



Sicurezza ed efficienza operativa dei dispositivi elettromedicali

il progetto nell'Azienda ospedaliera di Alessandria



Ing. Dario Ricci
Direttore S.C. I.C.T. e Innovazione Tecnologica
Azienda Ospedaliera di Alessandria

#sanita2030

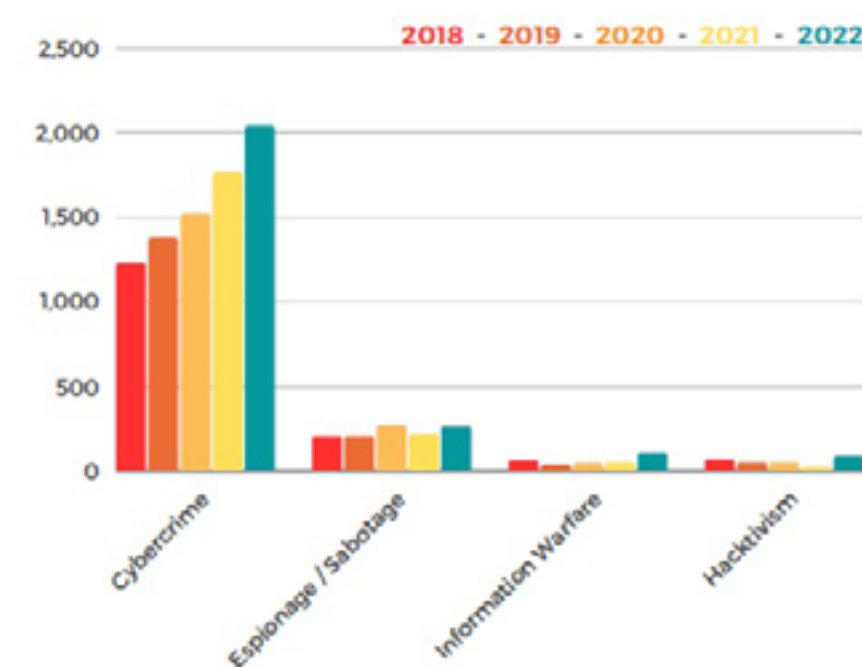


www.sanita2030.it



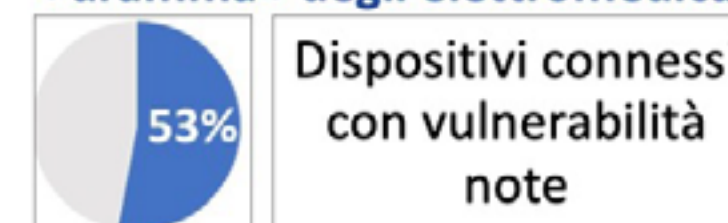


Gli attacchi

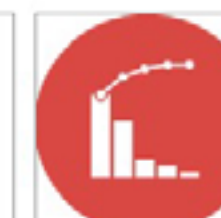


Fonte: HACKMANAC GLOBAL CYBERATTACKS REPORT 2023

Il contesto ospedaliero: il «dramma» degli elettromedicali



- Pompe per insulina
- Defibrillatori cardiaci
- Telemetria cardiaca mobile
- Pacemaker
- Pompe antidolorifiche intratecali



6,2 n. di vulnerabilità per Dispositivo Medico

Fonte: Private Industry Notification FBI, Settembre 2022

#sanita2030



www.sanita2030.it





Ragnar Locker ransomware



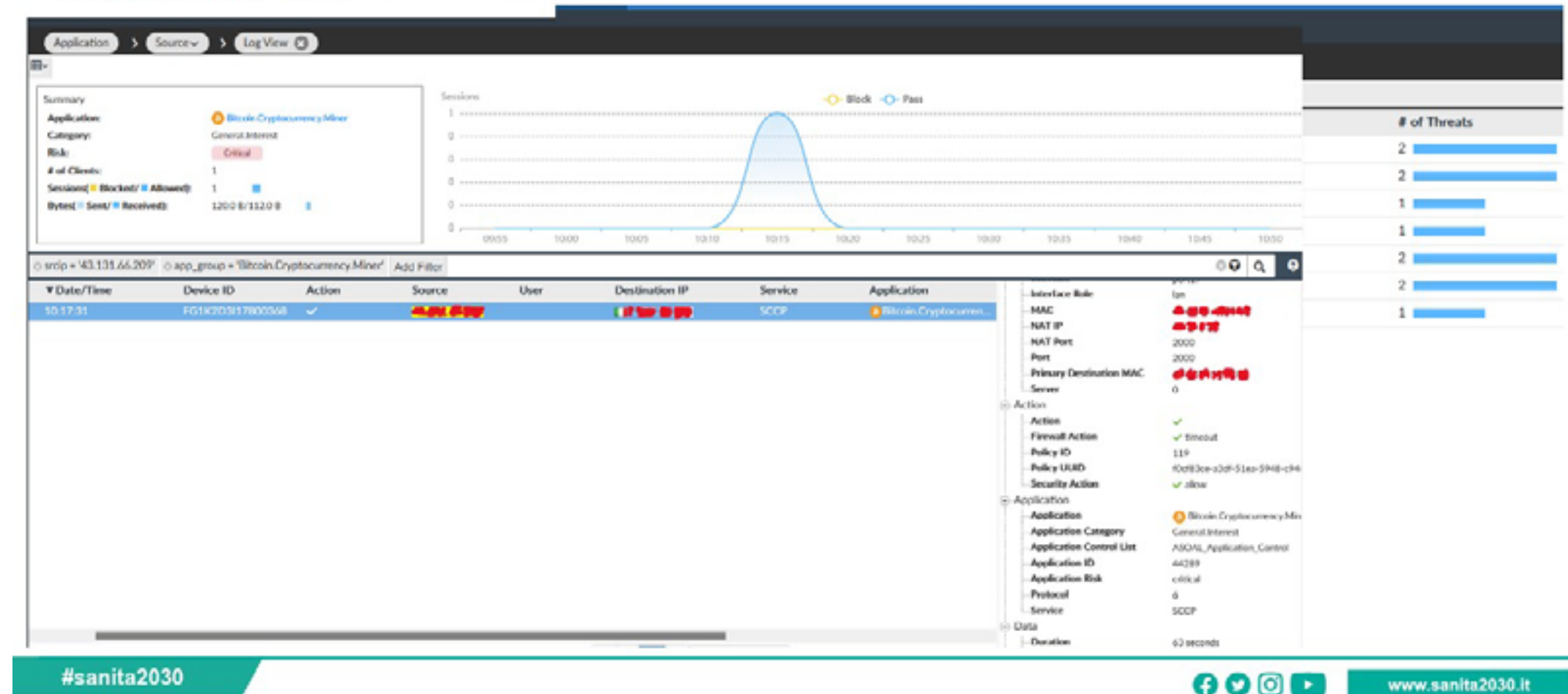
<https://www.agendadigitale.eu/sicurezza/pa-nel-mirino-degli-hacker-il-caso-emblematico-dellospedale-di-alessandria/>

