ItaliaSec
SECURING ITALY FROM
CYBER THREATS

Come Implementare Strategie Zero Trust per Mitigare Efficacemente le Insider Threats

VINCENZO CALABRÒ – Ministero dell'Interno

who am i

Formazione

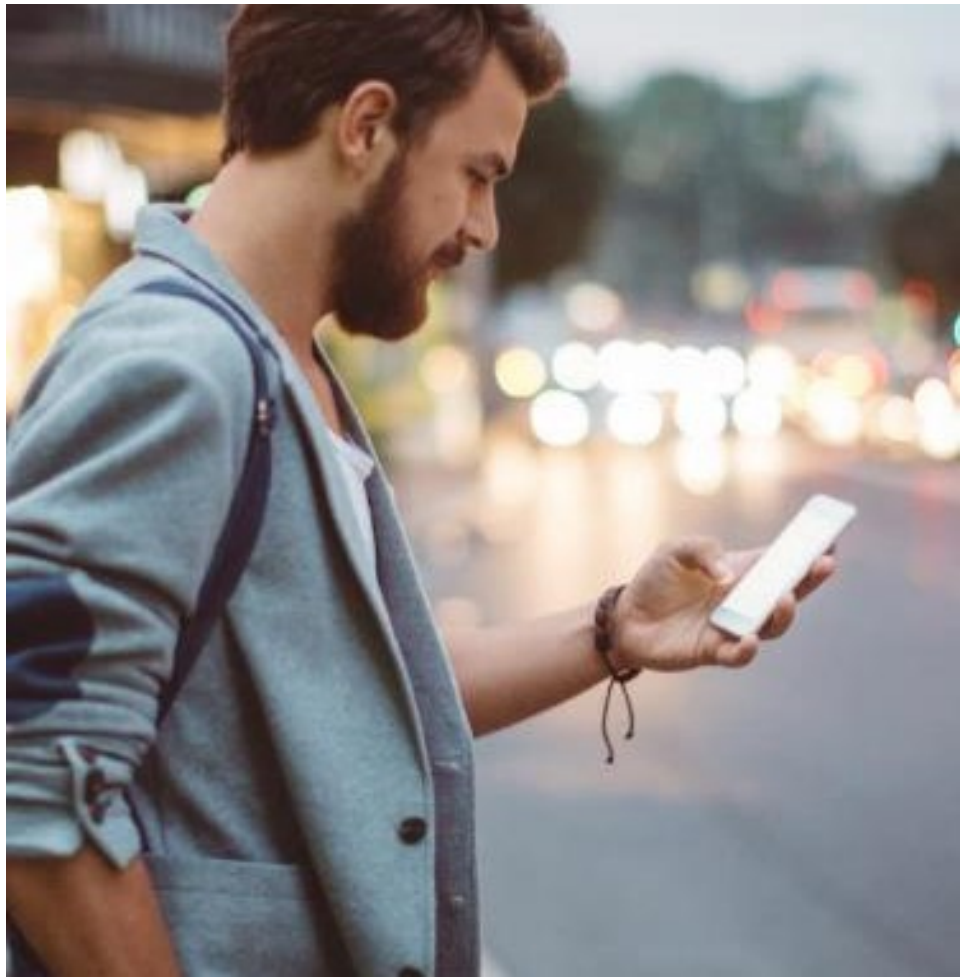
- laureato in ingegneria informatica (università la sapienza di roma) e sicurezza informatica (università di milano)
- specializzato in advanced cybersecurity (stanford university)
- certificato in cybersecurity engineering and software assurance e digital forensics (carnegie mellon university)

Esperienza professionale

- funzionario alla sicurezza cis (ministero dell'interno)
- professore a contratto di tecnologie per la sicurezza informatica
- consulente in sicurezza informatica e informatica forense
- relatore e autore sui temi della cybersecurity

LinkedIn vincenzocalabro.it

Agenda



Cosa sono l'Insider Threat e l'Insider Risk?

Gli scenari di Insider Threat

Le azioni per mitigare l'Insider Threats

Le peculiarità del Modello Zero Trust

Implementare Strategie Zero Trust

Considerazioni finali

Definizioni

Insider Threat

Il potenziale di un individuo che ha o ha avuto accesso autorizzato alle risorse critiche di un'organizzazione di utilizzare il proprio accesso, intenzionalmente o involontariamente, per agire in un modo che potrebbe influire negativamente sull'organizzazione

Insider Threat Actor (o Insider)

Un individuo che ha o ha avuto accesso autorizzato alle risorse critiche di un'organizzazione.

