Convenzione Intercent-ER

SERVIZI DI SICUREZZA INFORMATICA 2

FASTWEB EY IBM TINEXTA CYBER Gpi Cyberdefence.

GLI OBIETTIVI DI INTERCENT-ER

Istituita con la legge regionale n. 11 del 2004, l'Agenzia Intercent-ER è la centrale di acquisto dell'Emilia-Romagna.

Tramite lo svolgimento di procedure di gara aggregate e la gestione di sistemi telematici, si propone di:

RAZIONALIZZARE LA SPESA
per beni, servizi e lavori delle P.A. del territorio, con particolare riferimento alla spesa sanitaria

INCREMENTARE LA QUALITÀ
dei beni e dei servizi utilizzati dalla P.A.

MIGLIORARE EFFICIENZA E TRASPARENZA
dei processi di acquisto

DEMATERIALIZZARE
l'intero ciclo degli acquisti pubblici

ACCRESCERE LA COMPETITIVITÀ
del mercato e del tessuto produttivo regionale

PROMUOVERE L'E-PROCUREMENT
e l'uso dei sistemi telematici

GLI AMBITI DI ATTIVITA'

DEMATERIALIZZAZIONE DEGLI ACQUISTI

Gestione del nodo telematico di interscambio (NoTI-ER)

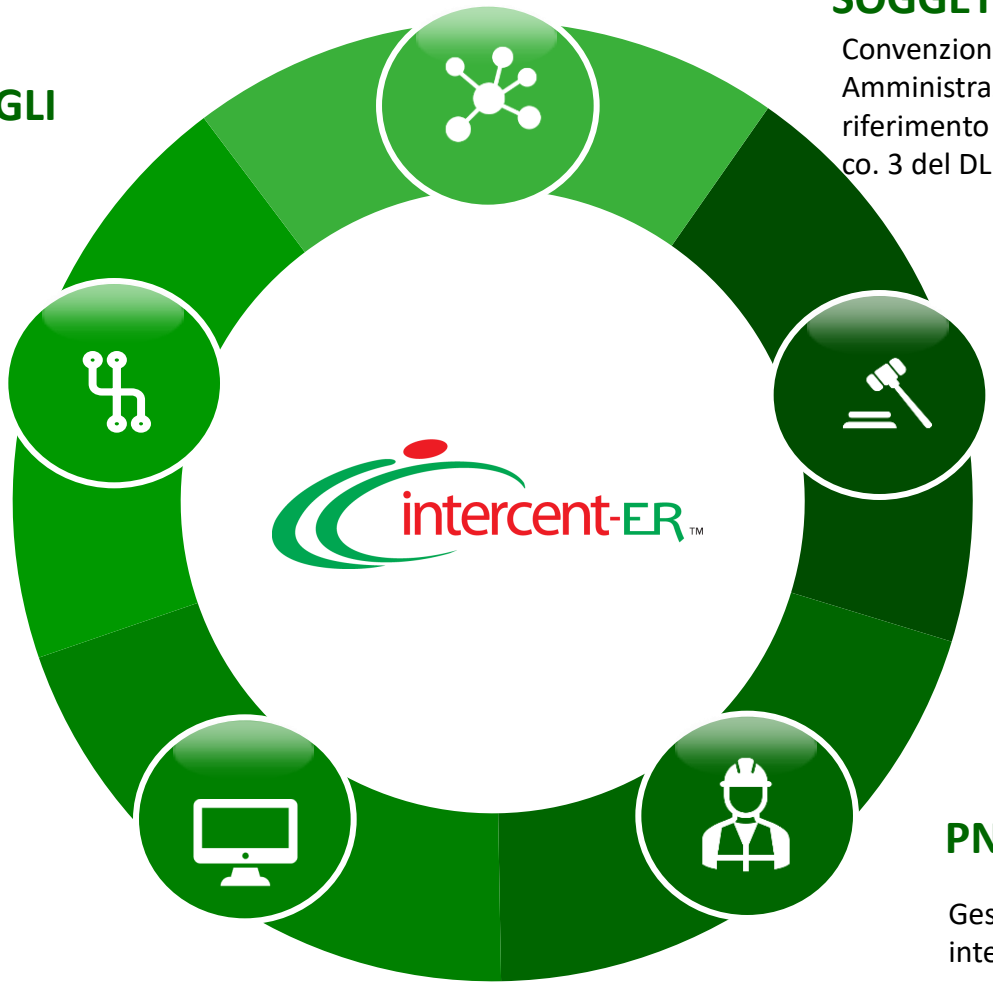
Promozione di strumenti di integrazione fra sistemi

SVILUPPO DELL'E-PROCUREMENT

Gestione e promozione del sistema di e-procurement regionale (SATER)

Mercato elettronico regionale (MERER)

Utilizzo autonomo della piattaforma da parte degli enti del territorio



CENTRALE DI ACQUISTO / SOGGETTO AGGREGATORE

Convenzioni/Accordi quadro in favore delle Pubbliche Amministrazioni dell'Emilia-Romagna, con particolare riferimento alla gestione delle categorie di cui ai DPCM ex art.9 co. 3 del DL 66/2014

CENTRALE DI COMMITTENZA

Gestione delle procedure di gara sopra soglia per le Direzioni Regionali e per gli Enti regionali

PNRR E LAVORI PUBBLICI

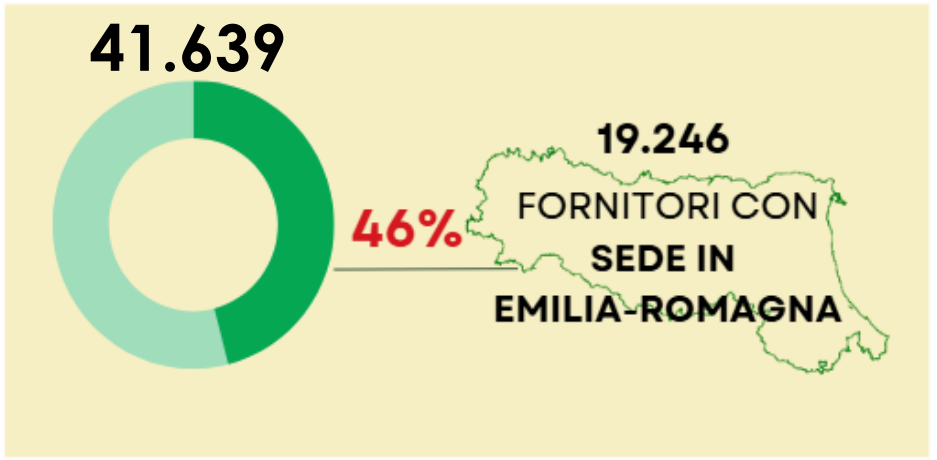
Gestione degli appalti per la realizzazione degli interventi del PNRR

Procedure di affidamento di lavori pubblici (in corso di implementazione)

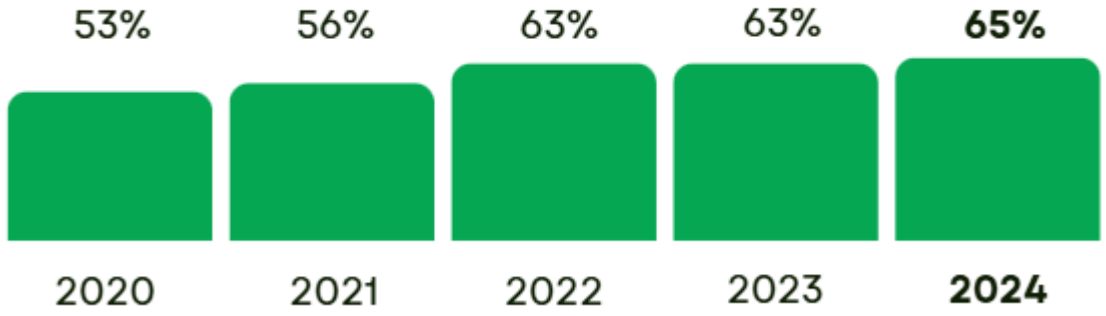
PRINCIPALI RISULTATI

SPESA GESTITA ANNUA

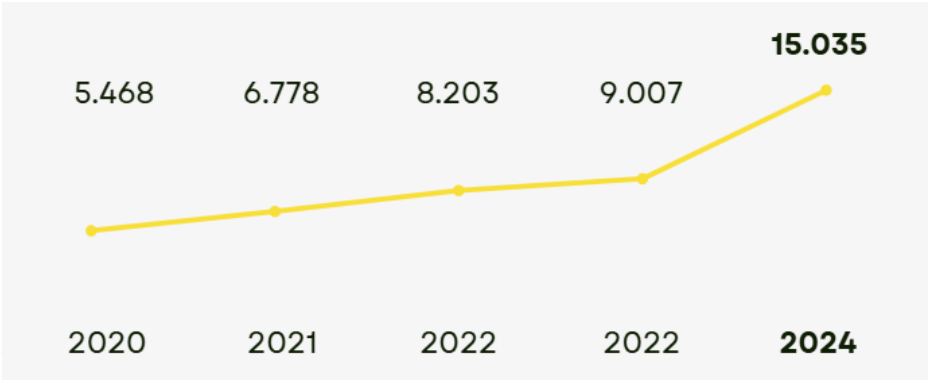
OPERATORI ECONOMICI PRESENTI SU SATER



INCIDENZA IC SU SPESA SANITARIA



GARE TELEMATICHE EFFETTUATE SU SATER



DESCRIZIONE E TEMPISTICHE DELLA CONVENZIONE

Convenzione per la fornitura di servizi relativi alla **Sicurezza Informatica** per le Pubbliche Amministrazioni della Regione Emilia-Romagna.

