Elijah Zion

elijahjzion@gmail.com | 425.364.1611 | Duvall, WA | linkedin.com/in/elijah-zion-753578278
U.S. citizen - eligible for Public Trust background investigation

SUMMARY

Entry-level SOC analyst certified in CySA+, CSAP, and Security+, with a completed cloud SOC detection lab covering SIEM monitoring, EDR, adversary emulation, and the alert-to-ticket investigation workflow. Backed by hands-on first-line operational monitoring, alert triage, and escalation experience and cross-platform IT support across Windows, Linux, and macOS. Strong networking fundamentals, clear technical documentation, and proven reliability under sustained shift tempo. U.S. citizen, eligible for a Public Trust.

CERTIFICATIONS

- CompTIA Cybersecurity Analyst (CySA+) - Jun 2026
- CompTIA Security Analytics Professional (CSAP) - Jun 2026
- CompTIA Security+ - May 2026
- CompTIA A+ Core 1 - passed (Core 2 in progress)

SKILLS

Security Operations: security monitoring, alert triage, alert investigation, incident escalation, incident response (fundamentals), log analysis, root cause analysis

SIEM, EDR & Detection: Security Information and Event Management (SIEM), Elastic Stack (ELK: Elasticsearch, Logstash, Kibana), Elastic Defend (EDR), Fleet and Elastic Agent, Sysmon, detection rule authoring, Kibana dashboards

Threat & Adversary Emulation: MITRE ATT&CK mapping, Mythic C2 (adversary emulation), brute-force attack detection, threat landscape awareness

Networking: TCP/IP, ports and services, DNS, firewall configuration, VLAN segmentation, network troubleshooting

Operating Systems & Tools: Windows, Linux/Unix (Ubuntu, Kali), macOS, Microsoft 365, osTicket, ticketing (Linear), Python (scripting)

EXPERIENCE

AI Technician - AIM Intelligent Machines
Redmond / Monroe, WA | Jun 2025 - Mar 2026

- Served as first-line monitor on a two-person watch across 2-5 prototype autonomous machines, triaging a live operational alert feed and escalating genuine and safety-critical faults to senior engineering.
- Verified ambiguous deviations against the defined operating plan to validate true anomalies and filter false alarms.
- Owned incident ticketing in Linear, authored procedure docs (SOPs), reported event status directly to senior engineering leadership, and assisted with new-hire IT provisioning and Ethernet cabling.

IT Support (contract) - Pirean Gallery
Moscow, ID | Dec 2024 - May 2025

- Provided independent on-site technical support across a mixed Windows and macOS environment, troubleshooting hardware, software, and network issues root cause first.

- Traced a live-event connectivity outage to incorrect switch-port cabling and restored service under time pressure.

Commercial Fisherman (greenhorn deckhand) - Silver Bay Seafoods
Dillingham, AK | Summer 2024

- Worked roughly 19-hour shifts for five consecutive weeks during peak salmon season, sustaining reliable performance and safe operation across an eight-week run.

Intern - Data Annotation - Vantage International
Moscow, ID | Feb - Apr 2024

- Labeled and prepared transcript and image datasets in Microsoft Excel used to train large language models, with strong attention to detail.

Retail Cashier / Warehouse Associate - Coastal Farm & Ranch
Monroe, WA | Apr 2022 - Apr 2023

- Delivered front-line customer support and trained a coworker in a fast-paced retail and warehouse environment.

PROJECTS

Cloud SOC Detection Lab - Elastic SIEM, EDR & Adversary Emulation

- Built and operated a cloud-hosted SOC on Vultr: deployed an Elastic SIEM (Elasticsearch, Logstash, Kibana) with a Fleet server and Elastic Agent, ingesting Sysmon and Windows Defender telemetry from a Windows Server endpoint.
- Exposed RDP to generate live attack telemetry, authored detection rules for RDP brute-force activity, and triaged and investigated the resulting alerts end to end.
- Deployed Elastic Defend (EDR), validated prevention with a malicious-download test, and configured an automated response action.
- Ran an adversary emulation with a Kali attacker and a Mythic C2 (Apollo agent), then mapped the attack chain to MITRE ATT&CK technique IDs (for example T1110, brute force).
- Integrated osTicket with Elastic so alerts auto-generate tickets, running the full alert-to-ticket investigation workflow.

Segmented Home Network (Unifi)

- Configured a segmented home network on Unifi gear with VLAN isolation (IoT and guest), inter-segment firewall rules, and network monitoring.

HackTheBox CPTS Path (in progress)

- Progressing through the HackTheBox Penetration Tester path: hands-on network enumeration, ports and services, and footprinting that sharpen detection instincts.

EDUCATION

Associate of Arts (AA), Liberal Arts & Sciences - New Saint Andrews College (Moscow, ID | Aug 2023 - May 2025)