale eventuali armi da fuoco e migliorare la sicurezza degli spazi pubblici.
Senza lo strumento:

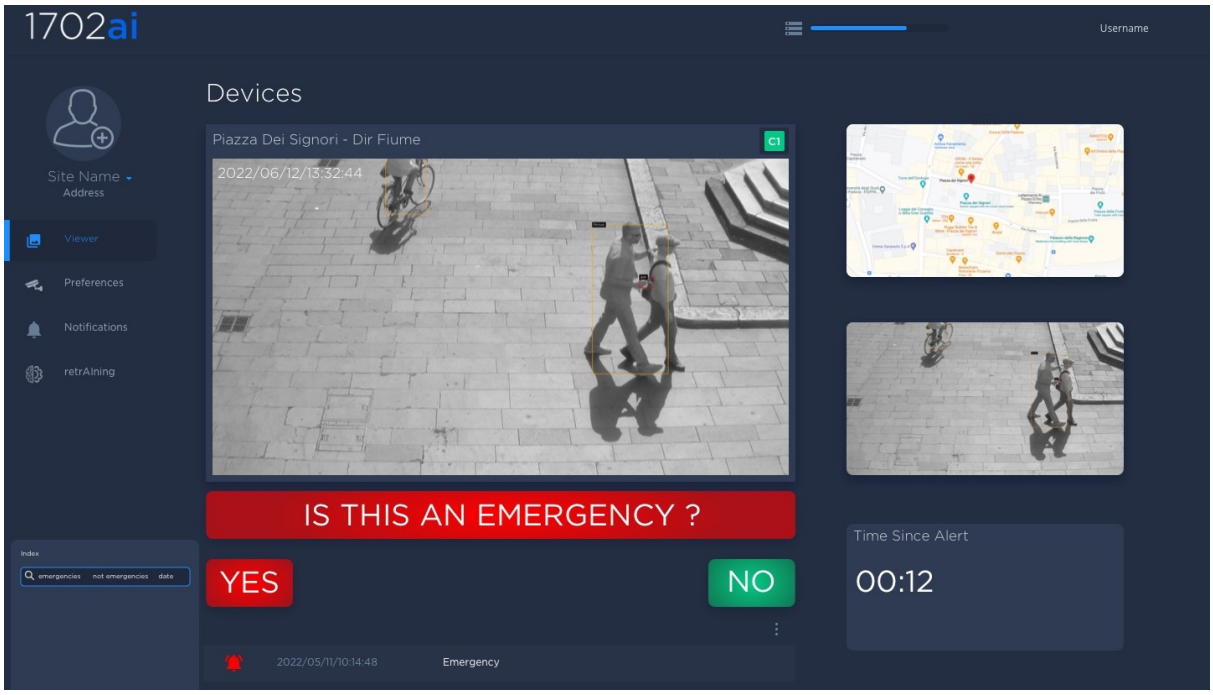
- Le forze di polizia non sono sempre efficaci se non hanno un quadro chiaro della situazione di pericolo (per segnalazioni ritardate, descrizioni incomplete, posizione imprecisa, ecc.).
- Il tempo di risposta può essere lungo e, quando ogni secondo conta, può costare vite umane.

Con lo strumento:

- La condivisione immediata di immagini e posizione consente tempi di risposta molto rapidi.
- Il rischio di morte è potenzialmente ridotto.
- Le operazioni della Centrale Operativa vengono semplificate.

COME VIENE UTILIZZATO IN IMPETUS?

- **Chi sono gli utilizzatori**: Operatori di Centrali Operative e forze di polizia (*first responders*).
- **Quali sono le situazioni critiche per il suo utilizzo:** il tool costantemente monitora le telecamere cercando armi (automaticamente). Rilevata un'arma, l'operatore viene allertato: può confermare il pericolo e nel caso, con la piattaforma IMPETUS, fornisce tutti i dettagli a chi interverrà



COME FUNZIONA?

Quando un'arma entra nel campo visivo della videocamera, la Centrale Operativa riceve un allarme che fornisce il quadro della situazione. Il tool è conforme GDPR, NATO e DHS (Dept. of Homeland Security).

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Bacteria Detector

Monitora costantemente l'aria per rilevare concentrazioni di batteri insolitamente elevate.

QUALE PROBLEMA RISOLVE QUESTO STRUMENTO?

