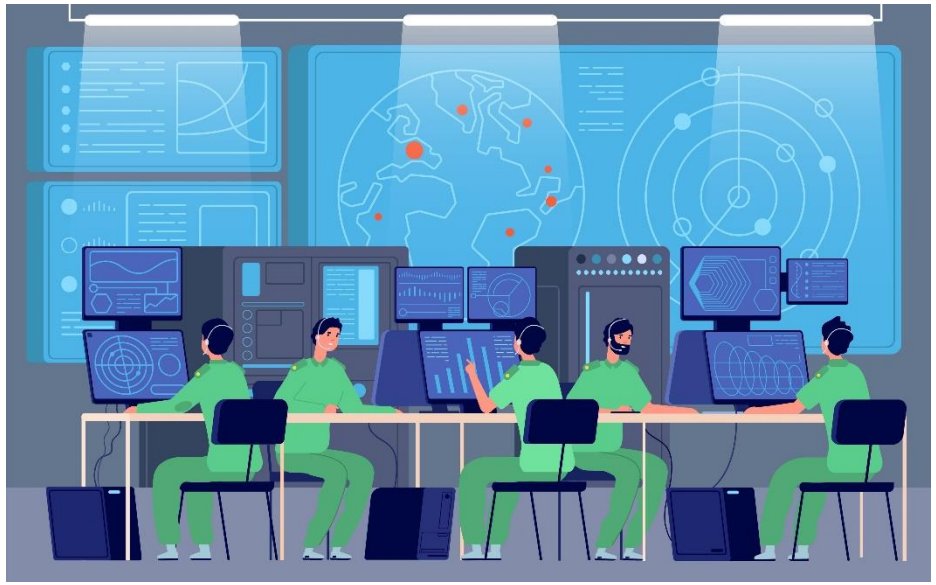
mead
YOUR DIGITAL INTEGRATOR

ADVANCED HEALTHCARE PROTECTION

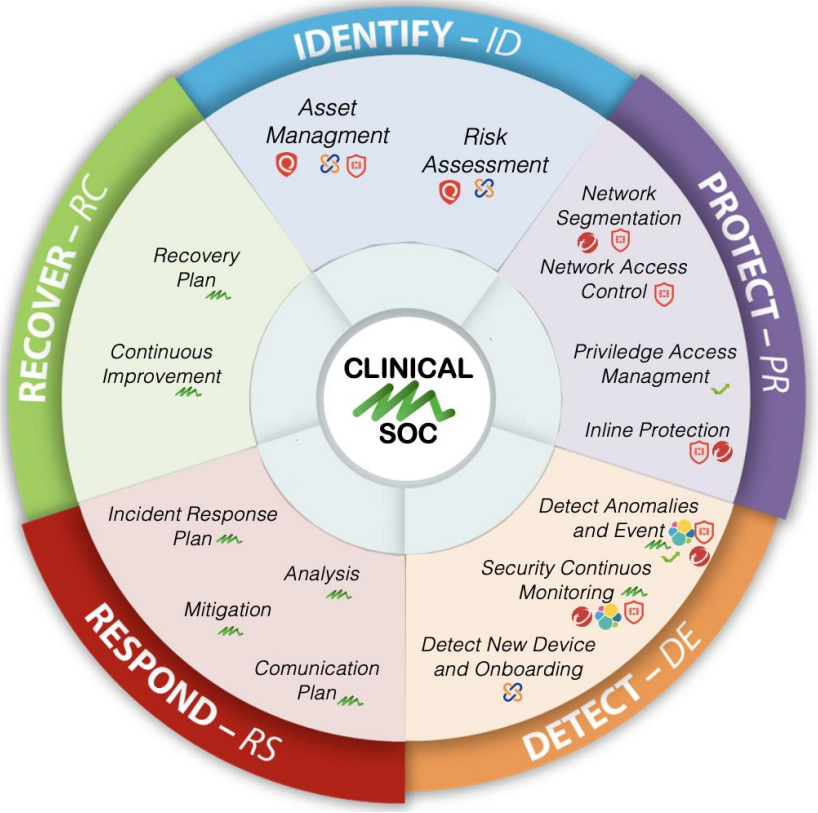
ROBERTO FANTINI
r.fantini@meadinformatica.it
+39.329.2638550

