
punto
impresa
digitale

Iniziative in programma

CLICCA SUL SINGOLO EVENTO PER APPROFONDIMENTI E ISCRIZIONI:

- **6-13 marzo** - Strategie e tecnologie per la gestione della conoscenza e dell'innovazione aziendale - modalità mista
- **18 marzo** - AI e brevetti: le nuove frontiere della ricerca brevettuale - webinar
- **20 marzo** - AI Revolution-Creare, Analizzare e Innovare con l'Intelligenza Artificiale Generativa - webinar
- **25 marzo** - Corso esperienziale: Lean Factory 4.0-La trasformazione digitale in un'impresa manifatturiera - in presenza
- **1-8-15 aprile** - La ricerca brevettuale: istruzioni per l'uso - webinar
- **9 aprile** - Aspetti etici e legali relativi all'AI (AI Act e Data Act) per un futuro responsabile - webinar

Iniziative in programma

CLICCA SUL SINGOLO EVENTO PER APPROFONDIMENTI E ISCRIZIONI:

- Corso di 32 ore Logistica integrata e sistema doganale - **iscrizioni entro il 20 mar**
- Percorso formativo gratuito sulla parità di genere - **scade 12 aprile**
- Bando PID-Next: sostegno alla trasformazione digitale - **scade 29 maggio**
- Check-up tecnologici e consulenza gratuita per introdurre innovazione in azienda - **scade 29 agosto**

UNIONCAMERE

Il web è un luogo pericoloso? Come le piccole e medie imprese possono difendersi con la cybersecurity

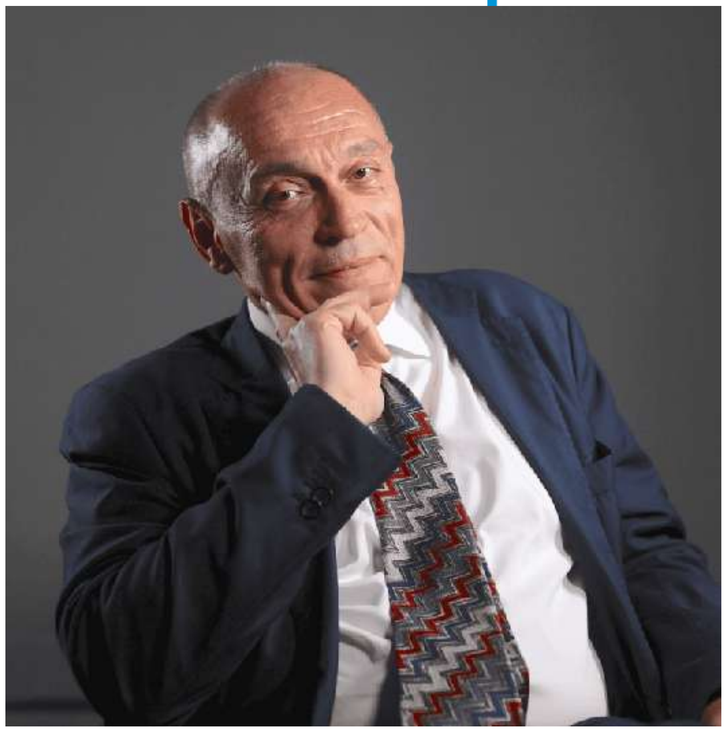
punto impresa digitale

a cura di
Giorgio Sbaraglia

DINTEC
CONSORZIO PER L'INNOVAZIONE TECNOLOGICA

27 febbraio 2025

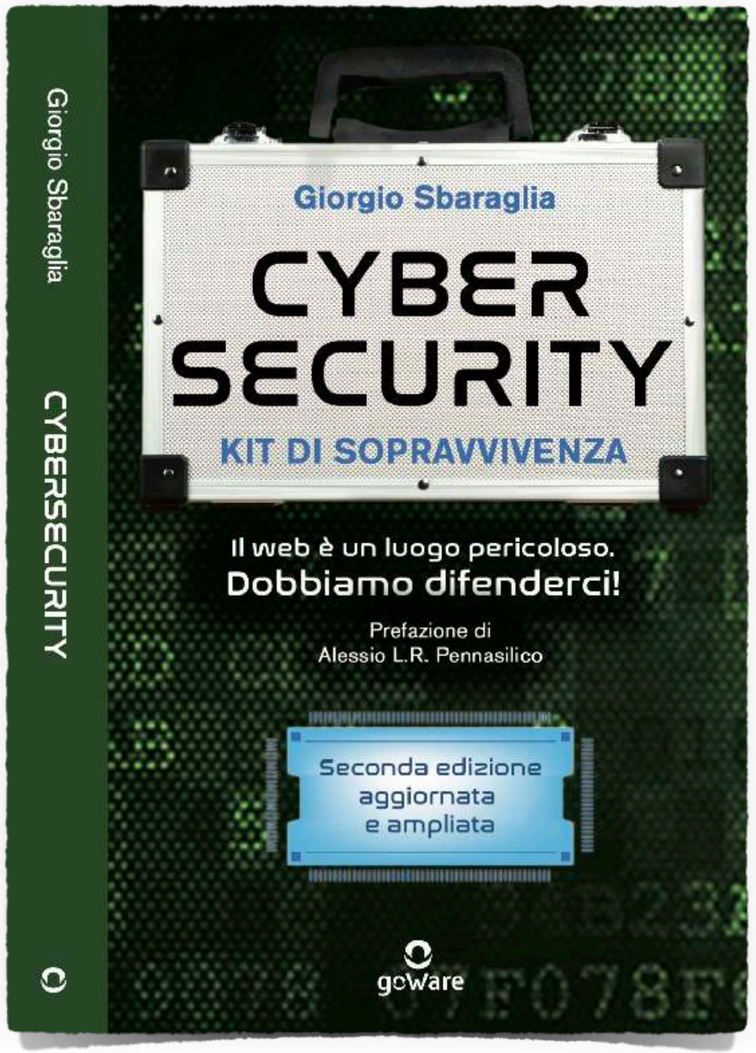
CHI SONO



Giorgio Sbaraglia, ingegnere

- ☑ Information & Cyber Security Advisor
- ☑ DPO (Data Protection Officer)
- ☑ Membro del Comitato Direttivo Clusit Associazione Italiana per la Sicurezza Informatica
- ☑ 24 ORE Coordinatore scientifico del Master “Cybersecurity e Data Protection” della 24Ore Business School
- ☑ Collaboratore redazione www.cybersecurity360.it CYBERSECURITY360
- ☑ Scrivo per https://www.datamanager.it DMO Data Manager Online il portale dell'ICT professionale

I MIEI LIBRI



Il quadro normativo e regolamentare nazionale ed europeo in materia di gestione dei cyber rischi (panoramica)

TIMELINE NORMATIVE ITALIANE ED EUROPEE SULLA CYBERSECURITY

Direttiva NIS 1
2016/1148

2016

2018

Decreto NIS
D. Lgs. n. 65/2018

Recepimento della direttiva NIS 1

Regolamento Cybersecurity Act

2019

2019

D.L. 21 settembre 2019, n. 105

Norma istitutiva del Perimetro di Sicurezza Nazionale Cibernetica (**PSNC**)

2021

D.L. 14 giugno 2021, n. 82

Norma istitutiva dell'Agenzia per la Cybersicurezza Nazionale

Direttiva NIS 2
Direttiva CER
Regolamento DORA

2023

Regolamento Cyber Resilience Act 2024/2847 e proposta Cyber Solidarity Act (?)

2024

L.28 giugno 2024, n. 90

Decreto NIS2
D. Lgs. n. 138/2024
(Recepimento della NIS 2)

*Gli anni indicati si riferiscono agli anni di **entrata in vigore** delle citate normative.*

DIRETTIVA (UE) 2022/2555 - NIS 2

L 333/80 IT Gazzetta ufficiale dell'Unione europea 27.12.2022

DIRETTIVE

DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 14 dicembre 2022

relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)

(Testo rilevante ai fini del SEE)

Abroga la **Direttiva (UE) 2016/1148 (Direttiva NIS)** e modifica anche il **Regolamento (UE) n. 910/2014 eIDAS (**electronic IDentification Authentication and Signature) del 23 luglio 2014 (UE 2014/910).

Approvata 14 dicembre 2022, entrata in vigore il 17 gennaio 2023.

Il termine per il recepimento nazionale della Direttiva NIS 2 è stato fissato al **17 ottobre 2024**

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32022L2555

DIRETTIVA (UE) 2022/2555 - NIS 2

ARTICOLO 2 - AMBITO DI APPLICAZIONE (IN SINTESI)

Secondo quanto disposto dall'art. 2 della NIS 2, questa si applica a:

Grandi organizzazioni: con più di 250 dipendenti
Medie imprese: con 50-250 dipendenti.

Sono escluse le imprese con meno di 50 dipendenti e un fatturato annuo inferiore a 10 milioni di euro, a meno che non siano ritenute di importanza critica per la società.

> 50

> 10 M

18 Settori

DIRETTIVA (UE) 2022/2555 - NIS 2: SETTORI E SOGGETTI

SETTORI:

AD ALTA CRITICITÀ

ALTRI SETTORI CRITICI

SOGGETTI:

ESSENZIALI

IMPORTANTI

NON IN AMBITO

DIRETTIVA (UE) 2022/2555 - NIS 2: I SETTORI INTERESSATI

ALLEGATO I SETTORI AD ALTA CRITICITÀ
1. Energia
2. Trasporti
3. Settore bancario
4. Infrastrutture dei mercati finanziari
5. Settore sanitario
6. Acqua potabile
7. Acque reflue
8. Infrastrutture digitali
9. Gestione dei servizi TIC (business-to-business)
10. Pubblica amministrazione
11. Spazio

ALLEGATO II ALTRI SETTORI CRITICI
1. Servizi postali e di corriere
2. Gestione dei rifiuti
3. Fabbricazione, produzione e distribuzione di sostanze chimiche
4. Produzione, trasformazione e distribuzione di alimenti
5. Fabbricazione (vedere dettagli ALLEGATO II)
6. Fornitori di servizi digitali
7. Ricerca

DIRETTIVA (UE) 2022/2555 - NIS 2: I SETTORI INTERESSATI

Settori essenziali Settori importanti

PRESENTI GIÀ NELLA NIS1

- Energia
- Trasporti
- Settore bancario
- Infrastrutture e mercati finanziari
- Settore sanitario
- Infrastrutture digitali
- Fornitura acqua potabile
- Fornitori di servizi digitali

AGGIUNTI NELLA NIS2

- Pubblica Amministrazione
- Gestione acque reflue
- Gestione dei servizi TIC
- Spazio
- Servizi postali e di corriere
- Gestione dei rifiuti
- Sostanze chimiche
- Alimenti
- Fabbricazione
- Ricerca

DIRETTIVA (UE) 2022/2555 - NIS 2

ART. 21 - MISURE DI GESTIONE DEI RISCHI DI CIBERSICUREZZA

2. Le misure di cui al paragrafo 1 sono basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti e comprendono **almeno** gli elementi seguenti:

a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;

b) gestione degli incidenti;

c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;

d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;

e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;

f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;

g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza;

h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;

i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;

j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

DIRETTIVA (UE) 2022/2555 - NIS 2

ART. 34 - SANZIONI AMMINISTRATIVE PECUNIARIE AI SOGGETTI ESSENZIALI E IMPORTANTI

A differenza di quanto precedentemente previsto dalla NIS,
che all'**articolo 21 delegava completamente ai singoli Stati membri la definizione delle sanzioni** in caso di violazione delle disposizioni della Direttiva, richiamando solamente e semplicemente il principio di proporzionalità e di finalità dissuasiva delle stesse,
con la NIS 2 il quadro sanzionatorio è estremamente più dettagliato.

All'articolo 34 il legislatore europeo ha già previsto un perimetro sanzionatorio da applicare che si differenzia tra soggetti essenziali e soggetti importanti.

Le sanzioni pecuniarie si riferiscono specificamente alle violazioni degli artt.:
✓ Art.21 (Misure di gestione dei rischi di cybersicurezza)
✓ Art.23 (Obblighi di segnalazione di incidenti).

DIRETTIVA (UE) 2022/2555 - NIS 2

ART. 34 - SANZIONI AMMINISTRATIVE PECUNIARIE AI SOGGETTI ESSENZIALI E IMPORTANTI

1. Gli Stati membri provvedono affinché le sanzioni amministrative pecuniarie imposte ai soggetti essenziali e importanti a norma del presente articolo in relazione alle violazioni della presente direttiva siano effettive, proporzionate e dissuasive, tenendo conto delle circostanze di ogni singolo caso.
2. Le sanzioni amministrative pecuniarie sono imposte in aggiunta a qualsiasi delle misure di cui all'articolo 32, paragrafo 4, lettere da a) a h), all'articolo 32, paragrafo 5, e all'articolo 33, paragrafo 4, lettere da a) a g).

Soggetti essenziali:
fino a 10 milioni di euro o al 2% del loro fatturato annuo globale.

Soggetti importanti:
fino a 7 milioni di euro o all'1,4% del loro fatturato annuo globale.

IL DECRETO LEGISLATIVO 4 SETTEMBRE 2024, N.138: L'ITALIA HA RECEPITO LA NIS 2

DECRETO LEGISLATIVO 4 settembre 2024, n. **138.**

Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 76 e 87, quinto comma, della Costituzione;

Vista la legge 23 agosto 1988, n. 400, recante «Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri» e, in particolare, l'articolo 14;

IL DECRETO LEGISLATIVO 4 SETTEMBRE 2024, N.138: L'ITALIA HA RECEPITO LA NIS 2

NIS 2 è una direttiva, quindi – a differenza di un regolamento che è immediatamente esecutivo - richiede il recepimento da parte degli Stati membri.

Questo deve essere fatto, secondo l'art. 41, entro il 17 ottobre 2024.