#sanita2030



www.sanita2030.it

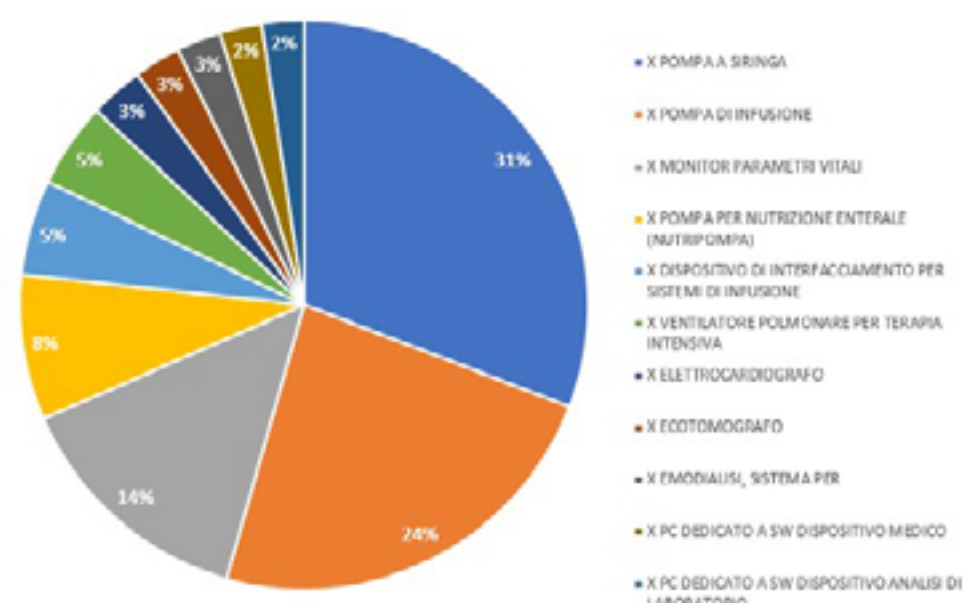






Descrizione: consolidamento della sicurezza degli EM in rete

Parco installato ASO Alessandria



- Circa 6.000 dispositivi
- 25 % in rete (in crescita)



Livelli di servizio vs protezione
 dispositivi medici in rete in costante aumento
 alto rischio di vulnerabilità cyber (non in dominio, non aggiornati, no antivirus)



Integrazioni
 nativa con le tecnologie di sicurezza della rete aziendale
 compliant con gli obblighi di release management di patch e fix



Inventory Asset Management
 gestione, classificazione e catalogazione passiva di tutti i dettagli degli EM in rete
 Tracciatura di attributi quali firmware, numeri di serie, stato di sicurezza, posizione

#sanita2030

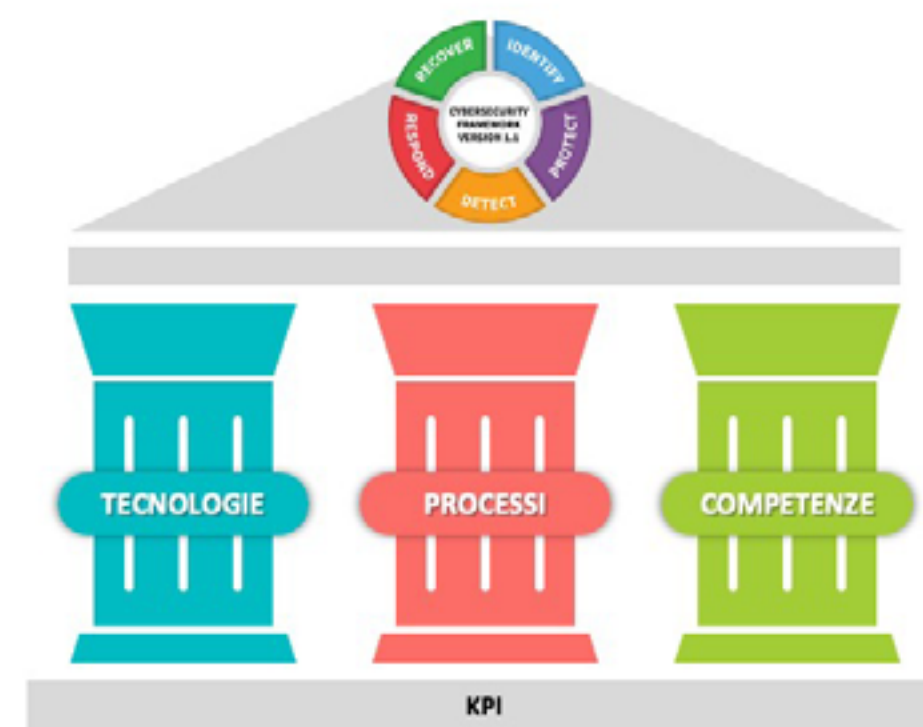


www.sanita2030.it





Descrizione: consolidamento della sicurezza degli EM in rete



- Firewall
- Endpoint Protection
- MDSP (Medical Device Security Platform)
- Business Continuity / Disaster Recovery
- Segmentazione della rete

