WIIT

THE PREMIUM CLOUD

JOB DESCRIPTION

JOB TITLE	CYBER SECURITY ANALYST
FUNZIONE ORGANIZZATIVA	CYBER SECURITY
RIPORTO	CYBER DEFENCE MANAGER
SEDE DI LAVORO	MILANO

OVERVIEW

In Wiit abbiamo scelto di fare la differenza per i nostri clienti. Siamo leader nell'erogazione di servizi di Hosted Private e Hybrid Cloud per aziende con necessità di servizi di gestione di applicazioni critiche e business continuity.

Ricerchiamo valore in ogni cosa che facciamo mettendo al centro le nostre persone.

Affidabilità, etica e innovazione sono i nostri ingredienti di successo.

Unisciti a noi per fare la differenza!

MISSION

Gestire e supportare le aziende clienti nell'incremento della propria *cyber security posture*

RESPONSABILITA' E ATTIVITA'

- Supervisionare e monitorare il secondo livello dei processi di gestione degli incidenti di sicurezza e degli avvisi di monitoraggio;
- Produrre documentazione puntuale in caso di eventi e /o incidenti di sicurezza;
- Eseguire l'onboarding log source (on prem e cloud) con analisi logs ingestion e parsing, ottimizzazione regole e bulding block e tuning per le piattaforme tecnologiche implementate con focus su QRadar di IBM;
- Essere il punto di riferimento in caso di escalation dagli analisti di primo livello;
- Monitorare e migliorare l'efficacia dello strumento SIEM;
- Identificare opportuni processi di automazione e/o playbook per rispondere ad eventi di sicurezza

ESPERIENZA

Siamo alla ricerca di profili junior e senior.

TITOLO DI STUDIO

Diploma o Laurea in discipline tecnico/scientifiche

COMPETENZE E CONOSCENZE

- Conoscenza dei processi di un Security Operation Center e delle best practice correlate (es. ISO 27035). Si richiede la conoscenza dei processi di Incident Detection, triage ed Incident Management. Competenze in ambito SOC (Es. troubleshooting, contribuzione per lo sviluppo tecnico del team SOC, supporto tecnico nelle attività di Incident Response & War Room Coordination).

- Esperienza con packet flow, traffico TCP/UDP, tecnologie firewall, IDS, Proxy, EPP, EDR, Antispam
- Conoscenza di piattaforme e processi di Vulnerability Management
- Familiarità con sistemi operativi Windows e Linux e relative evidenze Cyber
- Apprezzate conoscenze dei principali Cybersecurity Frameworks come Mitre Att&ck e Owasp
- Conoscenza delle principali tipologie di attacchi cyber

ATTITUDINI E CAPACITA'

- Propensione al team working;
- Autonomia organizzativa e problem solving;