GOKUL CHAKKALAPARAMBIL SOMAN

Kochi, India

+91 9187379239 | gokulsoman98@gmail.com| linkedin.com/in/gokulcsoman

Summary

Experienced Cyber Security Analyst with 4+ years of hands-on SOC experience in 24/7 environments, specialising in Microsoft Azure Security, SIEM operations, incident response, and threat hunting. Proven experience investigating real-world security incidents using Microsoft Sentinel, Defender for Endpoint, and Splunk, supported by strong Azure cloud fundamentals and lab-based offensive security exposure. Actively developing red-team skills through custom-built labs, TryHackMe CTFs, and OSCP-aligned training, enabling a strong attacker mindset to improve defensive detection and response.

Professional Experience

CyberOne Ltd-Milton Keynes, UK

Security Operations Centre Analyst | November 2022 – October 2025

- Monitor, triage, and investigate security alerts across multiple client environments using Microsoft Sentinel and Defender for Endpoint.
- Act as escalation point for L1 analysts, performing deep-dive investigations and root cause analysis.
- Develop and tune KQL detection queries and analytics rules, reducing false positives and improving detection accuracy.
- Conduct proactive threat hunting mapped to MITRE ATT&CK techniques.
- Lead incident response activities including evidence collection, containment, and remediation guidance.
- Mentor junior analysts and contribute to SOC process improvements aligned with NIST and ISO 27001.

Impact:

- Improved incident response efficiency by 30% through SIEM tuning and automation
- Reduced false positives and improved analyst workflow consistency

KryptoKloud Ltd- Lincoln, UK

Cyber Security Analyst | April2022 - November 2022 (8 months)

- Operated in a 24×7 Security Operations Centre, performing real-time monitoring, triage, investigation, escalation, and reporting of security incidents across multiple log sources.
- Investigated threats using WithSecure EDR, Splunk, IDS, and network traffic analysis (packets, flows, sensors), including phishing emails, malicious domains, and IPs, recommending effective containment and blocking actions.
- Supported incident response and vulnerability management, assisting with prioritisation, patching activities, remediation documentation, and post-incident prevention measures.
- Collaborated with clients and CSOC management by tracking SOC metrics, providing incident updates, delivering technical guidance, and supporting security controls, documentation, and response processes using TheHive platform.

Key skills

- **Defensive Security:** Microsoft Sentinel, Splunk, Microsoft Defender for Endpoint, WithSecure EDR, Incident Response, Threat Hunting, MITRE ATT&CK, KQL, Phishing Analysis, IOC/IOA Analysis.
- **Azure & Cloud Security:** Azure VMs, VNets, NSGs, Azure Firewall, Azure Monitor, Log Analytics, Azure AD (Entra ID), RBAC, Key Vault, Storage Security, Site-to-Site VPN.
- **Offensive Security (Labs):** Nmap, Metasploit, Hydra, Burp Suite, Active Directory Attacks, Privilege Escalation, Windows & Linux Attacks.
- **Security Operations:** SIEM (Sentinel, Splunk), EDR (MS Defender, With-Secure), Log Analysis, Censornet for email security.
- **Tools & Platforms:** Virus total, Polarity, ANY.RUN, Whois Lookup, MX Lookup tool, dnslytics, Scamalytics, AbuseIPDB, URL Scanner.
- **Soft Skills:** Stakeholder Collaboration, Shift Work Flexibility, SOP Documentation

Education

University Of Hertfordshire, United Kingdom 2019-2021
Master of Science in Cyber Security with Advance Research

Mahatma Gandhi University, India 2016-2019
Bachelor of Science in Cyber Forensic

Certifications

- Certified Ethical Hacker v10[EC Council]
- AZ-500
- CrowdStrike Certification
- Microsoft SC-200 (Ongoing)
- With-Secure Certification
- Autopsy Basics and Hands-on

Projects & Research

- **Topic, A case study on Web Ransomware.**

Description: The case study focuses on ransomware attacks in web server through file uploaded vulnerability and that is shown by creating two real life scenarios to show the workflow of these ransomwares.

- **Symmetric-key algorithm for cryptography using music**

Description: This paper proposes an alternative to steganography by designing an algorithm for the encryption of text messages into music and its attributes.

- **IOT (Internet of Things) Theft detection using Raspberry Pi 3**

Description: In this project, we used image processing on live video and detect theft using motion and highlighting the area where motion occurred.

- Research paper on “Artificial Intelligence and Robotics”
- Research paper on “Cyber Security and Breaching of Data”
- Research paper on “Impacts occurred by the pandemic to the cyber world”

- ➢ **Azure Multi-Region Infrastructure & Security Project (AZ-104 / AZ-500 aligned). Hands-on Cloud Project**

Description: Designed and implemented a secure, cost-controlled, multi-region Azure environment simulating enterprise infrastructure across UK and US regions.

- Designed and deployed UK and US Azure environments using separate resource groups and VNets.
- Implemented Network Security Groups and Azure Firewall to restrict access to trusted IPs only.
- Configured Site-to-Site VPN for encrypted cross-region connectivity.
- Hosted applications using Azure Load Balancer and Traffic Manager for high availability.
- Enabled Azure Monitor, alerts, cost management, and resource locks.
- Implemented Azure File Sync for secure cross-region data synchronisation.

Tools&Tech: Azure VMs, VNets, NSGs, Azure Firewall, VPN Gateway, Load Balancer, Traffic Manager, Azure Monitor, Storage, File Sync

Outcome: Secure, resilient, enterprise-style Azure environment. Demonstrated real-world cloud security, networking, and monitoring skills

- ➢ **Offensive Security Training & Home Lab (Ongoing)**

OSCP-Aligned Training & TryHackMe Labs

- Agent Sudo, Hydra Lab, Mr Robot CTF
- Nmap Enumeration, Metasploit Exploitation
- Active Directory Attacks & Windows Privilege Escalation
- Custom-built home lab environments
- Windows Machine Attacks (Blue Team perspective)

Lab Setup: Built and attacked custom home lab environments to understand attacker techniques and improve detection & response capabilities.

Value to SOC: Strong attacker mindset, better detection logic, triage accuracy and threat hunting