Il Bacteria Detector misura costantemente la concentrazione di batteri presenti nell'aria per proteggere i cittadini da rischi batteriologici. Mediante la piattaforma IMPETUS allerta gli enti preposti/specifici.
Senza lo strumento:

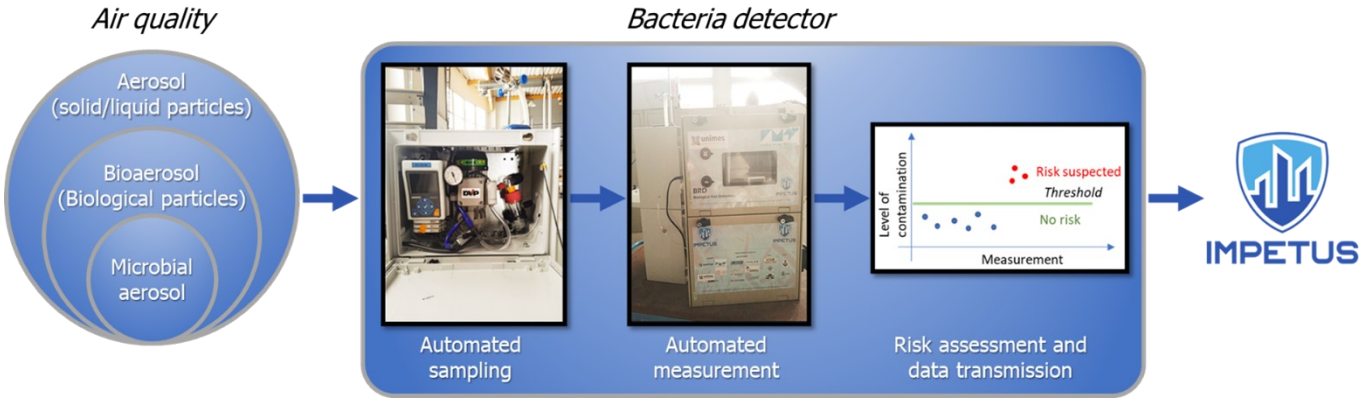
- Una persona può infettare 1-10 persone, a seconda della tipologia di patogeno.
- Gli specialisti devono prelevare campioni dai pazienti per un trattamento adeguato, serve tempo.
- Il personale medico non è protetto e si può confermare l'epidemia solo il giorno successivo alla comparsa della sintomatologia.

Con lo strumento:

- Solo le persone presenti nel luogo interessato vengono infettate.
- I campioni si prelevano solo nella stanza e dai pazienti (risultati in meno di 4 ore).
- I medici adattano subito la procedura e il piano di trattamento sanitario, risparmiando tempo
- Il personale ospedaliero opera in sicurezza e si limita la possibilità di diffondere il contagio.

COME VIENE UTILIZZATO IN IMPETUS?

- **Chi sono gli utilizzatori**: I tecnici qualificati che usano lo strumento. Gli specialisti (Vigili del Fuoco, Medici, ecc.), le forze di polizia, le autorità locali, ecc. possono ricevere dal sistema immediata notifica sul possibile rischio di contaminazione o di contagio massivo.
- **Quali sono le situazioni critiche per il suo utilizzo:** Sempre. Lo scopo del tool è permettere un monitoraggio continuo e generare un allarme quando è necessario.



COME FUNZIONA?

Il tool mette insieme un *air biocollector* (sviluppato da IMT Alès / Università di Nîmes) con un dispositivo che misura la concentrazione batterica* 1) L'aria viene campionata utilizzando un *impinger* e i batteri rilevati vengono bloccati in acqua. 2) L'acqua viene analizzata per definire la quantità di batteri. 3) i dati vengono inviati alla piattaforma IMPETUS: se viene superata la soglia predefinita, viene generato un allarme.

* distribuito da Glow'N'Care, GLBiocontrol Company.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Urban Anomaly Detector

Monitora costantemente i dati raccolti da più sensori urbani e rileva casi che si discostano dalla norma, indicando possibili situazioni pericolose

QUALE PROBLEMA RISOLVE QUESTO STRUMENTO?