L'Italia è stata molto puntuale: tale decreto di recepimento è stato presentato il 17 giugno 2024 per essere sottoposto al parere parlamentare. È stato poi approvato e pubblicato sulla G.U. del 01/10/2024 come **Decreto legislativo 4 settembre 2024, n.138.**

Tale decreto si applica a decorrere dal 18 ottobre 2024 e nella stessa data esso abroga il decreto legislativo 18 maggio 2018, n. 65 (NIS 1).

L'**Agenzia per la Cybersicurezza Nazionale** è designata in qualità di Autorità nazionale competente NIS, con funzioni di coordinatore ai sensi dell'art.9, paragrafo 2, della direttiva (vedasi art.1 del decreto). ACN è quindi il punto di riferimento centrale per l'applicazione e le attività di controllo (anche sanzionatorio) della Direttiva NIS 2.

All'art.11 vengono designate invece le Autorità di settore NIS, che riprendono in genere le stesse già indicate nel D.Lgs.n.65/2018 relativo alla NIS 1.

IL DECRETO LEGISLATIVO 4 SETTEMBRE 2024, N.138: L'ITALIA HA RECEPITO LA NIS 2

I passi indicati dal D.Lgs. 138 sono:

1) ogni anno, **dal 1° gennaio al 28 febbraio**, le aziende che rientrano nell'ambito NIS 2 (art.3 del decreto) devono registrarsi o aggiornare le proprie informazioni sulla piattaforma digitale creata dall'ACN (Agenzia per la Cybersicurezza Nazionale), fornendo dettagli fondamentali come la ragione sociale, il settore di appartenenza e un punto di contatto.

2) **Entro il 31 marzo di ogni anno:** ACN pubblica l'elenco aggiornato delle aziende registrate e comunica ufficialmente se queste siano incluse o escluse dall'elenco dei soggetti regolamentati.

3) **Tra il 1° aprile 2025 e il 15 aprile 2025**: ACN comunicherà ai soggetti registrati l'inserimento nell'elenco dei soggetti essenziali o importanti.

4) **Dal 15 aprile al 31 maggio:** le aziende che hanno ricevuto comunicazione dall'ACN devono fornire dati aggiornati riguardo agli indirizzi IP pubblici, ai domini e ai responsabili della sicurezza.

5) **Tra il 1° maggio e il 30 giugno:** le aziende devono fornire informazioni sui servizi e sulle attività svolte (Art. 24, commi 1 e 2), in modo da permettere una corretta categorizzazione da parte delle autorità competenti. L'ACN fornisce un riscontro sulla conformità entro 90 giorni dalla comunicazione; in assenza di tale riscontro, la conformità si considera convalidata.

Il cronoprogramma sopra riportato è specificato all'art.7 del decreto.

IL DECRETO LEGISLATIVO 4 SETTEMBRE 2024, N.138: LE SCADENZE PER LE AZIENDE INTERESSATE

I passi indicati dal D.Lgs. 138 sono (**Art. 42.Fase di prima applicazione**):

1) **entro il primo gennaio 2026**, i soggetti a cui si applica la NIS2 devono adeguarsi all'**articolo 25 Obblighi in materia di notifica di incidente**; questo richiede come minimo di stabilire il processo di gestione degli incidenti;
2) **entro il 1°gennaio 2026**, i soggetti a cui si applica la NIS2 devono adeguarsi all'art. 30 e quindi aggiornare ogni anno le informazioni richieste dalla piattaforma ACN con l'elenco di attività e servizi e la descrizione delle loro caratteristiche;
3) **entro 1°ottobre 2026** (18 mesi dalla comunicazione da ACN del 31 marzo 2025), i soggetti a cui si applica la NIS2 devono adeguarsi agli articoli:
   - ✓ Art.23 (sugli obblighi degli organi di amministrazione e direttivi),
   - ✓ **Art.24 Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica** (gestione dei rischi e implementazione delle misure di sicurezza),
   - ✓ Art.29 (relativo alla banca dati dei nomi a dominio).

Vedere anche:
https://www.acn.gov.it/portale/nis/obblighi

ACN: AMBITO E REGISTRAZIONE

Agenzia per la cybersicurezza nazionale

Segnala un incidente informatico

Agenzia | PNRR | NIS | Cloud | NCC Italia | Lavora con noi | Amministrazione traspa

Home / NIS / Ambito e registrazione

Ambito e registrazione

Registrazione

Entro il 28 febbraio 2025 i soggetti pubblici e privati a cui si applica la NIS devono manifestarsi all'Autorità nazionale competente NIS registrandosi sulla piattaforma digitale che sarà resa disponibile da ACN dal 1° dicembre 2024.

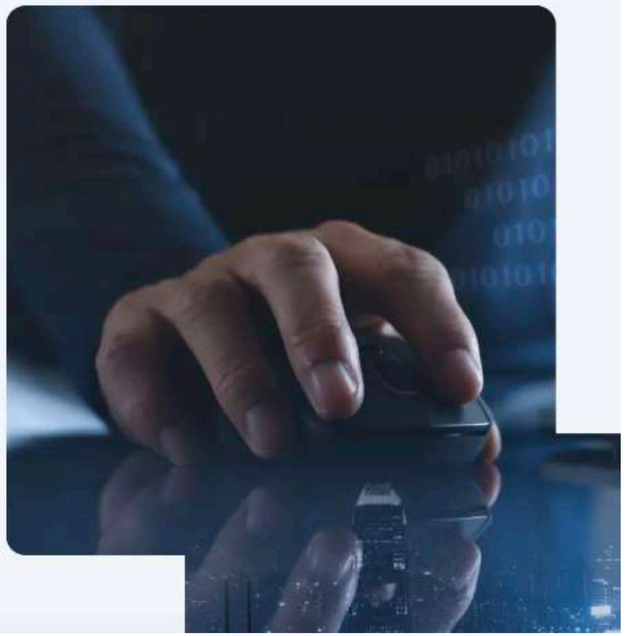
Resta ferma la possibilità per l'Autorità nazionale competente NIS, su proposta delle Autorità di settore, di individuare ulteriori soggetti ritenuti critici. Tali soggetti riceveranno una specifica comunicazione diretta, a valle della quale potranno procedere con la registrazione.

Le modalità di registrazione sono delineate dall'articolo 7 del decreto NIS e verranno dettagliate con un apposito provvedimento attuativo.

Tale adempimento è funzionale a consentire ad ACN di censire i soggetti operanti nei settori vigilati, anche al fine di fornire loro supporto in fase di implementazione degli obblighi, attraverso le articolate attività di monitoraggio e ausilio nel loro percorso condiviso di crescita, disciplinate dall'articolo 35.

La mancata registrazione è una violazione assistita da una sanzione amministrativa pecuniaria con un importo fino al 0.1% del fatturato annuo su scala mondiale del soggetto.

A valle della fase di registrazione, nel mese di aprile 2025, i soggetti che si sono registrati riceveranno una comunicazione per confermare, o meno, il loro l'inserimento nell'elenco dei soggetti NIS.



https://www.acn.gov.it/portale/nis/ambito-registrazione

ACN: AMBITO DI APPLICAZIONE

Agenzia | PNRR | NIS | Cloud | NCC Italia | Lavora con noi | Amministrazione trasparente

Ambito di applicazione

La nuova normativa NIS amplia il campo di applicazione della normativa a 18 settori di cui 11 altamente critici (originariamente 8) e 7 critici (di nuova introduzione) per oltre 80 tipologie di soggetti, distinguendoli tra essenziali e di servizi importanti.

Per ulteriori dettagli si fa riferimento agli allegati I, II, III e IV del Decreto legislativo 4 settembre 2024, n. 138 .

Consulta il dettaglio degli ambiti di applicazione.

Settore	Dettaglio	Grandi imprese	Medie imprese	Piccole e micro imprese
SETTORI ALTAMENTE CRITICI				
Energia	19 tipologie di soggetto	Essenziali	Importanti *	Fuori ambito **
Trasporti	10 tipologie di soggetto			
Settore bancario	DORA Lex specialis			
Infrastrutture dei mercati finanziari				
Settore sanitario	5 tipologie di soggetto			
Acqua potabile	1 tipologia di soggetto			
Acque reflue	1 tipologia di soggetto			
Infrastrutture digitali	9 tipologie di soggetto			
Gestione dei servizi TIC (b2b)	2 tipologie di soggetto		Importanti *	Fuori ambito **
Spazio	1 tipologia di soggetto			
SETTORI CRITICI				
Servizi postali e di corriere	1 tipologia di soggetto	Importanti *		Fuori ambito **
Gestione dei rifiuti	1 tipologia di soggetto			
Fabbricazione, produzione e distribuzione di sostanze chimiche	1 tipologia di soggetto			
Produzione, trasformazione e distribuzione di alimenti	1 tipologia di soggetto			
Fabbricazione	6 tipologie di soggetto			

https://www.acn.gov.it/portale/nis/ambito-registrazione

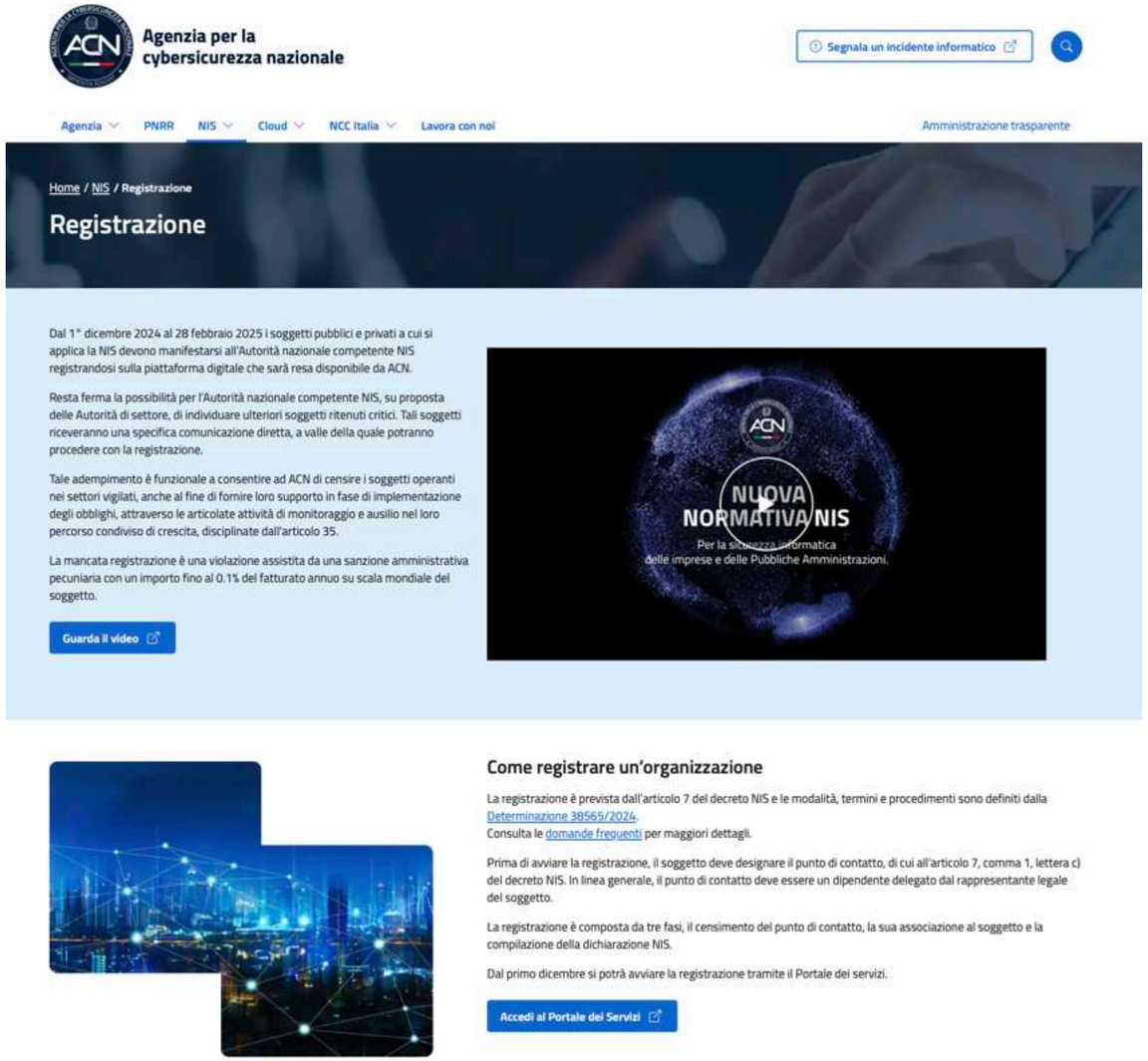
ACN: AMBITO DI APPLICAZIONE

Agenda di Ricerca e Innovazione per la Cybersicurezza

Settore	Sottosettore o tipologia di soggetto	Grandi imprese (occupano almeno 250 dipendenti oppure hanno un fatturato di almeno 50M€ oppure hanno un bilancio di almeno 43M€)	Medie imprese (occupano almeno 50 dipendenti oppure hanno un fatturato di almeno 10M€ oppure hanno un bilancio di almeno 10M€)	Piccole e micro imprese
Allegato I: Settori ad alta criticità				
1. Energia	1. Energia elettrica 2. Teleriscaldamento e teleraffrescamento 3. Petrolio 4. Gas 5. Idrogeno	Essenziali	Importanti[1]	Non in ambito[2]
2. Trasporti	1. Trasporto aereo 2. Trasporto ferroviario 3. Trasporto per vie d'acqua 4. Trasporto su strada			
3. Settore bancario	1. Enti creditizi quali definiti all'articolo 4, punto 1), del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio **(DORA lex specialis)**			
4. Infrastrutture dei mercati finanziari	1. Gestori delle sedi di negoziazione quali definiti all'articolo 4, punto 24), della direttiva 2014/65/UE del Parlamento europeo e del Consiglio 2. Controparti centrali (CCP) quali definite all'articolo 2, punto 1), del regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio **(DORA lex specialis)**			
5. Settore sanitario	1. Prestatori di assistenza sanitaria quali definiti all'articolo 3, lettera g), della direttiva 2011/24/UE del Parlamento europeo e del Consiglio 2. Laboratori di riferimento dell'UE quali definiti all'articolo 15 del regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio 3. Soggetti che svolgono attività di ricerca e sviluppo relative ai medicinali quali definiti all'articolo 1, punto 2), della direttiva 2001/83/CE del Parlamento europeo e del Consiglio 4. Soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici di cui alla sezione C, divisione 21, della NACE Rev. 2 5. Soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica (elenco dei dispositivi critici per l'emergenza di sanità pubblica) di cui all'articolo 22 del regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio			
6. Acqua potabile	1. Fornitori e distributori di acque destinate al consumo umano, quali definiti all'articolo 2, punto 1, lettera a), della direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio, ma esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano è una parte non essenziale dell'attività generale di distribuzione di altri prodotti e beni			
7. Acque reflue	1. Imprese che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche o industriali quali definite all'articolo 2, punti da 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, escluse le imprese per cui la raccolta, lo smaltimento o il trattamento di acque reflue urbane, domestiche o industriali è una parte non essenziale della loro attività generale			

https://www.acn.gov.it/portale/documents/d/guest/faq-1-5_dettaglio-ambiti-di-applicazione

ACN: PROCEDURA DI REGISTRAZIONE SUL PORTALE



Prima di avviare la registrazione, il soggetto deve designare il **punto di contatto**, di cui all'articolo 7, comma 1, lettera c) del decreto NIS. In linea generale, il punto di contatto deve essere un dipendente delegato dal rappresentante legale del soggetto.

