

SELEZIONE PUBBLICA, PER TITOLI ED ESAMI, PER IL RECLUTAMENTO DI N. 1 TECNOLOGO DI II LIVELLO, EX ART. 24 BIS LEGGE N. 240/2010, CON CONTRATTO DI LAVORO A TEMPO PIENO E DETERMINATO, DI DURATA COMPLESSIVA PARI A 24 MESI, EVENTUALMENTE PROROGABILE, NELL'AMBITO DEL PROGETTO DI TRANSIZIONE DIGITALE DELL'ATENEO-NIS2, CUP D99B25000040005, PRESSO LA U.O. SICUREZZA IT DELL'AREA SISTEMI INFORMATIVI DELL'UNIVERSITA' DI PARMA

## TRACCIA 1

1. Progetti l'architettura di rete di un Dipartimento articolato su due plessi collegati in fibra ottica con ridondanza. Descriva il ruolo e le principali configurazioni di switch, router e firewall. Indichi come organizzare il monitoraggio centralizzato verso un SIEM.
2. Spieghi quali pericoli possono emergere quando le credenziali di autenticazione non vengono gestite correttamente, sia durante il processo di sviluppo (ad esempio inserendo password in chiaro nel codice o nei file di configurazione) sia nell'amministrazione degli accessi ai vari servizi. Indichi inoltre quali contromisure, sia tecniche sia organizzative, adotterebbe per ridurre tali vulnerabilità, menzionando eventuali strumenti o pratiche di secrets management di cui è a conoscenza.
3. Spieghi cos'è uno CSIRT e quali requisiti, capacità tecniche deve avere e quali compiti deve svolgere secondo la Direttiva NIS2

SELEZIONE PUBBLICA, PER TITOLI ED ESAMI, PER IL RECLUTAMENTO DI N. 1 TECNOLOGO DI II LIVELLO, EX ART. 24 BIS LEGGE N. 240/2010, CON CONTRATTO DI LAVORO A TEMPO PIENO E DETERMINATO, DI DURATA COMPLESSIVA PARI A 24 MESI, EVENTUALMENTE PROROGABILE, NELL'AMBITO DEL PROGETTO DI TRANSIZIONE DIGITALE DELL'ATENEO-NIS2, CUP D99B25000040005, PRESSO LA U.O. SICUREZZA IT DELL'AREA SISTEMI INFORMATIVI DELL'UNIVERSITA' DI PARMA

## TRACCIA 2

1. Illustri quali tecnologie possono essere impiegate per individuare, monitorare e gestire incidenti di sicurezza informatica (ad esempio soluzioni SIEM, SOAR, EDR, EPP). Spieghi inoltre come tali strumenti possano collaborare e integrarsi all'interno di un contesto complesso e diversificato come quello di un ambiente universitario.
2. L'Ateneo intende verificare la propria postura di sicurezza attraverso un "penetration test". L'obiettivo è il furto di dati da un file server di Dipartimento. Descriva come raccoglierebbe informazioni sull'obiettivo, quale vettore iniziale utilizzerebbe, le fasi chiave dell'attacco, le regole d'ingaggio, i criteri di successo e le metriche.
3. La normativa NIS2 richiede alle organizzazioni di dotarsi di strategie per garantire la continuità operativa e il ripristino dei servizi in caso di eventi critici. Spieghi quali elementi essenziali devono essere inclusi in un piano di Business Continuity e in un piano di Disaster Recovery.

SELEZIONE PUBBLICA, PER TITOLI ED ESAMI, PER IL RECLUTAMENTO DI N. 1 TECNOLOGO DI II LIVELLO, EX ART. 24 BIS LEGGE N. 240/2010, CON CONTRATTO DI LAVORO A TEMPO PIENO E DETERMINATO, DI DURATA COMPLESSIVA PARI A 24 MESI, EVENTUALMENTE PROROGABILE, NELL'AMBITO DEL PROGETTO DI TRANSIZIONE DIGITALE DELL'ATENEO-NIS2, CUP D99B2500040005, PRESSO LA U.O. SICUREZZA IT DELL'AREA SISTEMI INFORMATIVI DELL'UNIVERSITA' DI PARMA

### TRACCIA 3

1. Un istituto universitario intende consolidare la propria infrastruttura informatica sostituendo parte dei server fisici con macchine virtuali. Illustri il concetto di virtualizzazione, mettendo in evidenza benefici e possibili criticità. Indichi inoltre quale tipologia di hypervisor ritiene più adatta al contesto ("bare-metal" o "hosted") e descriva le scelte progettuali necessarie per realizzare la soluzione.
2. Illustri le funzionalità principali dei dispositivi di rete quali switch, router e firewall. Spieghi inoltre in che modo tali apparati possono essere impiegati per progettare e configurare un'infrastruttura sicura distribuita su due sedi fisicamente separate.
3. Spieghi in che modo un ente pubblico deve predisporre il processo di segnalazione e gestione di un incidente informatico rilevante in conformità alla direttiva NIS2. Fornisca una descrizione operativa delle fasi da seguire, delle figure che devono essere attivate e dei canali formali attraverso cui effettuare le comunicazioni, includendo anche esempi di procedure applicabili.