Cybersecurity e Dispositivi Medici: scenari innovativi per la sanità nell'era del cloud, dell'IoT, dei big data e del mobile computing

Michele Bava

IRCCS "Burlo Garofolo"

2 parti

Parte 1: Nuove normative tecniche e regolamenti Europei per i dispositivi medici

Parte 2: Analisi dei dati dall'utilizzo dei sistemi Medigate c/o IRCCS Burlo Garofolo

Ringraziamenti

Mead Informatica (Lisa Bassetto, Fabio Tolomelli, Mirko Gorrieri, Roberto Fantini, Giorgia Marchesi, Daniele Giacomelli)

Medigate (Offir Levy, Amit Har-Esh)

TrendMicro (Marco Iorio, Alex Galimi)

Riccardo Zangrando e Piero Pascolo e ASUFC

Parte 2

Parte 2.1: cybersecurity, information security e data protection

Parte 2.2: demo sistema Medigate

Parte 2.1

cybersecurity, information security & data protection

Cybersecurity, di cosa parliamo?

NIST IR 7298 Revision 2, *Glossary of Key Information Security Terms*

cybersecurity | ˌsībərsiˈkyo͝oritē | :

The ability to protect or defend the use of **cyberspace** from **cyber attacks**.

Or

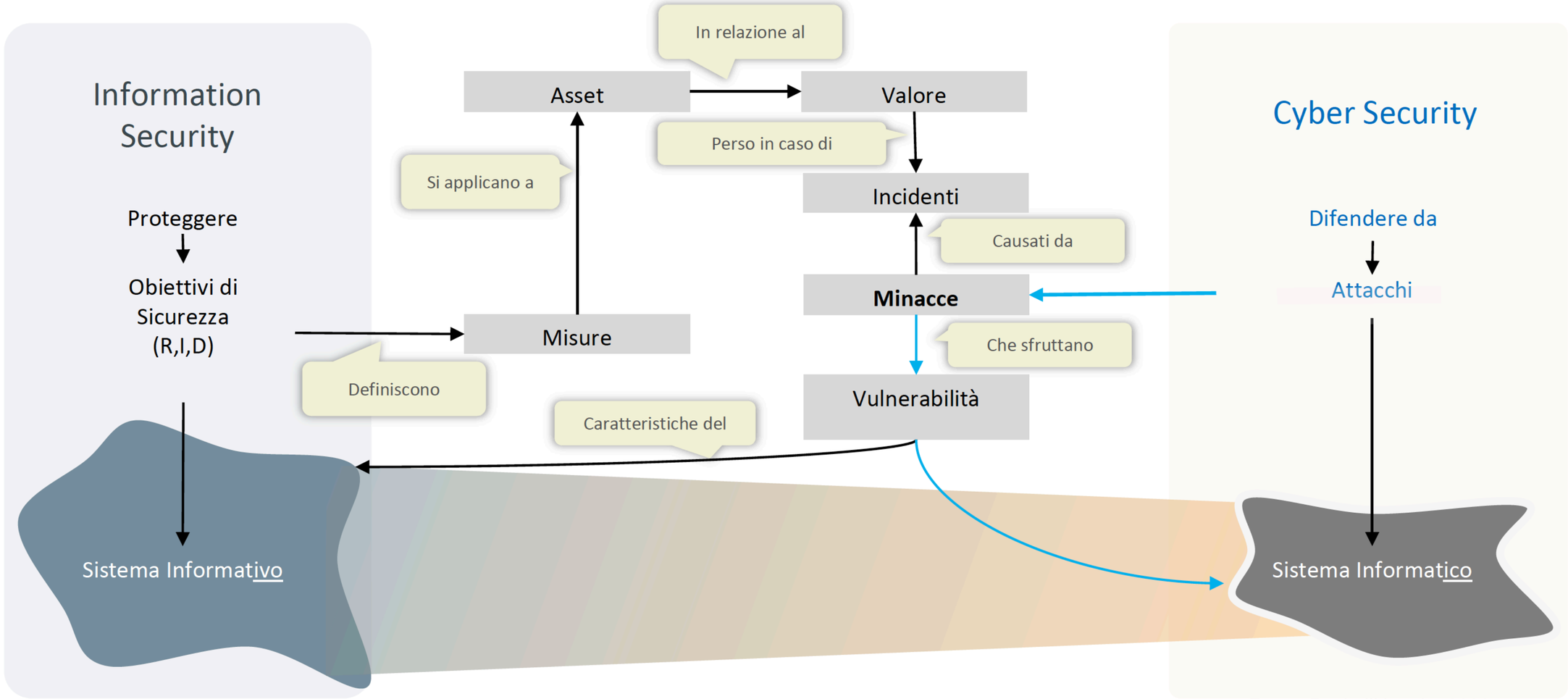
The **process** of protecting information by **preventing**, **detecting**, and **responding** to **attacks**.

Cyberspace:
A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyber Attack:
An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information

