Cyber Security Angels

Presentazione libro Cyber Mindset

13/05/2025

Giovanni Cerrato

Passione

Da sempre appassionato della Cybersecurity e ci lavoro da 13 e... incredibilmente, mi piace ancora!

Sopravvissuto: Agli attacchi hacker e, cosa più difficile, a infinite riunioni noiose

Offensive Security

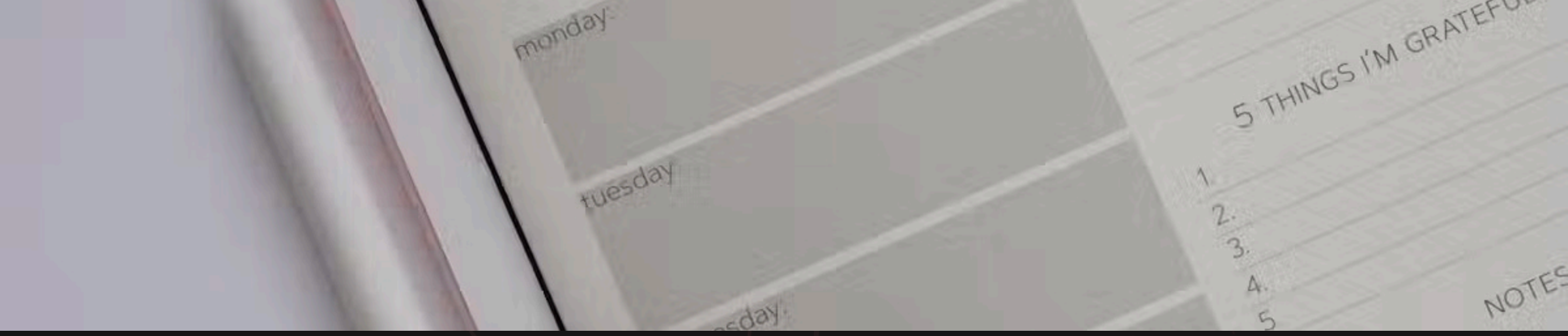
Ho iniziato nell'**offensive security** (sì, quello dove provi a bucare i sistemi... ma con il permesso 😉)

Gestione progetti

Ho gestito progetti importanti come il **Cyber Range** — ambienti virtuali dove si simulano attacchi reali per allenare i team di attacco e difesa (tipo una palestra per hacker buoni 💪)

Cybersecurity Manager

Oggi lavoro in una grande azienda del **fashion**, dove mi occupo a 360° di tutte le sfide legate alla cybersecurity: gestione degli incidenti, strategia, consapevolezza, compliance... e ogni tanto anche un po' di diplomazia 😅



Agenda

Struttura del libro

Come è organizzato Cyber Mindset

Genesi del progetto

Come è nato e perché l'ho scritto

Concetti chiave

Riflessioni estratte dal libro Cyber Mindset

Q&A

Domande e risposte

Struttura del libro

Aforismi

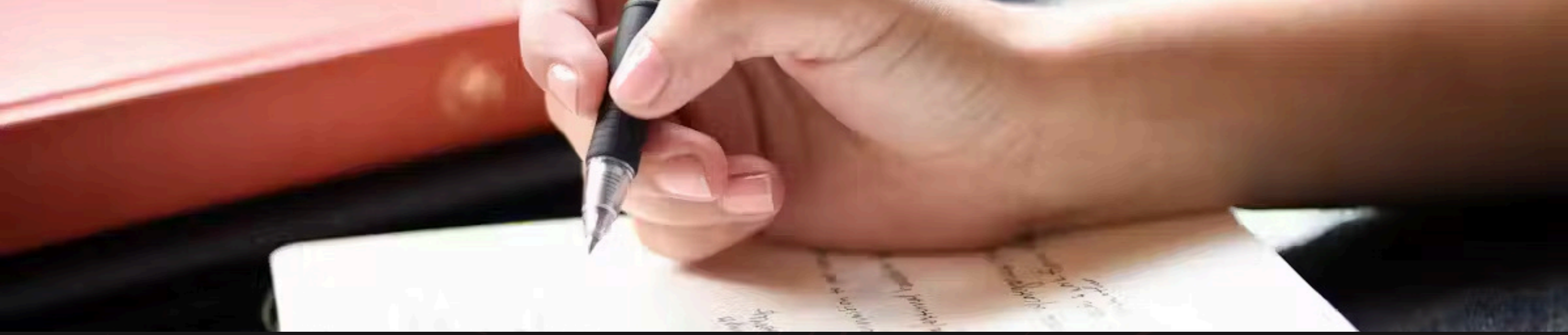
Ogni capitolo inizia con un aforisma che sintetizza un concetto chiave

Approfondimento

L'aforisma viene poi approfondito nel mini capitolo

Riflessione

Considerazioni personali basate sulla mia esperienza



Come è nato

Da post a libro

È nato come raccolta di post LinkedIn. Ad un certo punto ne avevo tanti e ho deciso di scrivere un libro.

