La checklist di preparazione a Mythos per i CISO

Le patch stanno arrivando. Prima che arrivino, il tuo consiglio di amministrazione, il team legale e le autorità di regolamentazione avranno domande.

1 Esposizione e visibilità degli asset

"Qual è la nostra esposizione, e disponiamo di un inventario degli asset accurato?"

- ☐ Aggiorna il tuo inventario degli asset affinché rifletta l'attuale ambiente di produzione.
- ☐ Verifica che la scansione continua sia attiva in tutti gli ambienti di produzione.
- ☐ Riclassifica le vulnerabilità utilizzando una prioritizzazione basata sul rischio, non sul semplice conteggio dei CVE.
- ☐ Prepara un documento di sintesi sull'esposizione di una pagina, pronto da presentare al management su richiesta.

2 Velocità di patching e sicurezza della produzione

"Riusciamo ad applicare le patch in modo sufficientemente rapido, su larga scala, senza interrompere la produzione?"

- ☐ Verifica la cadenza attuale del ciclo di patching rispetto alla finestra tra divulgazione e trasformazione in exploit.
- ☐ Classifica gli asset per criticità prima che l'ondata si abbatta, non durante.
- ☐ Formalizza un protocollo di change management con responsabili designati e percorsi di rollback.
- ☐ Esegui un'esercitazione su uno scenario di distribuzione di patch ad alta velocità, per testare sotto pressione i percorsi decisionali e la prontezza al rollback.

3 Supply chain ed esposizione open source

"Cosa si nasconde nel nostro software open source e di terze parti?"

- ☐ Genera o aggiorna la tua Software Bill of Materials (SBOM).
- ☐ Censisci le integrazioni di terze parti acquisite tramite operazioni di acquisizione.
- ☐ Attiva la scansione continua delle dipendenze delle librerie open source.
- ☐ Individua gli SLA di patching dei fornitori e i relativi punti di contatto prima che la divulgazione abbia luogo.

4 Capacità di ingegneria

"Disponiamo della capacità di ingegneria per rimediare al nostro stesso backlog?"

- ☐ Stima le ore di rimedio necessarie rispetto agli impegni attuali del tuo team.
- ☐ Esegui il triage del backlog per concentrare i team interni solo sugli elementi a maggior rischio.
- ☐ Individua in anticipo risorse di ingegneria esterne, prima di averne bisogno.
- ☐ Integra ora pratiche secure-by-default nello sviluppo in corso.

5 Rilevamento e contenimento

"Se una patch è in ritardo, siamo in grado di rilevare e contenere l'exploit?"

- ☐ Verifica che il monitoraggio SOC 24/7 sia attivo in tutti gli ambienti critici.
- ☐ Definisci un tempo medio target per il triage e l'isolamento (minuti, non ore).
- ☐ Esegui attività proattive di threat hunting concentrate sulle superfici di esposizione legate a Mythos.
- ☐ Convalida il tuo piano di risposta "assume-breach" attraverso un'esercitazione o simulazione recente.

Verifica di preparazione per il management

Prima di informare il management:

- ☐ Individua quali di queste risposte puoi sostenere oggi e quali richiedono un allineamento con il management o una copertura esecutiva.

Se stai valutando come colmare queste lacune:

Alcune organizzazioni sviluppano queste capacità internamente. Altre si affidano a un partner per accelerare la copertura o supportare team con risorse limitate. **Insight Managed Exposure Defence** è un approccio integrato che copre tutte le cinque aree indicate sopra, sviluppato e gestito prima internamente, e successivamente esteso ai clienti che affrontano le stesse domande.

Scopri di più su it.insight.com