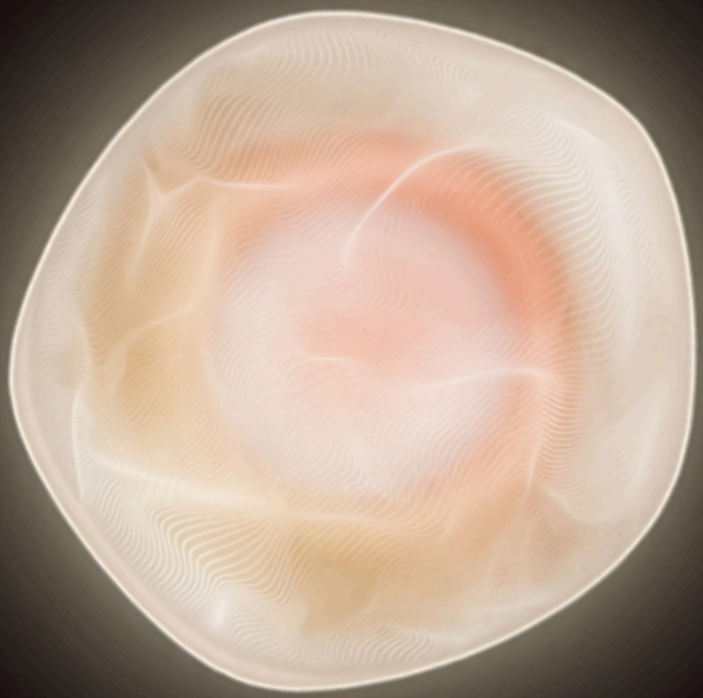
HADRIAN

# MODELLO DI MATURITÀ DELLE ESPOSIZIONI ESTERNE



A che punto si trova il tuo programma di gestione delle esposizioni in questo momento e quali azioni puoi intraprendere per migliorarlo?

# IL PROBLEMA DI ESPOSIZIONE CHE NESSUN PROGRAMMA RIESCE A RISOLVERE ATTUALMENTE

Le aziende tendono a investire ingenti risorse in strumenti di sicurezza. Eseguono scansioni di vulnerabilità, utilizzano piattaforme SIEM, effettuano test di penetrazione annuali o trimestrali e dispongono di programmi di gestione delle vulnerabilità con responsabili designati e accordi sul livello di servizio definiti. Eppure, si ripete sempre lo stesso copione: le vulnerabilità sfruttabili continuano a persistere, le code delle azioni correttive si allungano più velocemente di quanto si riducano e, quando qualcosa va storto, si scopre spesso che il problema che ha causato l'incidente era già presente in un report da mesi.

Il problema non è la mancanza di un'attività di sicurezza, ma la mancanza di una struttura programmatica che colleghi l'attività ai risultati. Le scansioni generano risultati, i risultati generano ticket, e i ticket vengono chiusi. Oppure no. Ma spesso la domanda che conta davvero, ovvero se l'esposizione sfruttabile dell'azienda stia effettivamente diminuendo, rimane senza risposta.

Il Modello di maturità dell'esposizione esterna è stato concepito esattamente per colmare questa lacuna. Descrive quattro modelli operativi riconoscibili, ognuno definito non dagli strumenti disponibili, bensì dalla struttura con cui un'azienda individua un'esposizione, ne conferma la reale esistenza e la risolve prima che un aggressore possa agire. Il modello offre ai responsabili della sicurezza un linguaggio preciso per comprendere a che punto si trova oggi il loro programma, quali sono gli ostacoli strutturali che ne impediscono il progresso e cosa occorre cambiare per migliorare.

## Come si inquadra questo modello in relazione al modello CTEM

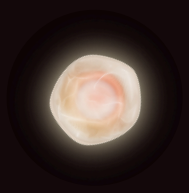
La gestione continua dell'esposizione alle minacce (CTEM, dall'inglese Continuous Threat Exposure Management) è un modello ideato da Gartner e articolato in cinque step che fornisce una struttura per passare da una gestione reattiva delle vulnerabilità a una riduzione continua delle esposizioni orientata ai risultati. Gli step sono i seguenti: definizione dell'ambito, scoperta, prioritizzazione, convalida e mobilitazione. Questo modello si riallaccia direttamente ai livelli di maturità CTEM: in Fase 1 e 2 le aziende stanno solitamente eseguendo i primi step, mentre quelle in Fase 3 e 4 hanno già completato il ciclo passando attraverso le fasi di convalida e mobilitazione. La fase in cui la maggior parte delle implementazioni CTEM si arena è quella della convalida, ovvero quando si deve confermare che i risultati individuati rappresentano un rischio realmente sfruttabile, non solo una minaccia teorica. Ed è proprio questo lo snodo strutturale attorno al quale è costruito questo modello.

# PERCHÉ LA PROGRESSIONE È IMPORTANTE

Il modello mappa quattro fasi della gestione dell'esposizione esterna, da reattiva e non rilevata a continua e autonoma.

# Cosa porta realmente il progresso

Il divario tra la Fase 1 e la Fase 4 non è una questione di risorse, ma di struttura, ovvero il modo in cui un'azienda individua un'esposizione, ne conferma la reale esistenza e la risolve prima che un aggressore possa agire.



FASE 1 → FASE 2

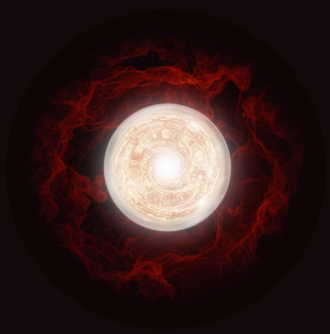
### Da Operare al Buio a una Portata Migliore, con Più Speranza

La copertura del monitoraggio della superficie di attacco passa da meno del 20% al 40–60%. Il tasso di veri positivi passa da meno del 10% al 15–25%. Questo significa che si passa da meno di 1 avviso su 10 che richiede una verifica a 1 avviso su 4-6. Il tempo medio necessario per le correzioni diminuisce, da oltre 90 giorni a 45–90 giorni. L'effetto pratico: il team di sicurezza smette di dedicare tanto tempo a risultati che si rivelano irrilevanti.

FASE 2 → FASE 3

### Da una Portata Migliore, con Più Speranza a Connettere i Punti

La copertura raggiunge il 75–90% della superficie. Il tasso di veri positivi sale al 40-60%, il che significa che quasi la metà dei risultati viene confermata come sfruttabile prima ancora che qualcuno li analizzi. L'MTTR si riduce a 15–45 giorni. La conformità SLA raggiunge il 60–80%. La coda delle azioni correttive si riduce e diventa più mirata: un numero minore di risultati complessivi, una maggiore affidabilità di ciascuno di essi e una riduzione misurabile delle esposizioni sfruttabili, non semplicemente dei ticket chiusi.



