GARRETT MORGAN

CYBERSECURITY ANALYST

Anna, TX 75409, (843) 986-7266, garrett.morgan.pro@gmail.com, linkedin.com/in/garrett-morgan4

SUMMARY

Cybersecurity professional with 3+ years across security operations, incident response, and Governance, Risk, and Compliance (GRC). Experienced in SIEM-based security monitoring, threat detection, vulnerability management, and risk assessment aligned to NIST, ISO 27001, PCI DSS, and SOC frameworks. Skilled at triaging and escalating security incidents, evaluating IT general and application controls, monitoring program risk, and communicating findings and remediation guidance to cross-functional stakeholders and leadership. ISACA CISA (passed 2025) and CISSP candidate (exam June 2026).

SKILLS

Security Operations: Security Monitoring, Incident Response, Incident Triage and Escalation, Threat Detection, Threat Intelligence, Threat Hunting, Security Awareness Training
Vulnerability and Detection: SIEM (Wazuh), Intrusion Detection Systems (IDS), Vulnerability Management, Vulnerability Scanning and Assessment, Log Analysis and Alerting, Kibana
Governance, Risk and Compliance: Risk Assessment, Risk Mitigation, Program Risk Monitoring, IT General and Application Controls, NIST, ISO 27001, ISO 42001, PCI DSS, SOC 1 and SOC 2, HITRUST
Identity, Privacy and Data Protection: Identity and Access Management (IAM), Active Directory, Data Protection, Privacy Controls, GDPR, CCPA
Cloud, Systems and Scripting: AWS, Azure, Linux, VMware ESXi, Python, PowerShell, REST APIs
Professional Skills: Agile, Analytical Thinking, Written and Verbal Communication, Adaptability, Creativity, Accuracy, Cross-Functional Collaboration, Stakeholder Management, Technical Documentation

WORK EXPERIENCE

Senior Audit Consultant

AARC-360, Anna, TX (Remote), 07/2023 - Present

- Conduct IT security audits and risk assessments across 6 security and privacy frameworks (SOC 1, SOC 2, PCI DSS, HITRUST, ISO 27001, and ISO 42001), evaluating IT general controls, application controls, and security processes.
- Identify control gaps and cybersecurity risks, then develop and recommend risk mitigation strategies that strengthen client compliance posture, governance, and overall security culture.
- Present findings, risks, and remediation roadmaps to client leadership, translating complex technical issues into clear guidance for non-technical stakeholders.
- Lead 3+ concurrent client engagements in a senior capacity, overseeing teams, reviewing workpapers, and mentoring staff consultants to ensure accurate and timely deliverables.
- Contributed to a unified one-test, multi-audit methodology that reduced duplicate control testing across overlapping compliance audits and improved engagement efficiency.

Triage Security Analyst

Arctic Wolf, Pleasant Grove, UT, 01/2023 - 07/2023

- Performed active security monitoring and triaged 500+ daily security alerts within a 24/7 SOC environment, applying playbook-driven analysis to detect, investigate, and escalate potential threats.
- Supported incident response activities, including the identification, containment, and escalation of security incidents across diverse customer environments.
- Developed and refined runbooks that streamlined incident response, improved threat detection workflows, and strengthened team knowledge management.
- Diagnosed and resolved 100+ technical issues involving security sensors and vulnerability scanners, ensuring continuous monitoring coverage and operational reliability.

Student Systems Engineer

Brigham Young University, Provo, UT, 02/2022 - 01/2023

- Administered VMware ESXi and vCenter environments supporting 200+ virtual machines, and resolved hardware, connectivity, and network switch issues across Dell MX chassis and blade servers to improve stability and uptime.

PROJECTS

Wazuh SIEM Deployment and Log Monitoring (Home Lab)

- Deployed and configured Wazuh SIEM on Ubuntu Linux for centralized log monitoring, threat detection, and real-time alerting.
- Installed endpoint agents to collect logs, detect anomalies, and validate rule-based detection alerts.
- Built custom Kibana dashboards for security event visualization, correlation, and analysis.

EDUCATION

Bachelor of Science in Cybersecurity, Brigham Young University, Provo, UT

CERTIFICATIONS

CISSP (ISC2) - Candidate, exam June 2026 **ISACA CISA** - Passed 2025, pending **CompTIA Network+** - 2024