La registrazione è composta da tre fasi, il censimento del punto di contatto, la sua associazione al soggetto e la compilazione della dichiarazione NIS.

Dal **primo dicembre 2024**, il Punto di contatto potrà autenticarsi sul portale dei Servizi dell'Agenzia tramite SPID.

Per associare il punto di contatto al soggetto è necessario indicare:

- per le pubbliche amministrazioni, il codice IPA;
- per i soggetti pubblici e privati, il codice fiscale.

https://www.acn.gov.it/portale/nis/registrazione

ACN: PROCEDURA DI REGISTRAZIONE SUL PORTALE

https://www.youtube.com/watch?v=mKjvdyNbI4s

CONCLUSIONI

NIS 2 manda un messaggio chiaro alle aziende:

- la cyber security non è più un problema limitato all'ambito IT, ma è una questione che riguarda l'intera organizzazione e deve essere trattata come tale.
- Le misure tecniche, operative e organizzative adottate dai soggetti in perimetro dovranno pertanto essere adeguate e proporzionate ai rischi identificati.
- Le misure adottate dovrebbero mirare a proteggere i sistemi informatici e di rete da attacchi, prevenire o ridurre al minimo l'impatto degli incidenti e garantire la continuità dei servizi.
- Le misure di gestione dei rischi di cyber sicurezza di cui all'art. 21 devono essere comprensive e includere, tra l'altro, politiche di **analisi dei rischi**, strategie per la **gestione degli incidenti**, piani di continuità operativa, **sicurezza della catena di approvvigionamento**, e pratiche di igiene informatica.
- La valutazione della supply chain sarà parte integrante e fondamentale.

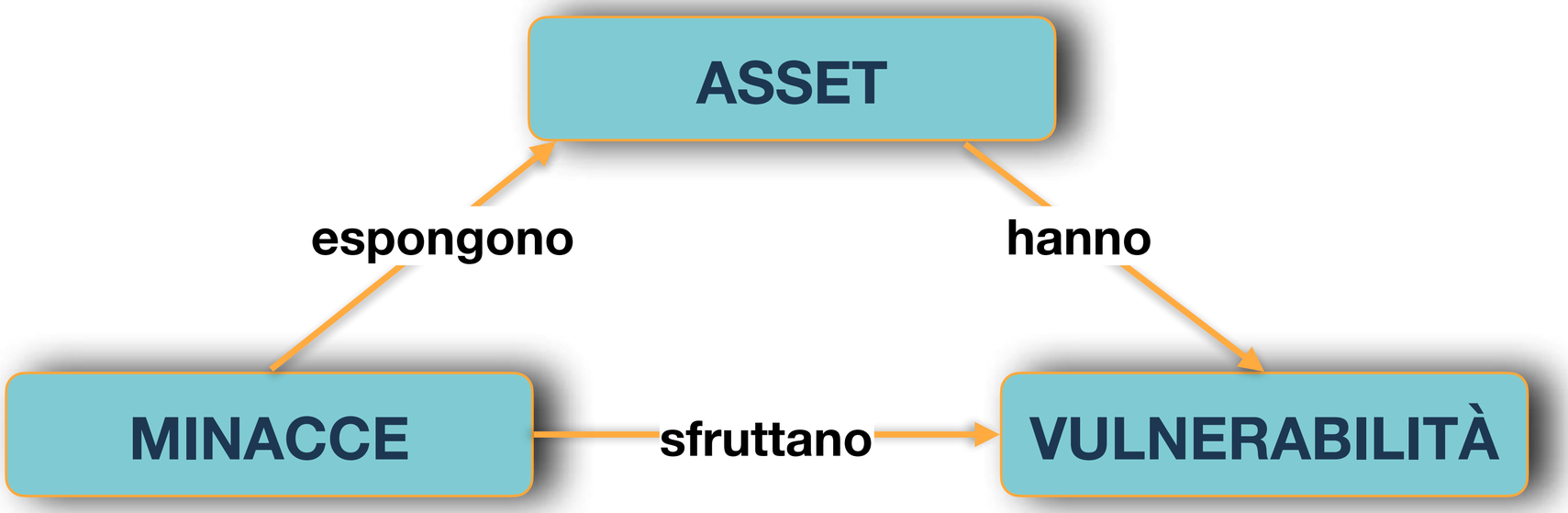
IN CONCLUSIONE

Se un’azienda è sottoposta a NIS deve iniziare a mettere in programma questi interventi di cyber sicurezza, senza attendere le scadenze di legge.

Essi andrebbero applicati comunque, cioè non perché ce lo richiede una norma: la sicurezza delle reti e la sicurezza informatica devono essere considerate **misure necessarie per la salute (e la sopravvivenza!) di un’organizzazione, prima ancora che per una compliance normativa.**

La gestione del rischio IT come elemento centrale della Sicurezza Informatica (e in ogni normativa)

LA VALUTAZIONE DEI RISCHI



La valutazione dei rischi inizia “qualificando” i rischi attraverso i fattori da cui dipendono: Asset, Minacce e Vulnerabilità.

Gli ASSET sono esposti a rischi (incidenti) a causa delle MINACCE che agiscono sfruttando le VULNERABILITÀ presenti negli asset stessi.

SICUREZZA DELLE INFORMAZIONI = DATI

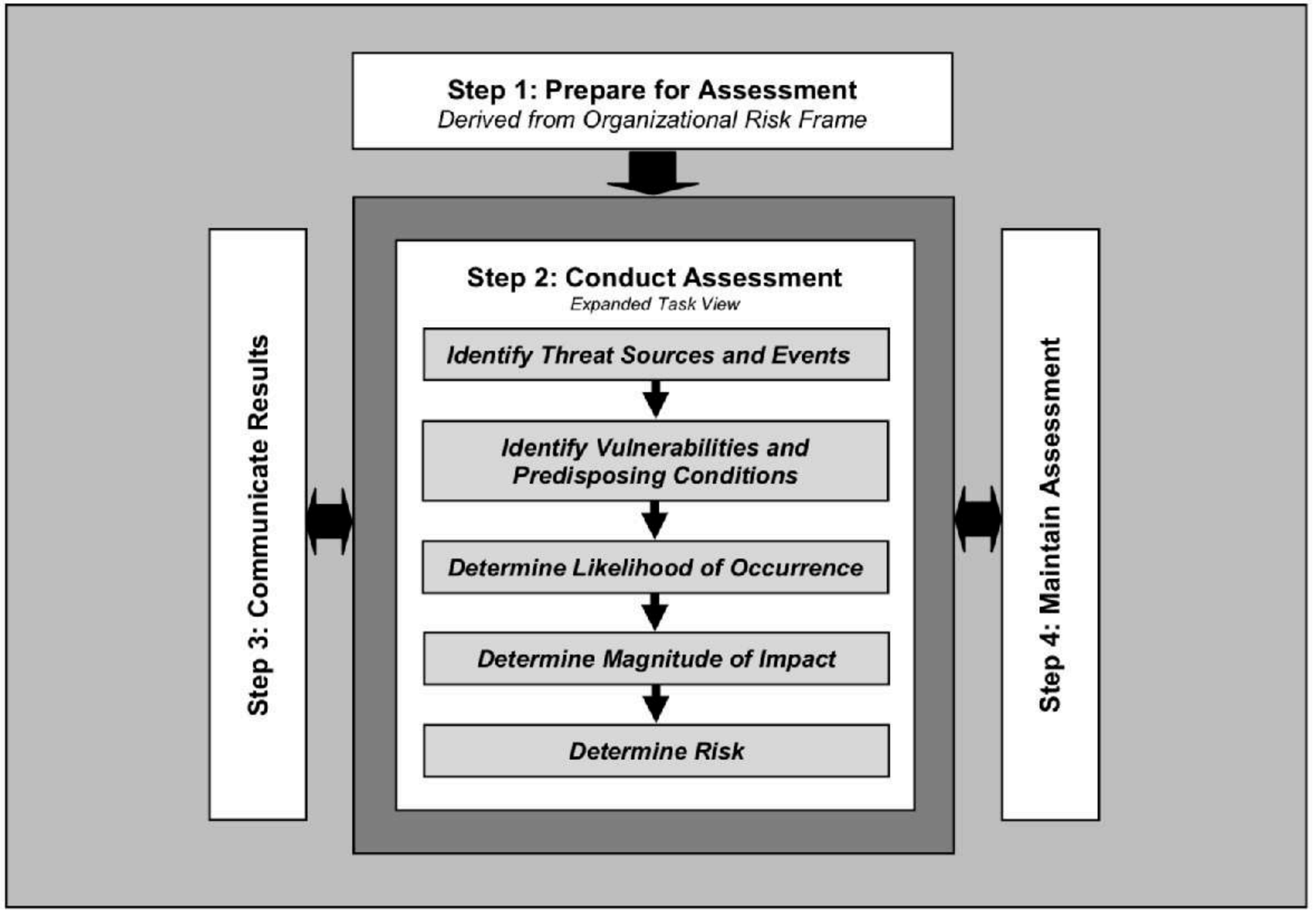
Sicurezza (dal latino «sine cura») significa essere esenti da pericoli; nell'ambito dei sistemi può essere definita come la "*conoscenza che l'evoluzione di un sistema non produrrà stati indesiderati*".

L'Informazione (etim. da informare, dare forma) è un concetto astratto, che viene comunemente identificato con il *significato* di un messaggio.

Sicurezza delle informazioni significa assicurare la riservatezza, integrità e disponibilità delle informazioni (ovvero degli asset informativi).

- **Riservatezza**: garantisce che l'asset informativo è accessibile solamente a coloro che hanno l'autorizzazione ad accedervi;
- **Integrità**: garantisce l'accuratezza e la completezza dell'asset informativo e dei metodi di elaborazione;
- **Disponibilità**: garantisce che gli utenti autorizzati possono accedere all'asset informativo quando vi è necessità.

LA VALUTAZIONE DEI RISCHI



NIST SP 800-30 - FIGURE 5: RISK ASSESSMENT PROCESS

RAF: RISK APPETITE FRAMEWORK

Circolare 285 BdI - Parte I - Titolo IV - Capitolo 3 - Allegato C – Il Risk Appetite Framework

*"**Risk Appetite Framework**" ("RAF": sistema degli obiettivi di rischio): definisce la **determinazione della propensione al rischio**, le soglie di tolleranza, i limiti di rischio, le politiche di governo dei rischi, i processi di riferimento necessari per definirli e attuarli*

*risk tolerance (**soglia di tollerenza**)*: la devianza massima dal *risk appetite* consentita; assicura margini sufficienti per operare, anche in condizioni di stress, entro il massimo rischio assumibile.

