

IL TUO FUTURO NEL NOSTRO. IL TUO TALENTO PER I NOSTRI VALORI!

Vuoi entrare a far parte della Società garante della fede pubblica in Italia ed essere protagonista di importanti progetti per la trasformazione digitale del Paese?

Siamo alla ricerca di risorse altamente motivate, proattive, dotate di una forte passione, integrità e che condividano la nostra mission ed i nostri valori.

Ci impegniamo a creare un ambiente sicuro e inclusivo, basato sul rispetto reciproco e sulla valorizzazione delle diversità, offrendo pari opportunità di lavoro a tutti i candidati qualificati.

CHI SIAMO?

Siamo una realtà industriale e tecnologica unica, poliedrica ed in continua evoluzione. Racchiudendo tradizione ed innovazione, progettiamo, sviluppiamo e realizziamo prodotti di sicurezza e soluzioni tecnologiche integrate a tutela della fede pubblica, a supporto dello Stato, delle Imprese e dei Cittadini.

4 siti produttivi, oltre 1.700 dipendenti, l'Istituto Poligrafico e Zecca dello Stato (IPZS) sviluppa soluzioni per l'identità digitale dei cittadini italiani e crea prodotti per la sicurezza, l'anticontraffazione, la tutela della salute e del Made in Italy.

CHI CERCHIAMO?

N. 2 SOC Analyst

DI COSA TI OCCUPERAI?

Nella struttura "Security & Cyber Defence" ti occuperai di garantire il monitoraggio degli eventi di sicurezza e la gestione della risposta a minacce e vulnerabilità di cybersecurity.

In particolare, sarai coinvolto/a nelle seguenti attività:

- Monitorare e rilevare minacce in tempo reale attraverso un sistema SIEM (Security Information and Event Management);
- Lavorare su eventi e alert di sicurezza informatica e di produzione, basati su metriche standard di servizio;
- Reagire e supportare l'avvio di azioni correttive riguardanti violazioni della sicurezza, tentativi di ottenere accesso non autorizzato, infezioni da malware che possono influire sulla rete o altri eventi che incidono sulla sicurezza logica;
- Eseguire approfondite analisi degli eventi durante il processo di gestione incidenti, combinando capacità analitiche a conoscenze trasversali di network, security, IT e threat analysis;

- Effettuare il tuning continuo delle regole e dei sistemi per garantire la diminuzione dei falsi positivi e ottimizzare l'uso delle risorse (FW, IDS/IPS, WAF, AntiSpam, AntiVirus, EDR, NDR, Proxy, SandBox, AntiDDoS, SIEM, ELK, AI Platform, Cloud Platform), nonché produrre e aggiornare le procedure/istruzioni operative;
- Eseguire attività di Cyber-Threat Intelligence;
- Identificare le opportune azioni di risposta e ripristino durante il processo di gestione degli incidenti;
- Condurre attività di Early Warning, per la raccolta, l'analisi e la divulgazione di informazioni in merito a vulnerabilità tecnologiche, elaborate e contestualizzate;
- Gestire gli IoC ricevuti da fonti esterne, per analisi su possibili eventi interni;
- Eseguire analisi forense e rapporti di verifica sulle conseguenze di attacchi segnalati;
- Redigere report su incidenti, vulnerabilità e altro materiale tecnico;
- Lavorare su eventi e alert di sicurezza informatica e di produzione, basati su metriche standard di servizio.

REQUISITI NECESSARI

- Diploma di Istruzione Secondaria Superiore
- Esperienza pregressa nella redazione di report su incidenti e vulnerabilità
- Buona conoscenza di:
 - processi di gestione incidenti e la loro progettazione
 - pratiche di sicurezza IT, tipi di attacco comuni e metodi di rilevamento/prevenzione

Completa il profilo la buona conoscenza della lingua inglese.