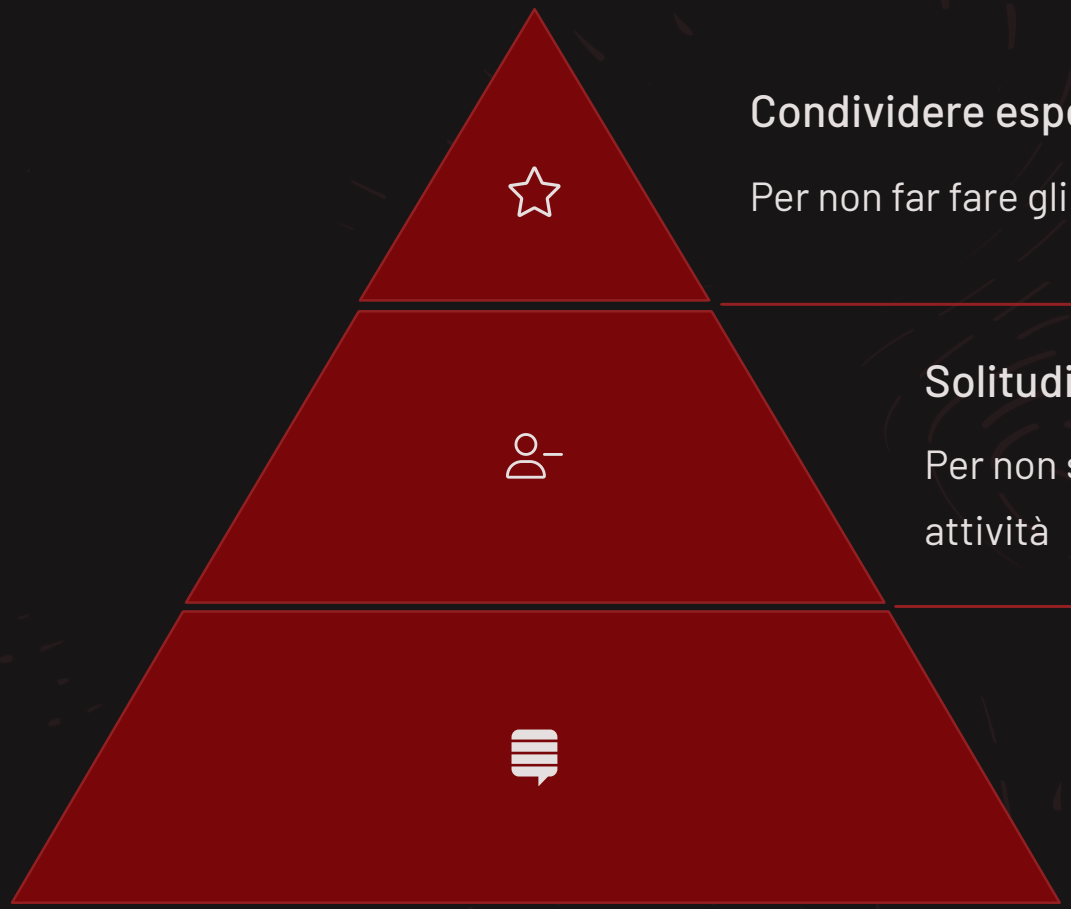
Nato per scherzo

Diciamo che è nato quasi per gioco, senza grandi aspettative iniziali.

L'essenziale sottovalutato

- Concetti semplici
- Linguaggio accessibile
- Riflessioni che sembrano ovvie, ma nel quotidiano non lo sono

Perché ho scritto un libro?



Condividere esperienze

Per non far fare gli stessi errori che ho visto e che vedo fare

Solitudine

Per non sentirmi e per non farvi sentire soli durante la vostra attività

Condivisione esperienze nel passaggio di ruolo

Evidenziare sfide e lezioni apprese nel passaggio da ruolo tecnico a manageriale

Migliorare la comunicazione

50% fare, 50% comunicare

Perché, come dico spesso, il **50% è fare le cose ma il 50% è saperle comunicare**.

Da anni studio marketing e comunicazione e volevo applicare alcuni concetti in prima persona.

Autenticità, valore ed esperienze vissute

Credo che la forza della comunicazione sia nel portare vero valore all'utente.

Uno degli elementi più apprezzato sono le situazioni vissute in prima persona.

Perché non ho scritto il libro

0€

Guadagno

Scrivere un libro non ti renderà ricco, a differenza di ciò che molti credono

100+

Ore di lavoro

Serve tempo per scrivere, rivedere e rifinire

€€€

Investimento

Servono risorse per lavorare sulla grafica e sull'editing

In definitiva, un libro è un **biglietto da visita costoso** che richiede un grande impegno personale.

Nato in un momento di crisi

Pochi stimoli

Un periodo lavorativo con poche sfide interessanti

Trasformazione

La crisi come opportunità di cambiamento e crescita

Difficoltà fisiche

Dopo un intervento chirurgico con ripercussioni fisiche

Messaggio positivo

La scrittura come risposta positiva alle difficoltà

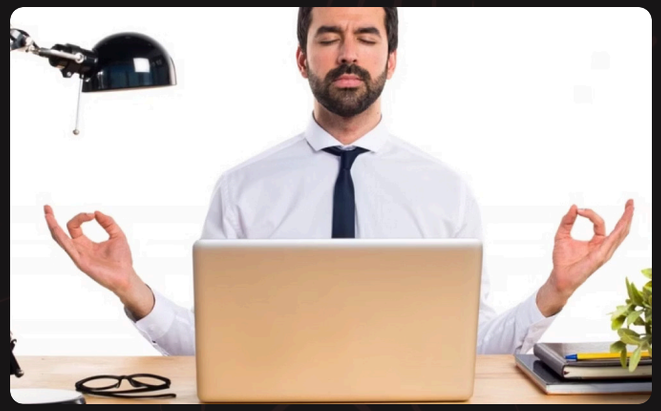
"È nelle crisi che il meglio (peggio) di ognuno di noi affiora"

Al primo attacco ransomware o nel primo momento in cui i sistemi sono bloccati si cade in crisi

Pressione e reazioni

Ho visto gente che è uscita fuori di testa durante attacchi gravi.

