Hector Diaz Junior SOC Analyst

San Antonio, TX · hector.diaz@gmail.com · +1 210-555-0139 · linkedin.com/in/hectordiaz

PROFILE SUMMARY

- **Junior SOC Analyst**, **2 years** on the **overnight tier-1 shift** of a **24/7 MSSP** covering **hosting and e-commerce clients**, focused on **alert triage, phishing reports, and first-look endpoint checks**.
- Uses SIEM (**Splunk**), EDR (**Defender for Endpoint**), case tracking (**ServiceNow SIR**), email security (**Proofpoint TRAP**), and sandboxing (**ANY.RUN**) every shift, with beginner KQL and PowerShell.
- Building depth in **SPL log searches**, **email header analysis**, and **IOC enrichment**, working from **the tier-1 runbooks** so tier 2 receives **escalations with the timeline already built**.
- Shares the night shift with **3 tier-1 peers and 2 tier-2 analysts**, calls **client IT contacts** when a host needs isolating, and brings **noisy-rule examples** to the **weekly tuning meeting**.
- Keeps the **shift handover template** and **5 phishing runbooks** up to date, runs a **weekly Security+ study group** for 4 Rackspace support engineers, and is preparing for **CySA+**.

TECHNICAL SKILLS

SIEM & Query Languages:	Splunk Enterprise Security (SPL, saved searches), Microsoft Sentinel (KQL basics)
EDR & Endpoint Security:	Microsoft Defender for Endpoint (device isolation, timeline), CrowdStrike Falcon (triage), Sysmon (basics)
Threat Intel & Frameworks:	MISP, VirusTotal, AbuseIPDB, MITRE ATT&CK (basics)
Incident Response & Forensics:	NIST SP 800-61, incident timelines, evidence notes, Sysinternals (Autoruns, Process Explorer)
Network & Cloud Telemetry:	Firewall and proxy logs, DNS queries, Microsoft Entra ID sign-in logs, Wireshark (basics)
Email Security & Malware Analysis:	Proofpoint (TRAP), Defender for Office 365, ANY.RUN, urlscan.io, header analysis
SOAR, Scripting & Case Management:	ServiceNow SIR, PowerShell, Python (basics), Confluence runbooks

EDUCATION

University of Texas at San Antonio — **B.S. in Cybersecurity** — San Antonio, TX · Aug 2019 to May 2023

CompTIA — **Security+ certification** — San Antonio, TX · Apr 2024

WORK EXPERIENCE

Rackspace Technology — Junior SOC Analyst — San Antonio, TX · Sep 2024 to Present

- Triaged the overnight **Splunk** and **Defender for Endpoint** queue for 27 hosting clients, closing false positives with notes and escalating real threats within the 20-minute SLA **96%** of the time.
- Cleared the user-reported phishing queue for 9 clients, checking headers and opening attachments in **ANY.RUN**, then pulling **38 live campaigns** from every affected mailbox with **Proofpoint TRAP**.
- Built **SPL** searches that join firewall, proxy, and DNS logs by host, cutting the time to put together an escalation timeline from 42 minutes to **16**.
- Ran a weekly IOC sweep of client **Splunk** data from the intel team's **MISP** feed, enriching hits in **VirusTotal**, which found **3 infected hosts** still beaconing to known C2 servers.
- Tracked a month of false positives on the impossible-travel rule, then proposed **Splunk** exclusions for corporate VPN egress IPs that tier 2 approved, cutting overnight alert volume by **17%**.

Best Buy Geek Squad — Advanced Repair Agent — San Antonio, TX · Jul 2020 to Aug 2024

- Removed malware from **about 640 customer PCs**, tracing persistence through services, Run keys, and scheduled tasks with **Sysinternals Autoruns** and Process Explorer, and reimaging only when cleanup failed.
- Worked **11 ransomware cases** for small-business customers, unplugging infected machines, imaging drives for their insurer, and restoring from backups so most offices were back up the next morning.
- Wrote a **PowerShell** intake script that dumps running processes, startup items, and browser extensions into one report, cutting diagnosis time per PC from 47 minutes to **18**.