Oggetto

- **Servizi di Sicurezza Informatica:** servizi necessari e funzionali a garantire adeguati livelli di sicurezza dei sistemi IT nel loro complesso, dei dati trattati e in generale delle informazioni.
- **Valore Economico 40M€**

Durata

- **Durata**: 36 mesi + eventuale rinnovo 24 mesi*
- **Ordinativi di Fornitura**: dai 12-36 mesi per i servizi a canone** - durata variabile per i fabbisogni professionali
- **Data di attivazione:** 5/02/2024

** Se prima della scadenza della Convenzione viene esaurito l'importo massimo spendibile, già eventualmente incrementato del quinto d'obbligo, la Convenzione viene considerata chiusa e le PA non potranno emettere ulteriori Ordinativi di Fornitura*

*** gli ordinativi di fornitura potranno avere durata massima pari alla data di scadenza della Convenzione. Durante l'ultimo anno di Convenzione sarà possibile sottoscrivere Ordinativi di Fornitura di durata inferiore ai 12 mesi*

Fornitore

Fastweb **mandataria** del RTI così composto:
Fastweb (52%) , EY (18%), IBM (15%), Tinexta Cyber (8%), GPI Cyberdefence (7%)

Yoroi srl (una delle mandanti del RTI aggiudicatario) è confluita nella società Tinexta Cyber SpA, la quale è subentrata ex lege e senza soluzione di continuità in tutti i rapporti, attivi e passivi della Società.

DESTINATARI DELLA CONVENZIONE

La Convenzione si colloca nell'ambito delle iniziative di acquisto della centrale di committenza dell'Emilia Romagna Intercent-er. Secondo quanto previsto dall' articolo 19, comma 5, della legge regionale n. 11/2004.

La Regione – AA.SS.LL.

- **Enti e Organismi regionali**
- **Associazioni e Consorzi**
- **Enti e Aziende del Servizio Sanitario**

Enti Locali - Istituti di istruzione

- **Enti ed Organismi locali**
  le loro associazioni, unioni e consorzi, quali le aziende e gli istituti, anche autonomi, le istituzioni, gli organismi di diritto pubblico e le società strumentali partecipate in misura totalitaria o maggioritaria da tali soggetti
- **Istituti di istruzione scolastica e universitaria**

EROSIONE – AMMINISTRAZIONI ADERENTI

La Convenzione, alla data del 14/05/2025, è stata utilizzata per oltre 5.000.000,00 di euro dalle seguenti amministrazioni regionali:

La Regione – AA.SS.LL.

- GIUNTA REGIONALE EMILIA-ROMAGNA
- LEPIDA S.C.P.A.
- CINECA
- AZIENDA USL DI IMOLA

Enti Locali - Istituti di istruzione

- COMUNE DI REGGIO NELL'EMILIA
- COMUNE DI FERRARA
- COMUNE DI RAVENNA
- COMUNE DI SAN LAZZARO DI SAVENA
- UNIVERSITÀ DI MODENA E REGGIO EMILIA
- ALMA MATER STUDIORUM - UNIVERSITA' DI BOLOGNA: SEDE DI (BOLOGNA, CESENA, FORLI', RAVENNA, RIMINI)

PRINCIPIO DI SEGREGAZIONE DEI COMPITI

La Convenzione Sicurezza Informatica nasce da una «costola» della precedente Convenzione IT System Management perché, in attuazione del principio di **“Segregazione dei compiti” (Segregation of Duties - SOD)**, per separare le responsabilità, si è ritenuto incompatibile l’affidamento in capo al medesimo operatore economico delle attività di **gestione, monitoraggio e sviluppo dei sistemi (Lotto 1)** e delle attività di **sicurezza sui medesimi sistemi (Lotto 2)**, qualora riferite alla stessa Amministrazione. Questo vale sia per il fornitore aggiudicatario che per i suoi eventuali subappaltatori.

ELENCO DEI SERVIZI PREVISTI

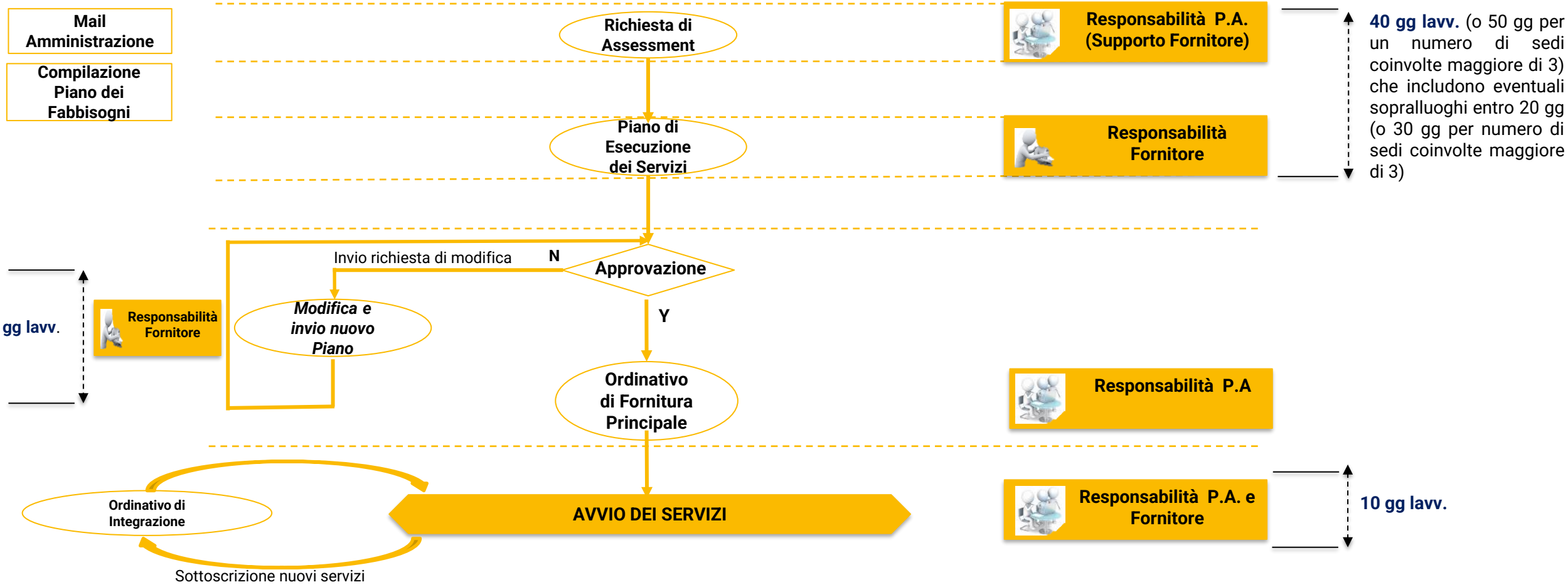
Servizio	Descrizione
SOC - Monitoraggio in tempo reale di eventi di sicurezza	Il servizio di Security Operation Center (SOC) gestisce e monitora i servizi di sicurezza, analizzando report e log per risolvere o mitigare le minacce.
Conduzione operativa e service Desk sistemistico di sicurezza informatica	Il servizio garantisce una gestione e manutenzione ordinaria dell'infrastruttura di sicurezza informatica dell'amministrazione secondo gli standard di continuità operativa, utilizzando sistemi di ticketing e gestione.
Servizio di Incident response & remediation	Il servizio di Incident Response & Remediation (IRR) analizza e investiga eventi che possono compromettere la disponibilità, integrità o riservatezza delle informazioni. Il servizio di Digital Forensic (DF) garantisce che le prove informatiche siano conformi ai requisiti legali e utilizzabili in processi penali.
Servizio di threat intelligence / APT-feed / asset tracker & data leak	Il servizio di Threat Intelligence (TI) monitora, raccoglie e analizza proattivamente informazioni su minacce per prevenire attacchi.
Servizio di User and entity behavior analytics (UEBA)	Il servizio di User and Entity Behaviour Analysis (UEBA) valuta i rischi tramite algoritmi di ML, AI e analytics, integrando dati nel SIEM.
Servizio di Host Hardening	Il servizio di Host Hardening aumenta la sicurezza di rete, server, storage e postazioni di lavoro delle amministrazioni.
Servizio di Security Awareness	Il servizio di Security Awareness sensibilizza l'amministrazione sulla sicurezza, sviluppando competenze per prevenire e reagire agli incidenti.
Servizio di Vulnerability Management	Il servizio di Vulnerability Assessment (VA) e Vulnerability Management (VM) identifica e mitiga proattivamente le vulnerabilità su dispositivi di rete, software e applicazioni.
Servizio di Application Security Testing	Il servizio di Application Security Testing (AST) evidenzia vulnerabilità e misure di mitigazione in applicativi e sistemi, seguendo normative e standard riconosciuti.
Figure professionali, disponibilità e aggiornamento delle risorse	Ad integrazione dei Servizi precedentemente indicate (Security Advisor, Governance & risk compliance (GRC) consultant. Security Specialist, Security Analyst, Vulnerability Researcher, Incident Handler, Digital forensic, CyberSecurity & Privacy Legal Advisor)