Le *smart cities* raccolgono continuamente dati da molteplici sensori dislocati in tutta la città. Se è vero che anomalie nei dati possano essere segnale di possibili problemi, le quantità di dati sono così elevate che non è possibile monitorarli manualmente o rilevare difformità.
Lo strumento utilizza algoritmi di Intelligenza Artificiale (AI) per raccogliere dati da più fonti su lunghi periodi per riconoscere schemi e definire ciò che è "normale" in momenti e luoghi diversi. Quindi utilizza quanto appreso per rilevare anomalie quando si verificano, anche se non sono state osservate prima. Lo strumento può classificare le anomalie e consentire a un operatore di valutare se il pericolo è reale.
Senza lo strumento:

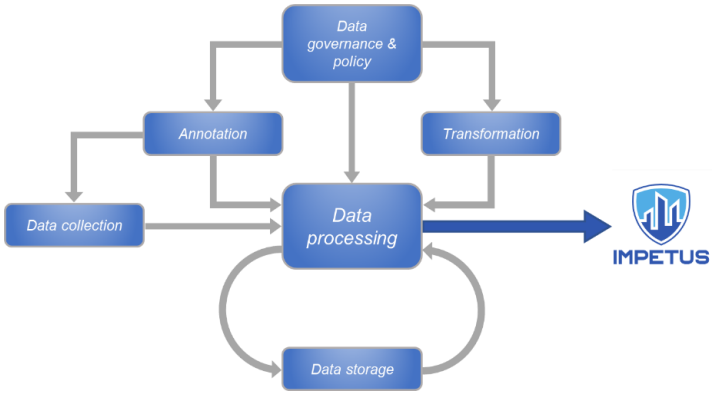
- eventi o situazioni anormali possono passare inosservati perché gli esseri umani non sono in grado di elaborare la quantità di dati necessaria per identificare un problema quando si verifica, il che può portare al caos o anche al disastro.

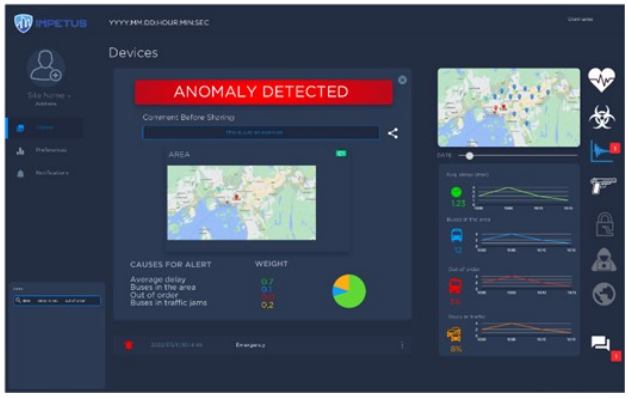
Con lo strumento:

- eventuali sviluppi anomali vengono automaticamente identificati, si possono quindi adottare misure per valutare la situazione, mitigare un rischio e, forse, evitare un disastro.

COME VIENE UTILIZZATO IN IMPETUS?

- **Chi sono gli utilizzatori**: personale operante nella sicurezza nei trasporti e nelle operations che monitora rischi imminenti, il flusso di traffico e/o le minacce alla sicurezza prima e dopo qualsiasi evento anomalo; altri attori quali forze di polizia, autorità locali, management, ecc.
- **Quali sono le situazioni critiche per il suo utilizzo:** Sempre. Lo strumento mira a fornire un costante monitoraggio della situazione: anomalie possono aver luogo in qualsiasi momento.





COME FUNZIONA?

Grandi quantità di dati vengono costantemente raccolte da diverse fonti, ad esempio telecamere, sensori, ecc. Vengono poi processati via *policy awareness, analytics* e *visualisation*. Se rilevate anomalie, viene inviato un allarme alla piattaforma IMPETUS.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Social Media Detection