- REVISIONE ORGANIZZAZIONE AZIENDALE
- REVISIONE PROCEDURE DI MANUTENZIONE
- REVISIONE CONTRATTI (INSTALLAZIONE)
- REVISIONE PROCEDURE CONTROLLO (VA, TIA)

- Data Breach Incident Management
- Cyber Incident Response
- Security Operations Centre (SOC)
- Formazione operatori

#sanita2030



www.sanita2030.it

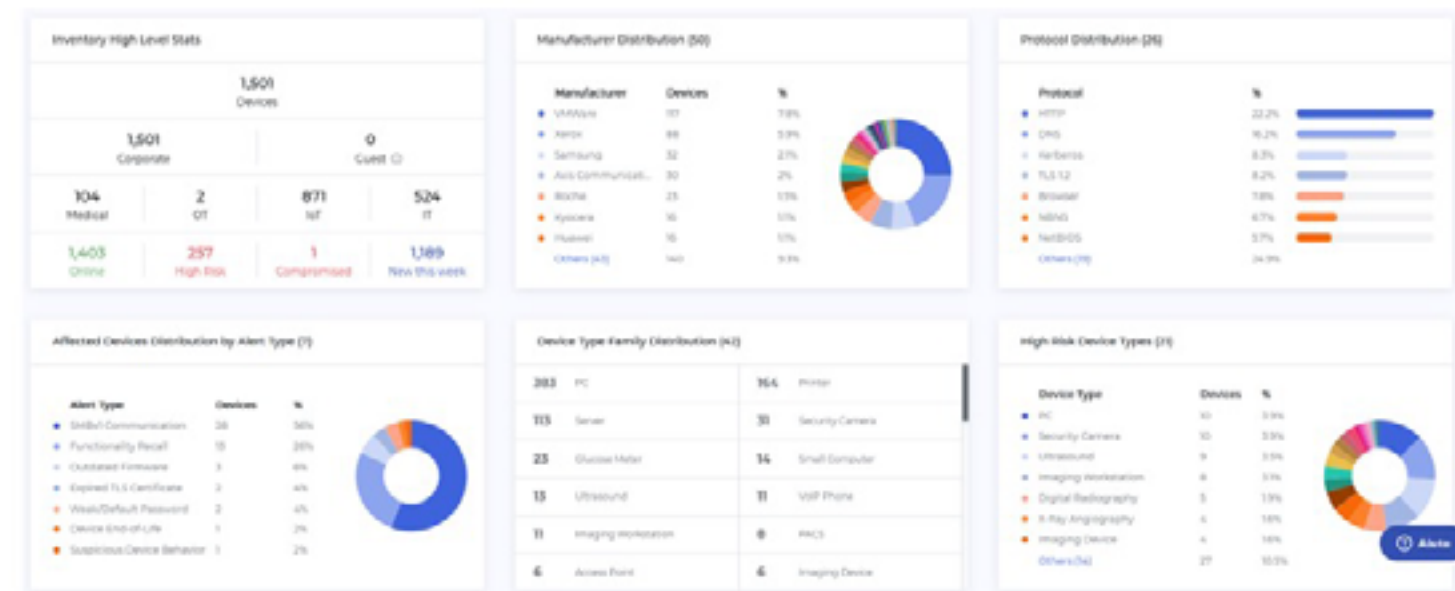




Firewall
 Endpoint Protection
MDSP (Medical Device Security Platform)
 Business Continuity / Disaster Recovery
 Segmentazione della rete



- 4 presidi
- 560 posti letto
- 2.300 dipendenti
- 1,3M prestazioni ambulatoriali
- 6.000 Device elettromedicali



#sanita2030



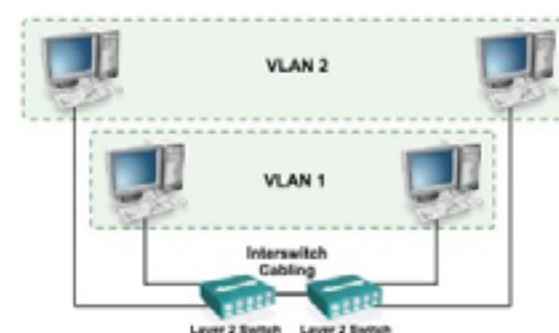
www.sanita2030.it





Firewall
 Endpoint Protection
 MDSP (Medical Device Security Platform)
 Business Continuity / Disaster Recovery
Segmentazione della rete

Virtualizzazione della rete



	Bl	Cl	Cl	Co	Comp...	Gener...	Imaging										Mr	Network	Patten...	Servers													
	Building Automation...	Defect Intake	Lab Device	VoIP Phone	PC	Small Computer	Printer	Other	C-Arm	Computed Radiograp...	Computed Tomograp...	Digital Radiography	Imaging Device	Imaging Processing S...	Imaging Workstation	Mammography	MSI	Nuclear Medicine	O-Arm	PMCS	Surgical Navigation Sy...	Ultrasound	Ultrasound Image Ma...	X-Ray Angiography	Generic Mobile Device	Access Point	Network Equipment	Switch	Course Meter	Course Meter Gateway	Domain Server	Server	
10																																	
21																																	
22																																	
27																																	
28																																	

#sanita2030



www.sanita2030.it



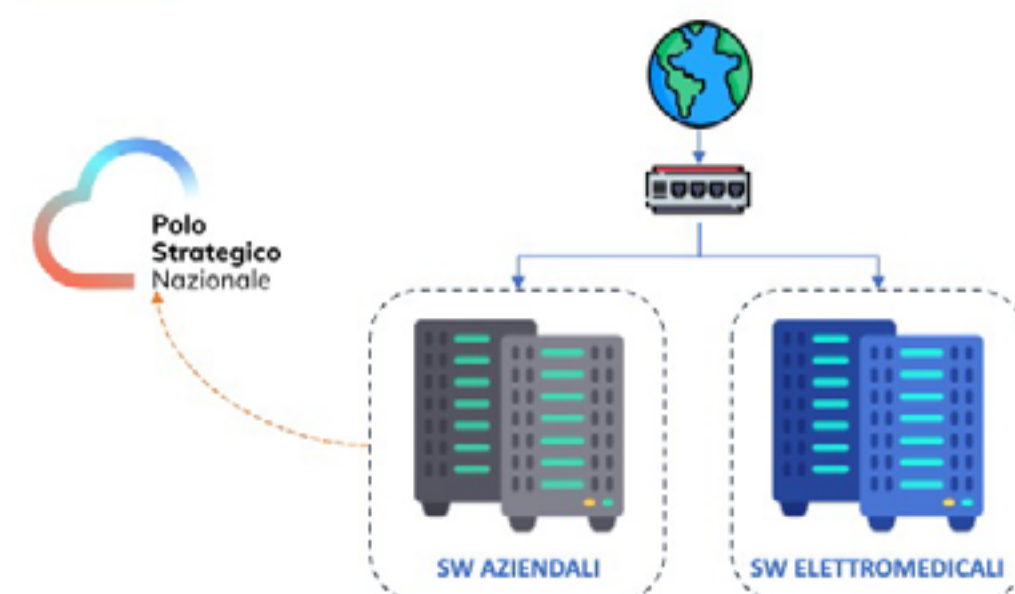


Firewall
Endpoint Protection
SIEM | SEG | PAM
MDSP (Medical Device Security Platform)
Business Continuity / Disaster Recovery
Segmentazione della rete



Cluster dedicato agli Elettromedicali

- Server quad-processore rackable
- Gestione separata di release, aggiornamenti, integrazioni
- Integrazioni dedicate al FSE
- Maggiore compliance ai requisiti di cybersecurity ACN e al GDPR

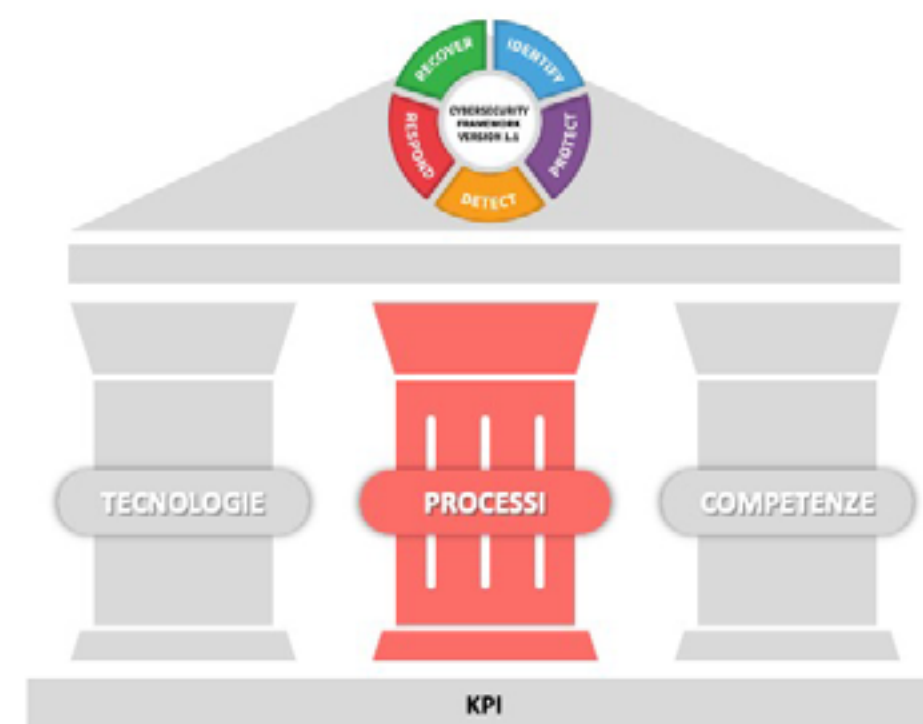


#sanita2030



www.sanita2030.it





- Firewall
- Endpoint Protection
- MDSP (Medical Device Security Platform)
- Business Continuity / Disaster Recovery
- Segmentazione della rete

- REVISIONE ORGANIZZAZIONE AZIENDALE
- REVISIONE PROCEDURE DI MANUTENZIONE
- REVISIONE CONTRATTI (INSTALLAZIONE)
- REVISIONE PROCEDURE CONTROLLO (VA, TIA)

- Data Breach Incident Management
- Cyber Incident Response
- Security Operations Centre (SOC)
- Formazione operatori

