Rachel Kang

DFIR Manager

Seasoned security professional with 5 years of experience in security engineering and Digital Forensics and Incident Response (DFIR). Proven track record defending and maintaining Identity and Access Management (IAM) systems with a strong focus on Azure cloud technologies.

Chicago, IL (Hybrid)

(404) 563-4353

kpxrachel@gmail.com

www.rachelk.com

EXPERIENCE

Stroz Friedberg, an Aon Company — *2019 - Present*

Manager - DFIR — *Mar 2024 - Present*
Senior Consultant - DFIR — *Apr 2022 - Mar 2024*
Consulant - DFIR — *Jun 2020 - Apr 2022*
Cyber Associate — *Aug 2019 - Jun 2020*

Roles + Responsibilities

- Led multi-disciplinary teams in response to advanced persistent threats (APTs), ransomware, DDoS attacks, IP theft, and business email compromise (BEC) incidents
- Analyzed petabytes of data from diverse sources (SIEMs, EDRs, NDRs, AV outputs) to reconstruct timeline and determine anatomy of attack
- Delivered executive-level briefings to C-suite and key stakeholders during active incident response engagements
- Conducted in-depth forensic investigations across a variety of platforms including Windows, Mac, and Linux servers/workstations, Apple and Android mobile devices and tables, and removable media
- Mentored junior consultants on advanced forensic and threat hunting techniques, emphasizing dead box and cloud forensics

Significant Engagements

- Led a multi-cloud investigation for a Fortune 500 client following a global breach, focusing on GKE infrastructure assessment to expedite incident containment
- Mitigated an internal security threat for a Fortune 500 client, using UEBA, web proxy analysis, and firewall + VPN monitoring
- Led a team of 10 to investigate a zero-day vulnerability exploit for a client affected by a sophisticated supply chain attack, leveraging cloud and network artifacts to map unauthorized data access
- Orchestrated a comprehensive privacy risk assessment for a Fortune 500 client, delivering actionable guidance to align data handling practices with government compliance standards

Projects

- Designed and deployed an automated threat intelligence system to identify and track Cobalt Strike C2 servers, creating a historical IP database for improved threat assessment
- Designed and implemented a real-time status tracking dashboard using Redash, integrating AWS pipelines and SQL databases to optimize DFIR workflows
- Collaborated on developing an automated CLI tool utilizing Microsoft Graph API for secure Microsoft Azure log collection, improving data availability for BEC investigations

EDUCATION

Middlebury College — *2015 - 2019*

B.A. in Computer Science, Political Science (Double Major)
Graduated with cum laude

Carnegie Mellon University, Heinz College — *2018*

Summer Fellowship - IT Lab

Enhanced network threat detection via IDS and fine-tuning rule sets, significantly reducing false positives across a large-scale academic network infrastructure

TECHNICAL SKILLS

Security Technologies:
IAM, EDR, Firewall, VPN, SIEM (ElasticSearch, Splunk, LogRhythm, QRadar), IDS/IPS, Antivirus, DLP, UBA, Kubernetes

Security Concepts:
Authentication, RBAC, Zero Trust, Threat Modelling, Risk Management, TCP/IP Model, OWASP Top 10, MITRE ATT&CK

Cloud Security:
Microsoft Azure, Google Cloud Platform, Amazon Web Services, Oracle Cloud

Programming & Scripting:
Intermediate: Python, PowerShell, Bash, SQL
Basic: Zeek, YARA, Volatility, JavaScript/ TypeScript

OTHERS

Certifications:

- GIAC Certified Intrusion Analyst (GCIA)
- Microsoft Certified: Azure Fundamentals (AZ-900)
- GIAC Cloud Forensics Responder (GCFA)
- GIAC Certified Forensic Analyst (GCFA)
- GIAC Certified Forensic Examiner (GCFE)

Publications:

- Author of 'Microsoft 365: Identifying Mailbox Access' [*Post*]
- Author of 'The Evolution of Phishing Campaigns' [*Post*]

Professional Development:

- Presenter at BSidesPGH 2024 ('The New Generation Of Phishing: Beyond the Mailbox') [*Slides*]
- Presenter at WiCyS 2024 ('Phishing 2.0 - The Rise of Artificial Intelligence') [*Slides*]

Professional Membership:

- Member of GIAC Advisory Board
- Member of Executive Women's Forum
- Member of Women in CyberSecurity