ADVANCED HEALTHCARE PROTECTION

CYBER SECURITY CONTROL ROOM

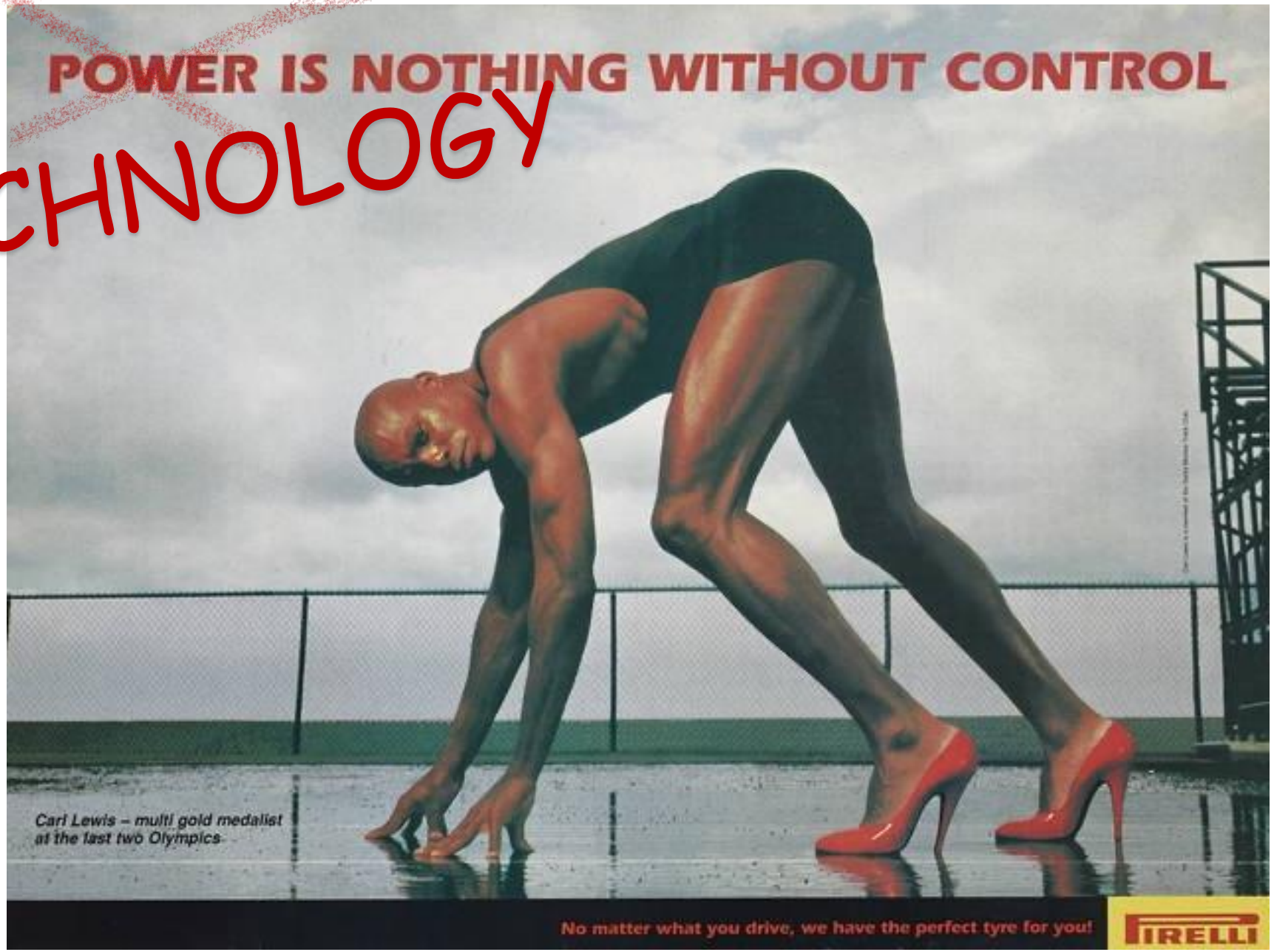


CLINICAL SOC



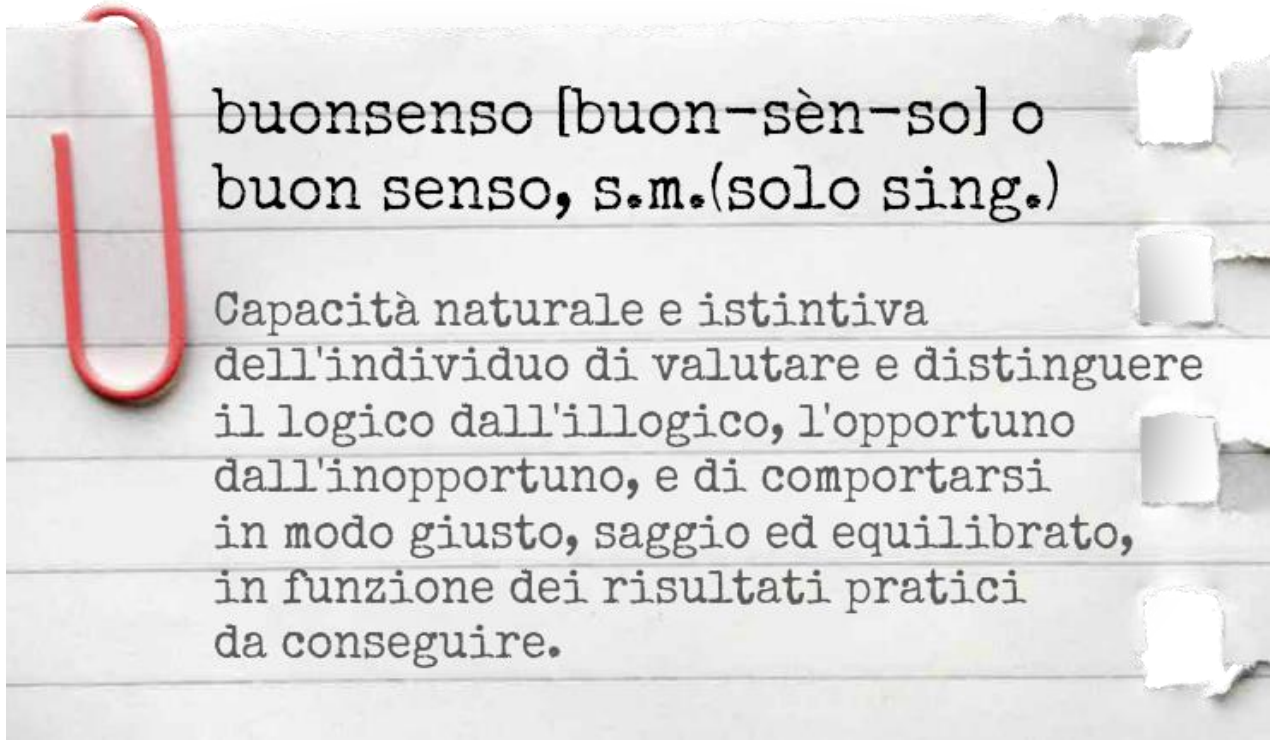
UNICO PUNTO DI GOVERNANCE PER LA GESTIONE OLISTICA DELLA INFRASTRUTTURA IT - IoMT

TECHNOLOGY



campagna pubblicitaria Pirelli del 1994 dall'agenzia Young&Rubicam

LINEE GUIDA


buonsenso [buon-sèn-so] o
buon senso, s.m.(solo sing.)
Capacità naturale e istintiva
dell'individuo di valutare e distinguere
il logico dall'illogico, l'opportuno
dall'inopportuno, e di comportarsi
in modo giusto, saggio ed equilibrato,
in funzione dei risultati pratici
da conseguire.

CYBER SECURITY CONTROL ROOM

Servizio Gestito di raccolta e correlazione delle informazioni da qualsiasi sorgente al fine di identificare gli incident di sicurezza

- Servizio Gestito
- Vendor Independent
- ML/AI Algorithm
- Intelligence Italiana
- Modularità
- Scalabilità
- Proattività

Perimetro Interno
Qualsiasi infrastruttura esistente del cliente, campus, server, cloud privato

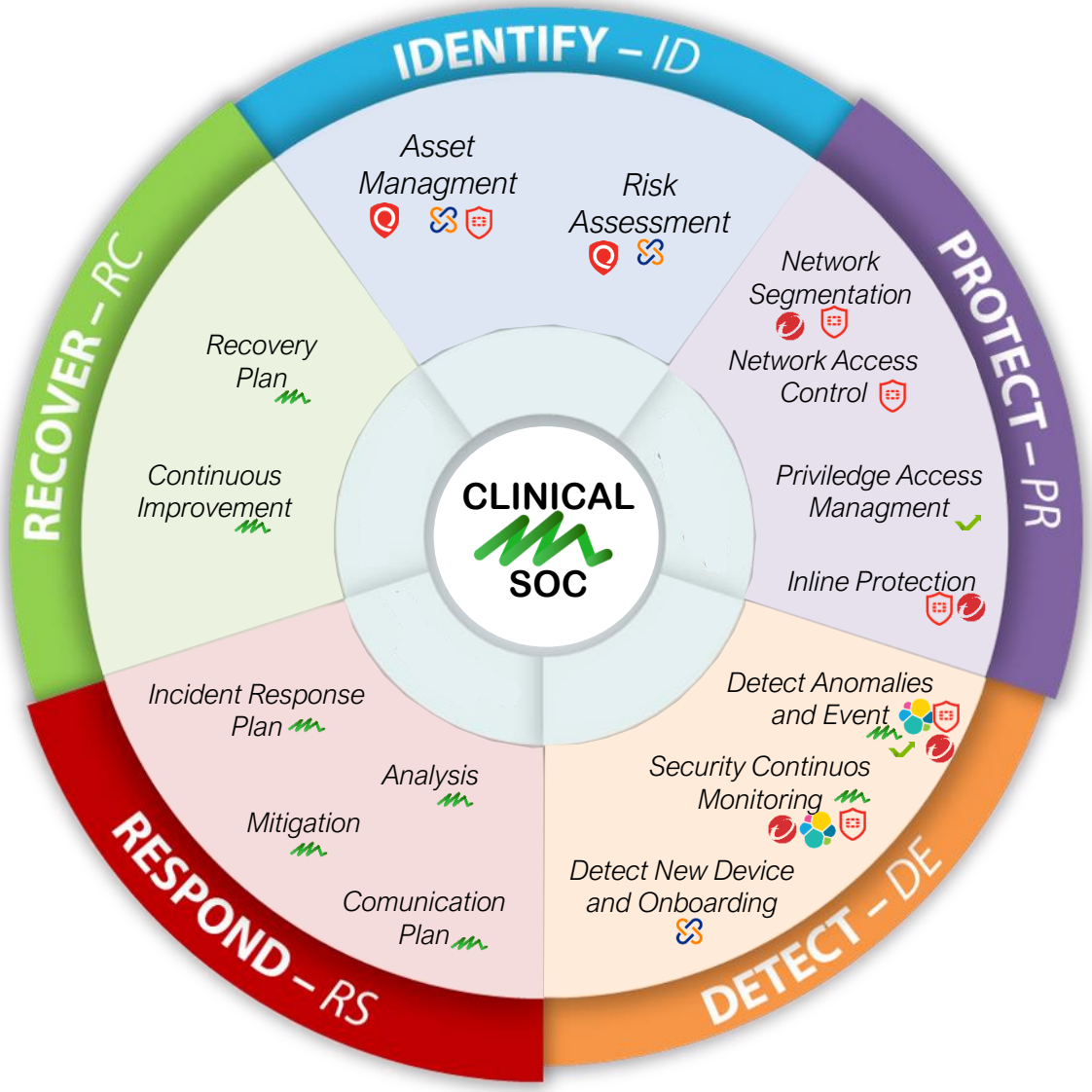
Perimetro Esterno
Cloud Pubblico, esposizione al rischio dei siti e servizi esposti al pubblico

Intelligence
Correlazione delle informazioni sulla base dello scenario italiano

Dark web
Analisi dell'esposizione dei dati aziendali nel sommerso

CLINICAL SOC

Un servizio dedicato alle aziende sanitarie per la gestione del rischio informatico in ambito medicale, tramite un team di analisti specializzati disponibili H24, che supportano sia l'IT che l'Ingegneria Clinica nella gestione delle problematiche di cybersecurity



Perimetro OT
Qualsiasi infrastruttura OT esistente

Non invasivo
Non vengono effettuate scansioni ma si analizza passivamente il traffico

Topologia
Crea automaticamente la topologia e le interazioni di traffico interne ed esterne

Asset Inventory
Crea un asset inventory di tutti i device OT collegati alla rete.