FASE 3 → FASE 4

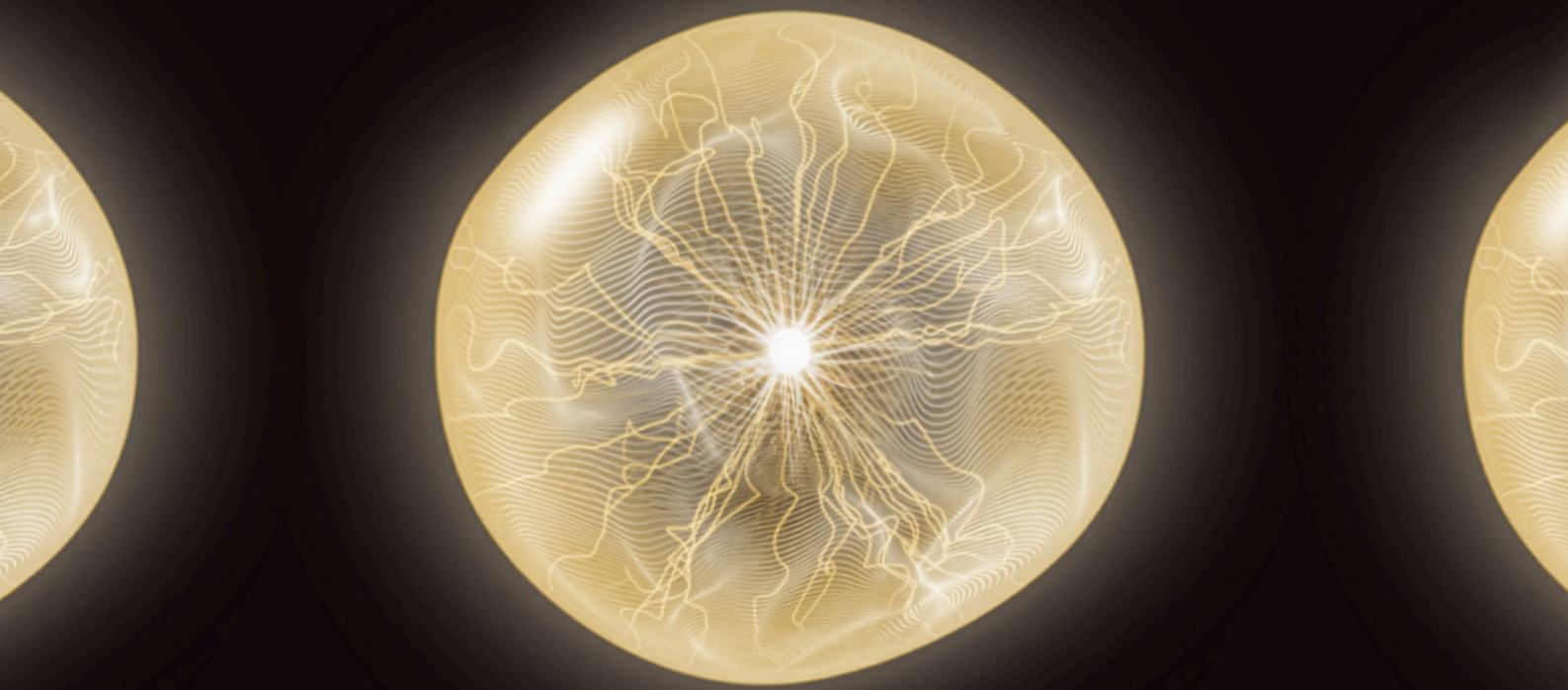
### Da Connettere i Punti a Quadro Chiaro

La copertura supera il 95%. Il tasso di veri positivi supera il 70%. L'MTTR si riduce a meno di 7 giorni, con esposizioni critiche risolte entro 48 ore. La conformità SLA supera il 90%. Il benchmark più importante: quando viene rilevata una nuova esposizione, l'azienda è in grado di verificare entro poche ore (non giorni) se è stata colpita. In Fase 3, per ottenere quella risposta erano necessarie una riunione del team e un'indagine manuale. In Fase 4, il programma la fornisce automaticamente.

Usa questo schema come strumento diagnostico, come guida o come linguaggio comune con la dirigenza. Non è stato pensato come un kit di strumenti e non impone alcuna tempistica. Non tutte le aziende devono necessariamente raggiungere la Fase 4 per ogni asset. La domanda giusta da porti non è quanto sei avanti, ma se il programma sta operando al livello richiesto dal tuo profilo di rischio.

SEZIONE 2

# IL MODELLO IN SINTESI



Sapere dove si trova il tuo programma è il punto di partenza per un avanzamento significativo. Questa sezione ti darà un quadro delle lacune specifiche nelle capacità e dei risultati misurabili che definiscono ogni fase.

## La tabella delle lenti

Per ogni “lente”, contrassegna la colonna che descrive più fedelmente il tuo programma attuale. Se le tue risposte ricadono sistematicamente in una colonna, quella rappresenta la tua fase attuale. Se invece sono distribuite su più colonne, il tuo punto di partenza è la colonna più a sinistra che hai contrassegnato.

| LENTE | FASE 1: VAGARE ALLA CIECA | FASE 2: AMBITO PIÙ CHIARO, MAGGIORE SPERANZA | FASE 3: UNIRE I PUNTINI | FASE 4: UNA VISIONE CHIARA |
|---|---|---|---|---|
| **Ritmo operativo**<br>Con quanta frequenza il tuo programma interagisce con le esposizioni? | REATTIVO | PERIODICO | CONTINUO | AUTONOMO |
| **Rapporto con il rischio**<br>Quanto sei consapevole del tuo livello effettivo di esposizione o come lo valuteresti? | ESPOSTO | CONSAPEVOLE | CONVALIDATO | PROATTIVO |
| **Approccio alla sicurezza**<br>Come si posiziona il tuo programma rispetto agli aggressori? | REATTIVO | STRUTTURATO | PROATTIVO | PREDITTIVO |
| **Approccio alla convalida**<br>In che modo il tuo programma affronta la questione: i nostri controlli funzionano davvero? | PRESUNTO | TESTATO | CONVALIDATO | CONTINUO |

## La matrice delle funzionalità

Cinque dimensioni operative, quattro fasi. Usa questo schema per capire quale dimensione è il fattore che ti sta limitando.

| FUNZIONALITÀ | FASE 1: VAGARE ALLA CIECA | FASE 2: AMBITO PIÙ CHIARO, MAGGIORE SPERANZA | FASE 3: UNIRE I PUNTINI | FASE 4: UNA VISIONE CHIARA |
|---|---|---|---|---|
| **Modello operativo** | Basato sugli eventi; esposizioni rilevate a seguito di incidenti o audit | Programma strutturato; responsabilità definite; step CTEM già introdotti | Ciclo chiuso; i risultati della convalida indirizzano le azioni correttive | Di default offensivo; adattivo; coordinamento manuale minimo |
| **Scoperta** | Inventario statico incompleto; scansione periodica degli asset noti | EASM implementato; cloud, SaaS, API, terze parti incluse nell'ambito di applicazione | Monitoraggio continuo; rilevamento delle anomalie quasi in tempo reale | Adattivo; correla automaticamente identità, infrastruttura e SaaS |
| **Prioritizzazione** | Punteggi CVSS e dei fornitori; contesto aziendale limitato | Basata sul rischio, tenendo conto della criticità aziendale | In base alla vulnerabilità e al percorso di attacco; meno problemi e con un livello di affidabilità più elevato | Predittiva e consapevole del contesto; le priorità cambiano dinamicamente |
| **Convalida** | Pentest annuali o ad hoc; vulnerabilità presunte, non confermate | Test periodici basati su scenari entro ambiti definiti | Convalida automatizzata continua; eliminazione dei tempi morti | Emulazione autonoma degli attacchi; le catene di attacco si adattano ai cambiamenti |
| **Automazione** | Manuale, basata su ticket; strumenti isolati | Flussi di lavoro integrati; passaggi di consegna standardizzati | La convalida attiva le azioni correttive; integrazioni SOC/IT attive | Operatività in gran parte autonoma; il personale si concentra sulle decisioni strategiche |