Fonte: Bechelli L.; Cyber Risk Management - Webinar CLUSIT 24/01/2020

Cybersecurity vs information security



Fonte: Bechelli L.; cit., 2020

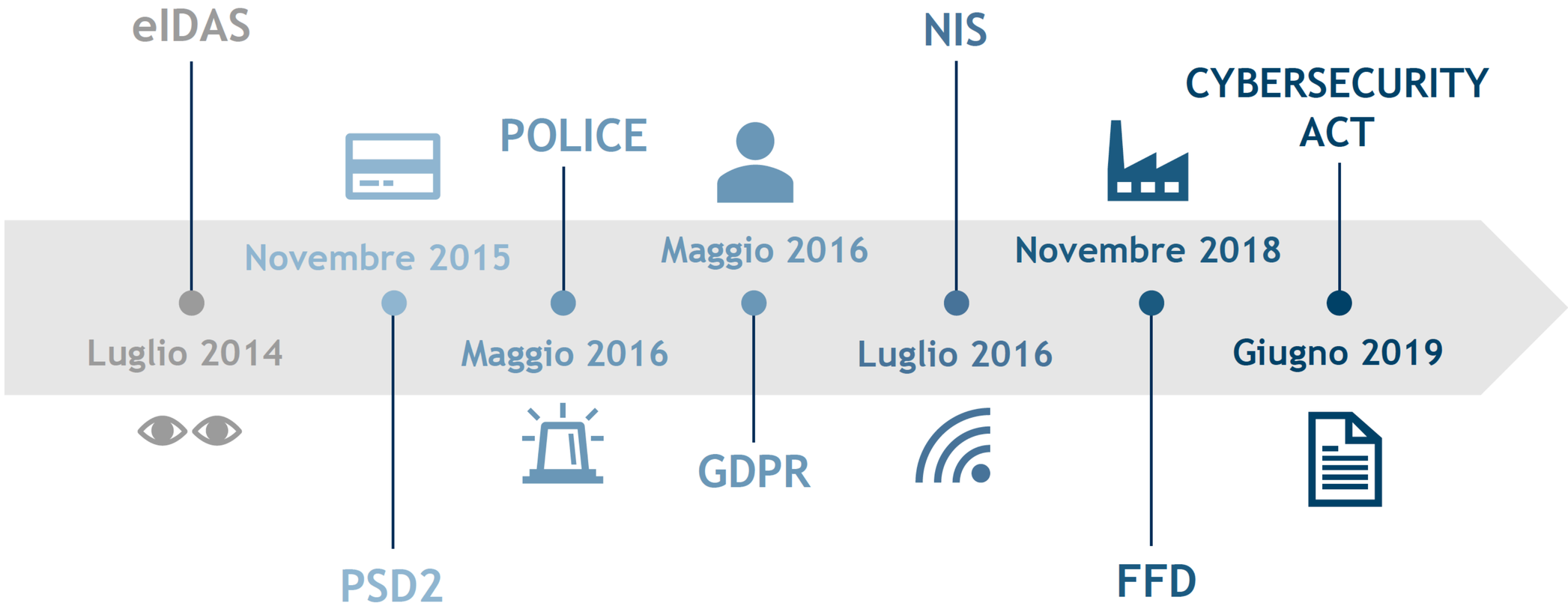
Cybersecurity vs information security

- **Analisi del rischio di sicurezza delle informazioni (information security)**
  - Favorisce la valutazione di rischi inattesi, basati su minacce non previste o prevedibili
  - Con informazioni affidabili può individuare con maggiore efficacia gli ambiti di più elevata criticità

- **Analisi del rischio “cyber”**
  - Focalizzata su eventi certi e gravi, riduce lo sforzo di analisi a favore di iniziative pratiche di attuazione
  - Spostando l’attenzione dalle misure alle minacce, consente più agevolmente di determinare se e quando i controlli in essere siano efficaci rispetto allo scenario di rischio

Fonte: Bechelli L.; cit., 2020

Information security e data protection



Fonte: Antonielli A.; Information security e data protection: il panorama normativo. Webinar Clusit, 2020

Information security e data protection

GDPR	POLICE	NIS	eIDAS	PSD2
Art. 32	**Art. 29**	**Art. 16**	**Art. 19**	**Art. 95**
Misure tecniche e organizzative	Misure tecniche e organizzative	Misure tecniche e organizzative	Misure tecniche e organizzative	Quadro di misure di mitigazione e meccanismi di controllo
Adeguate per garantire un livello di sicurezza adeguato al rischio	Adeguate per garantire un livello di sicurezza adeguato al rischio	Adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi	Appropriate per gestire i rischi legati alla sicurezza dei servizi fiduciari	Adeguati per gestire i rischi operativi e di sicurezza
Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento	Tenuto conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento	Tenuto conto delle conoscenze più aggiornate in materia	Tenuto conto degli ultimi sviluppi tecnologici	–

Fonte: Antonielli A.; cit., 2020

Information security e data protection

GDPR	POLICE	NIS	eIDAS	PSD2
Art. 33/34	Art. 30/31	Art. 16	Art. 19	Art. 96
Violazione dei dati personali	Violazione dei dati personali	Qualsiasi incidente avente un impatto rilevante sulla fornitura di un servizio digitale	Violazioni sicurezza o perdite di integrità con impatto significativo su servizi fiduciari prestati o su dati pers.	Grave incidente operativo o relativo alla sicurezza
Notifica Autorità di controllo competente/interessati*	Notifica Autorità di controllo competente/interessati*	Notifica Autorità competente o CSIRT	Notifica organismo di vigilanza e ad altri organismi interessati//a p. fisiche o giuridiche*//ENISA*	Notifica autorità competente/utenti di servizio di pagamento*
Senza ingiustificato ritardo Entro 72 ore (ove possibile)	Senza ingiustificato ritardo Entro 72 ore (ove possibile)	Senza indebito ritardo	Senza indugio ma in ogni caso entro 24 ore dall'esserne venuti a conoscenza	
Natura violazione, categorie e numero di interessati e di registrazioni dei dati	Natura violazione, categorie e numero di interessati e di registrazioni dei dati	Numero di utenti interessati Durata dell'incidente Diffusione geografica Portata della perturbazione	–	–
Nome e contatto DPO o altro punto di contatto	Nome e contatto DPO o altro punto di contatto	Portata dell'impatto sulle attività economiche e sociali	–	–
Probabili conseguenze	Probabili conseguenze		–	–
Misure adottate o proposte per rimediare/attenuare	Misure adottate o proposte per rimediare/attenuare		–	–

