CONTACT

Oldenburg, Germany

+49 160 950 64569

info@bogdanorel.de

Website
bogdanorel.de

LinkedIn
linkedin.com/in/bogdan-orel

GitHub
github.com/orelsv

Notion Portfolio
notion.so/Projects-Cybersteps

TECHNICAL SKILLS

Microsoft Cloud Security (Defender XDR)

Microsoft Sentinel, Microsoft Defender XDR, Defender for Cloud, Defender for Endpoint, Microsoft 365, Microsoft Entra ID (Azure AD), Advanced Threat Protection

SOC & Detection Engineering

KQL (Kusto Query Language), Threat Detection, Use-Case Development, Alert Triage, MITRE ATT&CK, Sysmon, Incident Response, SIEM (Splunk)

Identity & Access

Microsoft Entra ID, Active Directory, Conditional Access, MFA, Single Sign-On (SSO), RBAC, Microsoft Graph API

Automation & Forensics

PowerShell, Python, Bash, Azure CLI, Bicep, GitHub Actions, Wireshark, Volatility, Autopsy, Nmap

SOFT SKILLS

- Self-organization
- Customer focus & advisory mindset
- Analytical work style
- Strong willingness to learn
- Structured communication

LANGUAGES

Ukrainian	Native
Russian	Native
English	C1
German	B2

Bogdan Orel

Cyber Security Analyst · Microsoft Cloud Security

PROFILE

Cyber Security Analyst with a clear focus on the Microsoft Cloud Security stack: Microsoft Sentinel, Defender XDR, Defender for Cloud, and Microsoft Entra ID. In August 2026 I completed a 2,400-hour cybersecurity training program at Cybersteps. In my own lab projects I built a Microsoft Sentinel honeypot in Azure that captured over 3,200 real login attempts, wrote KQL detection rules mapped to MITRE ATT&CK, and developed an Entra ID security auditor in Python (Microsoft Graph API + Azure OpenAI) against the EntraGoat lab. Microsoft SC-300 (Identity and Access Administrator), AZ-900 and SC-900 certified; next I plan PECB ISO 27001 Foundation. From 8+ years as an operations lead I bring structured problem-solving, clear user communication and 24/7 standby experience. This is exactly where, in the Microsoft Cloud Security stack, I want to take my next step as a Cyber Security Analyst.

EDUCATION

Cybersteps — Aug 2025 - Aug 2026

Cybersecurity Analyst · Training Program

- 2,400 hours of hands-on focus on Microsoft Cloud Security: Microsoft Sentinel, Defender XDR, Defender for Cloud, Microsoft 365, and Microsoft Entra ID.
- Built and operated a Microsoft Sentinel environment in Azure: DCR with Sysmon, KQL detection rules mapped to MITRE ATT&CK; Splunk investigations (Boss of the SOC v1) and threat-hunting use cases.
- Developed a custom Entra ID security auditor in Python (Microsoft Graph API + Azure OpenAI) tested against the EntraGoat lab; implemented Conditional Access, MFA, RBAC, and SSO in own Entra ID tenants.
- DFIR scenarios (disk, memory, network) with Wireshark, Volatility, and Autopsy; Active Directory red+blue lab with Wazuh; automation in PowerShell, Python, and Bash.

IT Step Computer Academy — 2005 - 2007

Computer Graphics & Internet Technologies

CERTIFICATIONS

Cybersteps – Cybersecurity Analyst Program · Verify	Aug 2026
Microsoft – Identity and Access Administrator Associate (SC-300) · Verify	Aug 2026
Microsoft – Security, Compliance, and Identity Fundamentals (SC-900) · Verify	Jun 2026
Microsoft – Azure Fundamentals (AZ-900) · Verify	May 2026
CompTIA – Security+ ce · Verify	Feb 2026
CompTIA – Tech+ · Verify	Oct 2025

PROJECTS

Bait n' Switch – Azure Honeypot & SOC Monitoring (Microsoft Sentinel)

Full Microsoft Sentinel pipeline (DCR, Sysmon); analyzed 3,200+ real attacks from 7 countries, KQL detections mapped to MITRE ATT&CK, event prioritization and hardening recommendations

Chat With Your Entra – AI-Powered Security Auditor

Python + Microsoft Graph API + Azure OpenAI; detects misconfigurations in Conditional Access, B2B guests, and roles against the EntraGoat lab (4/6 scenarios detected automatically)

Capstone – Game of Active Directory (Blue Team with Wazuh)

AD lab with AS-REP Roasting and Kerberos hardening; SIEM monitoring and incident detection through Wazuh

oscan – Cybersecurity Self-Assessment Scanner

Python CLI for AI-generated apps and websites; hybrid deterministic + AI checks (SQLi, secrets in git history, weak headers, GDPR); published on PyPI with CI, MIT, 54 tests

WORK EXPERIENCE

EDDIKS GRAFIK — Oct 2023 - Mar 2025

3D Visualizer · Full-time — Oldenburg, Germany · On-site

- Delivered technically demanding 3D visualizations; ensured 100% data integrity and precision in client deliverables.
- Took responsibility for 2 large-scale projects and supported 4 team-based workflows; led workshops on AI-driven automated workflows.

DronAgronom LLC — Feb 2019 - Nov 2022

Operations Lead / Technical Support · Full-time — Dnipro, Ukraine · On-site

- Trained and supported 30+ drone pilots in safe system operation; provided 24/7 support for ongoing operations and rapid troubleshooting on hardware and software incidents.
- Coordinated operations across 5+ teams; advised stakeholders and translated customer requirements into technical solutions.
- Resolved 3–10 technical incidents per week in high-pressure environments; raised operational stability by approximately 20% through structured processes.

Laserbox C — Jul 2016 - Jan 2019

Product & Operations Lead · Full-time — Dnipro, Ukraine · On-site

- Organized sales contracts and data operations across 3 e-commerce platforms and 5 offline stores in 5 cities.
- Managed product lifecycle from concept to production; developed 100+ products and reduced material waste by 10% through strict quality control.