Joaquin Merritt

Tacoma, WA · joaquin.merritt@example.com · (253) 555-0146 · linkedin.com/in/example-joaquin-merritt

My Key Qualifications

- **11 years in enterprise cybersecurity** across incident response, threat detection, threat hunting, and vulnerability management at Nordstrom, Expedia, and Alaska Airlines, from 2015 to present.
- Leads high-severity **incident response** across enterprise, cloud, and customer-facing environments, cutting median MTTR from 9.4 to 6.1 hours over 12 months at Nordstrom.
- Hands-on **detection engineering in Microsoft Sentinel, Splunk, and CrowdStrike**, adding 23 ATT&CK-mapped detections in KQL and SPL and lowering false positives by 38%.
- Runs a recurring **threat hunting** program across EDR and identity telemetry, converting 7 of 18 hunt hypotheses in 2025 into production detections.
- Vulnerability management in **Tenable and ServiceNow** with risk-based prioritization and remediation governance, lifting critical SLA remediation from 62% to 84%.
- Executive-ready reporting on **MTTD, MTTR, detection fidelity, and patch compliance**, automated with Python and standardized dashboards.
- **GCIH certified** (GIAC), with cloud and identity security experience across Azure, AWS, Entra ID, Okta, and Active Directory.

Experience

Senior Cyber Security Analyst — **Nordstrom**, national department store and e-commerce retailer

Jun 2022 – Present · 4 yrs 5 mos

- Led high-severity incident response across identity compromise, endpoint malware, and cloud access anomalies, cutting median MTTR from 9.4 to 6.1 hours over 12 months by formalizing containment checklists and tightening escalation criteria
- Designed and tuned detections in Microsoft Sentinel, Splunk, and CrowdStrike, adding 23 ATT&CK-mapped detections for credential abuse, lateral movement, and suspicious PowerShell, and cutting false positives on targeted use cases by 38%
- Built a recurring threat hunting program across endpoint and identity telemetry, completing 18 hunts in 2025 and converting 7 hypotheses into production detections by querying Defender for Endpoint, CrowdStrike, and Entra ID data
- Restructured enterprise vulnerability reporting with Tenable and ServiceNow, improving critical remediation within SLA from 62% to 84% across 3 cycles by segmenting findings on asset criticality, internet exposure, and compensating controls
- Automated executive reporting on MTTD, MTTR, detection fidelity, patch compliance, and phishing trends with Python, reducing monthly report preparation from 2 days to 4 hours

Sample resume made with Specific Resume · specificresume.com

Cyber Security Analyst — **Expedia Group**, a global online travel and e-commerce platform

Feb 2018 – May 2022 · 4 yrs 3 mos

- Led or co-led 41 medium-severity incidents in 2021, covering cloud and identity cases such as suspicious authentication, endpoint compromise, and anomalous AWS activity, with 95% of post-incident actions closed on schedule.
- Correlated evidence across Splunk, CrowdStrike, Okta, CloudTrail, and AWS Security Hub during investigations, and drove follow-up remediation with the owning service teams.
- Improved alert quality for cloud privilege escalation and suspicious OAuth activity by refining SPL logic, adding identity enrichment, and mapping use cases to MITRE ATT&CK techniques, reducing duplicate or nonactionable alerts by 34%.
- Supported vulnerability governance for externally exposed systems and critical application assets, cutting open critical findings older than 14 days from 47 to 19 over two quarters by prioritizing scanner output on exploitability and business impact and tracking exceptions in Jira.
- Partnered with engineering teams on AWS and Azure logging, IAM, and detection coverage to strengthen incident readiness across the platform.

Information Security Analyst — Alaska Airlines

Jan 2015 – Jan 2018 · 3 yrs

- Standardized SOC investigation notes and escalation criteria for recurring endpoint and phishing cases, building analyst templates and evidence checklists that cut documentation rework from 5 cases a month to 1.
- Helped coordinate remediation follow-up on Qualys scanner findings across user and server assets, reconciling results with asset owners and tracking overdue tickets, improving monthly closure of high-severity findings from 74% to 85%.

Education

- **Western Washington University** — Bachelor of Science in Computer Science · 2010 – 2014

Skills

- **SIEM & Detection Engineering:** Microsoft Sentinel, Splunk, Kusto Query Language (KQL)
- **EDR & Identity:** CrowdStrike, Microsoft Defender for Endpoint
- **Cloud Security:** Azure, AWS
- **Vulnerability Management & Automation:** Tenable, ServiceNow

Certifications

- **GCIH** – GIAC (2021)