ASSET MANAGEMENT

IDENTIFY

Bone Densitometry
1 Device

1 Model — 1 High Risk

C-Arm
1 Device

1 Model — 1 High Risk

Computed Radiography
2 Devices

1 Model — 2 High Risk

Computed Tomography
9 Devices

6 Models — 9 High Risk

Defibrillator
16 Devices

1 Model — 16 High Risk

Glucose Meter
1 Device

1 Model — 1 High Risk

Imaging Workstation
18 Devices

2 Models — 18 High Risk

MRI
4 Devices

2 Models — 4 High Risk

Medical Device Integrator
1 Device

1 Model — 1 High Risk

Medication Dispensing System
108 Devices

2 Models — 108 High Risk

Patient Monitor
2 Devices

1 Model — 2 High Risk

Robotic Surgery System
2 Devices

2 Models — 2 High Risk

ASSET MANAGEMENT

IDENTIFY

RISK ASSESSMENT

IDENTIFY

Regolamento Europeo sui dispositivi medici (MDR)

Risk Score Distribution

%	Devices	Risk Score
30.4%	17	Critical
25.0%	14	High
39.3%	22	Medium
3.6%	2	Low
1.8%	1	Very Low

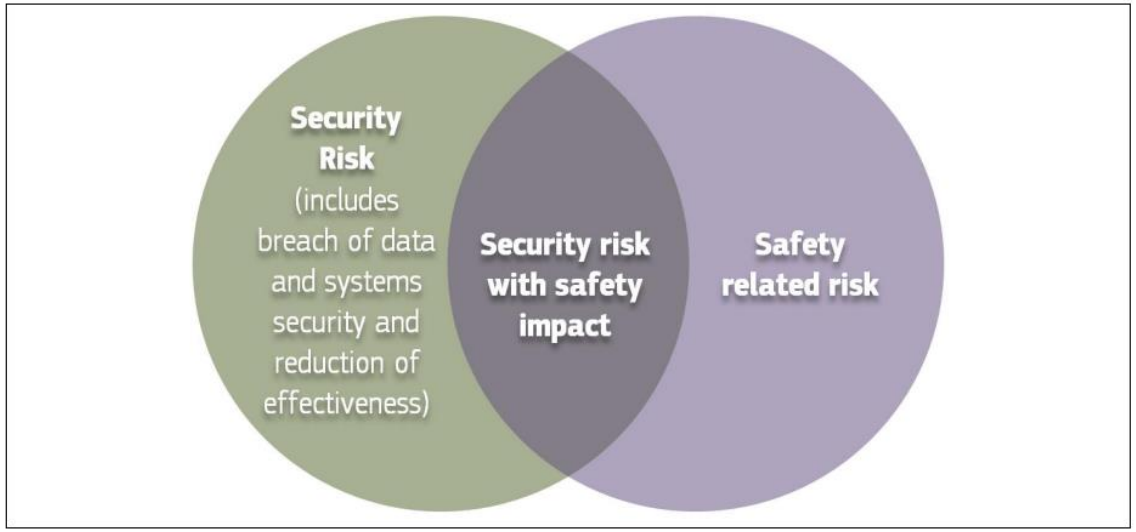
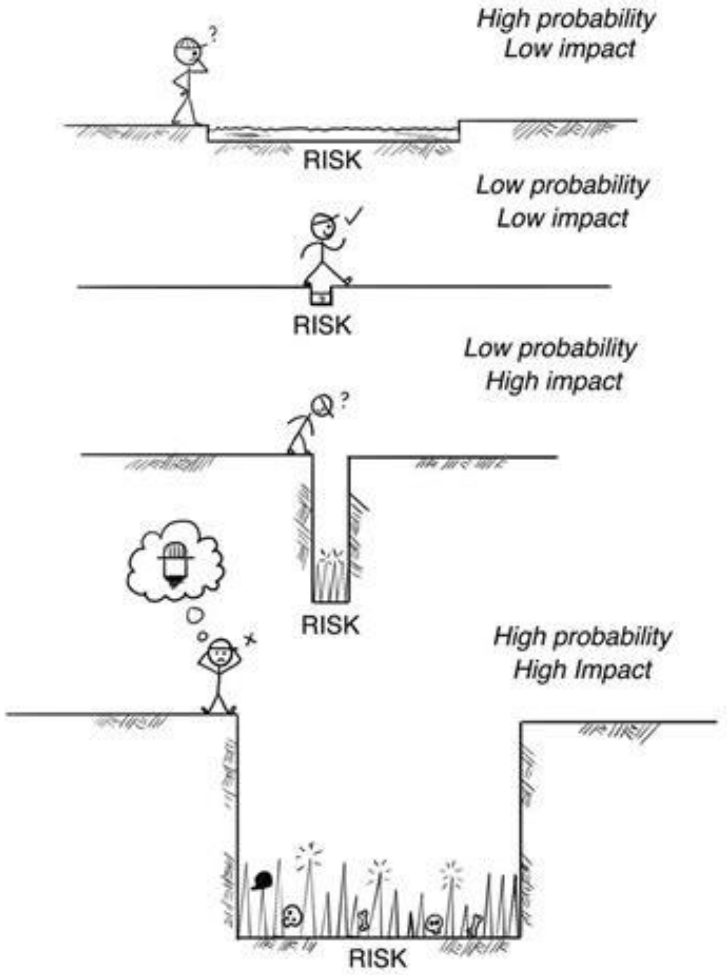


