Adam Kim

Akim456@gmail.com | (347) 554-3119 | Long Island, NY |

WORK EXPERIENCE

Jovia Financial Credit Union **Jan. 2022 – Current**

Cybersecurity Architect (Promoted from Analyst 1, Analyst 2, Engineer 1, Engineer 2) *Westbury, NY*

SIEM

- Led the deployment of the Arctic Wolf Siem followed by a migration to CrowdStrike NG SIEM, serving as technical project lead for deployment, onboarding, tuning, and operationalization of the platform.
- Engineered and optimized security detections and controls across SIEM, EDR, NAC, and DLP platforms to reduce false positives and improve detection fidelity.
- Designed and implemented SOC workflows including SOAR (Fusion) automation, case management processes, alert routing, escalation procedures, and incident lifecycle management.
- Investigated and triaged security alerts and incidents, performing root cause analysis, evidence collection, and remediation coordination across endpoint, network, and cloud environments.
- Conducted proactive threat hunting using SIEM and endpoint telemetry to identify indicators of compromise and anomalous behavior patterns.
- Performed security investigations across Microsoft security platforms, including email message tracing, phishing analysis, DLP alerts, and policy enforcement using Microsoft Defender telemetry.

EDR

- Administered CrowdStrike Falcon EDR, including agent deployment, upgrades, configuration, and endpoint lifecycle management across enterprise environments.
- Executed endpoint-level security response actions including isolation, process containment, and account restrictions to mitigate active threats and support incident remediation efforts.
- Investigated endpoint telemetry and security alerts to support threat validation and incident response coordination across enterprise systems.

Firewall

- Monitored and analyzed firewall logs and network traffic to identify policy violations, unauthorized access attempts, and abnormal communication patterns.
- Reviewed, validated, and governed firewall rule changes and configuration commits to ensure alignment with security standards and operational requirements.
- Supported network security operations by analyzing traffic flows, NAT rules, security policies, and application visibility data to troubleshoot connectivity and access issues.

Zero Trust Initiatives

- Supported Zero Trust security architecture using Palo Alto Prisma Access and GlobalProtect to enforce secure remote access and identity-based connectivity controls across users and apps.
- Assisted in enforcing endpoint posture validation and conditional access policies to ensure compliant devices meet security requirements prior to network and application access.
- Administered Cisco ISE network access control and device profiling to classify endpoints and enforce segmentation and access control policies across the enterprise network.
- Supported identity-based access control using Microsoft Entra ID, monitoring authentication activity

and analyzing security logs to investigate suspicious sign-in behavior and enforce access policies.

Vulnerability Management

- Led implementation and operationalization of vulnerability scanning processes, including tool deployment, scheduling, and configuration.
- Coordinated and managed enterprise vulnerability scans, prioritizing findings based on risk and business impact.
- Presented vulnerability findings to technical teams and leadership, driving remediation and risk reduction to track remediation progress and security posture improvements.

Red Team Engagements

- Participated in internal red team exercises, including network penetration testing, vendor security assessments, and physical security evaluations across branch locations to identify security control gaps and attack paths.
- Supported external penetration testing engagements by coordinating scope, providing technical evidence, and assisting with remediation tracking in collaboration with third-party security consultants.
- Participated in red and purple team exercises focused on improving detection coverage and incident response readiness by identifying gaps through adversary simulation exercises.

Security Governance & Security Operations Enablement

- Managed enterprise audit and security assessment processes across NCUA and NY DFS 23 NYCRR 500 frameworks, including technical evidence collection, regulatory response, and remediation of security control gaps and compliance findings.
- Contributed to security awareness and culture initiatives through gamification programs, internal security communications, and educational content to improve employee engagement and reduce security risk exposure.
- Developed and maintained security operations documentation, including incident response runbooks, SOPs, and investigation playbooks to standardize response processes and ensure consistent incident handling across the organization.
- Supported internal and legal security investigations related to potential insider threats and policy violations by providing technical analysis and structured investigative evidence.
- Evaluated and validated security vendors and technologies to ensure alignment with enterprise security architecture, operational requirements, and risk management objectives.

CERTIFICATIONS

(ISC)^2 CISSP (949956)
ISACA CISM
SANS GIAC GMON
SANS GIAC GSOC
Azure SC-900
EC CEH
CompTIA CASP+/SecurityX
CompTIA CySA+
CompTIA Pentest+
CompTIA Security+
CompTIA Network+
CompTIA A+
CompTIA Project+

INTERESTS

Chess
CTFs
Home Automation
Gaming
Defcon

EDUCATION

Queens College **Dec, 2014**
BA Degree *MediaStudies*