SAMYAK GOEL

+91 9557657134 · samyakgoel5@gmail.com · Mumbai, Maharashtra

SECURITY ENGINEER

Hands-on cybersecurity professional with real-world experience in detection engineering, endpoint defense, and adversary emulation. Skilled at handling live client environments, writing detection logic (XQL), and engaging directly with vendor TAC teams. Currently operating as the go-to XDR specialist at a client site, aiming to become a CISO within the next 9 years.

SKILLS

Cortex XDR	Autopsy	Scripting (Python, Yara Rules)
XQL	kape	Wireshark
MITRE ATT&CK	Splunk	Recon-NG

PROFESSIONAL EXPERIENCE

Swan Solutions & Services Pvt Ltd. — Security Engineer

Mumbai, India | Mar 2025 – Present - Act as Cortex XDR resource at a client, handling endpoint protection and incident response - Led deep analysis of a real-world XDRbypass (PowerShell, AMSI bypass, COM injection), engaged Palo Alto TAC & Engineering - Authored 36+ custom XQL queries to support InfoSec reporting, real-time detection, and use-case automation -Coordinate directly with client's InfoSec Manager, AVP, and Service Desk; trusted as key escalation point - Provide technical validation, troubleshooting, and detection support across departments

CERTIFICATION

Palo Alto PCDRA (Detection & Remediation Analyst)

Focused on endpoint protection and detection within the Cortex XDR environment. Demonstrates ability to detect, investigate, and respond to threats using behavioral indicators, XQL queries, and policy tuning in enterprise-grade deployments. Reinforces applied understanding of real-time detection use cases and telemetry mapping.

ISC2 Certified IN Cyber Security (CC)

Successfully attained foundational knowledge and skills essential for an entry- or junior-level cybersecurity role through ISC2's Certified Cybersecurity certification. Proficient in key domains including Security Principles, Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts, Access Controls Concepts, Network Security, and Security Operations.

Foundations of Operationalizing MITRE ATT&CK v13

Certified by AttackIQ, demonstrating a comprehensive understanding of the MITRE ATT&CK framework, including tactics, techniques, and procedures (TTPs). Skilled in using tools like CAR, D3FEND, and Navigator for threat intelligence analysis, adversary emulation, and strengthening organizational security posture through effective defense strategies.

EDUCATION

Bachlors of Technology (B.Tech)

Lovely Professional University — 2020-2024
Computer Science and Engineering (CSE) — Jalandhar, India

Intermediate

Dayavati Dharamvira Public School — 2020
Non-Medical Sciences (PCM) — Bijnor, India