FONDAZIONE BRUNO KESSLER

FUTURE BUILT ON KNOWLEDGE

Joint Lab per la Cybersecurity

Servizio Soluzioni Digitali e Infrastrutture IT
Centro per la Cybersecurity

20/02/2025

Fondazione Bruno Kessler

Mirco Vivaldi
mvivaldi@fbk.eu

Servizio Soluzioni Digitali & Infrastrutture IT

Chiara Cesareo
ccesareo@fbk.eu

Servizio Soluzioni Digitali & Infrastrutture IT

Umberto Morelli
umorelli@fbk.eu

Centro per la Cybersecurity

Laura Cristiano
l.cristiano@fbk.eu

Centro per la Cybersecurity

Matteo Rizzi
mrizzi@fbk.eu

Centro per la Cybersecurity

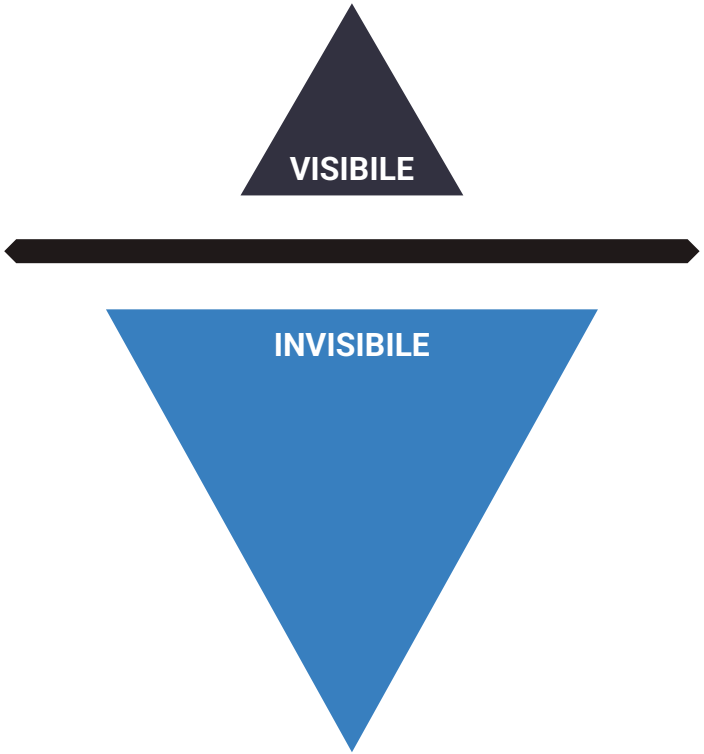
Marco De Rosa
derosa@fbk.eu

Responsabile Servizio Soluzioni Digitali & Infrastrutture IT

Silvio Ranise
ranise@fbk.eu

Direttore Centro per la Cybersecurity

Contesto



- **Il panorama IT è in continua evoluzione, con sempre maggiore complessità**
- **Cloud edge computing =**
  Progressiva migrazione verso il cloud, smart working, strumenti per il lavoro collaborativo, applicazioni per la ricerca

Aumento esponenziale dei rischi per la sicurezza, legati alla disponibilità ed alla privacy dei dati, nonché alla protezione dei sistemi stessi

Living Lab
Istituzione

Il Servizio IT ed il Centro per la Cybersecurity hanno iniziato a collaborare a progetti comuni per migliorare la postura di sicurezza dell'infrastruttura FBK:

1. **Istituzione del Living Lab** nel 2022
2. Progetto Sicurezza FBK 22-24: definizione di un programma per il miglioramento e ripensamento delle misure di sicurezza in uso

