Teamleiter (m/w/d) Protection Engineering

Du hast Erfahrung darin, Unternehmen aktiv gegen Cyberangriffe zu verteidigen? Du kennst reale Angriffsmuster aus der Praxis – nicht nur aus Whitepapers? Du möchtest dieses Wissen nutzen, um moderne Schutztechnologien zu entwickeln, die Angriffe frühzeitig erkennen und stoppen? Dann werde Teil unseres Teams in der Abteilung Prevention, Detection & Response am Standort Bochum oder deutschlandweit per remote und unterstütze uns als Lead R&D Engineer (m/w/d) im Bereich Protection Engineering.
In dieser Rolle bringst Du Deine praktische Erfahrung aus der Verteidigung komplexer IT-Infrastrukturen ein – etwa aus einem SOC, CERT oder Blue-Team – und übersetzt sie gemeinsam mit Deinem Team in innovative Detection- und Protection-Technologien.

Deine Aufgaben

- Du führst ein Team von Protection-Engineers, das sich auf die Entwicklung moderner Detection- und Protection-Regeln konzentriert
- Du bringst Deine praktische Erfahrung aus der aktiven Verteidigung gegen Cyberangriffe ein und nutzt dieses Wissen, um neue Schutzmechanismen und Detection-Logiken zu entwickeln
- Du analysierst reale Angriffstechniken, Malware-Kampagnen und Angreiferverhalten und leitest daraus neue Erkennungsstrategien ab
- Du nutzt bestehende Security-Tooling-Plattformen und Telemetriequellen, um neue Detection-Regeln und Analysemechanismen zu entwickeln
- Du entwickelst gemeinsam mit Deinem Team kreative Ansätze, um zusätzliche Sichtbarkeit zu schaffen und Angriffe zu erkennen, wenn vorhandene Datenquellen nicht ausreichen
- Du arbeitest eng mit anderen Engineering-Teams, Threat Researchern und Product Ownern zusammen, um Detection-Fähigkeiten kontinuierlich weiterzuentwickeln
- Du identifizierst technische Engpässe, optimierst Prozesse und stellst sicher, dass Dein Team effektiv hochwertige Lösungen liefert
- Du definierst gemeinsam mit anderen technischen Leads die strategische technische Roadmap für Schutz- und Detection-Strategien
- Du unterstützt Dein Team bei komplexen technischen Fragestellungen und bringst Dich bei Bedarf selbst hands-on ein – z. B. bei Prototypen, Detection-Logik oder Analysen

Dein Profil

- Du hast mehrjährige praktische Erfahrung in der Verteidigung von Unternehmensinfrastrukturen gegen Cyberangriffe, z. B. in einem SOC, CERT oder Blue-Team gesammelt
- Du konntest bereits Verantwortung bspw. als SOC Lead, SOC Manager, Detection Engineer oder Threat Hunter (m/w/d) übernehmen
- Du kennst reale Angriffsmuster und Taktiken (z. B. gemäß MITRE ATT&CK) und weißt, wie Angreifer sich in Netzwerken bewegen
- Du hast Erfahrung darin, Detection-Regeln, Threat-Hunting-Analysen oder Sicherheitsanalysen mit gängigen Security-Tools umzusetzen
- Du verstehst, welche Telemetrie notwendig ist, um Angriffe zuverlässig zu erkennen – und kannst kreative Lösungen entwickeln, wenn diese Daten noch fehlen
- Du verfügst über solide technische Kenntnisse in mindestens einem Bereich wie Endpoint Security, Netzwerk-Security, SIEM, EDR/XDR, Log-Analyse oder Incident Response
- Du hast Erfahrung in der Zusammenarbeit mit Engineering-Teams oder in der Entwicklung sicherheitsrelevanter Softwarelösungen

- Du kommunizierst klar und strukturiert, kannst Teams motivieren und technische Konzepte verständlich vermitteln
- Du sprichst fließend Deutsch (mind. C1) und gut Englisch (mind. B2)

Deine Vorteile bei G DATA

Mission
Schütze mit uns Menschen und Unternehmen vor Cyberkriminalität

Flexibilität
Du entscheidest, wann und wo Du arbeitest – früh oder spät, im Büro oder von zuhause

Onboarding
Strukturierter Start, moderne Ausstattung und Unterstützung durch Dein Team

Urlaub
30 Tage Erholung im Jahr

Gestaltungsfreiraum
Hier ist Platz für Visionen – Deine Ideen treiben uns voran

Perspektive
Weiterbildungen und Sprachkurse für Deine Weiterentwicklung

Altersvorsorge
Clever vorsorgen dank extra hohem Arbeitgeberzuschuss

Mobilität
Eigener Parkplatz, E-Ladesäulen, Jobrad, Anbindung zum Radweg, Fahrradkeller und Duschen

Vergünstigungen
Rabatte über „Corporate Benefits" und kostenlose Software-Lizenzen

Bio-Verpflegung
Frische, hochwertige Speisen zu günstigen Preisen im Bistro. Kostenlos: Obst, Brot, Kaffee und weitere Getränke

Campus-Feeling
Für Austausch und Spaß stehen Café, Arcade Raum, Kicker- und Billardtisch zur Verfügung

Gilden-Konzept
Wissen teilen, Sport-Zuschuss und Freizeit-Communities

Events
Ob Sommerfest, Weihnachtsfeier oder Teamevents – wir feiern und erleben gemeinsam

Jetzt bewerben

Deine Ansprechpartnerin

Talentmanagement

Lena Kurrat
+49 234 9762 265
personal@gdata.de

G DATA CyberDefense AG
Königsallee 178 a • 44799 Bochum