PARTNERSHIP E TECNOLOGIE DEL RTI

MODALITA' DI ADESIONE - PROCESSO

Percorso operativo per qualificare e dimensionare i fabbisogni ed arrivare alla stipula del Contratto Esecutivo/Ordinativo.

- **Fase 1: aggiudicazione della convenzione** a seguito di Gara indetta e **gestita da Intercenter**. Questa fase si è conclusa con l'individuazione dei Fornitori aggiudicatari
- **Fase 2:** le PA affidano ciascun singolo **Ordinativo di Fornitura** al fornitore aggiudicatario di riferimento **in relazione ai servizi richiesti:**

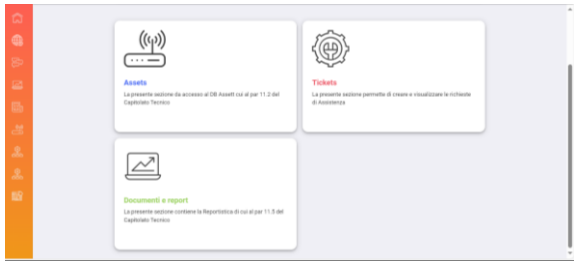


PORTALE DELLA FORNITURA

Il Portale della Fornitura (https://www.intercenter-sicurezza.it/) mette a disposizione dei clienti una dashboard riservata, con accesso facilitato ai principali servizi operativi previsti dal Capitolato Tecnico.

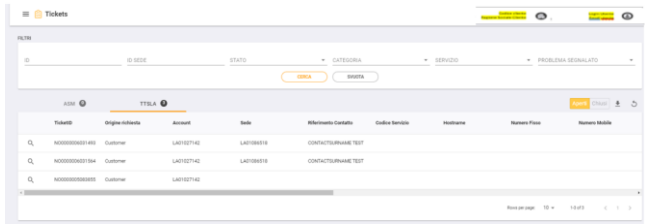
Dashboard di Accesso

- Navigazione semplice verso le aree: **Assets, Tickets, Documenti e Report**.
- Accesso diretto ai contenuti previsti ai paragrafi 11.2 e 11.5 del Capitolato Tecnico.



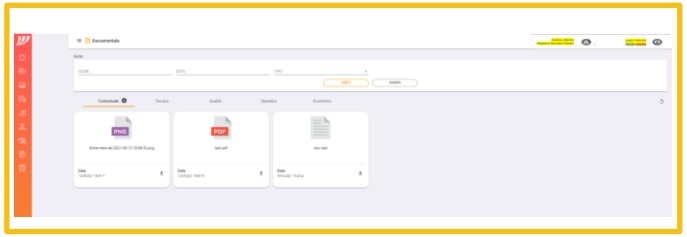
Sezione Tickets

- Inserimento richieste di **Change**.
- Inserimento richieste di **Intervento/Segnalazione evento**.
- **Gestione e visualizzazione dei ticket**.
- Monitoraggio dello stato di avanzamento (Incident **Aperti/Chiusi**).
- Filtri avanzati per una ricerca puntuale.
- Esportazione e download della lista ticket.



Sezione Documenti e Report

- Consultazione della documentazione tecnica e operativa.
- Sottosezioni: **Contrattuale, Tecnica, Qualità, Operativa, Economica**.
- Funzionalità di ricerca e download documenti.



SOC & INCIDENT RESPONSE AND REMEDIATION – USE CASE

Il **servizio SOC** offre monitoraggio continuo, rilevamento proattivo delle minacce e gestione tempestiva degli incidenti, **garantendo una risposta coordinata e mirata** per la protezione degli asset digitali della constituency.

Security Operation Center

Erogazione del servizio di Security Operations Center (SOC) con l'obiettivo di garantire **rilevamento tempestivo** e gestione efficace di eventi e incidenti informatici.
Le due macro-tematiche chiave su cui l'attività è basata sono il **monitoraggio continuo** e in tempo reale degli eventi di sicurezza relativi alle Entità della constituency e l'adozione di un processo strutturato per gestire l'incident life cycle.

Incident Response and Remediation

Attivazione del processo di incident response con **l'obiettivo di garantire una gestione strutturata e tempestiva degli incidenti di sicurezza** rilevati.
Le due macro-tematiche chiave su cui l'attività è basata sono **l'analisi tecnica** approfondita dell'incidente per **definirne impatto**, causa e ambito, e l'esecuzione di **azioni di contenimento e remediation** mirate, in coordinamento con le Entità coinvolte, per ripristinare la normale operatività e prevenire recidive.

SIEM On-Prem
SIEM Nel centro servizi Intercent-er
Incident Response as a Service
SOC As a Service
Gruppo Operativo componibile
Post incident review

SOC – GRUPPO OPERATIVO & INCIDENT LIFE CYCLE

L1 Team

Monitoraggio
Triage

Attività:
- Monitoraggio 24/7
- Triage allarmi
- Notifica al L2

L2 Team

Analisi
Blocco

Attività:
- Contenimento
- Analisi iniziale
- Escalation al L3

L3 Team

War room
Remediation

Attività:
- War Room
- Crisis Managment
- Remediation avanzata
- Root cause analysis

Architect Team

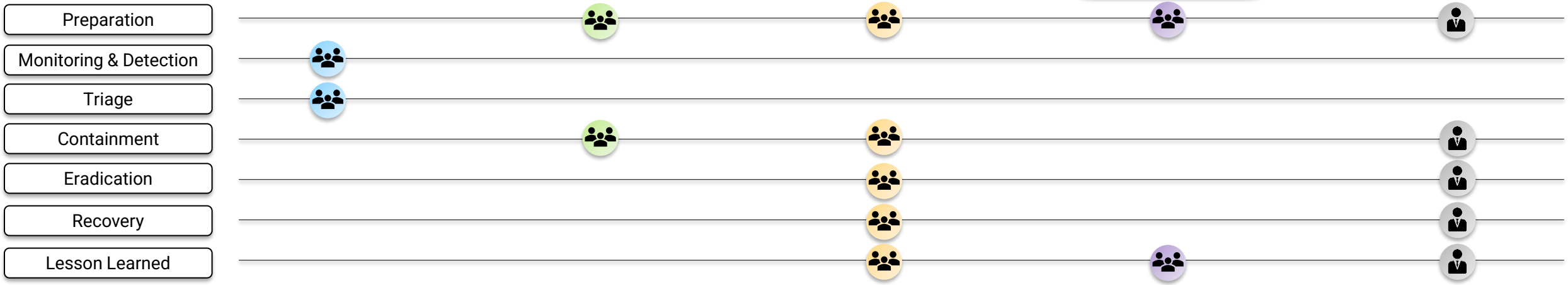
Configurazioni
Tuning

Attività:
- Tuning regole
- Ottimizzazione
- Supporto tecnico cross-team

SOC Manager

Leadership
Report

Attività:
- Coordinamento team
- Definizione SLA/KPI
- Reporting executive



STAGE 1

FONTI DATI:

🌐 Rete
Firewall (Palo Alto, Cisco, Checkpoint, Fortinet)
Monitorare traffico consentito/bloccato.

💻 Endpoint
Log server/workstation (Windows, Linux, macOS)
Rilevare malware, attività non autorizzate.

🔑 Autenticazione
Active Directory, IAM cloud
Identificare accessi legittimi vs. account compromessi.