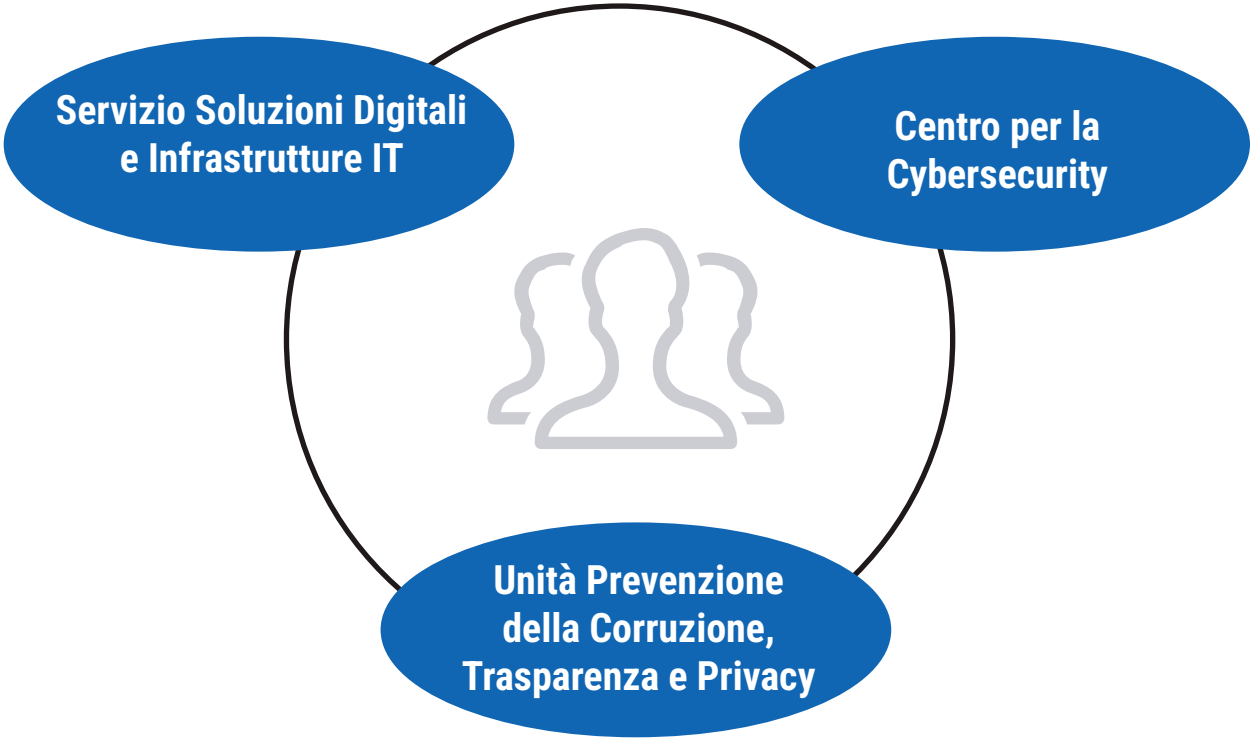
MISSION

Ricerca proattiva sulla sicurezza informatica, test di soluzioni innovative, analisi misure per la prevenzione, controllo e salvaguardia attiva dei dispositivi, educazione degli utenti

VANTAGGI

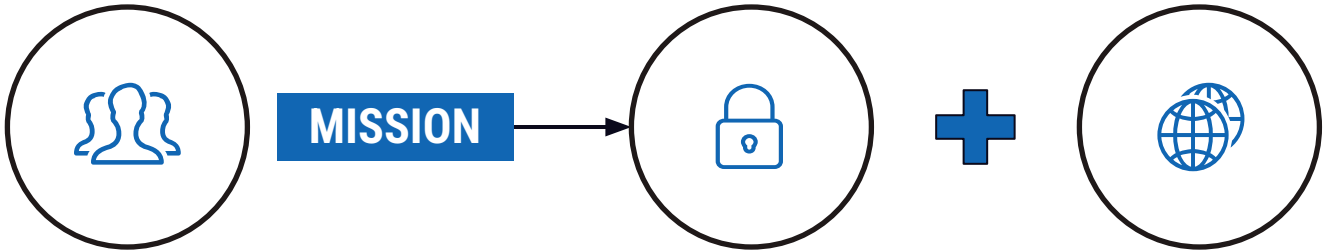
RICERCA+PRODUZIONE = Validazione PoC con casi reali ed applicazione di soluzioni all'avanguardia per l'infrastruttura IT, disegnate sulle necessità degli utenti e monitorando i trend del mercato

Living Lab
Partnership



- Audit di terza parte per compliance UNI EN ISO 9001:2015 "Qualità" e ISO/IEC 27001:2022 "Sicurezza delle informazioni"

Living Lab
Metodologia e Missione



Allineamento con Piano di Mandato 2024-2027 e Piano di sostenibilità tecnica per Macro-Area “Infrastrutture e Piattaforme”

Supportare la società nella gestione dell’impatto della transizione digitale e dell’IA

Catalizzatore di buone pratiche interne e da esportare sul territorio

Living Lab
Impatto rilevato

FORMAZIONE

Digital Cafè in-formativi

→ maggior consapevolezza nell'ambito della gestione degli strumenti informatici e della cybersecurity

