Mehmet Yilmaz

Senior Cybersecurity Incident Response Analyst

mehmet.yilmaz@email.de +49 152 83920475 Hamburg linkedin.com/in/mehmetyilmaz

Profil

Senior Cybersecurity Incident Response Analyst mit 9 Jahren Erfahrung in SOC und CERT, zuletzt als Fallleiter bei Ransomware-Angriffen auf Mittelstand und Logistik. Schwerpunkte sind Digitale Forensik mit Velociraptor, KAPE und Volatility, die Wiederherstellung von Active Directory und Krisenkommunikation mit Geschäftsführung und Behörden.

Berufserfahrung

Senior Cybersecurity Incident Response Analyst
06/2022 - heute

Alster CERT GmbH — Hamburg

- Fallleitung bei **45** Incident Response Einsätzen, davon 28 Ransomware-Angriffe bei Unternehmen mit bis zu 5.000 Beschäftigten
- Sicherung und Auswertung von Spuren mit Velociraptor und KAPE, Erstbefund meist innerhalb von 24 Stunden
- Speicheranalyse mit Volatility zum Nachweis von Persistenz und Datenabfluss in 12 Fällen
- Krisenkommunikation mit Geschäftsführung, Versicherern und Polizei, Playbooks für 6 Angriffsszenarien geschrieben

Incident Response Analyst
04/2019 - 05/2022

Hafenlogistik Nord AG — Hamburg

- Bearbeitung von **130** Sicherheitsvorfällen im konzernweiten CERT für 22 Tochtergesellschaften
- Wiederherstellung von Active Directory nach einem Angriff in 3 Tagen, Terminalbetrieb lief im Notbetrieb weiter
- Einführung von CrowdStrike Falcon auf 8.000 Endpunkten zur schnelleren Eindämmung
- Jährliche Notfallübungen mit IT-Betrieb und Kommunikation vorbereitet und ausgewertet

SOC Analyst
01/2017 - 03/2019

Hanse Rechenzentrum GmbH — Hamburg

- Alarmbearbeitung im SIEM für 30 Kunden im Schichtbetrieb, rund 70 Alarme pro Schicht
- Erste Forensikaufgaben an Festplattenabbildern unter Anleitung des CERT
- Übergabe von rund 15 bestätigten Vorfällen pro Monat an das CERT mit Zeitleiste

Ausbildung

Bachelor of Science
10/2012 - 12/2016

Universität Hamburg — Hamburg

Informatik

Kenntnisse

- Incident Response
- Digitale Forensik
- Velociraptor
- KAPE
- Volatility
- Ransomware
- Active Directory
- CrowdStrike Falcon
- Krisenkommunikation
- Playbooks

Sprachen

Deutsch	Muttersprache
Türkisch	Muttersprache
Englisch	C1

Zertifikate

GIAC Certified Forensic Analyst (GCFA)
05/2021

GIAC

Vorfall-Experte im Cyber-Sicherheitsnetzwerk
02/2023

Bundesamt für Sicherheit in der Informationstechnik (BSI)