

Amanda Hunt

Los Angeles, CA · [linkedin.com/in/a-hunt](https://www.linkedin.com/in/a-hunt) · github.com/achunt01

SUMMARY

Cloud Security Engineer. I spent four years in managed services. For the last two, I was the sole senior technical resource and final escalation point for an entire regional market across network security, endpoint, identity, cloud, email security, and vulnerability management. I deliver network, identity, and cloud projects, and I automate the work around them. I scope, design, build, document, and hand off. I train and mentor other engineers, and set the automation and documentation standards that other regions adopted. If a tool has an API, I can wire it in for triage, enrichment, and reporting.

EXPERIENCE

Senior Security Engineer, managed services provider

April 2025 to October 2026

- Lead end-to-end client projects across onboarding, networking, cloud, endpoint, and email.
- Run environment assessments covering infrastructure, identity, cloud posture, and security readiness.
- Plan and deliver Azure hybrid deployments, Microsoft 365 configuration, Intune device management, Conditional Access and MFA, SAML and SSO integrations, VPNs, and vulnerability management.
- Configure firewalls, switches, VLANs, and DMZs for client networks.
- Deploy and manage email security (Mimecast, Defender, Avanan) and SPF, DKIM, and DMARC records. Implemented DNS record monitoring.
- Led a .NET end-of-life dependency assessment across 424 systems for an audit: inventoried installed runtimes and SDKs, determined which versions were genuinely in use, and narrowed the real exposure to 2 dependencies; wrote the remediation script and validated findings cleared in Tenable.
- Built ticket-driven automation connecting a PSA platform to SentinelOne, Avanan, Tenable, NinjaOne, Pax8, Microsoft Graph, and Exchange Online. In one three-month period, twelve packages ran 2,560 times across 2,151 tickets. Packages included KnowBe4 phish-alert enrichment, mailbox online-archive provisioning, and new-hire onboarding via Azure AD activities.
- Triage SOC alerts from SentinelOne EDR and Arctic Wolf: true-positive analysis, static detection review, and client-facing incident writeups.
- Investigated real attacks: OAuth device-code phishing, ransomware detections on Linux hosts, and coordinated with third-party penetration testing teams on findings.
- Hardened Palo Alto security profiles: reviewed URL filtering and threat prevention policies against best practice and closed gaps in outbound inspection.
- Primary technical contact for clients during projects. Document every project for handoff to support teams.
- Mentor engineers and contribute to delivery standards. Covered after-hours and weekend on-call on an ad hoc basis for critical issues.

Managed Services Engineer, managed services provider

June 2022 to April 2025

- Onboarded and managed networking, endpoint, server, and host-based security services.
- Network and infrastructure administration across client environments.
- Escalation point for the help desk. Guided junior technicians through complex issues.
- Led professional services engagements from scoping to delivery.

Lab Manager, university networking and cybersecurity lab

Feb 2022 to June 2022

- Led a team of 7 lab assistants on projects with a focus on automation. Supported faculty with classroom virtualization.
- Deployed Splunk to monitor usage of more than 10 network devices, 10 servers, and 100 virtual machines.
- Aggregated and correlated over 15 log source types across 30 systems. Built 25 detections for anomalous user and system activity.

- Lead threat hunter. Threat hunting with Splunk and Elasticsearch in competition and lab environments.
- First place in the state and Midwest qualifiers and at the Iowa CDC in 2022. Competed at the Global CCDC in 2021.

SELECTED WORK

- **Alert triage automation** across SentinelOne, a PSA platform, and an automation engine over REST APIs. Cut analyst handling time by roughly 80 percent. Now standard practice across four regional markets.
- **Firewalls, switching, and wireless:** new firewall builds across Palo Alto, Fortinet, Cisco, Meraki, WatchGuard, and UniFi; cross-vendor and Palo Alto to Palo Alto migrations, including multi-site HA pairs (PA-200 to PA-1400); more than one Panorama, on-premises and in Azure; Strata Cloud Manager, SD-WAN across branch and multi-hub topologies, TLS decryption; switch migrations and refreshes; Meraki and UniFi wireless. PowerShell tooling against the Panorama API for license monitoring.
- **Microsoft 365** tenant separations and consolidations, migrations from Gmail and other tenants, federated domain migrations.
- **Identity and devices:** AD to Entra ID hybrid transitions, device moves to Entra ID join and hybrid join, Intune MDM and MAM on all platforms, GPO to configuration profile migration, Conditional Access enforcement, SSO with Entra ID as identity provider.
- **Identity and remote access:** Duo and Okta MFA rollouts, SAML and SSO integrations, VPNs, and Zero Trust remote access with Prisma Access and Cloudflare Zero Trust.
- **Cloud and DR:** Azure migrations from AWS and on-premises, IaaS builds, Nutanix AHV conversion with NC2 on Azure and DR, Veeam, Cohesity.
- **Citrix:** on-premises Citrix ADC to Citrix DaaS, VDA deployments from scratch for NetScaler and DaaS, XenApp migrations.
- **Security programs:** Tenable vulnerability management end to end, DMARC enforcement to p=reject, internal pen test remediation, email security across Mimecast, Defender for Office 365, Avanan, and Check Point Harmony.
- **Assessments:** environment assessments covering infrastructure, identity, cloud posture, and security readiness, and firewall health assessments.
- **Client onboarding and endpoint:** onboarding of networking, endpoint, server, and host-based security services, and SentinelOne and Tenable agent rollouts at scale.

CERTIFICATIONS

PCNSE · PCNSA · CCSP · SC-100 Microsoft Cybersecurity Architect · AZ-500 Azure Security Engineer · CCNA · SSCP · Tenable One

EDUCATION

BS in Cybersecurity, minor in Computer Science, DePaul University. Dean's List, Presidential Scholar. 2017 to 2022

TECHNOLOGIES

Network security: Palo Alto, Panorama, Strata Cloud Manager, Prisma Access, Cloudflare Zero Trust, Fortinet, Cisco, Meraki, UniFi, WatchGuard

Identity: Entra ID, Active Directory, Duo, Okta, SAML and SSO, SCIM

Cloud and virtualization: Azure, AWS, Nutanix, VMware, Hyper-V, Citrix, Veeam, Cohesity

Endpoint and detection: SentinelOne, CrowdStrike, Cylance, Rapid7, Arctic Wolf, Splunk, Elasticsearch, Microsoft Sentinel

Vulnerability management: Tenable, Nessus, Qualys, Prisma Cloud CSPM

Email security: Mimecast, Defender for Office 365, Avanan, Check Point Harmony, SPF, DKIM, DMARC

Automation: PowerShell, Python, REST APIs and request signing, Microsoft Graph, Exchange Online PowerShell, Pia, ConnectWise, NinjaOne, Pax8, Bash, SQL