I momenti di crisi obbligano persone e team a uscire dalla propria zona di comfort.



Mantenere la calma

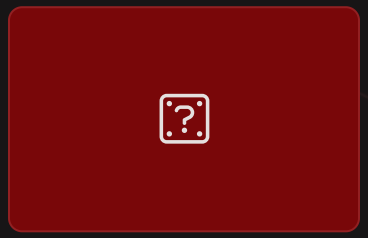
La lucidità è fondamentale nei momenti di crisi. Evita che la situazione degeneri, trasformando un momento critico in un esempio di leadership.

Qualità essenziali

La gestione delle crisi richiede:

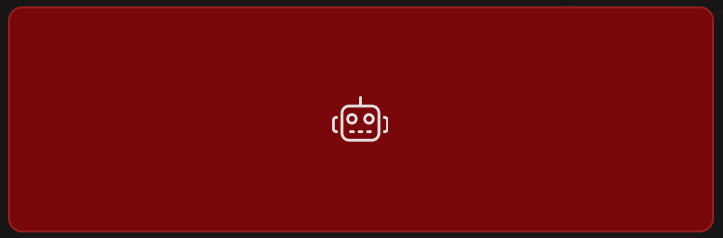
- avere un piano di gestione delle crisi
- procedure già decise e testate
- ruoli e responsabilità
- comunicazione sia interna che esterna

Le crisi innescano cambiamenti



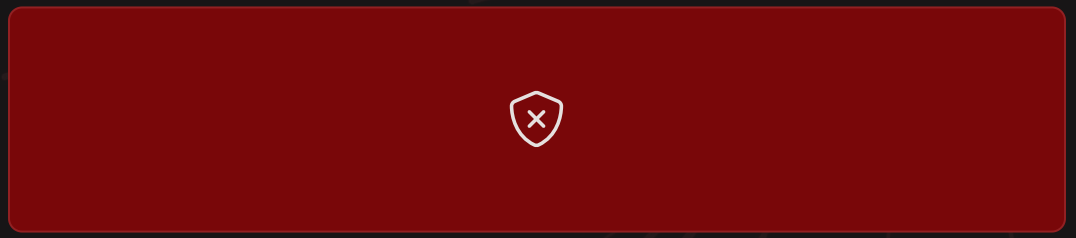
Caduta delle certezze

Le crisi fanno cadere le certezze (servizi che hanno sempre funzionato) e aprono a nuovi scenari



Nuove minacce

Come i deepfake generati da AI che sembrano autentici (caso Ferrari)



Nuove difese

Dobbiamo sviluppare nuove strategie di protezione

"L'intelligenza è la capacità di adattarsi al cambiamento"

Stephen Hawking

Nota: questa **presentazione** è stata preparata con l'aiuto dell'AI, che utilizzo ormai quotidianamente.

Le **query degli strumenti di Security** vanno in un ottica AI

Alleato, non sostituto

L'AI non è un sostituto dell'uomo, ma un potente alleato che sta rivoluzionando il settore.

Difesa potenziata

Analizza in tempo reale enormi quantità di dati, individua anomalie e anticipa potenziali minacce.

Valore umano

Il valore degli esperti risiederà in attività strategiche:

