AIIC 2024 AWARDS

Digital Security & Compliance

Il progetto di **Cybersicurezza** di ARES Sardegna per gli Enti Sanitari della Sardegna

ARESSardegna
Azienda Regionale Salute

AIIC associazione italiana ingegneri clinici

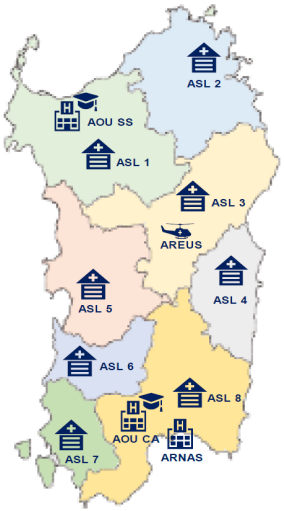
ARESSardegna
Azienda Regionale Salute

Dipartimento Sa.D.I.T.

Infrastrutture e Rete Dati	Sicurezza ICT	Governo delle Tecnologie Sanitarie
Sistemi informativi Sanitari e informatica Clinica	Acquisti di Tecnologie Informatiche	Gestione e Sicurezza Tecnologie Biomediche
Sistemi informativi Amministrativi		Procurement Tecnologie Biomediche

Legge Regionale 24/2020 conferisce ad ARES le funzioni accentrate e la gestione centralizzata per le:

- Otto Aziende Socio-sanitarie Locali (ASL)
- ARNAS G.Brotzu
- AREUS
- Aziende Ospedaliero-Universitaria di Cagliari (AOU)
- Aziende Ospedaliero-Universitarie di Sassari (AOU)



FUNZIONI ACCENTRATE:

- ❑ Gestione dei servizi tecnici per la valutazione delle tecnologie sanitarie (HTA)
- ❑ Servizi di Ingegneria clinica
- ❑ Gestione delle infrastrutture di tecnologia informatica
- ❑ Sicurezza informatica

PERCHE' E' NECESSARIO UN SISTEMA CYBERSECURITY ?

L'andamento attuale degli **attacchi cyber** nell'ambito **Sanitario** sta cambiando radicalmente:

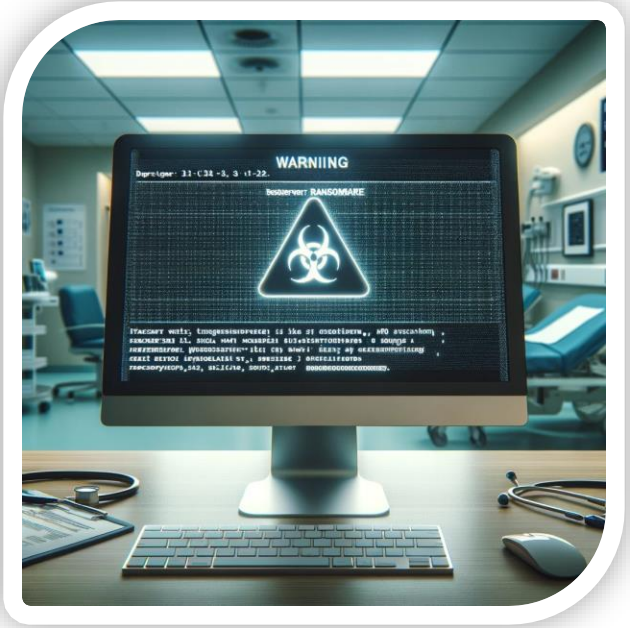
la Sanità è sottoposta a continui e diversificati attacchi di sicurezza

+105% di attacchi informatici alla **Sanità** dal **2023**

+31% di risorse nel **Dark web** che vendono **dati sanitari**

+24,8% di attacchi informatici registrati nel 2022/23 ha avuto come **obiettivo una struttura sanitaria**

18 mesi: 40 attacchi hacker ad **ospedali italiani**



*I DATI PROVENGONO DA CLUSIT – ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA – E DALL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE

AIIC 2024 AWARDS

CHIARA CRESCENZI SECURITY 23.10.2023

Gli ospedali di Verona sono stati colpiti da un cyberattacco

...atici hanno attaccato l'azienda, mettendo fuori uso i computer e il servizio prenotazioni

CORRIERE DELLA SERA | CORRIERE DEL VENETO | LE TUE NOTIZIE | Lettore_16083067

Verona, gli hacker pubblicano i dati rubati all'Azienda ospedaliera: «File amministrativi e analisi cliniche»

di Angiola Petronio

L'operazione degli hacker di Rhysida, gruppo criminale che una settimana fa aveva rivendicato il furto: il sito Red Hot Cyber svela il contenuto. L'Azienda sanitaria: «Partite le azioni legali per tutelare tutte le vittime dell'attacco»

