Cassidy "Cazz" Veney

ENTRY-LEVEL CYBERSECURITY ANALYST | SOC / BLUE TEAM | CLOUD SECURITY

Baltimore, MD| caven5@morgan.edu| 703-712-6836 | LinkedIn | Portfolio

SUMMARY

Entry-level Cybersecurity Analyst with hands-on experience in SIEM log triage, Windows event analysis, phishing investigations, threat intelligence, and cloud security labs. Demonstrated ability to map activity to MITRE ATT&CK and document SOC-ready findings.

SKILLS

Security Operations: SIEM Log Triage, Alert Investigation, Incident Analysis, Phishing Detection, Threat Intelligence, MITRE ATT&CK, Brute-Force Detection

Tools: Splunk, Windows Event Viewer, VirusTotal, Google Cloud Platform, Terraform, Google Cloud KMS

Logs & Data: Windows Security Logs (4625, 4688, 6005/6006), SSH Logs, JSON Datasets

Cloud & Infrastructure: Firewall Rules, VPCs, IAM Concepts, Encryption, Infrastructure as Code

PROJECTS

Lazarus Group – Threat Intelligence Report (Link)

• Analyzed Lazarus Group (G0032) campaigns using MITRE ATT&CK tactics, including Initial Access and Credential Access.

• Investigated major attacks, including Sony Pictures, WannaCry ransomware, and cryptocurrency heists, to identify common techniques.

• Produced defensive recommendations such as EDR adoption, MFA enforcement, and phishing awareness based on findings.

Windows Event Log Deep Dive – SIEM Analysis (Link)

• Analyzed Windows Security and System logs, focusing on Event IDs 4625, 4688, 6005, and 6006.

• Generated failed login activity to validate authentication logging and detection visibility.

• Correlated user and system events to distinguish normal behavior from suspicious activity.

SIEM Log Triage – Alert Investigation & MITRE Mapping (Link)

• Ingested security logs into Splunk to simulate SOC-style alert triage.

• Identified failed logins and suspicious patterns using SPL queries.

• Visualized abnormal activity in dashboards and documented findings mapped to MITRE ATT&CK.

Phishing Email Investigation (Link)

• Analyzed a phishing email using header inspection and VirusTotal enrichment.

• Identified spoofed sender domains and malicious URLs indicating credential-harvesting intent.

• Documented mitigation steps and user-awareness actions to reduce future risk.

Brute Force Attack Investigation – SOC Project (Link)

• Analyzed SSH brute-force datasets containing usernames, passwords, timestamps, and foreign IP addresses.

• Identified automated attacks targeting the root account through repeated authentication failures.

• Recommended MFA, account lockout policies, and IP blocking to mitigate attack vectors.

Terraform Cloud Firewall Project (Link)

• Deployed a custom VPC and firewall rules in Google Cloud using Terraform.

• Analyzed allowed ICMP and TCP traffic on ports 80, 8080, and 1000–2000 to assess exposure.

• Provisioned cloud resources using Infrastructure as Code to enforce consistent security controls.

Google Cloud Key Management Lab (Link)

• Implemented a symmetric encryption key with a 90-day rotation policy.

• Generated and analyzed an asymmetric key pair for encryption and signing use cases.

• Applied cloud key management practices to support data protection requirements.

EDUCATION

• B.S. Cybersecurity Intelligence Management — Expected May 2027

• Morgan State University | GPA: 4.0

CERTIFICATIONS

Google Cloud Cybersecurity

Microsoft Cybersecurity Analyst

Palo Alto Networks Cybersecurity

CompTIA Security+ (In Progress)