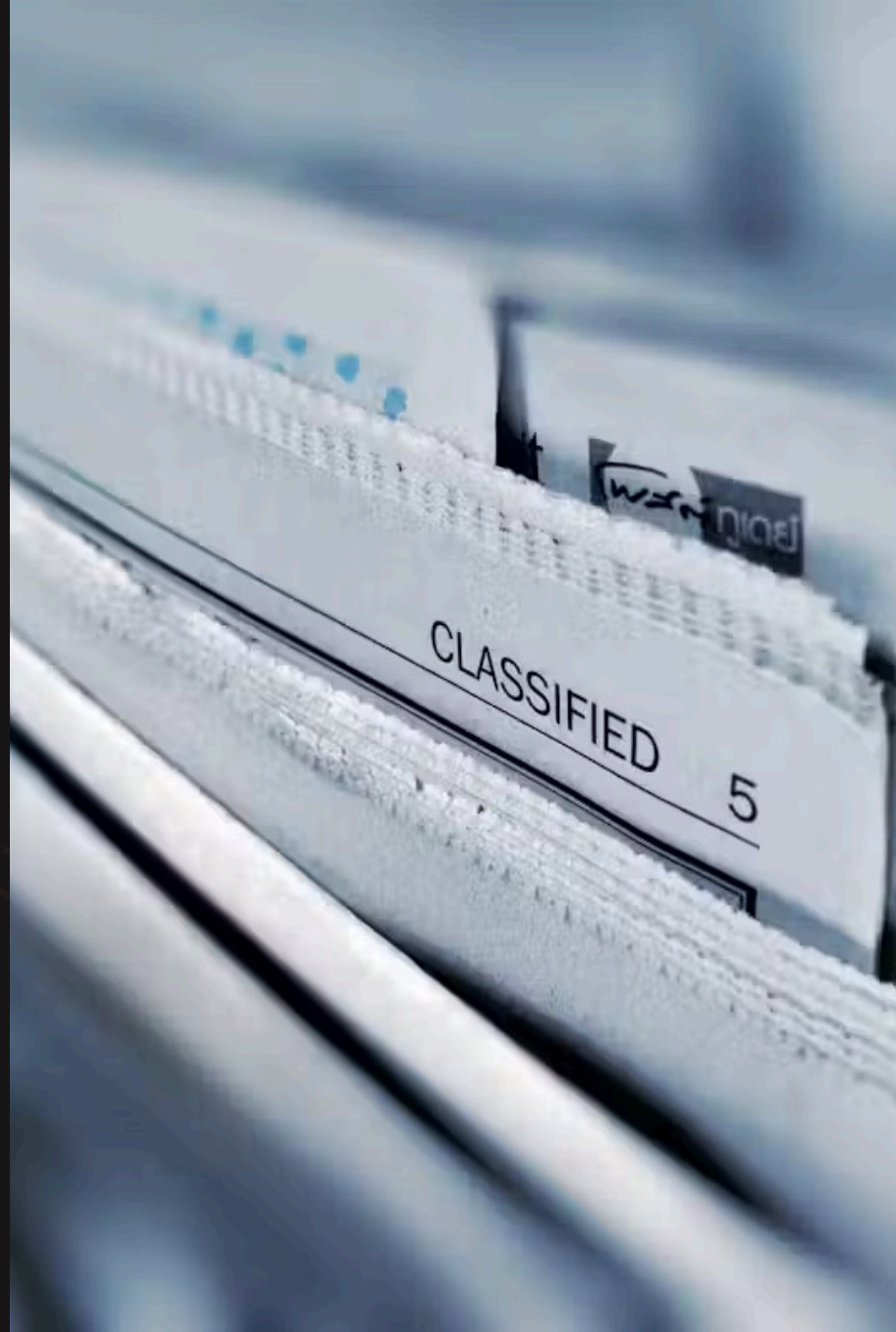
1. gestione crisi
2. analisi complesse
3. pianificazione

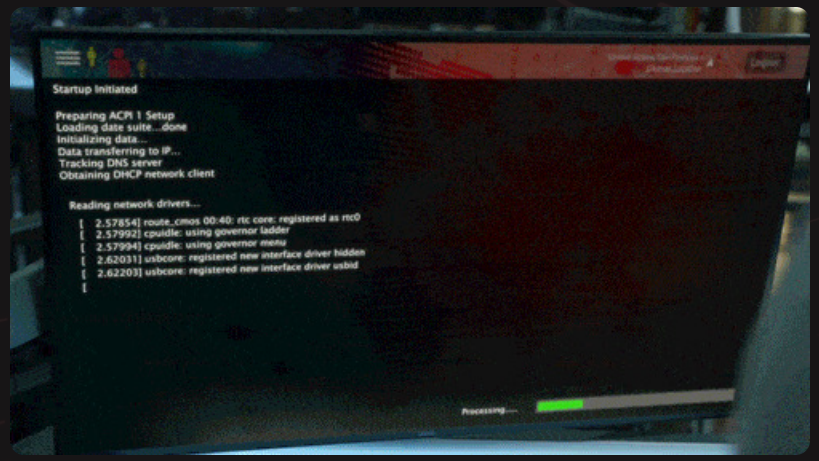
Chi rischia di perdere?

Il vero rischio non è l'AI, ma l'incapacità di adattarsi al cambiamento. L'intelligenza artificiale richiede di acquisire **nuove competenze**, e chi abbraccerà questa rivoluzione potrà trarne enormi benefici.

L'AI nella gestione della comunicazione in eventi di crisi

- **Generazione bozze:** generare bozze per comunicazioni durante le crisi Cyber
- **Comunicazioni efficaci:** analizzano best practices e casi storici simili identificano strategie di comunicazione efficaci
- **Comunicazioni in linea con l'audience:** valuta esigenze e aspettative dei diversi pubblici, suggerendo canali e approcci più adatti
- **Valutazione critica:** evidenziare potenziali debolezze nelle strategie comunicative che abbiamo già ideato





Non è una questione di "se" ma di "quando"

I criminali lo sanno bene: un attacco informatico è molto meno rischioso di una rapina tradizionale.

Secondo il report Mandiant "M-Trends 2024", il tempo medio di permanenza di un attaccante all'interno di un sistema è di circa 11 giorni. Questo significa che un attaccante ha a disposizione giorni per muoversi indisturbato.

