Eric Zorzi

Sesso: Maschile **Data di nascita:** 15 ott 90 **Nazionalità:** Italiana

ESPERIENZA LAVORATIVA

[giu 17 – Attuale] **Security IR Analyst & Cyber Threat Hunter**

Intesasanpaolo S.p.a.

Città: Moncalieri (TO)
Paese: Italia
Principali attività e responsabilità:
Le principali attività come Cyber Threat Hunter: Rilevare, isolare e neutralizzare in modo proattivo e iterativo le minacce avanzate che sfuggono alle soluzioni di sicurezza automatizzate. In caso di incidente informatico le principali attività come Incident Responder: fornire una risposta iniziale rapida a eventuali minacce alla sicurezza IT, incidenti o attacchi informatici indagando rapidamente su eventuali problemi man mano che si sviluppano. Una volta identificata la causa del problema, limitare eventuali danni, fornire soluzioni temporanee immediate e, se possibile, fornire una soluzione in modo che qualsiasi intrusione o minaccia all'organizzazione venga rapidamente eradicata.

[giu 16 – giu 17] **IT Security Analyst - SOC**

Intesasanpaolo S.p.a.

Città: Moncalieri (TO)
Paese: Italia
Principali attività e responsabilità:
Analista di sicurezza informatica presso un Security Operations Center (SOC) di IntesaSanPaolo con competenza tecnica (specialista di terzo livello su tecniche d'attacco tecniche di recognize, analisi forensi) con compiti di analisi dei dati/eventi nell'ambito della Sicurezza ICT e sviluppo di regole di correlazione al fine della rilevazione automatica degli eventi malevoli. Le principali attività svolte: Incident handling, rilevazione e prevenzione delle minacce informatiche, malware reverse engineering, security reporting.

[dic 14 – giu 16] **IT Security Architect**

Intesasanpaolo S.p.a.

Città: Moncalieri (TO)
Paese: Italia
Principali attività e responsabilità:
Implementazione di Identity Management (Identity Source e Identity Manager) e Access Management(Provisioning, Authentication, Proliferation, Authorization).

[apr 14 – gen 15] **Sviluppatore Software**

Intellidoc S.r.l. (Gruppo PRT)

Città: Beinasco (TO)
Paese: Italia
Principali attività e responsabilità:
Progettazione e sviluppo di sistemi e applicazioni software per la gestione documentale.

[nov 13 – apr 14] **Data Security Analyst - SOC**

Certimeter s.r.l.

Città: Milano
Paese: Italia
Principali attività e responsabilità:
Analista di sicurezza informatica presso un Security Operations Center (SOC) con competenza tecnica (specialista di secondo livello su tecniche d'attacco tecniche di recognize, analisi forensi) con compiti di analisi dei dati/eventi nell'ambito della Sicurezza ICT. Le attività svolte sono servizi di Security Monitoring in attività di: analisi eventi di sicurezza, correlazione con lo stato dei sistemi, analisi delle vulnerabilità, auditing e verifica dei profili di sicurezza, user policy, problem determination, monitoraggio delle minacce e delle vulnerabilità. Competenze nell'utilizzo e nel tuning di tecnologie di Intrusion Detection System, Security Information and Event Management; Network Discovery e Vulnerability Assessment . Redazione della documentazione di reporting dei risultati delle attività di analisi. Le attività sono state svolte all'interno dell'infrastruttura SOC di Reply sia in orario standard che in turnazione.

[mar 13 – nov 13] **Data Security Analyst - SOC**

Reply - Communication Valley

Città: Parma
Paese: Italia
Principali attività e responsabilità:
Analista di sicurezza informatica presso il Security Operations Center (SOC) con competenza tecnica (specialista di primo livello su tecniche d'attacco,tecniche di recognize) con compiti di analisi dei dati/eventi nell'ambito della Sicurezza ICT.Le attività svolte sono servizi di Security Monitoring in attività di: analisi eventi di sicurezza, correlazione con lo stato dei sistemi, analisi delle vulnerabilità, auditing e verifica dei profili di sicurezza, user policy, problem determination, monitoraggio delle minacce e delle vulnerabilità. Le attività sono state svolte all'interno dell'infrastruttura SOC di Reply sia in orario standard che in turnazione.