## Benchmark quantitativi

Intervalli di prestazione indicativi in base a ogni fase. Usali per calibrare la direzione, non come soglie di promozione/bocciatura.

| METRICA | FASE 1: VAGARE ALLA CIECA | FASE 2: AMBITO PIÙ CHIARO, MAGGIORE SPERANZA | FASE 3: UNIRE I PUNTINI | FASE 4: UNA VISIONE CHIARA |
|---|---|---|---|---|
| **Superficie di attacco sottoposta a monitoraggio continuo** | < 20% | 40–60% | 75–90% | > 95% |
| **Tasso di avvisi veri positivi** | < 10% | 15–25% | 40–60% | > 70% |
| **Tempo medio necessario per le correzioni (MTTR)** | > 90 giorni | 45–90 giorni | 15–45 giorni | < 7 giorni (critiche: < 48h) |
| **Conformità SLA** | < 20% | < 40% | 60–80% | > 90% |
| **Risultati convalidati come sfruttabili prima di un'escalation** | Raramente | In modo selettivo | Sistematicamente | In modo continuo e automatico |

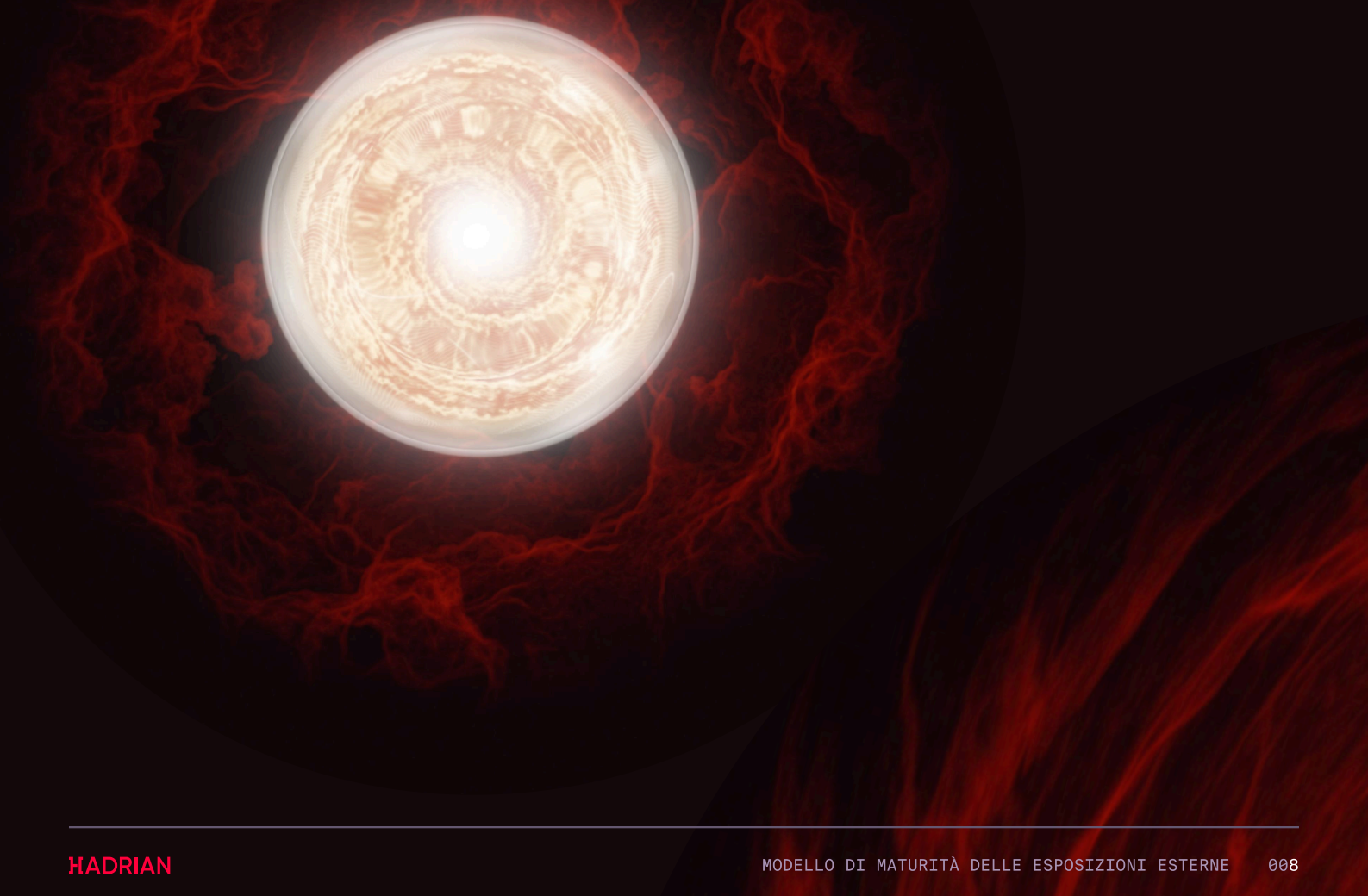
## VALUTATI:

Fai la valutazione interattiva

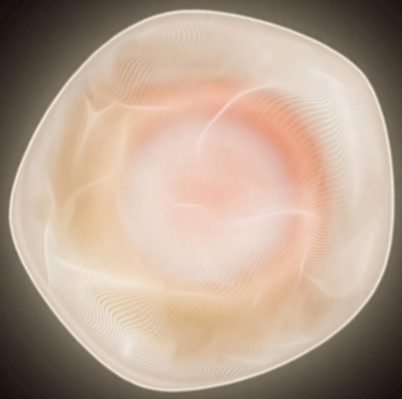
SCOPRI LA TUA FASE DI MATURITÀ

# LE QUATTRO FASI

Ogni fase rappresenta una modalità operativa ben definita, non un punteggio né un voto. Considerale come un ritratto di come funzionano effettivamente le aziende. Se una delle descrizioni ti suscita disagio, probabilmente è proprio quella giusta.



FASE 1



# VAGARE ALLA CIECA

“Scopriamo le esposizioni solo quando qualcosa va storto.”

Non a caso è stata usata la locuzione “alla cieca”. L’azienda non ha un quadro affidabile della propria superficie di attacco esterna. Gli asset vengono menzionati nelle discussioni solo dopo gli incidenti, non prima. Il team di sicurezza sa che ci sono delle lacune, ma non sa quali siano, dove si trovino né quanto siano gravi. Si eseguono scansioni, ma il risultato è un elenco di criticità di cui nessuno si fida completamente e che cresce più velocemente di quanto chiunque possa analizzare.

Ciò che distingue la Fase 1 dalla Fase 2 non sono gli strumenti, perché molte aziende in questa fase dispongono già di scanner, piattaforme SIEM e flussi di lavoro per la gestione dei ticket. Quello che manca è una struttura: non esiste una cadenza sistematica per l’individuazione delle vulnerabilità, né un modello di responsabilità definito, né un metodo coerente per verificare se i risultati rilevati rappresentino un rischio reale. Esiste un’attività, ma non un programma.

## Come la descrivono i team

“Non facciamo altro che correre ai ripari. Non riusciamo mai a giocare d’anticipo.”

“È arrivato il rapporto sul test di penetrazione ma abbiamo ancora metà delle questioni aperte dall’anno scorso.”

“La verità è che non so quanti asset connessi a Internet abbiamo. Nessuno lo sa.”

