JENNIFER MARTIN

CYBERSECURITY ENGINEER

jen.martin616@gmail.com

208.992.6995

Nampa, ID

Linkedin.com/in/
jenniferoliviamartin

TECHNICAL SKILLS

Microsoft Sentinel & KQL

Defender XDR & MDE

Microsoft Defender for IoT

Windows Event Log Analysis

Sysmon Telemetry

Detection Engineering

Threat Hunting

Incident Response

Network Traffic Analysis

Wireshark & Packet Capture

Palo Alto PAN-OS

Panorama Administration

IDS/IPS Monitoring

Snort & Nmap

ICS/OT Security

Vulnerability Assessment

Security Hardening

PowerShell & Python

Azure Networking

BGP, IPsec & TCP/IP

MITRE ATT&CK

SIEM Detection Tuning

Log Correlation

SUMMARY

Cybersecurity Engineer with 7 years of IT and security experience, specializing in ICS/OT security, network defense, incident response, and threat detection. Experienced in zero-trust architecture, vulnerability remediation, and translating complex technical findings into actionable security improvements.

PROFESSIONAL EXPERIENCE

Security Engineer – Detection & Incident Response 05/2026 – 09/2026

Microsoft | Cloud Operations & Infrastructure Engineering | Cyber Defense
Remote, Washington USA

- Engineered KQL detections across Microsoft Sentinel, Defender XDR, Palo Alto, and Defender for IoT telemetry.
- Developed detections for suspicious parent-child processes, cross-zone lateral movement, and anomalous ICS/OT activity.
- Validated detection fidelity using synthetic attack chains and positive, negative, and near-miss test cases.
- Performed threat hunting across endpoint activity, Windows events, firewall traffic, and ICS/OT network telemetry.
- Investigated high-severity, multi-site incidents using endpoint telemetry, firewall logs, routing data, packet captures, and Windows event logs.
- Correlated security and network evidence to establish scope, evaluate root-cause hypotheses, and direct technical escalations.
- Coordinated investigations across SOC, network, cloud, infrastructure, and site teams during complex operational incidents.
  Converted incident findings into detection improvements, post-incident analysis, troubleshooting procedures, and response playbooks.

Network Security Engineer II 10/2022 – 05/2026

Microsoft | Cloud Operations & Infrastructure Engineering | Cyber Defense
Remote, Washington USA

- Designed and deployed zero-trust configurations across 150+ Palo Alto firewalls supporting global ICS/OT networks.
- Managed Panorama onboarding, policy deployment, software upgrades, high availability, and security hardening.
- Integrated Palo Alto firewalls with Azure vWAN and resolved BGP, IPsec, routing, certificate, and connectivity failures.
- Deployed and supported Defender for IoT sensors and IDS monitoring across physical-security and critical-environment networks.
- Analyzed firewall and IDS/IPS telemetry to validate policy behavior, investigate outages, and isolate upstream failures.
- Assessed vulnerabilities and control gaps, translating findings into remediation plans and hardened configurations.
- Coordinated global deployments and network changes with cloud, infrastructure, site, vendor, and security teams.
- Authored technical designs, implementation plans, change procedures, troubleshooting guides, and operational runbooks.

JENNIFER MARTIN

CYBERSECURITY ENGINEER

EDUCATION

B.S. Cybersecurity & Information Assurance
Western Governors University
Salt Lake City, UT
08/2017 – 07/2020

M.S. Information Technology Management
Western Governors University
Salt Lake City, UT
08/2021 – 07/2022

CERTIFICATION

CompTIA A+
CompTIA Network +
CompTIA Security +
ITIL® Foundations
CompTIA – Secure Infrastructure Specialist
(ISC)2 – Systems Security Certified Practitioner (SSCP)
EC-Council – Certified Encryption Specialist (EC-ES)
Azure Fundamentals – AZ-900

COMMUNITY INVOLVEMENT

West Ada School District
Cybersecurity Education
Meridian, ID, 2026 - Present

Boise Code Camp
Volunteer/Presenter
Boise, ID, 2024 - Present

Boise DEFCON Group (DC208)
Active Member
Boise, ID 2024 - Present

PROFESSIONAL EXPERIENCE (continued)

Telecom Delivery Specialist - Lead 08/2020 – 10/2022
Microsoft | Cloud Operations & Infrastructure Engineering | Network Field Operations
Remote, Washington USA

- Coordinated more than 40 concurrent data center cross-connect implementations while maintaining delivery timelines and service-level requirements.
- Directed onsite technicians through fiber installation, validation, troubleshooting, and decommissioning procedures across data center environments.
- Managed more than 100 cross-connect requests per month, improving workflow visibility and reducing delays through standardized ticket-management processes.
- Resolved delivery blockers across carriers, data center teams, and internal stakeholders through service activation.
- Developed operational guidance and communicated technical requirements to remote technicians, engineering teams, service providers, and Microsoft stakeholders.

PastelIntel – Cybersecurity Researcher/Consultant 04/2020 – 10/2022
PastelIntel Cybersecurity Consulting – Remote, Idaho USA

- Performed scope-controlled web application security testing to identify vulnerabilities, configuration weaknesses, and potential attack paths.
- Used tools including OWASP ZAP and Nmap to conduct reconnaissance, validate findings, and assess externally exposed systems.
- Analyzed active cyberattacks and developed practical containment, recovery, and security-hardening recommendations for clients.
- Researched threat activity and translated technical findings into clear risk assessments, remediation priorities, and client-facing reports.
- Documented validated vulnerabilities with supporting evidence, potential impact, and actionable remediation guidance.

Data Center Technician 09/2019 – 08/2020
Amazon Web Services | Data Center Infrastructure
Boardman, Oregon USA

- Diagnosed and resolved approximately 1,000 hardware, server, cabling, and infrastructure tickets in high-availability data center environments.
- Performed server installation, component replacement, break-fix maintenance, and network connectivity troubleshooting while following operational and security controls.
- Supported incident recovery and service-restoration activities to minimize infrastructure downtime and protect service availability.
- Identified recurring failure patterns and documented troubleshooting procedures for use by technicians across multiple data center locations.
- Coordinated with remote engineering and operations teams to investigate infrastructure failures and complete time-sensitive repairs.