Novecentomila. Per l'esattezza **900.128. Sono i file «esfiltrati»**, termine tecnico per dire portati fuori, **dalle infrastrutture informatiche dell'azienda ospedaliera** universitaria integrata di Verona. Quella che in Veneto sta facendo da capofila al nuovo sistema informatico ospedaliero voluto dalla Regione e che lo scorso 23 ottobre era stata vittima di un attacco hacker. Saccheggio di dati, negli ospedali di Borgo Trento e Borgo Roma, portato a termine dalla **cybergang Rhysida** che la scorsa settimana aveva pubblicato il suo ultimatum: la vendita nella rete Onion, al miglior offerente, di quei file al prezzo di 10 Bitcoin, quelli che - sette giorni fa - sul mercato equivalevano a circa 350mila euro.

"Attacco hacker all'Ausl di Modena, vulnerabilità anche a Reggio"

Forza Italia chiede alla Regione di riferire sull'attacco hacker subito dall'Ausl di Modena. La vulnerabilità potrebbe riguardare tutti gli enti locali e le aziende sanitarie della regione. Richiesta di audizione dell'assessore alla Scuola, Università, Ricerca e Agenda digitale.

il Resto del Carlino | Accedi | Abbonati

Cronaca Attacco hacker a Modena: prestazioni Asl in tilt, dati sensibili a rischio diffusione

Home > Modena > Cronaca > Attacco hacker a Mode...

29 nov 2023

Attacco hacker a Modena: prestazioni Asl in tilt, dati sensibili a rischio diffusione

Quasi paralizzate le attività del Policlinico e dell'ospedale di Sassuolo. E' stato diffuso un Ransomware criptolocker che cripta i dati e li 'libera' solo dopo il pagamento di un riscatto

AIIC associazione italiana ingegneri clinici

TIPOLOGIA DELL'ECOSISTEMA DIGITALE REGIONALE

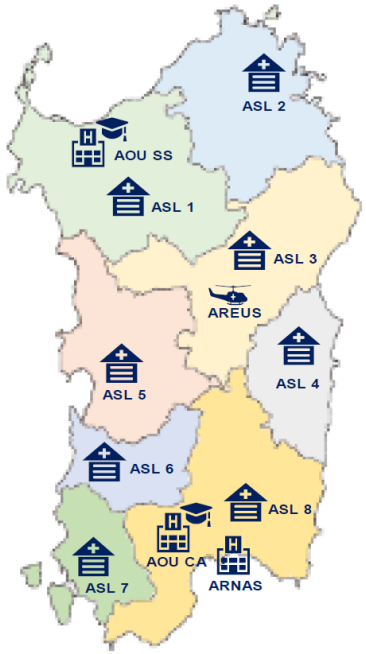
L'ecosistema tecnologico sanitario Regionale sardo integra differenti classi di tecnologie ognuna con caratteristiche e criticità specifiche:

- Le «classiche» tecnologie dell'informazione **(IT)**
- I sistemi di controllo industriali per reti elettriche e sistemi di condizionamento **(OT)**
- La nuvola di dispositivi e oggetto connessi c.d. Internet delle cose **(IoT)**
- **I dispositivi medici e i dispositivi diagnostici in vitro (MD/IVD)**

Un **ecosistema** così composto presenta diverse sfide:

- **Sicurezza informatica**: L'integrazione di dispositivi IoT, OT e MD nell'ambiente IT tradizionale aumenta la superficie di attacco aumentando il rischio in particolare per tutti i dispositivi critici.
- **Manutenzione e aggiornamenti**: tutti dispositivi connessi richiedono una manutenzione costante e tempestivi aggiornamenti software per rimanere sicuri e funzionali. Senza una gestione adeguata, questi dispositivi possono diventare gravemente vulnerabili.
- **Affidabilità e disponibilità**: La dipendenza da un numero elevato e multiforme di tecnologie connesse aumenta la probabilità di malfunzionamenti e incidenti dovuti a vulnerabilità non gestite che possono avere impatti diretti sui servizi, sulla somministrazione delle cure e, in alcuni casi, anche sulla sicurezza fisica dei pazienti e degli operatori.
- **Compliance normativa**: Il settore sanitario è altamente regolamentato. Le nuove tecnologie e l'organizzazione dei servizi devono soddisfare rigorosi standard normativi relativi alla sicurezza e alla privacy, come il **GDPR**, la **NIS2**, il **FNCS**.

