# Anthony Castleberry

## Systems & Cloud Administrator

AnthonyCastleberry.IT@gmail.com • 248-403-6557 • Metro Detroit, MI

linkedin.com/in/anthony-castleberry-it • anthonytechblog.com • github.com/ancascyber

## PROFESSIONAL SUMMARY

Systems Administrator and Cloud Engineer with 10+ years supporting enterprise Windows and Linux infrastructure across Azure, AWS, and hybrid environments. Experienced in Microsoft Intune, Entra ID, Active Directory, Terraform, PowerShell, Microsoft Sentinel, Azure Monitor, CI/CD automation, and infrastructure as code. Proven success designing, deploying, and securing scalable systems, from enterprise Active Directory environments to serverless cloud APIs, Kubernetes homelab, and automated security pipelines.

## PROFESSIONAL EXPERIENCE

### Antsys Technologies LLC

*Independent Cloud Engineer* *Jan 2026 – Current*

*Cloud Infrastructure, Security & Automation Projects | GitHub: github.com/ancascyber*

#### Cloud & Serverless

- Designed and deployed production-grade serverless applications on Microsoft Azure using Azure Functions, Python, API Management, Application Insights, and Terraform, implementing Infrastructure as Code (IaC) for repeatable cloud deployments.
- Developed REST APIs using Azure AI Language to automate sentiment analysis, alongside an inventory lookup workflow, replacing manual processes with scalable, on-demand cloud services.
- Provisioned and managed Azure cloud infrastructure using Terraform, enabling version-controlled, consistent, and repeatable infrastructure deployments.
- Brought existing AWS S3 static site infrastructure under Terraform management using config-driven import, verifying live configuration against console settings to achieve a zero-change plan on the first run.
- Built a custom Docker container image and deployed it to AWS Elastic Beanstalk, reusing existing IAM roles and resolving container networking conflicts.
- Hosted a personal technical portfolio as a static website on AWS S3 with Route 53 DNS resolution.

#### Automation & CI/CD

- Built automated CI/CD pipelines with GitHub Actions to deploy AWS applications, streamlining release workflows and reducing manual deployment effort.
- Designed a container security CI/CD pipeline using GitHub Actions and Trivy, implementing a blocking vulnerability gate for CRITICAL/HIGH findings alongside a non-blocking full report, and publishing scanned images to GitHub Container Registry.
- Published complete project documentation and source code on GitHub, demonstrating cloud architecture, Infrastructure as Code, serverless development, and DevOps best practices.

#### Identity & Endpoint Management

- Automated Windows endpoint compliance and administrative tasks using PowerShell, Microsoft Intune, and Entra ID.
- Built a 10-phase Intune endpoint compliance and configuration baseline, combining MDM enrollment, Settings Catalog profiles, Graph API PowerShell reporting, and a Log Analytics ingestion pipeline (DCE/DCR) with KQL alerting on non-compliant devices.
- Built and configured an Active Directory environment from scratch, including organizational units, department-scoped Group Policy (password complexity, inactivity lockout, USB deny-all), and automated user provisioning with PowerShell.
- Found and fixed a security flaw in the account setup script that was storing passwords in plain text, replacing it with a secure prompt and forced password reset.
- Deployed an Entra ID-joined Azure Virtual Desktop (AVD) environment with FSLogix profile containers, a host pool, application group, and workspace configuration.

#### Security & Monitoring

- Implemented centralized security event collection using Microsoft Sentinel and Windows Event Forwarding to improve incident detection and response.
- Deployed an intentionally exposed honeypot VM integrated with Microsoft Sentinel, capturing 16,000+ failed RDP login attempts in 24 hours and building a live Sentinel workbook to visualize attacker geolocation.

- Simulated a brute-force credential attack against an Active Directory domain controller using Kali Linux and Crowbar, validating detection in Splunk and extending coverage with MITRE ATT&CK technique simulation via Atomic Red Team.
- Built centralized monitoring and alerting with Prometheus, Grafana, Alertmanager, and Azure Monitor for Windows, Linux, and NAS systems, with Slack notification routing.

### AI & Containers

- Deployed a self-hosted LLM inference stack using Ollama, Docker, and Open WebUI on CPU-only hardware, enabling private AI workloads with full data sovereignty and zero per-token inference costs.
- Migrated a Docker Compose LLM inference stack to a two-node kubeadm Kubernetes cluster, deploying Ollama and Open WebUI as NodePort services with persistent storage.

**Career Break** *February 2024 – January 2026*

Served as primary family caregiver while acting as court-appointed probate executor responsible for administering three family estates.

**Tungsten Automation**

*Business Development Manager* *August 2022 – February 2024*

- Streamlined Salesforce workflows and standardized contract templates, reducing Statement of Work turnaround time by approximately 60%.

*Professional Services Consultant – Enterprise Infrastructure Administration* *January 2012 – August 2022*

- Served as North America technical lead for Ernst & Young's enterprise cost recovery deployment, configuring 500+ Windows servers, integrating with EY's enterprise Active Directory, and deploying 8,500+ print/scan endpoints supporting 100,000+ users.
- Led remote technical implementation for enterprise client deployments, configuring servers and endpoints, integrating with client Active Directory and hybrid Azure AD environments, and directing onsite crews, vendors, and client IT teams through installation and go-live.
- Administered Windows Server, Active Directory, SQL Server, backups, patching, and infrastructure troubleshooting across enterprise client environments.
- Built PowerShell scripts to automate SQL Server provisioning for enterprise deployments, creating service accounts, application databases, and db_owner permission assignments, accelerating installations and reducing configuration errors.
- Produced technical documentation and client training materials supporting enterprise infrastructure deployments.

**General Motors – OnStar Advanced Systems Development**

*Desktop Support & Active Directory Administrator* *October 2010 – December 2011*

- Managed Active Directory user accounts, security groups, and Group Policy supporting over 500 users.
- Provided desktop support and participated in a 24×7 Linux server on-call rotation supporting production OnStar infrastructure.

## EDUCATION

**Capella University – Minneapolis, MN**
Bachelor of Science – Information Technology

**Global Information Technology – Lathrup Village, MI**
Information Technology Fundamentals

## TECHNICAL SKILLS

**Cloud:** Azure • AWS • Azure Monitor • Azure CLI • Azure Functions • API Management • Azure Virtual Desktop
**Identity & Endpoint Management:** Active Directory • Microsoft Intune • Entra ID • Group Policy
**Systems:** Windows Server • Linux • Ubuntu • VMware • SQL Server
**Automation & CI/CD:** Terraform • PowerShell • Bash • Python • Git • GitHub Actions

**Containers & Orchestration:** Docker • Docker Compose • Kubernetes • Ollama • Open WebUI
**AI & Machine Learning:** Azure AI Language • Local LLM Inference (Ollama, Open WebUI)
**Monitoring & Security:** Microsoft Sentinel • Splunk • Prometheus • Grafana • Alertmanager • Windows Event Forwarding • Trivy

## CERTIFICATIONS

- AWS Certified Cloud Practitioner
- AWS Certified Solutions Architect – Associate
- Microsoft Certified: Azure Fundamentals
- Microsoft Certified: Azure AI Fundamentals
- CompTIA A+ Certification
- CompTIA Network+ Certification
- CompTIA IT Operations Specialist
- CompTIA Security+ Certification
- CompTIA Secure Infrastructure Specialist