ESPERIENZE

Esperienza consolidata in almeno due delle seguenti opzioni:

- Configurazione e gestione di dispositivi di sicurezza (Firewall, apparati IDS/IPS, ecc.) e dei Tipi di eventi che essi producono;
- Analisi e correlazione degli eventi di sicurezza tramite SIEM per il rilevamento delle minacce alla sicurezza delle informazioni;
- Gestione degli incidenti di sicurezza e attività di incident response;
- Utilizzo di piattaforme di threat intelligence per la raccolta e l'analisi di indicatori di compromissione (IoC);
- Investigazioni su eventi sospetti e produzione di report tecnici di dettaglio.

CONOSCENZE

Si richiede l'ottima conoscenza di almeno due delle seguenti opzioni:

- Tecnologie di rete e sicurezza informatica e principali protocolli di rete (e.g. HTTP, HTTPS, TFTP, FTP, SNMP, SMTP, DNS, IP, TCP, UDP, ICMP, ARP, RARP);
- Architetture di sicurezza perimetrale e interna (firewall, proxy, IDS/IPS, VPN, NAC);

- Sistemi operativi server e client (es. Microsoft, Linux, Unix, MacOS), con particolare attenzione alla sicurezza e alla gestione dei log;
- Strumenti e tecniche di analisi malware, sandboxing, e reverse engineering di base;
- Linguaggi di scripting utili all'automazione di attività SOC (es. Python, Bash, PowerShell);
- Conoscenza di base di cloud security e dei relativi modelli di logging e monitoring.

Inoltre, si richiede la buona conoscenza di almeno due delle seguenti opzioni:

- Pratiche di sicurezza IT, minacce, tipi di attacco comuni e metodi di rilevamento / prevenzione;
- Algoritmi e tecnologie per la crittografia simmetrica ed asimmetrica e gestione delle chiavi;
- Concetti relativi allo Stack ISO/OSI e principi generali di rete;
- Framework e standard di sicurezza (es. NIST, ISO 27001, MITRE ATT&CK);
- Tecniche di analisi forense su endpoint e rete.

REQUISITI PREFERENZIALI

- Laurea magistrale/specialistica in Ingegneria Informatica, Sicurezza Informatica, Cybersecurity, Ingegneria delle Telecomunicazioni, Ingegneria Elettronica, Informatica;
- Master/Dottorati di Specializzazione in ambito sicurezza delle informazioni;
- Esperienza pregressa, di almeno 2 anni, nel ruolo o in ruoli simili in realtà industriali di medie o grandi dimensioni o in società di consulenza;
- Certificazioni in ambito Sicurezza delle Informazioni (es. CSA, GCIH, CEH, CHFI, SANS, OSCP, CISSP);
- Certificazioni in ambito Project Management (es. ISIPM, PMP).

Nella valutazione si terrà inoltre conto delle seguenti:

CAPACITA' ED ATTITUDINI INDIVIDUALI

- Curiosità, proattività e propensione al *Problem Solving*
- Forte Orientamento al Risultato
- Spiccata attitudine alla Collaborazione e al lavoro in Team
- Buoni doti comunicative
- Buona capacità di Pianificazione e Organizzazione
- Forte inclinazione all'ascolto, empatia e cordialità
- Buona capacità di adattamento al cambiamento e alle innovazioni con attitudine all'aggiornamento

Relativamente alla conoscenza della lingua inglese, sarà valutato positivamente l'aver conseguito una certificazione attestante un livello pari o superiore a B2 (rif. QCER - Quadro Comune Europeo di Riferimento).

La ricerca è rivolta a candidati di entrambi i sessi (D.Lgs. n. 198/2006 e s.m.i.). Le caratteristiche delle attività sono compatibili con qualsiasi genere, età e condizione fisica (salvo, per quest'ultima, il necessario accertamento successivo ai fini della verifica dell'idoneità per l'effettivo espletamento delle mansioni).

COSA OFFRIAMO?

Tempo indeterminato full-time, inquadramento previsto fino al gruppo **"A"** ai sensi del vigente CCNL per le Aziende Grafiche e Affini e delle Aziende Editoriali anche Multimediali.

Il livello di inquadramento e la retribuzione saranno commisurati alla seniority.