Fonte: Antonielli A.; cit., 2020

Cybersecurity

- Individuazione delle minacce - possono avere conseguenze - attuo misure - rilevo e mitigo gli effetti negativi
- Proprio “perimetro”
- Approccio dinamico, pratico, basato più sulle tecnologie
- Molte minacce agiscono fuori dall’ambito del nostro controllo (data breach dei fornitori…)
- Ci sono o possono essere soluzioni “as a service”
- Da analisi (information security) ad azione (“cosa non ho fatto” piuttosto che “cosa potrebbe accadermi”)
- Devo fare delle scelte per difendermi da minacce (possibilmente rese quanto più) prevedibili

Cybersecurity - cosa cambia nell'approccio

Approccio tradizionale (risk management ISO 27005):

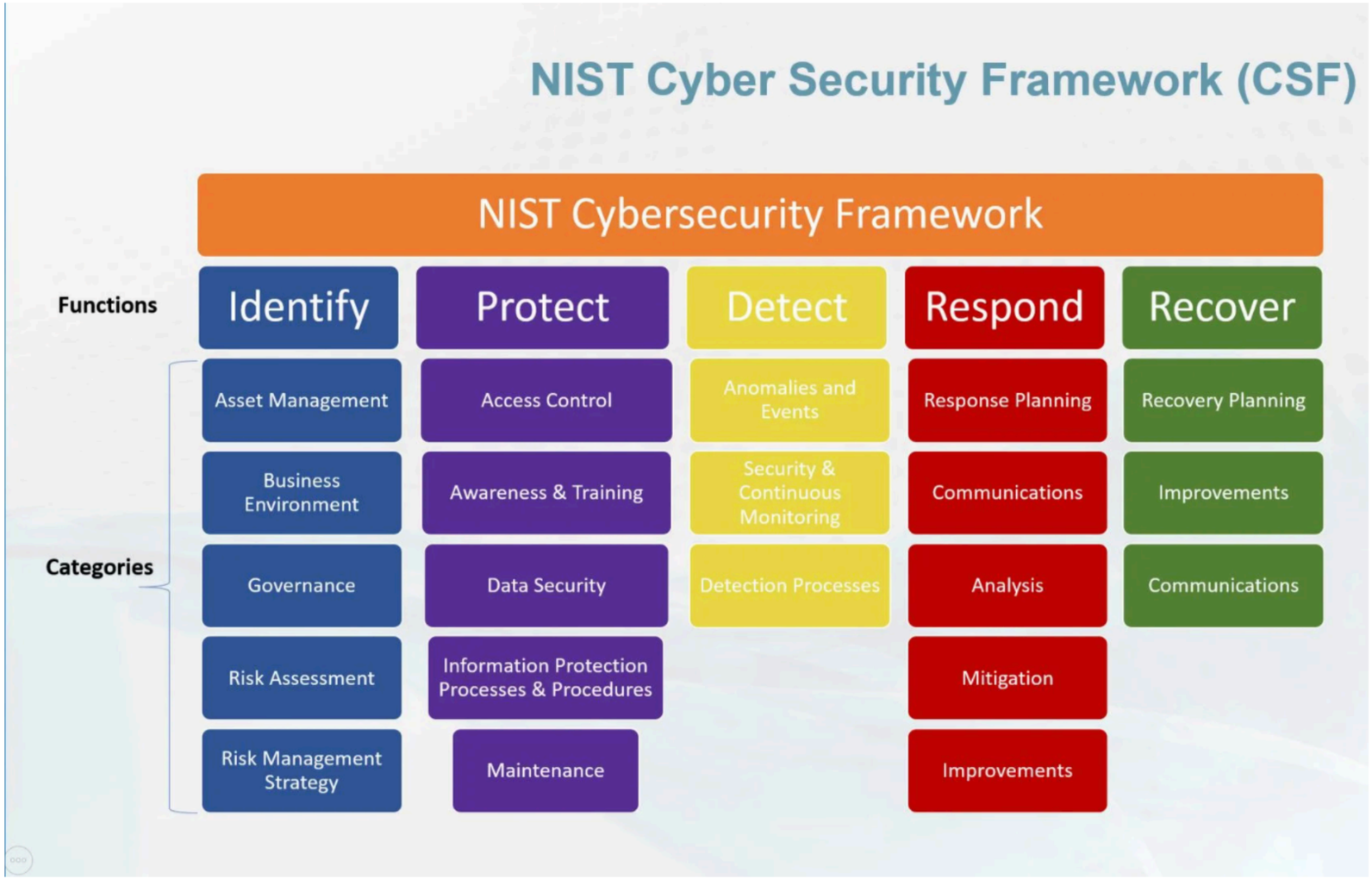
- L'analisi parte dal contesto, e sulla base delle minacce identificate e **giudicate rilevanti** nel contesto (in relazione a impatti e probabilità, influenzate dai controlli in essere), si definiscono le azioni

Approccio «cyber»:

- L'analisi parte dalle minacce **applicabili.** Con riguardo alle *scoperture*, si definiscono le azioni prioritizzate sulla base del valore degli asset impattati (o della **gravità che una violazione avrebbe sull'intero contesto**)

Fonte: Bechelli L.; cit., 2020

Cybersecurity framework



Cybersecurity framework

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

FUNCTION	CATEGORY	SUBCATEGORY
IDENTIFY (ID)	**Asset Management (ID.AM)**: I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**DP-ID.AM-7:** Sono definiti e resi noti ruoli e responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)
		DP-ID.AM-8: I trattamenti di dati personali sono identificati e catalogati
	Risk Assessment (ID.RA): L'impresa comprende il rischio di cybersecurity inerente all'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**DP-ID.RA-7:** Viene effettuata una valutazione di impatto sulla protezione dei dati personali
	Data Management (DP-ID.DM): i dati personali sono trattati attraverso processi definiti, in coerenza con le normative di riferimento.	**DP-ID.DM-1:** Il ciclo di vita dei dati è definito e documentato
		DP-ID.DM-2: Sono definiti, implementati e documentati i processi riguardanti l'informazione dell'interessato in merito al trattamento dei dati
		DP-ID.DM-3: Sono definiti, implementati e documentati i processi di raccolta e revoca del consenso dell'interessato al trattamento di dati
		DP-ID.DM-4: Sono definiti, implementati e documentati i processi per l'esercizio dei diritti (accesso, rettifica, cancellazione, ecc.) dell'interessato
		DP-ID.DM-5: Sono definiti, implementati e documentati i processi di trasferimento dei dati in ambito internazionale
RESPOND (RS)	**Communications (RS.CO):** Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	**DP-RS.CO-6:** Gli incidenti che si configurano come violazioni di dati personali sono documentati ed eventualmente vengono informati le autorità di riferimento e gli interessati

