Prajwal Kumar Pandey

Nepal prajwal5809@gmail.com +9779867454595 in/prajwalkpandey

SUMMARY

Security Engineer with expertise in cloud security, incident response, and threat hunting. Skilled in multi-cloud defense, automation, vulnerability analysis, and proactive threat mitigation using offensive and defensive strategies.

SKILLS

Cloud Platforms: Microsoft Azure, Google Cloud Platform (GCP), AWS, Salesforce

Cloud Security & Monitoring: Microsoft Sentinel, Defender for Cloud, Microsoft XDR/EDR, Entra ID (Azure AD), AWS CloudTrail, GCP Security Command Center, IAM

Network Security & Log Analysis: Firewalls, Security Event Log Analysis, Nmap, Wireshark, Nessus, OpenVAS

Web & Application Security: Burp Suite, OWASP ZAP, DVWA

Operating systems: Linux,Windows

Frameworks and Tools: Git, Docker, PowerShell, Python, Postman, Opensearch

EXPERIENCE

Cloud Security Engineer

Securigeek(Contract) **July 2025 - November2025**

- Developed end-to-end ITDR platform using open-source tools; researched, tested, and fine-tuned threat detection rules across Azure, Office 365, Salesforce, and ServiceNow.
- Simulated identity-based attacks to validate detection efficacy and strengthen security controls.
- Created SSPM checks for high-quality, proactive security controls.
- Built PowerShell scripts for CSPM audits aligned with CIS benchmarks.
- Managed Azure IAM, configured Conditional Access, MFA, risk policies, and PIM.
- Maintained clear technical documentation and collaborated with cross-functional teams to drive the security roadmap.
- Conducted Salesforce access mapping using Access Explorer: mapped users to profiles, roles, permission sets, object-level permissions, reports, dashboards, and all sharing types to identify direct and indirect access.
- Designed and deployed anomaly detectors in OpenSearch to identify unusual patterns in authentication and event logs, enhancing proactive threat detection.
- Developed identity analytics capabilities for the SaaS platform by aggregating and correlating MFA status, last-login activity, session patterns, and other behavioral signals to enable detailed analysis of both human and non-human identities.

Cybersecurity Consultant

DanpheLink(Contract) **March 2025 - July 2025**

- Delivered security consulting services to clients, covering SOC operations, incident response, and implementation of cybersecurity best practices.
- Created and facilitated cybersecurity training and workshops for technical and non-technical audiences.
- Led incident response for a brute-force malware attack, including detection, containment, eradication, and system recovery.
- Investigated and mitigated unauthorized SSH access by identifying persistence mechanisms (malicious files, cron jobs, rogue SSH keys) and enforcing SSH hardening measures.
- Handled an insider threat incident involving exposed Cloudflare tunnel and unauthorized MongoDB access; implemented access control, credential hygiene, and offboarding processes.
- Conducted forensic analysis, identified Indicators of Compromise (IOCs), and delivered stakeholder reports detailing root cause, timeline, and preventive recommendations.

Security Engineer - Incident Response

Stellar Computer Systems **August 2024 - January 2025**

- Lead end-to-end incident response and security monitoring in Azure-based environments, utilizing Microsoft Sentinel, XDR/EDR, Entra, and Recorded Future threat intelligence.
- Proactively detect, investigate, and mitigate security threats by analyzing SIEM (Microsoft Sentinel), Fortinet, and Palo Alto network logs.
- Improved team incident response times by 46.43%, reducing average resolution from 56 to 30 minutes, with personal average under 20 minutes.
- Collaborate closely with internal stakeholders and external vendors for incident escalation, containment, remediation, and post-incident reviews.
- Develop and enhance Standard Operating Procedures (SOPs) to streamline incident response workflows, ensuring faster and more consistent outcomes.

- Produce detailed True Positive (TP) reports to provide actionable threat intelligence for the SOC team and customers, enhancing threat visibility and response strategies.
- Continuously optimize detection, triage, and response processes to minimize operational overhead and improve the SOC's overall effectiveness and agility.

Mentorship
GAJABAR **May 2023 - July 2023**

- Successfully led the development of the "Gwitter" project using PHP, HTML, and CSS, demonstrating strong web development leadership
- Enhanced cybersecurity knowledge through intensive training on OpenVAS scans and SQL injection

EDUCATION

Bachelor in Computer Engineering
Institute of Engineering, Pulchowk Campus, Tribhuvan University • Lalitpur, Nepal • 2024

Major in Physics and Mathematics
Tilottama College • Butwal, Nepal • 2019

CERTIFICATIONS

Certified Azure Red Team Professional (CARTP)

Microsoft Certified: Azure Security Engineer Associate(Az-500)

Professional Cloud Security Engineer (GCP)

Microsoft Certified: Information Security Administrator Associate (SC-401)

Microsoft Certified: Azure Administrator Associate (Az-104)

Azure-900

Cloud Penetration Testing with Azure

DevSecOps with Azure

Hacking and Securing Docker Containers

ISC2 CC

Certified Network Security Practitioner (CNSP)

API Security Fundamentals

Foundations of Operationalizing MITRE ATT&CK v13

AWS Cloud Practitioner Essentials

PROJECTS

Salesforce Security Graph Visualization System

• Developed a graph-based security analysis tool using Neo4j and React to visualize complex Salesforce permission structures, enabling security teams to identify privilege escalation paths and detect access anomalies across 10+ object types

• Engineered a Python-based data extraction pipeline integrating Salesforce REST APIs to map relationships between Users, Profiles, PermissionSets, Roles, Groups, and Resources, processing 3000+ entities and 16 distinct relationship types

• Implemented risk-based user classification system (Global Admin/Privileged/Standard tiers) with interactive graph

visualization featuring collapsible legends, admin tier filtering, and real-time relationship inspection via hover tooltips

• Built modular architecture using hexagonal/ports-and-adapters pattern with abstract interfaces for Neo4j, Salesforce API, and token providers, enabling easy extensibility and OAuth migration path

• Created security tooling that transforms opaque permission models into queryable graphs, reducing access audit time and enabling rapid incident response for insider threat investigations

ACHIEVEMENTS

- Ranked among the Top 15 cybersecurity professionals in Nepal on LetsDefend.io.
- Secured Top 2 position in the LogPoint Capture the Flag (CTF) competition.
- Completed the 7-week Gajabaar Infosec Mentorship Program, focusing on hands-on security development.
- Served as an Advisor at IEEE LaunchPad, guiding students in cybersecurity and cloud security pathways.
- Speaker at the IT Club, Pulchowk Campus, delivering sessions on modern security practices.
- Trainer at DanpheLink Academy, teaching Blue Teaming with a focus on cloud security techniques and real-world scenarios.