Sede: **Roma**

L'azienda, per esigenze tecnico organizzative, si riserva la facoltà di estendere la presente ricerca ad altre sedi e/o presidi IPZS.

BENEFIT

- Buoni Pasto elettronici (valore unitario Euro 9,00)
- Assicurazione sanitaria
- Welfare
- Servizio navetta aziendale e ludoteca aziendale
- Bonus Nido
- Convenzioni aziendali

RITIENI DI ESSERE IL CANDIDATO IDEALE?

Potrai candidarti dal **12/09/2025 alle ore 23:59 del 28/09/2025** cliccando su "candidati ora" o direttamente dal link <https://selezione.pa.randstad.it/socanalystipzs>

Non sono ammesse altre forme di invio delle domande di partecipazione alla selezione e, pertanto, non saranno ritenute valide le domande presentate con modalità e tempistiche diverse da quella indicata, a pena di esclusione.

Il Poligrafico e la società incaricata Randstad Italia S.p.A. che si occuperà della ricezione delle domande e dello svolgimento dell'iter preselettivo, non si assumono alcuna responsabilità circa la mancata ricezione delle domande per qualsiasi motivo imputabile a terzi, a caso fortuito e forza maggiore.

PROCESSO DI SELEZIONE

Il processo di selezione prevede la preselezione da parte della società Randstad Italia S.p.A incaricata, che curerà la fase preselettiva volta all'individuazione dei candidati da ammettere alla fase selettiva.

Una seconda fase di selezione nella quale il Poligrafico condurrà colloqui tecnico/motivazionali. Verrà ritenuto idoneo chi otterrà un punteggio pari ad almeno 3/6, sia alla valutazione tecnica che alla valutazione motivazionale.

Laddove necessario potranno essere previste, sia nella fase di pre-selezione che nella fase di selezione delle prove tecniche e/o logico - attitudinali, che si intenderanno superate con il raggiungimento del punteggio minimo previsto – cosiddetto punteggio soglia – pari al 51% del punteggio massimo. Resta inteso che in fase di preselezione accederanno alle prove tecniche solo i candidati che abbiano i requisiti sopra richiesti.

È IMPORTANTE SAPERE CHE

La mancata allegazione del cv sarà causa di esclusione dalla selezione.

Le competenze specialistiche richieste e i requisiti preferenziali, qualora presenti, devono essere espressamente indicati nel CV – specificando le date di inizio e fine (mese e anno) sia del percorso formativo sia delle singole esperienze professionali, nonché il possesso delle competenze/conoscenze richieste.

Eventuali dati incompleti non potranno essere tenuti in considerazione ai fine della valutazione.

Le competenze specialistiche e i requisiti preferenziali devono essere maturati alla data di scadenza dei termini per la presentazione della candidatura.

L'Azienda si riserva di verificare in qualsiasi momento l'effettivo possesso dei requisiti previsti dal presente avviso, nonché dei titoli dichiarati, attraverso la richiesta della documentazione necessaria o di informazioni su di essa e di disporre, in qualsiasi momento, l'esclusione dei candidati nel caso di non veridicità delle dichiarazioni rese.

La società si riserva la facoltà di prorogare, modificare o revocare la presente ricerca in caso di:

- Mancata ricezione di candidature corrispondenti ai requisiti necessari richiesti;
- Nuove esigenze organizzative aziendali che richiedano la sospensione/cancellazione degli inserimenti pianificati e ad oggi approvati o la variazione del numero di ingressi previsti;

La presentazione della domanda implica inoltre l'accettazione di tutte le disposizioni del presente avviso.

Ai sensi dell'art. 46 del D.P.R. n. 445/2000, i candidati sono tenuti a dichiarare, sotto la loro responsabilità, la veridicità delle informazioni riportate nel curriculum vitae.

I dati personali saranno trattati dalla società Randstad Italia S.p.A. in qualità di Titolare ai sensi e per gli effetti della normativa Privacy vigente.

L'Informativa ex art. 13 del Regolamento UE 2016/679 è presente sul sito www.randstad.it nella sezione Informativa Privacy.