Figure 3: Cybersecurity measures may cause safety impacts

RISK ASSESSMENT



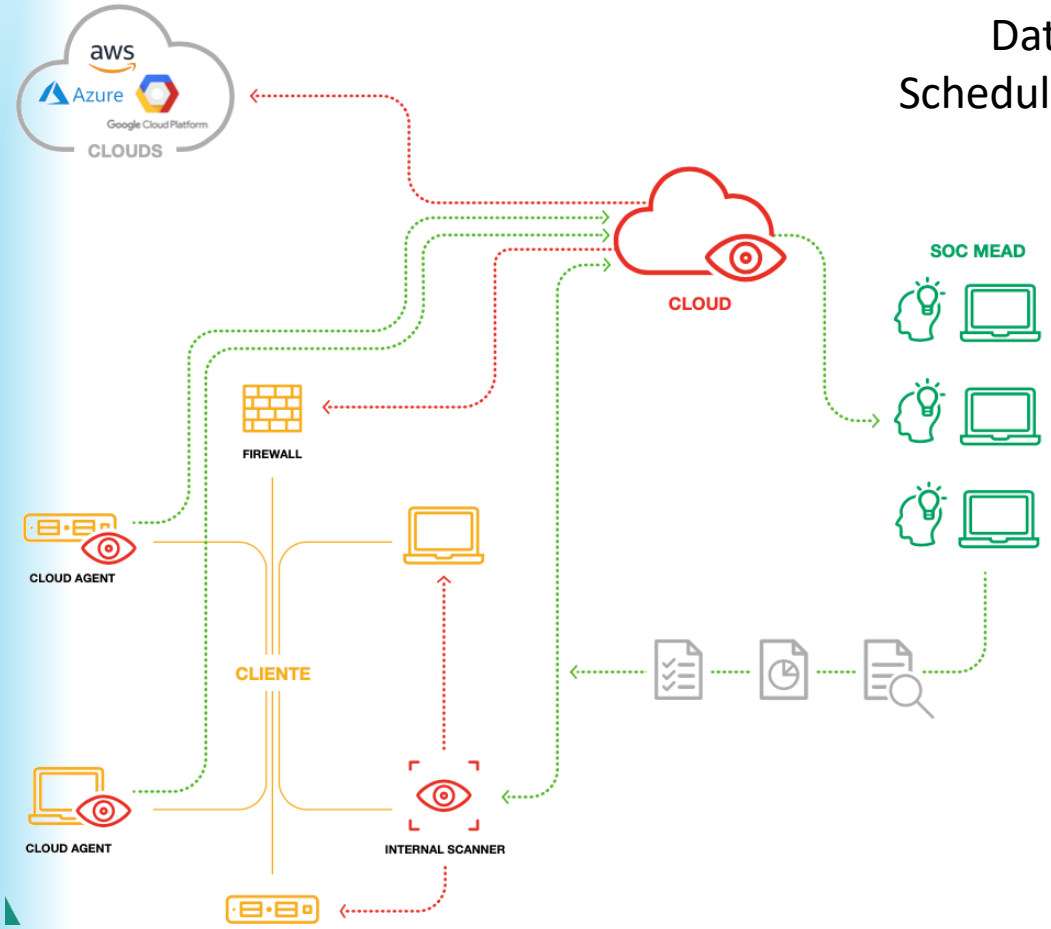
Probability vs. Severity Distribution

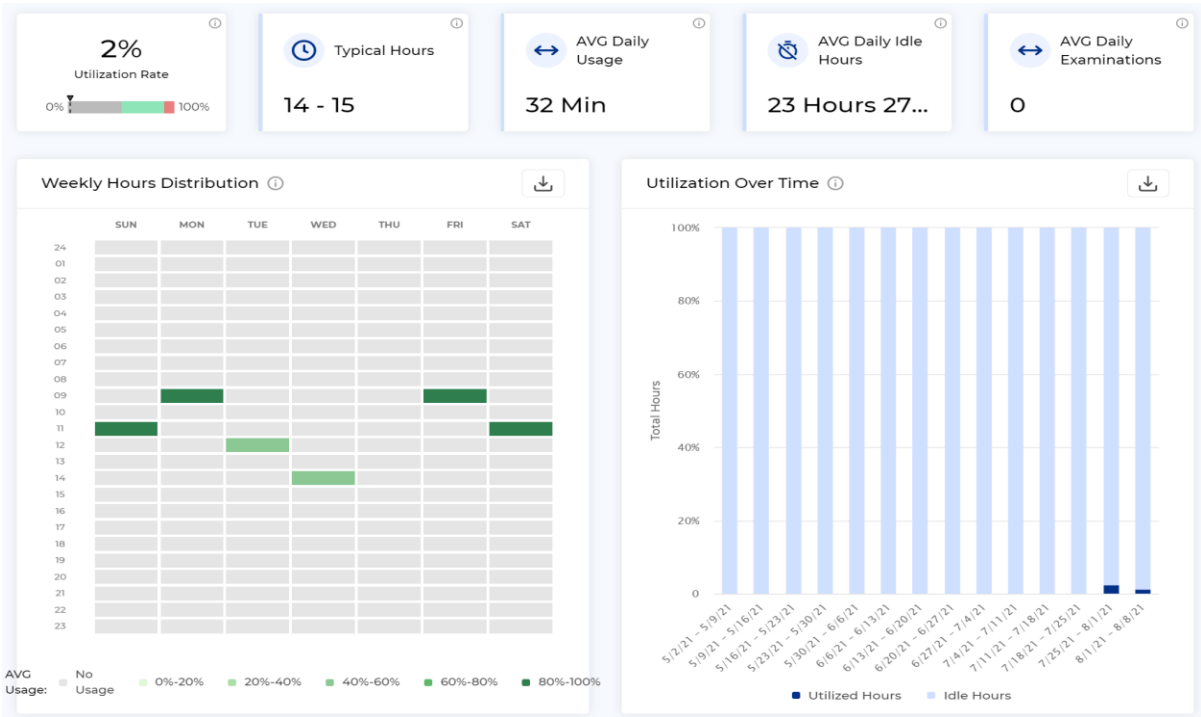
Probability \ Severity	Very Low	Low	Medium	High	Critical
Very Low	0	0	0	1	0
Low	0	0	0	0	10
Medium	1	1	7	4	2
High	0	0	2	11	5
Critical	0	1	1	10	0

IDENTIFY

VULNERABILITY MANAGEMENT

Comunicazione bilaterale tra le informazioni degli assett e delle vulnerabilità
Data Enrichement, sulle informazioni in merito alle vulnerabilità.
Schedulazione delle scansioni attive in momenti di non utilizzo dei device.





IDENTIFY

NETWORK SEGMENTATION

PROTECT

ENFORCE POLICIES

Implement policies that ensure devices communicate as intended and as required for clinical processes.

GAIN VISIBILITY

Identify all connected devices and their configuration, location and owners.

DESIGN POLICIES

Create policies that actively profiling endpoint to identify the type of device and how it should behave on the network.

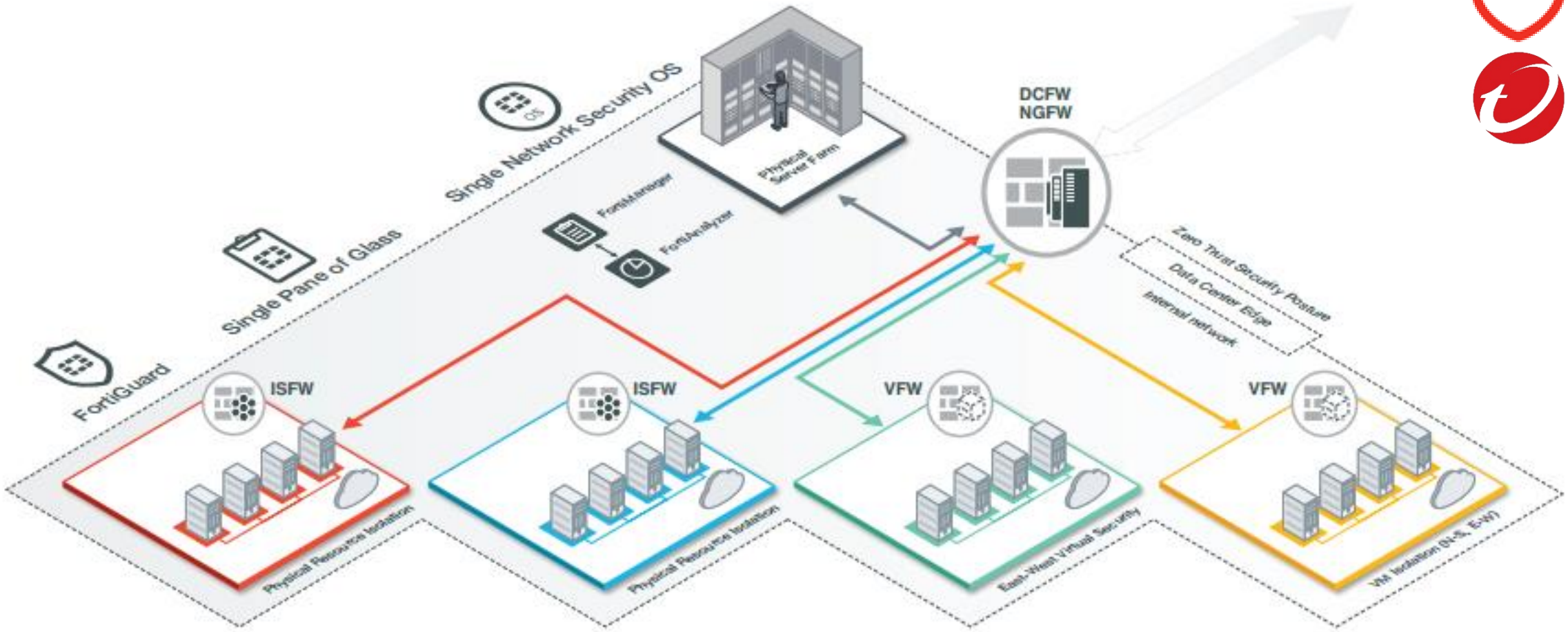
DEFINE STRATEGY

Determine your strategy based on data sensitivity, location and criticality and place.

