

TASK FORCE DI CYBERSECURITY PER GLI ENTI SANITARI

Arezzo, Novembre 2024



www.regione.lombardia.it

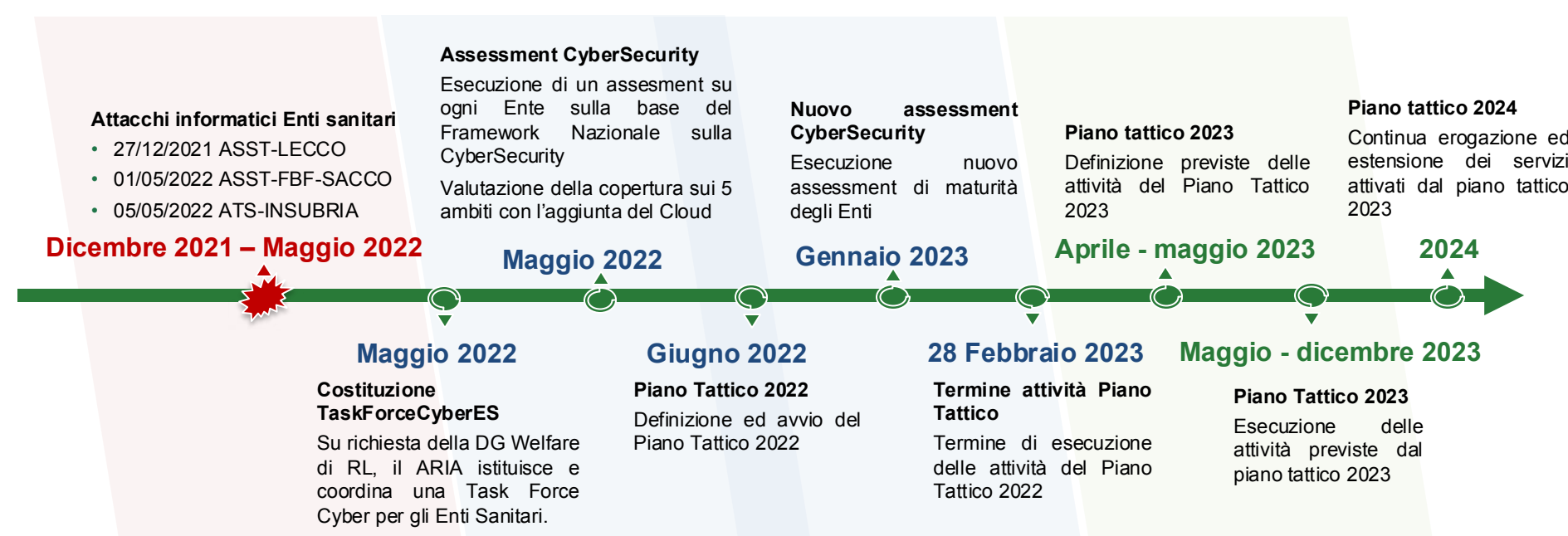


AGENDA



- TIMELINE DELLE ATTIVITA' SVOLTE NEL 2022
- DESCRIZIONE E NUMERI DEI SERVIZI FORNITI DA RL
- VALUTAZIONE DEL LIVELLO DI MATURITA'
- BUDGET CYBERSECURITY

Timeline



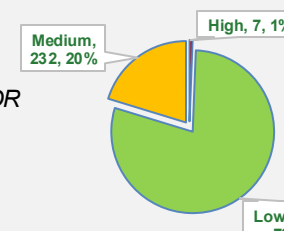
In aggiunta agli step rappresentati nella timeline, nel corso del 2023 è stata condivisa la metodologia di valutazione del livello di maturità cyber utilizzato da Regione Lombardia e ARIA anche agli Enti Sanitari Privati Accreditati con l'obiettivo di valutare in modo uniforme la cyber posture di tutto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



Descrizione e numeri dei servizi forniti da RL (1/4)

