Marco Wagner

SOC Analyst

marco.wagner@email.de +49 152 71938264 Bonn linkedin.com/in/marcowagner

PROFIL

SOC Analyst mit 4 Jahren Erfahrung im 24/7-Security-Operations-Center und ausgebildeter Fachinformatiker für Systemintegration. Triage und Analyse von Alarmen in IBM QRadar und Splunk, Eindämmung auf Endpunkten mit CrowdStrike Falcon und Netzwerkanalyse mit Wireshark. Arbeit nach Playbooks in TheHive mit Rufbereitschaft im Wechsel.

BERUFSERFAHRUNG

SOC Analyst

05/2022 - heute

Rhein-Sieg Cyber Defense GmbH — Bonn

- Triage von rund **90** Alarmen pro Tag im SIEM IBM QRadar und Splunk für Kunden aus Verwaltung und Gesundheit
- Eskalation und Dokumentation von 40 bestätigten Sicherheitsvorfällen pro Quartal in TheHive mit klaren Handlungsempfehlungen
- Eindämmung kompromittierter Endpunkte über das EDR CrowdStrike Falcon innerhalb von 15 Minuten nach Bestätigung
- Mapping neuer Use Cases auf MITRE ATT&CK, Abdeckung der relevanten Techniken von 48 % auf 71 % erhöht

Fachinformatiker für Systemintegration

07/2019 - 04/2022

Siebengebirge Logistik GmbH — Königswinter

- Betreuung von **350** Arbeitsplätzen und 40 Linux- und Windows-Servern an 3 Standorten
- Netzwerkanalyse mit Wireshark bei Störungen in Lager und Versand, Ursachen in 90 % der Fälle am selben Tag gefunden
- Einrichtung von Firewall-Regeln und VPN-Zugängen für 60 Außendienstmitarbeitende
- Mitarbeit bei der Einführung von EDR auf allen Clients und Schulung der Kollegen im Support

Auszubildender Fachinformatiker für Systemintegration

08/2016 - 06/2019

Siebengebirge Logistik GmbH — Königswinter

- Rollout von 120 Notebooks inklusive Imaging und Übergabe an die Fachabteilungen
- Abschlussprojekt zur zentralen Log-Sammlung unter Linux, IHK-Prüfung mit der Note gut
- Helpdesk im letzten Ausbildungsjahr mit rund 25 Tickets pro Tag

KENNTNISSE

- SIEM
- IBM QRadar
- Splunk
- Triage
- EDR
- CrowdStrike Falcon
- MITRE ATT&CK
- Wireshark
- TheHive
- Linux

AUSBILDUNG

Ausbildung Fachinformatiker für Systemintegration (IHK)

08/2016 - 06/2019

Berufskolleg Bonn-Duisdorf — Bonn

Systemintegration

SPRACHEN

Deutsch	Muttersprache
Englisch	B2
Italienisch	B1

ZERTIFIKATE

Splunk Core Certified Power User

02/2023

Splunk

Blue Team Level 1

09/2024

Security Blue Team