BUILD DEVICE PROFILES

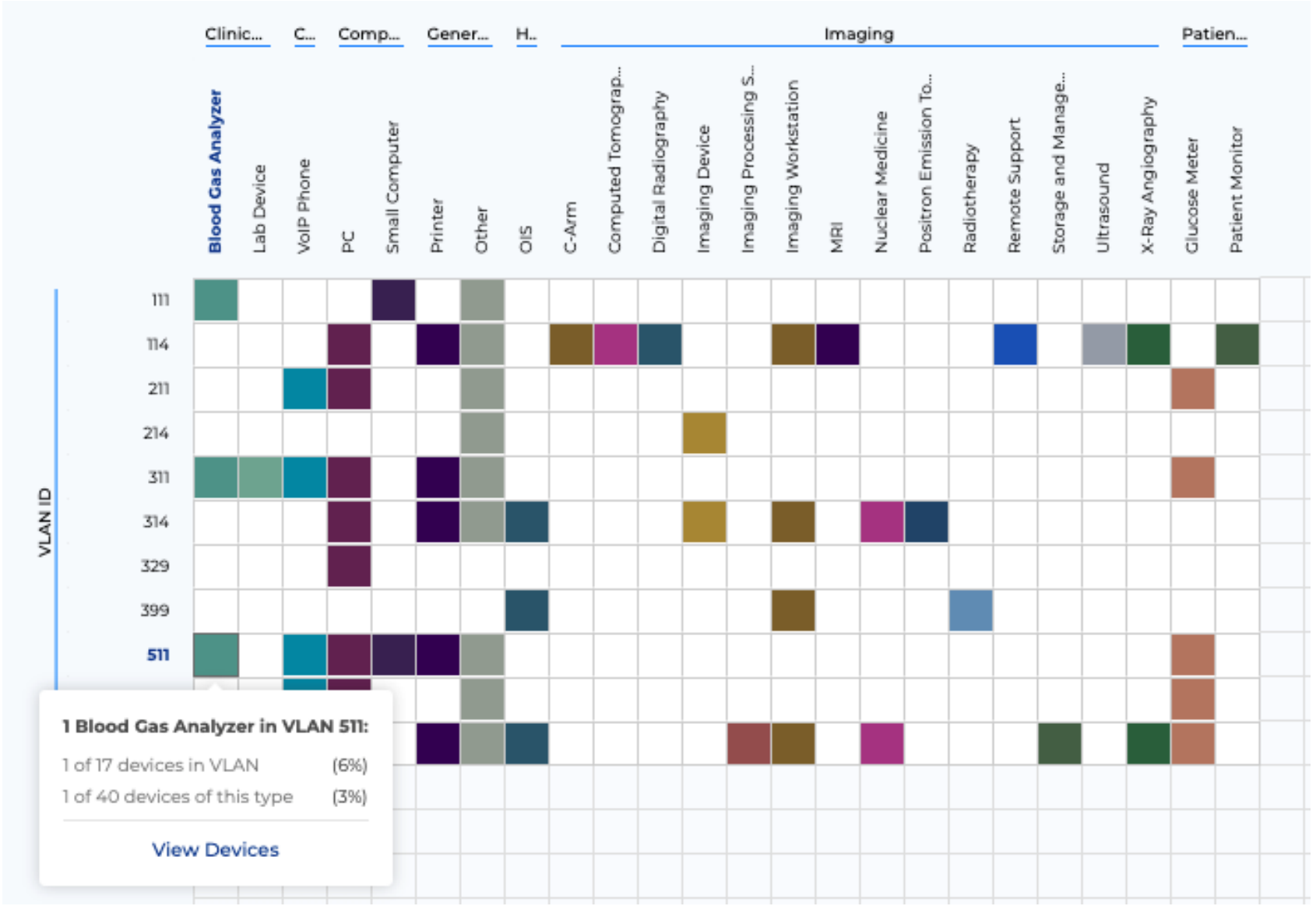
Study device communication protocols and manufacturer-intended workflows to define approved destinations, protocols, and ports for each device or cluster of devices.

NETWORK SEGMENTATION



PROTECT

NETWORK SEGMENTATION

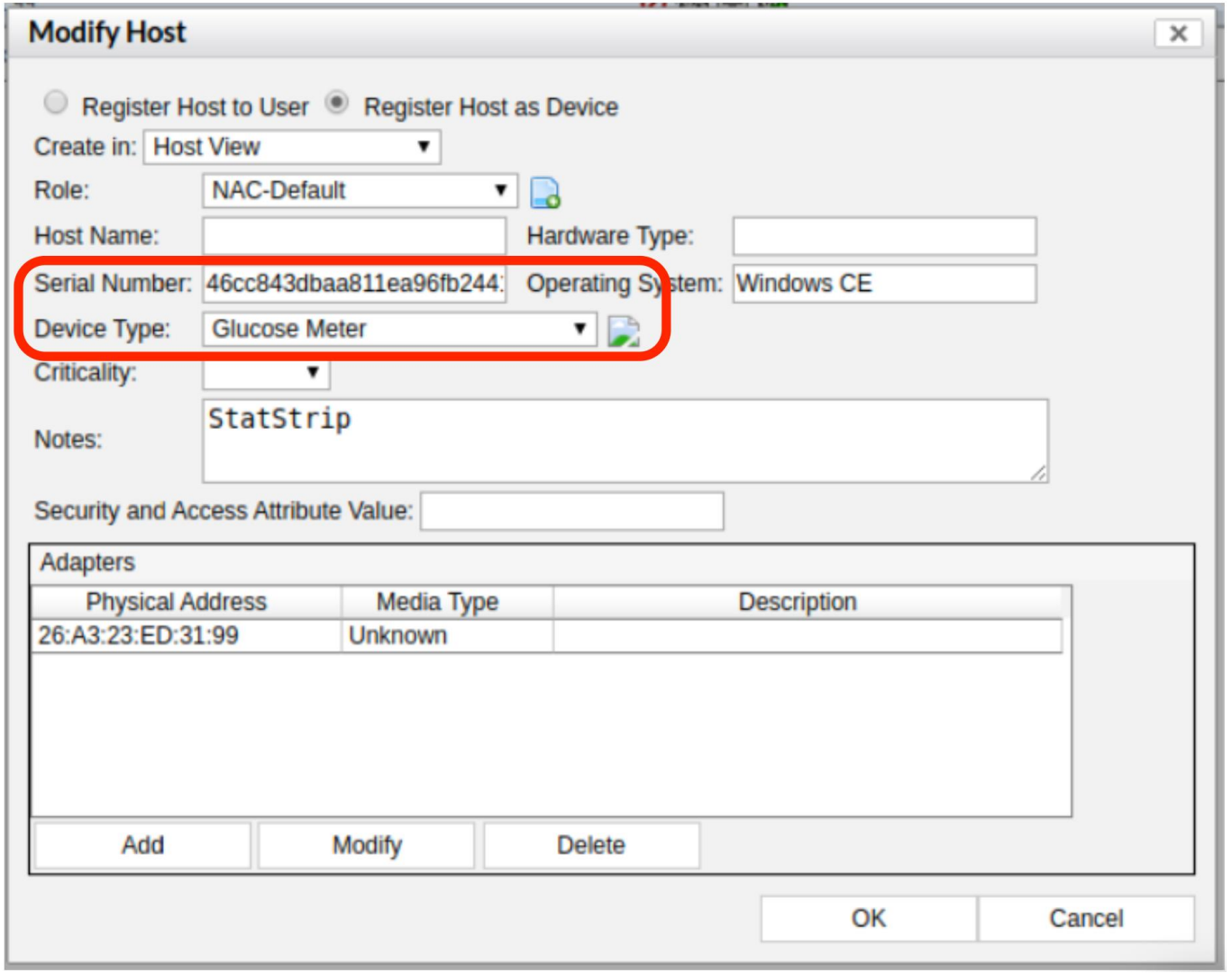


PROTECT

NETWORK ACCESS CONTROL - NAC

PROTECT

L’integrazione tra la piattaforma Medigate ed il FortiNAC ad esempio, permette di affinare l’identificazione del device, e quindi FortiNAC può impostare una micro-segmentazione e policy di accesso in tempo reale per contenere gli attacchi e garantire solo l'accesso appropriato alle risorse



PRIVILEDGE ACCESS MANAGEMENT

PROTECT

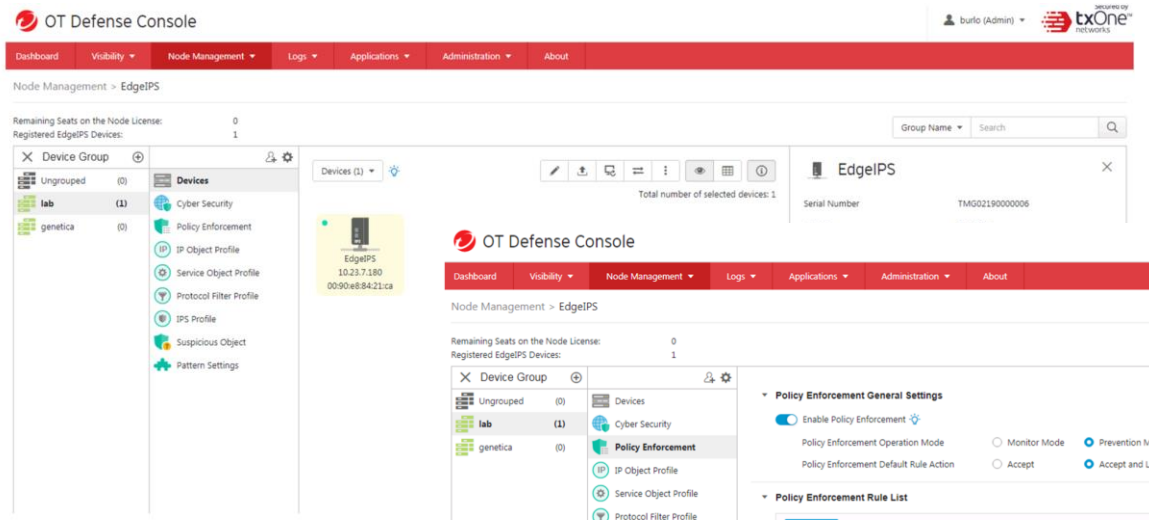
Quando si installano dispositivi IoMT, è molto importante garantire che le credenziali e le password di default siano configurate correttamente. È inoltre necessario gestire gli account privilegiati per proteggere questi dispositivi e garantire che sia consentito solo l'accesso autorizzato. Questi dispositivi infatti possono contenere informazioni sensibili dei pazienti.