IL GRUPPO DI LAVORO MULTIDISCIPLINARE



- **Ing. Giancarlo CONTI** Direttore Dipartimento Sa.D.I.T.
- **Ing. Marco GALISAI** Direttore S.C. Infrastrutture e Rete Dati
- **Ing. Barbara PODDA** Direttrice S.C. Governo delle Tecnologie Sanitarie
- **Ing. Davide ANGIUS** Direttore S.S. Gestione e Sicurezza Tecnologie Biomediche
- **Ing. Maurizio MEDDA** Direttore S.S.D. Sicurezza Informatica
- **Dott. Cesare DELUSSU** Direttore S.C. Sistemi Informativi Amministrativi
- **Dott. Gianfranco Bussalai** Direttore S.C. Sistemi informativi di AREUS

I rischi da mitigare presenti nell'ecosistema digitale sanitario possono essere classificati secondo tre tipologie:

Sicurezza
Infrastrutture e servizi

Sicurezza
Pazienti e operatori

Protezione dei Dati
Persone fisiche
pazienti, operatori ed altri soggetti coinvolti nelle attività di trattamento

Per mitigare adeguatamente questi rischi, è necessario:

- Avere una **visione end-to-end di tutto l'ecosistema digitale sanitario regionale**
- Adottare un **approccio olistico** alla sicurezza e alla «privacy»
- **Garantire la conformità alla norme cogenti** (CAD, GDPR, NIS2, FNCS ..
- Operare in stretta **collaborazione tra i servizi tecnologici e sanitari**
- Effettuare regolarmente attività di **formazione del personale tecnico e sanitario**

I NUMERI DELL'ECOSISTEMA DIGITALE REGIONALE

Ente	IT				INGCLIN	SERVTEC
	PdL censite	Server	PdL n/gestite	Device ICT	MD	IoT/OT
ASL 1 Sassari	1472	10	177	529	2195	74
ASL 2 Gallura	1233	61	148	446	2229	62
ASL 3 Nuoro	1292	70	155	468	1498	65
ASL 4 Ogliastra	486	49	58	177	451	24
ASL 5 Oristano	1335	4	160	479	1850	67
ASL 6 Medio Campidano	787	21	94	284	829	39
ASL 7 Sulcis	876	9	105	315	1344	44
ASL 8 Cagliari	2721	84	327	981	3026	136
ARNAS G Brotzu	1925	116	231	698	3850	96
AOU CA	1165	70	140	422	2330	58
AOU SS	2663	160	320	965	5325	133
AREUS	120	20	14	44	200	6
Totale	**16.075**	**674**	**1.929**	**5.808**	**25.127**	**804**

PdL censite	16.000
Server	674
PdL n/gestite	2.000
Device ICT	5.800
MD	25.000
IoT/OT	800

La **visione end-to-end** di un ecosistema digitale vasto e articolato è un obiettivo che presenta significative complessità tecniche ed organizzative. In particolare l'ecosistema digitale è composto da un lato «conosciuto» e un lato «oscuro». Nel **«lato oscuro»,** che sfugge alla visione e all'analisi dei sistemi di sicurezza convenzionali, si annidano la maggior parte delle vulnerabilità e dei rischi.

lato «conosciuto»

lato «oscuro»

Lato Conosciuto: il lato della rete che gli amministratori di **sistema conoscono e gestiscono. Include tutti i** dispositivi che hanno un «agent» installato come postazioni di lavoro e server, del «lato conosciuto fanno parte anche router, switch e firewall. Questa parte della **rete è monitorata e protetta** con misure e sistemi di sicurezza. Gli amministratori avendo una buona visibilità su questi dispositivi e possono gestire i dispositivi per mitigare le vulnerabilità.

Lato Oscuro: rappresenta quella parte della rete che non è completamente conosciuta o controllata dagli amministratori. Include dispositivi non autorizzati o dimenticati (es: tablet, vecchi computer, dispositivi IoT) e **dispositivi medici**. In genere è costituita da dispositivi che non hanno, o non possono istallare, un agent (p.e. un antivirus). Questa parte della rete per sua natura presenta vulnerabilità non gestite che possono essere sfruttate da attaccanti.