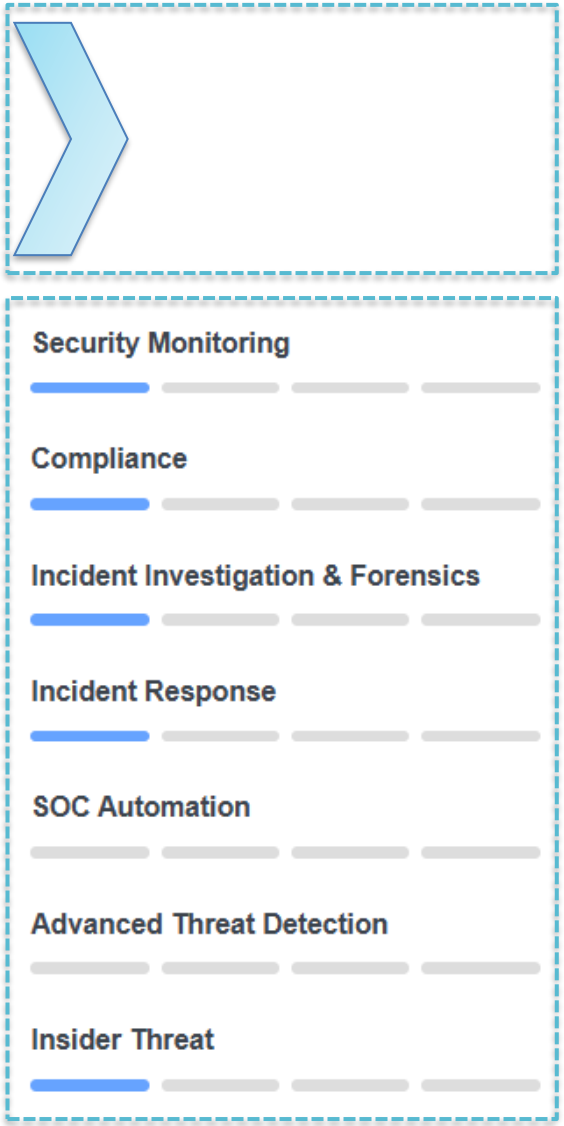
🌍 Web
Proxy, NGFW
Tracciare accessi a siti sospetti/exfiltrati.

1. PROTEZIONE LOG CRITICI
✔ Archiviazione in sistema isolato per prevenire manomissioni da parte di attaccanti.

2. DATI PER INDAGINI BASE
✔ Dati essenziali accessibili per analisi iniziali (team interno o specialisti esterni).

3. BASI PER ANALISI PROATTIVA
✔ Materiali grezzi per mappare l'ambiente e costruire strategie di difesa avanzate.

Collection
Collect basic security logs and other machine data from your environment



STAGE 2

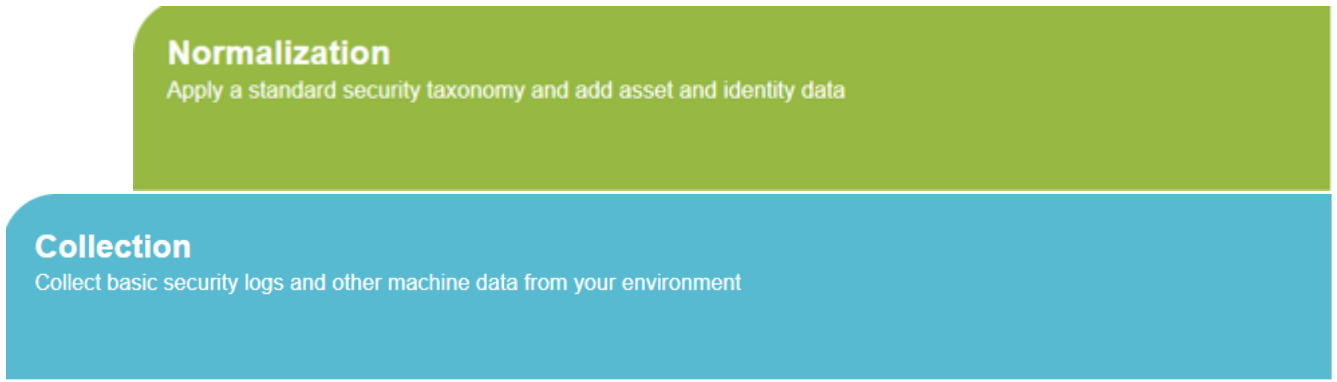
OBIETTIVI PRINCIPALI
✔ Mappatura dati al CIM per normalizzazione e ricerca ottimizzata (modelli accelerati).
✔ Correlazione eventi con asset e utenti (Active Directory, IAM/SSO, LDAP).
✔ Integrazione meccanismi di detection (vendor e community) tramite dati standardizzati.

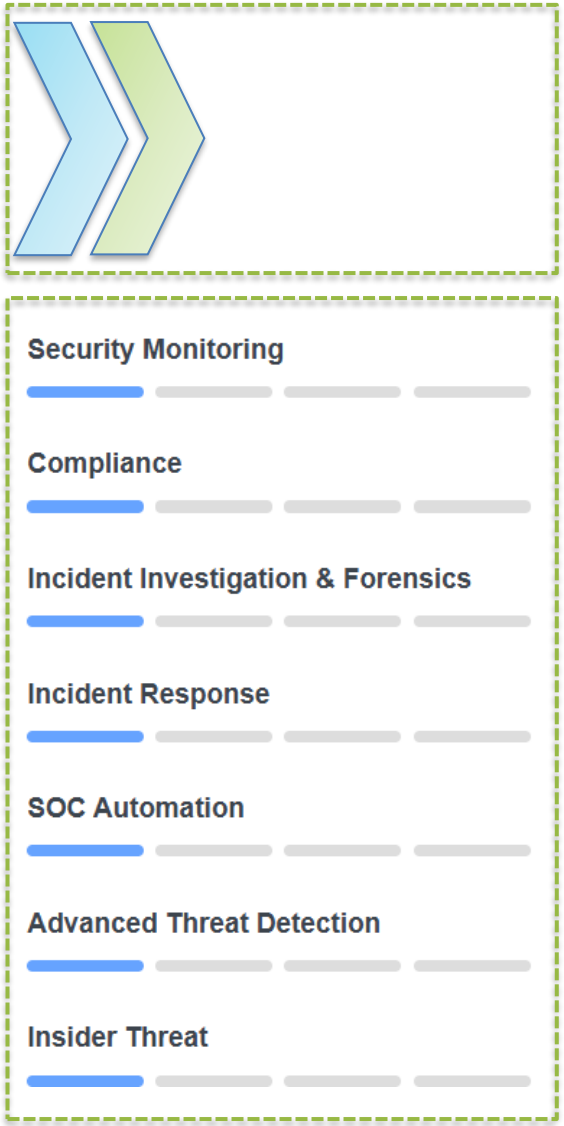
AZIONI CHIAVE
Adozione Common Information Model (CIM):
Campi standardizzati (IP sorgente, porta, utente, etc.).

Raccolta dati di contesto:
Inventario asset (reti, dispositivi, applicazioni).
Identità utenti (Active Directory, sistemi IAM).

VANTAGGI
🔍 Indagini più rapide: Dati omogenei riducono tempi di analisi.
🛡️ Scalabilità SOC: Struttura pronta per threat detection avanzata.
🌐 Interoperabilità: Integrazione agevolata di tool esterni e logiche di detection.

SFIDE & SOLUZIONI
⚠ Le detection più efficaci richiedono dati di rete e visibilità endpoint avanzata.
➔ Estendere raccolta a: packet capture (PCAP), EDR, XDR, ecc..





STAGE 3

OBIETTIVI PRINCIPALI
✔ Raccolta dati ad alta fedeltà:
» Log attività endpoint (processi, file, registri di sistema).
» Metadati di rete (flussi NetFlow, sessioni TCP/IP, DNS query).
✔ Correlazione avanzata per identificare attacchi multistadio (es. lateral movement, C2).
✔ Preparazione per analytics con modelli di machine learning (fasi successive).

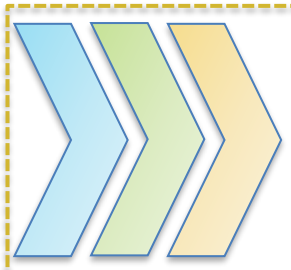
AZIONI CHIAVE

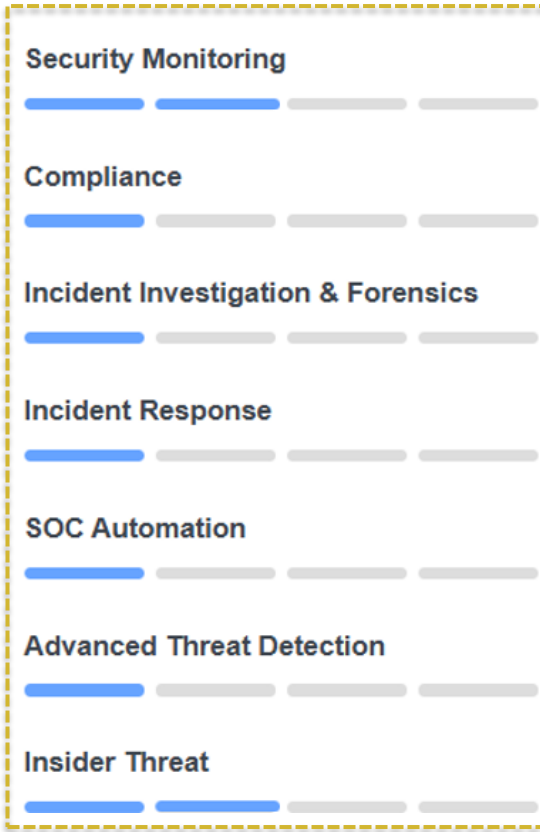
Integrazione EDR/XDR:
» Strumenti: CrowdStrike Falcon, Microsoft Defender for Endpoint.