Living Lab
Impatto rilevato

FORMAZIONE

Digital Cafè in-formativi

→ maggior consapevolezza nell'ambito della gestione degli strumenti informatici e della cybersecurity

USER EXPERIENCE

Progetto *Gestione responsabile e sicura degli strumenti e dei servizi FBK 23-24*: interviste ad un campione di Amministratori di Sistema di FBK e condivisione analisi svolte con il personale tramite Digital Cafè

→ approfondite e migliorate le pratiche di sicurezza
→ identificato aree di miglioramento e definite Linee guida
→ sviluppato un modello di monitoraggio annuale per la gestione degli strumenti in autogestione

Living Lab
Impatto rilevato

FORMAZIONE

Digital Cafè in-formativi

→ maggior consapevolezza nell'ambito della gestione degli strumenti informatici e della cybersecurity

USER EXPERIENCE

Progetto *Gestione responsabile e sicura degli strumenti e dei servizi FBK 23-24*: interviste ad un campione di Amministratori di Sistema di FBK e condivisione analisi svolte con il personale tramite Digital Cafè

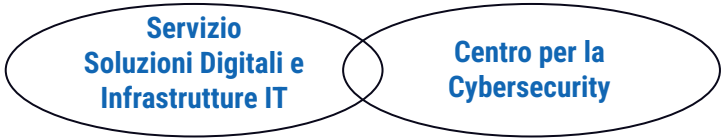
→ approfondite e migliorate le pratiche di sicurezza
→ identificato aree di miglioramento e definite Linee guida
→ sviluppato un modello di monitoraggio annuale per la gestione degli strumenti in autogestione

RICERCA

★ **Pubblicazione** del 03/24 e **condivisione all'interno di ITASEC 2024** (Italian Conference on Cybersecurity) del **paper scientifico *Protecting FBK IT Infrastructure: Towards Zero Trust*** e delle migliori pratiche come parte del ***progetto EU MERIT***

★ **Sviluppo di strumenti di security testing per la gestione delle identità** (es: Micro-Id-Gym, con pubblicazione del 09/24 del relativo paper in *IEEE Security & Privacy Journal*)

Da Living a Joint Lab
Evoluzione in Joint Lab per la Cybersecurity



CODESIGN delle attività congiunte di Servizio IT e Centro per la Cybersecurity

TRASFORMANDO IL LIVING LAB IN…

un **Joint Lab** nato dalla collaborazione tra ricerca, settore produttivo e sociale del territorio che permetta di sperimentare metodi per incrementare incisività e proattività in materia di cybersecurity, e contemporaneamente fungere da banco di prova per l'**esportazione del modello in forma di servizio** da offrire ad altri enti provinciali ed al tessuto produttivo locale

SFRUTTANDO LE COLLABORAZIONI ESISTENTI:

- **04/24 *Lab Cleanse - Cloud Native Application Security*** tra FBK e **Dedagroup** (rinnovamento del Co-Innovation Lab AI & Data Engineering del 2016)
- **12/22 protocollo d'intesa** siglato tra FBK, **Dipartimento di Ingegneria e Scienza dell'Informazione dell'Università di Trento** e **Confindustria di Trento**
- **2020 Laboratorio congiunto *Crittografia applicata e tecnologia blockchain*** con il **Dipartimento di Matematica dell'Università di Trento**
- **partenariati** con **Polizia Postale** e **Trentino Digitale** a livello regionale, **ACN** Agenzia per la Cybersicurezza nazionale ed **ENISA** europea

Joint Lab per la Cybersecurity
Nella pratica

Dove si posiziona e quando si avvia?

Joint Lab interno, tra Centro per la Cybersecurity e Servizio Soluzioni Digitali e Infrastrutture IT, attivo dal **1 gennaio 2025**

Di cosa si tratta?

Task Force di primo intervento in caso di incidenti, servizio di **consulenza e supporto** con soluzioni custom a problemi comuni, a livello combinato di **ricerca e produzione**, derivante dalle competenze interne verticali su gestione dell'identità digitale, risk assessment, cloud native security, crittografia applicata, amministrazione di sistemi IT complessi (Zero Trust approach)…

- ✓ Per le Unità interne: semplificazione e facilitazione di **awareness e condivisione di conoscenze** = supporto tecnologico e collaborazione con Privacy e Centri di ricerca per specifiche misure, supporto al team Certificazioni per conformità ISO/IEC 27001:2022 "Sicurezza delle informazioni", coordinamento normativa NIS2
- ✓ Per le aziende e gli enti: **consulenza di alto livello** = supporto in percorso di **awareness, training e adeguamento agli standard di sicurezza cutting edge**

