Prova V01 per selezione in Lepida Scpa 17_2025DN.

Avviso di Selezione pubblica per l'assunzione a tempo pieno e indeterminato di 1 posizione per i Dipartimenti Reti - Data Center&Cloud - Software&Piattaforme - Azioni Strategiche e Speciali - e per la Divisione Sicurezza, Ambiente&Emergenza in Lepida ScpA

* Indica una domanda obbligatoria

1. Email *

2. COGNOME *

3. NOME *

PROVA V01

E' RICHIESTA UNA SOLA RISPOSTA PER OGNI DOMANDA. LE 4 OPZIONI PROPOSTE SONO TUTTE PRECEDUTE DA UN CODICE ALFANUMERICO DI 4 LETTERE E DA UN TRATTINO (-). TEMPO A DISPOSIZIONE: 40 minuti

4. Cosa definisce una Vulnerabilità nel contesto della sicurezza informatica? *

Contrassegna solo un ovale.

- NGEV - Un difetto nel software o nella configurazione di un sistema che può consentirne un uso improprio o l'accesso non autorizzato.
- WBDT - L'azione riuscita di un attaccante per penetrare un sistema.
- OQHC - Una tecnica di attacco nota, come il brute force o l'SQL Injection.
- DZRF - Il tempo necessario allo sviluppatore per rilasciare una patch di sicurezza.

5. Cosa compone la quintupla di connessione (5-tupla) utilizzata dai firewall? *

Contrassegna solo un ovale.

- KMFJ - IP sorgente, IP destinazione, MAC address, Protocollo, Porta destinazione.
- UAAL - IP sorgente, Porta sorgente, IP destinazione, Porta destinazione, Protocollo.
- XHPV - Porta sorgente, Porta destinazione, Stato della connessione, Firewall ID, Protocollo.
- XWOF - Nome host, Protocollo, Porta, Interfacce di rete.

6. Un Attacco Zero-Day è definito come tale perché: *

Contrassegna solo un ovale.

- VQWY - Sfrutta una vulnerabilità alla quale lo sviluppatore non ha ancora potuto applicare una patch.
- DIWC - L'attaccante ha avuto zero giorni per pianificare l'attacco.
- KTPI - Si verifica quando un sistema è in modalità di test (Day Zero).
- CCSI - Richiede l'intervento umano (HUMINT).

7. Qual è l'obiettivo principale della fase di Classificazione e Gestione degli Allarmi per il personale SOC? *

Contrassegna solo un ovale.

- CIUP - Raccogliere e mantenere il registro delle attività di rete.
- QEXK - Iniziare immediatamente l'investigazione forense.
- DNNM - Determinare il livello di rischio e dare priorità agli eventi più urgenti da gestire per primi.
- QGKH - Rilasciare patch di sicurezza.

8. Cosa si intende con l'approccio 'Negazione Predefinita' (Default-Deny)? *

Contrassegna solo un ovale.

- WIKW - Scartare i pacchetti senza avviso (DROP).
- NBEU - La prima regola deve essere block all.
- IOAV - Bloccare tutto il traffico tranne quello espressamente consentito.
- CGSJ - Consentire tutto tranne ciò vietato.

9. Qual è l'obiettivo della fase di Contenimento nella gestione di un incidente di sicurezza delle informaizoni? *

Contrassegna solo un ovale.

- RVHM - Ripristinare completamente i sistemi.
- JIOU - Limitare i danni e bloccare la minaccia nel breve periodo.
- WBJU - Raccogliere prove digitali.
- FCUE - Rimuovere la causa principale.

10. Quale protocollo o porta è tradizionalmente associato al traffico di un server Web non crittografato (HTTP) *

Contrassegna solo un ovale.

- TORG - Porta 80 (TCP)
- BFXK - Porta 443 (TCP)
- GDII - Porta 22 (TCP)
- JEUH - Protocollo ICMP

11. Qual è lo scopo principale di uno strumento come MISP (Malware Information Sharing Platform) nel contesto della Threat Intelligence? *

Contrassegna solo un ovale.