<p>Servizio SOC</p>	<p>Attivazione di un servizio volto al monitoraggio e alla gestione degli allarmi di sicurezza provenienti dai sistemi dell'Ente (servizio SOC di ARIA) e implementazione degli strumenti tecnologici necessari al tracciamento e raccolta degli eventi informatici (es. Log Collector).</p>	<p>36 <i>Enti coinvolti</i> 22 <i>Enti per cui il servizio è attivo</i></p>	<p>183 <i>Segnalazioni di incidenti inviate agli Enti dal servizio CSOC nel corso del 2024 (dato riferito alla singola segnalazione)</i></p>
<p>PAM</p>	<p>Disegno e progettazione di una soluzione tecnologica deputata alla gestione delle utenze amministrative (PAM - Privileged Access Management).</p>	<p>39 <i>Enti coinvolti</i> 22 <i>Enti in fase di «Design»</i></p>	<p>16 <i>Enti in fase di «Implementazione»</i></p>

Descrizione e numeri dei servizi forniti da RL (2/4)

<p>Servizio EDR/XDR</p>	<p>Servizio di Managed Detection & Analysis con copertura 24x7 per la gestione dei Security Incidents rilevati dalle piattaforme EDR, relativi a minacce inerenti regole di protezione Execution e Ransomware/Malware (High e Critical).</p>	<p>34 <i>Enti coinvolti</i></p>	<p>+ 80.000 Sistemi monitorati tramite EDR</p> <p>+ 1.140 Allarmi EDR gestiti nel 2024</p> 
<p>Servizio CTI</p>	<p>L'attività di monitoraggio CTI sugli Enti Sanitari mira, attraverso analisi automatiche e manuali, ad identificare informazioni esposte pubblicamente, evidenziando potenziali rischi collegati alla loro presenza al di fuori del perimetro aziendale.</p>	<p>40 <i>Enti coinvolti</i></p>	<p>183 <i>Segnalazioni CTI nel corso del 2024</i></p>

Descrizione e numeri dei servizi forniti da RL (3/4)

<p>VAPT</p>	<p>Svolgimento di attività di Vulnerability Assessment and Penetration Testing atte ad identificare le vulnerabilità nei sistemi informatici degli Enti. A fronte di un primo test con identificazione delle vulnerabilità e suggerimento dei piani di rimedio, si prevede l'esecuzione di un secondo test per verificare l'applicazione delle remediation.</p>	<p>39 <i>Enti coinvolti nelle attività di VAPT nel 2023</i></p>	<p>5 <i>Enti che hanno svolto le attività di recheck delle vulnerabilità identificate</i></p> <p>27 <i>Enti che testeranno nuovi applicativi nel 2024</i></p>
<p>Simulazioni Incidenti di sicurezza</p>	<p>Simulazione di un incidente in modalità Table Top con l'obiettivo di rafforzare l'awareness e la resilience dell'Ente, permettendo all'Ente di acquisire consapevolezza dei principali problemi che dovrebbe affrontare in caso di una vera crisi di sicurezza informatica e, svolgendo un esercizio dedicato, di sviluppare una "memoria muscolare" di risposta tempestiva all'incidente</p>	<p>40 <i>Enti coinvolti su 3 anni (2023-2025)</i></p>	<p>13 <i>Simulazioni svolte dal 2023</i></p> <p>13 <i>Simulazioni pianificate nel Q4 2024</i></p>

Descrizione e numeri dei servizi forniti da RL (4/4)

Corso e-learning di cybersecurity awareness	2022	Formazione personale tecnico Sessioni formative rivolte a Responsabili e amministratori IT (personale SIA e IC), responsabili Sicurezza IT, Referenti NIS, Referenti applicativi/Key user, Responsabili trattamenti, Risk manager. Modalità di erogazione in presenza con collegamento da remoto	577 <i>Membri del personale tecnico partecipanti al corso di formazione</i>
	2023-2024	Corso e-learning cyber awareness 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)	35 <i>Enti che hanno partecipato</i> +49.400 <i>Dipendenti degli Enti che hanno completato il corso di cyber awareness in modalità e-learning</i>

Budget cybersecurity

Si riporta di seguito l'andamento dei costi imputabili alla Cybersecurity a partire dal 2021, fino ad arrivare all'anno in corso e indicando le previsioni di spesa per il triennio 2025-2027.

