Kiana Kiashemshaki

(415)-696-0546 | Sacramento, CA, 95630 | kianakia399@gmail.com

Kiana Kiashemshaki | Personal Website | GitHub

Profile

SOC Analyst with hands-on experience in real-world security operations, SIEM monitoring, alert triage, and incident investigation. Proven ability to analyze endpoint, server, and network logs to detect suspicious activity and support incident response. Strong background in digital forensics, systems, and networking with a blue-team mindset and shift-ready operational experience.

EDUCATION

- **Bowling Green State University** — *2023-2025*
  M.S. in Computer Science specializing in Cybersecurity (GPA:3.8/4.0) — Bowling Green, Ohio, U.S
- **Azad University** — *2015-2019*
  B.S. in Computer Engineering (GPA:4.0/4.0) — Tehran, Iran

EXPERIENCE

- **Redapple Digital Health, Inc.** — *Oct 2025 – Present*
  SOC Analyst Intern — Tustin, CA, U.S
  - Monitored security alerts and telemetry using SIEM platforms (Splunk, Elastic).
  - Performed alert triage, investigation, and incident classification.
  - Analyzed endpoint, server, and network logs to detect suspicious activity.
  - Executed initial incident response actions and escalation based on SOC playbooks.
  - Built and tuned detection rules to reduce false positives
- **Bowling Green State University** — *Aug 2023 – May 2025*
  Graduate Research Assistant — Digital Forensics — Bowling Green, OH, U.S
  - Conducted forensic investigations on Windows and Linux system.
  - Analyzed logs, memory, and disk artifacts to reconstruct attack timelines.
  - Performed evidence collection and incident reconstruction.
  - Supported cybersecurity and incident response research.
- **Bowling Green State University** — *Aug 2023 – May 2025*
  Graduate Teaching Assistant — Bowling Green, OH, U.S
  - Led Linux and networking labs focused on system internals and traffic analysis.
  - Taught TCP/IP, routing, and packet inspection using Wireshark.
  - Mentored students on security and troubleshooting labs.
- **Hamravesh** — *September 2021 – July 2022*
  Technical Support Analyst — Tehran, Iran
  - Provided L2/L3 support for production systems and infrastructure.
  - Investigated incidents using logs, metrics, and monitoring tools.
  - Performed root cause analysis and incident resolution.
  - Implemented monitoring and alerting for operational issues.
- **Erst Host** — *Jun 2020 – July 2021*
  Systems Support Analyst — Tehran, Iran
  - Administered Windows and Linux servers (patching, hardening, maintenance).
  - Investigated system failures using logs and monitoring tools.
  - Automated routine administrative tasks using PowerShell and Bash.

TECHNICAL STACK

- **Security Operations:** SOC Monitoring, Alert Triage, Incident Investigation, Threat Detection, Log Analysis, Incident Response
- **SIEM & Detection:** Splunk, Elastic Stack, Detection Rules, Dashboards, IOC Analysis
- **Operating Systems:** Windows Server, Windows 10/11, Linux (Ubuntu)
- **Identity & Access:** Active Directory, Azure AD, GPO, MFA, RBAC
- **Networking:** TCP/IP, DNS, DHCP, VPN, Firewalls, Wireshark
- **Monitoring:** Windows Event Logs, Zabbix, Server Monitoring
- **Scripting:** PowerShell, Bash, Python
- **Cloud:** AWS (EC2, S3, IAM)
- **Soft Skills:** Clear incident communication, analytical thinking, structured documentation, teamwork in high-pressure environments, ability to explain security issues in simple terms