Board

Responsabili del Centro e del Servizio IT + Matteo Meucci (OWASP) + membro di ACN

Sfide Cybersecurity

PROTEZIONE DI DATI E INFORMAZIONI, nucleo fondante delle attività di ricerca e pilastro su cui si basano operatività ed efficienza delle attività della Fondazione

PREVENIRE GLI ATTACCHI IN MODO DA PREVENIRE IL DANNO (prima che la situazione sia irrimediabile)

MONITORAGGIO E STUDIO CONTINUO di tutta la relativa casistica

Necessità di specifica programmazione di azioni per…

EVITARE DI SOTTOVALUTARE IL LAVORO DI SICUREZZA (causa apporto non immediatamente misurabile)

VALUTARE MERCATO E RISCHI REALI

SENSIBILIZZARE IL PERSONALE E LA GOVERNANCE

STRATEGIA DI SICUREZZA:
PUNTARE SU MISURE PROATTIVE & PRECAUZIONALI + SECURITY BY DESIGN

Joint Lab per la Cybersecurity
Programmazione / Formazione

#FORMAZIONE CONTINUA & PROATTIVA

- **Comunicazione e feedback:** apertura canale **help-cyber** per
  - report casi reali di attacchi e notizie del panorama mondiale
  - supporto in caso di **compromissione**

- **Corsi:**
  - buone pratiche di sicurezza e difesa attiva in percorso dedicato durante **onboarding**
  - buone pratiche di sicurezza e difesa attiva per **amministrazione** (corsi Academy con esempi concreti)
  - specifici per **ricerca** (argomenti derivanti da richieste a canale help-cyber + interviste a direttori di board)
  - pillole pubblicate su Academy

- **Digital Cafè pubblici**
  - per utenti interni
  - per PMI

- **Formazione e aggiornamento interno** (team Joint Lab): raccolta e rielaborazione materiale per training e awareness

Joint Lab per la Cybersecurity
Programmazione / Ricerca

#FORMAZIONE CONTINUA & PROATTIVA

#RICERCA

- **Trasferimento** delle **innovazioni sperimentate dalla ricerca sul campo,** nell'ambito cybersecurity in FBK
  - Sviluppo/estensione di **strumenti di security testing** per la gestione delle **identità**
  - **Analisi del rischio** di progetti interni/pubblici mediante **strumenti basati su AI**
  - Miglioramento della postura di sicurezza di **Authentication & Authorization Control (AAC)**

FONDAZIONE BRUNO KESSLER

- **Divulgazione di approcci e risultati** della ricerca sperimentata in FBK (es., **Zero Trust, Phishing, Pillar)**

FONDAZIONE BRUNO KESSLER

Joint Lab per la Cybersecurity
Programmazione / Consulenza

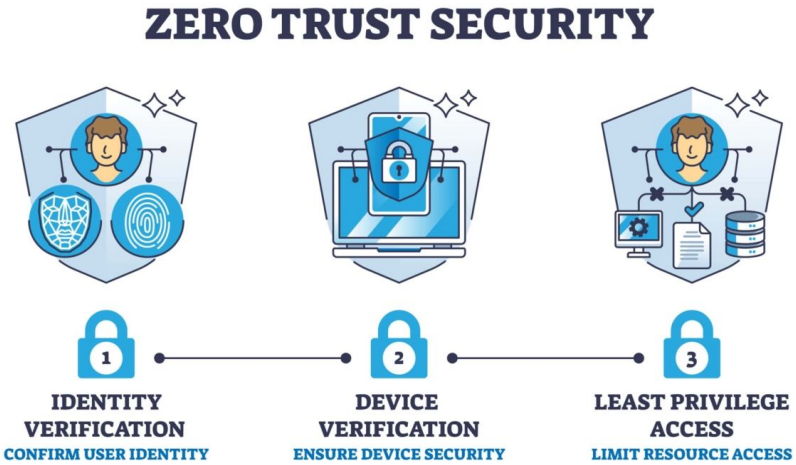
#FORMAZIONE CONTINUA & PROATTIVA
#RICERCA

#CONSULENZA

- **Utenti interni / amministrazione + ricerca:**
  apertura canale per utenti **help-cyber** per
  - **supporto** in caso di **compromissioni**
  - **impostazione security by design di progetti di ricerca e servizi** (ampliamento interviste amministratori di sistema e Linee Guida)

