Clusit
Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

SECURITY SUMMIT

Security Summit

Milano 19-20-21 marzo 2024

Clusit 2024 – Regione Lombardia

Agenda

- **Il Piano per la Sicurezza dei dati e dei servizi di Regione Lombardia**
- **Il Sistema Federato di Regione Lombardia**
- **Task Force di Cybersecurity per gli Enti Sanitari**
- **CSIRT di Regione Lombardia**

Il Piano per la Sicurezza dei dati e dei servizi di Regione Lombardia

Nuovo Programma per la sicurezza dei dati e dei servizi (1/2)

Con DELIBERAZIONE N° XII / 1542, Seduta del 18/12/2023, La Giunta Regionale della Regione Lombardia ha **approvato il Programma della XII legislatura per la sicurezza dei dati e dei servizi.**

Tale Programma è stato costruito

- mantenendo **elementi chiave di continuità** rispetto al precedente Programma Triennale Integrato di Sicurezza e Privacy del Sistema Federato di Regione Lombardia 2020-2022, adeguati, rivisti e aggiornati
- **introducendo nuove iniziative** in virtù dei mutati scenari di rischio e dell'evolversi del contesto organizzativo, tecnologico e geopolitico

Le ragioni per le quali il nuovo Programma poggia i suoi pilastri sul precedente derivano dai risultati da esso raggiunti che hanno infatti consentito a Regione Lombardia, Aria e gli altri Enti del sistema Federato, non solo il **raggiungimento degli obiettivi prefissati**, ma anche di rispondere alle esigenze, alle minacce e alle opportunità che si sono manifestate nel corso del periodo, confermando l'efficacia del programma e delle progettualità intraprese.

Il Piano per la Sicurezza dei dati e dei servizi di Regione Lombardia

Nuovo Programma per la sicurezza dei dati e dei servizi (2/2)

OBIETTIVI DEL PROGRAMMA

Definire la strategia e le priorità di intervento in tema di sicurezza delle informazioni, dei dati e infrastrutture e di conformità alle normative e standard.

La realizzazione del programma è coerente con il modello di attuazione per il Governo della Sicurezza delle Informazioni e Privacy che Regione Lombardia ha definito al fine di valorizzare e sfruttare tutte le possibili sinergie all'interno del Sistema Federato.

CAMPO DI APPLICAZIONE DEGLI INTERVENTI

Gli Interventi che compongono il Programma sono rivolti ai seguenti perimetri:

- Welfare Territorio;
- Welfare Regionale;
- Enti Regionali;
- Sistemi Informativi Regione;
- ARIA.

DURATA

Il piano degli interventi ha durata quinquennale, pari alla durata della legislatura.

Il Piano per la Sicurezza dei dati e dei servizi di Regione Lombardia
Obiettivi e domini di intervento (1/2)

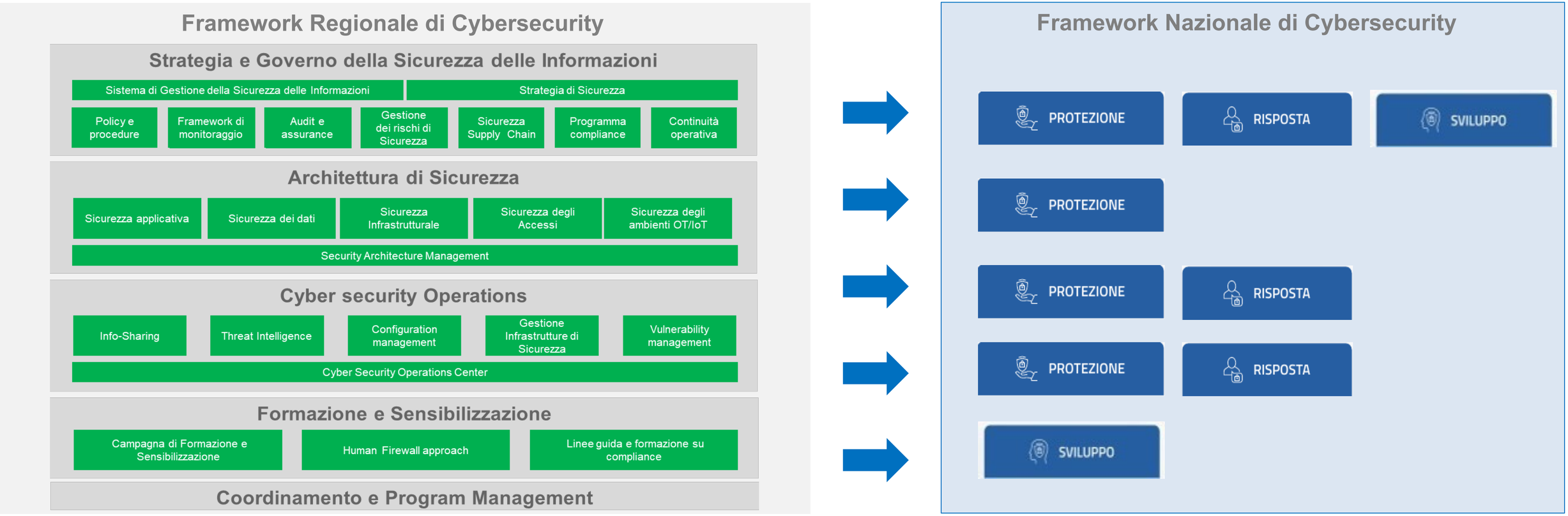
Rispetto alla precedente versione, il Framework è stato rivisto ed integrato di alcuni nuovi domini, coerenti con l'evoluzione dello scenario normativo e tecnologico.

