Paden C. Gillispie

Macomb, IL area | gillpad.dev | linkedin.com/in/paden-gillispie/ | github.com/pgill-dev

Infrastructure Security Engineer with experience designing secure enterprise platforms through virtualization, automation, Kubernetes, and Zero Trust architecture. Demonstrated success modernizing infrastructure, leading virtualization initiatives, implementing CIS/STIG security baselines, developing internal tooling, and automating operational workflows using Python and Ansible. Passionate about engineering resilient platforms that are secure by design through automation, infrastructure as code, and operational excellence. Combines military leadership with hands-on engineering to deliver secure, maintainable platforms. Experienced across on-premises and hybrid infrastructure environments with a previously held TS/SCI clearance.

Certifications

- CompTIA CASP+ (SecX) | August 2023
- CompTIA Security+ | July 2023
- CompTIA A+ | March 2024
- CompTIA Network+ | June 2025
- CompTIA CySA+ | August 2025
- CompTIA Project+ | August 2025
- ISC2 SSCP | August 2025
- ITIL v4 Foundations | November 2025

Skills

- **Infrastructure & Platforms**: Proxmox VE, VMware/vCenter, Kubernetes, Ceph, Docker
- **Security & Compliance**: ACAS/Tenable.SC, STIGs, SCAP, Nessus, Rapid7, CIS Benchmarks, Zero Trust
- **Automation & DevOps:** Python, Flask, Ansible, Bash, PowerShell, Git, FastAPI, REST APIs
- **Systems & Networking**: Windows Server, Linux (RHEL, Debian, Ubuntu, Alma, Rocky), AD/GPO, DNS/DHCP, VLANs, VPNs, ACLs

Education

- Bachelor of Science (B.S.), Cybersecurity and Information Assurance, Western Governors University – Expected November 2026
- ACAS Operator and Supervisor Course

Projects

Zero Trust Infrastructure Engineering Lab

- Architected a Proxmox-based enterprise virtualization environment supporting clustered infrastructure, segmented networking, and hybrid management workflows.
- Deployed and managed Talos-based Kubernetes environments with Ceph-backed storage, ingress routing, monitoring, and infrastructure observability.
- Implemented Prometheus and Grafana monitoring stacks to improve infrastructure visibility, alerting, and operational troubleshooting.
- Configured Zero Trust-aligned remote access solutions using Cloudflare Access, Guacamole, and identity-based access controls.
- Automated infrastructure validation, reporting, and operational workflows using Python, Bash, and Ansible.

Security Engineering & Compliance Automation

- Developed automation workflows for STIG validation, remediation tracking, and enterprise compliance support across Windows and Linux systems.
- Performed vulnerability analysis and remediation using ACAS/Nessus/Rapid7 findings, RMF-aligned processes, and DISA STIG/CIS Benchmark requirements.
- Built operational documentation, remediation procedures, and infrastructure reporting processes supporting enterprise security operations.
- Implemented baseline hardening, certificate management, and access-control enforcement across virtualized and hybrid infrastructure environments.
- Built repeatable validation and documentation processes.

Engineering Portfolio

gillpad.dev | Technical case studies • Architecture diagrams • Engineering journal • Open-source projects

Paden C. Gillispie

Macomb, IL area | gillpad.dev | linkedin.com/in/paden-gillispie/ | github.com/pgill-dev

Professional Experience

Western Illinois University Macomb, IL
Infrastructure Engineer **October 2025 – Present**

- Led the migration of cybersecurity lab workloads from VMware ESXi to Proxmox VE while implementing Proxmox Backup Server and validating backup integrity to improve disaster recovery capabilities.
- Engineered and maintained enterprise virtualization, storage, and container platforms supporting campus infrastructure using Proxmox VE, Ceph, and Talos Kubernetes.
- Designed and developed Python/Flask-based internal tooling to automate infrastructure administration, snapshot management, system validation, and operational reporting.
- Performed CIS Benchmark assessments and coordinated vulnerability remediation efforts using Rapid7 InsightVM, improving the security posture of Windows and Linux systems.
- Implemented enterprise monitoring and observability with Prometheus and Grafana, enabling proactive infrastructure health monitoring and faster incident response.
- Strengthened platform security through certificate management, access-control hardening, baseline enforcement, and secure infrastructure design.
- Resolved complex cross-platform issues spanning hypervisors, storage, networking, Kubernetes, and operating systems while documenting repeatable operational procedures**.**
- Collaborated with faculty and technical staff to modernize cybersecurity laboratory infrastructure, supporting hands-on education through scalable virtualization, backup, and platform engineering initiatives.