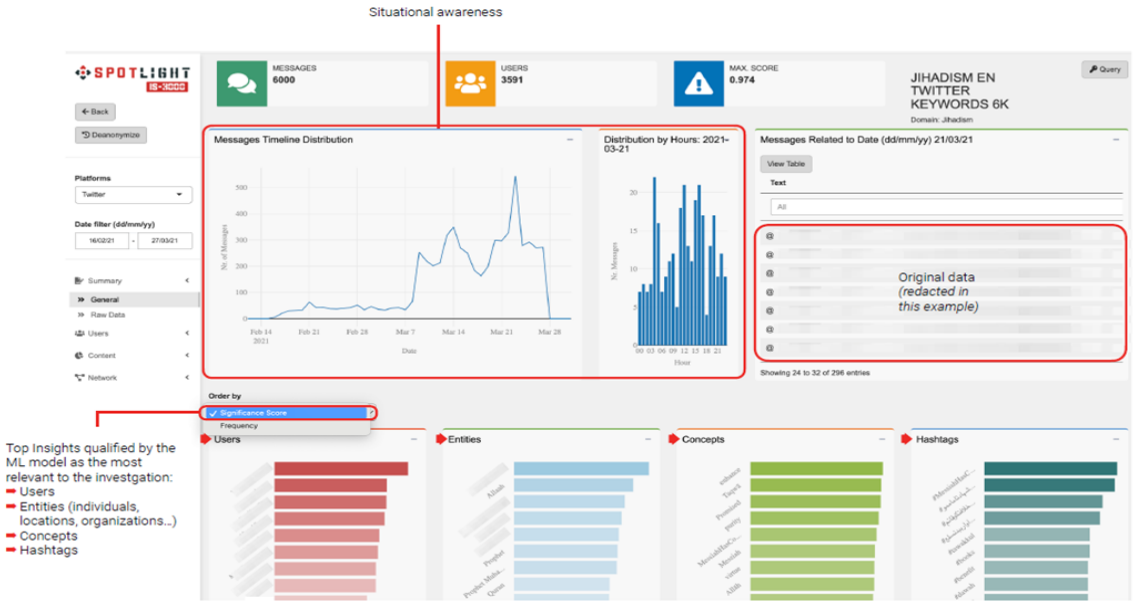
Esegue la scansione di grandi volumi di testo sui social media e altri siti online pubblici, alla ricerca di argomenti/parole chiave che potrebbero indicare potenziali problemi o minacce

QUALE PROBLEMA RISOLVE QUESTO STRUMENTO?

L'enorme quantità di dati sui social media può contenere informazioni rilevanti per chi si occupa di sicurezza; non è umanamente possibile monitorarli e analizzarli manualmente tutti: gli indizi di possibili problemi spesso non vengono rilevati. Lo scopo del tool è aumentare l'efficienza e l'ampiezza della ricerca di informazioni specifiche nel "mare magnum" di dati pubblicati sul web. Il software accelera l'analisi dei dati, l'utente può quindi eseguire più progetti di indagine, espandendo e/o perfezionando così la ricerca e per ottenere risultati più rilevanti.

COME VIENE UTILIZZATO IN IMPETUS?

- **Chi sono gli utilizzatori**: Investigatori e Analisti, che allerteranno le Centrali e il personale operativo riguardo a possibili situazioni pericolose / rischi o che continueranno a monitorare quanto rilevato, che può di interesse per altri attori quali forze di polizia, autorità locali, management, ecc.
- **Quali sono le situazioni critiche per il suo utilizzo:** previste 3 fasi:
  1. Creare un progetto di indagine nell'ambito di interesse.
  2. Acquisire e analizzare i dati.
  3. Utilizzare la dashboard per inviare avvisi di allerta quando vengono rilevate anomalie.



COME FUNZIONA?

L'Analista crea un progetto di indagine sul tema di interesse utilizzando criteri di ricerca, ad es. parole chiave. Il tool scansiona social media, siti, forum, ecc. a seconda dei parametri impostati; processa i dati scartando i contenuti non correlati e presenta i risultati ottenuti. L'utente viene avvisato tramite la piattaforma IMPETUS sui risultati generati che può poi filtrare o, perfezionando i criteri, approfondire. Il tool aiuta l'utente a identificare rischi non palesi e a monitorare il "*sentiment*" generale.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Workload Monitoring System

Misura il carico di lavoro mentale e lo stress degli operatori utilizzando un'interfaccia cervello-computer e genera allarmi in caso di anomalie

QUALE PROBLEMA RISOLVE QUESTO STRUMENTO?