## Che aspetto assume a livello aziendale

Le riunioni sulla sicurezza sono dominate dall’incidente più recente o dai risultati dell’ultimo audit. Gli aggiornamenti del CISO al consiglio di amministrazione vertono sullo stato di conformità, non sull’esposizione. Quando viene pubblicato un nuovo CVE critico, la prima domanda è: “Ce l’abbiamo quel software?”. Nessuno ha una risposta certa. Le discussioni sulle misure correttive iniziano più spesso con “A quale team spetta?” piuttosto che con “Quanto è sfruttabile?”. Il rapporto sul test di penetrazione di otto mesi fa è ancora aperto in un foglio di calcolo su cui non è mai stata intrapresa alcuna azione concreta.

## Cosa impedisce alle aziende di progredire

Il motivo più comune non è il budget, ma il fatto che l'azienda abbia definito la sicurezza più come un'attività di conformità che di gestione del rischio, e per la conformità non serve sapere cosa è sfruttabile, ma solo cosa è documentato. Questo crea un limite strutturale: il programma produce prove dell'attività svolta piuttosto che prove della riduzione del rischio, e la dirigenza non conosce ancora la differenza e per questo non la richiede.

Il collo di bottiglia operativo in Fase 1 è il collasso del rapporto segnale-rumore. Gli scanner generano migliaia di risultati senza alcun meccanismo per distinguere i rischi reali dal rumore di fondo. Il risultato? Tutte le risorse del team vengono impiegate nella fase di cernita, e nessuna nella fase correttiva. I volumi danno una falsa impressione di lavoro costante, ma non garantiscono risultati in termini di sicurezza.

Il terzo ostacolo è l'assunzione di responsabilità. L'esposizione si colloca all'intersezione tra sicurezza, informatica e ingegneria. Se nessuno è responsabile del quadro d'insieme, nulla viene considerato urgente finché qualcosa non si rompe.

## Quando si è pronti a cambiare

Le aziende tendono a fare passi avanti quando accade qualcosa che rende innegabile il divario esistente, solitamente un incidente che porta alla luce un asset di cui nessuno conosceva l'esistenza, oppure una domanda del consiglio di amministrazione che mette in luce la discrepanza tra la situazione dichiarata e quella reale. Il passaggio da un approccio basato sulla conformità a uno orientato al rischio richiede solitamente una figura interna che ne promuova l'adozione: qualcuno in grado di inquadrare il dibattito non in termini di "ci servono più strumenti", ma piuttosto di "dobbiamo sapere a quali rischi siamo effettivamente esposti".

## Cosa deve cambiare a livello strutturale

Il prerequisito per la Fase 2 non è l'acquisto di uno o più strumenti, ma una decisione che porti a un'assunzione di responsabilità. Qualcuno deve assumersi la responsabilità dell'inventario degli asset esterni nel suo complesso, non solo della sicurezza degli asset già noti. Una volta stabilita tale responsabilità, seguiranno le strutture di supporto: l'individuazione continua degli asset al di fuori dell'ambito predefinito, una prioritizzazione basata sul rischio che tenga conto del contesto aziendale oltre che dei punteggi di criticità e SLA definiti che vengano effettivamente applicati anziché rimanere solo teorici.

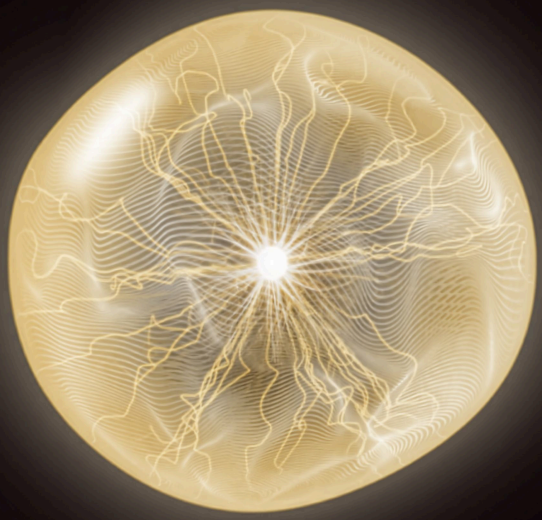
### Funzionalità che consentono questa transizione

- Una gestione della superficie di attacco esterna che scopre asset al di fuori dell'inventario predefinito: cloud, SaaS, filiali, terze parti
- Prioritizzazione basata sul rischio che integra criticità aziendali e raggiungibilità, non solo CVSS
- Flussi di lavoro che collegano gli asset scoperti ai team che ne sono responsabili

SCARICA IL PIANO DI PROGRESSIONE DALLA FASE 1 ALLA FASE 2

FASE 2

# AMBITO PIÙ CHIARO, MAGGIORE SPERANZA



"Sappiamo più di prima, ma non sappiamo ancora se è abbastanza."

Le aziende che arrivano alla Fase 2 hanno lavorato sodo. Adesso hanno un programma formale di gestione delle vulnerabilità. Gli asset principali sono stati inventariati. Effettuano test secondo un calendario prestabilito, non solo a seguito di incidenti. I team di sicurezza hanno voce in capitolo nelle decisioni e un mandato definito. Il CISO è in grado di redigere un rapporto sullo stato della sicurezza senza troppe difficoltà.

Il nome di questa fase riflette sia i progressi compiuti che i limiti esistenti. L'ambito di applicazione si è ampliato: più asset, maggiore copertura dei test, responsabilità più strutturate. E c'è davvero una speranza: la speranza che gli asset scoperti siano quelli rilevanti, la speranza che il pentest trimestrale abbia individuato ciò che conta, la speranza che il grado di sfruttabilità rifletta approssimativamente la gravità. Si tratta di speranze tutt'altro che irragionevoli, ma pur sempre di speranze, non di prove certe. Il programma è strutturato, ma non è ancora convalidato.

## Come la descrivono i team

"I risultati dell'ultimo pentest sono già superati quando si avvia il ciclo successivo."

"Abbiamo una buona copertura degli asset di cui siamo a conoscenza. Il problema sono quelli che non conosciamo."

"In teoria abbiamo un approccio basato sul rischio. Nella pratica, però, ci occupiamo ancora di CVSS 9 e 10."

## Che aspetto assume a livello aziendale

Il team di sicurezza segue un programma cadenzato: test di penetrazione trimestrali, scansioni periodiche delle vulnerabilità e una coda di ticket con responsabili ben definiti. La rendicontazione al consiglio di amministrazione è passata dalla semplice comunicazione dello stato di conformità a un'analisi dell'esposizione attuale alle vulnerabilità. Quando viene pubblicato un nuovo CVE, esiste una procedura per la verifica, ma è manuale e più lenta di quanto si vorrebbe.

## Cosa impedisce alle aziende di progredire

L'ostacolo strutturale in Fase 2 è il divario tra la frequenza dei test e la velocità del contesto. I test di penetrazione trimestrali sono stati concepiti per contesti che cambiavano ogni tre mesi, ma al giorno d'oggi la maggior parte dei contesti aziendali cambia quotidianamente. Il programma non è difettoso; semplicemente non è in linea con il ritmo con cui evolve il problema. Il collo di bottiglia operativo in Fase 2 è la convalida manuale. Per confermare che una vulnerabilità sia effettivamente sfruttabile è necessario un intervento umano. Quando questo step non riesce a scalare, le code delle azioni correttive si riempiono di risultati non convalidati e i team ricorrono a criteri empirici informali: qualsiasi risultato superiore a CVSS 8 viene considerato sfruttabile. È più veloce, ma è anche molto meno preciso e non contribuisce né a ridurre il lavoro arretrato né ad aumentare la fiducia nei risultati rimanenti.
A peggiorare entrambi i problemi è la misurazione. La maggior parte dei programmi di Fase 2 tiene traccia della copertura e dell'attività: risultati individuati, risultati risolti, conformità SLA. Queste metriche sembrano indicare un progresso, ma non rispondono alla domanda che interessa davvero alla leadership: la nostra esposizione sfruttabile sta diminuendo?