- **Sicurezza della Supply Chain** al fine di garantire da parte dei fornitori ICT il rispetto di misure di sicurezza adeguate ai requisiti di sicurezza dei beni e/o servizi acquisiti, per evitare che eventuali vulnerabilità che insistono sui fornitori possano compromettere la sicurezza degli Enti del Sistema Federato Regionale.
- **Sicurezza degli accessi** con l'obiettivo di sviluppare una serie di iniziative al fine di proteggere l'accesso a dati ed applicazioni attraverso un controllo degli accessi incentrato sull'identità piuttosto che sugli account, in modo da mappare con precisione chi fa cosa e a quali risorse ha accesso e rafforzare la sicurezza dell'autenticazione.
- **Sicurezza degli ambienti OT/IoT** al fine di Garantire la protezione dei dispositivi OT/IoT medicali utilizzati dagli Enti Welfare Territoriale in termini di disponibilità del dispositivo e di riservatezza e integrità dei dati trattati

Il Piano per la Sicurezza dei dati e dei servizi di Regione Lombardia

Obiettivi e domini di intervento (2/2)

Per ciascuna delle iniziative è stato infine identificato il riferimento agli **obiettivi definiti della Strategia Nazionale di Cybersicurezza 2022-2026,** al fine di confermare e validare l'adeguatezza del programma di Regione Lombardia rispetto alla visione definita a Livello Nazionale e avere un ulteriore strumento per il monitoraggio degli obiettivi raggiunti.



Agenda

- Il Piano per la Sicurezza dei dati e dei servizi di Regione Lombardia
- Il Sistema Federato di Regione Lombardia
- Task Force di Cybersecurity per gli Enti Sanitari
- CSIRT di Regione Lombardia

Sistema Federato di Regione Lombardia

Introduzione

Regione Lombardia ha deciso di adottare un Sistema Federato quale **modello di governo** volto al raggiungimento di comuni obiettivi di prevenzione incidenti e protezione asset aziendali, assicurando la conformità normativa per tutti gli Enti che ne fanno parte.

Lo scopo è quello di promuovere un'azione comune sulle tematiche di Sicurezza Informatica e Privacy, con una ***visione unica,*** a livello sia centrale sia territoriale, e sviluppare le ***sinergie*** tra i diversi ambiti di intervento per garantire:

- una chiara ed efficiente attribuzione delle responsabilità, sia nella gestione che nell'operatività,
- l'ottimizzazione delle risorse di disposizione,

generando *valore aggiunto* sia in termini di contenuti che di efficacia degli interventi.

Sistema Federato di Regione Lombardia
Descrizione del modello

Il modello prevede 2 comitati:

- **Comitato strategico unico in ambito Sicurezza e Privacy**;
- **Comitati operativi distinti in ambito Sicurezza e in ambito Privacy**.

Comitato strategico

Frequenza: 2 sessioni annuali e a chiamata ove richiesto.

