Cyrus Petros Senior Incident Response Engineer

Seattle, WA · cyrus.petros@gmail.com · +1 206-555-0158 · linkedin.com/in/cyruspetros

PROFILE SUMMARY

- **Senior Incident Response Engineer** with **8 years** on **in-house security teams** at a live streaming platform and a global travel company, specializing in **AWS intrusions, account takeover and Linux host forensics**.
- Works across EDR (**CrowdStrike Falcon**), SIEM (**Splunk**), cloud logs (**AWS CloudTrail**, GuardDuty, Okta), forensics (**Velociraptor**, **Volatility 3**), reversing (**Ghidra**) and **Python** for collection and parsing.
- Knows **AWS control plane attacks**, **Linux memory forensics** and **streamer account takeover** patterns well, and closes every case with a **root cause**, a new detection and an updated runbook.
- Works with **Legal, Trust & Safety**, cloud engineering and the **SOC**, runs the bridge on high-severity incidents, and writes the **executive summary** the **CISO** takes to leadership after each one.
- Mentors **3 SOC analysts** moving into IR, wrote the **AWS key compromise** and **account takeover playbooks**, runs the **quarterly tabletop** for engineering leads, and holds **GCFA** and **GREM**.

TECHNICAL SKILLS

Frameworks & Certifications:	NIST 800-61, MITRE ATT&CK, Cyber Kill Chain, GCFA, GREM
EDR & SIEM:	CrowdStrike Falcon (Insight, Real Time Response), Splunk Enterprise Security (SPL), Microsoft Defender for Endpoint
Forensic Collection & Timelines:	Velociraptor, KAPE, Plaso, Timesketch, Eric Zimmerman's Tools, chain of custody
Memory & Malware Analysis:	Volatility 3, AVML, Ghidra, YARA, CAPA, Joe Sandbox
Network & Packet Analysis:	Zeek, Wireshark, Suricata, VPC Flow Logs, JA3/JA4
Cloud & SaaS Logs:	AWS CloudTrail, Amazon GuardDuty, Okta System Log, Microsoft Entra ID, Google Workspace audit logs
Scripting, SOAR & Threat Intel:	Python, Sigma, Tines, MISP, VirusTotal, Jira

EDUCATION

University of Washington — B.S. in Informatics, Information Assurance and Cybersecurity — Seattle, WA · Sep 2014 to Jun 2018

GIAC — GCFA and GREM certifications — Seattle, WA · 2020 and 2023

WORK EXPERIENCE

Twitch — Senior Incident Response Engineer — Seattle, WA · Mar 2022 to Present

- Ran incident command on **17 high-severity incidents**, keeping one timeline and decision log in **Jira** and updating Legal, Trust & Safety and executives on a fixed schedule until closure.
- Traced an exposed CI access key through **AWS CloudTrail** and GuardDuty, mapping every API call the attacker made, and confirmed in **7 hours** that no bucket with user data was read.
- Pulled memory from compromised Linux build servers with **Velociraptor** and analyzed it in **Volatility 3**, finding an in-memory backdoor that disk triage had missed on **4 hosts**.
- Built containment runbooks that pair **CrowdStrike RTR** host isolation with Okta session revocation and AWS key rotation, cutting median time to contain from 74 minutes to **19**.
- Ran quarterly hunts mapped to MITRE ATT&CK across **Splunk**, Falcon and CloudTrail data, turning **14 confirmed findings** into tested detections the SOC now owns.

Expedia Group — Incident Response Engineer — Seattle, WA · Jul 2018 to Feb 2022

- Found beaconing from a compromised booking server by sorting **Zeek** connection logs by interval and JA3 hash, then sized the data that left at **2.3 GB** for the legal team.
- Reversed a credential-stealing loader from a phishing campaign in **Ghidra**, pulled its config and C2 list, and wrote **YARA** rules that found it on **27 more laptops**.
- Rewrote the incident response plan and ransomware playbook, then ran quarterly tabletops for engineering and communications leads, cutting the time to declare an incident from 3 hours to **40 minutes**.