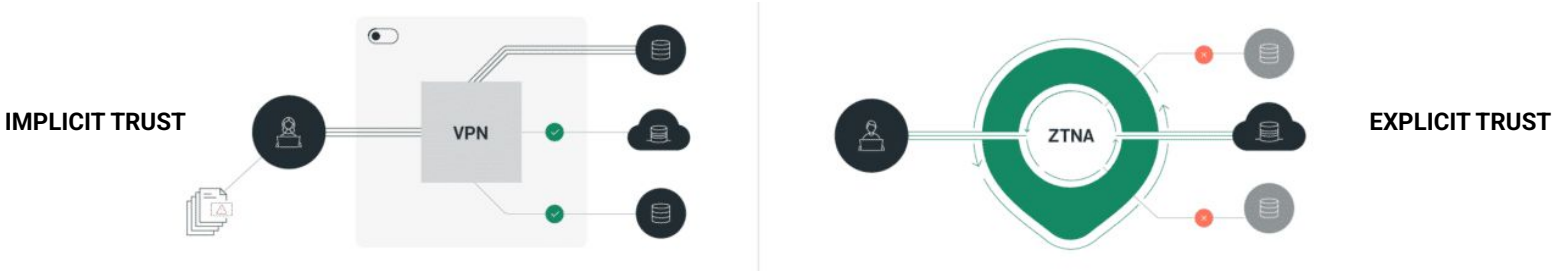
- **Team Certificazioni**:
  - supporto Certificazioni ISO e NIS2

- **Utenti esterni / PMI + Università + partner**
  (Polizia Postale, Trentino Digitale, FEM, ACN, ENISA):
  - training tecnico specifico su richiesta
  - training normativo specifico su richiesta
  - formazione e awareness utenti
  - progetti concordati



- Semplificare l'**autenticazione**, anche per l'accesso alle risorse interne di FBK, e cambiare i **sistemi di collegamento**

  → Passaggio da uso reti **VPN** tradizionali a **Zero Trust Network Access**

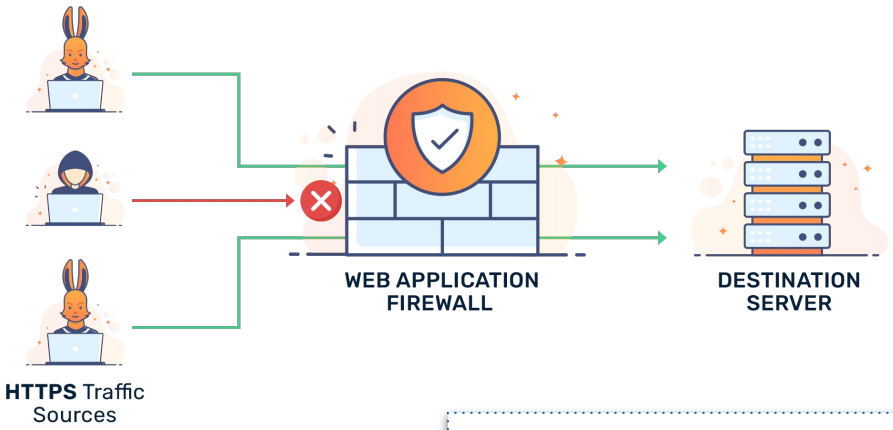


Con le **VPN** gli utenti autenticati ottengono implicitamente l'**accesso a tutto** ciò che si trova nella stessa sottorete (protezione con password)

Con **ZTNA** gli utenti possono "vedere" **solo applicazioni e risorse esplicitamente consentite**

Si rafforza sicurezza di rete e dati attraverso **microsegmentazione**, che limita i movimenti laterali in caso di violazione dei sistemi

- Aumentare la **protezione** dei servizi esposti su **Internet** → Installazione Web Application Firewall **WAF**



Firewall = componente che, come un muro ideale posto tra una rete geografica e una rete locale, offre una **difesa perimetrale** per controllare gli accessi alle risorse di un sistema, filtrando tutto il traffico scambiato tra ambiente interno e mondo esterno

WAF = protegge **applicazioni Web** distribuite nel cloud e on-premise da attacchi dannosi e traffico Internet indesiderato, inclusi bot, injection e denial of service (DoS) **filtrando, monitorando e bloccando qualsiasi traffico HTTP dannoso** in entrata e impedendo al contempo l'uscita di dati non autorizzati dall'applicazione