Attività: definisce la strategia in ambito Sicurezza e Privacy a livello Federato, esamina in via preventiva (e rivaluta periodicamente) il Programma pluriennale e gli investimenti rilevanti a livello Federato di cui valuta la congruità strategica, approva il Piano interventi annuale e ne ratifica il raggiungimento degli obiettivi a consuntivo sulla base degli indicatori definiti.

Componenti: il Segretario Generale di Regione Lombardia e i suoi vice, il Direttore Generale del Welfare di Regione Lombardia, il Responsabile dei Rapporti con gli Enti del SIREG, il DPO di Regione Lombardia, il Direttore Generale di ARIA.

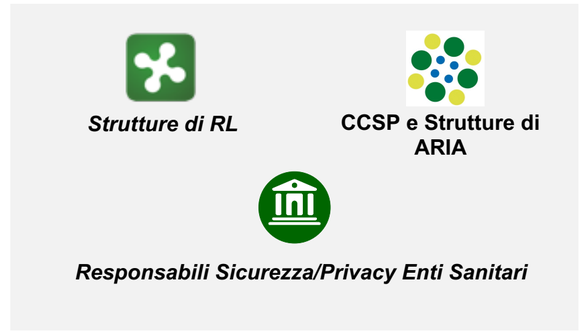
Organi a supporto: Strutture di Regione Lombardia competenti in materia di sistemi informativi e cybersicurezza, Strutture privacy di Regione Lombardia, Competence Center Security e Privacy ARIA (CCSP).

Comitato operativo

Frequenza: trimestrale.

Attività: monitora i progetti definiti all'interno del Piano annuale approvato, verifica il raggiungimento degli obiettivi operativi e garantisce il popolamento degli indicatori strategici.

Componenti: Unità Organizzative STDSI e SIGBS, Direzioni RL coinvolte, Privacy RL (Privacy Officer, DPO, Privacy WT), Competence Center Security e Privacy Aria , Strutture Aria coinvolte, Responsabili Sicurezza degli Enti e Consiglio, Referenti Privacy/DPO degli Enti, Eventuali terze parti/fornitori coinvolti



Agenda

- Il Piano per la Sicurezza dei dati e dei servizi di Regione Lombardia
- Il Sistema Federato di Regione Lombardia
- Task Force di Cybersecurity per gli Enti Sanitari
- CSIRT di Regione Lombardia

Task Force di Cybersecurity per gli Enti Sanitari

Timeline

Attacchi informatici Enti sanitari

- 27/12/2021 ASST-LECCO
- 01/05/2022 ASST-FBF-SACCO
- 05/05/2022 ATS-INSUBRIA

Dicembre 2021 – Maggio 2022

Maggio 2022

Costituzione TaskForceCyberES

Su richiesta della DG Welfare di RL, il ARIA istituisce e coordina una Task Force Cyber per gli Enti Sanitari.

Assessment CyberSecurity

Esecuzione di un assesment su ogni Ente sulla base del Framework Nazionale sulla CyberSecurity per la valutazione del livello di maturità as-is.