EVOLUZIONE DEL PARADIGMA DEL RISCHIO ASSOCIATO AI DM

ECRI

EVOLUZIONE DEL PARADIGMA DEL RISCHIO ASSOCIATO AI DM

2008 ECRI

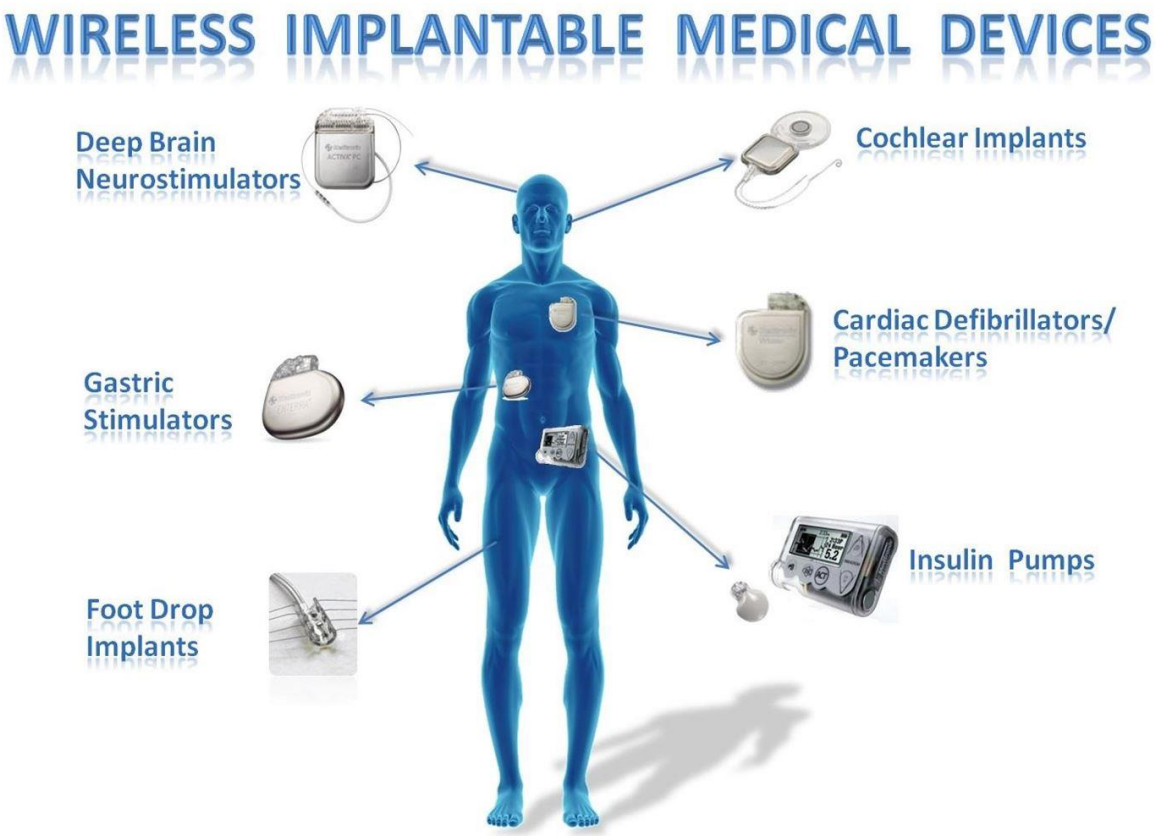
1. Alarm Hazards
2. Burns during Electrosurgery
3. Burns during Magnetic Resonance Imaging
4. Caster Failures
5. Infusion Pump Programming Errors
6. Misconnection of Blood Pressure Monitors to IV Lines
7. Needlesticks and Other Sharps Injuries
8. Radiation Dose in Computed Tomography
9. Radiation Therapy Errors
10. Surgical Fires

ECRI

Anno	RISCHIO	Q.
2008	• none	0
2009	• none	0
2010	• Problemi con le apparecchiature e i sistemi computerizzati	1
2011	• Perdita di dati, incompatibilità di sistema e altre complicazioni dell'IT sanitario	1
2012	• Poca attenzione al change management per la connettività dei dispositivi medici	1
2013	• Disallineamento tra dati e pazienti nei sistemi EHR e in altri sistemi informativi sanitari • Errori di interoperabilità con dispositivi medici e sistemi informativi sanitari • Distrazioni del caregiver da smartphone e altri dispositivi mobili	3
2014	• Errori nell'integrità dei dati nei sistemi EHR e in altri sistemi IT sanitari • Trascurare il change management per i dispositivi e i sistemi in rete	2
2015	• Integrità dei dati: dati errati o mancanti nei sistemi EHR e in altri sistemi IT per la salute • Cybersecurity: Protezioni insufficienti per dispositivi e sistemi	2
2016	• Gli errori si verificano quando le configurazioni HIT e il flusso di lavoro della struttura non sono allineati • L'uso improprio delle porte USB può causare il malfunzionamento dei dispositivi medici	2
2017	• Le lacune nella gestione del software mettono a rischio i pazienti e i dati dei pazienti	1
2018	• Il ransomware e altre minacce alla sicurezza informatica possono mettere in pericolo i pazienti. • I workaround possono annullare i vantaggi in termini di sicurezza dei sistemi di somministrazione dei farmaci con codice a barre • Malfunzionamenti della rete dei dispositivi medici possono portare a cure ritardate o inappropriate	3
2019	• Gli hacker possono sfruttare l'accesso remoto ai sistemi, interrompendo le attività sanitarie	1