Monitoraggio metadati di rete:
» Esempi: Zeek (Bro), Suricata, Corelight.

Normalizzazione avanzata:
» Estensione del CIM per campi specifici (es. hash file, user-agent).

VANTAGGI
🔎 **Detection granulare:** Rilevare attacchi evasivi (es. fileless malware).
🌐 **Mappatura comportamenti sospetti:** Collegare attività endpoint a pattern di rete.





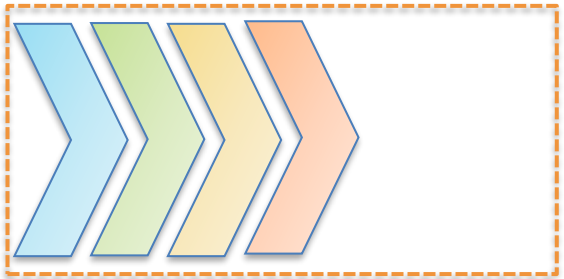
STAGE 4

AZIONI CHIAVE
✔ Priorità basata su criticità asset
✔ Arricchimento alert con threat intelligence (OSINT, feed commerciali).
✔ Pivot contestuale verso sistemi esterni per indagini approfondite.

FONTI DATI AGGIUNTIVE
🚫 **Blocklist interne:** IP/URL sospetti locali.
🌐 **OSINT:** Minacce da fonti open-source (es. AlienVault OTX).
💼 **TI Commerciale:** Feed premium.

VANTAGGI
🔎 **Detection proattiva:** Identificazione minacce prima del danno.
🎯 **Prioritizzazione degli alert:** Focalizzarsi su asset critici.
🔄 **Integrazione dinamica:** Cross-check con dati esterni.

SFIDE PRINCIPALI
📘Creazione playbook per scenari ricorrenti.
💡Repository centralizzato per "lessons learned".



Security Monitoring
Compliance
Incident Investigation & Forensics
Incident Response
SOC Automation
Advanced Threat Detection
Insider Threat

STAGE 5

OBIETTIVI PRINCIPALI
✔ Tracciamento incidenti con metriche di priorità e stato.
✔ Misurazione efficacia analisti (tempo di risposta, falsi positivi).
✔ Esecuzione playbook predefiniti per scenari critici.
✔ Orchestrazione risposte (automazione base → complessa).

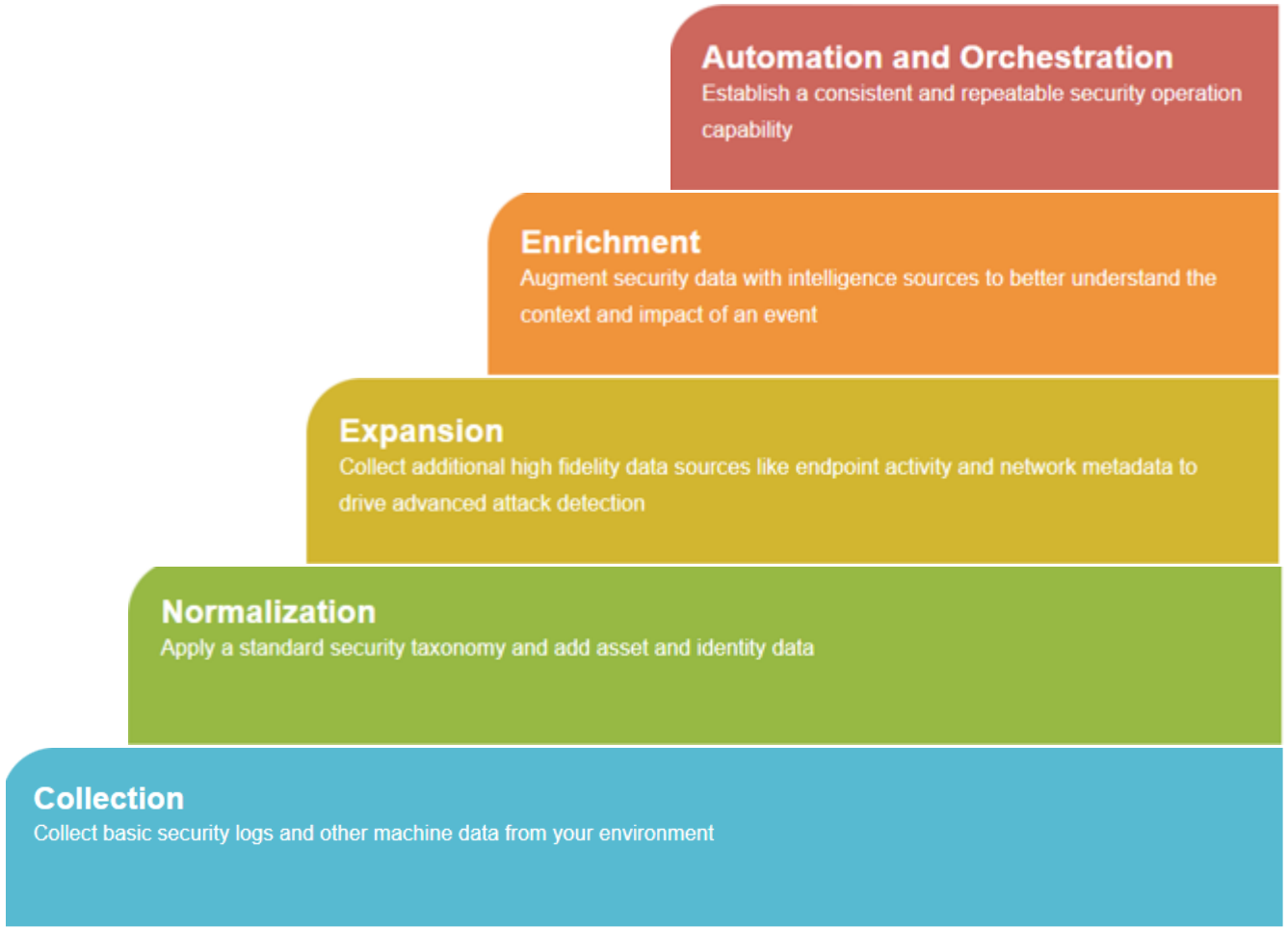
AZIONI CHIAVE

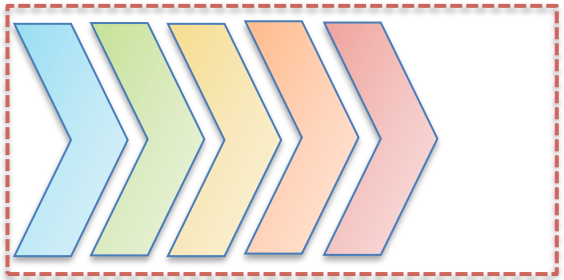
📈 **Dashboard di monitoraggio:**
» Strumenti: Jira, ServiceNow, SIEM integrato.

📊 **Metriche KPI:**
» Esempi: MTTR (Mean Time to Respond), tasso di falsi positivi.

🤖 **Automazione SOAR:**
» Integrazione con Palo Alto Cortex XSOAR.

VANTAGGI
🚀 **Risposta rapida:** Automazione di azioni ripetitive (es. blocchi IP).
🎯 **Accountability:** Chiarezza su performance del team.
🧩 **Scalabilità:** Combinazione di workflow per threat complessi.





STAGE 6

OBIETTIVI PRINCIPALI

✔ Individuazione anomalie tramite ML/AI su utenti, endpoint e applicazioni.

✔ Rilevamento minacce sconosciute (adversary/insider con tracce minime).

✔ Adozione continua di tecniche avanzate e ricerca collaborativa.

AZIONI CHIAVE

🕵 **Threat Hunting:**
» Analisi comportamentale (UEBA) e modelli statistici avanzati.

🧠 **Machine Learning:**
» Implementazione algoritmi per pattern anomali (es. Splunk ES).