Maggio 2022

Giugno 2022

Piano Tattico 2022

Definizione ed avvio del Piano Tattico 2022

Nuovo assessment CyberSecurity

Esecuzione nuovo assessment di maturità degli Enti

Gennaio 2023

28 Febbraio 2023

Termine attività Piano Tattico

Termine di esecuzione delle attività del Piano Tattico 2022

Piano tattico 2023

Definizione previste delle attività del Piano Tattico 2023

Aprile - maggio 2023

Maggio - dicembre 2023

Piano Tattico 2023

Esecuzione delle attività previste dal piano tattico 2023

Piano tattico 2024

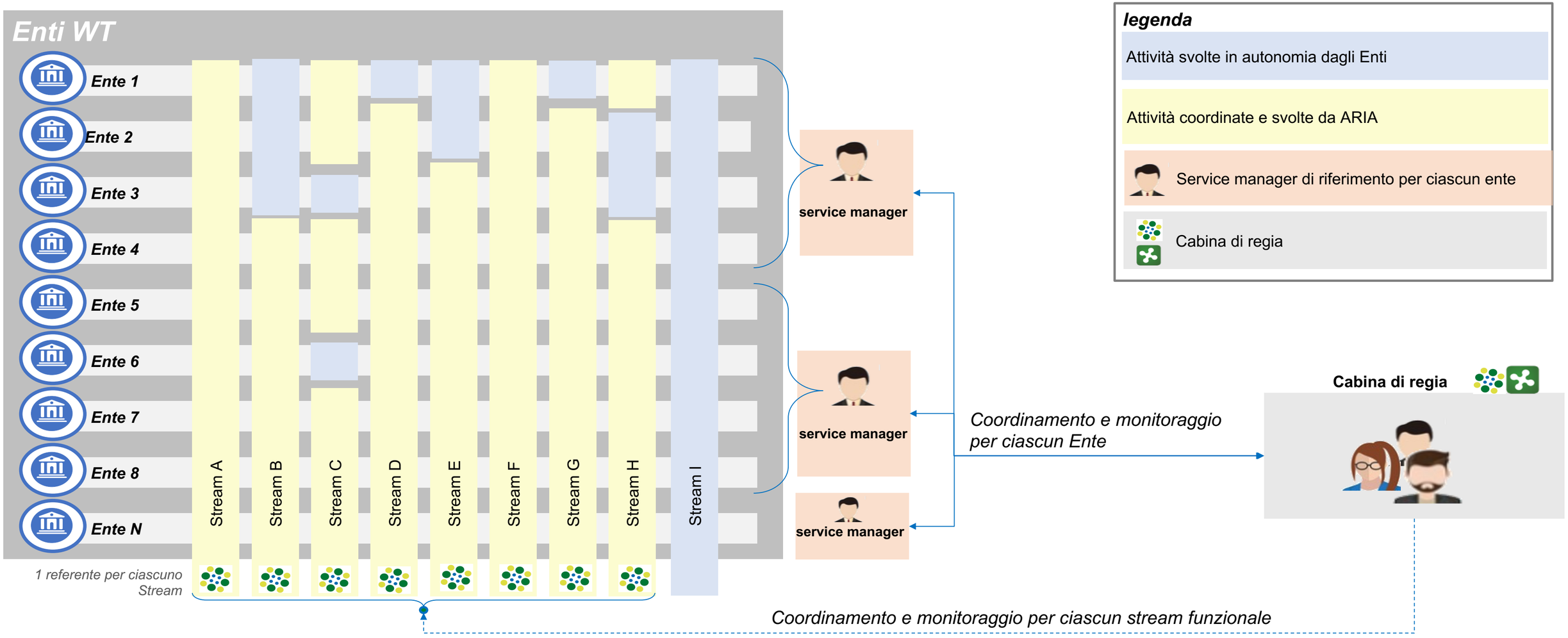
Continua erogazione ed estensione dei servizi attivati dal piano tattico 2023

2024

In aggiunta agli step rappresentati nella timeline, nel corso del 2023 è stata condivisa la metodologia di valutazione del livello di maturità cyber utilizzato da Regione Lombardia e ARIA anche agli **Enti Sanitari Privati Accreditati** con l'obiettivo di valutare in modo uniforme la cyber posture di tutto il Sistema Regionale, oltre che condividere con tali Enti la competenza maturata da Regione Lombardia e indirizzare anche per essi un piano di miglioramento.

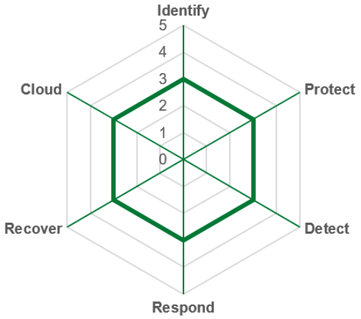
Task Force di Cybersecurity per gli Enti Sanitari

Modello operativo



Task Force di Cybersecurity per gli Enti Sanitari

Metodologia di analisi



Per la valutazione del livello di maturità rispetto alle tematiche di cybersecurity, Regione Lombardia utilizza una **metodologia condivisa** tra tutte le entità appartenenti al Sistema Federato.