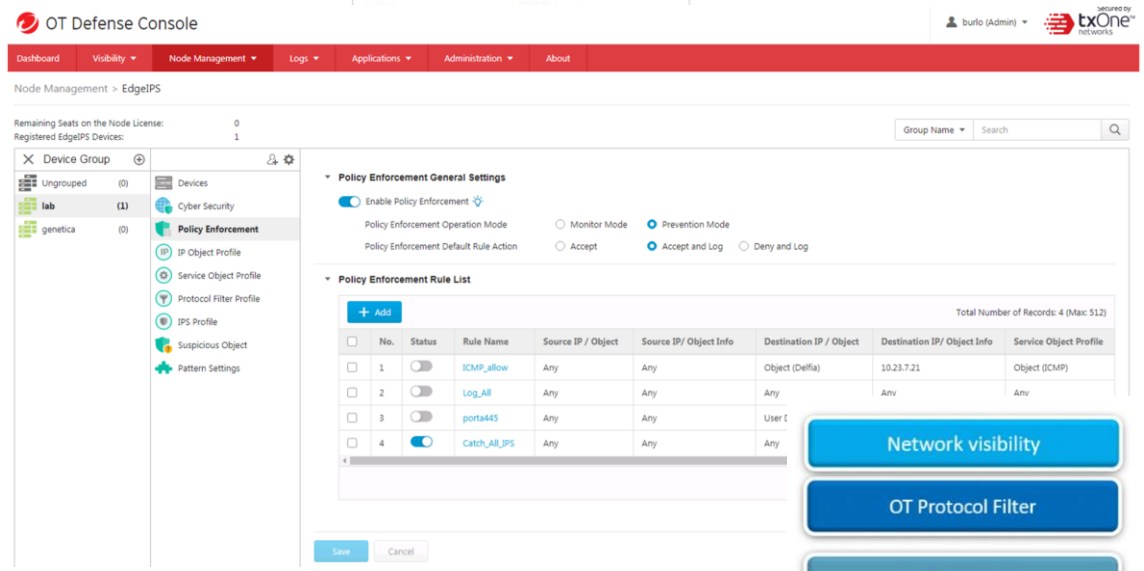
Possiamo quindi utilizzate una soluzione di gestione degli accessi privilegiati ed abilitate la gestione automatica degli account per aggiungere ulteriori controlli di sicurezza tenere traccia completa degli accessi, e impedire che i vostri dispositivi vengano compromessi, sia per accedere alla vostra rete che per attaccare un altro obiettivo.

- **Proteggete le credenziali** privilegiate con un audit completo IT.
- Controllate che le credenziali e **impostate degli avvisi** per sapere quando un amministratore cambia una password.
- **Controllate continuamente** gli account privilegiati.
- Tenere le credenziali ben nascoste**.**
- Abilitare **l'accesso di terzi in modo sicuro.**
- Praticare la randomizzazione delle password, il ciclaggio e il checkout.
- **Registrare e monitorare le sessioni**.
- Rimuovete gli account inutilizzati.

INLINE PROTECTION

PROTECT



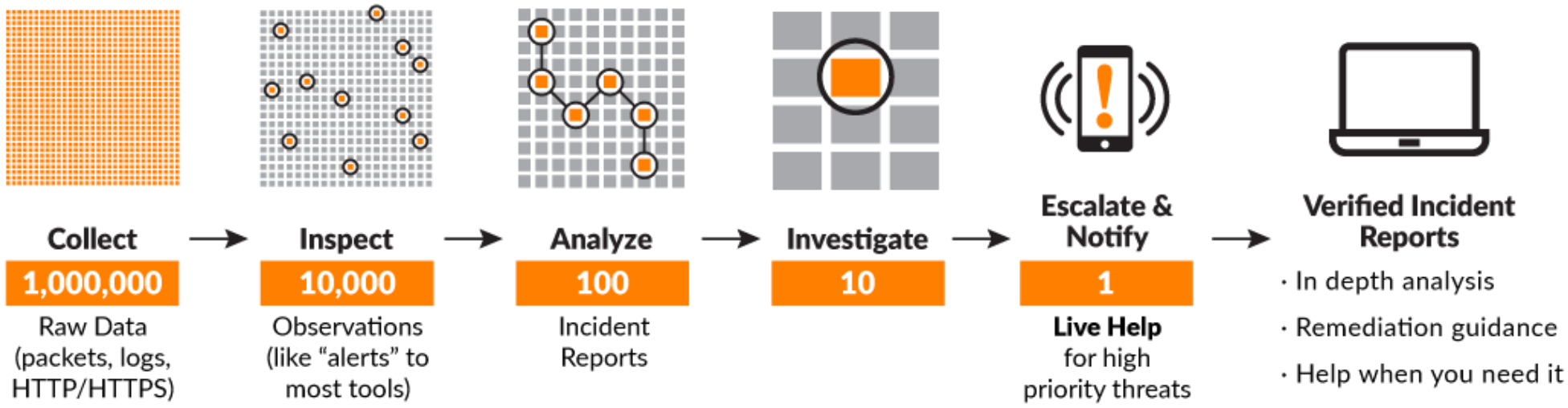


- Network visibility
- OT Protocol Filter
- Virtual Patch
- TXODI inside
- Dual Power Input
- Hardware Bypass
- Network Segmentation
- NAT - Firewall

DETECT ANOMALIES

Il Security Operation Center (SOC) è composto da un team di professionisti IT con esperienza nella sicurezza informatica che monitora, analizza e protegge un'organizzazione dagli attacchi informatici.

Scopo del SOC è quello di analizzare le informazioni che il cliente mette a disposizione, per identificare le informazioni che necessitano di una investigazione approfondita per poter essere identificate come incidente informatico. Di seguito uno schema esemplificativo della modalità operativa.



DETECT

DETECT

Esempio di segnalazione SOC

Cc ○ SOC

Salve,
abbiamo rilevato una comunicazioe dirette a un IP malevolo (nodo tor) da parte di un device, in dettaglio le tabelle sotto:

ALERT TYPE	DETECTED	DESCRIPTION	EXTERNAL IP	INTERNAL IP	MAC	CATEFORY
Attempted Malicious Internet Communication	8/2/21, 11:09 PM	Attempted outbound Internet communication detected	104.244.73.93	10.23.5.14	00:22:64:98:DB:88	General IOT