Una Centrale Operativa può essere un ambiente di lavoro altamente stressante e il personale può reagire rallentando o addirittura commettendo errori se lo stress non viene gestito. La situazione opposta – troppo poco da fare – può portare alla noia e alla disattenzione.
Questo strumento vuole ridurre l'errore umano e migliorare l'interazione uomo-macchina del singolo e di gruppo, monitorando il carico di lavoro fisico, emotivo e mentale degli operatori mentre svolgono le loro mansioni. Segnala un anomalo carico sia individuale che del team e la resilienza allo stress durante le emergenze.
Senza lo strumento:

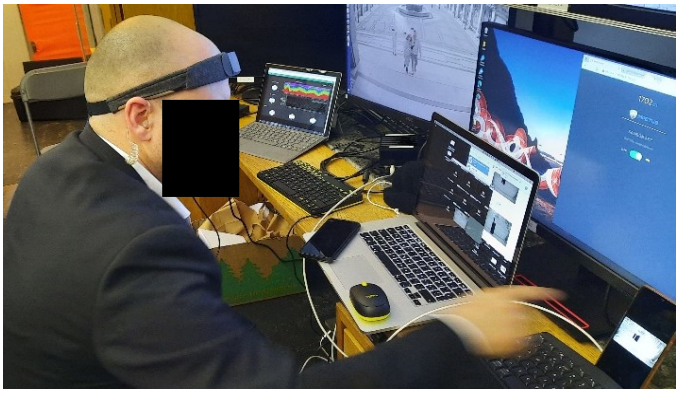
- La percezione del carico di lavoro è inconsapevole, soggettiva e sporadica.

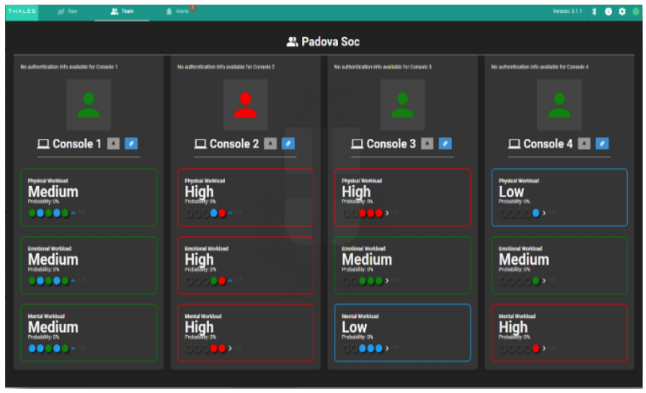
Con lo strumento:

- Il carico di lavoro può essere monitorato in maniera esplicita, oggettiva.

COME VIENE UTILIZZATO IN IMPETUS?

- **Chi sono gli utilizzatori**: Operatori e supervisori delle Centrali Operative, specialisti IT, scienziati comportamentali, analisti dello stress.
- **Quali sono le situazioni critiche per il suo utilizzo:** Il tool e i suoi sensori sono discreti e possono essere utilizzati sempre mentre gli operatori lavorano, anche durante le emergenze.





COME FUNZIONA?

Ogni operatore indossa una fascia sulla fronte (discreta) che rileva i segnali biometrici (cardio, onde cerebrali) e li trasmette allo strumento. Il carico di lavoro dell'operatore viene comparato con modelli personalizzati pre-calibrati (con algoritmi di machine learning). Lo strumento può essere utilizzato a livello individuale e di team. Il supervisore viene avvisato quando viene rilevato un carico anomalo.
L'interfaccia utente grafica fornisce al supervisore:

- il carico di ciascun membro del team, comprese le possibili variazioni nel tempo
- avvisi relativi a:
  - funzionamento del sensore (la fascia sulla fronte)
  - carico di lavoro (troppo alto/troppo basso) per ciascun operatore

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Evacuation Optimiser

Fornisce indicazioni su come gestire efficacemente un'evacuazione, basandosi su diverse simulazioni di possibili scenari di evacuazione

QUALE PROBLEMA RISOLVE QUESTO STRUMENTO?

