Krish Patel Lead SOC Analyst

Foster City, CA · krish.patel@gmail.com · +1 650-555-0192 · linkedin.com/in/krishpatel

PROFILE SUMMARY

- **Lead SOC Analyst** bringing **11 years** of **payments security operations** at a **global card network and a digital wallet**, specializing in **incident command, detection engineering at scale, and PCI DSS audit evidence**.
- Leads a SOC built on SIEM (**Splunk Enterprise Security**), EDR (**CrowdStrike Falcon**), SOAR (**Tines**), threat intel (**Recorded Future**), and cloud telemetry (**AWS CloudTrail**), keeping every detection as **Sigma** in Git.
- Deep expertise in **detection-as-code**, **ATT&CK coverage measurement**, and **major incident command**, using **purple-team exercises** to prove which rules fire and **retiring the ones that never do**.
- Works with **fraud operations, IAM, cloud engineering, and the red team**, chairs the **weekly detection review**, and briefs the **CISO** each month on open incidents and ATT&CK coverage.
- Manages **9 analysts** in Foster City and Singapore, designed the **follow-the-sun handover** and the **SOC hiring loop**, and has coached **4 analysts** into senior roles.

TECHNICAL SKILLS

SIEM & Query Languages:	Splunk Enterprise Security (SPL, risk-based alerting), Microsoft Sentinel (KQL), Sigma, Splunk UBA
EDR & Endpoint Security:	CrowdStrike Falcon Insight and RTR, Microsoft Defender for Endpoint, Carbon Black, Sysmon
Threat Intel & Frameworks:	MITRE ATT&CK, Recorded Future, FS-ISAC feeds, MISP, Cyber Kill Chain
Incident Response & Forensics:	NIST SP 800-61, incident command, Velociraptor, KAPE, chain of custody, post-incident reviews
Network & Cloud Telemetry:	AWS CloudTrail, VPC Flow Logs, Google Cloud audit logs, Zeek, Okta, Microsoft Entra ID
Email Security & Malware Analysis:	Proofpoint, Microsoft Defender for Office 365, YARA, ANY.RUN, DMARC reporting
SOAR, Scripting & Case Management:	Tines, Splunk SOAR, Python, ServiceNow SIR, Jira, GitLab CI

EDUCATION

Stevens Institute of Technology — M.S. in Cybersecurity — Hoboken, NJ · Sep 2013 to May 2015

GIAC and ISC2 — GCIH and CISSP certifications — San Jose, CA · 2017 and 2020

WORK EXPERIENCE

Visa — Lead SOC Analyst — Foster City, CA · Apr 2021 to Present

- Ran incident command when a compromised contractor laptop reached a jump host, working with IAM and legal under NIST SP 800-61 to contain it **2 hours 41 minutes** after first alert.
- Rebuilt **Splunk ES** correlation searches around risk-based alerting, scoring ATT&CK-tagged events per user and host, which cut analyst-facing alerts by **58%** while catching every purple-team scenario.
- Brought **Recorded Future** and FS-ISAC indicators into Splunk and ran quarterly hunts for payment-sector threat actors, which found **2 dormant web shells** on an acquired company's servers before network integration.
- Built **Tines** workflows that enrich alerts with Recorded Future and asset data, then open ServiceNow SIR cases with the runbook attached, which gives analysts back **about 31 hours a week**.
- Led onboarding of **AWS CloudTrail** and VPC Flow Logs from 212 accounts into Splunk, so analysts could correlate cloud activity with Okta sign-ins, cutting cloud investigation time by **46%**.

PayPal — Senior SOC Analyst — San Jose, CA · Jun 2015 to Mar 2021

- Triaged account-takeover and insider alerts on the payments platform, then rewrote the severity matrix for the 24/7 queue, cutting wrong-severity escalations by **44%** in a year.
- Co-led the **CrowdStrike Falcon** rollout to PayPal laptops and servers, then used Real Time Response for isolation and IOC sweeps, cutting containment of an infected laptop to **11 minutes**.
- Owned the employee phishing queue in **Proofpoint**, adding header and URL checks plus automatic pull-back of confirmed messages, which cut report-to-purge time from 3 hours to **14 minutes**.