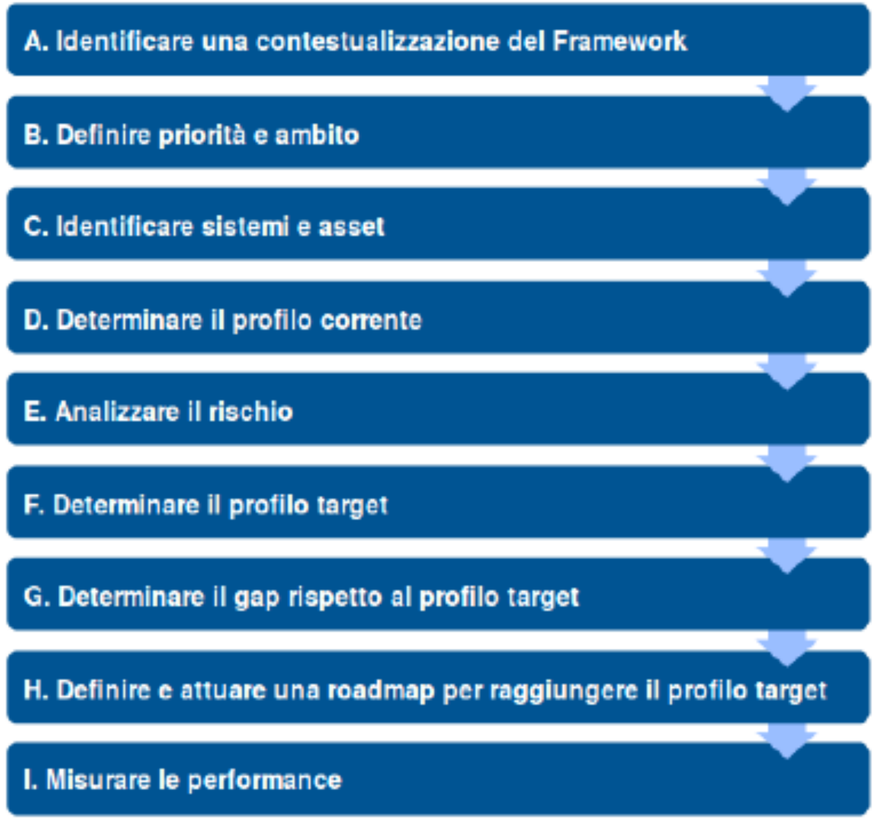
Cybersecurity framework

Identify	Protect	Detect	Respond	Recover
La function IDENTIFY è legata alla comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati. Tale comprensione permette a un'organizzazione di definire risorse e investimenti in linea con la strategia di gestione del rischio e con gli obiettivi aziendali. Le category all'interno di questa function sono: Asset Management, Business Environment; Governance, Risk Assessment, Risk Management Strategy, Supply Chain Risk Management e Data Management.	La function PROTECT è associata all'implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica. Le category all'interno di questa function sono: Identity Management, Authentication and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, Protective Technology.	La function DETECT è associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica. Le category all'interno di questa function sono: Anomalies and Events, Security Continuous Monitoring, Detection Processes.	La function RESPOND è associata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato. L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica. Le category all'interno di questa function sono: Response Planning, Communications, Analysis, Mitigation, Improvements.	La function RECOVER è associata alla definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente. L'obiettivo è garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle business operations. Le category all'interno di questa function sono: Recovery Planning, Improvements, Communications.

Dati personali, tier, profili, livelli di priorità…

Cybersecurity framework

Applicazione del framework



Controlli essenziali

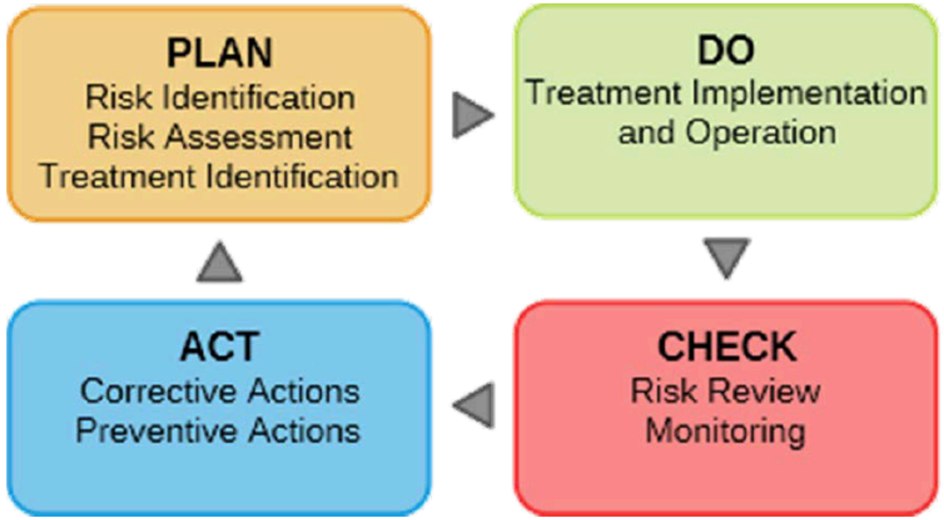
Inventario dispositivi e software
Governance
Protezione da malware
Gestione password e account
Formazione e consapevolezza
Protezione dei dati
Protezione delle reti
Prevenzione e mitigazione