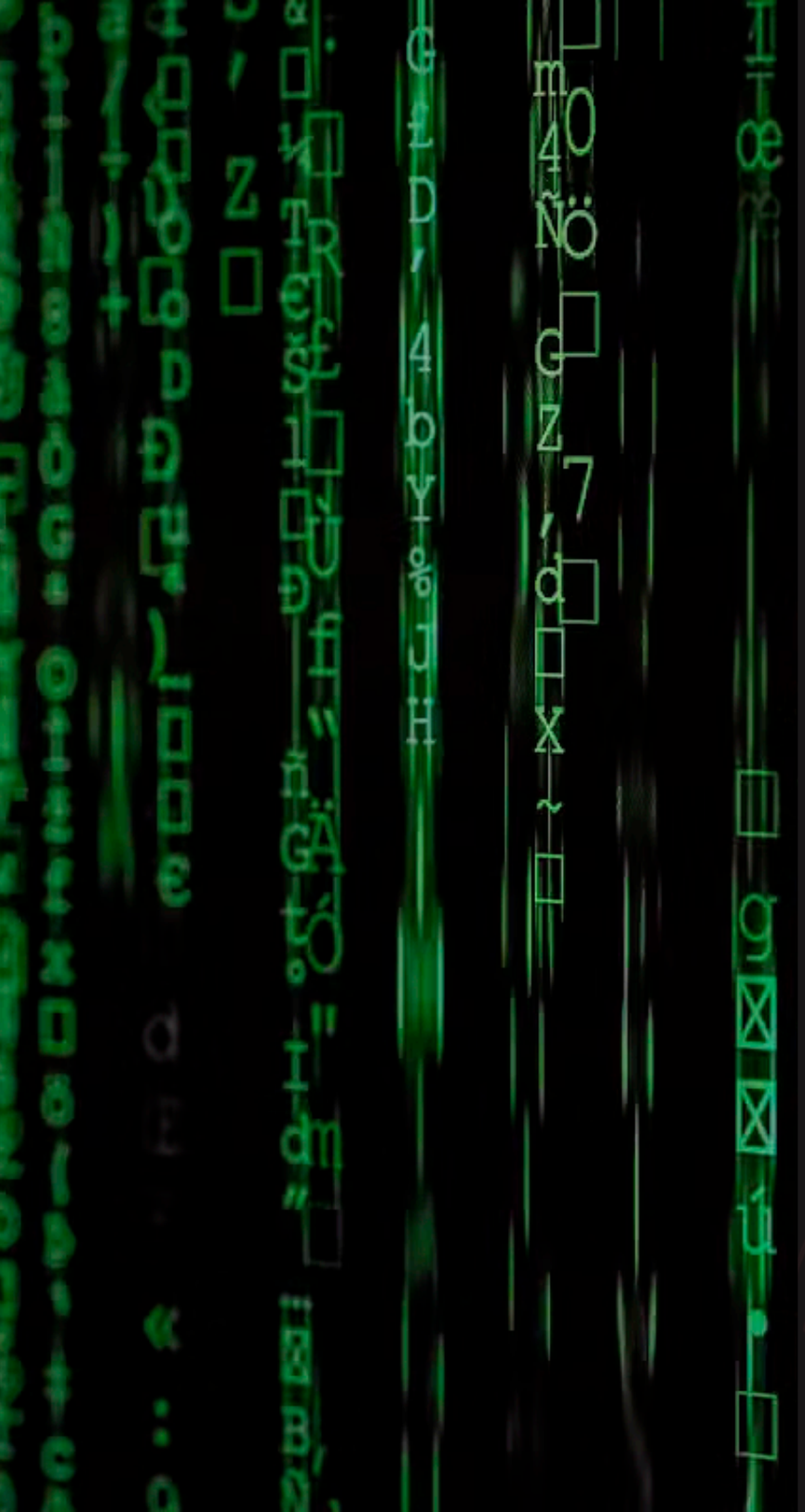
Asimmetria nel cyberspazio

Attaccanti: risorse e costi minimi rispetto ai danni potenziali.

Difensori: costo elevato e strategie in continua evoluzione.

Quinto dominio di guerra

Dal 2016, la NATO ha riconosciuto il cyberspazio come quinto dominio di guerra, al pari di aria, terra, mare e spazio.



"La fortuna favorisce i preparati"

Louis Pasteur

La preparazione è fondamentale: essere pronti con adeguati sistemi di monitoraggio e risposta per **ridurre i tempi di gestione e limitare i danni potenziali**.

Chi investe nella preparazione non lascia al caso la propria sicurezza.

Focus sul post-breach

Le aziende devono spostare l'attenzione sul concetto di post breach: non solo prevenire gli attacchi, ma essere pronte a gestirli.

Anche i servizi interni non devono essere vulnerabili.

Checklist post-breach

- Cosa farò quando accadrà?
- Ho un piano di continuità operativa?
- Il mio piano di backup è davvero efficace?
- Come gestisco gli incidenti?

I ransomware hanno cambiato tutto

1. I ransomware incidono sui tempi di rilevamento degli incidenti

2. I ransomware hanno aumentato la consapevolezza sulla sicurezza informatica nelle organizzazioni

5

Giorni

Tempo medio di notifica da parte dei sistemi di sicurezza di un attacco ransomware

26

Giorni

Tempo medio di notifica da enti esterni (threat actor)

Fonte: Mandiant "M-Trends 2025"

"Hanno fatto più awareness i ransomware che tutti gli esperti del mondo"

Alessio Pennasilico

Da nicchia a mainstream

Per anni, esperti hanno lanciato avvertimenti, ma il messaggio cadeva nel vuoto. Poi sono arrivati i ransomware.