- WPOS - Gestire il ciclo di patching e aggiornamento dei sistemi vulnerabili.
- JBOS - Condividere in modo strutturato indicatori di compromissione (IoC) e informazioni su minacce tra organizzazioni.
- TQTY - Fornire una tassonomia standardizzata delle evidenze di attacco e ricavarne ulteriori dati per la condivisione.
- IXJG - Eseguire la scansione in tempo reale dei file alla ricerca di malware conosciuti

12. In Windows, quale utility consente di gestire i processi e monitorare le prestazioni del sistema? *

Contrassegna solo un ovale.

- XNZX - Task Manager (Gestione attività).
- BELY - Regedit.
- FBVH - Services.msc.
- KBSU - CMD.

13. Cosa distingue l'Analisi Statica da quella Dinamica di un malware? *

Contrassegna solo un ovale.

- GKCZ - Eseguita su VM per osservare il comportamento.
- TPQQ - Ispezione del codice senza eseguirlo.
- NXRN - Serve solo per malware basilari.
- BMHB - Acquisizione della memoria volatile.

14. Qual è il primo passo nel processo di gestione dei ticket di assistenza tecnica? *

Contrassegna solo un ovale.

- HCTO - Registrare e categorizzare la richiesta dell'utente.
- DEKA - Chiudere immediatamente il ticket se non critico.
- ORXZ - Eseguire la reinstallazione del sistema operativo.
- CNBA - Contattare direttamente l'utente per chiedere una valutazione.

15. Perché eseguire una Deep Packet Inspection (DPI)? *

Contrassegna solo un ovale.

- PMCU - Per protocolli L2.
- TTSD - Per filtrare solo header.
- LYAM - Per rilevare codice dannoso nel payload.
- YLXQ - Per velocizzare consultazione regole.

16. Qual è la funzione principale di un SIEM? *

Contrassegna solo un ovale.

- YYAJ - Raccogliere log da fonti diverse e correlarli.
- EFFS - Bloccare pacchetti malevoli.
- HTVX - Crittografare dati sensibili.
- BXVY - Mantenere firme dei malware.

17. Qual è il linguaggio di filtraggio usato da Wireshark/tcpdump? *

Contrassegna solo un ovale.

- JNJK - Lua.
- RMVJ - BPF (Berkeley Packet Filter).
- XFHL - SQL.
- UGPY - YAML.

18. Qual è l'obiettivo principale di un sistema DLP? *

Contrassegna solo un ovale.

- HAQG - Proteggere i dati in uso, in movimento e a riposo.
- EWTX - Prevenire attacchi di tipo Injection.
- CULV - Garantire regole aggiornate sui firewall.
- ENFL - Obbligare uso di protocolli cifrati.

19. Perché le policy scritte sono fondamentali nella fase di Preparazione? *

Contrassegna solo un ovale.

- EQQW - Stabiliscono i criteri di classificazione di un evento, se è incidente o meno.
- LQBM - Configurano firewall e IDS.
- NUQC - Elencano gli IoC da ricercare.
- ARKS - Aiutano a recuperare i dati.

20. Qual è il protocollo che permette di stabilire una sessione remota cifrata tramite interfaccia a riga di comando con un altro host di una rete informatica? *

Contrassegna solo un ovale.

- SXWG - SSH
- SDBA - Telnet
- URHL - CLP
- WAHN - TPC/IP

21. Qual è la prima fase della Kill Chain di un attacco informatico? *

Contrassegna solo un ovale.

- IPUH - Weaponization.
- CLQA - Command & Control.
- EGMC - Reconnaissance.
- UPZO - Delivery.

22. Cosa sono i Rootkit e quale livello di accesso cercano? *

Contrassegna solo un ovale.

- XCUL - Malware per crittografare file e chiedere riscatto.
- WJVW - Malware per ottenere accesso con diritti elevati e nascondersi.
- SZEC - Software drive-by download per rubare info.
- NQTU - Programmi autoreplicanti.

23. Qual è l'obiettivo principale della fase Lesson Learned nella gestione di un incidente di sicurezza delle informazioni? *

Contrassegna solo un ovale.

- ENTS - Garantire disponibilità dei sistemi.
- LXXM - Ragionare sulle azioni intraprese, documentare l'incidente e individuare miglioramenti per prevenire o gestire meglio eventi futuri.
- MNQT - Determinare asset e policy.
- QFLI - Documentare l'attacco per fini legali.