Descrizione della metodologia

- L'analisi del livello di maturità viene svolta mediante la compilazione di una checklist composta da **236 controlli**, referenziati agli standard NIST Cyber Security Framework e CSA con riferimento alla sezione Cloud («**framework di riferimento**»)
- I controlli sono divisi in 22 aree e per ciascuno di essi è assegnata una tipologia a seconda che il quesito è:
  - M: direttamente utilizzato per valutare il livello di maturità
  - C: utilizzato per comprendere il contesto dell'Ente, informazione utili nella fase di definizione del piano di azioni tattiche
- **I livelli di maturità** per ciascuna category relativa al «framework di riferimento» sono strutturati su un modello CMMI a 6 livelli da «Non Adeguato» (Livello 0) fino a «Stabile e Flessibile» (Livello 5)
- È stato individuato il **Livello 3 «Approccio Proattivo» quale livello target** a cui tendere

Scala valutazione Maturità

4,1 - 5	**Stabile e Flessibile.** Le attività volte alla copertura del controllo e dei rischi inerenti rispettano gli standard del livello precedente, integrando l'uso di strumenti dedicati alla misurazione dei risultati ai fini del miglioramento continuo e dell'aggiornamento dei processi
3,1 - 4,0	**Approccio Misurato e Controllato.** Le attività volte alla copertura del controllo e dei rischi inerenti prevedono la presenza di standard di sicurezza aggiuntivi rispetto ai requisiti minimi identificati
2,1 - 3,0	**Approccio Proattivo e Soddisfacimento dei requisiti minimi.** Le attività volte alla copertura del controllo e dei rischi inerenti avvengono secondo un processo standardizzato che prevede il soddisfacimento dei requisiti minimi di sicurezza identificati
1,1 - 2,0	**Approccio Destrutturato.** Le attività volte alla copertura del controllo e dei rischi inerenti avvengono secondo un processo ripetibile ma non sono presenti processi formali diffusi su tutto il perimetro in oggetto
0,6 - 1,0	**Approccio Reattivo.** Le attività volte alla copertura del controllo e dei rischi inerenti sono implementati occasionalmente, in base alla necessità o all'iniziativa dei singoli
0 - 0,5	**Non Adeguato.** Non sono rilevati un numero sufficiente di elementi atti alla copertura dei requisiti oggetto del controllo

Task Force di Cybersecurity per gli Enti Sanitari
Piano tattico 2022 e 2023

Sono di seguito riportate le attività verticali erogate dalla Task Force ARIA nel corso del 2022 e del 2023 sui diversi Enti Sanitari.

Azioni svolte col piano tattico 2022

Ambito di interesse dell'azione svolta
Formazione per il personale tecnico
Servizio di monitoraggio *EDR – Endpoint Detection and Response*
Servizio di cyber Threat Intelligence
Identificazione e gestione degli asset critici
Segmentazione della rete informatica
Gestione degli accessi amministrativi
Sistemi di autenticazione forte (multifattore)
Logging delle operazioni svolte sugli asset critici
Assessment per implementazione servizi CSIRT
Processo di gestione degli incidenti di sicurezza
Conservazione delle copie di sicurezza

Azioni proposte come prioritarie e rivolte a tutti gli Enti
Azioni erogate singolarmente sugli Enti che ne hanno fatto richiesta

Azioni svolte col piano tattico 2023

ATTIVITA' SVOLTE IN BASE ALLE PRIORITA' DEGLI ENTI

CSIRT e Log Collector

Attivazione di un servizio volto al **monitoraggio e alla gestione degli allarmi di sicurezza** provenienti dai sistemi dell'Ente (servizio CSIRT di ARIA) e implementazione degli strumenti tecnologici necessari al tracciamento e raccolta degli eventi informatici (es. Log Collector).

PAM

Disegno e progettazione di una soluzione tecnologica deputata alla gestione delle utenze amministrative.

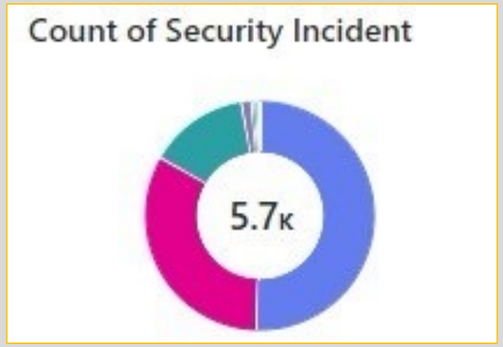
ATTIVITA' TRASVERSALI E CONTINUATIVE

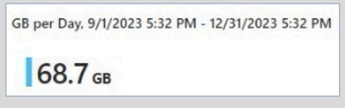
- Prosecuzione dei servizi **Cyber Threat Intelligence** e della **soluzione *Endpoint Detection and Response* per la rilevazione di eventi di sicurezza sui sistemi** avviati nel 2022
- Erogazione di **Vulnerability Assessment & Penetration Test**
- Erogazione di **simulazioni di incidenti di sicurezza**
- Predisposizione di un **corso e-learning di cybersecurity awareness** per l'erogazione a tutto il personale di ciascun Ente (in autonomia sulla propria piattaforma o tramite la piattaforma FAD di ARIA)

