KK

Kenneth King

Cybersecurity

Senior cybersecurity analyst with eight years across SaaS and e-commerce, focused on detection engineering, cloud security posture, and incident response. Comfortable owning a domain end to end, from log onboarding to executive briefings after a major event.

Contact Information

(512) 555-0173

elena.kovacs@example.com

Austin, TX 12345

Education

- B.S. in Information Systems Security, University of Texas at San Antonio, 2016
- GIAC Certified Incident Handler (GCIH), 2020
- GIAC Cloud Security Automation (GCSA), 2022
- AWS Certified Security - Specialty, 2023

Key Skills

- Detection engineering (Sigma, Panther, Splunk)
- Incident response and forensics
- AWS and GCP security architecture
- CSPM tooling (Wiz, Prisma Cloud)
- SIEM and data pipeline design on Snowflake
- Threat hunting and purple team operations
- IAM and identity threat detection (Okta, Azure AD)
- Vulnerability management (Rapid7 InsightVM, Tenable)
- Python and Terraform for security automation

Professional Experience

Senior Security Engineer | Marlowe Commerce Platform, Austin, TX
2021 - Present

- Rebuilt the detection pipeline in Panther on top of Snowflake, cutting mean time to detect from 47 minutes to 11 minutes for cloud control-plane events.
- Led response on an exposed IAM key incident, contained blast radius in under 90 minutes, and presented the root cause to the CTO and audit committee.
- Designed CSPM guardrails in Wiz that block public S3 buckets and overly permissive IAM roles before merge, used by 60+ engineering teams.
- Wrote 38 production Sigma-style detections covering OAuth abuse, GitHub token theft, and Okta session hijack patterns.
- Runs a quarterly purple team exercise with the offensive security vendor and tracks gaps to closure in Jira.

Security Analyst | Halcyon Travel Group, San Antonio, TX
2018 - 2021

- Owned phishing triage for 6,500 employees and built a Cofense-based reporting workflow that cut average review time roughly in half.
- Investigated a business email compromise targeting the finance team and helped recover a wire before settlement.
- Stood up the first vulnerability management program using Rapid7 InsightVM, with monthly reporting to IT leadership.
- Trained the help desk on initial credential-theft triage so the SOC stopped getting paged on routine resets.

Junior Security Analyst | Cypress Federal Credit Union, San Antonio, TX
2016 - 2018

- Worked a rotating SOC shift covering 2,400 endpoints and three branch networks.
- Tuned IPS signatures on Palo Alto firewalls and reduced noisy blocks affecting member-facing banking apps.
- Supported quarterly PCI scans and remediation tracking with the infrastructure team.

- MITRE ATT&CK mapping and detection coverage
- Executive and audit committee reporting
- SOC 2 and PCI DSS compliance