*risk appetite (**obiettivo di rischio** o **propensione al rischio**)*: il livello di rischio (complessivo e per tipologia) che la banca intende assumere per il perseguimento dei suoi obiettivi strategici

*risk capacity (**massimo rischio assumibile**)*: il livello massimo di rischio che una banca è tecnicamente in grado di assumere

Analisi Qualitativa: Probabilità e Impatto

ANALISI QUALITATIVA: PROBABILITÀ E IMPATTO

Il “Risk Management” considera le due principali dimensioni connesse al rischio:

P = la probabilità di accadimento

I = l’intensità dell’impatto (la gravità)

Il rischio R è espresso da:

$$R = f(P, I) = (\text{Probabilità}) \times (\text{Impatto})$$

ANALISI QUALITATIVA: PROBABILITÀ E IMPATTO

Quindi i passi per la gestione del rischio sono:

A. valutazione della probabilità di accadimento (P)

B. valutazione dell'intensità dell'impatto (I)

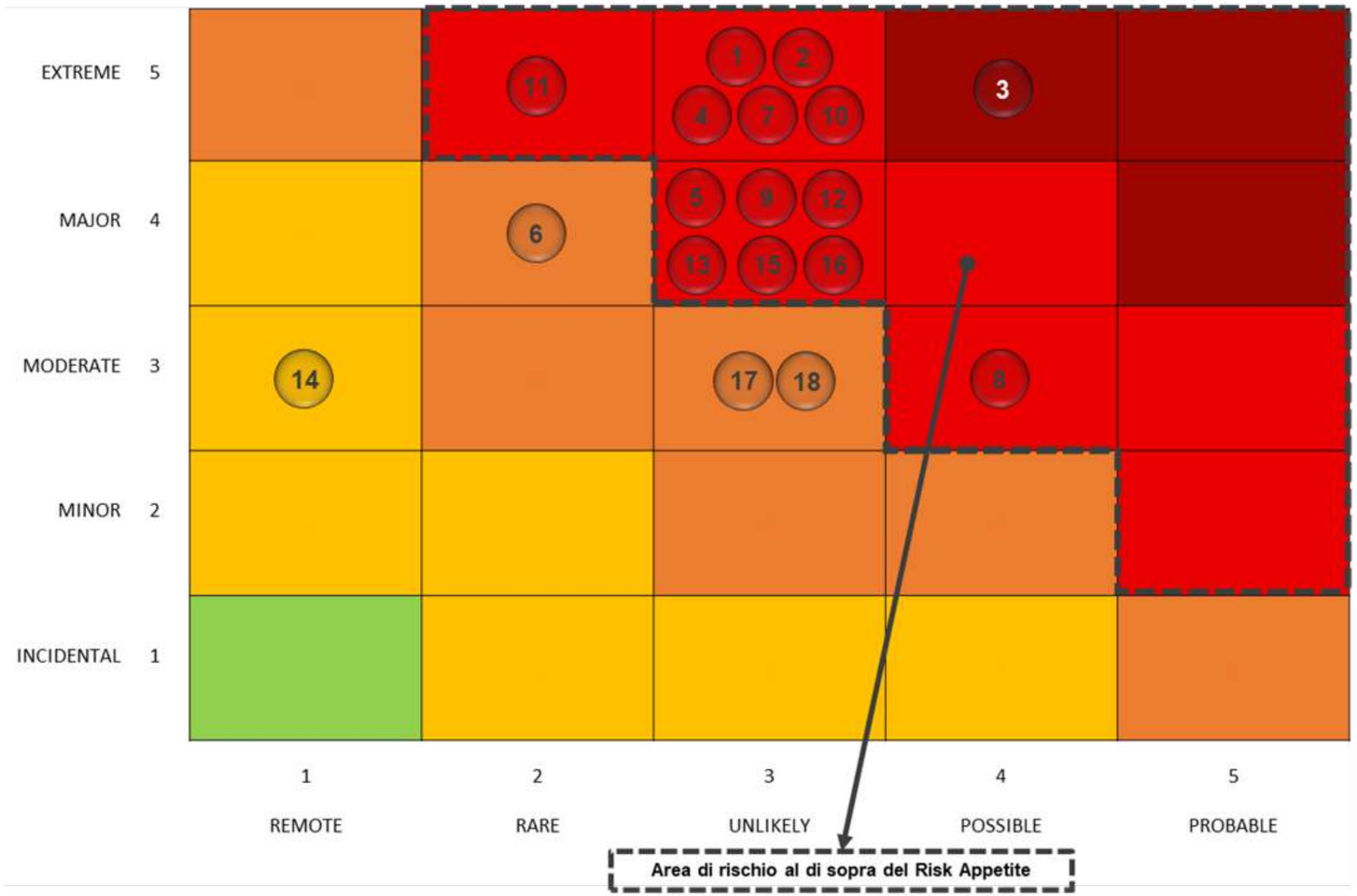
C. valutazione del rischio

D. trattamento del rischio

ANALISI QUALITATIVA: L'APPROCCIO EMPIRICO
LA MATRICE DEL RISCHIO O MATRICE DI PROBABILITÀ

Probabilità		Impatto				
		1 Insignificante	2 Minore	3 Moderato	4 Maggiore	5 Catastrofico
	5 Quasi certo	5 Rischio Medio	10 Rischio Medio	15 Rischio Alto	20 Rischio Alto	25 Rischio Alto
	4 Probabile	4 Rischio Basso	8 Rischio Medio	12 Rischio Medio	16 Rischio Alto	20 Rischio Alto
	3 Possibile	3 Rischio Basso	6 Rischio Medio	9 Rischio Medio	12 Rischio Medio	15 Rischio Alto
	2 Remoto	2 Rischio Basso	4 Rischio Basso	6 Rischio Medio	8 Rischio Medio	10 Rischio Medio
	1 Improbabile	1 Rischio Basso	2 Rischio Basso	3 Rischio Basso	4 Rischio Basso	5 Rischio Medio

RISK HEATMAP



Una volta definiti sulla matrice (**Heatmap**) i livelli di rischio degli asset analizzati

dovremo trattare il rischio per "spostare" i livelli di rischio al di sotto della soglia di accettabilità (**Risk Appetite**)

Il Trattamento del rischio

TRATTAMENTO DEL RISCHIO

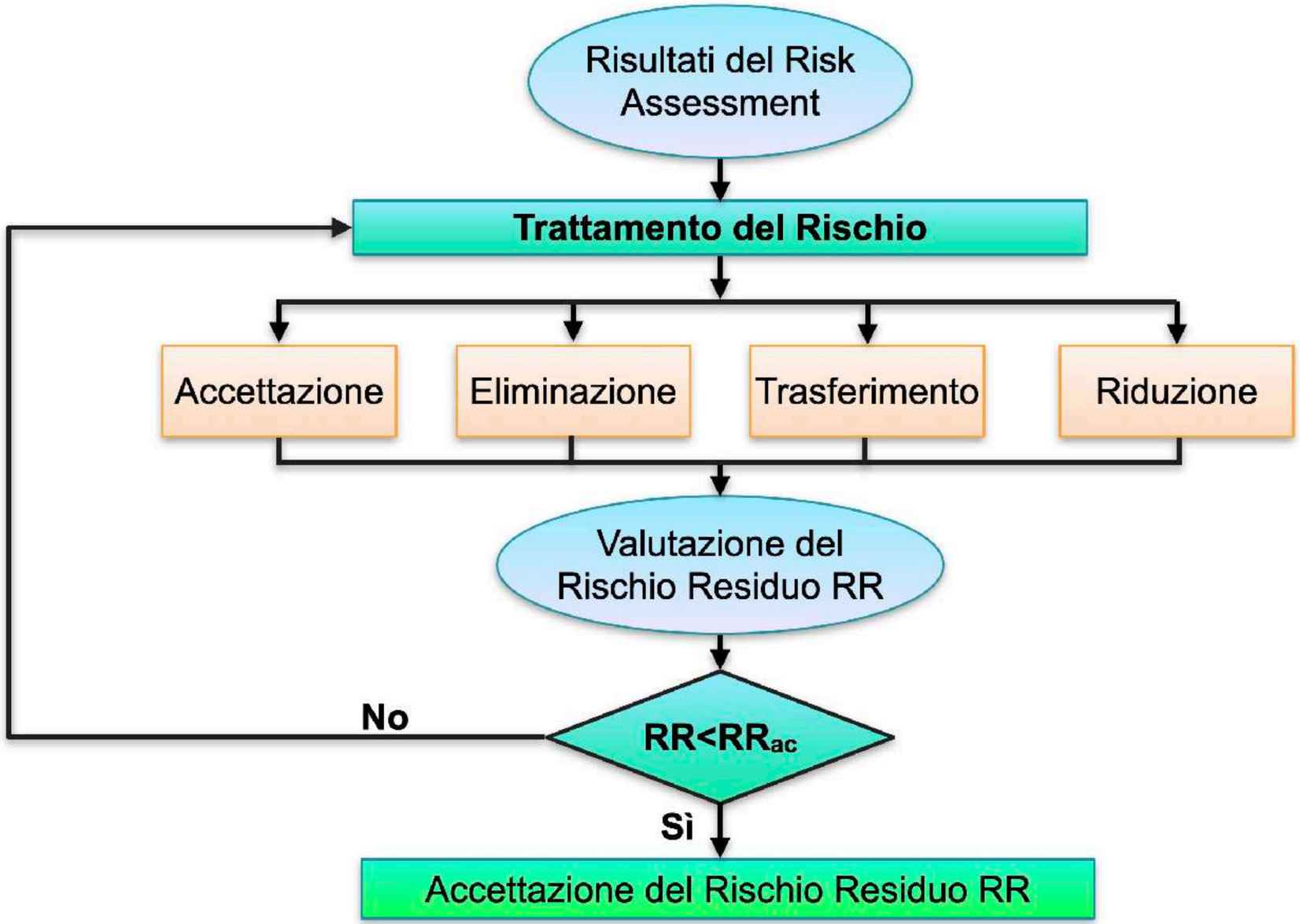
Accettazione del rischio: viene presa la decisione di accettare i rischi perché compatibili con i criteri adottati e/o perché il costo del trattamento del rischio è ritenuto troppo elevato (Analisi costi/benefici).

Eliminazione del rischio: l'attività o la condizione che dà luogo al rischio deve essere evitata e/o eliminata.

Trasferimento del rischio: il rischio deve essere trasferito a terzi in grado di gestire più efficacemente il rischio, a seconda della valutazione del rischio stesso (p.es.: trasferimenti dati in Cloud).

Riduzione (mitigazione) del rischio: il livello di rischio deve essere ridotto attraverso interventi prestabiliti, in modo che il rischio residuo possa essere rivalutato come accettabile.

TRATTAMENTO DEL RISCHIO



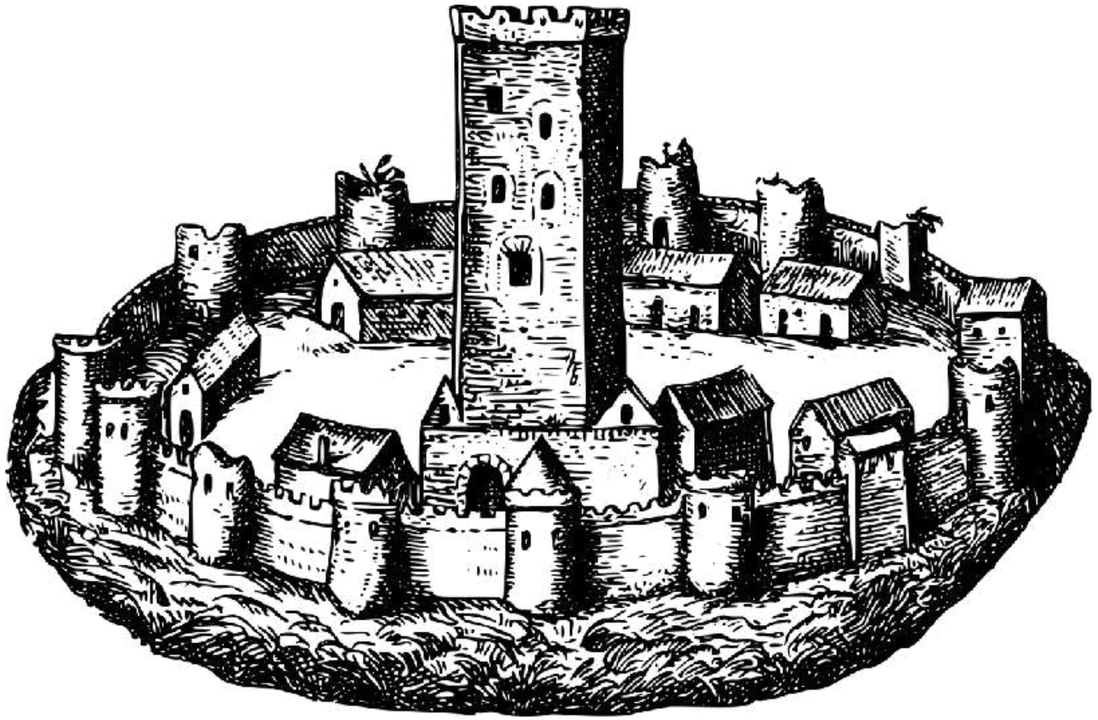
Mettere in pratica la Cybersecurity in azienda: quali sono le misure da adottare

ATTACKER MINDSET:
PENSA COME PENSA L'ATTACCANTE

"Chi conosce il proprio nemico e conosce se stesso potrà affrontare senza timore cento battaglie."

Sun Tzu, "L'arte della guerra" (544-496 a.C.)

IL “TEOREMA DEL FORTINO”



Il “Teorema del Fortino” oggi non è più valido perché:

- ☑ I Devices mobili sono esterni al perimetro aziendale
- ☑ I dati sono salvati sul Cloud e su server esterni
- ☑ I Social Network sono esterni al perimetro aziendale
- ☑ Lo Smart Working…

Modello ZERO TRUST

«Fidarsi è bene, non fidarsi è meglio»

ZERO TRUST ARCHITECTURE (ZTA):

presuppone che non ci sia alcuna fiducia implicita concessa alle risorse o agli account utente basati esclusivamente sulla loro posizione fisica o di rete (cioè, reti locali rispetto a Internet) o basati sulla proprietà delle risorse (aziendale o personale).

“Dentro” e “Fuori” cambia poco in termini di sicurezza.

Si spostano le difese da perimetri statici, basati sulla rete, per concentrarsi su utenti, beni e risorse. Debbo autenticare ogni utente, dispositivo e flusso e costruire una connessione sicura a livello più alto.

L'autenticazione e l'autorizzazione (sia del soggetto che del dispositivo) sono funzioni discrete eseguite prima di stabilire una sessione con una risorsa aziendale.

La ZTA è una risposta alle tendenze di collegare alla rete aziendale utenti remoti, con il proprio dispositivo (BYOD) e risorse basate sul cloud che non si trovano all'interno di un confine di rete di proprietà dell'azienda.

https://www.nist.gov/publications/zero-trust-architecture

IL PERICOLO ARRIVA DALL'INTERNO: "SHADOW IT"

È qualsiasi software, dispositivo o servizio utilizzato su una rete aziendale all'insaputa del reparto IT.