- Lavoratore in servizio e ex dipendente
- Consulente esterno
- Partner

Insider Threat Scenarios

I diversi modelli con cui un insider threat actor può influenzare negativamente l'organizzazione.

Insider Risk

L'impatto e la probabilità della realizzazione di una minaccia interna

Insider Risk Management Program (IRMP)

Un insieme deputato di capacità e risorse appositamente allocate per mitigare le minacce interne e gestire i rischi interni

I principali scenari di insider threat

1. Frode
2. Furto di proprietà intellettuale
3. Sabotaggio informatico
4. Uso improprio dell'accesso autorizzato
5. Incidenti non intenzionali
   (disclosure o perdita di strumenti o documenti)
6. Spionaggio per la sicurezza nazionale
7. Social Engineering
8. Violenza sul posto di lavoro

ItaliaSec
SECURING ITALY FROM CYBER THREATS

Azioni per mitigare l'insider threat

Conosce e proteggere le risorse critiche

1. Condurre una valutazione del rischio
2. Mantenere un inventario delle risorse
3. Condurre una valutazione dell'impatto sulla privacy (PIA)

Sviluppare un programma di gestione del rischio Insider (IRMP)

- la risorsa deputata e dedicata dell'organizzazione
  per mitigare le minacce interne e gestire il rischio interno.

Documentare in modo chiaro e applicare in modo coerente i controlli amministrativi

Monitorare e rispondere a comportamenti sospetti o dannosi, a partire dal processo di assunzione

Anticipare e gestire i problemi negativi nell'ambiente di lavoro

Considerare attendibili le minacce provenienti da insider e entità esterne nelle valutazioni dei rischi a livello aziendale

Essere particolarmente vigili riguardo ai social media

Gestire la struttura e le attività per ridurre al minimo lo stress e gli errori interni

Incorporare la consapevolezza delle minacce interne nella formazione periodica sulla sicurezza per tutti i lavoratori

Sviluppare una procedura completa di licenziamento

Adottare incentivi positivi per allineare la forza lavoro e l'organizzazione

Azioni per mitigare l'insider threat

Implementare rigide politiche e policies di gestione delle password e degli account

Istituire severi controlli di accesso e politiche di monitoraggio sugli utenti privilegiati

Implementare soluzioni per monitorare le azioni dei lavoratori e correlare le informazioni da più origini dati

Monitorare e controllare l'accesso remoto da tutti gli endpoint, compresi i dispositivi mobili

Stabilire una regole di base per il comportamento normale sia per le reti che per i lavoratori

Applicare la separazione dei doveri e del privilegio minimo

Definire accordi di sicurezza espliciti per i servizi cloud, in particolare le restrizioni di accesso e le capacità di monitoraggio

Istituzionalizzare i controlli di modifica del sistema

Implementare processi di backup e ripristino sicuri

Mitigare l'esfiltrazione di dati non autorizzata

Imparare dagli episodi di minacce interne del passato

ItaliaSec
SECURING ITALY FROM
CYBER THREATS

Implementare Strategie Zero Trust

Zero Trust

Lo Zero Trust è un insieme di principi di sicurezza che considera ogni componente, servizio e utente di un sistema come se fosse continuamente esposto, e quindi potenzialmente compromesso, da un attore (interno o esterno) malintenzionato.

L'identità di un utente è verificata ogni volta che richiede di accedere ad una nuova risorsa e ogni accesso viene mediato, registrato e analizzato. È come mettere dei sensori all'interno di un sistema, ogni volta che scatta un allarme, si riceve un segnale, viene analizzato e convalidato, per capire cosa sia successo.

In pratica, un approccio zero-trust potrebbe somigliare alla sostituzione di un sistema single sign-on, che consente agli utenti di accedere una sola volta per utilizzare più applicazioni, con un'identità nota e verificata basata su cloud.

