INDICAM

PER LA TUTELA DELLA PROPRIETÀ INTELLETTUALE

CONFINDUSTRIA VENETO EST

Area Metropolitana
Venezia Padova Rovigo Treviso

INVESTIGATION®
INTELLIGENCE
CYBER SECURITY

TRADE SECRETS

Le regole di protezione a monte: il Piano di Security

Jacopo Maria Tavaroli Eichholzer

INTRODUZIONE

1. IMPLEMENTARE UNA STRATEGIA

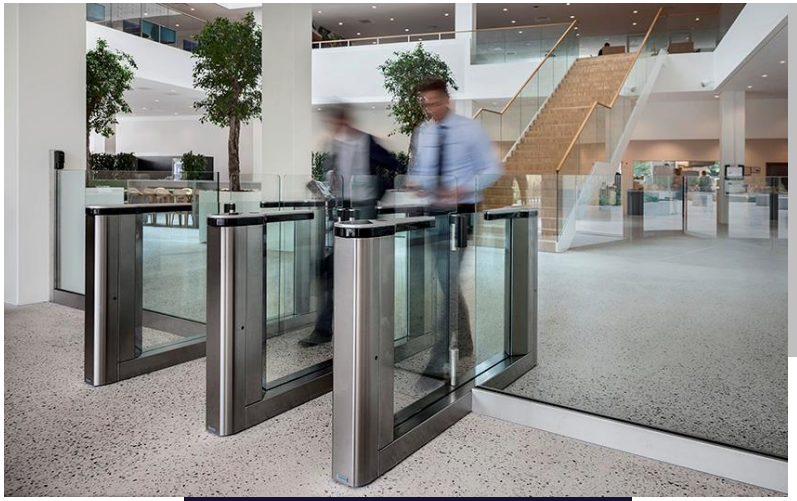
- Panoramica sui framework di sicurezza e la loro applicazione
- Piano di sicurezza strutturato
- Garantire conformità, mitigazione dei rischi e resilienza.

2. PRINCIPALI FRAMEWORK DI CYBERSECURITY

- NIST CSF: Gestione della sicurezza basata sul rischio
- ISO 27001: Standard globali di sicurezza e conformità
- CIS Controls: Controlli di sicurezza pratici per le organizzazioni
- MITRE ATT&CK: Analisi delle minacce e dei modelli di attacco
- Zero Trust Architecture: Accesso con privilegi minimi e monitoraggio continuo.

3. DEFINIZIONE DI UN AMBIENTE SICURO

- Identificare rischi ed asset
- Identificare quali principi di sicurezza si vogliono applicare alla rete
- Definire i controlli al fine della protezione
- Monitorare ed identificare le potenziali minacce



MISURE FISICHE

... ma attenzione alla gestione delle variabili laterali:

GDPR guide*

FT graphic/Dreamstime
© FT

* General Data Protection Regulation

MISURE FISICHE

CLEAN DESK

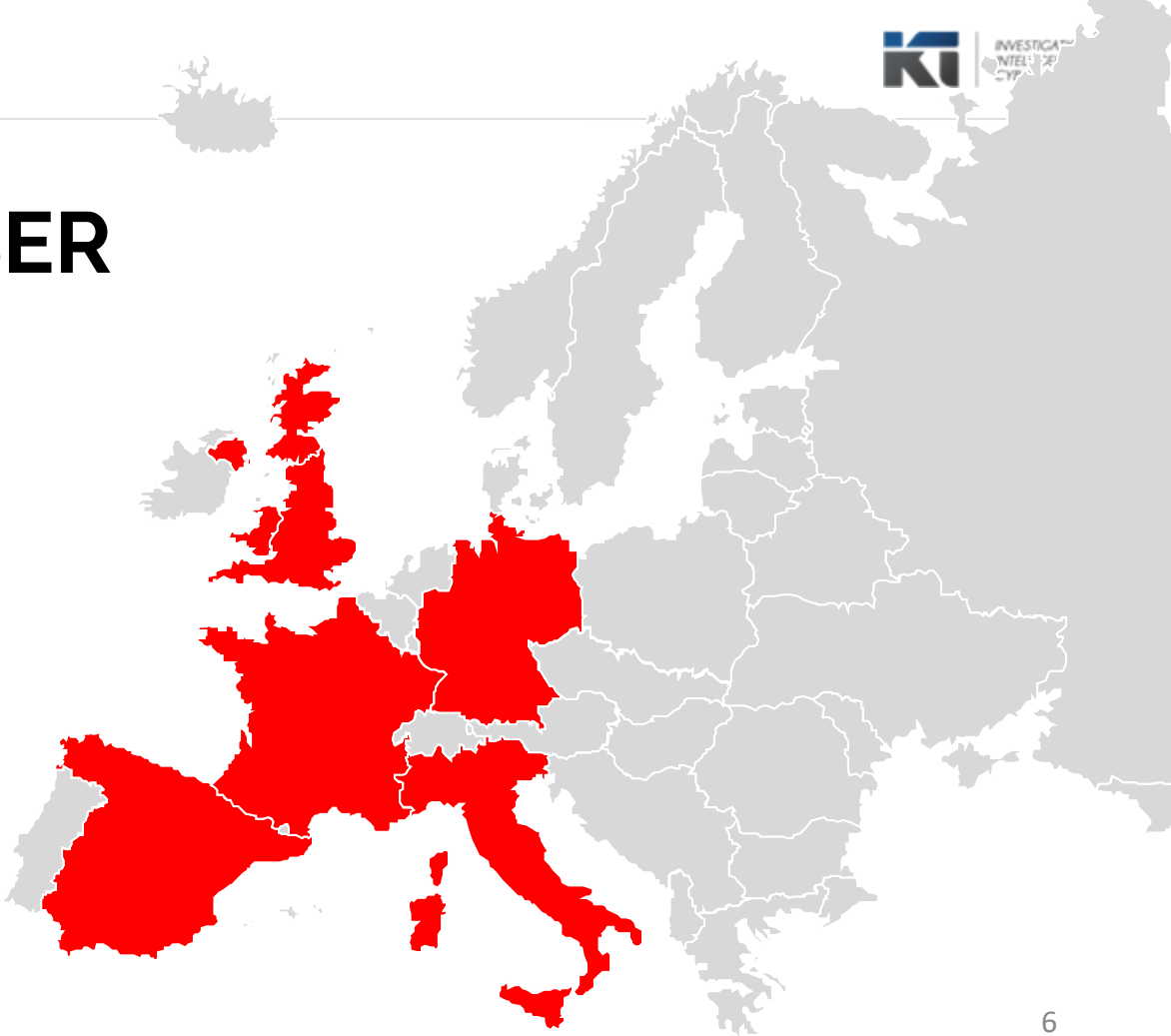
GESTIONE DOCUMENTALE

SOCIAL ENGINEERING

- Phishing: Email fraudolente che spingono a fornire dati sensibili
- Vishing: Truffe telefoniche per carpire informazioni riservate
- Baiting: Uso di dispositivi infetti (USB) per compromettere sistemi
- Pretexting: Creazione di scenari falsi per ottenere informazioni
- Tailgating: Accesso fisico non autorizzato sfruttando la fiducia

INCIDENTI CYBER EUROPA 2024

Nel 2024, diversi paesi europei hanno registrato un aumento significativo degli attacchi informatici, in particolare dei ransomware. Secondo il "Rapporto Clusit 2024", l'Europa ha subito il 29% degli attacchi informatici globali nel primo semestre dell'anno, in crescita rispetto al 23% del 2023.
(fonte innovationpost.it)
In particolare, l'Italia ha registrato un aumento degli attacchi ransomware, posizionandosi al 3° posto a livello mondiale e al 1° nell'Unione Europea nel mese di luglio 2024. (fonte ACN)
Anche la Spagna ha visto un incremento significativo, salendo al 5° posto tra i paesi più colpiti al mondo da ransomware nel 2024. (fonte elpais.com)
Questi dati evidenziano una crescente minaccia informatica in Europa, sottolineando la necessità di rafforzare le misure di sicurezza cibernetica a livello nazionale e comunitario.



