MOHSIN KHAN

Information Security Engineer · Security Operations & Engineering
Tromsø, Norway
+47 46750558 | khann.mohsin@icloud.com | khannmohsin.github.io | github.com/khannmohsin |
linkedin.com/in/khannmohsin/ | khannmohsin

Information security professional with 4+ years of experience designing, testing, and hardening security controls across cloud and distributed systems. Experienced in security monitoring, incident analysis, and vulnerability assessment, with a focus on building resilient systems for real-world operations.

SECURITY ENGINEERING & OPERATIONS HIGHLIGHTS

- Conducted security assessments of APIs and services to identify vulnerabilities, access control weaknesses, and misconfigurations.
- Performed security monitoring and incident investigation through analysis of web, API, and system logs using SIEM tools.
- Validated remediation and system hardening through issue reproduction, retesting, and regression verification.
- Supported security operations through Python-based automation, IAM policy validation, and endpoint protection concepts aligned with enterprise EDR solutions.

CORE COMPETENCIES

Security Engineering	Design and validation of security controls, system hardening, least-privilege enforcement
Cloud & Identity Security	IAM concepts, authentication and authorization controls, secure access design
Security Operations	Security monitoring, alert analysis, incident investigation, vulnerability assessment
Automation & Scripting	Python-based automation, regression testing, log analysis, and basic PowerShell scripting
Logs & Traffic Analysis	SIEM (Splunk), log correlation, traffic inspection (Wireshark), configuration review
Security Testing & Validation	API and backend security testing, access control validation, remediation verification
Tools & Platforms	Burp Suite, Nmap, Metasploit, Docker, Kubernetes
Security Standards & Practices	OWASP Top 10, secure coding principles, SDLC, verification of security fixes
Microsoft Security Stack	Azure security fundamentals, Entra ID (Azure AD), endpoint protection (EDR)

PROFESSIONAL EXPERIENCE

UiT Norges arktiske universitet, *PhD Research Fellow – Applied Cybersecurity* | Tromsø, Norway — Nov 2021 – Dec 2025

- Designed and implemented secure access-control mechanisms for distributed IoT and cloud systems, enabling dynamic authentication and authorization.
- Supported security monitoring, incident investigation, and vulnerability assessment to protect system availability through log analysis and Python-based telemetry workflows.
- Aligned technical security controls with GDPR and ISO 27001, with foundational awareness of NIS/NIS2 requirements for availability and incident handling.

Security Analyst – API Incident Analysis (Deloitte, Forage) — Dec 2025

- Analyzed web and API access logs to assess suspected security incidents, identifying anomalous patterns and automated API abuse.
- Evaluated authentication and authorization behavior and reproduced security issues to validate exploitability and support remediation decisions.

Incident Response & Vulnerability Analyst (AIG, Forage) — Jan 2026

- Assessed vulnerability exposure using CISA advisories (e.g., Log4j) to define risk-based remediation actions.
- Supported incident recovery through Python-based response tooling and post-incident remediation validation.

Cybersecurity Analyst – Identity & Access Security (Tata, Forage) — Jan 2026

- Evaluated enterprise IAM readiness and identified access gaps impacting authentication and authorization.
- Produced IAM design documentation supporting least-privilege enforcement and compliance objectives.

Blackbuck Insight, *Data Engineer* | Bangalore, India — Jan 2021 – Nov 2021

- Migrated sensitive datasets to AWS cloud environments with IAM-based access controls.
- Monitored and optimized production workloads to ensure data integrity, availability, and secure operations.

PROJECTS

Security Monitoring & Incident Analysis — 2025 – 2026

- Performed SIEM-based alert triage, log analysis, and traffic inspection across Windows and Linux environments to identify security incidents.
- Applied structured incident investigation techniques using threat indicators and attack pattern mapping to support detection and response.

Vulnerability Impact Analysis & Threat Mitigation 2025

- Assessed system vulnerabilities using risk- and impact-based analysis to prioritize remediation actions.
- Validated mitigation effectiveness through structured reassessment and verification.

Cloud Security Architecture & Risk Analysis 2025

- Evaluated cloud deployment models to identify security risks and recommend appropriate security controls.
- Applied shared responsibility and cloud security best practices to strengthen system resilience.

BlockCap: Capability-Based Authorization for Distributed Systems 2023 – 2025

- Designed and validated a distributed authorization mechanism using cryptographic identities and capability-based tokens.
- Improved system resilience by enforcing least-privilege access and securing inter-node communication.

TRAINING AND CERTIFICATIONS

OSCP	Ongoing
IBM – Incident Response and System Forensics	Jan 2026
IBM – Vulnerability Management	Dec 2025
IBM – Cloud Security	Dec 2025
Qualys – Vulnerability Management Foundation	Dec 2025
LinkedIn Learning – ISO 27001 Compliant Cybersecurity	Dec 2025
LinkedIn Learning – ISO 27001: The Annex A Controls	Dec 2025
AWS – Certified Developer – Associate	Feb 2021

EDUCATION

UiT Norges Arktiske Universitet, *PhD in Cybersecurity* | Tromsø, Norway — Nov 2021 – Dec 2025
Indira Gandhi National Open University, *MBA in Operations Management* | New Delhi, India — Jan 2019 – Jul 2022
Central University of Jammu, *M.Tech in Computer Science and Engineering* | J&K, India — Aug 2018 – Nov 2020
Baba Ghulam Shah Badshah University, *B.Tech in IT & Telecom Engineering* | J&K, India — Aug 2014 – Jun 2018

LANGUAGES

English	Professional proficiency
Norwegian (Bokmål)	Beginner proficiency
Kasmiri	Native proficiency
Hindi	Native proficiency

REFERENCES

Håvard Johansen
UiT The Arctic University of Norway
havard.johansen@uit.no

Dag Johansen
UiT The Arctic University of Norway
dag.johansen@uit.no

Elisavet Kozyri
UiT The Arctic University of Norway
elisavet.kozyri@uit.no