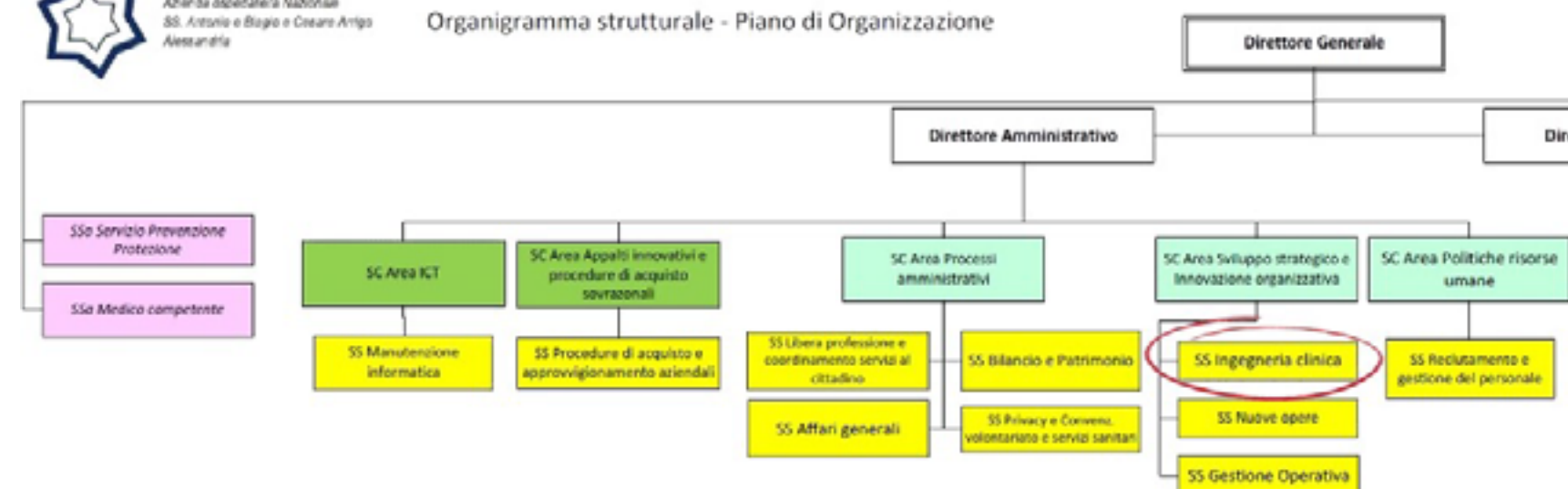


REVISIONE ORGANIZZAZIONE AZIENDALE
 REVISIONE PROCEDURE DI MANUTENZIONE
 REVISIONE CONTRATTI (INSTALLAZIONE)
 REVISIONE PROCEDURE CONTROLLO (VA, TIA)



Azienda ospedaliera Nazionale
 SS. Antonio e Biagio e Cesare Arrigo
 Assandria

Organigramma strutturale - Piano di Organizzazione



#sanita2030

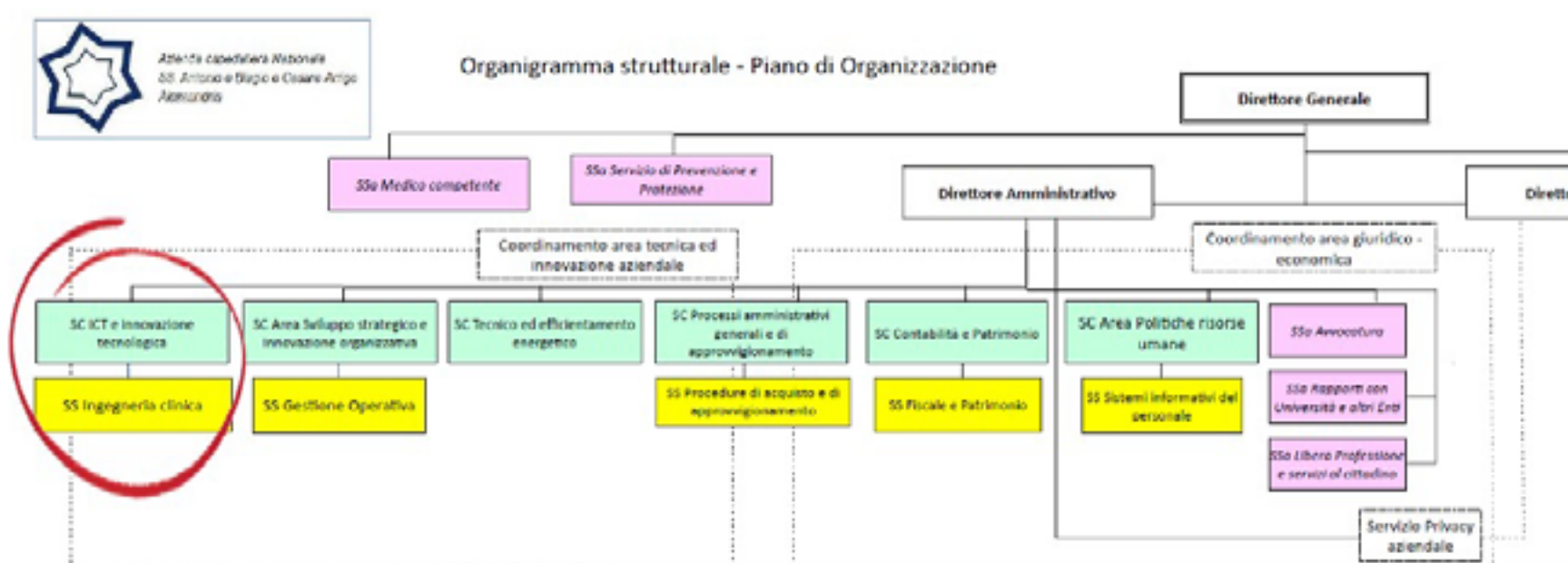


www.sanita2030.it





REVISIONE ORGANIZZAZIONE AZIENDALE
 REVISIONE PROCEDURE DI MANUTENZIONE
 REVISIONE CONTRATTI (INSTALLAZIONE)
 REVISIONE PROCEDURE CONTROLLO (VA, TIA)



#sanita2030



www.sanita2030.it





REVISIONE ORGANIZZAZIONE AZIENDALE
REVISIONE PROCEDURE DI MANUTENZIONE
REVISIONE CONTRATTI (INSTALLAZIONE)
REVISIONE PROCEDURE CONTROLLO (VA, TIA)

1. Marca e modello
2. Sistema operativo
3. MAC address
4. Borchia su cui sono collegate
5. Certificazione medica che indichi il livello di hardening, antivirus, autenticazione

Ateneo Ispettorato Tecnico
22. Agosto e Sapi e Saverio Sapi
Ateneo

INFORMATICA
22. Agosto e Sapi e Saverio Sapi
Ateneo

Collaudi rete progetti biomedicali

Esposito di cui sono sottile la macchina:
Firma: Caposera, Sapi e Saverio Sapi per l'installazione:
Firma: Caposera, Sapi e Saverio Sapi della Fornitura per l'installazione:

Delice apparecchiatura:
 Radiologia, apparecchiatura per immagini
 Laboratorio
 Altro

POS	Mac Address	Borchia	Marca e Modello	Serial

NOTE in caso di problemi aderisce regole standard:

MODELLO "SCHEMA COMUNICATIVO"