Oltre l'80% dei dipendenti ammette di utilizzare applicazioni SaaS non autorizzate sul lavoro.

La maggior parte delle volte, le intenzioni di questi dipendenti non sono maliziose,
ma Gartner ha affermato che nel 2020 un terzo dei cyberattacchi aziendali di successo sono lanciati su applicativi "Shadow IT".

Lo Shadow IT è cresciuto in modo esponenziale in periodo di **Smart Working**, anche a causa dell'aumento di adozione di applicazioni consumer per un utilizzo professionale.

Anche una chiavetta USB, se non autorizzata, diventa "Shadow IT".

Attenzione anche al SW senza licenza: **reato ai sensi D.Lgs. 231/2001** (art.25 novies: delitti in materia di violazione del diritto d'autore)

“PRINCIPLE OF LEAST PRIVILEGE” (POLP)

Jerome Saltzer (1975) definiva così quello che in inglese viene chiamato “**Principle of Least Privilege**” (POLP):

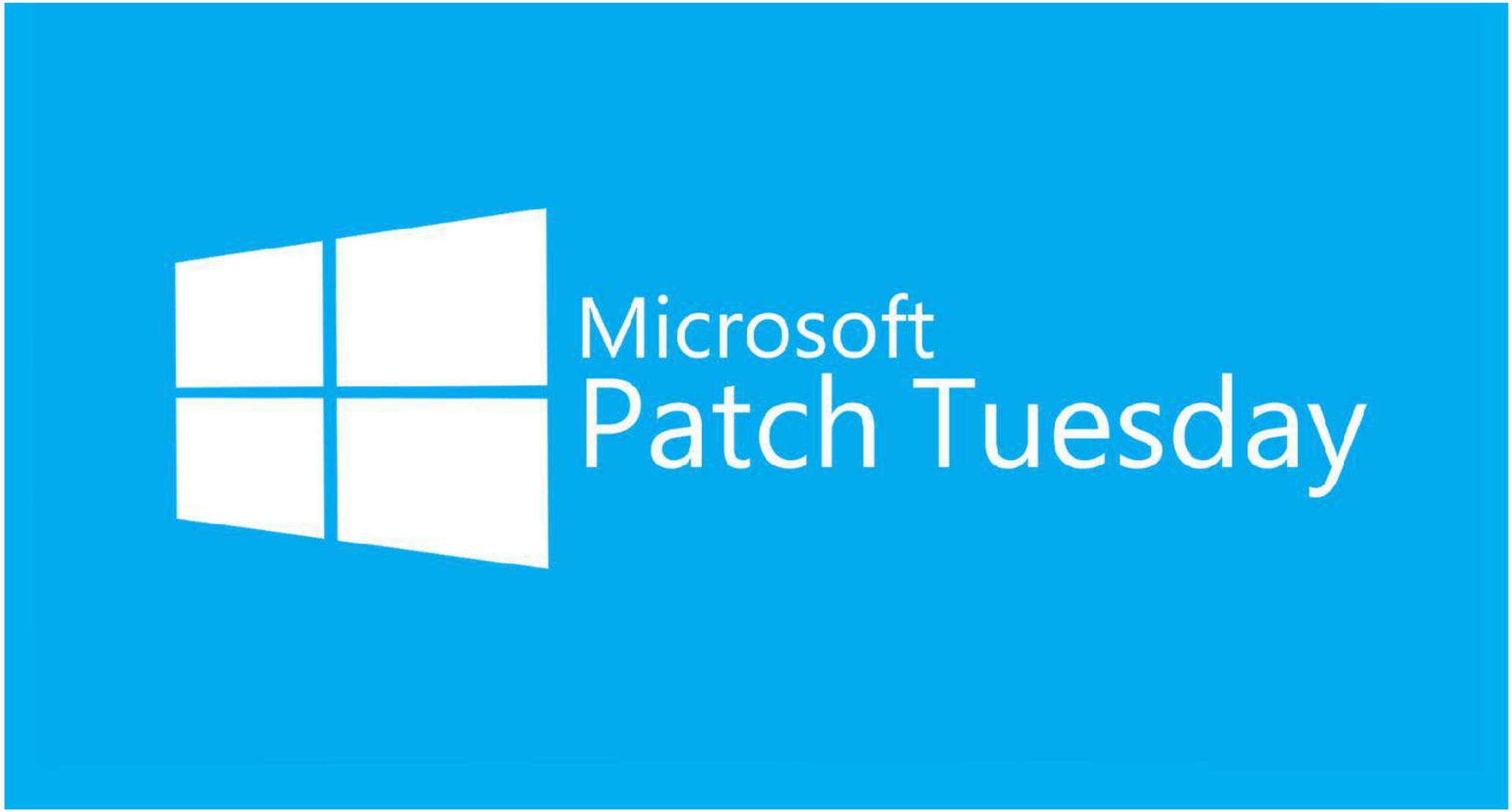
“Ogni programma ed ogni utente del sistema dovrebbero operare utilizzando il **più basso livello di “diritti”** necessari a portare a termine il proprio compito”.

In altre parole:

- ☑ **Limitare i privilegi degli utenti.**
- ☑ **Limitare il numero e l’utilizzo di account privilegiati.**
- ☑ **Separare e gestire gli account con privilegi.**
- ☑ **Evitare di esporre credenziali privilegiate su sistemi meno privilegiati e potenzialmente compromessi.**

Patch Management

PATCH TUESDAY…



PATCH TUESDAY…

“Patch Tuesday, Exploit Wednesday”

Molti sfruttamenti delle falle nei vari sistemi avvengono poco dopo la pubblicazione di una patch.
Analizzando la patch medesima, gli Hackers possono capire con facilità come approfittare delle vulnerabilità evidenziate (con tecniche di “reverse engineering”) ed attaccare i sistemi che non sono stati ancora patchati.

In media, sono necessari solo 14 giorni per rendere disponibile un exploit dopo che una vulnerabilità è stata divulgata pubblicamente.

PATCH TUESDAY…

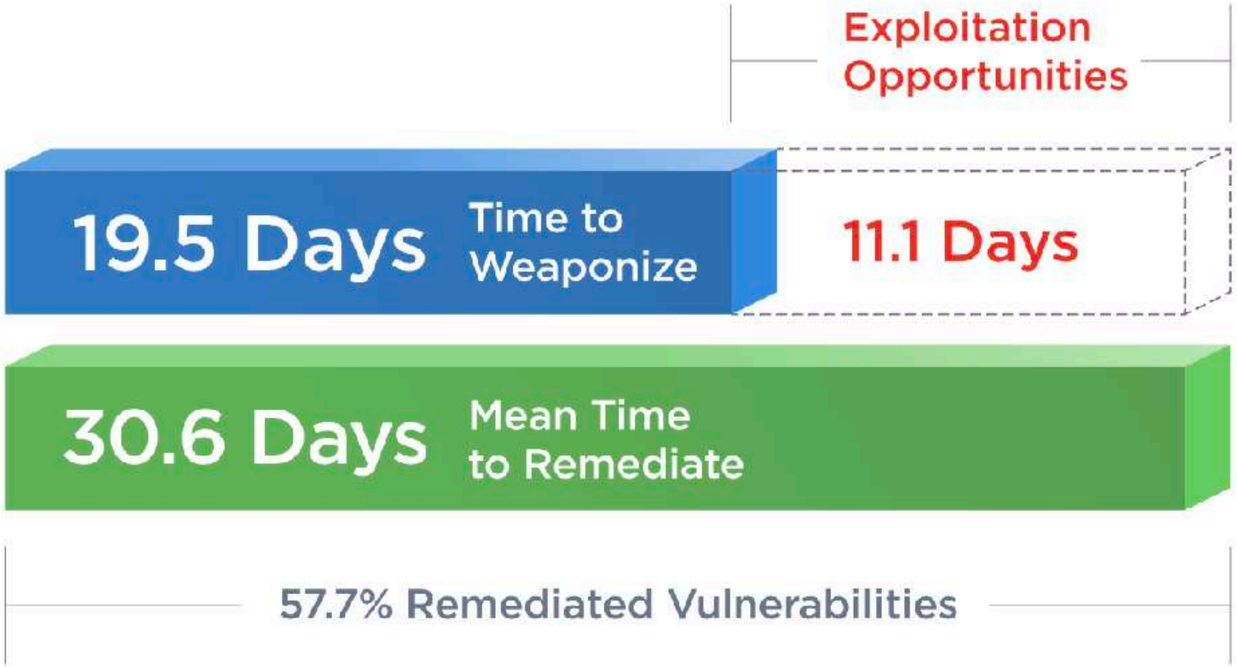
“Patch Tuesday, Exploit Wednesday”

Gartner riporta che:
il 90% degli attacchi che hanno successo vengono portati contro vulnerabilità note per le quali sono già disponibili patch o configurazioni sicure.
Statistica VERIZON: 85% degli attacchi andati a buon fine dovuti a solo 10 vulnerabilità di cui 6 note da 10 anni.

Secondo il **Rapporto CLUSIT 2025** lo sfruttamento delle vulnerabilità rappresenta **il 15% dei vettori d’attacco,** in crescita rispetto agli anni precedenti.

PATCH TUESDAY…

“Patch Tuesday, Exploit Wednesday”



In media, le vulnerabilità vengono patchate entro 30,6 giorni, ma solo nel 57,7% dei casi.

Queste stesse vulnerabilità vengono sfruttate dagli aggressori in media in 19,5 giorni.

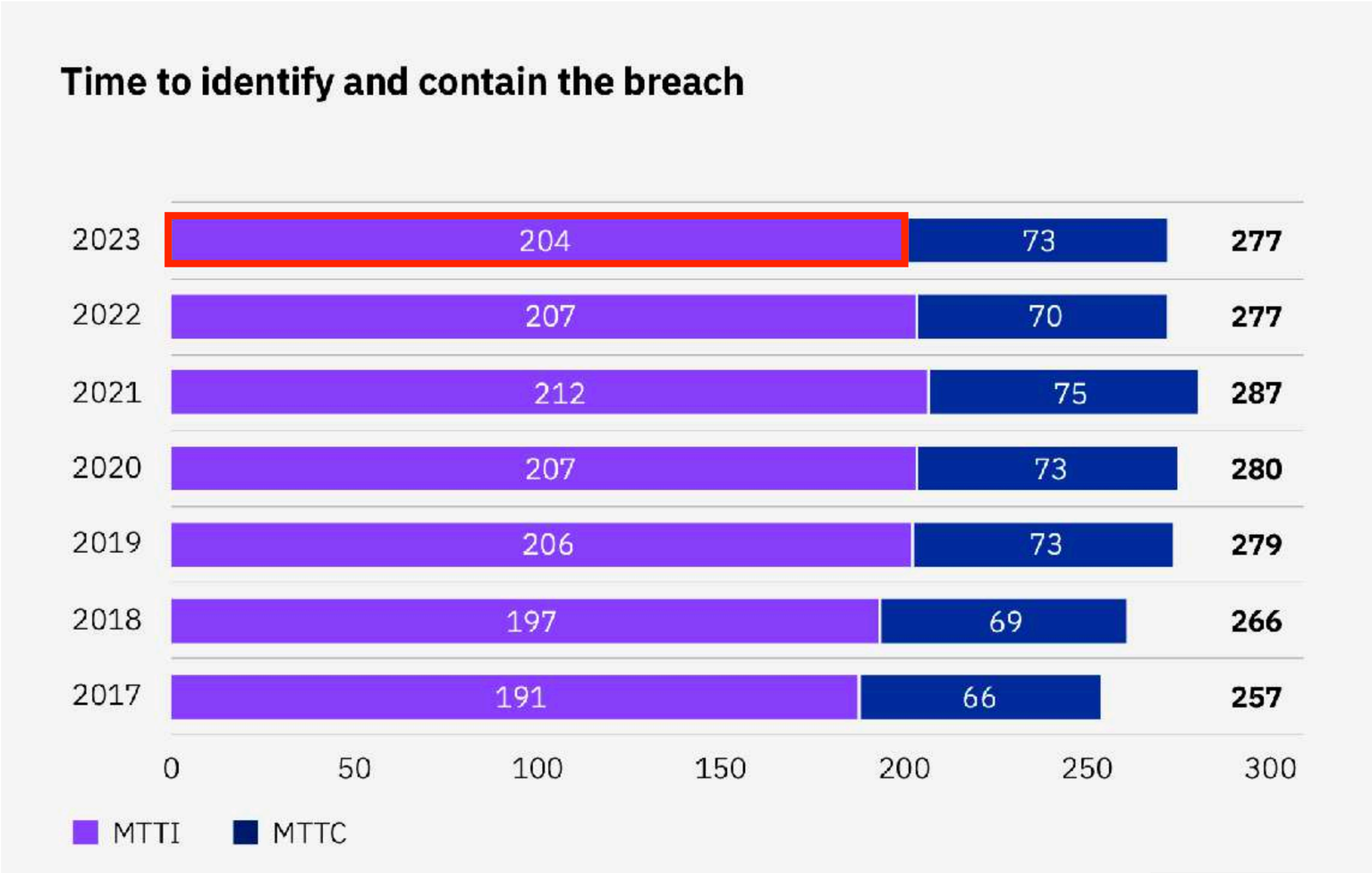
Ciò significa che gli aggressori hanno a disposizione **11,1 giorni di finestra di sfruttamento** prima che le organizzazioni inizino ad applicare le patch.