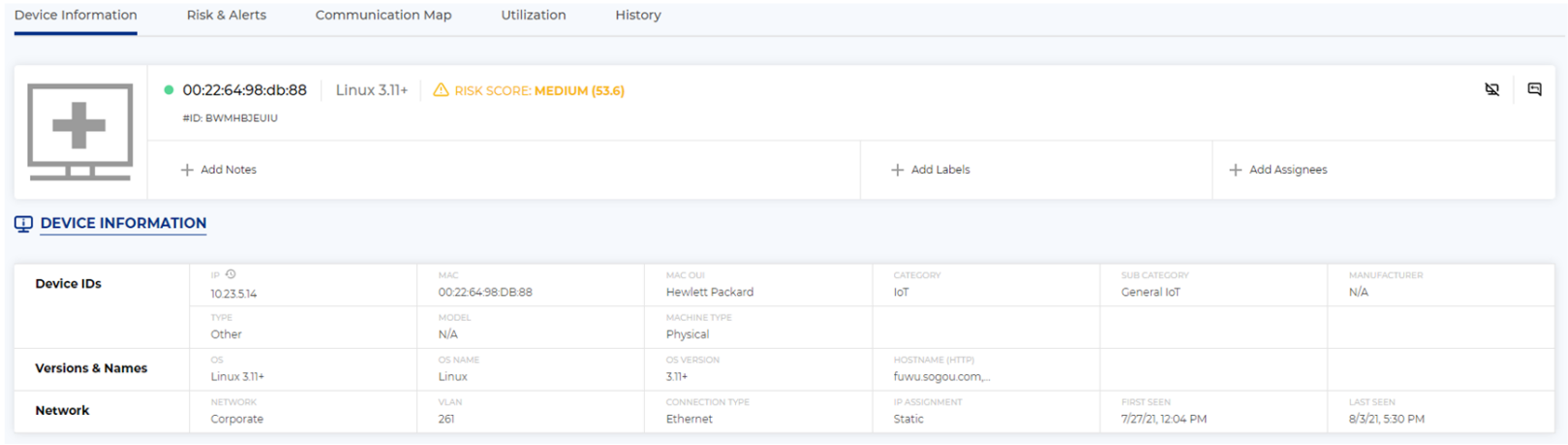
mead

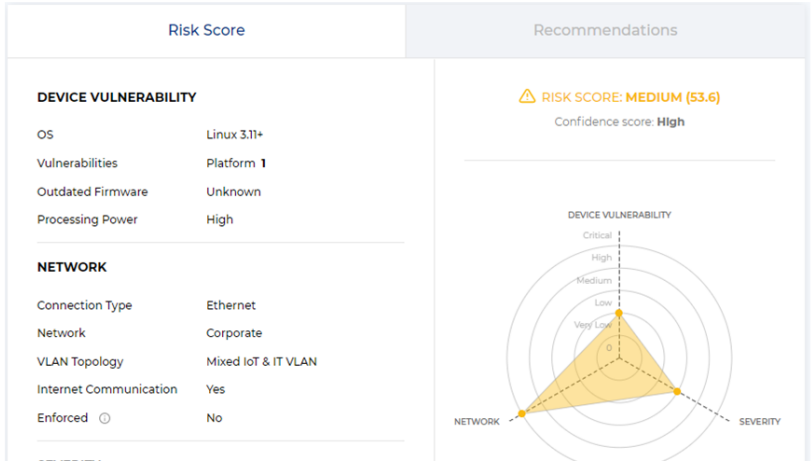
SEVERITY
3

Si consiglia di inserire in blacklist gli IP di destinazione e un eventuale controllo del device

1 (Informational): anomalie traffico di rete, informazioni generiche;
2 (Low impact): rilevamento vulnerabilità non gravi, basso rischio di violazione integrità dei sistemi;
3 (Moderate impact): rilevamento vulnerabilità gravi, rischio concreto di violazione integrità dei sistemi (malware generico);
4 (High impact): rischio elevato di violazione disponibilità di server in produzione, violazione di confidenzialità di dati sensibili e/o soggetti a normative Privacy, possibile presenza di malware ransomware, vulnerabilità gravi e così via;
5 (Critical Impact): evidenze di violazione disponibilità di server in produzione, violazione di confidenzialità di dati sensibili e/o soggetti a normative Privacy, evidenze della presenza di malware ransomware, vulnerabilità critiche e così via.

Informazioni rilevate sul device:





DETECT

Esempio di segnalazione SOC

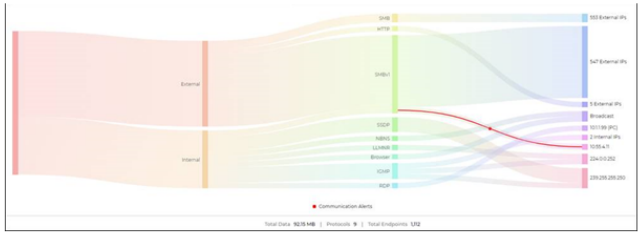
Cc SOC

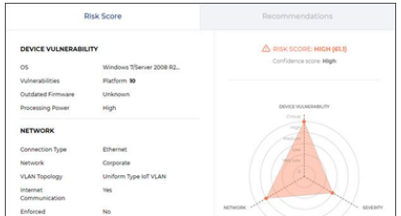
Salve,
abbiamo rilevato una delle comunicazione dirette verso IP malevoli dalla macchina 10.23.3.31

ALERT TYPE	DETECTED	INTERNAL IP	MAC ADDRESS	OS	CATEGORY	EXTERNAL IP	MALICIOUS IP TYPE	MALICIOUS IP SEVERITY	MALICIOUS IP CONFIDENCE
Attempted Malicious Internet Communication	10/08/2021, 14:10	10.23.3.31	00:10:f3:9c:69:af	Windows 7/Server 2008 R2	IoT	176.31.159.203	Phishing IP	High	85%
Attempted Malicious Internet Communication	10/08/2021, 13:29	10.23.3.31	00:10:f3:9c:69:af	Windows 7/Server 2008 R2	IoT	133.242.208.183	Malware C&C IP	Very High	90%
Attempted Malicious Internet Communication	10/08/2021, 12:54	10.23.3.31	00:10:f3:9c:69:af	Windows 7/Server 2008 R2	IoT	51.15.247.166	Compromised IP	Medium	83%
Attempted Malicious Internet Communication	10/08/2021, 11:58	10.23.3.31	00:10:f3:9c:69:af	Windows 7/Server 2008 R2	IoT	43.128.60.110	Compromised IP	Medium	98%
Attempted Malicious Internet Communication	10/08/2021, 11:57	10.23.3.31	00:10:f3:9c:69:af	Windows 7/Server 2008 R2	IoT	43.128.60.5	Compromised IP	Medium	100%
Attempted Malicious Internet Communication	10/08/2021, 12:32	10.23.3.31	00:10:f3:9c:69:af	Windows 7/Server 2008 R2	IoT	51.15.146.240	Command & Control (c2) IP	High	100%
Attempted Malicious Internet Communication	10/08/2021, 11:59	10.23.3.31	00:10:f3:9c:69:af	Windows 7/Server 2008 R2	IoT	43.128.60.24	Compromised IP	Medium	100%
Attempted Malicious Internet Communication	10/08/2021, 12:10	10.23.3.31	00:10:f3:9c:69:af	Windows 7/Server 2008 R2	IoT	51.15.7.202	Tor IP	Low	91%
Attempted Malicious Internet Communication	10/08/2021, 12:09	10.23.3.31	00:10:f3:9c:69:af	Windows 7/Server 2008 R2	IoT	51.15.7.145	Malware C&C IP	Very High	100%
Attempted Malicious Internet Communication	10/08/2021, 12:09	10.23.3.31	00:10:f3:9c:69:af	Windows 7/Server 2008 R2	IoT	51.15.7.140	Tor IP	Low	100%
Attempted Malicious Internet Communication	10/08/2021, 12:06	10.23.3.31	00:10:f3:9c:69:af	Windows 7/Server 2008 R2	IoT	49.51.184.162	Command & Control (c2) IP	High	100%
Attempted Malicious Internet Communication	10/08/2021, 11:31	10.23.3.31	00:10:f3:9c:69:af	Windows 7/Server 2008 R2	IoT	104.161.32.85	Malware C&C IP	Very High	87%
Attempted Malicious Internet Communication	10/08/2021, 09:42	10.23.3.31	00:10:f3:9c:69:af	Windows 7/Server 2008 R2	IoT	49.51.189.144	Command & Control (c2) IP	High	100%
Attempted Malicious Internet Communication	10/08/2021, 10:38	10.23.3.31	00:10:f3:9c:69:af	Windows 7/Server 2008 R2	IoT	62.171.142.179	Command & Control (c2) IP	Very High	90%
Attempted Malicious Internet Communication	10/08/2021, 10:13	10.23.3.31	00:10:f3:9c:69:af	Windows 7/Server 2008 R2	IoT	77.68.126.241	Tor IP	Low	100%
Attempted Malicious Internet Communication	09/08/2021, 17:04	10.23.3.31	00:10:f3:9c:69:af	Windows 7/Server 2008 R2	IoT	45.146.164.193	Malware C&C IP	High	100%

1 (Informational): anomalie traffico di rete, informazioni generiche;
2 (Low Impact): rilevamento vulnerabilità non gravi, basso rischio di violazione integrità dei sistemi;
3 (Moderate impact): rilevamento vulnerabilità gravi, rischio concreto di violazione integrità dei sistemi (malware generico);
4 (High impact): rischio elevato di violazione disponibilità di server in produzione, violazione di confidenzialità di dati sensibili e/o soggetti a normative Privacy, possibile presenza di malware ransomware, vulnerabilità gravi e così via;
5 (Critical Impact): evidenze di violazione disponibilità di server in produzione, violazione di confidenzialità di dati sensibili e/o soggetti a normative Privacy, evidenze della presenza di malware ransomware, vulnerabilità critiche e così via.

