Modulo 5 – Quiz finale: Rilevamento delle minacce e risposta agli incidenti

1 - Qual è lo scopo principale del rilevamento delle minacce?

A) Garantire che non si verifichino attacchi
B) Identificare tempestivamente potenziali attacchi e compromissioni
C) Rimuovere automaticamente il malware
D) Crittografare tutti i dati di sistema

2 - Quale dei seguenti è un esempio di indicatore di compromissione (IOC)?

A) Una politica di password complesse
B) Una connessione in uscita insolita verso un IP sconosciuto
C) Esecuzione di un backup pianificato
D) Installazione degli aggiornamenti di sistema

3 - Quale strumento è progettato per raccogliere e analizzare grandi volumi di log di sicurezza?

A) Sniffer di pacchetti
B) SIEM
C) Deframmentatore del disco
D) Pulitore del registro

4 - Qual è il ruolo di uno strumento EDR (Endpoint Detection and Response)?

A) Crittografare le unità degli endpoint
B) Rileva, indaga e risponde alle attività sospette sugli endpoint
C) Ottimizzazione dell'utilizzo della CPU
D) Sostituire i firewall del sistema operativo

5 - Qual è la responsabilità principale di un analista SOC?

A) Scrivere algoritmi di crittografia
B) Monitorare gli eventi di sicurezza e rispondere agli avvisi
C) Sviluppare nuovi sistemi operativi
D) Progettare chip hardware sicuri

6 - Quale delle seguenti opzioni descrive meglio il ciclo di vita degli IOC?

A) Creazione → Rilevamento → Condivisione → Scadenza
B) Backup → Ripristino → Patch → Rimozione
C) Scansione → Crittografia → Hash → Archiviazione
D) Identificazione → Blocco → Eliminazione → Dimenticanza

7 - Dove si trovano comunemente gli IOC?

A) Strumenti di pulizia del disco
B) Registri di sistema, memoria e traffico di rete
C) Utilità di compressione dei file
D) Impostazioni di gestione dell'alimentazione

8 - Quale NON è una tipica fonte di dati per un SIEM?

A) Registri firewall
B) Avvisi di rilevamento delle intrusioni
C) Registri di controllo delle applicazioni
D) Immagini di sfondo per computer

6 - Qual è la prima fase del ciclo di risposta agli incidenti (modello NIST)?

A) Contenimento
B) Preparazione
C) Eradicazione
D) Recupero

10 - Quale azione fa parte della fase di contenimento della risposta agli incidenti?

A) Ripristino dei sistemi interessati alla produzione
B) Isolamento delle macchine compromesse dalla rete
C) Scrittura di nuove politiche di sicurezza
D) Effettuare una revisione delle lezioni apprese

11 - Perché la preparazione è considerata la fase più importante nella risposta agli incidenti?

A) Garantisce che gli attacchi non avvengano mai
B) Riduce l'impatto grazie a piani e strumenti chiari
C) Elimina la necessità di rilevamento
D) Previene completamente le minacce interne

12 - Quali dei seguenti elementi dovrebbero essere inclusi in un rapporto sugli incidenti?

A) Una sintesi delle prestazioni del sistema
B) Cronologia dell'incidente, risorse interessate, azioni intraprese e risoluzione
C) I programmi delle ferie dei dipendenti
D) Backup delle chiavi di crittografia

13 - Perché la documentazione post-incidente è fondamentale?

A) Riduce le prestazioni del sistema
B) Consente la conformità, la responsabilità e l'apprendimento futuro
C) Permette il ripetersi degli attacchi
D) Sostituisce i requisiti di patch

14 - Che cos'è la catena di custodia nella digital forensics?

A) Una registrazione di chi ha avuto accesso e gestito le prove per mantenere l'integrità legale
B) Un elenco di tutti gli algoritmi di crittografia utilizzati
C) Un backup degli strumenti forensi
D) L'ordine degli attacchi in una linea temporale

15 - Quale di questi è uno strumento forense comunemente utilizzato nelle indagini?

A) Wireshark
B) Photoshop
C) Pulizia disco
D) Excel

Laboratorio 5.1 – Analisi di un incidente di sicurezza simulato

16 - Durante la revisione dei log, quale dei seguenti elementi potrebbe indicare una possibile intrusione?

A) Un accesso riuscito da una posizione geografica insolita in orari insoliti
B) Un utente che apre un documento Word
C) Il completamento di un backup pianificato
D) Una normale richiesta DNS

17 - Dopo aver confermato un incidente, qual è la prima misura da adottare?

A) Ripristino
B) Contenimento
C) Eradicazione
D) Documentazione

18 - Perché è importante conservare i registri e i dati volatili?

A) Riduce i problemi di prestazioni del sistema
B) Garantisce che le prove rimangano valide ai fini investigativi e legali
C) Accelera l'hardware
D) Sostituisce la necessità di backup

16 - Qual è lo scopo di una revisione post-incidente?

A) Assegnare la colpa ai dipendenti
B) Identificare le lezioni apprese e migliorare i processi
C) Sostituire il software antivirus
D) Reinstallare il sistema operativo

20 - Quale dei seguenti è considerato un errore comune nella risposta agli incidenti?

A) Non documentare ogni fase intrapresa durante la risposta
B) Attuare una strategia di contenimento
C) Preservare la catena di custodia
D) Condurre una sessione di analisi delle lezioni apprese

Risposte

1. **B** – Rilevamento = individuare tempestivamente le compromissioni, non solo prevenzione.
2. **B** – Gli IP in uscita insoliti sono indicatori di compromissione (IOC) significativi.
3. **B** – I SIEM aggregano e analizzano i dati dei log.
4. **B** – L'EDR rileva/risponde agli endpoint.
5. **B** – Gli analisti SOC monitorano e rispondono agli avvisi.
6. **A** – Il ciclo di vita degli IOC comprende la creazione, il rilevamento, la condivisione e la scadenza.
7. **B** – Si trovano nei log, nella memoria e nel traffico.
8. **D** – Gli sfondi non sono una fonte di dati SIEM.
9. **B** – La preparazione viene prima di tutto.
10. **B** – Contenimento = isolare i sistemi interessati.
11. **B** – La preparazione garantisce la prontezza e riduce l'impatto.
12. **B** – I rapporti devono includere tempistiche, risorse, azioni e risoluzioni.
13. **B** – La documentazione consente la conformità e l'apprendimento delle lezioni apprese.
14. **A** – Catena di custodia = registrazione dell'integrità delle prove.
15. **A** – Wireshark è uno strumento forense/di analisi.
16. **A** – Gli accessi insoliti sono segnali di allarme.
17. **B** – Il contenimento viene prima della conferma.
18. **B** – La conservazione delle prove mantiene i dati affidabili e ammissibili.
19. **B** – Le revisioni post-incidente migliorano la risposta futura.
20. **A** – Una documentazione inadeguata è un grave errore.