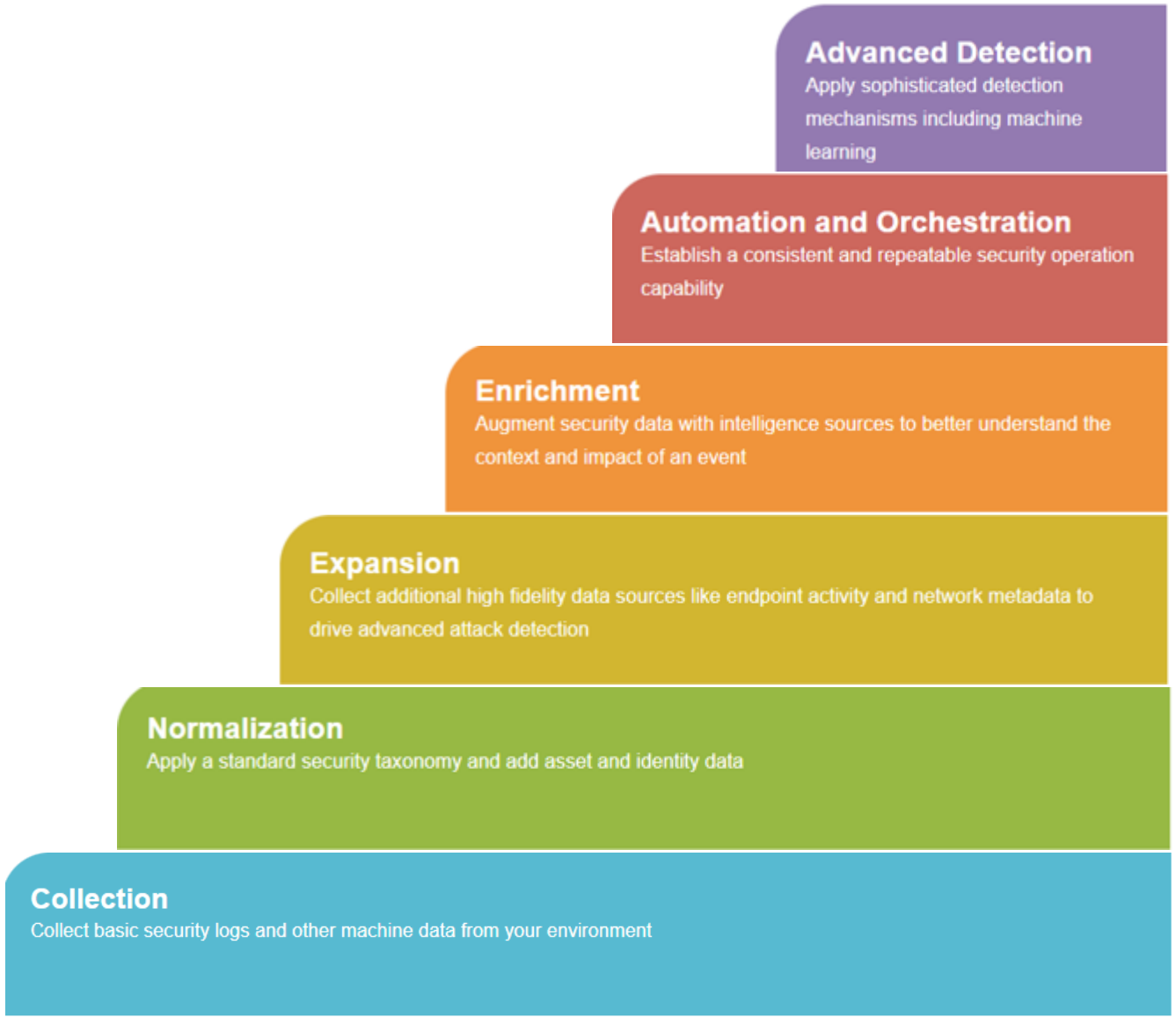
🔬 **Ricerca esterna:**
» Collaborazione con CERT, MITRE ATT&CK, community threat intel.

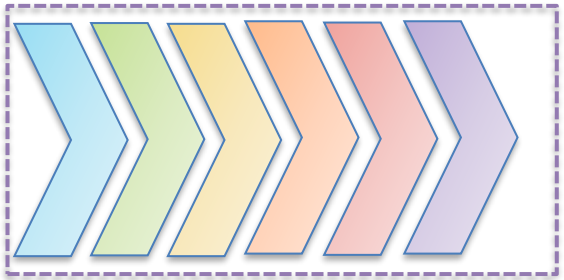
VANTAGGI

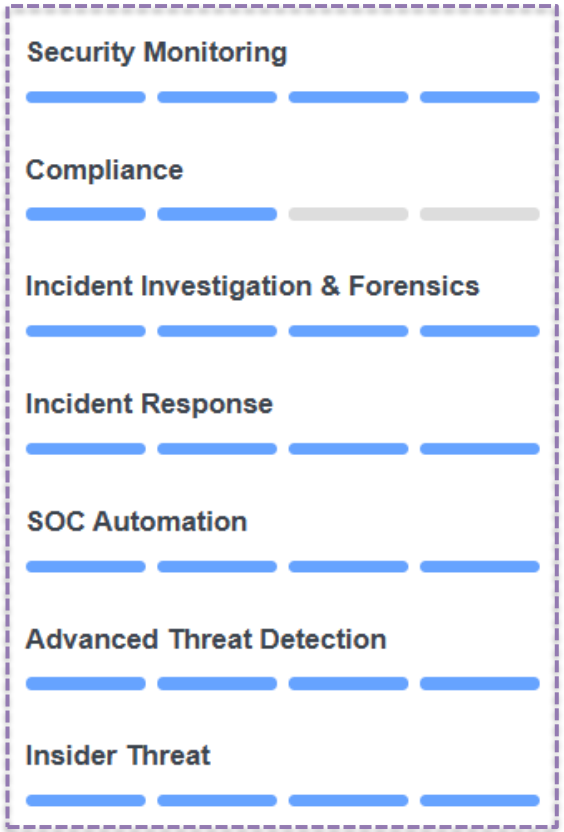
🔮 **Previsione minacce:** Identificare rischi prima della materializzazione.

🎲 **Resilienza:** Mitigare attacchi zero-day e campagne mirate.

🤝 **Synergy:** Integrare expertise interna e innovazione esterna.