Consapevolezza attraverso i danni

La consapevolezza è cresciuta grazie ai danni reali subiti dalle aziende e dai cittadini. Il tema è diventato particolarmente importante da quando sentiamo parlare di attacchi che **bloccano ospedali, aeroporti e sistemi di trasporto ferroviario**.

Consapevolezza dei media

Oggi la cybersecurity è discussa in TV, nei bar e nelle conversazioni quotidiane. Serie come Mr. Robot sono diventate cult.

"Non puoi fare tutto da solo ma puoi scegliere con cura chi ti aiuterà"

Uno degli errori più frequenti che vedo è la delega. È importante delegare altrimenti si diventa il collo di bottiglia dell'organizzazione.

Ruolo strategico

Un bravo CISO deve concentrarsi su obiettivi strategici, pianificazione del budget e visione a lungo termine.

Servizi delegabili

SOC, MDR, penetration test: attività che possono essere esternalizzate con efficacia.

Gestione interna (non delegabili)

Alcune attività richiedono controllo diretto, soprattutto quando coinvolgono dati sensibili.

Vantaggi della delega interna

Ottimizzare risorse, prevenire burnout e garantire attenzione agli aspetti critici dell'organizzazione e a conservare la conoscenze all'interno dell'azienda

"Se conosci te stesso, ma non il nemico, per ogni vittoria ottenuta subirai anche una sconfitta. Se non conosci te stesso né il nemico, soccomberai in ogni battaglia."

Sun Tzu

1

Un bravo CISO o Cybersecurity Manager non deve solo avere una profonda conoscenza delle minacce cyber, ma avere il talento di **contestualizzarle** in base a:

- tipo azienda (startup, PMI, Grande impresa)
- cultura organizzativa: grado di conoscenza dei rischi
- livello di maturità digitale
- settore merceologico specifico (banca, retail, farmaceutico, trasporti)

2

Infrastruttura tecnologica

- Cloud
- On-premises
- Modelli ibridi

3

La strategia vincente risiede nell'armonizzare:

- tecnologie di difesa
- budget
- contesto
- competenze del team

La strategia vincente non consiste nel dotarsi di tutte le tecnologie più quotate nel **Magic Quadrant di Gartner**

"La Cybersecurity è una responsabilità condivisa"

Barack Obama

Responsabilità di tutti

La sicurezza informatica coinvolge ogni membro dell'organizzazione, indipendentemente dalla posizione. Non è solo una responsabilità del CISO

Collaborazioni strategiche

Anche collaborazioni apparentemente irrilevanti, come tra FinOps e Cybersecurity, possono rivelarsi fondamentali.

Ridurre la superficie di attacco

Il team FinOps può individuare servizi inutilizzati, riducendo costi e migliorando la sicurezza.

Rilevare anomalie

Aumenti improvvisi nei costi potrebbero indicare crypto mining non autorizzato o altre compromissioni.

Gioco di squadra

La chiave per una sicurezza informatica efficace è la collaborazione tra tutti i team. Dal FinOps al personale operativo, ognuno deve comprendere il proprio ruolo nella protezione dell'azienda.

"Il nemico non dorme mai"

24/7/365

I cybercriminali operano senza sosta, senza limiti geografici o di fuso orario.

SOC

Security Operations Center attivo in ogni momento per monitorare minacce.

MDR

Managed Detection and Response per identificare e rispondere rapidamente con procedure concordate.

Protezione continua

Un servizio attivo 6X8 è molto limitante. Gli attacchi possono verificarsi in qualsiasi momento, spesso nelle ore meno presidiate.

"Cerca di imparare qualcosa di tutto e tutto di qualcosa"

Thomas Henry Huxley

Un buon esperto deve avere un approccio multidisciplinare.

Tecnica

Competenze specifiche di cybersecurity.

Conoscere gli strumenti di difesa.

Capire come agiscono gli attaccanti. Saper analizzare e rispondere agli incidenti.

Leadership

Saper guidare team diversi.

Motivare e coordinare le persone verso obiettivi comuni di sicurezza.

Business

Allineare le strategie di sicurezza alle necessità aziendali è ciò che distingue un buon professionista da un grande leader.

La sicurezza deve essere un abilitatore del business, non un ostacolo.

Finanziarie

Gestire budget e allocare le risorse in maniera strategica

La cybersecurity ha bisogno sia di esperti tecnici, sia di professionisti versatili capaci di unire diverse discipline.

"Pensare fuori dagli schemi non significa cambiare le risposte, ma riformulare le domande"

Paul Arden

Mentalità hacker

"Gli hacker non sono cattivi; semplicemente vedono cose che gli altri non vedono." - Dan Kaminsky

Chi progetta un'applicazione lo fa con un chiaro obiettivo: farla funzionare come previsto. Un penetration tester deve andare oltre questa logica convenzionale.

Esempi di mentalità da Hacker

Se il programmatore ha previsto un parametro come id=1, il penetration tester proverà:

- id=2, id=3 per verificare Broken Access Control
- "OR 1=1 --" per testare SQL injection

Chi lavora nella Cybersecurity deve sviluppare un pensiero critico avanzato.

