Concorso pubblico, per titoli ed esami, per n. 1 unità di personale, da inquadrare nell'Area professionale dei Funzionari, Settore professionale tecnico-informatico, con contratto di lavoro di apprendistato ai sensi dell'articolo 3-ter, comma 1, del D. L. n. 44/2023, per l'Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici – profilo cybersecurity

Estratto del verbale n. 2 del 3 settembre 2026

Tracce Prova Scritta

Traccia 1

Diversi utenti dell'Ateneo segnalano la ricezione di un'e-mail sospetta che invita a reinserire le credenziali di posta istituzionali su un sito web esterno all'Ateneo.

Il candidato descriva per gli aspetti tecnici e per gli eventuali riferimenti normativi:

1. Come riconoscere i principali indicatori di un attacco di Phishing.
2. Le prime azioni operative e i controlli base da effettuare per verificare la minaccia e contenere la diffusione dell'attacco.
3. I principi base da rispettare per garantire la riservatezza e la protezione dei dati degli utenti di Ateneo e l'importanza dell'autenticazione a più fattori (MFA)

Per gli eventuali riferimenti normativi il candidato potrà tenere conto, ove pertinenti, del D. Lgs. 138/2024 (i.e. art. 24), della Determinazione ACN n. 379907/2025 (i.e. Allegato 1) e del GDPR (i.e. artt. 5 e 32).

Traccia 2 - "traccia estratta".

Una postazione di lavoro di un ufficio amministrativo mostra comportamenti anomali che fanno ipotizzare un'infezione da Malware.

Il candidato descriva per gli aspetti tecnici e per gli eventuali riferimenti normativi:

1. Le misure immediate di contenimento da suggerire all'utente.
2. La scheda o il report di prima segnalazione dell'incidente che predisporrebbe per il Responsabile della Sicurezza, riportando tutte le informazioni necessarie per l'analisi e la risoluzione dell'incidente.
3. L'importanza ed il ruolo di strumenti EDR (Endpoint Detection and Response) centralizzati in un incidente come quello presentato, le caratteristiche e le funzionalità aggiuntive che offrono rispetto ai sistemi antivirus tradizionali.

Per gli eventuali riferimenti normativi il candidato potrà tenere conto, ove pertinenti, del D.Lgs. 138/2024 (i.e. art. 24), della Determinazione ACN n. 379907/2025 (i.e. Allegato 1) e del GDPR (i.e. artt. 5 e 32).

Traccia 3

Nei log del server VPN (Virtual Private Network) ci sono un certo numero di connessioni di utenti (docenti, studenti, personale tecnico amministrativo) da indirizzi IP localizzati all'estero. Il candidato descriva per gli aspetti tecnici e per gli eventuali riferimenti normativi:

I controlli da effettuare e gli indicatori da considerare per stabilire se tali connessioni possano essere legittime o a rischio relativamente alla problematica della compromissione delle credenziali dell'utente.

Le azioni da compiere riguardo l'utente, qualora ci sia il sospetto (o la certezza) di una compromissione di credenziali.

L'importanza del monitoraggio e dell'analisi dei log, in generale, per il rilevamento tempestivo delle minacce (*threat hunting/detection*).

Per gli eventuali riferimenti normativi il candidato potrà tenere conto, ove pertinenti, del D. Lgs. 138/2024 (i.e. art. 24), della Determinazione ACN n. 379907/2025 (i.e. Allegato 1) e del GDPR (i.e. artt. 5 e 32).

***

Il Dirigente

Dott. Simone Migliarini

Firmato digitalmente da SIMONE MIGLIARINI
Data: 03/09/2026 17:29:19 CEST