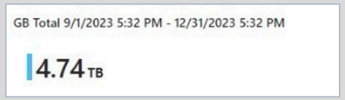
Task Force di Cybersecurity per gli Enti Sanitari

Risultati raggiunti – Alcuni numeri

Monitoraggio e gestione degli eventi di sicurezza







Numero di segnalazioni CTI inviate dall'avvio dell'attività:

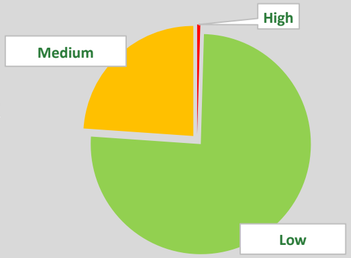
144

+ 76.000

Sistemi monitorati tramite EDR

+ 2.300

Allarmi EDR gestiti



Attività di Vulnerability Assessment e Penetration Test

39 Enti coinvolti dalle attività di VAPT

App esposte su internet

15

App con VPN

25

App in ambiente di test

22

App in ambiente di produzione

25

Formazione e awareness

577

Membri del personale tecnico partecipanti al corso di formazione nel 2022

49k

Persone che hanno completato il corso di cyber awareness in modalità **e-learning**

Clusit
Associazione Italiana per la Sicurezza Informatica

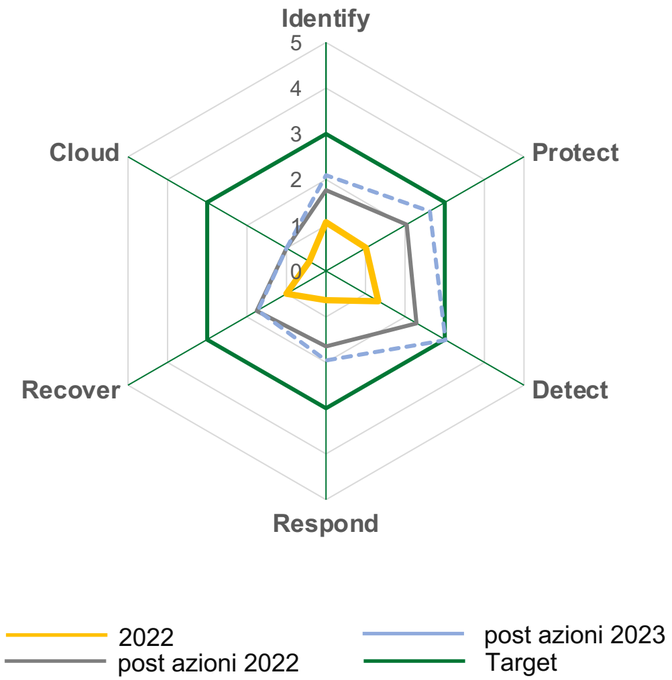
SECURITY SUMMIT

Task Force di Cybersecurity per gli Enti Sanitari

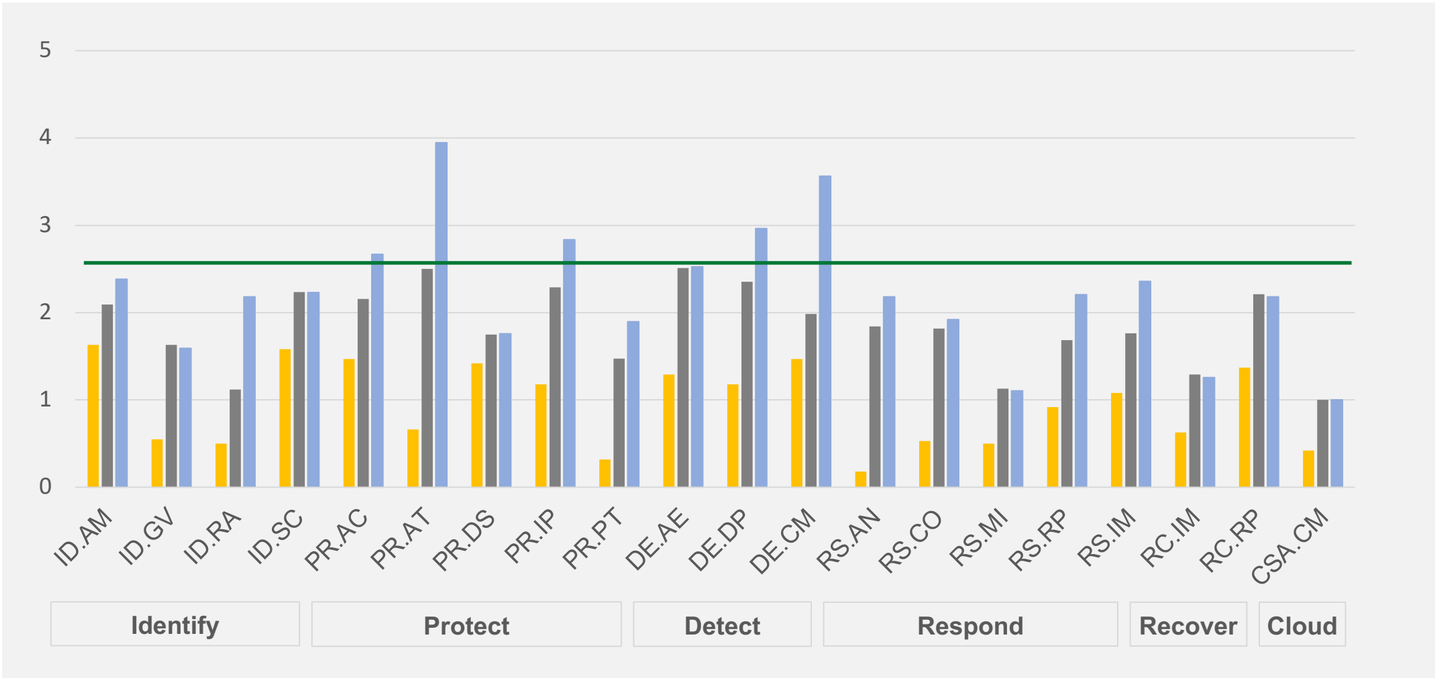
Risultati raggiunti – Livello di maturità raggiunto

Viene di seguito riportata una rappresentazione rispetto alle function e category del Framework Nazionale sulla CyberSecurity del livello di maturità raggiunto sui diversi anni a fronte delle azioni messe in campo dalla Task Force di Cybersecurity.

Maturità *function* NIST e CSA



Maturità *category* NIST e CSA



Task Force di Cybersecurity per gli Enti Sanitari
Attività previste per il 2024

- Prosecuzione dei servizi **Cyber Threat Intelligence** e della **soluzione *Endpoint Detection and Response*** per la rilevazione di eventi di sicurezza sui sistemi
- Erogazione di **Vulnerability Assessment & Penetration Test**