## Quando si è pronti a cambiare

Il fattore scatenante è solitamente una scoperta che dovrebbe essere stata individuata prima, come un'esposizione sfruttabile scoperta tra un ciclo di test e l'altro, durante una verifica non programmata o da un ricercatore esterno. La domanda che ne consegue ("da quanto tempo ci sarà?") è spesso il catalizzatore che porta a riconoscere che la convalida periodica non è più in grado di stare al passo. La questione fondamentale è se l'azienda sia pronta a passare dai test programmati al monitoraggio continuo e se la leadership sia disposta a finanziare il cambiamento strutturale che questo richiede.

## Cosa deve cambiare a livello strutturale

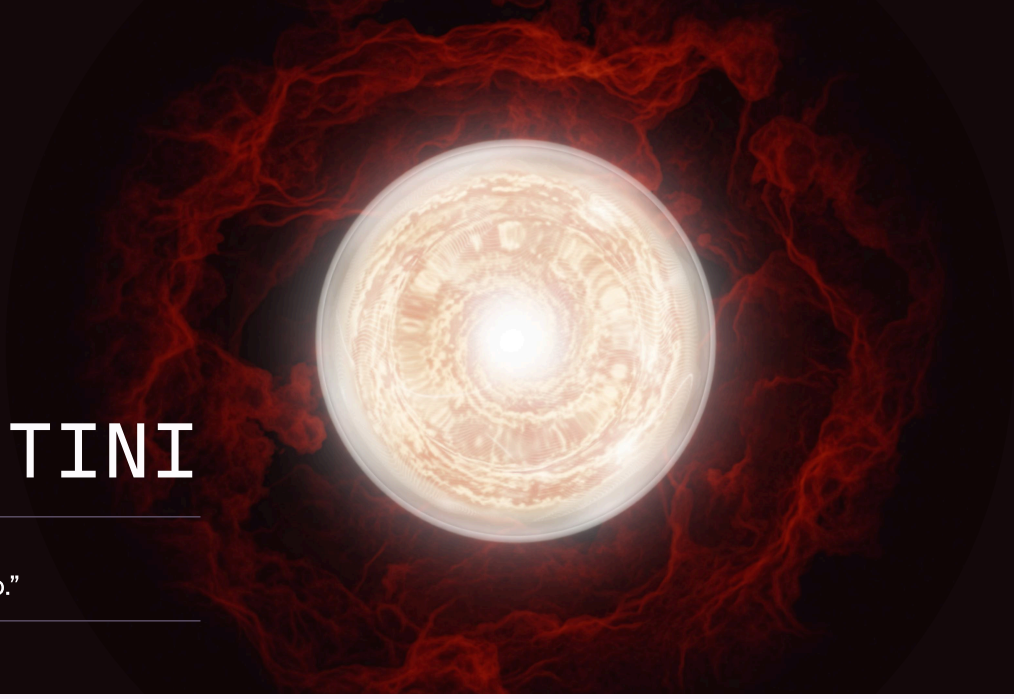
Per passare dalla Fase 2 alla Fase 3 è necessario colmare il divario tra la frequenza dei test e la velocità del contesto, il che implica un monitoraggio esterno continuo che rilevi le nuove esposizioni a mano a mano che emergono, non solo in occasione della successiva scansione programmata. Ai fini di questo passaggio, è anche necessario che la convalida delle sfruttabilità venga trattata come uno step del flusso di lavoro, non come un'indagine manuale. Se la conferma dei risultati viene automatizzata anziché dipendere dall'intervento umano, si elimina il collo di bottiglia che si crea in fase di cernita dei risultati. Anche i parametri di misurazione devono cambiare: il programma dovrebbe tenere traccia dei rischi sfruttabili eliminati, non solo dei risultati considerati risolti.

### Funzionalità che consentono questa transizione

- Un monitoraggio continuo della superficie di attacco esterna che segnala nuovi asset e modifiche tra un ciclo di pentest e l'altro
- Convalida automatizzata della sfruttabilità che conferma quali risultati siano effettivamente raggiungibili e verificabili
- Inoltro integrato delle azioni correttive affinché i risultati convalidati raggiungano il responsabile competente senza bisogno di passaggi di consegna manuali

SCARICA IL PIANO DI PROGRESSIONE DALLA FASE 2 ALLA FASE 3

FASE 3



# UNIRE I PUNTINI

"Sappiamo cos'è sfruttabile. Stiamo iniziando a capire come si incastra il tutto."

La Fase 3 rappresenta un vero e proprio punto di svolta operativo. La convalida non è più periodica; è continua. I tempi morti tra i cicli di test si sono in gran parte ridotti. Le sfruttabilità vengono confermate (non solo ipotizzate in base ai punteggi di gravità) prima di segnalare i risultati. I flussi di lavoro di correzione sono integrati con gli strumenti di sicurezza, quindi i risultati convalidati vengono inoltrati automaticamente anziché finire in una casella di posta condivisa.
Il nome stesso della fase evidenzia la novità: per la prima volta, il programma non si limita a catalogare le falle in modo isolato, ma le assembla all'interno di un quadro che illustra come potrebbe effettivamente agire un aggressore. I singoli risultati convalidati vengono mappati rispetto ai percorsi di attacco. La prioritizzazione passa da "qual è il CVSS più alto?" a "cosa può essere concatenato a un danno reale?". Si tratta di una visione radicalmente diversa. Il limite è che la creazione e il mantenimento di questo quadro richiedono ancora un intervento umano significativo. Il programma vede i puntini, ma collegarli rapidamente e su larga scala è ancora un'operazione manuale.

## Come la descrivono i team

"Sappiamo cos'è sfruttabile. Adesso la sfida consiste nel tenere il passo con la rapidità con cui cambia il contesto."

"I nostri risultati vengono convalidati ancor prima di essere inseriti nella coda. Il problema è collegarli all'interno di un quadro completo di attacco."

"Possiamo comunicare al consiglio di amministrazione quali vulnerabilità sono state confermate come sfruttabili, ma non siamo ancora in grado di spiegare come potrebbero essere concatenate da un aggressore."

## Che aspetto assume a livello aziendale

I ritmi quotidiani del team di sicurezza sono cambiati. I risultati arrivano già convalidati. I ticket vengono inoltrati automaticamente ai responsabili. In fase di cernita dei risultati il dibattito è passato da "si tratta di una vulnerabilità reale?" a "come si inserisce all'interno del quadro più ampio di esposizione?". L'MTTR viene monitorato attivamente, mostra un andamento al ribasso ed è definito in base ai rischi sfruttabili risolti piuttosto che al numero di ticket.