PREPARARE UN PIANO DI SECURITY - PRIMA

ANALISI

È fondamentale condurre un'analisi puntuale rispetto che cosa vogliamo procedere e quali sono i rischi accettabili e non

PROGETTO

Il proprio team di sicurezza con l'eventuale support di consulenti è in grado di condurre un'analisi di quanto si può realizzare ed il budget conseguente

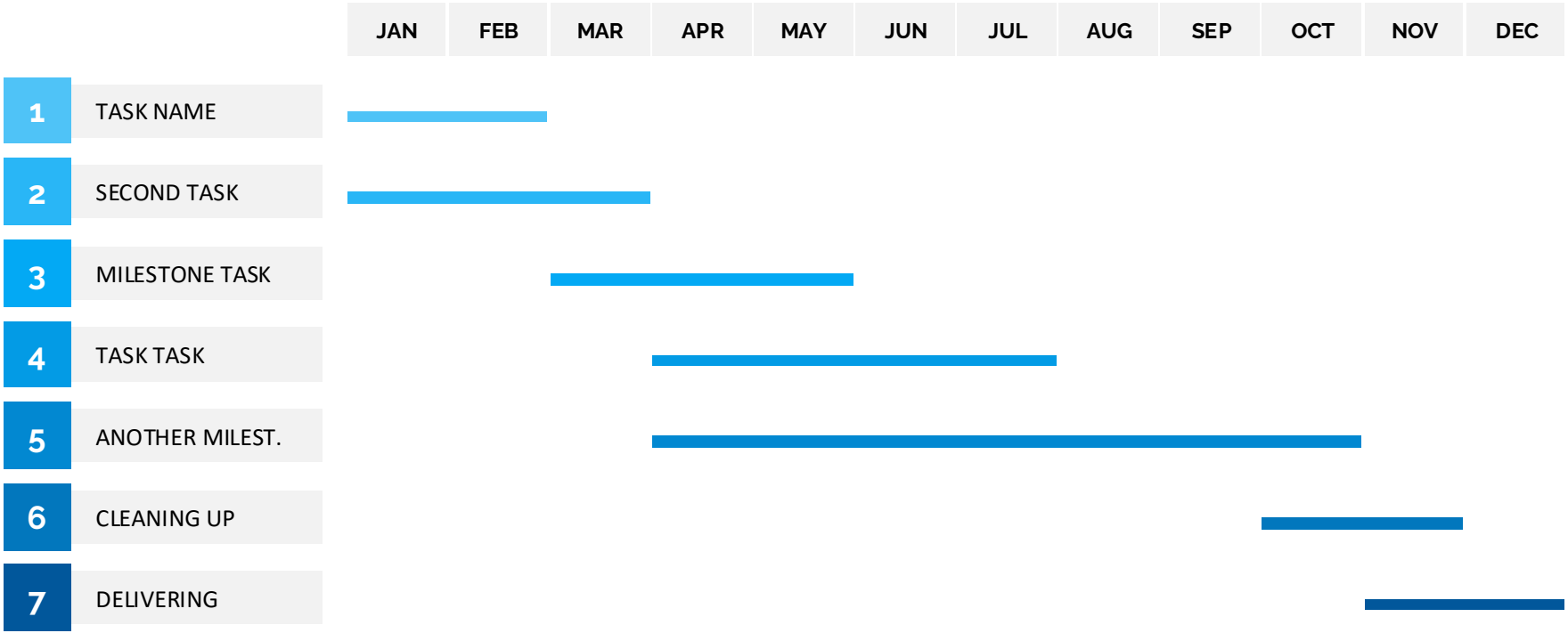
IMPLEMENTAZIONE

L'implementazione comporta anche diversi mesi di attività una volta avviata e prima di arrivare al completamento è normale avere delle aree più scoperte di alte, per questo è importante la pianificazione del progetto