- Erogazione di **simulazioni di incidenti di sicurezza**
- Erogazione del **servizio CSIRT** agli Enti Sanitari già attivi
- Continuazione delle attività di implementazione dello strumento **PAM** sugli Enti Sanitari coinvolti

Agenda

- Il Piano per la Sicurezza dei dati e dei servizi di Regione Lombardia
- Il Sistema Federato di Regione Lombardia
- Task Force di Cybersecurity per gli Enti Sanitari
- CSIRT di Regione Lombardia

IL CSIRT di Regione Lombardia

Overview

Regione Lombardia si è dotata fin dal 2017 di un proprio CSIRT, gestito da ARIA S.p.A. che costituisce il riferimento per la prevenzione, raccolta dati, analisi e gestione degli eventi e incidenti di sicurezza informatica.

COMPITI DEL CSIRT

- ✓Definisce e progetta soluzioni infrastrutturali atte alla rilevazione di eventi di sicurezza
- ✓Configura e provvede all'aggiornamento delle soluzioni di monitoraggio preposte alle rilevazioni degli eventi e delle vulnerabilità
- ✓Esegue analisi infrastrutturali atte ad identificare vulnerabilità
- ✓Segnala le vulnerabilità di sicurezza rilevate all'interno del perimetro monitorato
- ✓Analizza gli eventi di sicurezza rilevati all'interno del perimetro monitorato
- ✓Segnala gli incidenti di sicurezza rilevati all'interno del perimetro monitorato
- ✓Supporta le Strutture durante il processo di gestione degli incidenti di sicurezza
- ✓Svolge investigazioni e analisi approfondite degli incidenti di sicurezza

EVOLUZIONE DEL CSIRT

Il CSIRT di Regione Lombardia **evolverà sulla base delle LINEE GUIDA PER LA REALIZZAZIONE DI CSIRT definite da ACN** e verrà incardinato nella struttura organizzativa di Regione che ne manterrà la governance.

