RIFAT ERDEM SAHIN

SENIOR INCIDENT RESPONSE MANAGER | CYBER SECURITY INCIDENT RESPONSE & CRISIS MANAGEMENT

📍 **Location:** London, United Kingdom
🇬🇧 **Citizenship:** British
✉️ **Email:** contact@rifaterdemsahin.com
📞 **Phone:** +44 7848 024173
🔗 **LinkedIn:** linkedin.com/in/rifaterdemsahin
💻 **GitHub:** github.com/rifaterdemsahin
🌐 **Portfolio:** https://rifaterdemsahin.com
📅 **Schedule a Call:** https://calendly.com/rifaterdem/schedule

PROFESSIONAL SUMMARY

Senior Incident Response Manager specializing in **managing high-severity cyber incidents, threat hunting, and crisis communication**. Deep expertise in leading incident response teams (CSIRT) through complex security breaches, ransomware attacks, and nation-state threats. Proven track record in reducing mean time to detect (MTTD) and mean time to respond (MTTR) by 50% across financial services, healthcare, and critical infrastructure sectors. Expert in NIST Incident Response Framework and cyber resilience strategies.

CORE COMPETENCIES

🚨 **Incident Response & Management** - End-to-end incident lifecycle management (NIST/ISO 27035) - Crisis management and executive communication - Digital forensics and evidence handling - Playbook development and tabletop exercises (TTX)

🔍 **Threat Intelligence & Hunting** - Threat hunting operations and IoC analysis - Cyber threat intelligence (CTI) integration - Malware analysis and sandboxing awareness -

SIEM/SOAR optimization for threat detection

KEY ACCOMPLISHMENTS

🏆 2024 | Global Financial Institution | London

Ransomware Response & Recovery - **Challenge:** Managed a critical ransomware attack affecting global operations. - **Solution:** Led the crisis management team, coordinated containment strategies, and managed stakeholder communications. - **Impact:** - Successfully contained the breach within 4 hours, preventing data exfiltration. - Guided the organization through a full recovery without paying the ransom. - Implemented post-incident improvements reducing future attack surface by 40%. - **Technologies:** SentinelOne, Splunk, CrowdStrike, Palo Alto Networks

🏆 2023 | Critical Infrastructure Provider | UK

SOC/CSIRT Maturity Transformation - **Challenge:** Improve the maturity and response capabilities of an underperforming SOC. - **Solution:** Redefined incident response processes, introduced automated playbooks, and conducted regular tabletop exercises. - **Impact:** - Reduced MTTR by 60% through automation and clear process definitions. - Improved SOC analyst retention by 80% through better tooling and training. - Achieved ISO 27035 compliance for incident management.

PROFESSIONAL EXPERIENCE HIGHLIGHTS

Senior Senior Incident Response Manager / AI Solutions Architect | January 2025 - Present *IBM* | *London, UK*

- Architecting hybrid cloud transformation using IBM Cloud and Red Hat OpenShift for Fortune 500 enterprises
- Implementing watsonx AI solutions for intelligent automation, reducing operational overhead by 35%
- Leading DevSecOps transformation with Ansible Automation Platform and Terraform IaC across multi-cloud environments
- Delivering zero-downtime Kubernetes cluster migrations for mission-critical financial and government workloads

- Building enterprise CI/CD pipelines with GitHub Actions and Jenkins serving 500+ developers globally

Senior Senior Incident Response Manager / Technical Lead | 2020 - 2025 *Goldman Sachs, Ypsomed, Cushman & Wakefield*

- Led senior incident response manager initiatives across finance, healthcare, and real estate sectors
- Designed and implemented solutions supporting millions of daily transactions
- Established best practices and automated frameworks
- Mentored engineering teams on modern technologies and practices
- Delivered solutions achieving 300% improvement in operational efficiency

Senior Incident Response Manager | 2016 - 2020 *Microsoft, Emerson, Various Fortune 500*

- Built enterprise solutions for digital transformation initiatives
- Led cross-functional teams designing scalable applications
- Established frameworks and implementation strategies
- Evangelized modern technologies through technical leadership

---

EDUCATION

🎓 **Bachelor of Science**
Southern New Hampshire University, USA 🇺🇸 | 2013

CERTIFICATIONS & CONTINUOUS LEARNING

📜 **Microsoft Certified Solutions Architect Expert**
📜 **AWS Certified Solutions Architect Professional**
📜 **Azure Solutions Architect Expert**
📜 **Certified Kubernetes Administrator (CKA)**

Continuous Learning:
- Active contributor to open-source projects - Regular participant in technical communities - Following latest developments in technology - Experimenting with emerging tools and practices

SECURITY CLEARANCES

🔒 **UK SC (Security Check)** - Valid until 2028
🔒 **NATO Clearance** - Valid until 2029
✓ **Background Checks:** Watchdog (2024), Sterling (2019)

AVAILABILITY & CONTACT

Immediate Availability for senior incident response manager roles

📅 **Schedule a Discussion:** https://calendly.com/rifaterdem/schedule
📧 **Email:** contact@rifaterdemsahin.com
📞 **Phone:** +44 7848 024173

SUPPORTING DOCUMENTS

📊 **Technical Portfolio & Presentations:**
https://rifaterdemsahin.com/wp-content/uploads/2025/02/rifaterdemsahinprofilepresentation.v2025.2.pdf

References and detailed project portfolios available upon request