## Cosa impedisce alle aziende di progredire

Il limite è il tempo necessario per le operazioni. La gestione di uno scenario complesso di attacchi mirati, che segua le catene di attacco tra i vari sistemi, verifichi percorsi di intrusione realistici e si adatti ai cambiamenti del contesto, richiede un notevole impiego di tempo da parte degli esperti. I singoli risultati possono essere convalidati in modo continuo; tuttavia, la simulazione di cosa farebbe effettivamente un aggressore sofisticato con tali risultati rimane un'operazione manuale e richiede un impiego massiccio di risorse. Il programma vede i puntini, ma collegarli a grande velocità è ancora un'operazione umana.
Il collo di bottiglia operativo in Fase 3 è la scala delle emulazioni. Il programma è in grado di convalidare continuamente i singoli risultati, ma tradurli in un quadro completo e in tempo reale di come tali risultati si combinino in percorsi di attacco sfruttabili richiede ancora l'intervento umano per ogni scenario. Man mano che gli ambienti diventano più complessi, il divario tra ciò che può essere convalidato e ciò che può essere emulato diventa il fattore limitante in termini di rapidità. Esiste inoltre un disallineamento a livello aziendale: le operazioni procedono senza sosta, ma la governance non tiene il passo. I report per la dirigenza, le metriche del consiglio di amministrazione e i KPI sono spesso ancora basati su istantanee periodiche piuttosto che su dati in tempo reale. Il programma genera più informazioni di quante l'azienda abbia imparato a gestire.

## Quando si è pronti a cambiare

Le aziende in Fase 3 sono pronte a compiere il passo successivo quando si trovano di fronte a una domanda specifica alla quale non sono ancora in grado di rispondere rapidamente: se oggi venisse scoperta una nuova classe di vulnerabilità, quanto tempo ci vorrebbe per confermare se la nostra superficie di esposizione è interessata? Se la risposta più onesta da dare è "giorni" e non "ore", significa che il principale fattore limitante è il divario tra la capacità di rilevamento e quella di emulazione. A quel punto ci si dovrà chiedere se la dirigenza è disposta a investire per colmare quel gap e se la governance del programma consente un funzionamento autonomo.

## Cosa deve cambiare a livello strutturale

Il passaggio alla Fase 4 richiede la sostituzione del coordinamento manuale degli scenari di attacco con un'emulazione automatizzata in grado di adattarsi ai cambiamenti del contesto senza l'intervento umano per ogni singolo scenario. Richiede inoltre di chiudere il cerchio tra i dati operativi in tempo reale e la visibilità da parte della dirigenza tramite dashboard sullo stato di sicurezza in tempo reale ricavate direttamente dai risultati del programma, anziché compilate periodicamente. Richiede inoltre una decisione a livello di governance: preautorizzare i protocolli di risposta rapida in modo che, quando emerge una nuova superficie di esposizione, il programma possa reagire nel giro di poche ore anziché attendere una riunione di valutazione.

### Funzionalità che consentono questa transizione

- Un'emulazione automatizzata degli attacchi che si adatta ai cambiamenti del contesto senza necessità di un intervento manuale per ogni singolo scenario
- Una valutazione in tempo reale dello stato di sicurezza e metriche pronte per la presentazione al consiglio di amministrazione, tutto ricavato direttamente dai dati in tempo reale del programma
- Un'analisi continua della catena di attacchi che illustra in che modo i risultati convalidati si combinano per formare percorsi sfruttabili

SCARICA IL PIANO DI PROGRESSIONE DALLA FASE 3 ALLA FASE 4

FASE 4

# UNA VISIONE CHIARA

"Per la prima volta, sappiamo sempre cosa vede un aggressore, in qualunque momento."

Questa fase non è un livello ideale a cui aspirare, ma è l'aspetto che assume la gestione dell'esposizione quando tutti i limiti strutturali delle fasi precedenti (scoperta reattiva, convalida periodica, interventi manuali e visibilità limitata da parte della dirigenza) sono stati risolti. Il programma è continuo, adattivo e in gran parte autonomo. L'attenzione del team di sicurezza è rivolta alle decisioni strategiche e alla gestione delle eccezioni, non alla cernita dei falsi allarmi o alla ricostruzione manuale dei percorsi di attacco.

Il nome è quanto mai azzeccato. Per la prima volta, l'azienda ha una visione completa e in tempo reale della propria superficie di attacco esterna dal punto di vista di un aggressore: non solo quali asset sono presenti, ma quali sono raggiungibili, quali sono sfruttabili, come si concatenano tra loro e quali sono i probabili percorsi di intrusione in questo momento. È un quadro che si aggiorna continuamente, man mano che il contesto cambia. Non attende il ciclo di scansione successivo né il prossimo pentest.

Ciò che contraddistingue questa fase non è una singola funzionalità, ma l'assenza delle lacune strutturali che caratterizzano ogni fase precedente. Non ci sono tempi morti o punti ciechi. Non c'è lavoro di cernita arretrato accumulatosi a causa di risultati non convalidati. Non c'è alcun divario tra quello che il programma conosce e quello che vede la dirigenza. L'azienda non reagisce più all'esposizione: la anticipa.

## Cosa è stato fatto per arrivare fino a qui

L'azienda ha sostituito la gestione manuale degli scenari di attacco con un'emulazione automatizzata che si adatta continuamente ai cambiamenti del contesto. Ha chiuso il cerchio tra i dati operativi in tempo reale e le comunicazioni alla dirigenza. Ha preso inoltre una decisione di governance: protocolli di risposta rapida preautorizzati e percorsi di escalation definiti per il funzionamento autonomo, che hanno consentito al programma di reagire con la velocità di una macchina senza richiedere una decisione umana ad ogni passaggio.

## Che aspetto assume a livello aziendale

Le conversazioni del team di sicurezza sullo stato attuale hanno cambiato registro. La domanda non è più “a cosa siamo esposti?”, perché il programma fornisce continuamente una risposta. Le domande sono “in quanto tempo riusciamo a risolvere il problema?” e “quali sono le attività a maggiore impatto su cui il nostro personale dovrebbe concentrarsi e che l’automazione non è ancora in grado di gestire?”. Le comunicazioni al consiglio di amministrazione sono ricavate direttamente dai dati in tempo reale del programma. I team di ingegneri ricevono risultati convalidati e inoltrati senza che il team di sicurezza debba consegnarli manualmente. Quando viene rilevata una nuova esposizione, il programma conferma entro poche ore (non giorni) se la superficie ne è interessata.

In questa fase, il team di sicurezza è più ridotto in termini di copertura della superficie rispetto a qualsiasi fase precedente, poiché l’automazione ha assorbito il lavoro che in precedenza richiedeva un intervento umano di cernita dei risultati. Le competenze si sono spostate verso livelli più alti: il team si occupa dei problemi che richiedono capacità di giudizio, non di quelli che richiedono un intervento su larga scala.

### Come la descrivono i team

- “Veniamo a conoscenza di una nuova esposizione ancora prima che gli aggressori possano sfruttarla.”
- “La domanda che ci facciamo adesso non è se siamo esposti, ma quanto velocemente possiamo risolvere una vulnerabilità.”
- “Posso illustrare al consiglio di amministrazione la nostra situazione attuale sulla base dei dati generati nelle ultime 24 ore. Questo prima non era possibile.”

## Requisiti per restare in questa fase

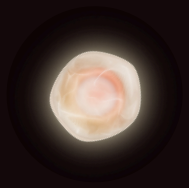
La Fase 4 non è un punto d’arrivo che, una volta raggiunto, si mantiene da solo. Le tecniche di attacco si evolvono e la qualità dell’emulazione del programma deve evolversi di pari passo. Ci sono nuove categorie di infrastrutture, tra cui i sistemi di intelligenza artificiale, i flussi di lavoro basati su agenti e le nuove integrazioni SaaS, che richiedono un aggiornamento continuo dei modelli di scoperta e convalida.