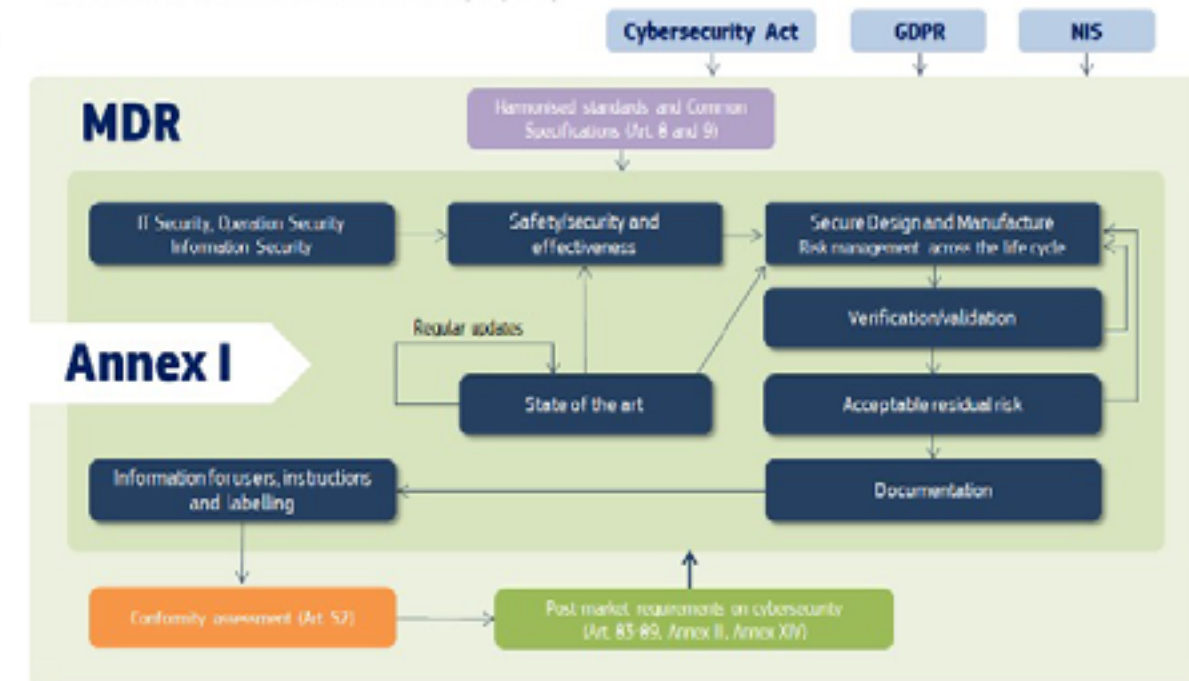
IP SOGGETTO	IP DESTINAZIONE	PORTA DI DESTINAZIONE	NOTE

Firma collaudo di rete, da firmare il giorno dell'installazione:
Firma e timbro Responsabili Saverio Sapi, Saverio Sapi
Firma e timbro Data, Fornitore



REVISIONE ORGANIZZAZIONE AZIENDALE
 REVISIONE PROCEDURE DI MANUTENZIONE
 REVISIONE CONTRATTI (INSTALLAZIONE)
 REVISIONE PROCEDURE CONTROLLO (VA, TIA)

Finanziato dall'Unione europea
 NextGenerationEU



#sanita2030



www.sanita2030.it





REVISIONE ORGANIZZAZIONE AZIENDALE
 REVISIONE PROCEDURE DI MANUTENZIONE
 REVISIONE CONTRATTI (INSTALLAZIONE)
 REVISIONE PROCEDURE CONTROLLO (VA, TIA)

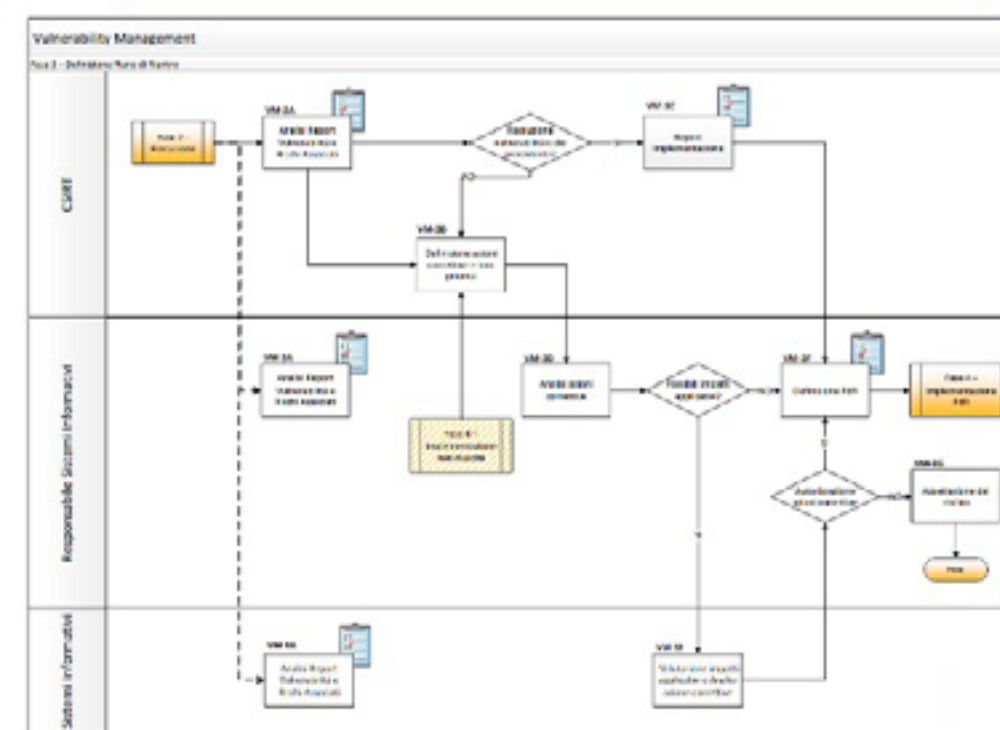
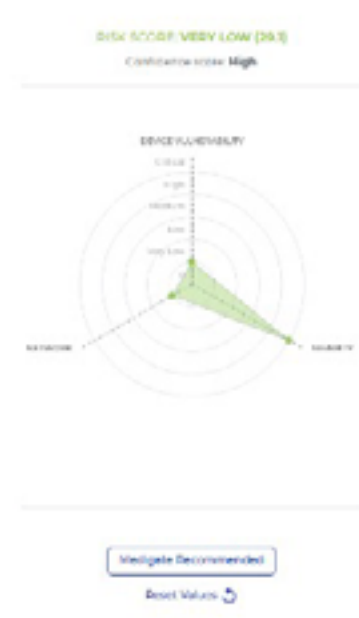


⚠️ Attenzione alle patch!