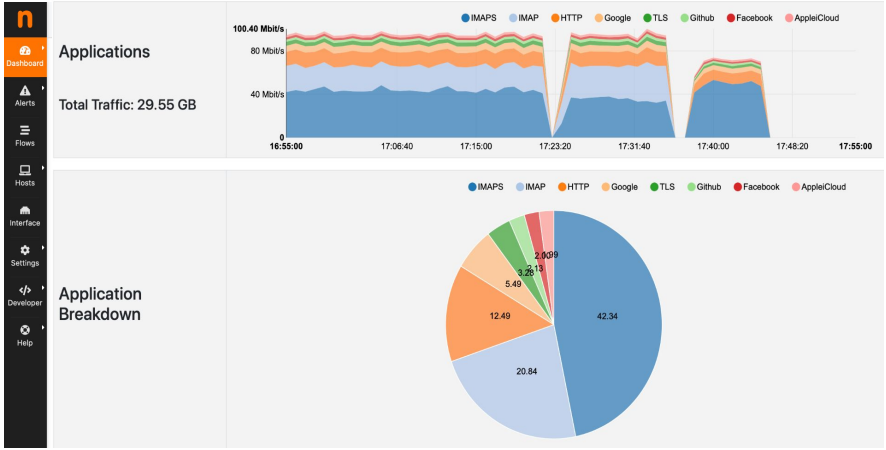
Joint Lab per la Cybersecurity
Programmazione / Parte tecnica

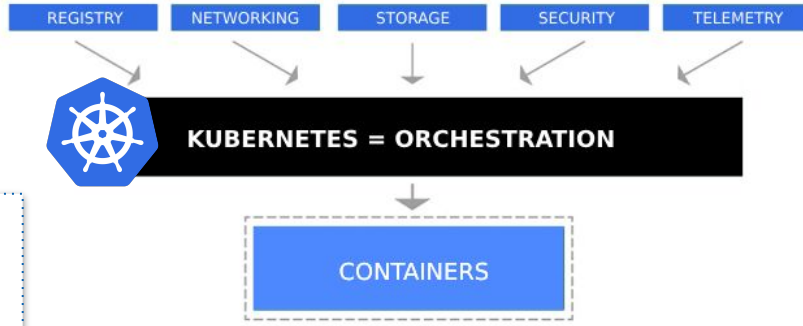
- Potenziare la **difesa attiva** tramite **monitoraggio e rilevazione di anomalie**

  → Uso sistematico di **ntop e elastiflow**

ntop = **sonda di traffico di rete** che fornisce un'interfaccia utente web crittografata per l'esplorazione di informazioni sul **traffico in tempo reale**

elastiflow = tool di network observability per **monitorare tutti i flussi di rete** tramite visualizzazioni dettagliate, analisi delle prestazioni e rilevamento delle anomalie

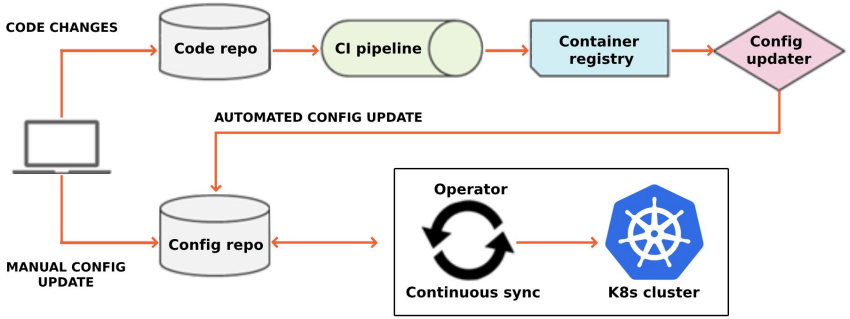




- Proteggere le **credenziali**

gestendo centralmente i **secret sotto Kubernetes** (software di orchestrazione e gestione di container) = **protezione delle credenziali** (come certificati, chiavi, password e token) per utenti non umani come app e server, per accedere alle risorse IT

- Validare continuamente gli **applicativi** monitorando le differenze tra codice sorgente e configurazioni dell'infrastruttura



tramite **GitOps** (Git = sistema di controllo delle versioni che monitora le variazioni al codice)

Si semplificano i workflow automatizzati prevenendo violazioni dei dati, manomissioni, furti ed accessi non autorizzati

Mentimeter

Time to interact!

Answer this quick survey to help us improve

(Remember to write down your username @fbk in the open answers)


Grazie
www.fbk.eu