I requisiti per l’azienda sono importanti tanto quanto quelli tecnici. Le strutture di governance devono supportare il funzionamento autonomo senza rappresentarne un ostacolo: protocolli di risposta preautorizzati, soglie di escalation chiaramente definite e un allineamento della leadership su cosa significhi effettivamente e nella pratica la visibilità in tempo reale dello stato di sicurezza. Se un programma raggiunge la Fase 4 ma poi si introducono barriere burocratiche alle risposte automatizzate, la sua capacità finirà per declinare verso la Fase 3.

Lo scenario più comune di ritorno alla Fase 3 è il cambio di leadership: un nuovo CISO che reintroduce controlli di revisione manuali o un consiglio di amministrazione che perde fiducia nel funzionamento autonomo dopo un falso positivo. Per mantenere la Fase 4, “Una visione chiara”, serve una gestione attiva del mandato organizzativo, non solo della capacità tecnica.

## Funzionalità che definiscono questa fase

- Un'emulazione autonoma degli attacchi che si adatta continuamente ai cambiamenti del contesto senza necessità di un intervento manuale per ogni singolo scenario
- Una prioritizzazione predittiva e dinamica che si adatta automaticamente all'emergere di nuove vulnerabilità e ai cambiamenti nel contesto della catena di attacco
- Un modello della superficie di attacco in tempo reale che mette in correlazione i cambi di identità, infrastruttura, SaaS e terze parti in un quadro unificato e costantemente aggiornato
- Integrazione completa del programma, dal rilevamento delle esposizioni alla convalida dei risultati fino al completamento della correzione, con un numero minimo di passaggi manuali

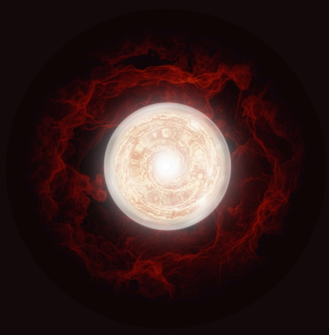


### FASE 1 → FASE 2

Passare dalla Fase 1 alla Fase 2 può essere raggiunto in pochi mesi con un impegno mirato e una responsabilità chiara.

### FASE 2 → FASE 3

Dalla Fase 2 alla Fase 3 richiede in genere da sei a diciotto mesi, a seconda della complessità dell'ambiente e della profondità di integrazione.

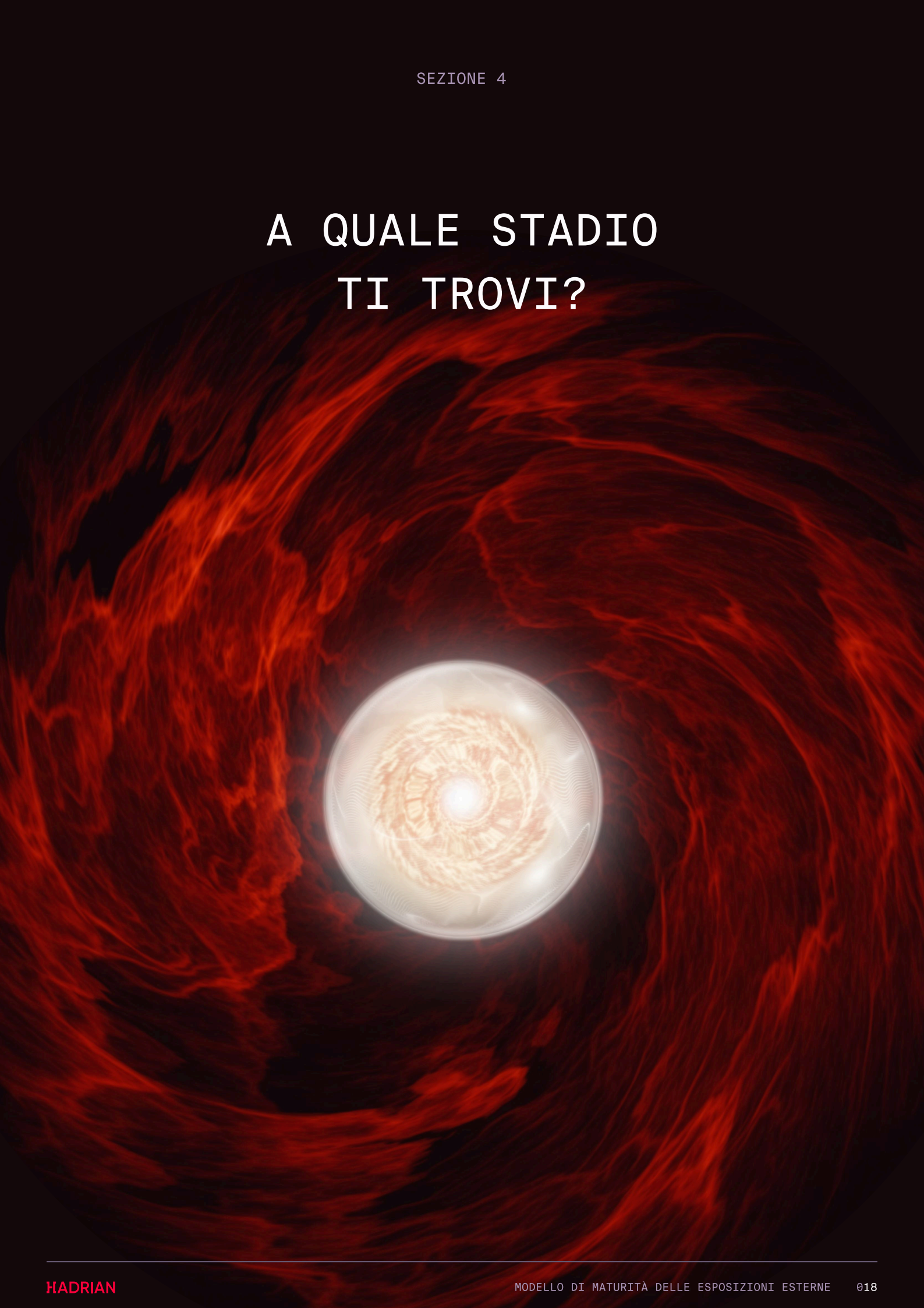


### FASE 3 → FASE 4

La transizione alla Fase 4 è continua; richiede un investimento operativo sostenuto piuttosto che un progetto definito. Ciò che accelera il progresso non è una maggiore dotazione di strumenti, ma la chiarezza: chiarezza sulla titolarità dell'esposizione, definizioni chiare di come appare il lavoro completato e misurazione del rischio sfruttabile eliminato piuttosto che dell'attività generata.

SEZIONE 4

# A QUALE STADIO TI TROVI?



La maggior parte delle aziende che lavorano per avanzare tra queste quattro fasi scopre che la risposta più sincera si colloca a metà strada tra due di esse. Magari la scoperta è più matura rispetto alla convalida o la convalida è più matura rispetto all'inoltro dell'azioni correttive. Un punteggio complessivo può dirti approssimativamente dove ti trovi, ma non può dirti quale dimensione specifica stia frenando il resto del processo.

Questa distinzione conta più di quanto possa sembrare. Un programma che registra una media di Fase 3 ma ha una convalida di Fase 1 non è un programma di Fase 3, ma un programma con un collo di bottiglia di Fase 1 che sta penalizzando le prestazioni di tutte le altre dimensioni. Gli SLA di correzione, la rendicontazione al consiglio di amministrazione, il livello di automazione: tutto è limitato dall'anello più debole, non da quello più forte. La maggior parte delle valutazioni interne trascura questo aspetto perché valuta la situazione complessiva anziché scomporla e analizzarla in base alle singole dimensioni operative.