DEVICE VULNERABILITY	
Endpoint Security	Installed
Operating System	Windows Server 2008 R2 SP6
Outdated Firmware	No
Default Credentials Login	No
Known Vulnerabilities	No Vulnerabilities
Web/Cache/Networks	No

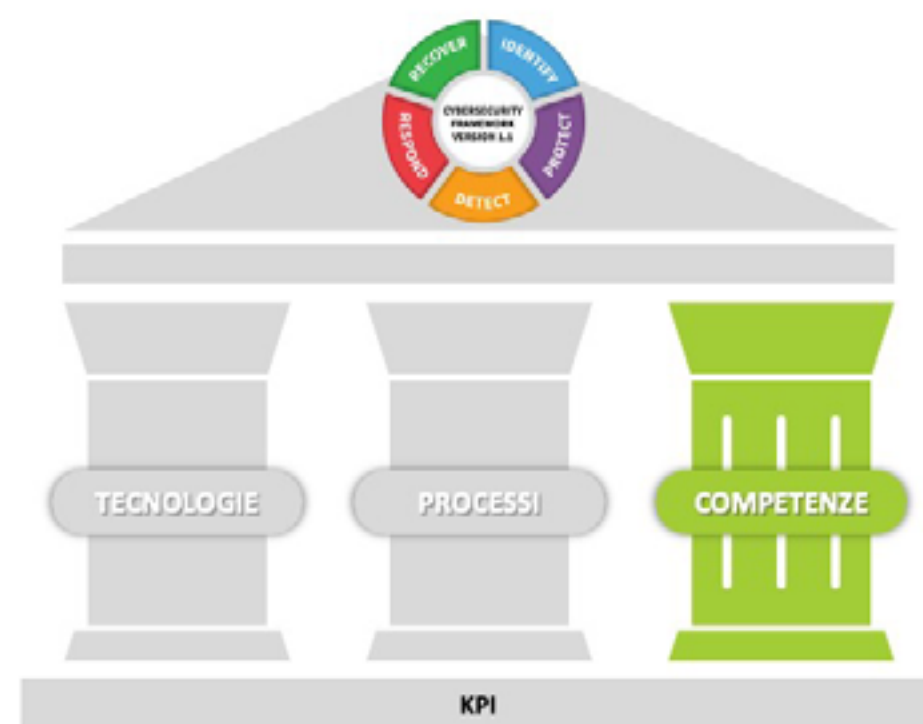
NETWORK	
Connection Type	Ethernet
Accessment Level	Optimized ACL
Internet Communication	Multiplurist
Managed	AD
Network	Corporate
VLAN Tagging	Unknown Type Medical VLAN

SEVERITY	
Internal Cost	500,000-1,000,000
Consequence of Failure	Inappropriate Therapy or Misdiagnosis
Customer Class	Diagnostic Device
PHI	Stored & Transmitted



#sanita2030

www.sanita2030.it



- Firewall
- Endpoint Protection
- MDSP (Medical Device Security Platform)
- Business Continuity / Disaster Recovery
- Segmentazione della rete

- REVISIONE ORGANIZZAZIONE AZIENDALE
- REVISIONE PROCEDURE DI MANUTENZIONE
- REVISIONE CONTRATTI (INSTALLAZIONE)
- REVISIONE PROCEDURE CONTROLLO (VA, TIA)

- Data Breach Incident Management
- Cyber Incident Response
- Security Operations Centre (SOC)
- Formazione operatori