Lead Technical Instructor – Cybersecurity Club *(Concurrent)*

- Lead weekly hands-on technical instruction for university cybersecurity club members covering enterprise infrastructure, virtualization, Linux administration, networking, Active Directory, and offensive/defensive security concepts.
- Design and deliver practical lab exercises using Proxmox, Kubernetes, GOAD, Kali Linux and enterprise infrastructure to provide students with real-world engineering experience.
- Mentor students in troubleshooting, systems engineering, and cybersecurity best practices while fostering collaborative problem solving.
- Develop technical documentation and learning materials to support repeatable laboratory instruction.

General Dynamics Information Technology | Fort Drum, NY
Information Assurance Engineer **January 2025 – September 2025**

- Implemented STIGs across Windows Server, RHEL, and VMware systems; validates hardening using SCAP Compliance Checker and audited discrepancies with STIG Viewer.
- Automated Zero Trust-aligned STIG enforcement and policy-based access controls across Windows, RHEL, and VMware systems using Ansible; ensures configuration drift prevention and continuous compliance with identity and system baselines.
- Tracked and remediated IAVM vulnerabilities within mandated timelines; verified patch deployments and ensured complete documentation for audit readiness.
- Performed detailed analysis and remediation of ACAS scan findings; generated prioritized reports through Tenable Security Center based on asset criticality and CVSS scoring.
- Conducted OS and firmware patching on physical and virtual servers using WSUS and YUM/DNF; verified service restoration and logs change history.
- Resolved Tier II/III escalated issues involving Linux/Windows OS faults, vSphere host access problems, and critical service disruptions across 100+ nodes.
- Administered ESXi infrastructure through vCenter; deployed VM templates, managed distributed switch configs, and maintains cluster health (HA/DRS).
- Authored SOPs and documentation for vulnerability management and STIG enforcement, scan configuration, remediation procedures, and compliance verification, while maintaining STIG tracking sheets.

TechWise | Fort Drum, NY
Network Systems Operations Specialist II **September 2024 – January 2025**

- Network administrator for an organization that provides training and training support to multiple organizations across the

Paden C. Gillispie

Macomb, IL area | gillpad.dev | linkedin.com/in/paden-gillispie/ | github.com/pgill-dev

Northeastern United States.

- Designed and deployed a new network enclave with VLANs, ACLs, while enforcing segmentation for supporting communications for multinational training between geographically dispersed organizations.
- Monitored, Maintained, and troubleshot network infrastructure across five separate network enclaves, ensuring optimal performance and uptime.
- Configured and maintained the server network infrastructure for VMWare ESXi host and VSAN clusters.
- Built and managed configurations for switches, routers, and load balancers, ensuring documentation is up to date and meets all DISA STIG requirements.
- Performed vulnerability assessments on network equipment identifying vulnerabilities and applying security updates to maintain compliance with DoD cybersecurity standards, including RMF and STIG requirements.
- Provided tier II/III support to resolve and diagnose escalated network issues and collaborated with cross-functional teams to implement improvements and solutions.
- Followed a methodical troubleshooting process to identify and resolve complex hardware and software issues.
- Built and updated documentation to establish repeatable processes and standard network administration and management procedures.

TechWise | Fort Drum, NY
System Technician **July 2023 – September 2024**

- Managed and maintained the IT infrastructure, ensuring operational system performance and security.
- Provided endpoint, network, and infrastructure support across Windows and Linux based enterprise environments.
- Assisted with network/system deployments and operational improvement initiatives

United States Army | Various Locations
Operations Manager **January 2014 – April 2022**

- Led teams of up to 54 personnel in high-tempo operational environments, coordinating training, mission planning, equipment readiness, and operational execution.
- Mentored junior leaders while maintaining personnel accountability, operational readiness, and safety across multiple deployments and training environments.