Anno	RISCHIO (ECRI)	Q.
2020	• Rischi di cybersecurity nell'ambiente sanitario domestico connesso • Errori di medicazione dovuti a errori nella tempistica delle dosi nei sistemi EHR	2
2021	• La rapida adozione delle tecnologie di teleassistenza può mettere a rischio pazienti e dati • Le vulnerabilità dei componenti software di terze parti pongono problemi di sicurezza informatica • Le applicazioni di intelligenza artificiale per la diagnostica per immagini possono rappresentare in modo errato alcune popolazioni di pazienti • L'utilizzo remoto di dispositivi medici progettati per l'uso a letto introduce rischi • L'insufficiente garanzia di qualità dei dispositivi medici specifici per il paziente stampati in 3D può danneggiare i pazienti	5
2022	• Gli attacchi di cybersecurity possono interrompere l'erogazione dell'assistenza sanitaria, incidendo sulla sicurezza dei pazienti • Le carenze del flusso di lavoro della teleassistenza e dei fattori umani possono causare risultati insoddisfacenti • La ricostruzione basata sull'intelligenza artificiale può distorcere le immagini, mettendo a rischio i risultati diagnostici • Le interruzioni del Wi-Fi e le zone morte possono causare ritardi nell'assistenza ai pazienti, infortuni e decessi.	4
2023	• Le lacune nei richiami dei dispositivi medici domestici causano confusione e danni ai pazienti • La mancata gestione dei rischi di cybersecurity associati ai sistemi clinici basati su cloud può causare interruzioni dell'assistenza • L'uso eccessivo della telemetria cardiaca può portare a un sovraccarico cognitivo del medico e a eventi critici mancati	3

AVVENTO DELLA TELEMEDICINA COMPORTA UN AUMENTO DEL RISCHIO CYBERNETICO ASSOCIATO AI DM IMPIANTABILI



PECULIARITA' DI UN SISTEM DI CYBER SECURITY

Il valore di un progetto di **CYBER SECURITY** può essere misurato in termini di utilità e garanzia

Utilità:

- **Rispondenza ai Bisogni**: Il progetto deve soddisfare un bisogno o risolvere un problema specifico.
- **Impatto e Benefici**: Deve produrre un impatto positivo nel contesto in cui verrà implementato e sugli utenti finali
- **Efficienza ed Efficacia**: deve ottimizzare le risorse impiegate e produrre i benefici attesi nei termini e nei tempi adeguati.

Garanzia:

- **Sostenibilità**: il progetto è tecnicamente realizzabile e sostenibile a lungo termine,
- **Raggiungimento degli obiettivi**: sono identificati e mitigati i rischi potenziali che possono minacciare il successo del progetto, ovvero la sua utilità.
- **Conformità Legale e Normativa**: il progetto deve rispettare le leggi e le normative pertinenti.

SOC Operating Model - REALIZZAZIONE DEL PROGETTO

AZIONI CARDINE 1

Azioni adottate con regole concorrenti che un modello di cyber security dovrebbe garantire:

- **IDENTIFY** Identificare il rischio
- **PROTECT** Proteggere i dati
- **DETECT** Rilevare gli attacchi
- **RESPOND** Adottare azioni mirate
- **RECOVER** Ripristinare il disservizio

CARATTERISTICHE PER UN STRUMENTO DI CYBER SECURITY 2

- **Soluzione integrata** per ICT device e Medical device
- Capacità di **implementare automaticamente** le regole di sicurezza
- Implementare nuove policy basate su **AI - MACHINE LEARNING**
- **Monitoraggio passivo** e **sniffing** continuo del traffico di rete sugli apparati in real-time

SECURITY OPERATION CENTER (S.O.C.)

PROGETTAZIONE INFRASTUTTURA DI RETE 4

- **Centralizzazione SW di monitoraggio** con installazione centralizzata del server web che gestisce le policy
- **Installazione sonde** in ciascuna sede individuata per monitoraggio il traffico di rete
- **Soluzione passiva** che non alteri l'efficienza e l'efficacia diagnostica

SERVIZIO SAAS 3

La mancanza di skill interne necessita di implementare un «servizio» h24 7/7gg composto da un team di esperti che utilizzano appositi strumenti e tecnologie per rilevare, analizzare e rispondere a incidenti di sicurezza informatica

SOC Operating Model - REALIZZAZIONE DEL PROGETTO

La strategia di Digital Security è declinata secondo **11 obiettivi**

Innovazione

Ob1: Asset intelligence sull'intero perimetro dell'infrastruttura sanitaria regionale, tramite l'utilizzo di tecnologie innovative che consentono la visione completa dell'ecosistema digitale compreso il suo «lato oscuro»