Cybersecurity - AgID

Il Risk Management si compone di quattro fasi:

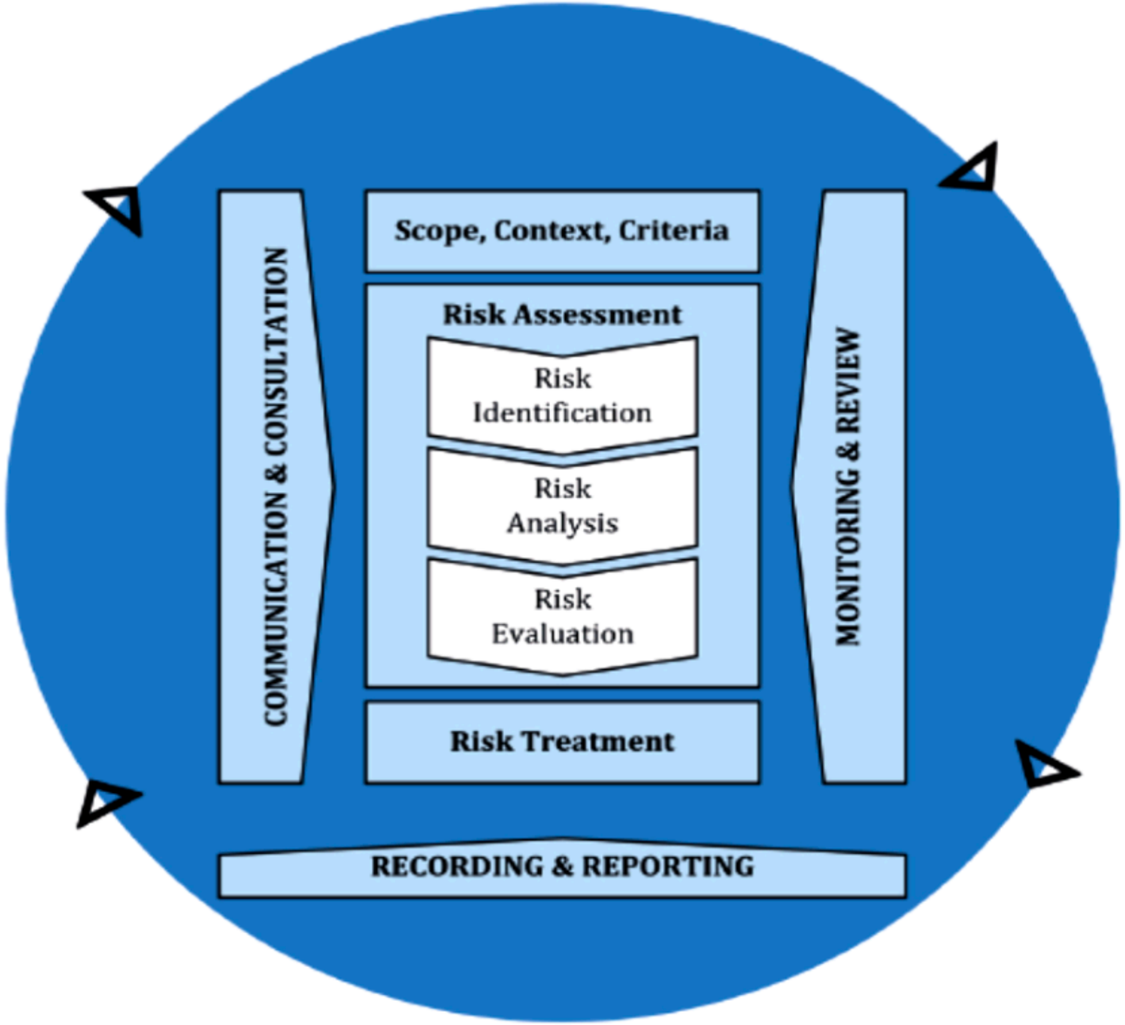
- **Identificazione** in questa fase si cerca di determinare le possibili fonti di Rischio e individuare quegli eventi che potrebbe causare l'insorgere di Pericoli
- **Valutazione qualitativa e quantitativa** consiste nel determinare impatto e probabilità di un Pericolo e nell'assegnare, in modo qualitativo o quantitativo, un ordine di priorità (o, se si preferisce, un indice di pericolosità) dei Rischi
- **Pianificazione** in questa fase si passa a identificare l'insieme delle contromisure applicabili ad un certo rischio. Si fa l'analisi costi/benefici di ognuna di esse e si passa a selezionare quelle da applicare
- **Controllo** anche dopo che sono state poste in essere le contromisure, bisogna continuare a monitorare i rischi per capire se le contromisure stanno effettivamente funzionando e valutare l'insorgere di nuovi rischi

L'output di ognuna delle 4 fasi confluisce nel Piano del Rischio (Risk Plan) complessivo.



