Gabriel Carbaugh

Phone: 972-861-0233 | Email: gabedc216@gmail.com | Location: Arlington, TX

Professional Summary:

CISSP-certified Security Engineer and customer-facing technical advisor with 7+ years of experience helping enterprise organizations deploy, secure, and optimize cloud, endpoint, and SIEM platforms. Experienced in presenting technical solutions to stakeholders, leading security investigations, developing automation, and translating complex security challenges into actionable business outcomes.

Education:

MS in Cyber Security and Assurance / Western Governors University	May 2025 - Apr 2026
BS in Cyber Security and Assurance / Western Governors University	Dec 2019 - Aug 2024
Assistant Network Technician (Vocational)/ Southern Oklahoma Technology Center	Aug 2014 - May 2016

Skills:

Identity & Security: Azure Entra ID, IAM, RBAC, SSO, SAML, MFA, Identity Governance, Least Privilege, PKI, TLS, X.509, XDR/EDR, SIEM/SOAR, Threat Hunting, Zero Trust

Cloud & Infrastructure: AWS (IAM, EC2, VPC, S3, CloudTrail, Security Groups), Terraform, Ansible, Python, Kubernetes, Elastic, Kibana, NIST CSF/800-53, API Security (AuthN/AuthZ), Threat Modeling (STRIDE), Network Security

Certifications:

Certified Information Systems Security Professional (CISSP)	Jun 01, 2025 - May 31, 2028
Systems Security Certified Practitioner (SSCP)	Feb 21, 2021 – May 16, 2030
CompTIA CySA+	Jan 1, 2024 - Dec 31, 2026
CompTIA PenTest+	May 16, 2024 – May 16, 2030
CompTIA Project+	Jan 05, 2024 - NA
CompTIA Security+	Feb 21, 2021 - May 16, 2030
CompTIA Network+	Nov 25, 2020 - May 16, 2030
LPI Linux Essentials	Aug 23, 2023 - NA
AWS Certified Solutions Architect – Associate (Expired)	Dec 16, 2022 – Dec 16, 2025

Work Experience:

TrendAI **Feb 2022 – Present**

DevOps Platform Engineer - Security Operations Lead (Feb 2024 – Present) | Customer Support Engineer (Aug 2022 – Jan 2024)

- Advised enterprise customers on threat detection strategies by analyzing cloud and endpoint telemetry and translating findings into actionable security improvements.
- Supported Azure Entra ID SSO deployments by configuring identity federation, SAML authentication, role mappings, and secure access controls.
- Investigated endpoint and cloud security telemetry to identify unauthorized activity, lead incident investigations, perform threat hunting, and provide risk-based remediation recommendations.
- Collaborated with enterprise customers to implement and tune XDR, EDR, and anti-malware security controls, improving threat visibility, maximizing platform performance, and reducing security risk across Windows and Linux environments.
- Supported SIEM/SOAR integrations and API-driven security workflows, aligning Trend Vision One capabilities with customer SOC operations.
- Served as primary point of contact for enterprise customers, resolving endpoint and workload security issues across Linux and Windows systems while maintaining a 4.8/5 CSAT.
- • Led post-penetration test remediation by prioritizing security findings, developing custom detection rules, validating mitigations, and communicating remediation progress to enterprise stakeholders.
- Discovered and resolved a Kubernetes authentication handling issue that improved operational visibility and failure reporting.

National HME **May 2019 – Aug 2022**

Systems Administrator (Jul 2021 – Aug 2022) | IT Support Specialist (May 2019 – Jul 2021)

- Automated AWS disaster recovery infrastructure deployments using Terraform and streamlined server configuration with Ansible, reducing manual provisioning time and improving deployment consistency.
- Reduced risk exposure by refining Azure Entra ID IAM configurations, implementing RBAC through security groups, enforcing least-privilege access, and strengthening identity governance across enterprise systems.
- Automated onboarding/offboarding workflows and IAM controls aligned with NIST best practices, improving governance and audit readiness.
- Configured secure network infrastructure, including AWS-to-Palo Alto VPNs and Juniper VLAN segmentation to reduce lateral movement risk.
- Led migration from MPLS to secure broadband connectivity, implementing network segmentation and firewall controls, reducing network operating costs by approximately 30%.
- Enhanced business continuity and disaster recovery capabilities through infrastructure automation, security improvements, and operational resilience initiatives.

First Rate | *Systems Technician I* **May 2018 – May 2019**

- Provided endpoint and systems support within a financial services technology firm specializing in wealth management reporting platforms, maintaining secure configurations in a compliance-driven environment, and supporting financial data integrity.
- Assisted with user account administration, access provisioning, and endpoint support activities within a regulated financial services environment, ensuring adherence to security and compliance requirements.