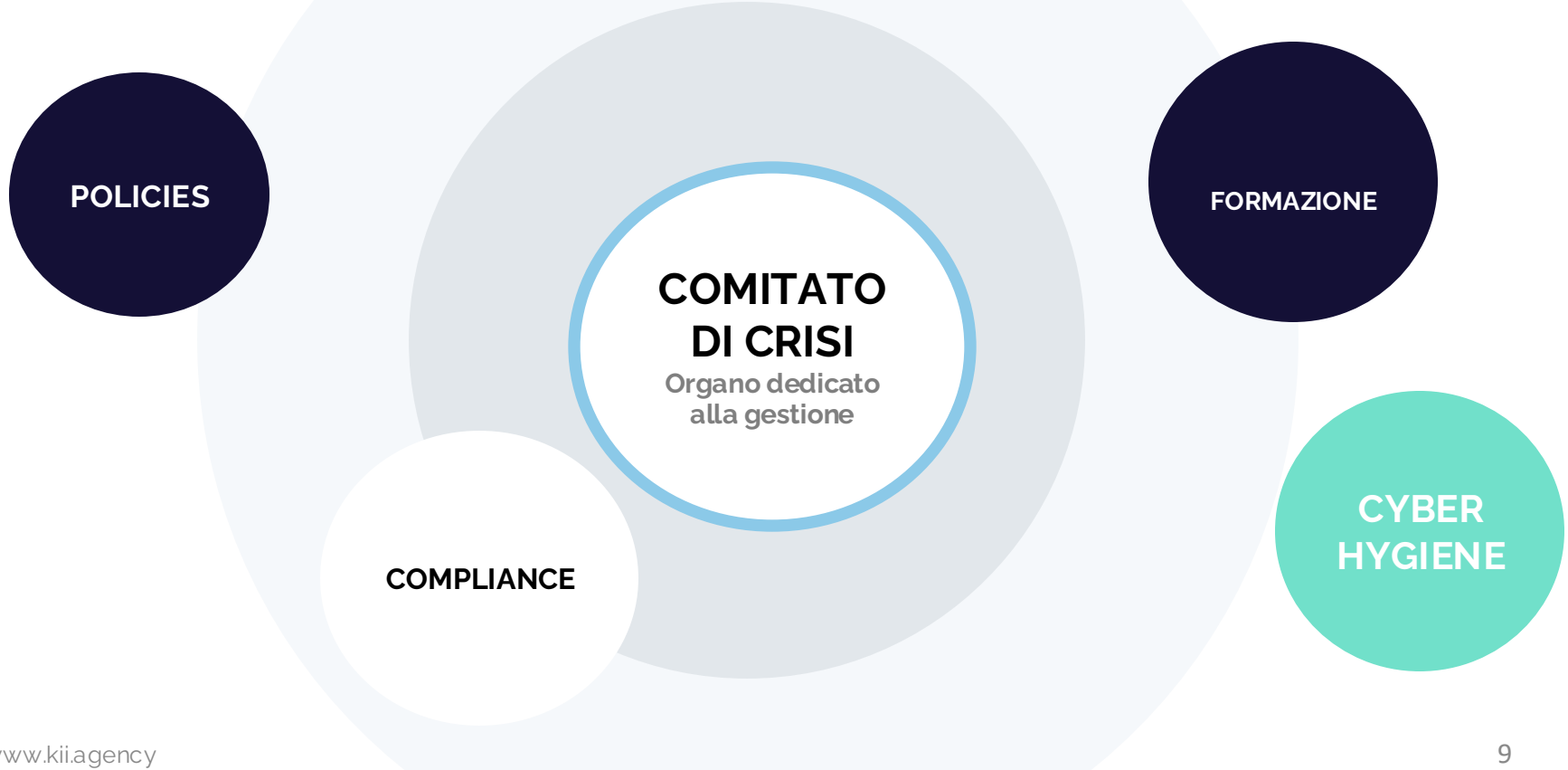
MONITORAGGIO

Una volta realizzato è molto importante mantenere il corretto monitoraggio di quanto implentato per accertarsi che non si presentino eventi critici o malfunzionamenti

PREPARARE UN PIANO DI SECURITY - DOPO



COSA FARE ADESSO



DOMANDE?

GRAZIE!

INVESTIGATION®
INTELLIGENCE
CYBER SECURITY