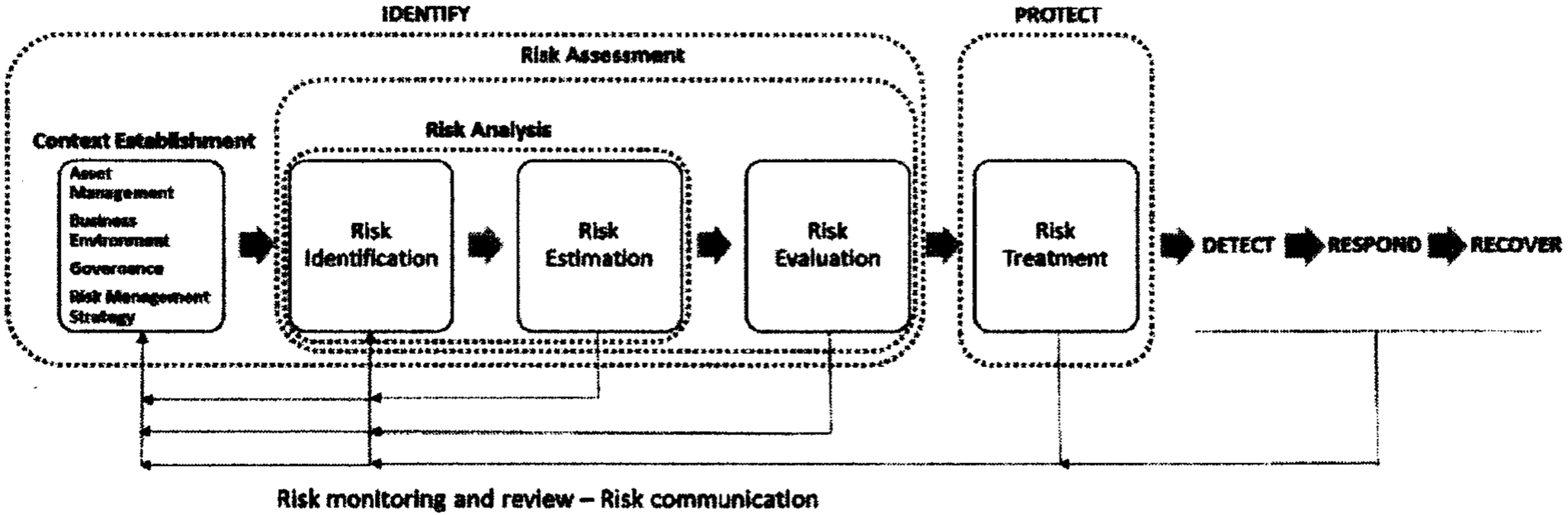
Fonte: Sinibaldi A.;
La sicurezza informatica nella pubblica amministrazione - AgID corso pilota per RTD - 2020

Cybersecurity - NIST e ISO 14971



Cybersecurity - NIST e ISO 14971

Processo di gestione dei rischi



Cybersecurity e DM

Fonte: Pascolo P.;
Il sistema informativo e la sicurezza informatica - Corso La sicurezza informatica dei DM - IRCCS “Burlo Garofolo” 2019

Cybersecurity e DM

- Fatta l’analisi e la rilevazione dei rischi viene il momento di mitigare il rischio legato ad aspetti tecnici, tecnologici e organizzativi dei DM attraverso l’utilizzo di sistemi, controlli, misure, policies, strumenti, tecnologie…
- All’atto pratico:
  - Identifico minacce e vulnerabilità su quelli che sono i diversi layer dei modelli tcp/ip oppure iso/osi di un determinato DM
  - Utilizzo sistemi e tecnologie per fare queste analisi e approntare un piano per la riduzione del rischio (nmap, vulnerability scanner, AV, firewall, nac, wireshark, siem, ecc…)
  - Tutta l’azione successiva, in un modello super semplificato, è quella di ridurre probabilità (P) e impatto (I) delle minacce aumentando l’efficacia (E) dei controlli

R = P x I x E

Cybersecurity e DM

- **Medigate**
  - Permette una **identificazione** degli asset collegati alla rete (identify)
  - Effettua una **valutazione del rischi** basata su tre parametri: network, severity e device vulnerability (protect)
  - Dà **indicazioni** su vulnerabilità, porte, servizi, utilizzo del DM (detect)
  - Permette di configurare la rete (VLAN, reti pubbliche e private, ecc) e di **integrare** una serie di sistemi sia lato vendor medicali sia IT
  - MDS^2

- **EDGE IPS - TrendMicro**
  - Evoluzione di un device come l'Extreme IoT Defender: integra un IPS
  - Posso lavorare sulle regole - come per un firewall layer 3-4
  - Ho la versatilità di un IPS su cui posso, una volta identificate le vulnerabilità, intervenire per evitare lo sfruttamento della vulnerabilità stessa (respond)

