Maya Douglas

425-655-9312 | mayadouglas1101@gmail.com

Statement

Security analyst with Microsoft training and 2+ years of cybersecurity experience specializing in security assessments, risk analysis, and operational security in cloud-based environments. Focused on organizational maturity through process definition and standardization. Security+ and eJPT certified.

Technical Skills

Security Operations: SIEM log analysis, DFIR, triaging, severity assessment, attack categorization, incident scoping, timeline reconstruction.
Vulnerability Management: Vulnerability assessment and prioritization, asset inventory and exposure analysis, CVE and severity scoring (CVSS); remediation planning, risk acceptance, exception handling, and documentation.
Governance and Security Assessments: NIST CSF 2.0, cyber insurance auditing, policy development and documentation, change management.
Spoken Languages: English, Japanese (Fluent), Mandarin (Basic)

Experience

Cybersecurity Analyst 12/02/2024 - Present
RedShift Technologies *Littleton, CO*

- Authored and operationalized the organization's first incident response plan, reducing time to containment to around 5 minutes from 10.
- Owned triage, severity classification, containment, and investigation for over 300 security alerts using Todyl's SIEM, containing attacks promptly.
- Led analysis of similar TTPs across tenant environments and provided recommendations for email security improvements to stakeholders.
- Performed security assessments across multiple tenants aligned to NIST CSF 2.0, HIPAA, and PCI DSS to support regulatory and cyber-insurance requirements.
- Established our vulnerability management program using ConnectSecure, prioritizing fixes using CVSS scores and relative risk.

Network Engineer 02/01/2024 - 08/09/2024
Microsoft (Contract) *Bellevue, WA*

- Contracted through LTIMindtree to troubleshoot and respond to critical networking issues on Azure infrastructure, reducing downtime and revenue loss for internal and external users.
- Investigated a critical insider threat faced by a customer on Azure CDN, and delivered the news to a non-technical executive.
- Parsed Azure cloud telemetry using Kusto Query Language (KQL) to determine whether activity was malicious or benign.

Vulnerability Tester 05/15/2023 - 11/23/2023
Mycos Technologies (Contract) *Remote*

- Conducted authorized assessments to identify vulnerabilities using Metasploit in test environments.
- Spearheaded internal cybersecurity policies that formalized secure software development processes.
- Worked with the DevOps team to incorporate security checks in their CI/CD pipeline using GitLab's built-in feature.

Software Development Intern 05/23/2022 - 08/10/2022
Travelport *Centennial, CO*

- Automated a CI/CD pipeline to test coverage and tech debt using SonarQube, streamlining quality control.
- Cross-referenced with large SQL databases to keep track of data for travel booking providers.
- Created end-to-end processing for an internal tool via JSON RESTful API, used by the majority of employees today.

Education

University of Colorado Boulder 08/21/2019 – 05/11/2023
Bachelor's in Computer Science *Boulder, Colorado*

Projects and Certifications

Certifications 12/02/2025 - Present

- CompTIA Security+.
- eJPT - eLearning Junior Penetration Tester.

Security Research and Detection Lab 02/01/2025 - Present

- Created VLAN segmentation rules to prevent lateral movement and test endpoint alerts.
- Conducted open-source research focused on identifying behavioral patterns of attackers, leveraging publicly available data from online platforms, forums, and public records, including Google Dorks.

Hack The Box Labs 10/15/2025 - Present

- Analyzed attacker tradecraft by simulating them on Hack The Box, including SMB/HTTP enumeration, SQLi, LFI/RFI exploitation, reverse shells, Windows/Linux privilege escalation, and Active Directory footholds.
- Completed 22 machines and earned 2 badges.

Professional Development 08/10/2023 - Present

- DEF CON (blue-team / detection-focused content)
- WiCyS Colorado (technical workshops, panels)
- DenverSec (regular SOC-focused meetups)
- Girl Security (mentee)