JULIAN MERCER

INFORMATION SECURITY ANALYST

San Francisco, CA | (415) 555-0148 | julian.mercer@email.com | linkedin.com/in/julianmercer

PROFESSIONAL SUMMARY

Information Security Analyst with 6+ years monitoring enterprise environments, triaging alerts, and driving vulnerability remediation. Pairs disciplined detection work with clear risk communication so engineering teams fix the issues that matter first.

PROFESSIONAL EXPERIENCE

Senior Information Security Analyst Jan 2025 - Present
Okta, San Francisco, CA

- Built a risk-ranked remediation dashboard that engineering leads used to prioritize patching in sprint planning.
- Piloted automated phishing-report triage with a SOAR playbook, enriching 300+ reported emails monthly and freeing analysts for deeper investigations.
- Briefed the CISO's staff each quarter on open critical vulnerabilities, aging trends, and accepted risks to support remediation funding.
- Documented four incident timelines and lessons learned, helping close two recurring phishing-response gaps.

Information Security Analyst Mar 2023 - Dec 2024

- Monitored identity and endpoint telemetry in Splunk, triaging 140+ weekly alerts and escalating confirmed incidents within 20 minutes.
- Tuned 38 noisy detection rules against historical alerts, cutting false positives 41% without missing any red-team scenarios.
- Ran weekly Qualys scans across 2,400 assets and tracked critical findings, lowering median remediation time from 19 to 11 days.
- Reviewed access-log anomalies for privileged accounts each week, escalating six suspicious sessions with complete evidence.

Security Analyst Jun 2020 - Feb 2023
Cisco, San Jose, CA

- Investigated phishing and malware cases using CrowdStrike and email logs, resolving 92% of tickets within the SLA.
- Supported quarterly access reviews for 31 applications, revoking 220 stale accounts and documenting evidence for auditors.
- Partnered with IT operations to enforce disk encryption and MFA, raising endpoint compliance from 84% to 97%.
- Delivered monthly security awareness briefings to 600 employees, reducing simulated phishing click rates from 14% to 6%.
- Built an incident-response tabletop for 40 IT staff, exposing two escalation gaps that were fixed before the next audit cycle.
- Maintained a catalog of 45 documented detection use cases, giving analysts consistent triage steps and escalation paths.

CORE SKILLS

Security monitoring | Vulnerability management | Incident triage | Splunk | CrowdStrike | Qualys | Phishing analysis | Access reviews | MITRE ATT&CK | Log analysis | NIST CSF | Python scripting | Risk communication | Endpoint security

EDUCATION

B.S. in Information Systems, San Jose State University, San Jose, CA

CERTIFICATIONS

CompTIA Security+ | GIAC Security Essentials (GSEC)