Principi di Zero Trust

ItaliaSec
SECURING ITALY FROM
CYBER THREATS

Tutti i sistemi aziendali sono considerati risorse

L'azienda garantisce che tutti i sistemi di proprietà siano nel loro stato più sicuro possibile

Tutte le comunicazioni vengono effettuate in modo sicuro indipendentemente dalla posizione nella rete

L'accesso alle singole risorse aziendali viene concesso in base alla connessione

L'autenticazione dell'utente è dinamica e rigorosamente applicata prima dell'accesso

L'accesso alle risorse è determinato dalla policy, incluso lo stato osservabile dell'utente, del sistema e dell'ambiente

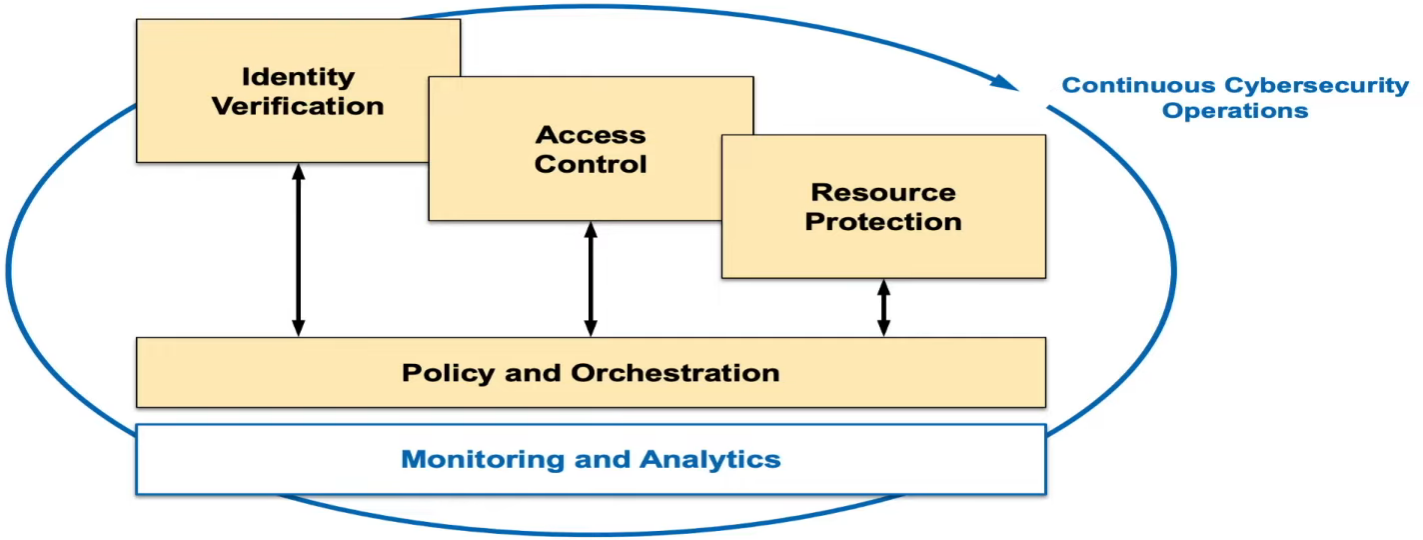
Zero Trust Architecture

La **Zero Trust Architecture** (ZTA) è un modello che assicura i requisiti di riservatezza, integrità e disponibilità (CIA) seguendo i principi di sicurezza **Zero Trust**.

Le ZTA generalmente includono i seguenti componenti:

- **Identity verification** – strong multi-factor authentication di utenti e dispositivi
- **Access control** - accesso sicuro e approvato alle risorse
- **Resource protection** - controllo granulare dell'utilizzo delle risorse approvato in base all'identità
- **Policy and orchestration** - gestione dinamica dell'uso del sistema
- **Monitoring and analytics** - analisi dell'utilizzo del sistema e delle funzioni di sicurezza
- **Continuous operations** - processo per gestire i rischi supportando la continuità operativa

