Payton Erickson

Infrastructure & Automation Engineer

Menifee, CA | (951) 428-4331 | payton.erickson02@gmail.com | linkedin.com/in/payton-erickson | fireflyhacker.com | github.com/FireflyHacker

CORE SKILLS

Languages & Automation: Python (primary); PowerShell and Bash (working knowledge); Git, REST API integration, Datto RMM, Windows Configuration Designer, Chocolatey

Cloud & Identity: Microsoft 365 and Azure administration, Entra ID, Exchange Online, Microsoft Purview (content search / eDiscovery), AWS (EC2, S3, Route53, SES), Authentik SSO (OIDC / LDAP / SAML)

Monitoring & Operations: Zabbix, Wazuh SIEM, Huntress, Sophos XDR, endpoint and agent health auditing, alerting, documentation and runbooks

Virtualization & Containers: Proxmox, KVM/QEMU, VMware ESXi, LXC, Docker, Kubernetes

Networking & Security: VLANs, firewall configuration and policy (Sophos XGS, OPNsense), VPN (WireGuard, NetBird, OpenVPN), DNS/DHCP/RADIUS

Storage & OS: TrueNAS, ZFS, NFS/iSCSI/SMB, SAN/NAS; Debian/Ubuntu, Fedora, Alpine, FreeBSD, Windows Server 2012–2022

EXPERIENCE

IT Engineer | Tech Guardian (MSP)

Sept 2024 – Present

Provide 2nd and 3rd level infrastructure and systems support for a managed services provider, covering ~950 workstations across 28 client companies.

- Designed and built a workstation deployment pipeline from scratch using PPKG (Windows Configuration Designer), Datto RMM, Chocolatey, and PowerShell, reducing provisioning from a manual 4+ hour process to a 30 minute base provision with full user setup within an hour; used across 30+ workstation deployments.
- Administer Microsoft 365 and Exchange Online, resolving user mailbox issues and using Microsoft Purview content search to investigate email problems: identifying who deleted messages from a shared mailbox, diagnosing a phone sync fault that automatically routed a user's mail to trash, and recovering an accidental deletion of six months of sent items.
- Scoped a client's CMMC Level 2 / NIST 800-171 wireless and CUI access requirements: flagged a FIPS gap in existing hardware and proposed a zero trust (ZTNA) access design enforcing compliance checks and FIPS validated encryption, with CUI (SharePoint) restricted to the compliant access path, delivered with remediation options and timelines.
- Designed, deployed, and maintained a Python device audit tool cross referencing Huntress, Sophos, and Datto RMM exports to catch coverage gaps: flagged 100+ endpoints with EDR installed but not reporting to the management cloud and 20+ replacement devices missing required agents, cutting average time per ticket from 30 to 20 minutes with automated client notifications.
- Automated Sophos XGS firewall provisioning with zero touch deployment and config import, completing 30 firewall replacements in 30 days from provisioning to full cutover.
- Recovered a 250+ device UniFi network (12 switches, 10 P2P antennas) spanning a /23 subnet with no configuration backup, restoring full operation in under 8 hours.

Infrastructure Engineer | Western Region CCDC

Volunteer, May 2025 – Present

- Deploy and operate the production service stack (Proxmox, TrueNAS, Authentik SSO, NetBird VPN), supporting 300+ concurrent users during competition.
- Migrated the environment from VMware to Proxmox, including cluster architecture, ZFS pool layout, and storage optimization for a 48 drive SAS array.
- Designed a dual 10GbE topology with separate storage and VM fabrics, LACP bonded for roughly 20 Gbps.

Infrastructure Lead | NUCC *Volunteer, Jan 2023 – Present*

- Architect and maintain distributed, fully remote infrastructure serving ~150 members across five universities on no budget.
- Operate the full stack: Proxmox, TrueNAS, Authentik SSO (OIDC with group sync), NetBird VPN, Zabbix monitoring, Wazuh SIEM, and Nginx reverse proxy.
- Implemented SSO across all services (NetBird, Bookstack, Nextcloud, LeanTime, CTFd) via Authentik OIDC with automated group sync and permission mapping.

Co-Team Captain | Collegiate Cyber Defense Competition (CCDC) *Oct 2021 – Apr 2024*

- Led UCI to 2nd at WRCCDC Regionals and 4th at NCCDC Nationals (2024); built practice networks simulating live attacks, covering firewall configuration, network defense, and Palo Alto threat detection.

EDUCATION

B.S. in Computer Science (3.5 GPA), University of California, Irvine *Oct 2020 – Mar 2024*

Relevant coursework: Advanced Computer Networks, Network Security, Information Retrieval, C++, Java

PROJECTS & COMMUNITY

- **DEF CON Official Party, Organizer and Lead:** Organize and run an official DEF CON party for several hundred attendees, managing logistics, budget, and a team of ~15.
- **passgen (Go):** Secure, reproducible password generator: rewrote portions of the Atoll library, added a SHA-256 hashed seed option for deterministic regeneration, and used ChaCha20 for secure random generation.
- **Upcycled Sophos XG Docker Platform:** Repurposed a decommissioned Sophos XG 310 firewall into a Docker host running multiple containers (KASM, an SSH honeypot, a game server, and a TTY emulator) across mapped ethernet ports.

CERTIFICATIONS & AWARDS

Certifications: Sophos Certified Firewall and Endpoint Technician, Microsoft 365 Fundamentals (MS-900), Azure Administrator (AZ-104, in progress)

Awards: 4th at NCCDC Nationals (2024), 1st at Hivestorm (2023), 2nd at WRCCDC Regionals (2022), featured in the 'Extreme Homelabbing' talk at SCaLE 23X