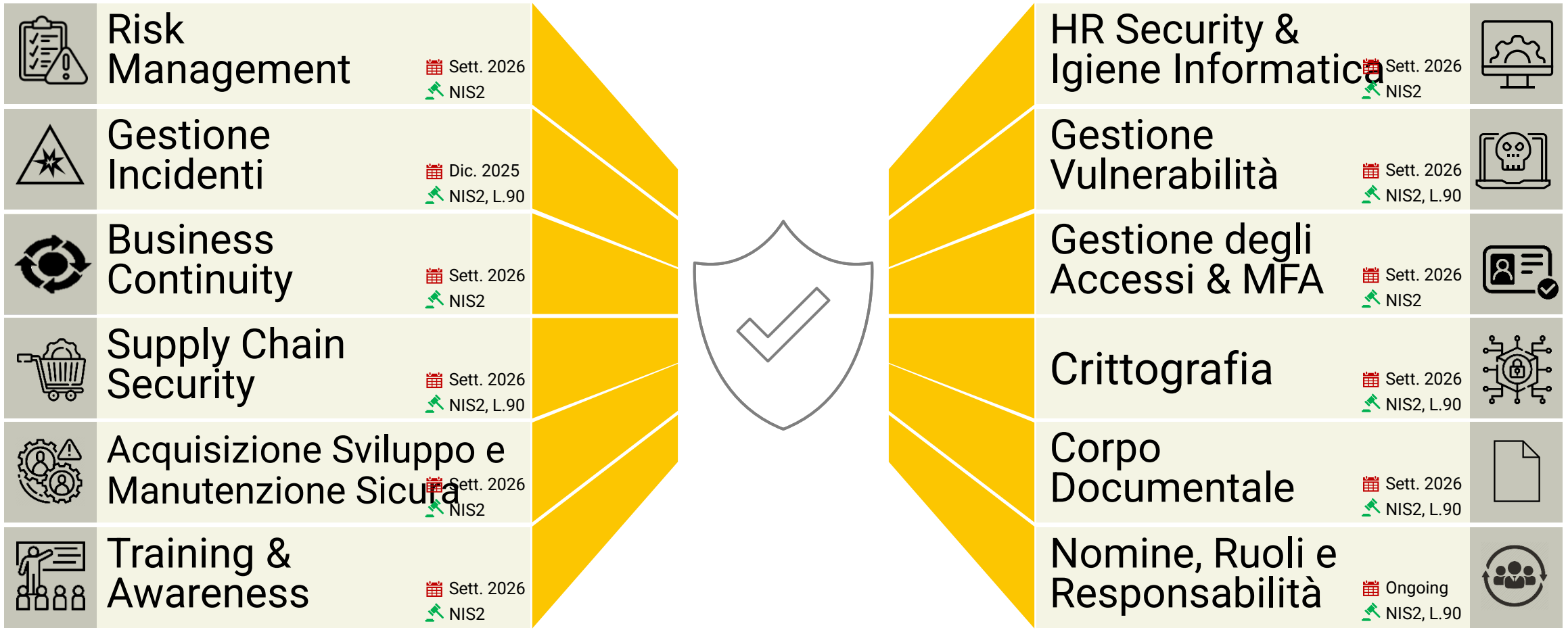






OBBLIGHI & SCADENZE NIS2 & LEGGE 90 - SUMMARY

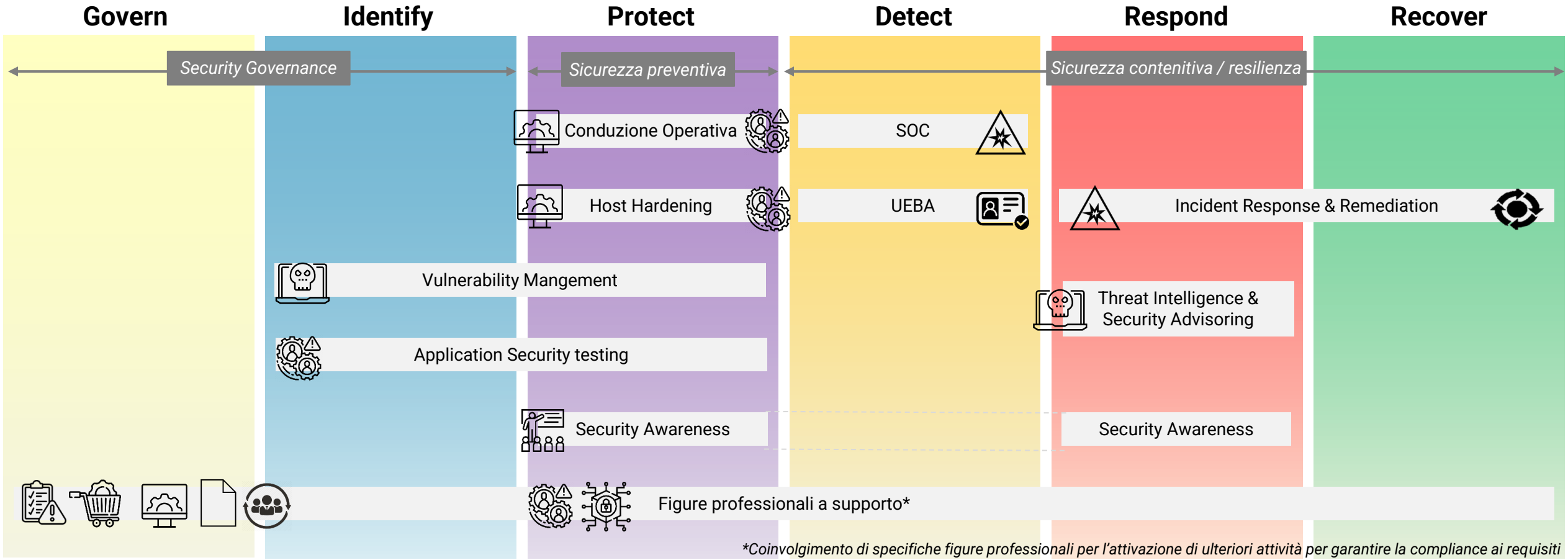
La **Direttiva NIS 2** (comprensiva di **Decreto Legislativo 138/2024**) e la Legge sulla Cybersicurezza (**Legge 28 giugno 2024, n. 90**) indirizzano per i soggetti interessati, tra cui *Regioni, Città Metropolitane, Comuni con popolazione superiore a 100.000 abitanti, Comuni capoluoghi di Regione, Aziende Sanitarie Locali, Società inhouse e Società di trasporto pubblico Urbano ed Extraurbano* una serie di obblighi* tra cui l'implementazione di misure di sicurezza di tipo tecnico e organizzativo per le quali è stato definito un calendario di implementazione.



(*) Per maggiori dettagli circa i requisiti derivanti dalla Direttiva NIS 2 e dalla Legge sulla Cybersicurezza si rimanda all'Annex I.

SERVIZI A SUPPORTO DELLA COMPLIANCE NIS2-LEGGE 90

Sia la **NIS 2** che la **Legge 90/2024** identificano le Function del **NIST CSF 2.0** come framework di riferimento per la Compliance. I *servizi di IT system management e sicurezza informatica della Convenzione Intercent-ER* possono quindi supportare le Pubbliche Amministrazione della Regione Emilia Romagna nell'indirizzamento dei relativi adempimenti sia di natura procedurale e organizzativa (*es: Security Awareness e Servizi professionali*) che tecnica (*es: SOC e Vulnerability Management*).



Legenda ambiti NIS2-L.90

- *Risk management*
- *Gestione incidenti*
- *Business Continuity*
- *Supply Chain Security*
- *Acquisizione, Sviluppo e manutenzione Sicura*
- *Training & Awareness*
- *HR Security & Igiene Informatica*
- *Gestione delle vulnerabilità*
- *Gestione degli accessi & MFA*
- *Crittografia*
- *Corpo documentale*
- *Nomine, ruoli e responsabilità*

POTENZIAMENTO DELLA RESILIENZA CYBER – USE CASE

Lo Use Case illustra una serie di **iniziative** intraprese da un Comune della Regione Emilia Romagna con il supporto dell'RTI volte a **garantire adeguati livelli di sicurezza dei sistemi IT**, dei dati trattati e in generale delle informazioni gestite dall'ente e complessivamente ***incrementare*** la propria **postura di sicurezza.**

Definizione del **corpo documentale** in ambito **Information Security** al fine di stabilire e fomalizzare i processi attuati dell'organizzazione

Erogazione di **sessioni formative** in ambito **Sicurezza Informatica** volto ad accrescere la consapevolezza di tutti i dipendenti dell'Ente.

Definizione di una **metodologia di Analisi del rischio Cyber** che tenga in considerazione, minacce, impatti, probabilità di accadimento e contromisure adottate o da adottare

Analisi **dell'architettura di sicurezza** per prevenire la perdita di dati e garantire l'accesso sicuro alla rete

Definizione dei requisiti essenziali per una corretta **gestione delle identità aziendali** e successiva implementazione di nuovi tool e tecnologie a supporto

Esecuzione di test tecnici di sicurezza dei sistemi (**VAPT**) volti ad identificare eventuali vulnerabilità e debolezze presenti sui sistemi e intervenire tempestivamente per mitigarne i rischi

Realizzazione di attività di **supporto alla compliance Privacy** e finalizzate a garantire l'adeguamento alla normativa vigente.

Esecuzione di attività in ambito **Continuità Operativa** al fine di definire i processi critici aziendali ed eseguire di una simulazione di crisi post incidente avente l'obiettivo di di ripristinare la normale operatività nel minor tempo

Legenda ambiti NIS2-L.90

Risk management | *Business Continuity* | *Acquisizione, Sviluppo e manutenzione Sicura* | *HR Security & Igiene Informatica* | *Gestione degli accessi & MFA* | *Corpo documentale*

Gestione incidenti | *Supply Chain Security* | *Training & Awareness* | *Gestione delle vulnerabilità* | *Crittografia* | *Nomine, ruoli e responsabilità*

DIGITAL PROTECTION & PREVENTION – USE CASE

Con l'obiettivo di potenziare le capacità di **prevenzione** e **protezione** di **attacchi informatici** nel contesto Regionale di riferimento, sono stati svolti con il supporto dell'RTI **interventi** mirati per:

- Supportare la definizione dei processi del CSIRT Regionale per il monitoraggio e la risposta agli incidenti di sicurezza.
- Favorire la conoscenza del personale e verificare l'adeguatezza i processi di gestione delle situazioni di crisi.
- Individuare le vulnerabilità tecniche presenti nei sistemi.

Processi del CSIRT

Supporto alla definizione del modello di erogazione dei servizi del CSIRT Regionale deputato al monitoraggio e risposta degli incidenti di sicurezza, con relativa definizione e formalizzazione dei processi organizzativi ed operativi in aderenza a quanto stabilito dalle "Linee guida per la realizzazione di CSIRT" (ACN, agosto 2023) e al Modello ENISA.

Tali processi sono divisi tra processi interni al CSIRT e processi condivisi con la Constituency di riferimento.

Cyber Crisis Management Simulation

Esecuzione di un'esercitazione Cyber Crisis Management Simulation con l'obiettivo di testare e migliorare le strategie di gestione di eventuali scenari di crisi cibernetica

Tale simulazione ha proposto uno scenario reale di incident in cui sono stati analizzati aspetti quali l'attivazione tempestiva delle remediation, l'efficacia delle comunicazioni interne e delle prassi di coordinamento, la gestione delle comunicazioni esterne e la gestione di security/data breach.