Informazioni aggiuntive sulla macchina:

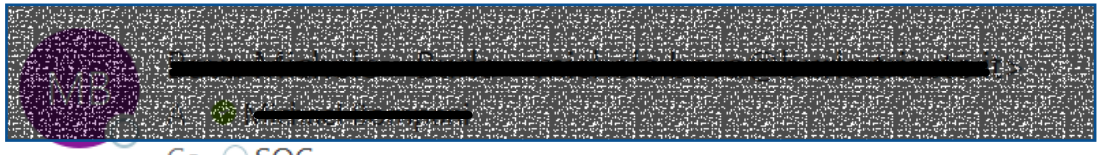




mead
SEVERITY
3

mead
YOUR DIGITAL INTEGRATOR

RE: Rilevato tentativo di comunicazione verso IP malevoli



Cc SOC

Fare clic per scaricare le immagini. Per tutelare la privacy, Outlook ha impedito il download automatico di alcu

Grazie per la segnalazione.
La macchina è affetta da wannacry ed è quella di un fornitore esterno.
Intanto sto droppando tutto il traffico grazie ad una regola sul fw.
Cordiali saluti.

DETECT

Esempio di segnalazione SOC

Richiamo funzionalità per ABL90 FLEX

Mirko Gorrieri
A [redacted]
Cc ⊞ **SOC**

PDF 20200401RadiometerABL90FLEXandABL90FLEXPLUSClientUS_Redacted(ECRI).pdf
192 KB

Salve
Vi segnaliamo un richiamo per i sistemi di campionamento dei gas ematici ABL90 FLEX e ABL90 FLEX PLUS, questi possono riportare risultati distorti per la bilirubina (tBil). Il bias aumenta in modo non lineare con la concentrazione di emoglobina totale (tHb).
In allegato potete trovare copia del richiamo di Radiometer America.

MANUFACTURER REASON FOR RECALL

Radiometer states that ABL90 FLEX and ABL90 FLEX PLUS Blood Gas Sampling Systems may report biased results for bilirubin (tBil). The bias increases nonlinearly with total hemoglobin (tHb) concentration.
For adult patients, Radiometer states that the problem has a remote risk of leading to minor adverse health consequences. In the worst-case scenario based on the described positive bias for ctBil, an adult patient may be subjected to unnecessary diagnostic investigation. Radiometer does not consider it likely that the problem can cause permanent damage to the body structure or necessitate medical or surgical intervention to preclude irreversible impairment or damage. Radiometer states that reporting ctBil for adult samples is outside the intended use for the above systems in the U.S. market. Radiometer further states that the described elevated bias on measurements on newborn samples is considered insignificant in terms of risk.

Apparato oggetto della segnalazione:

ABL90 FLEX | Radiometer | RISK SCORE: HIGH (57.5)
#ID: BWMIQMBJKU

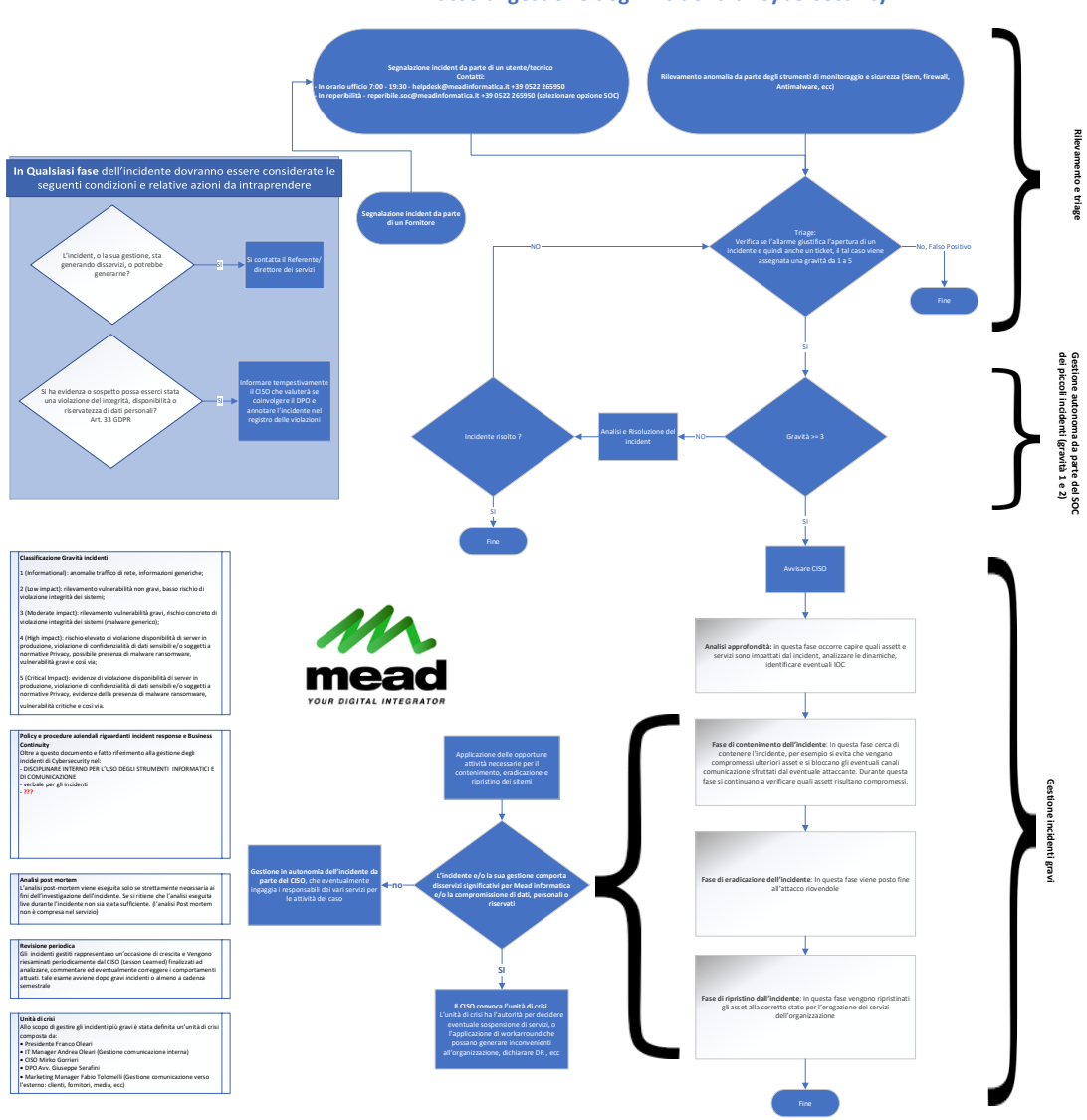
+ Add Notes | + Add Labels | + Add Assignees | 1 MDS² Form | + Suggest MDS² Files

DEVICE INFORMATION

Device IDs	IP 10.23.35.4	MAC 00:04:5F:72:50:25	MAC OUI Avalue Technology, Inc.
	CATEGORY Medical	SUB CATEGORY Clinical Lab	MANUFACTURER Radiometer
	TYPE Blood Gas Analyzer	MODEL ABL90 FLEX	MACHINE TYPE Physical
	MOBILITY Portable	SERIAL NUMBER 090R0985N0012	FDA CLASS 2
Versions & Names	OS Windows Vista/7/8	OS NAME Windows	OS VERSION Vista/7/8
	HOSTNAME (WIN) \090R0985N0012		
Network	NETWORK Corporate	VLAN 57	VLAN NAME POCT
	CONNECTION TYPE Ethernet	IP ASSIGNMENT Static	FIRST SEEN 7/27/21, 11:50
	LAST SEEN 8/8/21, 16:41		

INCIDENT RESPONSE PLAN

RESPOND



FASE 1 - GAP analisi sul livello di preparazione dell'azienda per affrontare incidenti di cybersecurity

FASE 2 – Definizione di:

- ruoli e responsabilità,
- strumenti di raccolta log,
- strumenti di rilevamento anomalie e attacchi,
- procedure risposta agli incidenti
- (triage e analisi,
- contenimento,
- eradicazione,
- ripristino),
- gestione della comunicazione,
- gestione dei data Breach

RECOVERY PLAN

RECOVER

IT DEPARTMENT

INGEGNERIA CLINICA

EMERGENCY RESPONSE TEAM

COMMUNICATION PLAN

GPDP
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

polizia delle comunicazioni

CNAIPIC

CSIRT Italia

ONSITE SUPPORT

CLINICAL SOC
CYBER SECURITY CONTROL ROOM

BOARD AZIENDALE

CONTINUOS IMPROVEMENT

DON’T BE AN EASY TARGET

RECOVER

mead
YOUR DIGITAL INTEGRATOR

ADVANCED HEALTHCARE PROTECTION

Grazie

ROBERTO FANTINI
r.fantini@meadinformatica.it
3292638550