Aliyah Thompson Senior SOC Analyst

Reston, VA · aliyah.thompson@gmail.com · +1 703-555-0124 · linkedin.com/in/aliyahthompson

PROFILE SUMMARY

- **Senior SOC Analyst** and threat hunter, **6 years** at **MDR providers** watching **Fortune 500 and defense-industry customers** around the clock, specializing in **hypothesis-driven hunts and identity attacks in AWS and Microsoft 365**.
- Works across SIEM (**Google SecOps** in YARA-L, **Microsoft Sentinel** in KQL), EDR (**CrowdStrike Falcon**, **SentinelOne**), threat intel (**VirusTotal**, **Mandiant Advantage**), live response (**Velociraptor**), and scripting (**Python**).
- Deep in **ATT&CK-mapped hunting**, **noise tuning**, and **cloud audit log analysis**, turning each confirmed hunt finding into a **tested detection** so the next attempt **triggers an alert on its own**.
- Partners with **incident responders, intel analysts, and customer security leads** on **14 enterprise accounts**, joins the bridge on confirmed intrusions, and gives each customer a **monthly threat briefing**.
- Mentors **4 analysts** through their first hunts, wrote the **hunt report template** and **Entra ID investigation runbook** the whole team uses, and holds **GCIH** and **GCFA**.

TECHNICAL SKILLS

SIEM & Query Languages:	Google SecOps (YARA-L, UDM search), Microsoft Sentinel (KQL), Splunk (SPL), Sigma
EDR & Endpoint Security:	CrowdStrike Falcon (Insight, Real Time Response), SentinelOne Singularity, Defender for Endpoint, Sysmon
Threat Intel & Frameworks:	MITRE ATT&CK, Mandiant Advantage, VirusTotal, MISP, STIX/TAXII, Diamond Model
Incident Response & Forensics:	NIST SP 800-61, Velociraptor, KAPE, Volatility 3, memory and disk triage
Network & Cloud Telemetry:	AWS CloudTrail, Amazon GuardDuty, Microsoft Entra ID, Okta System Log, Zeek
Email Security & Malware Analysis:	Defender for Office 365, Joe Sandbox, YARA, CAPA, static file triage
SOAR, Scripting & Case Management:	Python, Google SecOps SOAR, Cortex XSOAR, Jira, Git

EDUCATION

Howard University — **M.S. in Cybersecurity** — Washington, DC · Aug 2018 to May 2020

GIAC — **GCIH and GCFA certifications** — Reston, VA · 2021 and 2024

WORK EXPERIENCE

Mandiant (Google Cloud) — Senior SOC Analyst — Reston, VA · Aug 2022 to Present

- Ran monthly hypothesis hunts across 14 customers' EDR and cloud logs in **Google SecOps**, and **3 of last year's 12 hunts** found live intruder activity the existing rules had missed.
- Turned hunt findings into **YARA-L** and **KQL** detections mapped to MITRE ATT&CK, each tested with Atomic Red Team, raising coverage of priority cloud techniques from 31% to **64%**.
- Correlated CloudTrail, GuardDuty, and **Okta** logs to trace a stolen **AWS** access key for a retailer, building the attacker timeline in **6 hours** and confirming no data left the account.
- Investigated **CrowdStrike Falcon** and **SentinelOne** detections down to the process tree, isolating hosts and sweeping each customer's fleet for matching hashes, keeping median time to containment at **22 minutes**.
- Wrote **Python** actions for the **Google SecOps SOAR** playbooks that pull VirusTotal verdicts, asset owners, and recent sign-ins into each case, cutting median time to first analyst action by **41%**.

Secureworks — SOC Analyst — Atlanta, GA · Jul 2020 to Jul 2022

- Triaged **Taegis XDR** and **Splunk** alerts for 33 mid-market customers on rotating 12-hour shifts, writing escalation notes the response team accepted without rework on **93%** of cases.
- Worked the customer phishing queue in **Defender for Office 365**, detonating suspect files in Joe Sandbox and running tenant-wide purges that removed **2,860 malicious messages** in 2021.
- Handled containment on **17 confirmed incidents**, mostly ransomware precursors and BEC, collecting evidence with **Velociraptor** and writing the NIST SP 800-61 reports customers sent to their insurers.