Lo scopo del tool è pre-ottimizzare e supportare la gestione del movimento controllato della folla in spazi pubblici in eventi complessi, per prevenire lesioni e/o perdite di vite, ad es. in evacuazioni di emergenza.
Senza lo strumento:

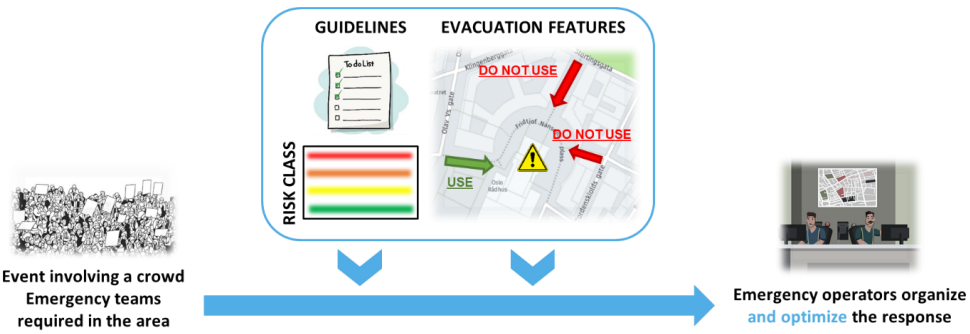
- L'adeguatezza del numero e della dimensione delle vie di uscita non è identificata.
- Non sono noti varchi specifici per i servizi di emergenza.
- Il tempo totale di evacuazione e il rischio associato all'evacuazione rimangono sconosciuti.

Con lo strumento:

- Viene valutato il numero e la direzione delle vie di uscita per la dimensione della folla.
- Vengono identificati i varchi per i servizi di emergenza.
- Un calcolo accurato del tempo totale di evacuazione e del rischio viene presentato agli operatori tramite la piattaforma IMPETUS.
- Procedure di evacuazione efficaci.

COME VIENE UTILIZZATO IN IMPETUS?

- **Chi sono gli utilizzatori**: I soccorritori e gli operatori delle Centrali Operative chiamati a segnalare tempestivamente possibili situazioni pericolose/ rischi, o a monitorare online in tempo reale l'evento/emergenza; altri attori quali forze di polizia, autorità locali, management, ecc.
- **Quali sono le situazioni critiche per il suo utilizzo:** Il tool facilita il coordinamento tra le diverse realtà, il personale nelle centrali operative e in loco e membri del pubblico prima e durante un evento critico. Può aiutare a inviare supporto nel modo più efficiente. Lo strumento facilita inoltre la pianificazione e l'esecuzione delle evacuazioni individuando il percorso più rapido e diretto per il controllo e il movimento della folla.



COME FUNZIONA?

- **Preparazione per un'emergenza:** con i dati dei sensori conta-persone, lo strumento pre-simula scenari di evacuazione da uno spazio pubblico in diverse circostanze e fornisce linee guida per la gestione dell'uscita della folla nei diversi scenari.
- **Durante un'emergenza**: considerando precedenti simulazioni, il numero di persone e delle vie di ingresso/uscita e la capacità delle vie di evacuazione, il tool stima il tempo necessario per evacuare la folla e i rischi connessi. Le linee guida sulle vie di ingresso ed evacuazione ottimali vengono presentate ai soccorritori e agli operatori della sicurezza tramite la piattaforma IMPETUS.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Cyber Threat Intelligence

Rileva e classifica le minacce del cyberspazio, aiuta gli operatori IT di un'organizzazione a mitigarne gli effetti

QUALE PROBLEMA RISOLVE QUESTO STRUMENTO?

Lo scopo del tool è rilevare costantemente gli indizi anche più piccoli di rischi informatici per la rete di un'organizzazione sia in forum e compravendite nel deep e dark web, sia in siti di messaggistica.
Senza lo strumento, gli analisti devono manualmente effettuare complesse attività come:

- Raccolta dati relativi a dominio, indirizzi IP e di terze parti.
- Indicizzazione, codifica e analisi dei metadati dei dati raccolti.
- Estrazione dei dati rilevanti, ripristino e predisposizione per l'archiviazione in un database gestito dal fornitore (Cybersixgill).

Con lo strumento si è in grado di:

- Ricevere e utilizzare un elenco di allarmi diversi a seconda del tipo di asset.
- Effettuare indagini offline e circostanziate su minacce presenti o attività in corso nel cyberspazio.
- Ricevere informazioni relative a rischi per l'organizzazione (chi, dove, cosa) e mitigarli.

COME VIENE UTILIZZATO IN IMPETUS?