[ago 09 – apr 13] **Responsabile coordinatore, Guida turistica, Bigliettaio**

Fai - Fondo Ambiente Italiano

Città: Masino (TO)
Paese: Italia
Principali attività e responsabilità:
Addetto biglietteria, addetto negozio,accoglienza e accompagnamento del pubblico con visite guidate.

ISTRUZIONE E FORMAZIONE

[08 – 13] **Dottore in informatica, Sistemi e Reti**

Università degli Studi di Torino https://www.unito.it/

Indirizzo: Torino, Italia

[03 – 09] **Maturità scientifica tecnologica**

Istituto Istruzione superiore "P. Martinetti" https://www.iismartinetti.edu.it/

Indirizzo: Caluso (TO), Italia

LICENZE E CERTIFICAZIONI

[19 – 24] **GIAC Certified Forensic Analyst (GCFA)**
https://www.youracclaim.com/badges/84ee473e-4435-4407-b8b7-4588bf86256c/linked_in_profile

[18 – 22] **Certified Ethical Hacker (CEH)**
https://aspen.eccouncil.org/VerifyBadge?type=certification&a=XGQ3uejLx4yoGBANcvWr0nvNzsySdOyULcpD7qs8nqE=

CORSI

CISCO CCNA Routing and Switching

Eccouncil CEH - Certified Ethical Hacker

European Innovation Academy (EIA)

SANS FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics

Penetration Testing with Kali Linux (PWK/PEN-200)

COMPETENZE PROFESSIONALI

Competenze di programmazione e sicurezza informatica

Ottime conoscenze dei linguaggi Java, go, C# ,ASP .NET ,C ,C++, PHP, HTML / HTML5, CSS ,JavaScript, XML, python orientati sia sul tema della programmazione che sulla sicurezza. Ottima conoscenza e padronanza degli strumenti di correlazione degli eventi e l'individuazione degli incidenti informatici anche argomento di tesi(SIEM RSA SecurityAnalytics). Esperienza e di analisi forense classica (Autopsy,ecc..) e LiveForensic (ECAT,Rekallecc..). Ottime conoscenze dell'architettura e delle reti di elaboratori, dei sistemi operativi Microsoft e Open Source di base UNIX (Linux,Kali,ecc..).

Ottima conoscenza dei sistemi informativi aziendali e della loro sicurezza. Esperienza di lavoro con sistemi distribuiti su larga scala su diverse realtà. Esperienza e formazione su ambienti di hosting, networking, firewall e application security. Conoscenza avanzata dello stack TCP/IP e di tutti i suoi protocolli. Approfondita conoscenza delle tecniche per la conduzione di attacchi informatici e sviluppo di misure di contrasto degli attacchi informatici a livello preventivo e di contenimento acquisita nell'esperienza di Security IR Analyst & Cyber Threat Hunter.

COMPETENZE DIGITALI

Le mie competenze digitali

Elaborazioni delle informazioni | Risoluzione di problemi | creazione di contenuti | SICUREZZA INFORMATICA | Conoscenza del sistema operativo di penetration testing Kali Linux | SOC Analyst e Incident Responder | Threat Hunting | Malware Analyst | Reverse engineering

COMPETENZE LINGUISTICHE

Lingua madre: italiano

Altre lingue:

Inglese

ASCOLTO B2 **LETTURA** B2 **SCRITTURA** B2

PRODUZIONE ORALE B2 **INTERAZIONE ORALE** B2

PATENTE DI GUIDA

Motocicletta: A
Automobile: B

HOBBY E INTERESSI

Karate
Citura nera 1°dan di Karate

Sicurezza informatica

Robotica

VOLONTARIATO

[gen 13 – nov 13] **Volontario - Anpas Comitato Regionale Piemonte** Caluso

---

Autorizzo il trattamento dei miei dati personali presenti nel CV ai sensi dell'art. 13 d. lgs. 30 giugno 2003 n. 196 - "Codice in materia di protezione dei dati personali" e dell'art. 13 GDPR 679/16 - "Regolamento europeo sulla protezione dei dati personali".

Orbassano, 4 ago 22

Eric Zorzi