VAPT

Conduzione di attività di Vulnerability Assessment e Penetration Test (VAPT) su servizi applicativi.

Tali attività hanno l'obiettivo di ottenere una visione costante e aggiornata delle eventuali vulnerabilità e debolezze presenti sui sistemi, e intervenire tempestivamente per mitigare i rischi e ridurre il perimetro di esposizione dell'organizzazione ad attacchi esterni.

Legenda ambiti NIS2-L.90

Risk management | *Business Continuity* | *Acquisizione, Sviluppo e manutenzione Sicura* | *HR Security & Igiene Informatica* | *Gestione degli accessi & MFA* | *Corpo documentale*

Gestione incidenti | *Supply Chain Security* | *Training & Awareness* | *Gestione delle vulnerabilità* | *Crittografia* | *Nomine, ruoli e responsabilità*

CTI E MATURITY ASSESSMENT – USE CASE

Nell'ambito dei **servizi di cybersecurity** erogati dal CSIRT ai membri della propria constituency sono state condotte **attività** di cyber threat intelligence e di valutazione del livello di maturità in ambito cybersecurity con l'indirizzamento di un piano di azioni correttive.

Cyber Threat Intelligence

Conduzione di attività di cyber threat intelligence con l'obiettivo di massimizzare la prevenzione verso attacchi o incidenti informatici.
La due macro-tematiche chiave su cui l'attività è basata sono il monitoraggio continuo delle informazioni pubblicamente disponibili (Clear, Deep e Dark Web) delle Entità e sfruttabili da un threat actor nella conduzione di un attacco, e la condivisione continua di indicatori di intelligence relativi a minacce in corso in Italia (feed di threat intelligence e reportistica di dettaglio).

Cyber Maturity Assessment

Conduzione di assessment con l'obiettivo di comprendere la postura di maturità in termini di cybersecurity di ciascun Ente e definire le opportune azioni di rimedio.
L'assessment è basato sul Framework Nazionale di Cybersecurity e Data Protection, dividendo i controlli presenti al suo interno tra minimi, standard e avanzati, da somministrare a seconda della complessità dell'entità interessata.
Il report di output contenenti i risultati dell'analisi con indicazione del livello di maturità AS-IS e una serie di azioni di rimedio consigliate.

Legenda ambiti NIS2-L.90

Risk management | *Business Continuity* | *Acquisizione, Sviluppo e manutenzione Sicura* | *HR Security & Igiene Informatica* | *Gestione degli accessi & MFA* | *Corpo documentale*

Gestione incidenti | *Supply Chain Security* | *Training & Awareness* | *Gestione delle vulnerabilità* | *Crittografia* | *Nomine, ruoli e responsabilità*

Annex I - Dettaglio Requisiti NIS2 e Legge 90/2024

REQUISITI DIRETTIVA NIS2 – SUMMARY (1/2)

La Direttiva NIS 2, anche alla luce dell'interpretazione accordata allo Schema di Decreto Legislativo di recepimento, arricchisce e amplia la portata rispetto alla precedente Direttiva NIS 1, introducendo una serie di obblighi* in capo ai destinatari.

Politiche di analisi dei rischi e di sicurezza

I soggetti in-scope devono individuare i rischi specifici per il settore operativo di riferimento e valutarne i relativi impatti.

Misure di gestione degli incidenti

I soggetti in-scope devono effettuare una revisione del processo aziendale di gestione degli incidenti di sicurezza e devono integrare la procedura aziendale di comunicazione degli incidenti verso l'autorità avendo cura di assicurare le tempistiche richieste dalla normativa

Continuità operativa

I soggetti in-scope devono rivedere, o laddove non presenti, implementare, i processi aziendali inerenti a:

- Crisis Management;
- Disaster Recovery;
- Backup;
- …

Sicurezza della Supply Chain

I soggetti in-scope devono rivedere il processo di approvvigionamento aziendale al fine di integrare gli obblighi relativi all'acquisto di Prodotti certificate e dei rischi relativi al Procurement ICT (ex-artt.22-24).

Acquisizione, sviluppo e manutenzione

I soggetti in-scope devono effettuare un'analisi del processo aziendale relativo alla sicurezza dell'acquisizione, sviluppo e manutenzione dei sistemi informatici e di rete.

(*) Il mancato rispetto degli obblighi comporterà sanzioni pecuniarie fino ad un massimo di 7 milioni di euro e fino ad un massimo dell'1,4% del fatturato annuo mondiale (se superiore).

REQUISITI DIRETTIVA NIS2 – SUMMARY (2/2)

La Direttiva NIS 2, anche alla luce dell'interpretazione accordata allo Schema di Decreto Legislativo di recepimento, arricchisce e amplia la portata rispetto alla precedente Direttiva NIS 1, introducendo una serie di obblighi* in capo ai destinatari.

Valutazione efficacia misure di gestione dei rischi

I soggetti in-scope devono effettuare la revisione delle strategie e delle procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza.

Formazione e consapevolezza

I soggetti in-scope devono assicurare l'awareness aziendale relativamente alle tematiche di cybersecurity attraverso l'organizzazione di corsi di formazione;

I soggetti in-scope devono assicurare l'implementazione di pratiche di igiene informatica di base al proprio interno.

Crittografia e cifratura

I soggetti in-scope devono provvedere alla revisione, o se non presenti, alla formalizzazione, delle politiche e procedure aziendali relative all'uso della crittografia e, se del caso, della cifratura.

Sicurezza delle risorse umane, degli accessi logici e degli asset

I soggetti in-scope devono revisionare, o se non già presente, formalizzare, la politica relativa alla sicurezza delle risorse umane;

I soggetti in-scope devono revisionare le misure e le politiche di sicurezza aziendali relative alla gestione del controllo degli accessi nonché alla revisione delle utenze attive.

Autenticazione e comunicazione protetta

I soggetti in-scope devono revisionare e aggiornare, o laddove non presenti, implementare, soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti, se del caso.

(*) Il mancato rispetto degli obblighi comporterà sanzioni pecuniarie fino ad un massimo di 7 milioni di euro e fino ad un massimo dell'1,4% del fatturato annuo mondiale (se superiore).

REQUISITI LEGGE 90/2024 - SUMMARY

Legge sulla Cybersicurezza n.90/2024 introduce una serie di obblighi in capo ai destinatari.

Gestione delle vulnerabilità

I soggetti in-scope sono tenuti ad implementare interventi risolutivi delle vulnerabilità individuate e comunicate da ACN entro tempistiche prestabilite.

Approvvigionamento ICT

I soggetti in-scope devono tenere in considerazione una serie di specifici elementi di cybersicurezza in caso di approvvigionamento ICT.

Gestione e notifiche incidenti

I soggetti in-scope devono segnalare gli incidenti di sicurezza entro 24h dall'avvenuta conoscenza ed effettuare la notifica completa entro 72h.

Struttura e referente cybersecurity

I soggetti in-scope devono individuare una struttura incaricata di assicurare la sicurezza delle informazioni;

I soggetti in-scope hanno l'obbligo di procedere alla nomina di un referente per la Cybersecurity, responsabile della gestione e del governo delle tematiche relative alla sicurezza informatica.

Robustezza delle soluzioni crittografiche

I soggetti in-scope hanno l'obbligo di verificare se le soluzioni crittografiche in uso rispettano le imposizioni previste dal Garante e dall'ACN.

(*) Il mancato rispetto degli obblighi comporterà sanzioni pecuniarie da un minimo di 25.000 euro a un massimo di 125.000 euro. Tale violazione, inoltre, può anche costituire causa di responsabilità disciplinare e amministrativo-contabile nei confronti dei funzionari e dei dirigenti responsabili.

CONTATTI

Contatti RTI

Contatto per adesione alla convenzione

enterprice.intercenter@fastweb.it

Help desk
la.gare@pec.fastweb.it
Numero dedicato: 800 177 777

Responsabile del servizio
348 9010249
Moris MARIANI moris.mariani@fastweb.it

Referente per l'esecuzione
375 5205809
Leonardo LIVIERA ZUGIANI leonardo.livierazugiani@fastweb.it

INTERCENTER – REGIONE EMILIA ROMAGNA

Area Innovazione Tecnologica e Trasformazione Digitale. Spesa ICT e Farmaceutica
servizioictintercenter@regione.emilia-romagna.it

RUP Gianluca IMPERATO
051 5273430
gianluca.imperato@regione.emilia-romagna.it

Manuela GIOVAGNONI
051 5273542
manuela.giovagnoni@regione.emilia-romagna.it

Clara IALLONARDO
051 5278374
clara.iallonardo@regione.emilia-romagna.it

Grazie per l’attenzione!