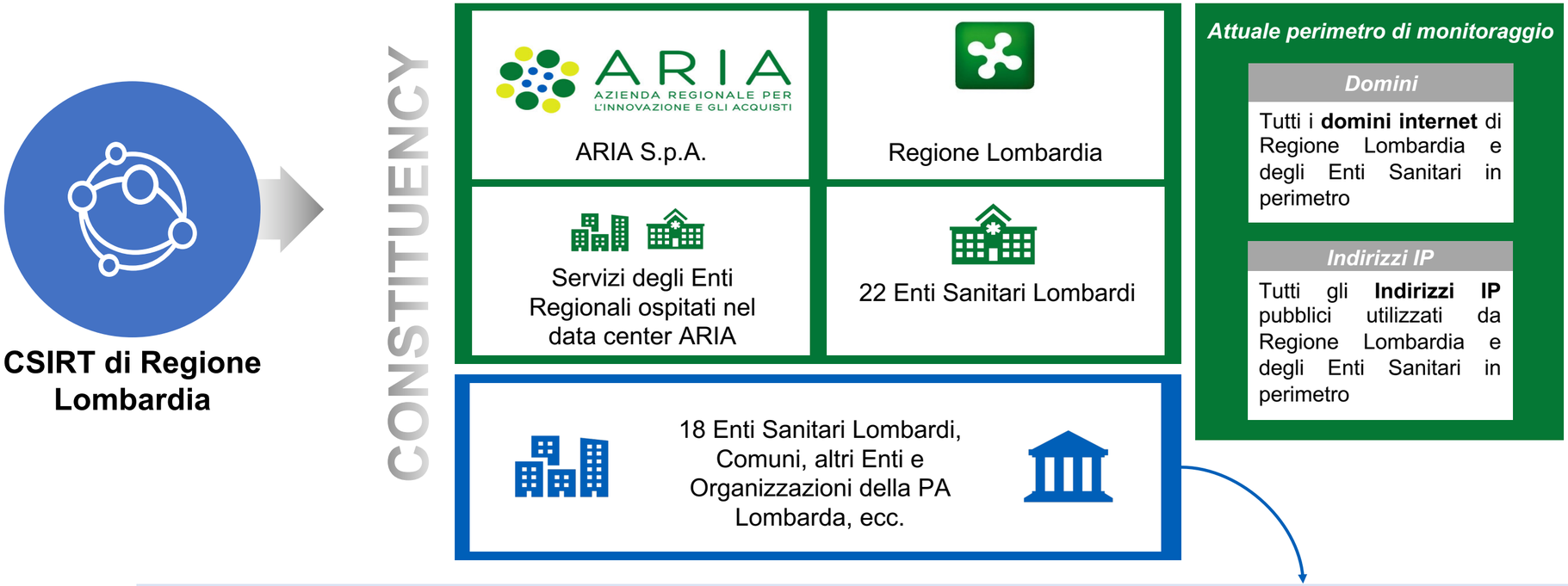
In visione prospettica, il CSIRT potrà offrire i propri servizi ad altre amministrazioni dell'Ecosistema Regionale.

Il CSIRT di Regione Lombardia è accreditato a Trusted Introducer

IL CSIRT di Regione Lombardia

Costituency

L'attuale **Constituency**, quale gruppo specifico di soggetti fisici e giuridici che beneficiano dei servizi di sicurezza erogati dal CSOC, comprende tutto il **personale della Regione Lombardia**, le **organizzazioni governative locali, le istituzioni che utilizzano i servizi forniti da ARIA S.p.A.** e **22 Enti Sanitari Lombardi.**



L'obiettivo è l'ampliamento della Constituency, estendendo l'erogazione dei Servizi ai 18 Enti Sanitari Lombardi attualmente non presenti, Comuni, altri Enti e Organizzazioni della PA Lombarda, ecc.

GRAZIE