MUHAMMED KILIG

Phoenix, AZ | mskilic98@gmail.com | 480-800-7650 | linkedin.com/in/mkilig

PROFESSIONAL SUMMARY

Cybersecurity professional with 7+ years of progressively expanding experience: from cyber threat intelligence and penetration testing to cloud security and enterprise risk consulting at PricewaterhouseCoopers. This breadth of hands-on technical and strategic experience enables a rare ability to assess risk from multiple vantage points: understanding how threats materialize at the technical level while translating that context into actionable governance, controls, and remediation strategies at the executive level. Currently advising Fortune 500 clients across financial services, insurance, energy, and aerospace on cybersecurity risk, compliance, and control frameworks.

PROFESSIONAL EXPERIENCE

Cyber Defense & Engineering Consultant | *PricewaterhouseCoopers (PwC)* | Phoenix, AZ | 07/2022 – Present

- Contributed to an aerospace and defense engagement that generated ~$2.8M in consulting revenue over 8 months through two successive high-impact workstreams: an OT asset inventory assessment producing consolidation roadmaps and integration architecture diagrams, followed by a crown jewel application protection program defining board-level risk metrics and cross-functional protection plans across classified, OT, IT, and lab environments.
- Led NYDFS Part 500 readiness engagement for insurance client as SME, assessing cybersecurity program gaps against amended regulation requirements; facilitated CISO relationship that generated $70K+ in follow-on work.
- Translated third-party penetration test findings into detailed vulnerability management remediation plans for a major financial services client, driving four contract change orders through consistent delivery of high-quality, actionable security guidance.
- Conducted SSH, RDP, and Telnet network log analysis to identify employees accessing high-risk protocols, directly informing the design of role-based access approval workflows that reduced unauthorized infrastructure access exposure.
- Performed cloud security posture assessments across multi-account AWS environments using CSPM tooling, identifying critical IAM misconfigurations and logging gaps that were translated into prioritized remediation roadmaps which enabled clients to measurably improve their cloud security posture.
- Validated audit findings, led root cause analysis, and partnered with control owners to define corrective action plans (CAPs) - ensuring findings were remediated within regulatory deadlines and reducing clients' risk exposure ahead of auditor reviews.
- Leverage Claude, ChatGPT, & other AI platforms to develop internal tooling and automate risk tracking, report generation, and control validation workflows resulting in reduced man-hours and accelerating delivery across concurrent client engagements

Cybersecurity Engineer | *CYR3CON / CSW – Cyber Security Works* | Tempe, AZ | 02/2017 – 01/2022

- Led cloud infrastructure transition post-acquisition, migrating and securing 3 AWS accounts to new architecture with zero downtime, meeting critical acquisition integration deadlines
- Conducted bilingual dark web threat intelligence operations across dozens of forums, marketplaces, and hacker communities; maintaining multiple covert digital identities to sustain long-term access, feeding a proprietary intelligence database, and serving as the sole analyst covering Turkish-language threat actor ecosystems for clients with regional exposure.
- Managed security operations across 4 on-premises servers and 20+ VMs and organizational devices; implemented sandboxed network architecture to isolate and protect dark web analyst access, and conducted quarterly internal penetration testing hackathons that uncovered and remediated critical vulnerabilities across all systems.
- Drove a company-wide cybersecurity culture transformation, elevating the organization from basic awareness to a fully cyber-resilient workforce through targeted training, resulting in zero successful phishing or vishing incidents.

Penetration Tester Intern | *Intel Corporation* | Chandler, AZ | 05/2019 – 08/2019

- Conducted black-box penetration testing on a military-grade Windows system, investigating potential exploit paths in Intel ME, Boot Guard, and Secure Boot; performed BIOS/UEFI vulnerability assessments against CVE databases using industry-standard penetration testing frameworks.

EDUCATION

B.S., Computer Science | *Arizona State University – Ira A. Fulton Schools of Engineering* | Tempe, AZ | 05/2021

CERTIFICATIONS

CISSP – Exam Scheduled Q3 2026 | AWS Solutions Architect – Associate (Renewal In Progress) | Microsoft Certified: Azure Fundamentals (2024) | Oracle Cloud Infrastructure Foundations (2023)

TECHNICAL SKILLS

Frameworks: NIST CSF, NIST 800-53, ISO 27001, NYDFS Part 500, SOX ITGCs, IEC 62443

GRC & Risk: Risk Assessment, Control Design, Gap Analysis, Audit Management, CAP Tracking, Executive Reporting

Tools & Project Management: ServiceNow, Jira, Visio, Miro, Microsoft Office Suite, SharePoint

Cloud: AWS Cloud Environments, Cloud Security Posture Management

Offensive Security: Penetration Testing, Vulnerability Assessment, Threat Intelligence, Adversary Simulation

Languages: English (Native) | Turkish (Native)