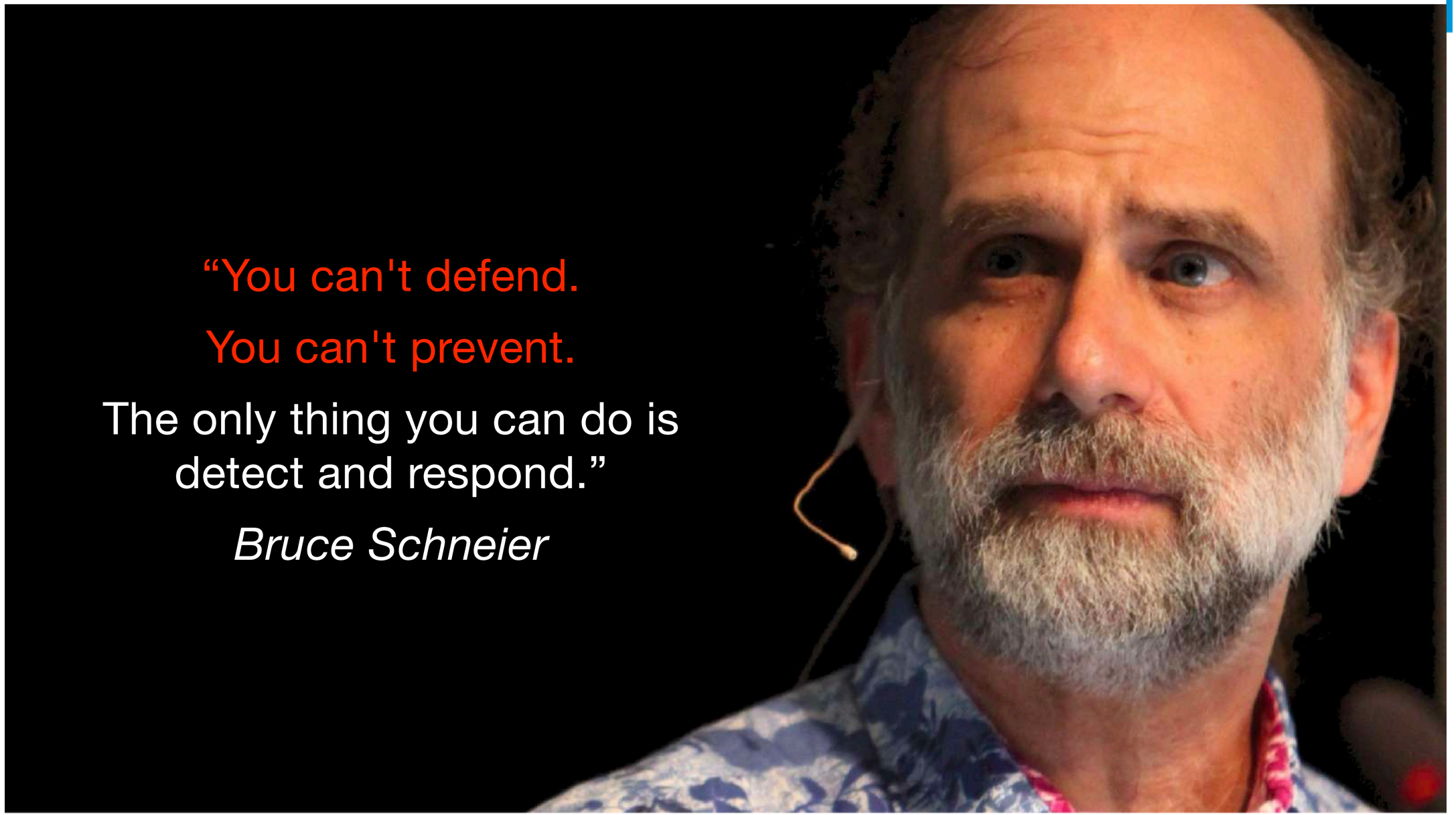
L’importanza della DETECTION (rilevare l’incidente)

QUAL È IL PROBLEMA?

Il tempo medio complessivo per **identificare** e **contenere** una violazione dei dati è stato di 277 giorni (204 + 73).

Fonte: IBM Cost of a Data Breach Report 2023





IMPORTANZA DELLA GESTIONE EVENTI E INCIDENTI

- ☑ Finora l'attenzione è stata fortemente sulla **PREVENTION**.
- ☑ Lo scenario attuale richiede di considerare minacce aggressive che riescono a superare le nostre difese, e che devono essere individuate e contenute: **DETECTION.**

MONITORAGGIO EVENTI E INCIDENTI

QUALSIASI ATTACCO CREA RUMORE

Ogni organizzazione deve saper rilevare il livello di rumore quale causa scatenante di una prima reazione da parte dei sistemi a difesa del perimetro aziendale (IDS, SIEM, EDR).

La chiave per aumentare il proprio livello di sicurezza a difesa del perimetro è capire cosa si nasconde dietro al rumore che ogni Hacker prima o poi emette con le proprie azioni.

Riconoscere l'attaccante sin dal momento in cui inizia la fase di Information Gathering.

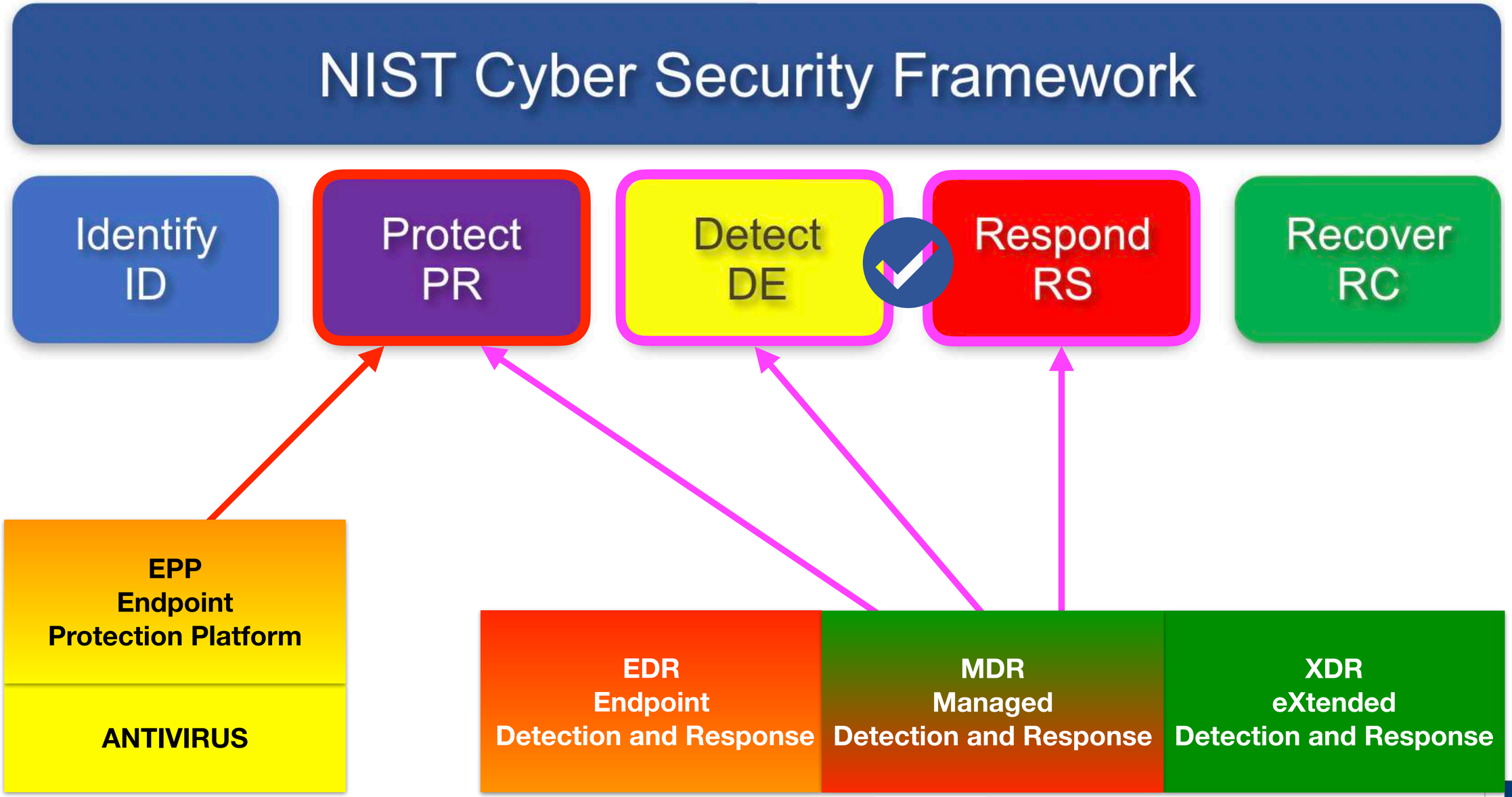
EPP, EDR, MDR, XDR: COSA SONO?

EPP	Endpoint Protection Platform
EDR	Endpoint Detection and Response
MDR	Managed Detection and Response
XDR	eXtended Detection and Response

EPP, EDR, MDR, XDR: COSA SONO?

XDR **eXtended** **Detection and Response**	Fornisce una visione molto più robusta su reti, carichi di lavoro cloud, server ed endpoint. integra la visibilità della sicurezza attraverso l'**intera infrastruttura**, compresi gli endpoint, l'infrastruttura cloud, i dispositivi mobili , ecc. Pannello unico di visibilità e gestione semplifica la gestione della sicurezza e l'applicazione di politiche di sicurezza coerenti in tutta l'azienda
MDR **Managed** **Detection and Response**	Estende una componente umana che migliora le piattaforme EDR, con un team di esperti di sicurezza. MDR fornisce monitoraggio continuo delle minacce, rilevamento e attività di risposta 24x7x365. Il tempo medio di rilevamento (MTTD) e il tempo medio di risposta (MTTR) ridotti garantiscono un rilevamento e una risposta più rapidi alle minacce avanzate. Ci sono diversi tipi di offerte di servizi MDR (aspetti commerciali da valutare)
EDR **Endpoint** **Detection and Response**	Monitoraggio continuo e raccolta di dati di attività dagli endpoint che potrebbero indicare una minaccia, Analizza questi dati per identificare i modelli di minaccia. **Threat intelligence: MITRE ATT&CK framework.** Protezione **attiva:** risponde **automaticamente** alle minacce identificate per rimuoverle o contenerle, Informa il team di sicurezza o il team SOC quando viene riconosciuta una minaccia, Anche strumento di analisi forense per ricercare le minacce identificate e cercare attività sospette.
EPP **Endpoint** **Protection Platform**	Protezione **passiva** degli endpoint Previene le minacce tradizionali come il malware conosciuto e le minacce avanzate come gli attacchi fileless, il ransomware e le vulnerabilità zero-day **blocklisting:** blocca o permette l'accesso solo a specifici indirizzi IP, URL, applicazioni e processi
ANTIVIRUS	Protezione solo **reattiva**: signature based (basata sulle firme dei virus noti) Rileva le le minacce usando firme di malware conosciute. Non più sufficiente!

EPP, EDR, MDR, XDR: COSA SONO?



EPP, EDR, MDR, XDR: COSA SONO?

XDR **eXtended** **Detection and Response**	Fornisce una visione molto più completa su reti, cloud, server ed endpoint. Integra la visibilità della sicurezza attraverso l'**intera infrastruttura**, compresi gli endpoint, l'infrastruttura cloud, i dispositivi mobili , ecc.: analisi del traffico interno ed esterno, intelligence integrata sulle minacce, rilevamento basato sull'apprendimento automatico. Pannello unico di visibilità e gestione semplifica la gestione della sicurezza e l'applicazione di politiche di sicurezza coerenti in tutta l'azienda

La definizione di Gartner è:

"XDR è uno strumento di rilevamento delle minacce alla sicurezza e di risposta agli incidenti, basato su SaaS e specifico per ogni fornitore, che integra in modo nativo più prodotti di sicurezza in un sistema operativo di sicurezza coeso che unifica tutti i componenti di sicurezza con licenza".

XDR è un'evoluzione dell'EDR che amplia la portata del rilevamento ben oltre gli endpoint.

XDR è più economico e meno complesso di uno strumento SIEM ed è più ampio e più capace dell'EDR.

XDR (EXTENDED DETECTION AND RESPONSE)

I PIÙ NOTI

- **SentinelOne Singularity XDR**
- **Bitdefender GravityZone XDR**
- **Elastic Security for XDR** (codice open source)
- **Sistema XDR Microsoft** (combina diverse suite di lavoro, quali Microsoft Sentinel, Microsoft 365 Defender e Microsoft Defender for Cloud)
- **Cybereason XDR**
- **CrowdStrike Falcon Insight XDR**
- **Palo Alto Networks Cortex XDR**
- **Cynet 360 AutoXDR**
- **VMware Carbon Black XDR**
- **Acronis Security + Extended Detection and Response (XDR)**

SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT):

è uno strumento (software) che raccoglie i log degli eventi che accadono all'interno della rete e sui vari sistemi di sicurezza.

Esegue il monitoraggio fornendo una correlazione e aggregazione tra essi.

L'interfaccia è una console (dashboard) che fornisce una rappresentazione dei dati sotto forma di diagrammi o altri modelli, consentendo agli analisti di individuare rapidamente attività anomale.

SOC (SECURITY OPERATIONS CENTER):

è un'unità centralizzata di analisti della sicurezza che si occupano di problemi di sicurezza, utilizzando una serie di strumenti.

Uno degli strumenti principali utilizzati dagli analisti della sicurezza è un SIEM.

SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)
LE FUNZIONI

SIEM aggrega dati significativi provenienti da molteplici fonti,
poi individua deviazioni, anomalie rispetto alla norma,
e fa scattare azioni appropriate per risolvere i problema di sicurezza rilevati.

Compliance Normativa
La normativa vigente prevede obblighi di raccolta dei LOG, (es.: GDPR, Amministratori di Sistema)

Security Monitoring
Correlazione dei dati in tempo reale e la presenza di regole, consentono di identificare attacchi fino ai più sofisticati come APT.

Dashboard e Reporting
Dashboard centralizzata, che include più eventi sospetti e che consente di produrre report puntuali.

SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)

I PIÙ NOTI

- **Splunk** Enterprise Security
- **IBM QRadar**
- **Microsoft Sentinel**
- **Wazuh** (open source SIEM)
- **ManageEngine** Log360
- **ArcSight** (by Micro Focus/Opentext)
- **LogRhythm**
- **AlienVault USM** (AT&T Cybersecurity)
- **McAfee Enterprise Security Manager**
- **SolarWinds Security Event Manager**
- **Graylog** (open source SIEM)
- **Sumo Logic Cloud SIEM** (Cloud-native SIEM)
- **Elastic SIEM** (open-source SIEM parte di Elastic Stack ELK Stack)

SOC (SECURITY OPERATIONS CENTER)

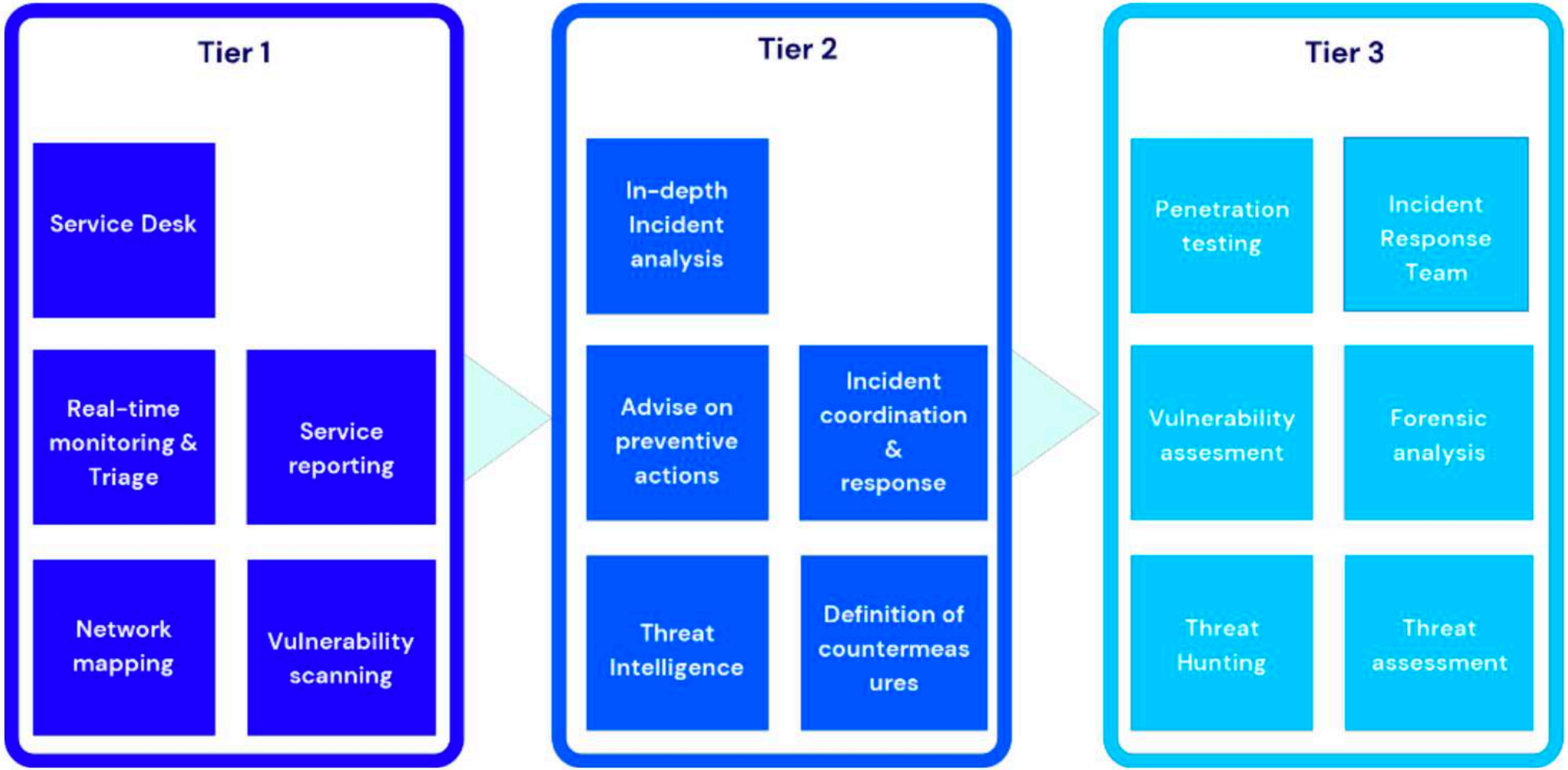
Struttura dove sono centralizzate tutte le informazioni sullo stato di sicurezza dell'IT di un'azienda o di più aziende (nel caso che il SOC appartenga a un Managed Security Service Provider, **MSSP**).

- Nel SOC (livello 1) sono ospitate i sistemi di sicurezza SIEM (Security Information and Event Management).
- Il SOC (livello 2) gestisce anche l'Incident Response (IR).
- Il SOC (livello 3) può fornire anche servizi proattivi per verificare in modo preventivo la sicurezza il livello di protezione dell'organizzazione (Vulnerability assessment, Penetration Test).

NOC (Network Operation Center): può essere integrato nel SOC.

Attenzione: **il SOC gestisce IR, non gestisce la Comunicazione!**

SOC (SECURITY OPERATIONS CENTER)



SIEM, monitoring e reporting

Incident Response (IR): Defense e remediation

Servizi proattivi: VA/PT, forensic

SOC: INTERNO O ESTERNALIZZATO?

SOC interno

- [x] conosce nel dettaglio l'organizzazione e si integra nei diversi processi di gestione
- [x] non comporta in generale la fuoriuscita di informazioni riservate
- [ ] Vede solo gli incidenti della singola organizzazione
- [ ] Ha un costo importante, specialmente se si vogliono garantire i servizi H24

SOC esternalizzato

- [ ] Gestisce l'organizzazione sulla base degli accordi contrattuali e organizzativi, insieme ad altri clienti; i contratti devono essere predisposti con cura in termini di livelli di servizio (SLA)
- [ ] Ha accesso a informazioni riservate e a flussi di eventi interni
- [ ] Ha accesso a configurazioni e servizi critici, quindi comporta un livello molto alto di fiducia
- [ ] È più difficile monitorarne l'efficacia su eventi che non generino disservizi
- [x] Ha informazioni aggregate di più clienti
- [x] **Ha in generale maggiori competenze e strumenti più specialistici**
- [x] **Fornisce tipicamente un servizio H24 a costi ragionevoli**

SOC (SECURITY OPERATIONS CENTER): LE TIPOLOGIE

SOC Gerarchico

Struttura piramidale con competenze crescenti con il ruolo.
Organizzazione con copertura h24 in reperibilità per analisti .
Le figure più pregiate (specialisti/ architetti ecc.) di solito sono ingaggiate fuori orario solo per particolari livelli di escalation.

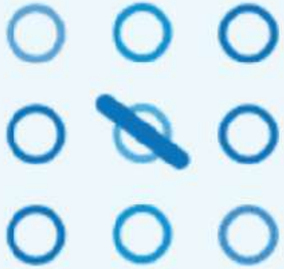
SOC "Follow the Sun"

Struttura «piatta» non piramidale: generalmente non c'è distinzione tra analisti e specialisti in termini di skill.
Garantito il supporto multilingue.
Organizzazione con copertura h24 con passaggio di gestione tra diversi Team.
Supporto in lingua italiana solo in orario lavorativo: possibile difficoltà ad interagire in lingua (inglese) durante la gestione di incidenti complessi.

Backup
e
Disaster Recovery

31 MARZO:
GIORNATA MONDIALE DEL BACKUP

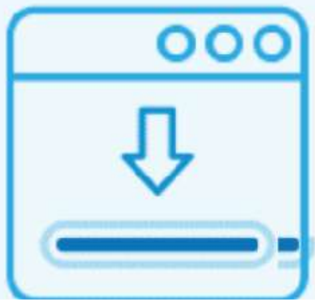
31 MARZO:
GIORNATA MONDIALE DEL BACKUP



30% of people
have never backed up [1]

113 phones
lost or stolen every minute [2]

29% of disasters
are caused by accident [3]



1 in 10 computers
infected with viruses each month [4]

L'IMPORTANZA DEL BACKUP: 1-LA RIDONDANZA

Per prevenire perdite di dati per qualsiasi ragione, fare sempre **copia di sicurezza dei propri dati (almeno il 30% degli utenti NON lo fa!).**

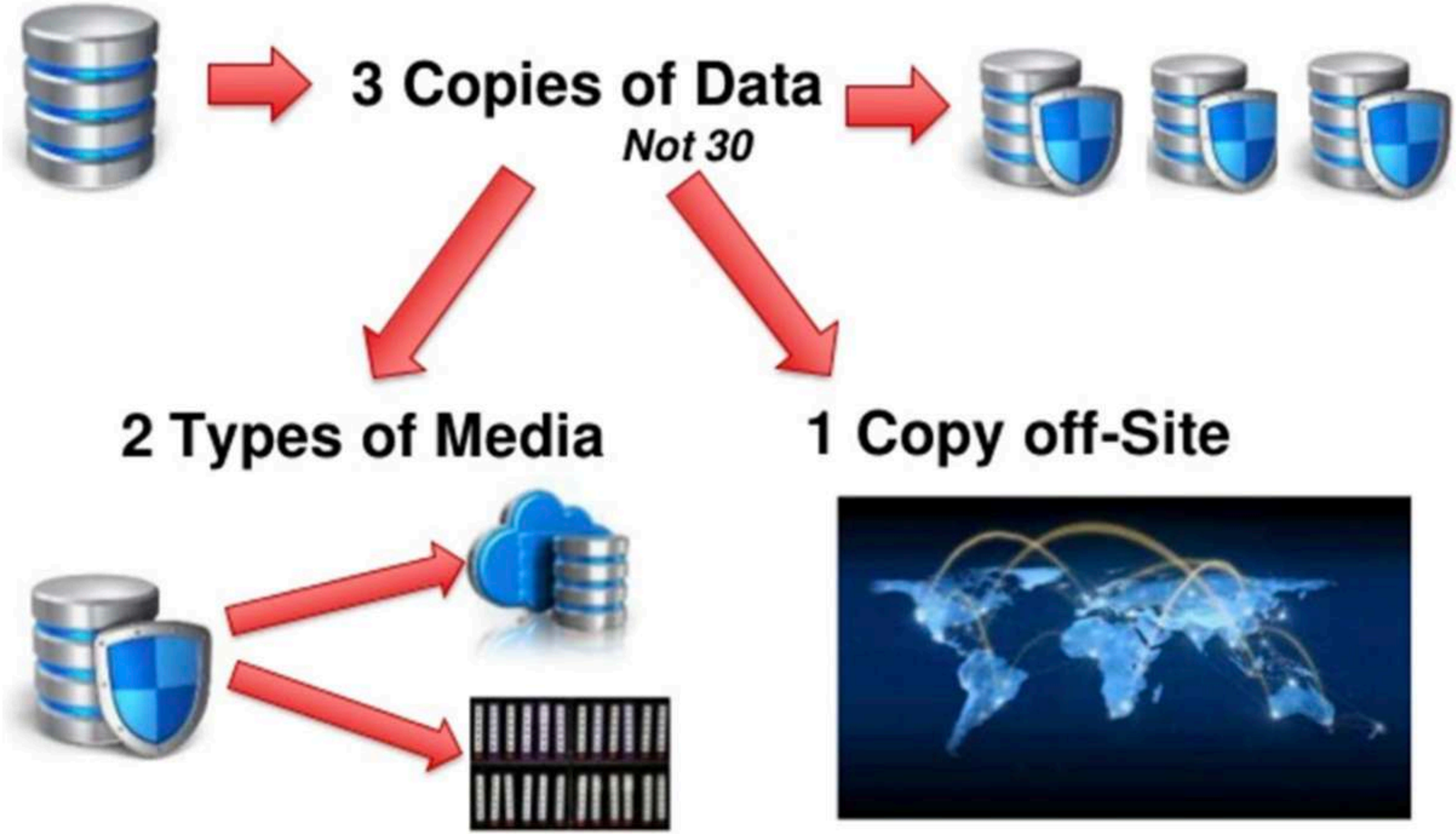
Un buon metodo:
3-2-1 Backup Strategy

✅ **3** copie di ogni dato che si vuole conservare (L'errore più frequente è la presenza di un'unica copia di backup)

✅ **2** copie "onsite" ma su storage differenti (HD, NAS, Cloud,…)

✅ **1** copia in sito remoto "off-site" (ev. Cloud)

3-2-1 BACKUP STRATEGY



L'IMPORTANZA DEL BACKUP: 2-LA VALUTAZIONE

Valutare preventivamente:

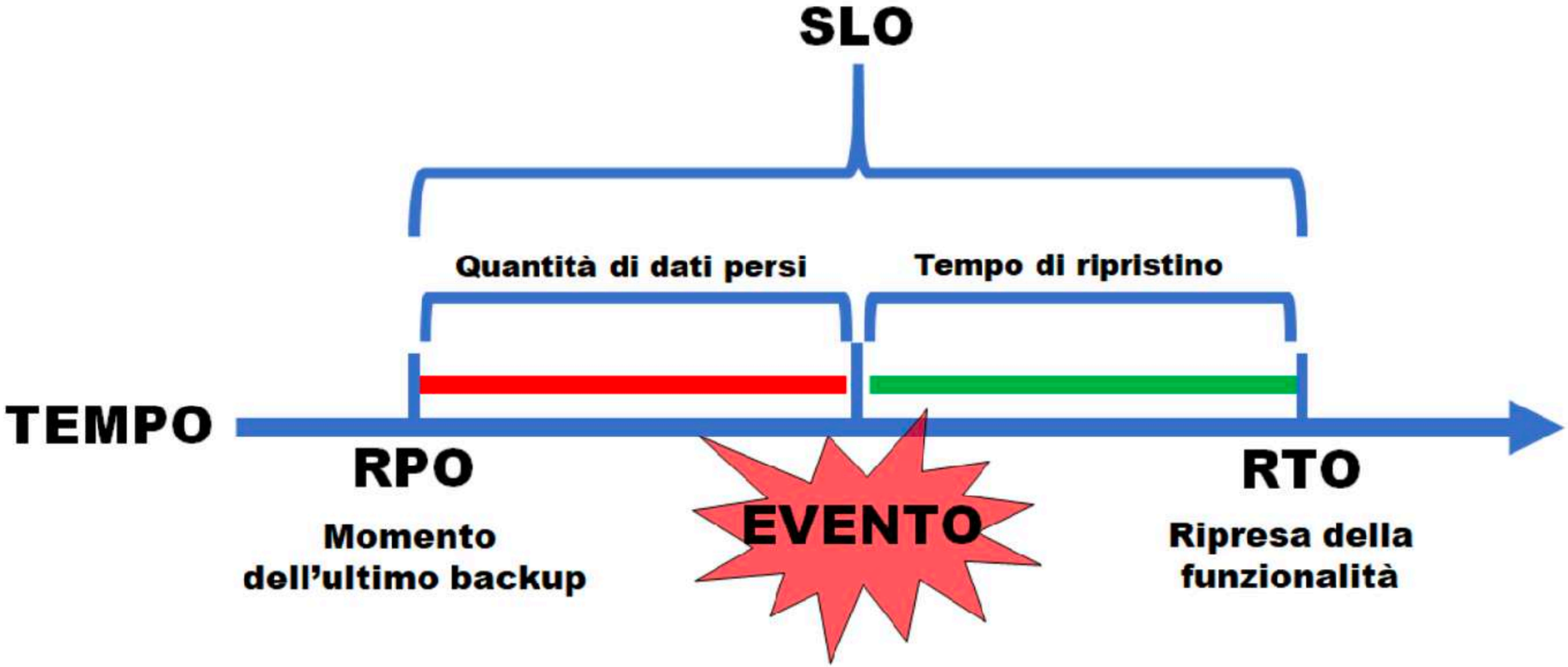
- **Recovery Point Objective (RPO)**: rappresenta il massimo tempo entro il quale deve essere fatto il backup di un dato. Ci indica la misura della massima quantità di dati che siamo disposti a perdere a causa di incidente. Dal RPO discende la scelta della frequenza temporale dei backup.
- **Recovery Time Objective (RTO)**: è il tempo entro il quale l'azienda deve essere in grado di ripristinare la sua operatività. In pratica il tempo massimo che si ritiene tollerabile per un downtime (blocco dell'operatività, MTPD).
- **Data Retention**: tempo di conservazioni dei dati. La data retention stabilisce per quanto tempo i dati salvati andranno conservati prima di essere cancellati.

L'IMPORTANZA DEL BACKUP: 2-LA VALUTAZIONE

Recovery Point Objective (RPO)

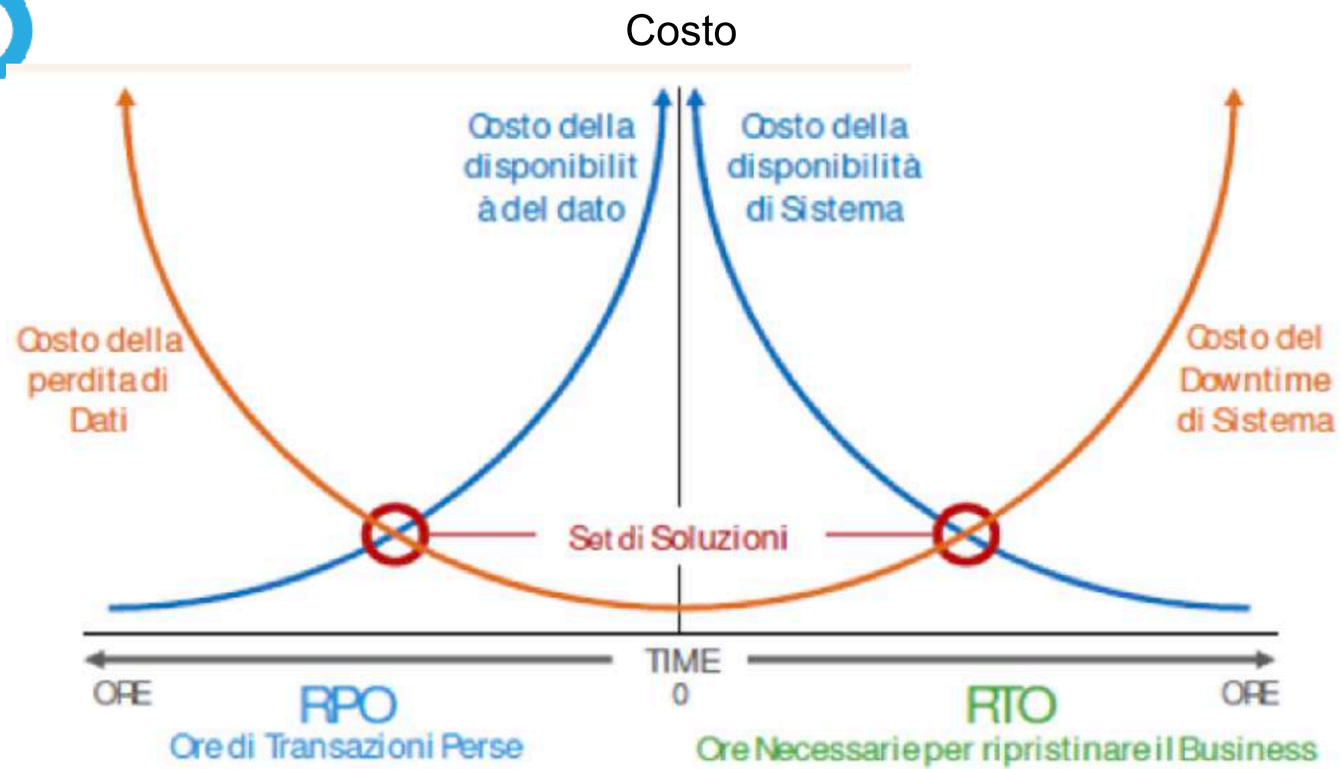
Recovery Time Objective (RTO)

SLO (Service Level Objective) comprende RPO + RTO



Ridurre RPO e RTO ha un costo

L'IMPORTANZA DEL BACKUP: 2-LA VALUTAZIONE



L'ottimizzazione dei tempi RTO e RPO si traduce in un compromesso tra i costi dovuti alla perdita di dati e i costi d'implementazione di un'architettura ad alta affidabilità

Gartner Group propone di classificare i servizi erogati in termini di RTO e RPO:

- **servizi di classe 1:** con RTO e RPO prossimi a zero;
- **servizi di classe 2:** con RTO dell'ordine delle 24 ore, e RPO prossimo a 4 ore;
- **servizi di classe 3:** con RTO dell'ordine delle 72 ore, e RPO prossimo a 24 ore;
- **servizi di classe 4:** con RTO misurabile in giorni, e RPO superiore a 24 ore. I servizi delle prime due classi sono, in generale, quelli definibili "critici".

L'IMPORTANZA DEL BACKUP: 3-LA PROTEZIONE

Nella logica BACKUP 3-2-1 dobbiamo avere una copia Immutabile o Offline

- **Immutabile**: assegnare l'attributo Linux di immutabilità (chattr) al file
  # chattr +i file.txt
- **Offline**: copia su nastro (Linear Tape-Open, LTO Ultrium). Oggi lo standard è LTO-9 con capacità fino a 18 TB e velocità 400 MB/s

NAS E SISTEMI RAID

NAS (Network Attached Storage) sono dei **veri e propri computer** (dotati solitamente di un sistema operativo basato su Linux) che collegandosi alla rete (casa, ufficio, ecc.) **permettono di archiviare e condividere dati e file con gli altri dispositivi**.

CAPACITÀ DI ARCHIVIAZIONE

Dipende dal numero di “Bay” (baie) che sono presenti sul NAS, ciascuna alloggia un HD. Un NAS può avere 2, 4, 6 o anche più alloggiamenti.
Lo spazio totale di archiviazione è inferiore alla somma dello spazio dei dischi inseriti (per il principio della Ridondanza).

NAS E SISTEMI RAID

RIDONDANZA:

Uno dei principali strumenti dei NAS per evitare la perdita dati è la configurazione detta **RAID (Redundant Array of Independent Disks):** è un sistema usato in varie configurazioni per condividere o replicare informazioni tra un gruppo di dischi rigidi.

Va da RAID 1 (conf. minima) a RAID 6.
Permette di gestire senza perdita di dati l'avaria di 1 o 2 dischi.

La configurazione in RAID può ridurre lo spazio totale anche del 50%.

IN CONCLUSIONE…

COSA ABBIAMO DIMENTICATO?

IL “FATTORE UMANO”

“Il fattore umano è veramente l'anello più debole della sicurezza”

(“The Art of Deception” Kevin Mitnick - 2002)

IL “FATTORE UMANO”

Oltre il 90% degli attacchi informatici sono causati dall’ERRORE UMANO

…quindi…

FARE FORMAZIONE !

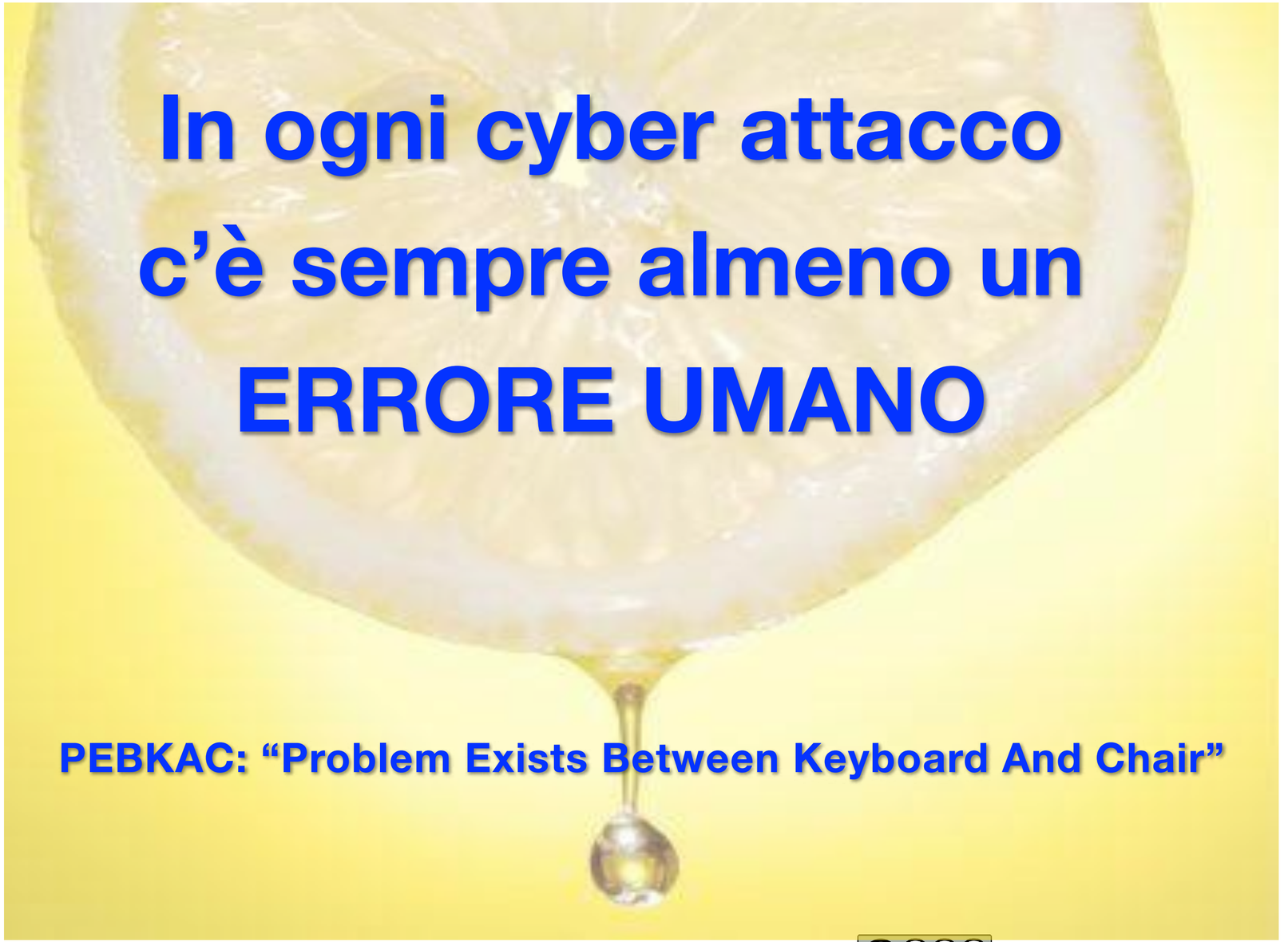
FARE FORMAZIONE !

GDPR Articolo 39 - Compiti del responsabile della protezione dei dati (DPO)

Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

b) …la sensibilizzazione e **la formazione del personale che partecipa ai trattamenti** e alle connesse attività di controllo;

IL SUCCO DEL DISCORSO…



UNIONCAMERE

GRAZIE PER L'ATTENZIONE

cybersec@giorgiosbaraglia.it
www.giorgiosbaraglia.it

punto impresa digitale

DINTEC
CONSORZIO PER L'INNOVAZIONE TECNOLOGICA

SOCIO Clusit
Associazione Italiana per la Sicurezza Informatica