



✉ andrij.kovalenko@beispiel.de

☎ +49 000 0000000

📍 Dortmund

Kenntnisse

SOC & Alarm-Triage

Incident Response

SIEM-Recherche

Log-Analyse

MITRE ATT&CK

Phishing-Analyse

Linux

TCP/IP & Firewalls

OWASP Top 10

Case Reporting

Python

Vibe Coding

Sprachen

Ukrainisch Muttersprache

Russisch fließend

Deutsch fließend

Englisch Grundkenntnisse

Andrij Kovalenko

Junior SOC Analyst

Alarme sicher einordnen, lückenlos dokumentieren, verlässlich übergeben

Profil

Zwölf Jahre Schichtdienst und Verantwortung im Lager haben mich gelehrt, unter Zeitdruck ruhig zu bleiben und sauber zu übergeben. Diese Haltung trage ich ins Sicherheitsteam: Sieben Wochen Schichten im SOC-Simulator, drei TryHackMe-Prüfungen und ein Portfolio, das zeigt, wie ich arbeite.

Weiterbildung

01/2027 –
10/2027

AI-Driven Security Operations Specialist

CYBERSQUAD Akademie, Düsseldorf · online, live, Vollzeit · 1.400 Unterrichtseinheiten

- Fundament: Windows, Linux, TCP/IP, Routing, Firewalls
- Web-Schwachstellen (OWASP Top 10), Schadsoftware, Protokolldateien
- Sieben Wochen Schichten im SOC-Simulator: priorisieren, im SIEM recherchieren, Playbooks, Case Reports, Eskalation
- Python-Einstieg und Vibe Coding: eigene Werkzeuge bauen, lesen, testen

Praxisnachweise · Portfolio auf GitHub

Case Report: Kontoübernahme

Aus dem SOC-Simulator: Anmeldung um 3 Uhr aus einem Land ohne Firmenbezug, neues Gerät, 14 Weiterleitungsregeln. Als True Positive eskaliert.

alert-triage (Python)

Sortiert Alarme nach Dringlichkeit und markiert Fehlalarm-Kandidaten. Die Entscheidung bleibt beim Analysten.

brute-force-watch (Python)

Erkennt Anmeldeserien in Logdateien, etwa fünf Fehlversuche in einer Minute, und formuliert die Meldung fürs Ticket.

Berufserfahrung

2022 –
2026

Lagermitarbeiter im Schichtbetrieb

Logistikzentrum, Dortmund

- Schichtübergaben lückenlos dokumentiert

2013 –
2022

Lagerleiter

Logistikunternehmen, Charkiw (Ukraine)

- Team von acht Personen geführt, Warenfluss gesteuert

2008 –
2013

Bachelor Logistik

Nationale Universität, Charkiw (Ukraine)



SEC0
04/2027

TryHackMe Pre-Security:
Netzwerke, Datenwege,
Angriffsspuren



SEC1
06/2027

TryHackMe Cyber Security 101:
Schwachstellen erkennen,
Protokolle lesen



SAL1
07/2027

TryHackMe Security Analyst
Level 1: Vorfälle im
Sicherheitsteam bearbeiten



Akademie
10/2027

Zertifikat der CYBERSQUAD
Akademie über die abgeschlossene
Weiterbildung

Abgenommen von TryHackMe, nachprüfbar über Credly und im öffentlichen TryHackMe-Profil (Rang, Badges, Räume).



BEISPIEL

Lebenslauf der CYBERSQUAD Akademie. Person und Werdegang sind frei erfunden, das Foto ist ein Symbolfoto. Ob Prüfungen bestanden werden und ob eine Stelle folgt, können wir nicht zusagen.

Symbolfoto: Pexels