"La semplicità è la suprema sofisticazione"

Leonardo da Vinci

La complessità eccessiva non solo rende difficile la gestione, ma apre nuove vulnerabilità. La vera maestria sta nel creare sistemi semplici ma efficaci.

Ridurre la superficie di attacco

Eliminare servizi obsoleti o dismessi riduce le potenziali vulnerabilità e semplifica la gestione della sicurezza.

Nei penetration test si trovano spesso servizi dimenticati e vulnerabili.

Principio del "least privilege"

Assegnare solo i permessi strettamente necessari limita i danni potenziali e semplifica il monitoraggio delle attività.

Evitare l'utilizzo di root ove non necessario.

Unificare strumenti

Una piattaforma centralizzata per log e alert non solo semplifica la gestione ma riduce il rischio di perdere segnali critici.

Si vedono strumenti di Security totalmente slegati tra di loro

Bloccare utenze inutilizzate

Ogni account dimenticato o inutilizzato è un'arma pronta per essere sfruttata dagli attaccanti. Automatizzare il blocco di account inattivi per un certo periodo è un passo semplice ma potente.

"Fare qualcosa è sempre meglio che non fare nulla"

La sfida del CISO

Un CISO non può controllare completamente il comportamento umano.

La sua sfida principale consiste nell'agire su molteplici fattori che sfuggono al suo diretto controllo.

Marketing vs Cybersecurity

Un **direttore marketing** ha controllo diretto sulle leve strategiche e può misurare i risultati.

Un CISO, invece, può implementare difese avanzate, ma un singolo errore umano può compromettere tutto.

"Solo dicendo no puoi concentrarti sulle cose importanti"

Steve Jobs

Non è un caso che i responsabili della sicurezza vengano spesso percepiti come i "signori del no".

Il valore del rifiuto

Rifiutare ciò che non è essenziale è una delle chiavi per **focalizzarsi** su ciò che **davvero conta**.

Permette di allocare le persone su progetti che contano.

No strategico

Dire "no" non significa chiudere le porte, ma proporre delle **alternative** più sicure.

Protezione

Dire "no" a progetti, pratiche di sicurezza carenti è un obbligo es. bloccare il passaggio in produzione di codice con vulnerabilità critiche

"Le piccole correzioni di oggi prevengono i grandi disastri di domani"

> Secondo Mandiant (**report M-Trends 2025**), gli exploit sono il vettore di attacco iniziale più comune utilizzato dagli attaccanti per entrare in un organizzazione (33%)

Processo di Vulnerabilty Management

Un approccio efficace al patching non deve considerare il solo CVSS score, ma altri parametri.

I limiti del CVSS

Il CVSS è uno strumento datato che non considera adeguatamente il contesto aziendale, l'esposizione reale e l'evoluzione delle minacce nel tempo.

Patchare o non patchare?

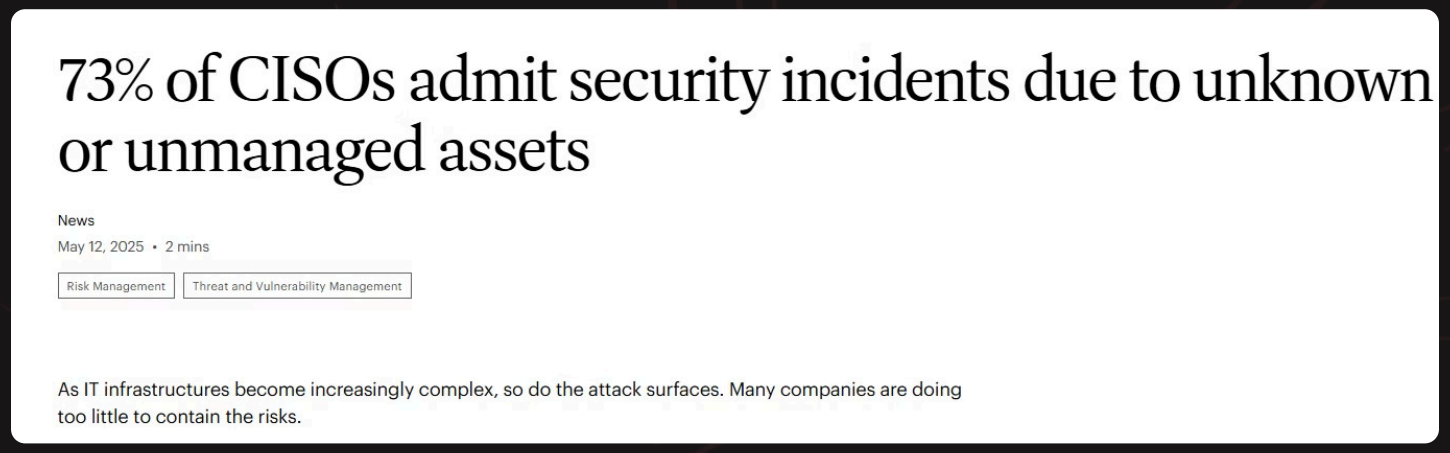
È necessario un approccio basato sul rischio che consideri:

- Esposizione effettiva degli asset, se esposti du Internet hanno una maggiore criticità
- Esistenza di exploit funzionanti
- La probabilità che una vulnerabilità sia attivamente sfruttata dai criminali
- Criticità dell'asset
- **L'impatto operativo e di business**: nel caso è necessario riavviare i servizi

Utilizzare l' Exploit Prediction Scoring System (EPSS) che rappresenta una metrica più affidabile

"Non puoi proteggere ciò che non sai di avere"

Non si può proteggere ciò che non si conosce. Questa semplice verità è la base di ogni strategia di Security efficace e alla base di ogni standard di Cybersecurity.