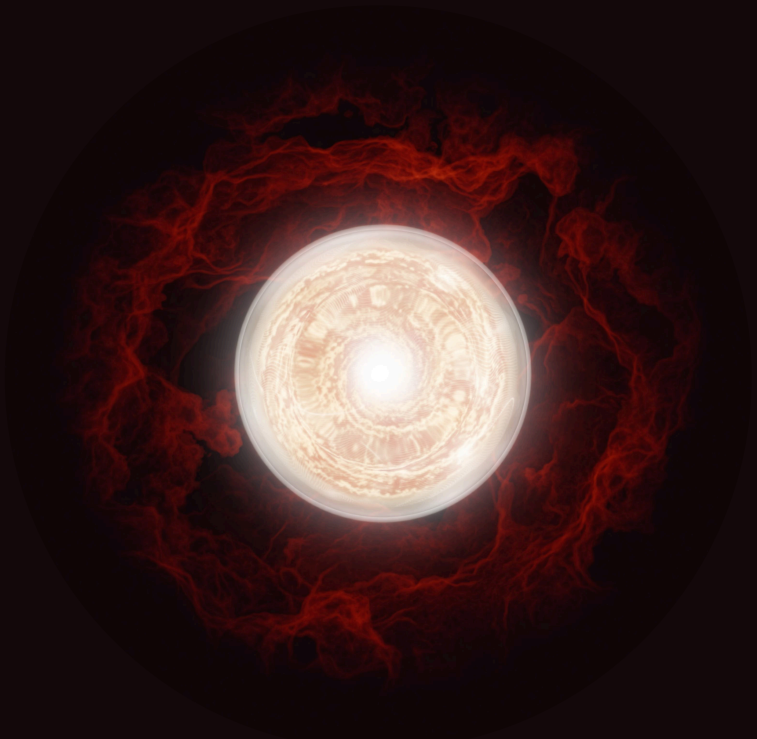
L'autovalutazione interattiva, invece, è strutturata in modo diverso. Valuta il tuo programma in base a sei dimensioni indipendenti e le pondera per individuare dov'è maggiore il divario tra la tua situazione attuale e il tuo profilo di rischio. Il risultato non è un numero, ma un'analisi dettagliata della tua situazione per ciascuna dimensione, un'indicazione del tuo collo di bottiglia più critico e un piano d'azione specifico per fase su cui il tuo team può intervenire direttamente.

Se sai già in quale fase ti trovi, vale comunque la pena completare la valutazione. La sua struttura basata sulle dimensioni, infatti, la rende particolarmente utile in un incontro con la dirigenza, perché non basta dire "siamo in Fase 2", ma occorre specificare "siamo in Fase 3 per quel che riguarda la scoperta, ma in Fase 1 per la convalida, e questo è il tempo necessario per colmare questo divario".

## VALUTATI:

Fai la valutazione interattiva per un profilo di maturità personalizzato e un piano d'azione

SCOPRI LA TUA FASE DI MATURITÀ



# Domande frequenti

### È necessario che tutte le aziende raggiungano la Fase 4, “Una visione chiara”?

No, la Fase 4 è indicata per quelle aziende in cui le conseguenze di una violazione giustifichino una convalida continua e autonoma. Per molte aziende, la Fase 2 o la Fase 3 rappresentano l’obiettivo giusto per la maggior parte della loro superficie di attacco, mentre le pratiche della Fase 4 sono riservate agli asset di maggior valore. La domanda giusta non è come raggiungere la Fase 4, bensì quali asset e classi di rischio richiedono un trattamento di Fase 4.

### Usiamo già molti strumenti. Perché la nostra maturità è ancora bassa?

L’adozione di strumenti non equivale alla maturità del programma. Il 93% delle aziende utilizza scanner di vulnerabilità; solo il 40% ha adottato test di penetrazione automatizzati. Per la maggior parte delle aziende, l’adozione di molti strumenti non si è tradotta in una maggiore rapidità delle azioni correttive, perché il fattore limitante non è quali strumenti usano, bensì se tali strumenti operano all’interno di una struttura in grado di convalidare le sfruttabilità, di integrarsi con le azioni correttive e di misurare i risultati piuttosto che la sola attività.

### Abbiamo un programma CTEM attivo e operativo. Perché questo non si traduce in azioni correttive più rapide?

La maggior parte dei programmi CTEM misura il successo secondo criteri che non riflettono l’effettiva riduzione del rischio. Il 67% delle aziende misura il CTEM in base alle lacune di copertura individuate; solo il 33% monitora la riduzione delle esposizioni sfruttabili nel tempo. Se la convalida delle sfruttabilità non viene considerata un risultato prioritario e se non vi è un allineamento delle responsabilità che colleghi i risultati convalidati alle persone in grado di risolverli, il CTEM genera solo più risultati senza migliorare gli esiti che contano.

### Abbiamo piena visibilità sulla pipeline. Perché la nostra esposizione non diminuisce?

La scoperta e la convalida sono problemi distinti, e la maggior parte dei programmi li tratta alla stregua di uno solo. Ampliare la copertura dell’EASM o aumentare la frequenza delle scansioni genera più risultati, ma se non esiste un meccanismo automatizzato per confermare quali di questi risultati siano realmente sfruttabili, il risultato è solo un aumento del lavoro arretrato, non un miglioramento dello stato di sicurezza. Un maggior numero di risultati scoperti senza una capacità di convalida aumenta il carico di lavoro degli analisti senza ridurre i rischi effettivamente sfruttabili. Pertanto, il problema di base è raro che sia il numero di risultati trovati dal programma, ma piuttosto il numero di risultati che possono essere trovati, confermati come reali e inoltrati per la correzione prima che un aggressore possa sfruttarli.

# Informazioni su Hadrian

Hadrian è una piattaforma di sicurezza offensiva creata per team che hanno bisogno di prove concrete, non di previsioni. Mentre gli strumenti tradizionali partono da un inventario già noto, Hadrian parte da zero: scopre gli asset, ricostruisce i percorsi di attacco e convalida le vulnerabilità proprio come farebbe un aggressore, non come farebbe uno scanner. Funziona in modo continuo, senza finestre di scansione né cicli di test, quindi non ci sono mai discrepanze tra lo stato reale del tuo ambiente e ciò di cui è a conoscenza il tuo programma.

SCOPRI DI PIÙ: HADRIAN.IO

FROST & SULLIVAN BEST PRACTICES AWARDS

GIGAOM RADAR REPORT LEADER 2025

Gartner Peer Insights 4.9/5 ★

AICPA SOC · ISO 27001

## PERFORMANCE SUPPORTATA DAGLI ANALISTI

"Hadrian è classificata come Outperformer grazie all'implementazione delle sue capacità di AI agentiva e alla costante espansione dei suoi moduli di test offensivi automatizzati negli ultimi 12 mesi"

CHRIS RAY
FIELD CTO, GIGAOM

**10x** PIÙ VISIBILITÀ SUI RISCHI CRITICI

**80%** RIDUZIONE DELL'MTTR

**10h** RISPARMIATI A SETTIMANA IN MEDIA

## SCELTO DA

NBC · amadeus · McKESSON · BLINQX · CRÉDIT AGRICOLE · LEROY MERLIN · SHV · ABN·AMRO · London Business School · RITUALS... · SIEMENS energy · LOTTOMATICA · FP FRANCISCO PARTNERS · CHRISTIE'S · BIOLANDES · WeatherTech · BLINQX · DAMEN · jamf · =exact · ICT GROUP · nedap · celio* · Inova · XM Cyber · AROMA360

E ALTRI 300+