Zero Trust Architecture Framework



Transizione verso una Zero Trust Architecture

ItaliaSec
SECURING ITALY FROM CYBER THREATS

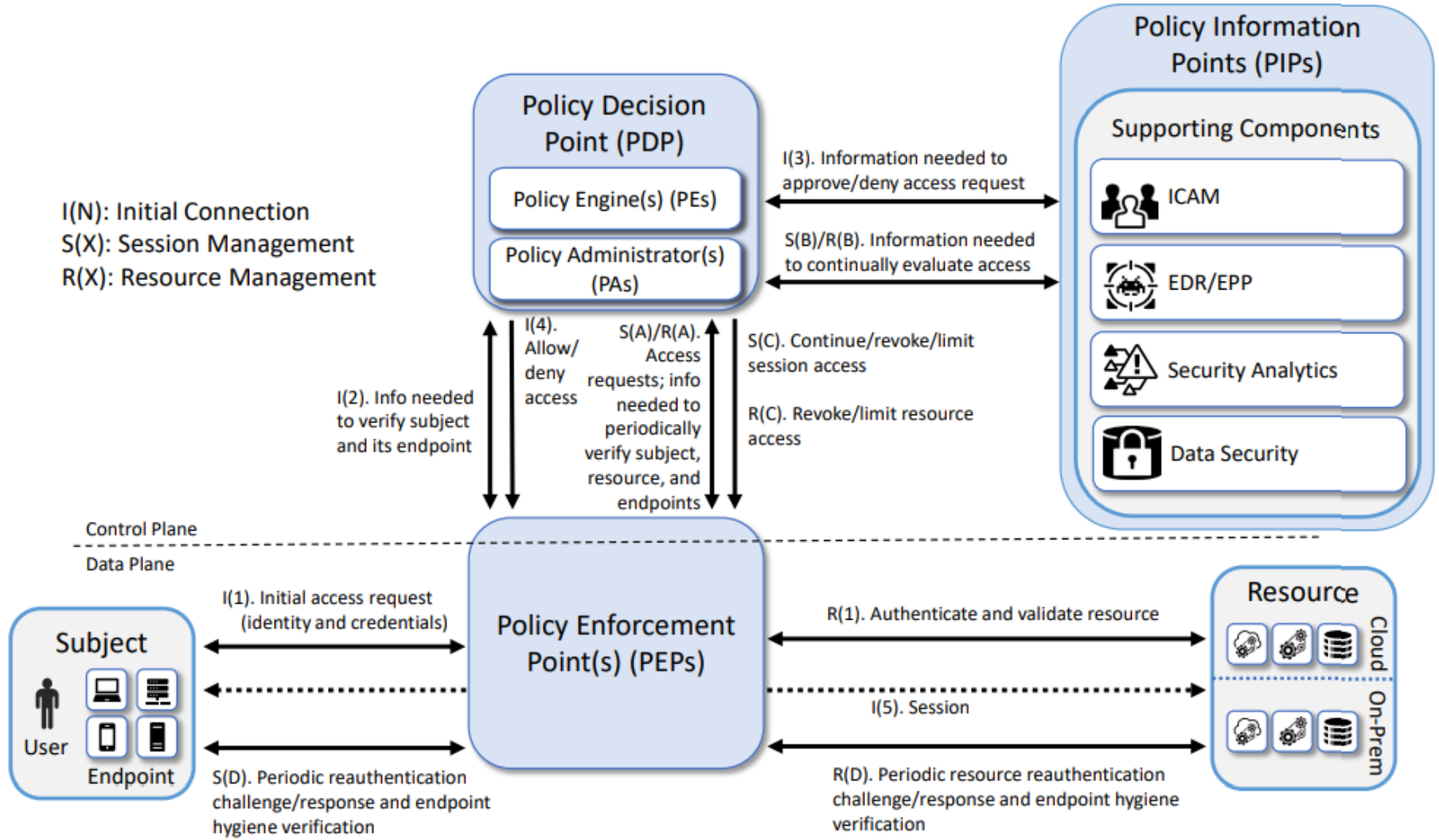
Zero Trust Components	Current State	Future State
Identity Verification	Corporate-hosted Single Sign-on (SSO)	Cloud-based Identity
Access Control	Continuous all-to-all connectivity	Brokered one-to-one connectivity (e.g. ZTNA)
Resource Protection	Encryption at rest, Redundant applications	Just-In-Time authentication, DRM, Data provenance, Resilient applications
Policy and Orchestration	Static, bespoke, siloed configurations	Dynamic decision making
Monitoring and Analytics	Edge and endpoint monitoring	Integrated system-wide monitoring and analytics
Continuous Cybersecurity Operations	Compliance focused	Periodic adversarial testing

