Leo Edwards

(503) 555-6184 leo.edwards@example.com linkedin.com/example/leoedwards Portland, OR 97205

SUMMARY

Senior security operations engineer with 9 years across **incident response**, **digital forensics**, **cloud security**, detection engineering, and **employee investigations**. Leads high severity incidents as Incident Commander, coordinating engineering, legal, HR, compliance, and executive stakeholders through containment, recovery, and closure. Uses SIEM investigation, Python automation, endpoint analysis, evidence collection, and cloud telemetry across macOS, Windows, Linux, AWS, and GCP. Builds practical runbooks, investigative workflows, evidence packages, and repeatable reporting processes that support defensible decisions. Mentors security engineers through case reviews, collection exercises, tabletop sessions, and reporting feedback. GCIH certified with a computer science background and working knowledge of NIST Cybersecurity Framework, ISO 27001, and FedRAMP. Brings calm judgment, clear communication, and useful technical guidance to sensitive investigations.

EXPERIENCE

Senior Security Operations Engineer

March 2023 - Present

Cascade Cloud Systems

Portland, OR

Leads global security operations across incident response, digital forensics, cloud investigations, **insider threat** matters, and stakeholder communications. Guides engineers through sensitive cases while improving investigative workflows, reporting quality, and response consistency.

- Led high severity incidents through containment and recovery, coordinating engineering, **legal**, HR, and executive stakeholders.
- Preserved endpoint evidence across macOS, Windows, and Linux for **employee relations** and security investigations.
- Built **Python** utilities for artifact normalization, indicator enrichment, and repeatable evidence package assembly.
- Developed SIEM workflows across AWS and GCP logs, identity events, endpoint telemetry, and application activity.
- Mentored security engineers through case reviews, collection exercises, reporting feedback, and incident simulations.
- Maintained incident **runbooks** and stakeholder templates aligned with **NIST Cybersecurity Framework** practices.

Security Incident Response Engineer

June 2020 - February 2023

Summit Commerce Technologies

Denver, CO

Served as technical lead for account compromise, malware, data access, policy violation, and insider threat cases. Connected **SIEM** analysis, cloud evidence, Python tooling, documented collection, and legal coordination across investigations.

- Triaged identity, endpoint, network, and cloud alerts, separating benign activity from incidents requiring investigation.
- Led account compromise investigations through closure, correlating AWS, GCP, **Windows**, **Linux**, and SaaS evidence.
- Created Python scripts for log parsing, indicator enrichment, and repetitive collection checks.
- Supported **insider threat** cases with documented collection procedures, evidence handling, factual reporting, and legal coordination.
- Refined incident playbooks after investigations and tabletop exercises, adding escalation criteria and communications checkpoints.
- Presented investigation findings and response options to technical teams, legal partners, and business stakeholders.

Security Operations Analyst

July 2017 - May 2020

Blue Mesa Financial

Phoenix, AZ

Monitored security telemetry and supported forensic investigations across authentication, phishing, malware, and anomalous access cases. Built reusable searches and collection utilities that improved evidence consistency, reporting, and **compliance** coordination.

- Monitored SIEM alerts and endpoint events, escalating credible threats with concise evidence and recommended actions.
- Investigated suspicious authentication, phishing, malware, and anomalous access using host, identity, email, and network records.
- Built reusable searches and **Python** utilities that improved evidence consistency across recurring investigations.
- Supported Windows and Linux forensic collection with documented sources, timestamps, and senior investigator guidance.
- Contributed to incident reports and post incident reviews for security and compliance stakeholders.
- Mapped security controls against **NIST Cybersecurity Framework** and **ISO 27001** concepts during review cycles.

PROJECTS

Forensic Evidence Workflow 2024

Built a repeatable investigation workflow that organized endpoint artifacts, indicator enrichment, evidence review, and concise reporting for sensitive cases.

Cloud Incident Investigation Lab 2023

Created a practical lab spanning AWS and GCP telemetry, SIEM queries, identity events, and response decisions for cloud incidents.

LEADERSHIP & AWARDS

- Security Incident Tabletop Facilitator, led recurring response simulations and practical discussions from 2024 to Present.

- Security Operations Mentorship Program, Senior Mentor, coached engineers through case reviews and investigative methods from 2023 to Present.
- GIAC Certified Incident Handler recipient, recognized for incident response knowledge and applied investigation practice in 2024.

EDUCATION

Bachelor's Degree in Computer Science 2017

Arizona State University GPA: 3.7 *Tempe, AZ*

Coursework: *Computer Networks, Operating Systems, Computer Security, Programming Languages*

CERTIFICATIONS

- GIAC Certified Incident Handler 2024
- AWS Certified Security Specialty 2025

TECHNICAL SKILLS

- **Programming and Scripting:** Python, PowerShell, Bash
- **SIEM Platforms:** SIEM queries, log review, event correlation
- **Endpoint Forensics:** macOS, Windows, Linux
- **Cloud Platforms:** AWS, GCP, cloud based services
- **Incident Response:** Incident command, triage, containment
- **Investigation Methods:** Evidence collection, artifact analysis, forensic reporting
- **Security Frameworks:** NIST Cybersecurity Framework, ISO 27001, FedRAMP
- **Automation and Workflows:** Python utilities, runbooks, workflow automation
- **Security Telemetry:** Identity events, endpoint telemetry, application activity
- **Response Communications:** Executive updates, legal reporting, stakeholder briefings

SKILLS

- Incident response
- Incident command
- Digital forensics
- Insider threat
- Employee investigations
- SIEM
- Python
- Cloud security
- Evidence collection
- Log analysis
- Runbook development
- Security monitoring
- Incident triage
- Forensic analysis
- Stakeholder communication

PROFESSIONAL AFFILIATIONS

- Security Incident Tabletop Facilitator, 2024 to Present.
- Security Operations Mentorship Program, Senior Mentor, 2023 to Present.

LANGUAGES

- English (Native)
- Spanish (Intermediate)

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST