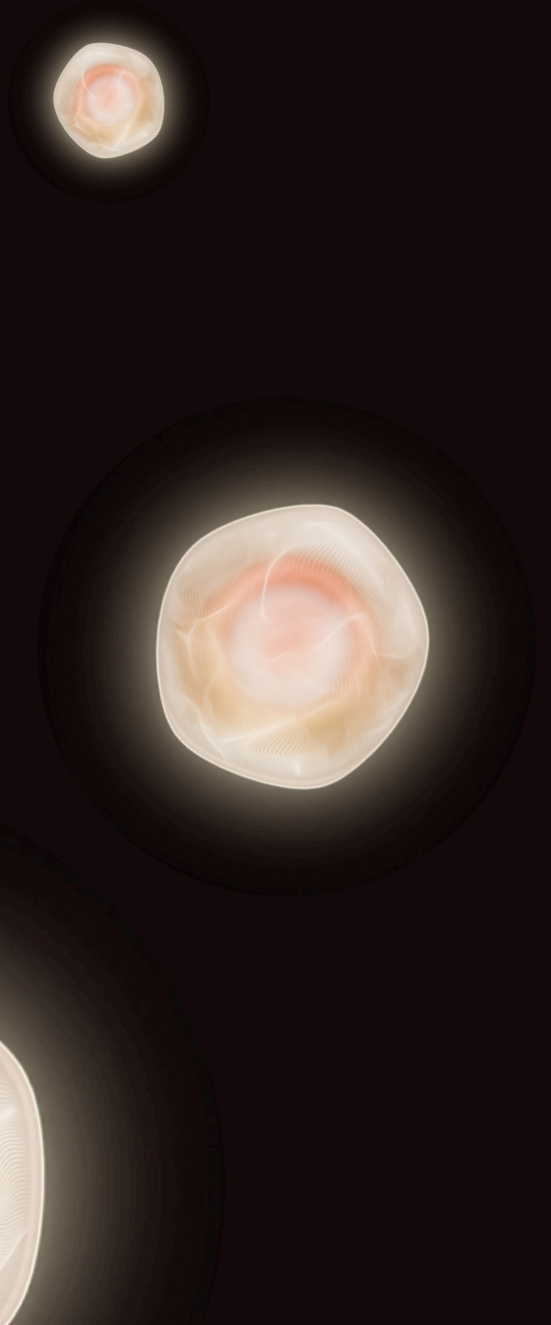
L'efficacia del tuo programma di esposizione dipende dal suo anello più debole.

La maggior parte dei responsabili della sicurezza delle informazioni (CISO) sa bene che il proprio programma non è ancora all'altezza delle aspettative. La difficoltà sta nel capire esattamente quale aspetto stia frenando il resto del processo e quali vantaggi ne deriverebbero in termini di velocità di correzione, affidabilità della convalida e visibilità da parte della dirigenza, una volta risolto quel singolo problema.

Il divario raramente riguarda le risorse. Le organizzazioni a ogni livello di maturità provano lo stesso senso di frustrazione: gli strumenti vengono implementati e i processi definiti, eppure l'arretrato di interventi risolutivi cresce, i risultati si accumulano più velocemente di quanto chiunque possa convalidarli e il consiglio di amministrazione vuole risposte che il programma non è ancora in grado di fornire.

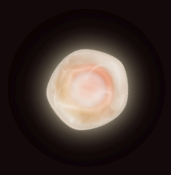
Il motivo è strutturale. La gestione dell'esposizione esterna presenta quattro distinti approcci operativi. La maggior parte delle organizzazioni è più forte in alcune aree rispetto ad altre. L'area più debole limita il potenziale di tutte le altre. Finché tale criticità non viene identificata e colmata, il progresso si interrompe, a prescindere dall'introduzione di eventuali altri cambiamenti



In cosa consiste il modello

Il Modello di maturità dell'esposizione di Hadrian delinea quattro fasi della gestione dell'esposizione esterna, da quella reattiva e non rilevata a quella continua e autonoma. Ogni fase rappresenta un approccio operativo ben definito, basato su modelli di programma reali, e non un semplice quadro teorico. Il modello utilizza sette dimensioni operative per indicare la posizione attuale dell'organizzazione e individuare gli ostacoli operativi che ne limitano il progresso.

PERCHÉ IL PROCESSO DI MATURAZIONE È IMPORTANTE

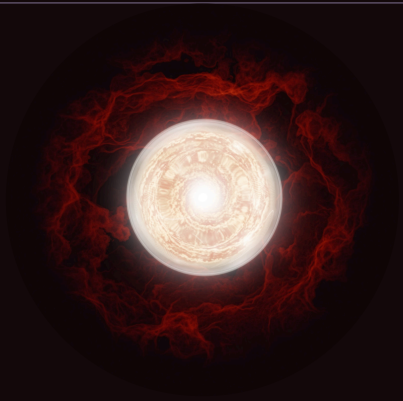


DALLA FASE 1 ALLA FASE 2

L'MTTR scende da oltre 90 giorni a circa 45. La copertura passa da meno del 20% al 40-60%.

DALLA FASE 2 ALLA FASE 3

Le percentuali di veri positivi salgono al 40-60%. Il rispetto degli SLA raggiunge il 60-80%. L'MTTR si riduce a 15-45 giorni.



DALLA FASE 3 ALLA FASE 4

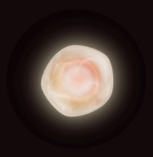
La copertura supera il 95%. Le vulnerabilità critiche vengono risolte entro 48 ore. La segnalazione delle vulnerabilità viene confermata nel giro di poche ore, non di giorni.

IL PERICOLO NON ASPETTA

Il tempo medio che intercorre tra la rivelazione di una vulnerabilità e il suo sfruttamento effettivo è sceso da 32 a 5 giorni. Quasi una vulnerabilità su tre viene ora sfruttata il giorno stesso della sua rivelazione o prima.

La maggior parte dei programmi di sicurezza si basa su cicli di valutazione settimanali e test trimestrali. Il divario tra la rapidità degli attacchi e la maturità dei programmi non è un rischio potenziale, ma una realtà già in atto.

Le quattro fasi



FASE 1

Andare alla cieca

Le vulnerabilità vengono individuate in modo reattivo. La responsabilità non è chiara. La lista delle azioni risolutive cresce più rapidamente di quanto si riduca. Il team dedica gran parte delle proprie risorse a problemi che si rivelano irrilevanti.

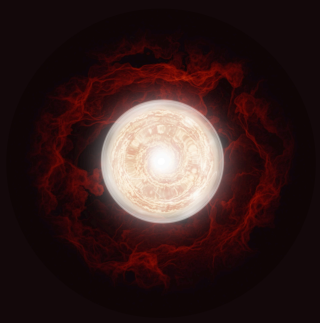
- Rilevamento reattivo
- Nessuna proprietà sistematica degli asset
- Triage basato sul CVSS
- Reportistica mirata alla conformità

FASE 2

Più visibilità, più opportunità

Il programma è ben strutturato e la copertura sta migliorando. Il punto critico è la convalida: la sfruttabilità viene dedotta dai punteggi di gravità piuttosto che confermata. L'MTTR è compreso tra 45 e 90 giorni.

- Penetration test programmati
- Copertura degli asset noti
- Analisi manuale della vulnerabilità
- Metriche basate sulle attività

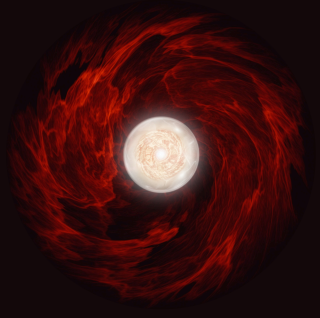


FASE 3

Unire i puntini

I risultati vengono convalidati prima di essere inseriti in coda. I tassi di veri positivi raggiungono il 40-60%. L'MTTR si riduce a 15-45 giorni. La difficoltà consiste nel collegare i risultati per ottenere un quadro completo dell'attacco senza un intervento manuale significativo.

- Monitoraggio continuo
- Validazione automatica
- Percorsi risolutivi integrati
- Misurazione dei rischi sfruttabili



FASE 4

Panoramica completa

Il rilevamento è continuo, la convalida è autonoma e i responsabili possono visualizzare i dati in tempo reale sullo stato di sicurezza. La copertura supera il 95%. Le vulnerabilità critiche vengono risolte entro 48 ore. I nuovi exploit vengono confermati nel giro di poche ore.

- Emulazione automatica
- Visibilità in tempo reale della postura
- Prioritizzazione predittiva
- Reportistica in tempo reale

LA MAGGIOR PARTE DEI PROGRAMMI PRESENTA UN ASPETTO CHE NE LIMITA LA PORTATA.

L'autovalutazione interattiva assegna un punteggio al tuo programma in tutte e sette le dimensioni in modo indipendente, individua i tuoi punti critici specifici e genera un piano d'azione su misura per la tua fase attuale, che il tuo team potrà mettere in pratica immediatamente. Bastano cinque minuti.

FAI IL TEST SU HADRIAN.IO

INFORMAZIONI SU HADRIAN

Hadrian è una piattaforma di sicurezza offensiva che individua e verifica le vulnerabilità esterne proprio come farebbe un hacker: partendo da un ambito non predefinito, seguendo i percorsi di attacco ovunque essi conducano e confermando l'autenticità di ogni risultato prima che raggiunga il tuo team. Premiata dal Gartner Hype Cycle for Security Operations, nonché da GigaOm e Frost & Sullivan.

PER SAPERNE DI PIÙ: HADRIAN.IO

Frost & Sullivan Best Practices Awards

GigaOm Radar Report Leader 2025

Gartner Peer Insights 4.9/5 ★

AICPA SOC · ISO 27001

SCELTO DA OLTRE 300 GRANDI AZIENDE

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