Abel Tamrat

abel@abeltamrat.tech | +49 17664739808 | LinkedIn | Website | Github

PROEJEKTE

Microsoft Sentinel Detection Lab *October 2026 – November 2026*

- Isolierte Windows-Server-2022-VM (VirtualBox, NAT, sauberer Basis-Snapshot) aufgebaut und per Azure Arc angebunden; Security- und Sysmon-Ereignisse über Data Collection Rules in Microsoft Sentinel eingespeist, Tageslimit von 1 GB mit E-Mail-Alarm.
- 4 MITRE-ATT&CK-Techniken mit Atomic Red Team simuliert (T1136.001, T1053.005, T1547.001, T1087.001) und 4 von 4 mit KQL-Analytics-Rules innerhalb von etwa 6–14 Minuten erkannt; dabei entstanden 8 Incidents.
- Incidents als Tier 1 in 3 Tickets triagiert (2 True Positives eskaliert, 1 Benign True Positive) und Ergebnisse, Duplikate und Erkennungslücken mit Tuning-Empfehlungen in einem einseitigen SOC-Report dokumentiert.
- Incident-Bearbeitung mit einer Automation Rule (Tagging, Zuweisung) automatisiert; fehlende Audit-Richtlinien und einen fehlenden DCR-Filter behoben, sodass die Event-IDs 4688 und 4698 in Sentinel ankamen.

Active-Directory-Lab in Azure *November 2026*

- Windows-Server-VM in Azure (Germany West Central) mit statischer privater IP bereitgestellt, Active Directory Domain Services installiert und zum Domänencontroller (abel-lab.local) hochgestuft.
- Organisationseinheiten für einen Standort (Munich: Users, Workstations, Laptops), Benutzerkonten und 3 Sicherheitsgruppen (Helpdesk, ITSupport, Accounting) angelegt sowie Zurücksetzen von Passwörtern für die Helpdesk-Gruppe delegiert.
- Windows-Client-VM in die Domäne aufgenommen (DNS auf den Domänencontroller gesetzt), RDP-Zugriff per Regel auf die eigene IP-Adresse beschränkt und Anmeldung sowie Gruppenmitgliedschaft mit whoami /groups geprüft.

Interaktive Helpdesk Simulationen (Servicedesk Simulator) *fortlaufend*

- Über 20 ticketbasierte Supportfälle selbstständig gelöst: Drucker, Monitore, Dockingstationen, WLAN, VPN, Netzlaufwerke und Zwei-Faktor-Authentifizierung.
- Fehler durch Rückfragen an simulierte Nutzer sowie mit Dokumentation und Administrationswerkzeugen eingegrenzt und behoben.

STUDIUM

Ludwig Maximilians Universität **München**

B.Sc. Informatik (Computer Science) *Abschluss: März 2026*

- Vierstufiges, präregistriertes Online-Experiment (N = 96) konzipiert und als Streamlit-Web-App umgesetzt (Python, Gemini API, Live-Erfassung des KI-Anteils, automatisierter Datenexport).
- Unerlaubte externe KI-Nutzung bei 50 % der Pilotteilnehmenden entdeckt und mehrschichtige Vorbeugungs- und Erkennungsmaßnahmen zum Schutz der Datenqualität eingeführt.
- Ergebnis: Identifizierbarkeit stellte das Gefühl von Ownership wieder her, löste aber KI-Vermeidung aus und senkte die Textqualität.

ZERTIFIKATE

Microsoft Certified: Azure Fundamentals Certificate	bestanden 09/2026
Google: Technical Support Fundamentals Certificate	bestanden 10/2026
Google: The Bits and Bytes of Computer Networking	bestanden 11/2026

SKILLS & INTERESSEN

Security & Monitoring: Microsoft Sentinel | KQL | Analytics Rules | Sysmon | Windows Event Logs | Azure Monitor | Log Analytics | MITRE ATT&CK | Atomic Red Team
Infrastruktur: Windows Server 2022 | Active Directory | Group Policy | Azure Arc | Oracle VirtualBox | Ubuntu
Networking: TCP/IP | DNS | DHCP | VPN
Scripting: PowerShell | cmd | Linux command line | Java

Interessen: Cybersecurity, Lesen, Fussball, Trainieren