- **Chi sono gli utilizzatori**: Specialisti IT chiamati ad allertare subito gli operatori delle Centrali Operative o altri attori quali forze di polizia, autorità locali, management, ecc. riguardo a potenziali rischi per gli asset dell'organizzazione.
- **Quali sono le situazioni critiche per il suo utilizzo:** Regolarmente. In genere le scansioni si effettuano quotidianamente. Lo strumento fornisce tutte le informazioni sulla natura e l'origine delle minacce informatiche rilevate. Poiché ne nascono di nuove continuamente, la scansione va replicata

COME FUNZIONA?

I passaggi principali sono:

1. **Data collection:** trovare le fonti rilevanti, accedere a forum e gruppi chiusi e reperire i dati (*crawling*). **Data processing and analysis:** il tool processa ogni elemento raccolto via: *indexing, enrichment, tagging, entity extraction, metadata,* ripristino e salvataggio dati in un database.
2. **Data lake query:** ricerche automatizzate o manuali sono effettuabili sul database del fornitore che conserva ampia casistica di problemi informatici e attività cybercriminali.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Cyber Threat Detection and Response

Rileva le vulnerabilità informatiche nei sistemi IT: genera allarmi e suggerisce contromisure

QUALE PROBLEMA RISOLVE QUESTO STRUMENTO?

I sistemi informatici presentano in genere così tante vulnerabilità che non è possibile monitorarle continuamente o gestirle tutte manualmente. Inoltre, esistono complesse interdipendenze tra le vulnerabilità. Ad esempio: alcune diventano critiche solo quando un'altra è stata "sfruttata" (come dopo un attacco riuscito). Questo strumento:

- Identifica le vulnerabilità sfruttate e quelle potenzialmente utilizzabili
- Assegna priorità alle azioni per sistemare le vulnerabilità sfruttate e le eventuali vulnerabilità sfruttabili in base alla criticità della situazione

Senza lo strumento:

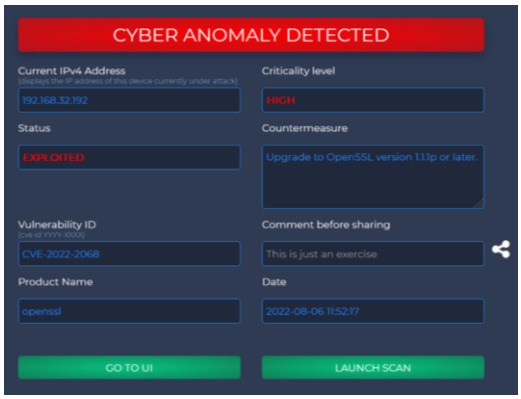
- Le analisi svolte manualmente identificano solo una parte delle vulnerabilità del sistema
- Gli utenti non possono sapere come l'interconnessione tra vulnerabilità può esporre il sistema
- Gli utenti non possono sapere quando una vulnerabilità è stata effettivamente sfruttata

Con lo strumento:

- Gli utenti possono scandagliare sistemi complessi e identificare vulnerabilità e loro connessioni
- Gli utenti possono monitorare i sistemi in tempo reale e ricevere un avviso sulla piattaforma IMPETUS quando una vulnerabilità viene utilizzate.
- Le contromisure possono essere prioritizzate in base alla criticità del rischio

COME VIENE UTILIZZATO IN IMPETUS?

- **Chi sono gli utilizzatori**: (A) specialisti IT responsabili della protezione della rete da possibili attacchi informatici (attraverso analisi, monitoraggio e mitigazione); (B) Sistemisti e operatori delle Centrali Operative centri che vengono allertati in caso di rischi imminenti/situazioni problematiche.
- **Quali sono le situazioni critiche per il suo utilizzo:** Regolarmente: le scansioni e le analisi verrebbero eseguite periodicamente. Lo strumento è progettato per un monitoraggio continuo



COME FUNZIONA?

Analizza i dati in rete e li correla con le vulnerabilità rilevate scansionando l'infrastruttura IT. Quando viene rilevata una minaccia alle vulnerabilità del sistema, le contromisure vengono classificate in base alla gravità del rischio. Viene generato un allarme e inviato alla piattaforma IMPETUS. Gli utenti possono quindi implementare la contromisura. Ad esempio, se un utente tenta più volte di accedere da remoto a una macchina, lo strumento genererà un allarme suggerendo di inibire l'accesso.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

La Piattaforma IMPETUS

Integra più strumenti in un'unica interfaccia

QUALE PROBLEMA RISOLVE QUESTO STRUMENTO?