Protezione

Ob2: Protezione degli asset digitali
Ob3: Monitoraggio continuo dell'efficacia delle misure di sicurezza
Ob4: Rilevazione e risposta tempestiva agli attacchi cyber
Ob5: Protezione dei dati personali degli interessati
Ob6: Rafforzamento della "safety" dei sistemi critici medicali a garanzia dei pazienti e degli operatori

Conformità

Ob7: Adeguamento delle organizzazioni sanitarie alle normative nazionali ed europee in ambito security e data protection (det.628, NIS2, GDPR)
Ob8: Adeguamento di AREUS al PSCN

Standard

Ob9: Certificazione ISO 27001, ISO 27017, ISO 27018 di ARES
Ob10: Qualificazione ACN per i servizi SAAS di ARES

Efficienza

Ob11: Continuità operativa e integrità dei servizi di sanità digitale

Iniziative

Gli obiettivi si concretizzano attraverso **14 «iniziative»** corrispondenti ad un sottoinsieme dei servizi disponibili su Lotto 1 e 2 AQ 2296 + una iniziativa relativa all'antivirus da definire

AQ 2296

- Lotto 2
- Lotto 1

Endpoint Protection

SOC Operating Model - REALIZZAZIONE DEL PROGETTO

AQ 2296

Lotto 2

Lotto 1

	Iniziative	Servizi AQ 2296	
1.	Security Strategy	L2.S16	
2.	Vulnerability Assessment	L2.S17	
3.	Testing Dinamico del Codice	L2.S19	
4.	Supporto all'analisi/ incidenti	L2.S21	
5.	Penetration Testing	L2.S22	
6.	Compliance Normativa	L2.S23	
7.	Security Operation Center		L1.S1
8.	Next Generation Firewall		L1.S2
9.	Web Application Firewall		L1.S3
10.	Vulnerability Management		L1.S4
11.	Threat Intelligence		L1.S5
12.	Security Awareness		L1.S9
13.	Gestione identità e accesso utente	L1.S10	
14.	Servizi Specialistici	L1.S15	

Tecnologie: FORTINET, ARMIS, splunk>, IBM Radar

- Endpoint protection

Tecnologie: SOPHOS, TREND MICRO

SOC Operating Model - COSTI DEL PROGETTO

AQ 2296

- Lotto 2
- Lotto 1

	Iniziative	Servizi AQ 2296		Costi IVA Esclusa
1.	Security Strategy		L2.S16	12.250.484,16 €
2.	Vulnerability Assessment		L2.S17	
3.	Testing Dinamico del Codice		L2.S19	
4.	Supporto all'analisi e gestione degli incidenti	L2.S21		
5.	Penetration Testing	L2.S22		
6.	Compliance Normativa	L2.S23		
7.	Security Operation Center		L1.S1	3.343.070,00 €
8.	Next Generation Firewall		L1.S2	
9.	Web Application Firewall	L1.S3		
10.	Vulnerability Management		L1.S4	
11.	Threat Intelligence	L1.S5		
12.	Security Awareness	L1.S9		
13.	Gestione identità e accesso utente	L1.S10		
14.	Servizi Specialistici	L1.S15		
○	Endpoint protection			1.100.000,00 €

