(Senior) Consultant – Digital Forensics & Incident Response (w/m/d)

Die ResponseOne GmbH ist ein spezialisierter IT-Krisendienstleister mit Sitz in Berlin. Wir werden immer dann gerufen, wenn es brennt: kompromittierte Accounts, ausgenutzte Sicherheitslücken, Malware, verschlüsselte Server, usw. Unser Fokus liegt dabei auf der Aufklärung, Bewältigung und Abwehr von Cyberangriffen. Wir unterstützen betroffene Unternehmen remote & vor Ort u.a. bei den Themen IT-Forensik, Datarecovery, IT-Wiederaufbau, Notbetrieb, Krisenmanagement und Krisenkommunikation.

Für unser Forensik-Team suchen wir begeisterungsfähige Talente mit forensischem Fundament, die ihre Fähigkeiten an der Seite von Experten mit langjähriger Erfahrung in der Praxis weiter ausbauen wollen. Wir sind ein fokussiertes Team, welches eng zusammenarbeitet, großen Wert auf das Miteinander legt und gemeinsam neue Qualitätsmaßstäbe in der Branche setzen möchte. Bei uns geht es um mehr als nur Arbeit – es geht um Leidenschaft und anderen zu helfen.

Was deine Aufgaben sind:

Unterstützung von Kunden bei Cyberangriffen (remote & vor Ort) als Teil unseres Incident Response Teams • Sicherung und Duplikation von forensischen Beweismitteln (Festplatten, Images, Logs, Cloud, etc.) unter Einhaltung Chain of Custody • Durchführung von manuellen forensischen Analysen (keine Triage / Agents) zur Beantwortung konkreter Fragestellungen (z.B. Einfallstor, Hergang und Ausmaß, Datenabfluss) • Saubere und nachvollziehbare Dokumentation deiner Analyseschritte und Findings inkl. Timeline und Bericht • Mitgestaltung bei der Weiterentwicklung und Verbesserung: Tooling, Methodik, Know-How

Must-haves – bei uns vor allem persönlicher Natur

Analytisch-strukturierte Problemlösung: Problemverständnis wichtiger als eigentliche Lösung • Taktisches Denken (Kill-Chain / MITRE ATT&CK) und Zusammenhänge zwischen Artefakten erkennen • Intrinsische Neugier & Ermittler-Gen: Kein Fallabschluss ohne Root-Cause und Storyline • Herausforderungen motivieren dich • Forensische Sorgfalt und strukturierte Dokumentation: Unsere Qualität wird am Bericht gemessen • Besonnenheit statt Aktionismus • Team-first: früh fragen, Wissen teilen, gemeinsam Erfolge feiern

Abgeschlossenes techn. Studium (Informatik, IT-Security, Forensik) • 1 – 3 Jahre Berufserfahrung in der digitalen Forensik (SOC ≠ Forensik) im Microsoft-Umfeld • XWays, Eric Zimmerman Tools, Eventlog Explorer • Linux Grundkenntnisse • Deutsch auf C2-Niveau (Misskommunikation in der Krise vermeiden)

Nice-to-haves – nichts davon ist ein Muss

Ergebnisse aufbereiten und vermitteln: Zielgruppenorientiert (z.B. Entscheider:innen, IT-Abteilung, Versicherungen, Behörden) und Ableitung von konkreten Handlungsempfehlungen

SANS FOR500, FOR508, FOR509, FOR577 • Chainsaw, Hayabusa, Velociraptor, KAPE, Volatility, Nirsoft, Elastic • Berufserfahrung als Penetrationstester:in • Programmiererfahrung in Python oder Go • HTB-Forensics-Labs, TryHackMe, CTFs

Was wir Dir bieten:

Work-Buddy, der dir zur Seite steht • Mitarbeit in Kundenprojekten (echten Incidents) von Anfang an • Eigene Fälle erst wenn du bereit bist • hybrides Modell (2 Tage pro Woche Büro in Berlin, Rest Homeoffice) • Vollzeit / Teilzeit ab 32 Std. • 30 Tage Urlaub • 60.000 – 80.000 € brutto p.a., transparentes Stufen- und Gehaltsmodell • voraussichtlich 3 – 4 Fälle vor Ort pro Jahr: Kompensation durch Freizeitausgleich, Zusatzvergütung • Pers. Entwicklungs- und Ausbildungsplan • Mentoring • Klare Perspektive: Einsatzleitung, Teammanagement, Fachverantwortung oder Spezialisierung • Förderung von Frauen in technischen Berufen

Bewerbung:

Keep it simple – Lebenslauf genügt • Deine Persönlichkeit und die Art wie du denkst interessieren uns mehr als jede Zertifikatsliste • Frauen ermutigen wir ausdrücklich zur Bewerbung

→ [E-Mail] → Bewerbungsgespräch: zwei Runden (1 x remote, 1 x vor Ort) → Willkommen im Team

⚠ Rolle ist bewusst Early-Career (Consultant mit Erfahrung / Anfang Senior) angesetzt. Quereinsteiger:innen können wir in diesem Verfahren leider nicht berücksichtigen.