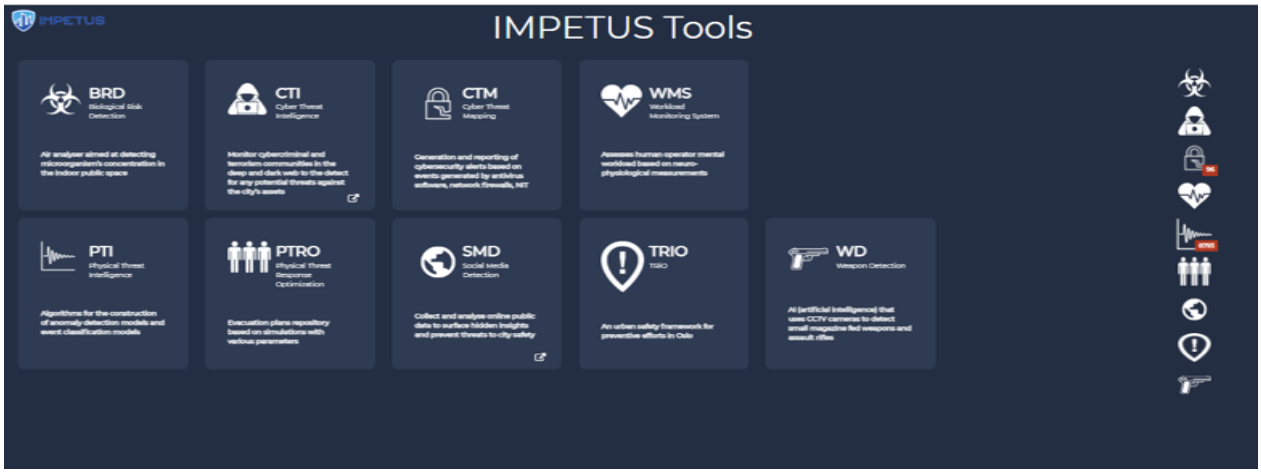
Chi opera nella sicurezza spesso deve interagire con più strumenti contemporaneamente. Quando se ne utilizza uno specifico, deve esserci sempre consapevolezza su situazioni critiche che altri strumenti potrebbero aver rilevato. Se gli utenti interagiscono con i vari strumenti tramite interfacce diverse, non è facile essere sempre efficaci, soprattutto in situazioni di stress. Inoltre, utenti diversi possono avere una differente percezione della situazione a seconda di quale strumento stanno utilizzando.

La piattaforma IMPETUS permette di riunire più strumenti in un'unica interfaccia, in modo che chi deve utilizzarne più di uno possa farlo in un unico ambito. Mostra lo stato di tutti i tool disponibili ma consente all'operatore di interagire con uno specifico per maggiori dettagli. Permette di condividere il quadro della situazione con tutti gli operatori collegati. È possibile, inoltre, personalizzare il cruscotto a seconda del ruolo e delle mansioni dei diversi utenti (possibile quindi abilitare l'uso solo di alcuni dei tool disponibili).

La piattaforma si presenta con tutti gli strumenti sviluppati nel progetto IMPETUS, ma è progettata per integrarne anche altri (sia quelli già in uso sia quelli che l'organizzazione potrebbe acquisire in futuro).

COME SI PRESENTA LA PIATTAFORMA?

- **Chi sono gli utilizzatori**: operatori di Centrali Operative e loro supervisori; analisti e tecnici informatici; altro personale responsabile del monitoraggio e della gestione della sicurezza urbana.
- **Quali sono le situazioni critiche per il suo utilizzo:** Continue: sicurezza è un'operazione 24/7



COME FUNZIONA?

La piattaforma fornisce un cruscotto che riunisce strumenti che permettono di monitorare potenziali pericoli non appena si palesano. La dashboard principale mostra lo stato di tutti gli strumenti e permette di accedere all'interfaccia di ciascuno per un utilizzo puntuale.
Vengono visualizzati allarmi (con diversi livelli di priorità), se sono stati presi in carico e/o risolti. Ove possibile, i dati vengono presentati graficamente per una visualizzazione più efficace, inoltre viene fornita una mappa del luogo del pericolo rilevato. Possibile l'interazione con altri utenti via chat.
La piattaforma è stata implementata utilizzando la piattaforma Snap4City: http://www.snap4city.org/

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.