73% of CISOs admit security incidents due to unknown or unmanaged assets

News

May 12, 2025 • 2 mins

Risk Management | Threat and Vulnerability Management

As IT infrastructures become increasingly complex, so do the attack surfaces. Many companies are doing too little to contain the risks.

Inventario Dettagliato

Un asset inventory deve andare oltre il semplice elenco di hardware e software.

Interconnessioni

È fondamentale mappare le dipendenze tra sistemi e le loro relazioni con i processi aziendali.

Criticità degli asset

Conoscere la criticità degli asset permette di allocare risorse difensive in modo efficiente.

Inventario dinamico

L'inventario deve evolversi in tempo reale, superando i limiti degli strumenti statici (Excel).

La risposta efficace agli incidenti inizia dalla conoscenza approfondita del proprio ambiente. Senza questa base, ogni strategia di Cybersecurity diventa un castello di carta.

"Il controllo inizia dalla comprensione"

Edward Deming

Rob Joyce forte della sua esperienza alla NSA (National Security Agency) ha svelato dettagli illuminanti in una presentazione dal titolo "NSA's six-phase plan for targeted intrusions", dedicata all'hacking delle reti.

Conoscere un sistema meglio di chi lo ha creato

Per penetrare in un sistema target, bisogna conoscerlo meglio di chi l'ha costruito.

Trovare la prima falla

Una volta acquisita la conoscenza del sistema bisogna trovare una falla

Esperienza personale

La complessità delle infrastrutture moderne rende quasi inevitabile la presenza di servizi dimenticati o asset non mappati, un terreno fertile per potenziali attaccanti.

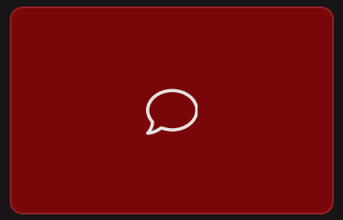
Se non conosci la tua rete, qualcuno con intenzioni malevole lo farà al posto tuo.

"Sono tutti bravi con gli incidenti (e i budget) degli altri"

Saggezza popolare

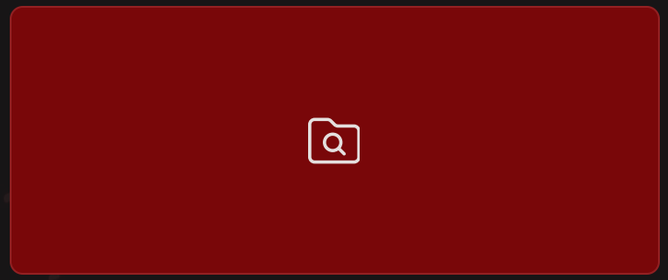
Quando un'azienda subisce un attacco informatico e la notizia diventa di dominio pubblico all'improvviso tutti diventano esperti (leoni da tastiera)

1. **Virologi improvvisati durante il COVID**
2. **gli allenatori da bar nei periodi bui della nazionale**
3. **diplomatici da salotto nelle crisi internazionali**



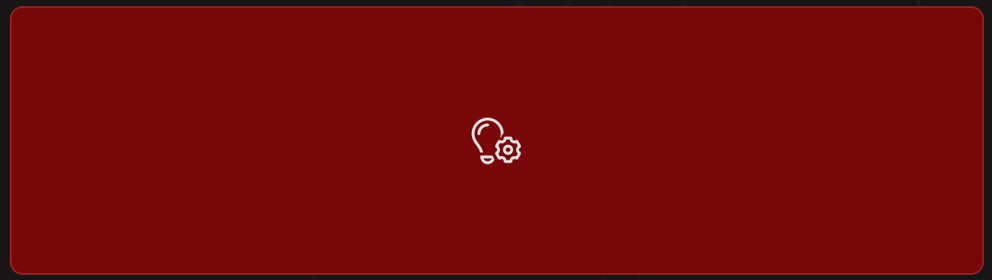
Realtà complessa

Ogni attacco ha una storia che non conosciamo completamente



Vincoli e pressioni

Spesso il team di Cybersecurity fa del suo meglio, ma deve affrontare fretta, consegne immediate e priorità contrastanti degli altri team



Imparare dagli altri

La strada migliore è imparare dagli errori altrui senza giudicare

Cyber Mindset in sintesi

Preparazione tecnica e multidisciplinare

Non bastano le competenze tecniche

Procedure

Non è questione di "se" ma di "quando" avverrà un attacco e quindi dobbiamo essere preparati con procedure collaudate

Conoscenza del contesto

Adattare la strategia di Cybersecurity al contesto in cui si opera

Conoscenza degli asset

Conoscere la propria rete e i propri asset da proteggere

Domande?

Se non ne avete,

o ho spaccato...

...o vi ho completamente disorientati.

In entrambi i casi: parliamone