Batuhan ALKOC
Senior Infrastructure & SecOps Engineer

Open to Relocation | info@batualkoc.com | LinkedIn Url | Website | +90 530 201 8823

CAREER SUMMARY

Results driven Infrastructure & Security Operations (SecOps) Engineer with expertise in managing highly available, large scale enterprise environments (**4,000+ users, 600+ endpoints**). Proven track record in orchestrating zero downtime migrations to HCI architectures, engineering ransomware resilient disaster recovery strategies, and architecting proactive defense lines using SIEM/Vulnerability management. Passionate about modernizing IT operations by integrating **workflow automation (n8n)** and **Private AI/Local LLM infrastructure** to minimize technical debt and accelerate business continuity.

PROFESSIONAL EXPERIENCE

AKO Group (Petlas Tire Industry and Trade) **Ankara, Turkey**
Senior Infrastructure & SecOps Engineer *September 2024 – Present*

- **Enterprise Infrastructure Management:** Managed and optimized a highly available enterprise infrastructure supporting **4,000+ employees and 600+ active endpoints**, utilizing a 4 node HPE SimpliVity HCI architecture distributed across primary and disaster recovery (DR) sites.

- **Zero Downtime Modernization:** Spearheaded the seamless migration of 90+ critical VMs and upgraded legacy domain infrastructure (Windows Server 2012 R2 to 2022). Maintained an Active Active High Availability setup for AD and DHCP during in place upgrades, achieving zero operational downtime.

- **Exchange & Identity Management:** Administered on-premises Microsoft Exchange Server including SSL certificate lifecycle management, patch deployment, mailflow/relay configuration, ADFS/IIS integration, and full mailbox operations across 600+ user accounts.

- **Security Operations & Automation (SecOps):** Engineered automated security workflows using **n8n**, implementing continuous monitoring for compromised corporate credentials via 'Have I Been Pwned' API, proactively auditing Active Directory for orphaned 'ghost' accounts, and tracking domain/IP spam reputations.

- **Ransomware Resilience & DR:** Architected a ransomware-resilient DR strategy using Veeam (Full + Incremental) with 7-day immutable air-gapped backups on a 100TB HPE Alletra array. Configured Zerto for real-time geographic replication with a dedicated FKM vCenter for automated failover orchestration. Managed a separate Veeam instance for the Gen9 lab cluster backing up to QNAP storage.

- **Network & Perimeter Defense:** Administered perimeter security and network traffic flow across 200+ H3C L2/L3 switches, 300+ access points, and the H3C backbone switch. Hardened the perimeter using the Fortinet ecosystem (FortiGate VPN/policy management, FortiMail anti-spam and log controls). Managed Subgate RADIUS for strict guest Wi-Fi access control and enforced regulatory compliance logging per Law No. 5651 (365-day retention).

- **Threat Hunting & Vulnerability Management:** Deployed Wazuh SIEM to ingest and correlate logs from 90+ servers and FortiGate, creating custom detection rules for RDP/SSH anomalies and file server deletion events. Conducted biannual network-wide vulnerability assessments using Greenbone (OpenVAS) to proactively patch emerging threats.

- **Lab & R&D Infrastructure:** Managed a secondary vCenter environment on HPE Gen9 servers for R&D and lab workloads (EVE-NG network simulation, Ollama AI inference), with dedicated Veeam backup to QNAP NAS storage.

- **Endpoint Security Support:** Supported the administration of Trellix DLP and Avast endpoint security platforms, configuring USB restrictions and drive encryption policies to prevent unauthorized data exfiltration.

- **Monitoring:** Deployed **Grafana and Zabbix** dashboards to monitor real-time server health and network traffic, enabling preemptive incident response.

Turkish Armed Forces (55th Mechanized Infantry Brigade) **Ankara, Turkey**
Communication Information Systems Officer *(First Lieutenant)* *October 2021 – August 2024*

- **Large Scale IT Management:** Directed the IT infrastructure, secure communications, and data center operations for a critical facility supporting **2,500+ personnel**, ensuring strict compliance with military grade security protocols.
- **Business Continuity & Incident Response:** Led emergency incident response teams during critical network outages. Designed and executed robust data backup and disaster recovery protocols to guarantee zero data loss and uninterrupted secure communications.
- **Infrastructure Optimization:** Conducted continuous monitoring and performance tuning of servers and enterprise network equipment, proactively identifying bottlenecks and reducing system latency.
- **Team Leadership & Operations:** Managed a technical team responsible for daily hardware/software deployments, routine maintenance, and Tier 2/3 technical support across a highly secure, restricted environment.

TECHNICAL PROJECTS & R&D INITIATIVES
Self Hosted & Automation Projects

- **Private AI & LLM Infrastructure (Self Hosted):** Architected and deployed privacy focused, on-premise AI environments. Configured local Large Language Models (LLMs) via **Ollama**, utilized **OpenWebUI** for conversational interfaces, and deployed **ComfyUI** for local generative AI workloads. Integrated **OpenClaw** for autonomous AI agent management, demonstrating expertise in AI infrastructure security and data sovereignty.
- **Microservices & Secure Networking:** Engineered a private cloud architecture using Docker containers on Raspberry Pi 5. Secured externally exposed local services without port forwarding using **Cloudflare Tunnels**, and enforced network wide DNS filtering with **AdGuard Home**.
- **Enterprise Mail Infrastructure:** Deployed and currently managing a highly secure, dockerized Mailcow suite. Enforced strict email deliverability and anti-spoofing policies by configuring complex DNS records **(SPF, DKIM, DMARC, BIMI)** and integrated Rspamd for robust threat mitigation.

EDUCATION & CERTIFICATIONS

National Defense University (Turkish Military Academy) **Ankara,Turkey**
Bachelor of Science, Computer Engineering September *2017 – August 2021*

Certifications: Fortinet NSE 1-3, Cisco CCNA (Course Completed), Currently preparing: Fortinet NSE 4 and CCNA

SKILLS

Infrastructure & Cloud:
- HPE SimpliVity (HCI), VMware vSphere/ESXi, vCenter, Hyper-V, Windows Server 2019/2022, Linux, Docker & Docker Compose, Active Directory, DNS/DHCP

Microsoft On-Premises:
- Exchange Server (ADFS, IIS), Active Directory, Group Policy (GPO), WSUS

Security Operations (SecOps):
- Wazuh SIEM, Greenbone (OpenVAS), Fortinet (FortiGate, FortiMail), RADIUS/802.1x, Trellix DLP, 5651 Compliance Logging

Networking:
- H3C L2/L3 Switches (200+), AP Controller (300+ APs), SSL-VPN, Guest Wi-Fi

Backup, DR & Storage:
- Veeam Backup & Replication (Immutable/Air Gapped), Zerto (Geographic Replication), HPE Alletra Storage, High Availability (HA) Planning.

Automation & AI Infrastructure:
- n8n Workflow Automation, Docker, Local LLM Deployment (Ollama, OpenWebUI, Unsloth, llama.cpp), AI Agent Management.

Scripting & Monitoring:
- Python, PowerShell, Bash, Grafana, Zabbix.