Edward Griggs

edwardjgriggs@gmail.com | linkedin.com/in/edward-griggs | edwardgriggs.com | github.com/edwardjgriggs | Hampton, VA

PROFESSIONAL SUMMARY

Systems administrator with 5+ years building and hardening infrastructure for federal contractor and nonprofit environments. Earned CompTIA Security+ (2026) and Google Cybersecurity Certificate while running production M365 tenants, automating IT operations, and deploying AI integrations. Built hands-on detection infrastructure outside the day job: SSH hardening with fail2ban, host firewalls, systemd service isolation, VLAN segmentation for IoT devices, and centralized log alerting. Reduced attack surface across 30+ endpoints through a structured hardening initiative; cut repeat support tickets ~40% by deploying internal AI agents. Now moving into detection engineering and AI engineering full-time -- where systems thinking, security instincts, and automation experience compound into real organizational impact.

CORE COMPETENCIES

Endpoint Hardening & Detection | Log Analysis & Alerting | M365 Security Administration | Linux System Security | Network Segmentation (VLAN/Firewall) | AI Integration & Automation | NIST SP 800-171 Compliance | Incident Detection & Response

WORK EXPERIENCE

Aalis Management Consulting

Jul 2023 -- Present

Systems Administrator -- Alexandria, VA (Remote)

- Audited and remediated endpoint configurations across **30+ machines**, reducing attack surface and driving NIST SP 800-171 alignment; supported successful ISO 9001 certification.
- Deployed internal AI agents for common IT requests, cutting repeat support tickets by **~40%**; authored company-wide AI policy covering security, compliance, and ethical use.
- Automated offer letter generation and routing workflows, reducing HR processing time by **~80%**; also automated onboarding/offboarding account setup and role-based access provisioning.
- Built the IT function from scratch for a growing small business -- established policies, procedures, helpdesk workflows, and M365 governance for a two-person team.
- Administered full Microsoft 365 ecosystem: account provisioning, group policies, Exchange Online, Teams, SharePoint, MFA enforcement, and DLP configurations.
- Designed and launched "Aalis Connect," a SharePoint-based intranet centralizing knowledge sharing and organizational communication.

NewView Oklahoma

Nov 2024 -- Apr 2026

Contract Closeout Specialist -- Remote [contract ended]

- Managed federal contract documentation and closeout processes in compliance with FAR and internal standards.
- Maintained accurate records under audit-ready conditions; assigned additional responsibilities due to consistent, accurate performance.

Planting Hope Global

Dec 2020 -- Jul 2023

Web & IT Support Specialist -- Remote

- Provided IT support across hardware, software, networking, and accounts for a distributed remote team.
- Maintained WordPress site, hosting, backups, and access controls; integrated analytics and communication tools (Mailchimp).
- Documented systems, configurations, and processes to support continuity and onboarding.

SECURITY PROJECTS

Raspberry Pi 5 -- Hardened Linux Detection Node Home Lab

Built and hardened a Linux node with layered host security controls: SSH hardening (public-key only, root disabled), fail2ban rate limiting, UFW default-deny firewall policy, systemd unit isolation (ProtectSystem, NoNewPrivileges, CapabilityBoundingSet), and automated patch windows via systemd timers. Centralized log review and alerting for authentication events and service failures.

Linux · SSH hardening · fail2ban · UFW · systemd · log alerting

Docker / n8n -- Containerized Automation Platform Home Lab

Deployed a containerized automation VPS with secure-by-default configuration: automatic TLS termination via reverse proxy (no plaintext traffic), credentials isolated via .env with restricted file permissions, SSH hardening on host, Docker network segmentation (reverse proxy is the only externally reachable container), and structured container log collection for operational visibility.

Docker · Caddy/Nginx · n8n · Ubuntu VPS · network segmentation

Home Assistant -- IoT VLAN Segmentation Home Lab

Segmented IoT devices into an isolated VLAN to limit lateral movement: separate SSID, firewall ACLs blocking east-west traffic into the trusted LAN, local-only Home Assistant (no cloud relay), Zigbee CVE evaluation before procurement, and IoT event logging forwarded to a central log store.

VLAN · firewall ACLs · Home Assistant · Zigbee · log forwarding

EDUCATION

Bachelor of Arts, Fine Arts May 2019

University of Virginia's College at Wise -- Wise, VA | GPA 3.2

CERTIFICATIONS

CompTIA Security+ Jan 2026 [verify]

Google Cybersecurity Certificate 2025

SKILLS

Security: NIST 800-171, ISO 9001, endpoint hardening, access controls, firewall policy, log analysis

Cloud & Identity: Microsoft 365, Entra ID, Exchange Online, SharePoint, Teams, MFA, DLP

Linux & Infra: Ubuntu, Raspberry Pi, systemd, SSH hardening, UFW, fail2ban, Docker, VLAN

AI & Automation: AI agent deployment, workflow automation, n8n, AI policy development

Development: Next.js, TypeScript, React, HTML, CSS, WordPress, SharePoint dev

Compliance & Docs: FAR, IT policy authoring, process documentation, knowledge base management