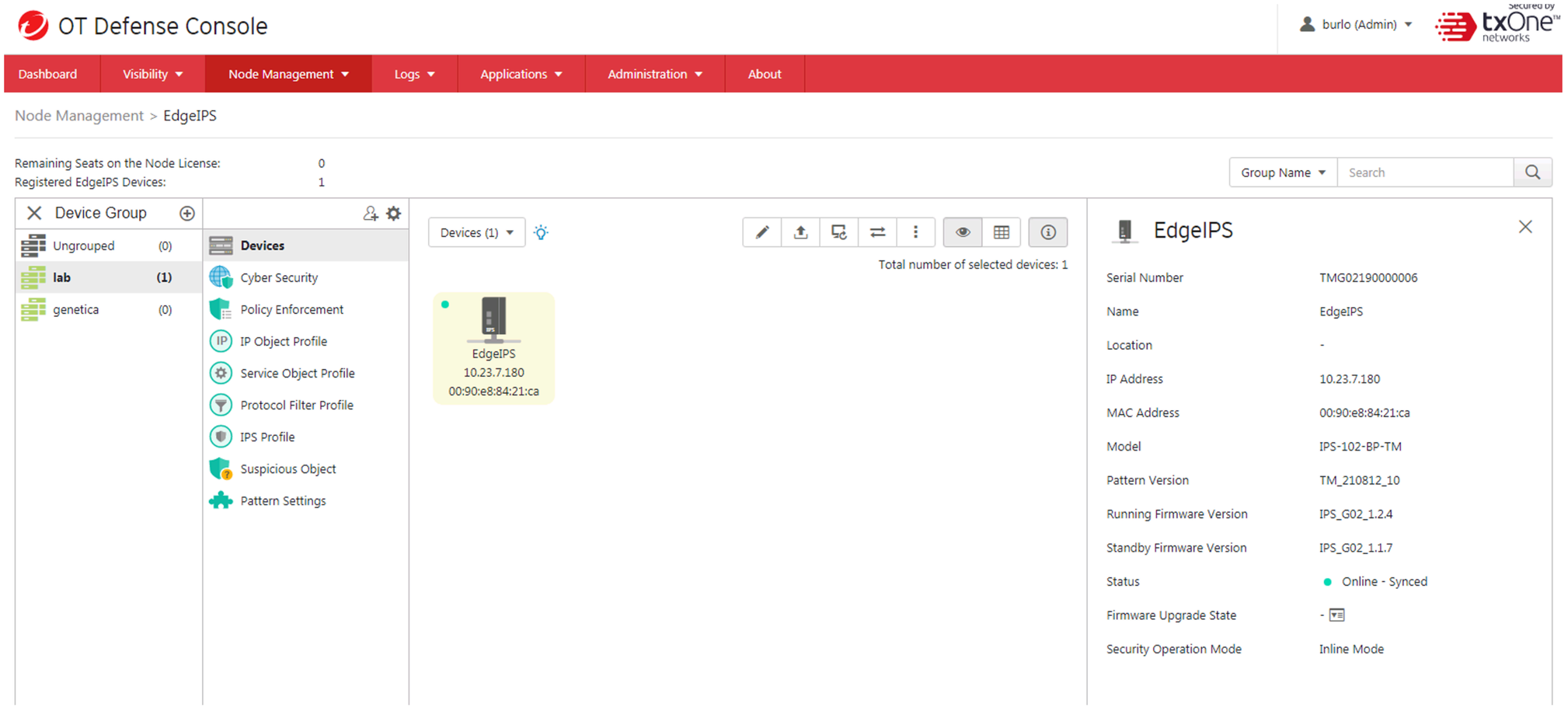
EDGE IPS

TXOne Edge Solutions

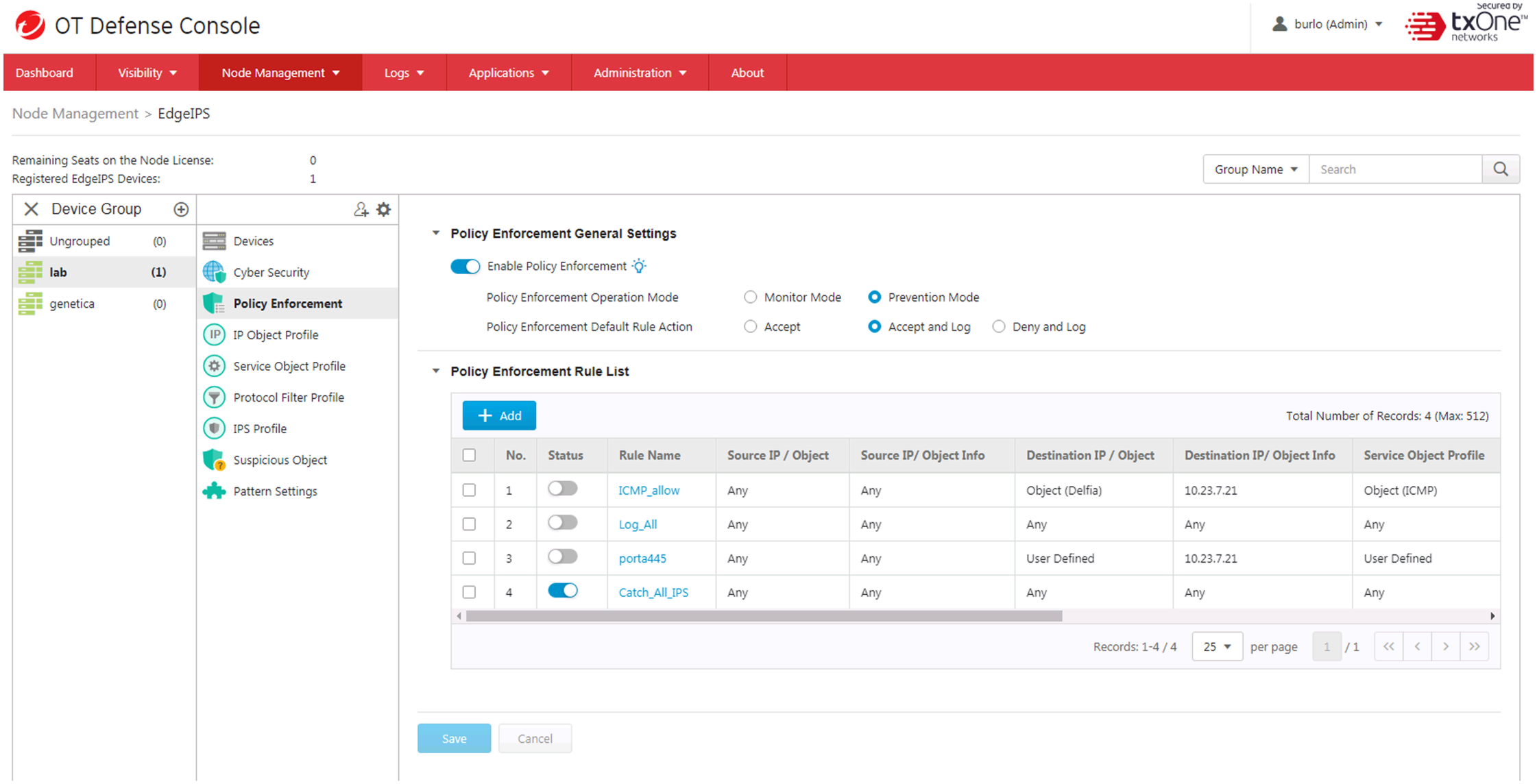
EdgeIPS (NG-Industrial IPS)

- Network visibility
- OT Protocol Filter
- Virtual Patch
- TXODI inside
- Dual Power Input
- Hardware Bypass
- Network Segmentation
- NAT - Firewall

