COLIN KELLY

CONTACT

Cottonwood Heights, Utah, United States

484-238-2595

cfkelly18@gmail.com

cybercareerschool.com

www.linkedin.com/in/colin-f-kelly

https://www.youtube.com/c/cybercareerschool

TECHNICAL SKILLS

Blockchain: (Learning)
CosmWasm, Cosmos SDK, Terra, DeFi Power User

Cloud Security:
AWS, Azure, GCP, and Kubernetes

DevSecOps:
AWS, Git, Ansible, Terraform, Jira, CI/CD, MS Flow, Docker, API development/ implementation, and code review

AWS Development:
AWS Lambda, CloudFormation, API Gateway, IAM, System Manager, EC2, S3, Organizations, CLI and CloudFront

Red Teaming:
Cobalt Strike, Burp Suite, Nmap, Metasploit, and Kali Linux

Purple Teaming:
MITRE ATT&CK, Vectr, and Rule Review/Tuning

PROFESSIONAL SUMMARY

Accomplished Cyber Security Professional, Cloud Security Engineer, Purple Team Operator, & DevSecOps Engineer with over three years of proven experience in security the public cloud, performing purple team assessments, and architecting both attacker and defender automations and infrastructure. Looking to break into the world of Blockchain security and prevent the cybersecurity attacks of the future.

CAREER HIGHLIGHTS

Cloud Security Engineer:
Developed and researched security policies and best practices for securing customer's AWS, Azure, GCP, and Kubernetes environments. Developed intricate knowledge and understanding of the services provided in the public cloud and their common security misconfigurations and indicators of attack. Experienced in reviewing and testing IaC for security misconfigurations.

DevSecOps Engineer:
Software development experience spanning Solution Architecture, DevOps, Security, Big Data, hands-on application troubleshooting in enterprise environments, and Amazon Web Services (AWS) for multiple production workloads.

Experienced Purple Team Operator:
Leading and managing Purple Team exercises for multiple clients, performing specialized campaigns to mimic APT groups and threats to specific industries, and performing client updates and reports to managerial and C-level audiences.

WORK EXPIERENCE

Cloud Security Engineer II - CrowdStrike — May 2021 - Present

Cloud Security Engineering

- Researched and developed security policies for CSPM tool Falcon Horizon. Worked on a team of engineers who were responsible for the creation of IOA (Indicator of Attack) and IOM (Indicator of Misconfiguration) for securing customers public cloud environments (AWS, GCP, Azure, and Kubernetes)
- (In-Progress) Major Initiative lead and sole developer behind IaC (Infrastructure as Code) tool. Designing and developing a tool capable of detecting and eliminating misconfigurations in CloudFormation and Terraform templates before deployment.

Security Consultant – Security Risk Advisors — July 2019 – April 2021

DevSecOps

- Designed and developed the artifact collection tool/pipeline for the stable and safe collection of malicious artifacts from client environments to Amazon S3 with easy and safe retrieval into a malware analysis VM for analysis and automated YARA rule detection upon uploading.
- Developed custom AWS engineering solutions to address client needs.
- Designed and developed Jira workflows and automations for both purple team and incident response/malware analysis projects.
- Designed and developed a threat intelligence workflow to expedite threat bulletin delivery to clients.
- Developed big data scripts to facilitate incident response and e-discovery efforts.
- Assisted with the implementation of AWS Control Tower to manage and deploy custom AWS accounts for client engagements.

Purple Team Lead

- Performed quarterly purple teams for multiple Fortune 10/100 companies as the lead red team operator. Working closely with blue team members to develop strategies and rules to improve the security posture of the client.
- Performed specialty purple team exercises for clients ranging from APT simulation to toolset bake-offs.
- Developed purple team test cases based on the MITRE ATT&CK Matrix. Helped clients implement changes to improve their security posture.
- Fully trained three purple team operators to perform assessments autonomously.
- Performed red team attack simulations against external customer networks. Established persistence on internal networks for goal-oriented results and provided value by identifying detailed attack chains that could be utilized by real attackers.
- Led a weekly series of Lunch and Learns to teach Red Team Attacks to junior analysts.

CyberSOC Consultant - Co-Op – Security Risk Advisors Jan 2019 – July 2019

SOC Analyst

- Worked with Fortune 10/100 companies as a key SOC analyst, triaging incidents, and developing documentation, Standard Operating Procedures, Incident Runbooks. Experienced working with many SIEM, EDR, DLP, and SOAR solutions from various vendors (Splunk, QRadar, CrowdStrike, Cylance, Carbon Black, SentinelOne, McAfee, Symantec, and Phantom).
- Contributed to internal tool development (Python, PowerShell, Bash, MSFlow) for process and analysis automation.

Security Operations Intern - Thomson Reuters May 2018 – July 2018

- Performed security operations for a global organization. Triaging incidents, developing documentation, gained exposure to SIEM, EDR, and DLP platforms.
- Designed and developed a Capture the Flag using Splunk to teach SOC analysts Splunk processing language (SPL) and threat hunting.
- Assisted and observed the Security Operations Team in digital forensics and incident response.

EDUCATION HISTORY

The Pennsylvania State University | University Park, Pennsylvania June 2016-May 2020

College of Information Sciences and Technology

Bachelor of Science: Security and Risk Analysis - Information and Cyber Security

• **GPA:** 3.7 Cumulative

• **Dean's List**: Spring '17,'18, '20 and Fall '17,'18

• **Relevant Coursework**: Computer Forensics, Network Security, Machine Learning, Python, Java, Database, Networking, Fraud Informatics, and Risk Analysis

CERTIFICATIONS

- GIAC Defending Advanced Threats (GDAT)
- CompTIA CySA+
- CompTIA Security+

LANGUAGES

- Python
- Bash
- PowerShell
- Sleep
- YARA
- SPL
- YAML
- PostgreSQL

PROJECTS

Cyber Career School

Cyber Career School is a platform dedicated to preparing aspiring cyber security professionals for a career in cyber security. Created in 2018, my goal was to provide my advice and experience to help my audience achieve their dream careers. 20,000+ monthly viewers between CyberCareerSchool.com and my YouTube channel (10,000+ subscribers) utilize my free content ranging from certification prep to career advice.

Blog: CyberCareerSchool.com

YouTube: https://www.youtube.com/c/cybercareerschool