#sanita2030

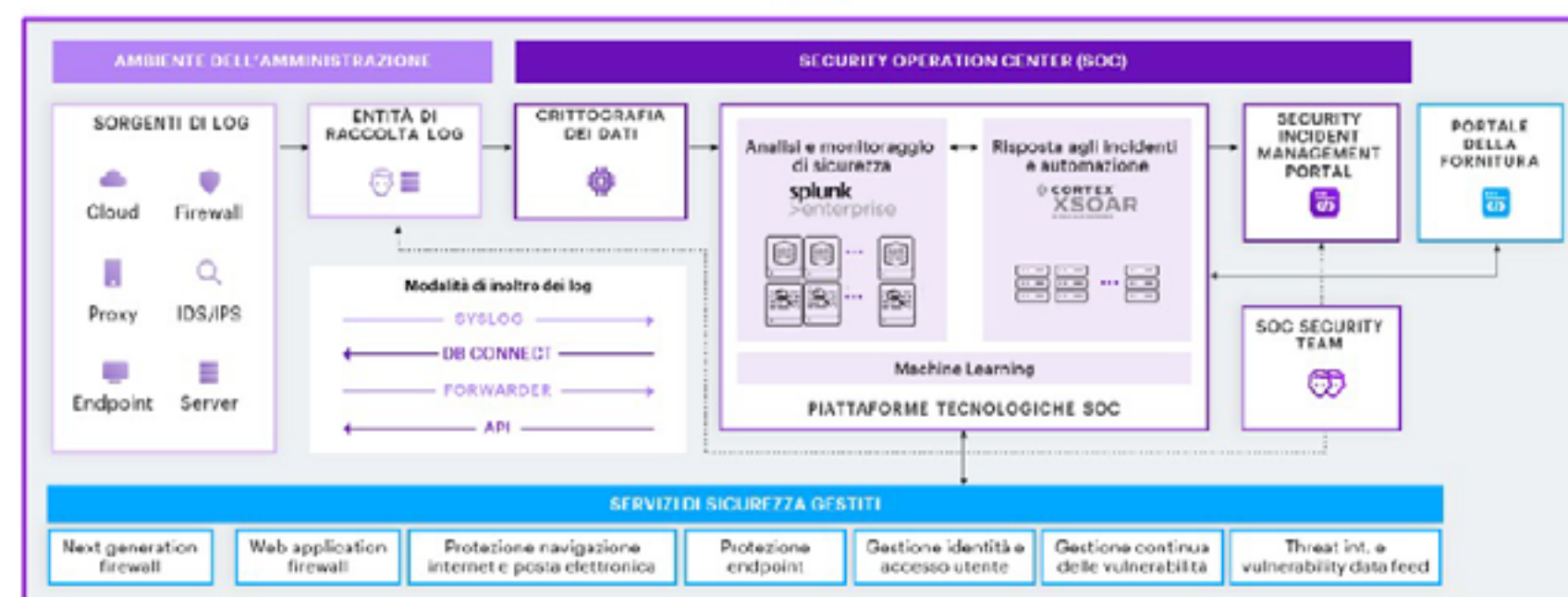


www.sanita2030.it





Data Breach Incident Management
 Cyber Incident Response
 Security Operations Centre (SOC)
 Formazione operatori



#sanita2030


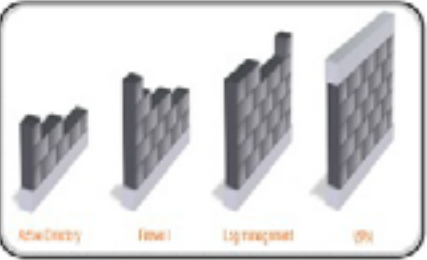


www.sanita2030.it

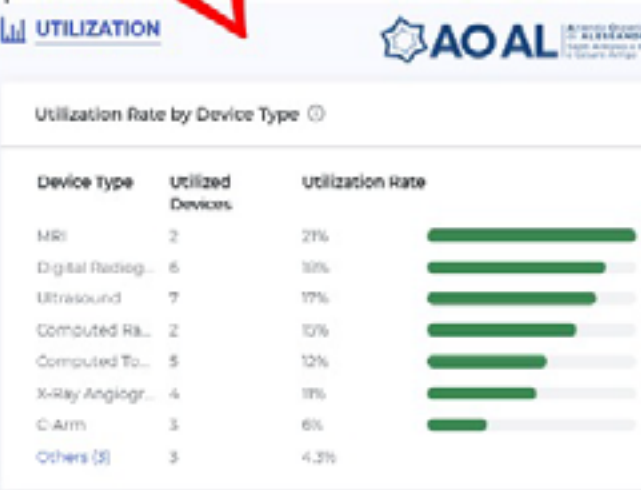




ICT e Ingegneria Clinica integrate per la sicurezza e l'efficienza







1. Chi è davvero l'hacker

<https://blog.malwarebytes.com/cyber-crime/2018/08/under-the-hoodie-why-money-power-and-ego-drive-hackers-to-cybercrime/>



2. Partire dalle basi:

- Gestione Active Directory
- Gestione firewall
- Gestione VPN
- Log management

3. sicurezza è organizzazione:

- la tecnologia non basta: meccanismi di accountability
- Formazione
- Gestione integrata delle informazioni

#sanita2030

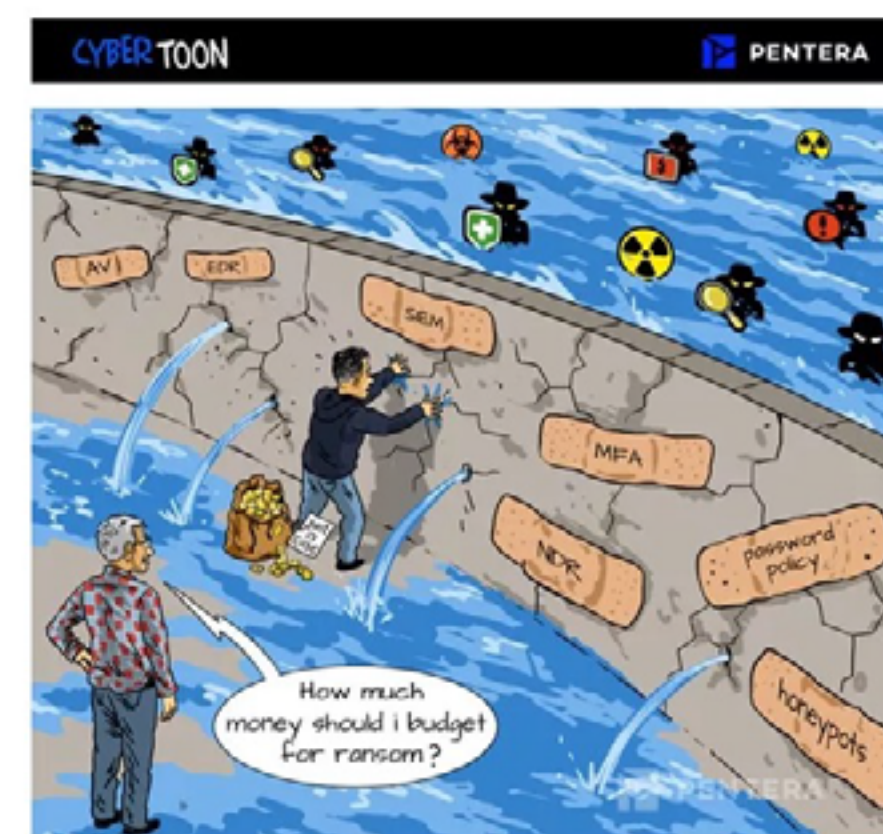


www.sanita2030.it





grazie !



Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941)
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

[Torna all'inizio](#)