OT Defense Console



OT Defense Console



Risultato preliminare - Utilizzo dell'EDGE IPS per la mitigazione del rischio

Soltanto utilizzando la funzione IPS - analisi condotta con VS Nessus Professional 8.15.1

1	1	13	1	44
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 60

SEVERITY	CVSS V2.0	PLUGIN	NAME
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure

10.23.7.21 4

0	1	11	1	36
CRITICAL	HIGH	MEDIUM	LOW	INFO

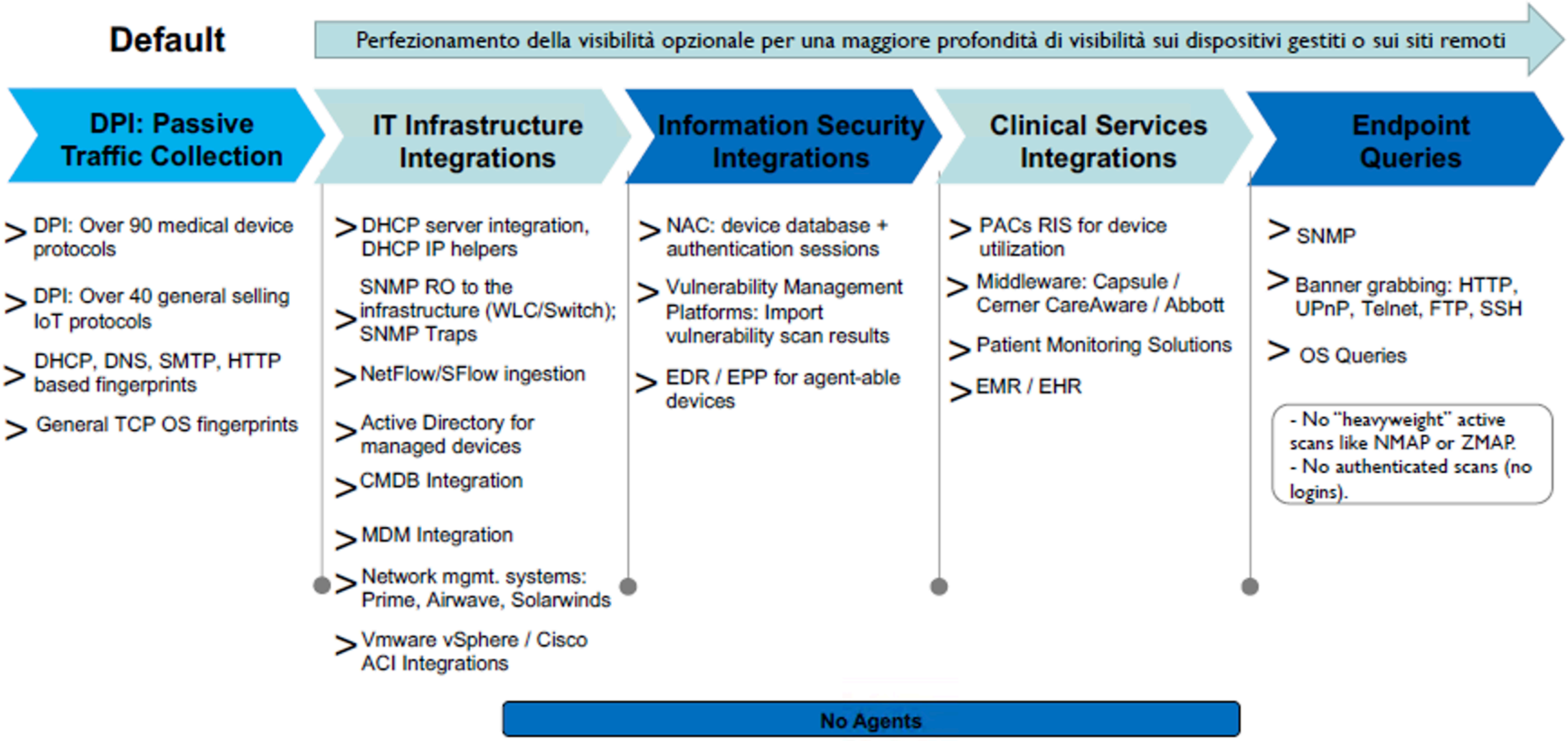
Vulnerabilities — Total: 49

SEVERITY	CVSS V2.0	PLUGIN	NAME
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	132634	Deprecated SSLv2 Connection Attempts

Parte 2.2

Demo sistema Medigate

Medigate


Default
Perfezionamento della visibilità opzionale per una maggiore profondità di visibilità sui dispositivi gestiti o sui siti remoti
DPI: Passive Traffic Collection
IT Infrastructure Integrations
Information Security Integrations
Clinical Services Integrations
Endpoint Queries
DPI: Over 90 medical device protocols
DPI: Over 40 general selling IoT protocols
DHCP, DNS, SMTP, HTTP based fingerprints
General TCP OS fingerprints
DHCP server integration, DHCP IP helpers
SNMP RO to the infrastructure (WLC/Switch); SNMP Traps
NetFlow/SFlow ingestion
Active Directory for managed devices
CMDB Integration
MDM Integration
Network mgmt. systems: Prime, Airwave, Solarwinds
Vmware vSphere / Cisco ACI Integrations
NAC: device database + authentication sessions
Vulnerability Management Platforms: Import vulnerability scan results
EDR / EPP for agent-able devices
PACs RIS for device utilization
Middleware: Capsule / Cerner CareAware / Abbott
Patient Monitoring Solutions
EMR / EHR
SNMP
Banner grabbing: HTTP, UPnP, Telnet, FTP, SSH
OS Queries
- No "heavyweight" active scans like NMAP or ZMAP.
- No authenticated scans (no logins).
No Agents

MEDIGATE

mead
YOUR DIGITAL INTEGRATOR

DEMO