Implementations can iterate towards future state capabilities

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

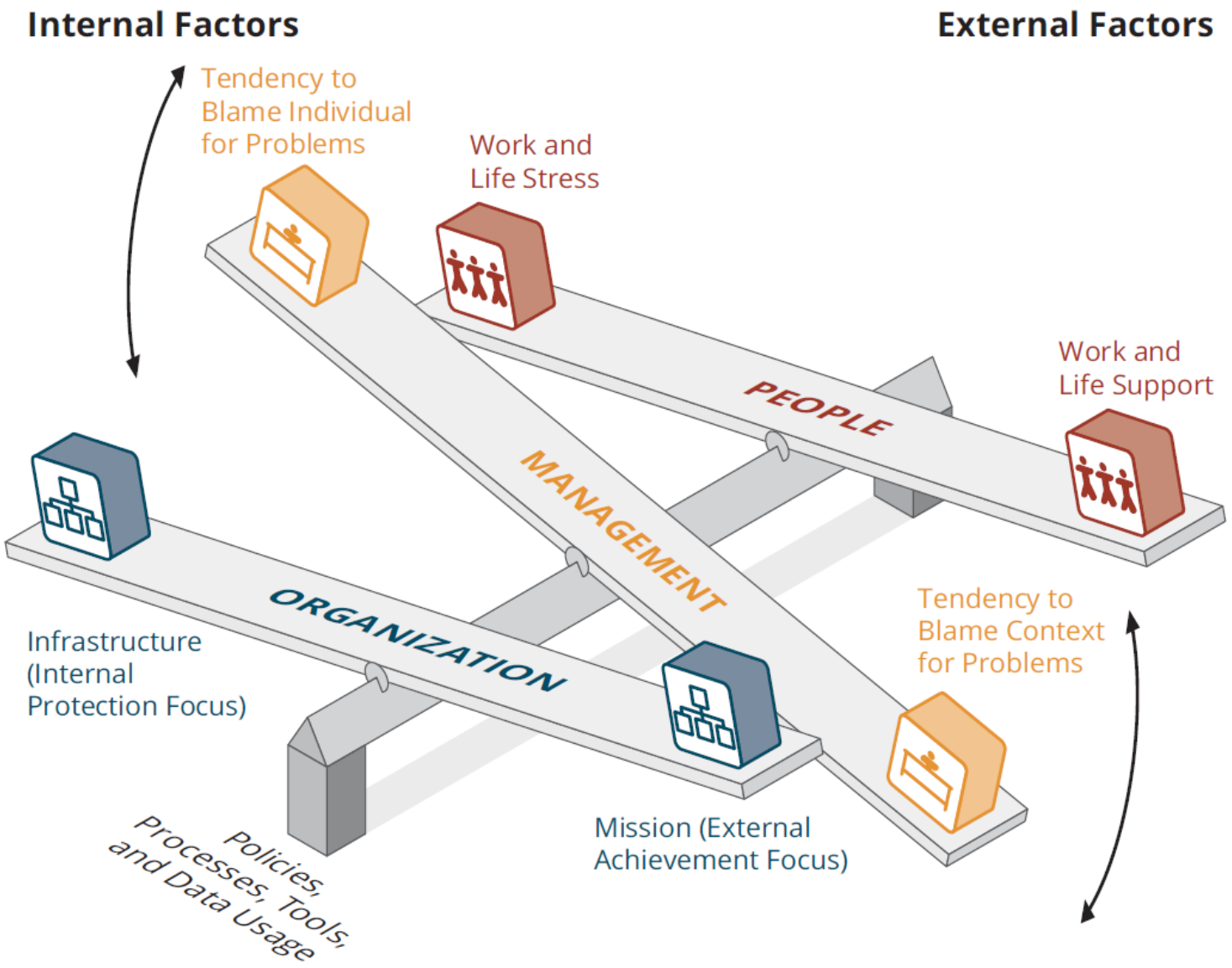
Zero Trust Architecture Core Components



NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Trovare il Giusto Bilanciamento



Criticità

L'inserimento di nuove politiche, processi, strumenti e utilizzo dei dati deve tenere conto dei valori e della cultura organizzativa.
Occorre trovare il giusto equilibrio, ovvero considerare una certa tolleranza al rischio, per evitare frizioni o blocchi legati alla resistenza al cambiamento e ai vincoli normativi.

Soluzione

Implementare una strategia graduale, con la giusta combinazione di politiche, procedure e controlli tecnici, che riduca progressivamente il rischio degli insider threats.

Considerazioni finali

Non esiste un unico approccio per tutte le organizzazioni - occorre tenere conto delle esigenze di ogni organizzazione

Utilizzare un approccio olistico – per implementare efficacemente il modello zero trust è necessario il commitment dell'organizzazione, un impegno per il cambiamento organizzativo

Le implementazioni zero trust richiedono modifiche alla cultura della cyber security

L'architettura zero trust non richiede necessariamente nuove apparecchiature e non rende i sistemi bloccati tali da non poter essere utilizzabili