Kunj Patel

(551) 220-7637 | kunjp410@gmail.com | www.linkedin.com/in/kunjpatel410

Profile

Cybersecurity professional with 7+ years of experience spanning hands-on security engineering, security operations, and team management. Proven expertise in designing and implementing SOAR solutions to automate security workflows using Python and reduce risk exposure. Adept at AWS security controls, vulnerability management, identity and access management (IAM), and compliance with industry frameworks (HIPAA, SOC 2, PCI DSS, HITRUST, SOx, CyberEssentials Plus). Strong background in threat detection, forensic analysis, vendor risk assessments, and security automation. A proactive leader in improving security posture through vulnerability management programs, data loss prevention (DLP), threat intelligence integration, and security awareness training.

Experience

MANAGER, CYBERSECURITY | WW INTERNATIONAL, NY | APRIL 2025 - PRESENT

- Managed and mentored a team of security analysts and engineers, driving performance through structured goal-setting, regular 1:1s, and professional development planning.
- Led the evaluation, selection, and deployment of a Managed Detection and Response (MDR) solution, enhancing 24/7 threat monitoring and reducing mean time to detect and respond to security incidents.
- Consolidated overlapping security tools and eliminated redundant vendor contracts, reducing annual tooling costs while maintaining full coverage across detection, response, and compliance.
- Identified and retired legacy security infrastructure, replacing end-of-life systems with modern, API-driven platforms that improved integration and reduced operational overhead.
- Integrated AI-driven enrichment into the incident response pipeline, automating alert triage, contextual threat analysis, and recommended response actions, accelerating investigation time.
- Embedded AI capabilities into the vulnerability management program, automating risk scoring, asset-context correlation, and remediation prioritization across cloud environments.
- Conducted enterprise-wide risk posture analysis, identifying control gaps across cloud infrastructure, endpoints, and SaaS applications and prioritizing remediation by business impact.
- Led recurring risk assessments across business units, evaluating control effectiveness and producing executive-level risk reports for senior leadership and board stakeholders.
- Revamped the security awareness training program with AI-personalized phishing simulations and role-based training modules, improving organizational phishing resilience and reporting rates.
- Built executive security dashboards and reporting frameworks, providing real-time visibility into vulnerability trends, incident metrics, compliance status, and risk exposure across the organization.
- Drove cross-functional collaboration with IT, Engineering, Legal, and Privacy teams to embed security into business processes and product development lifecycles.

SENIOR PLATFORM SECURITY OPERATIONS ENGINEER | WW INTERNATIONAL, NY | OCTOBER 2023 – APRIL 2025

- Designed and implemented an AI-powered browser extension to detect unauthorized chatbot navigation, enforcing acceptable use policies for corporate AI.
- Developed a Gmail Add-on using Google Apps Script & AWS S3 to streamline phishing email reporting, cutting incident response time by 50%.

- Built a Gmail DLP solution to detect and prevent unauthorized data sharing, strengthening security controls and compliance.
- Deployed & managed Proofpoint CASB & CrowdStrike DLP to enforce DLP policies across cloud apps and endpoints.
- Developed a self-hosted JavaScript Integrity Monitoring tool using Python programming, mitigating Magecart-style attacks on payment pages, securing $10M+ in monthly transactions.
- Automated threat intelligence ingestion into security monitoring systems, improving proactive threat detection.
- Optimized incident response with SOAR & webhooks, reducing false positive resolution time by 70%.
- Developed a Slack-based SOC alerting app, improving security operations workflow efficiency by 50%
- Streamlined vendor risk assessments by automating security reviews within Jira workflows, increasing compliance efficiency.
- Created an automated access management dashboard, tracking policy adherence across security tools to reduce manual audits.
- Designed a password management compliance dashboard, automating policy enforcement monitoring.
- Implemented reCAPTCHA for fraud prevention, reducing bot sign-ups and financial risks.
- Developed removable media security controls, enforcing policy compliance and preventing unauthorized data transfers.

CYBERSECURITY OPERATIONS MANAGER | WW INTERNATIONAL, NY | MAY 2023 - OCTOBER 2023

- Led the deployment of open-source security tools (GoPhish for phishing simulations, OpenVAS for vulnerability management, and OpenSearch for log analysis), increasing security coverage by 50%.
- Managed IAM security controls, ensuring secure user provisioning and de-provisioning, reducing unauthorized access incidents by 80%.
- Integrated SailPoint, Okta, and Jira to automate offboarding security controls, reducing manual efforts by 90%.
- Developed a risk-based patch management framework, prioritizing critical vulnerabilities for remediation and reducing risk exposure by 35%.
- Conducted internal security awareness training, improving organization-wide security culture and phishing resilience by 60%.
- Enhanced cloud security monitoring by integrating AWS CloudTrail logs into centralized log analysis platforms, reducing incident detection time by 40%.
- Authored comprehensive security documentation, including network diagrams and security process workflows.

CYBER SECURITY ENGINEER | WW INTERNATIONAL, NY | MAR 2022 - MAY 2023

- Designed and implemented an automated vulnerability management pipeline, integrating Nessus, Jira, and Slack.
- Developed an automated compliance dashboard, providing real-time visibility into security control effectiveness, reducing compliance gaps by 40%.
- Built IAM governance policies, reducing excessive access risks and improving least privilege enforcement.
- Conducted forensic investigations on security incidents, leveraging AWS OpenSearch and CrowdStrike EDR.

- Developed an API-based security monitoring tool to detect unauthorized SaaS application usage, reducing shadow IT risks by 45%.
- Assisted in configuring AWS CloudTrail to ensure comprehensive logging and monitoring of all cloud activities.
- Developed detailed technical documentation, including network and data flow diagrams, to support security operations.
- Implemented real-time phishing detection and response strategies, integrating security tools with email security platforms.

IT SECURITY ANALYST | WW INTERNATIONAL, NY |MAY 2019 – MARCH 2022

- Led SIEM rule development and log correlation, improving threat detection capabilities by 35%.
- Developed a phishing simulation program, improving employee phishing awareness training, reducing phishing click rates, and improving email reporting metrics.
- Implemented an endpoint security solution, reducing malware incidents by 60%.Assisted in implementing, operating, and maintaining IT Security Controls, ensuring the protection of internal information systems and databases.
- Conducted risk assessments and security audits, ensuring compliance with regulatory frameworks and reducing audit findings by 50%.
- Led the planning, implementation, and execution of SIG tools for automating Business-to-Business (B2B) Security Questionnaires, reducing turnaround time by 30+ days and eliminating redundant resource utilization.
- Acted as the SME for MetaCompliance security awareness training and Active Directory tools (ADManager, ADAuditPlus), improving security training adoption.

Education (University Of Maryland, Baltimore County & Gujarat Technological University, India)

- M.P.S Cybersecurity Graduated May 2020
- B.E. Information Technology Graduated May 2018
- Certified AWS CCP, Cloud Audit Academy, AI Security & Governance & Ethical Hacking