CUP ASSEGNATO : D76G24000040002

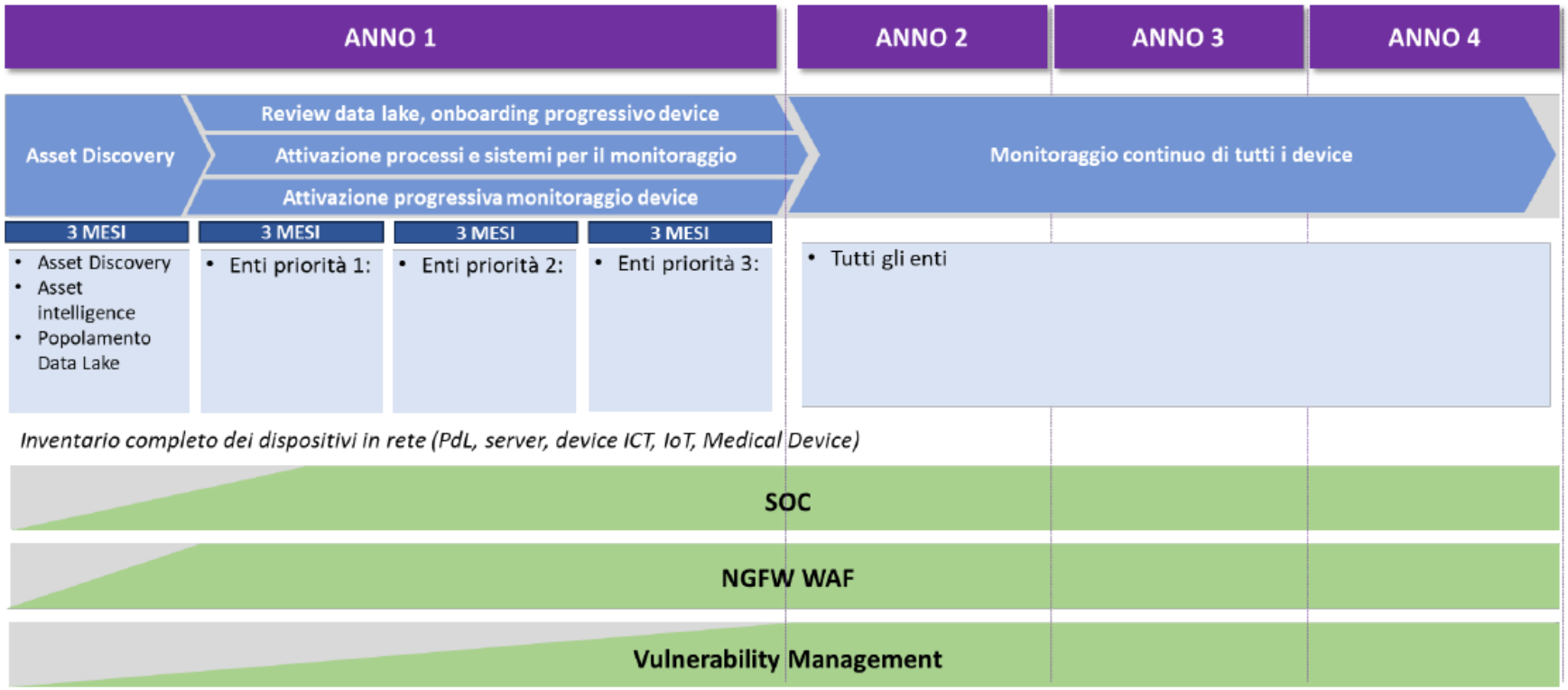
SOC Operating Model - COSTI DEL PROGETTO

		Complessivo	Anno 1	Anno 2	Anno 3	Anno 4
Security Operation Center	L1.S1	**3.009.200,00 €**	*752.300,00 €*	*752.300,00 €*	*752.300,00 €*	*752.300,00 €*
Next Generation Firewall	L1.S2	**856.440,00 €**	*214.110,00 €*	*214.110,00 €*	*214.110,00 €*	*214.110,00 €*
Web Application Firewall	L1.S3	**44.800,00 €**	*11.200,00 €*	*11.200,00 €*	*11.200,00 €*	*11.200,00 €*
Vulnerability Management	L1.S4	**909.640,80 €**	*227.410,20 €*	*227.410,20 €*	*227.410,20 €*	*227.410,20 €*
Threat Intelligence	L1.S5	**56.800,00 €**	*14.200,00 €*	*14.200,00 €*	*14.200,00 €*	*14.200,00 €*
Security Awareness	L1.S9	**251.975,36 €**	*251.975,36 €*	- €	- €	- €
Endpoint protection	L1.S7	- €	- €	- €	- €	- €
Servizi Specialistici	L1.S15	**7.121.628,00 €**	*3.672.890,00 €*	*1.149.579,33 €*	*1.149.579,33 €*	*1.149.579,33 €*

Security Strategy	L2.S16	**1.837.500,00 €**	*643.125,00 €*	*551.250,00 €*	*367.500,00 €*	*275.625,00 €*
Vulnerability assessment	L2.S17	**337.920,00 €**	*84.480,00 €*	*84.480,00 €*	*84.480,00 €*	*84.480,00 €*
Dynamic Application Security Testing	L2.S19	**56.100,00 €**	*14.025,00 €*	*14.025,00 €*	*14.025,00 €*	*14.025,00 €*
Supporto all'analisi e gestione degli incidenti	L2.S21	**159.120,00 €**	*87.516,00 €*	*23.868,00 €*	*23.868,00 €*	*23.868,00 €*
Penetration testing	L2.S22	**114.840,00 €**	*28.710,00 €*	*28.710,00 €*	*28.710,00 €*	*28.710,00 €*
Compliance normativa	L2.S23	**837.590,00 €**	*293.156,50 €*	*209.397,50 €*	*209.397,50 €*	*125.638,50 €*
	TOT	15.593.554,16 €	6.295.098,06 €	3.280.530,03 €	3.096.780,03 €	2.921.146,03 €

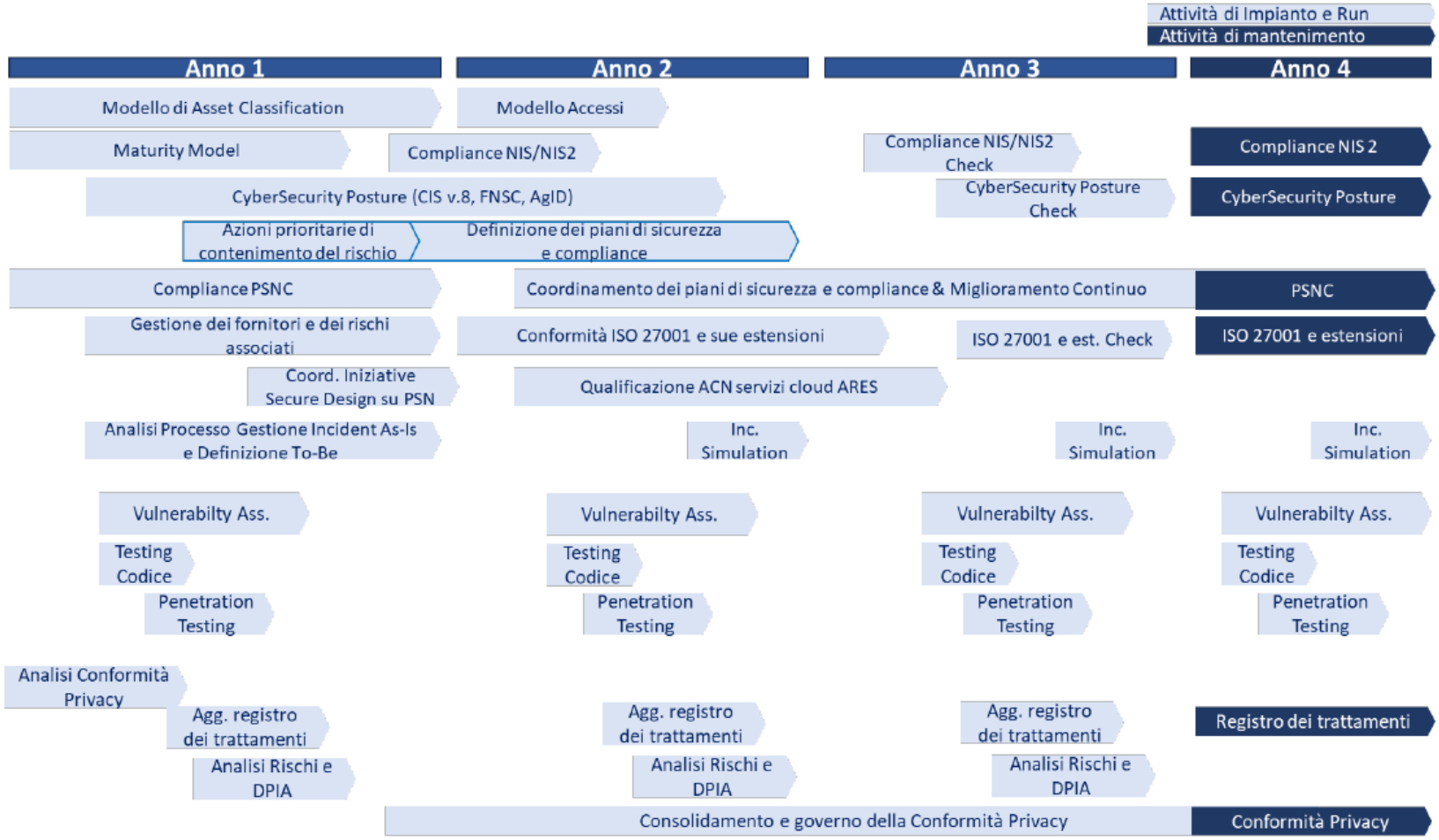
Attivazione dei principali servizi CRONOPROGRAMMI

LOTTO1



Attivazione dei principali servizi CRONOPROGRAMMI

LOTTO2



Grazie

Digital Security & Compliance

DAVIDE ANGIUS

Direttore S.S. Gestione e Sicurezza Tecnologie Biomediche
SC Governo Tecnologie Sanitarie
Dipartimento per la Sanità Digitale e l'Innovazione Tecnologica
sic.tecbio@aressardegna.it - davide.angius@aressardegna.it

«…nel ricordo di un amico e collega che ha partecipato alla stesura del progetto. Ci hai lasciato troppo presto

Ciao Gianfranco……»

A nome di tutti I colleghi del Dipartimento SaDIT di ARES

AIIC associazione italiana ingegneri clinici

ARESSardegna Azienda Regionale Salute