ADYASA PRIYADARSANI

SENIOR ANALYST

Bengaluru, India | +91-9040525141 | adya018@gmail.com | Experience: 3 Years 4 Months | LinkedIn: linkedin.com/in/adyasa-priyadarsani

Cybersecurity Senior Analyst with 3+ years of experience in SOC operations, specializing in **Cloud Security (Azure/Entra ID)** and **XDR/SIEM engineering**. Proven track record of securing 1,000+ endpoints by automating threat detection using **KQL** and streamlining incident response workflows. Demonstrated success in reducing Mean Time to Respond (MTTR) by up to 35% through advanced log correlation and malware analysis aligned with the **MITRE ATT&CK** framework.

TECHNICAL SKILLS

SIEM & Analytics: Microsoft Sentinel (Advanced KQL), Rapid7 InsightIDR.
EDR/XDR Platforms: CrowdStrike Falcon, SentinelOne, Palo Alto Cortex XDR.
Identity & Cloud Security: Azure AD (Entra ID), Active Directory, Privileged Access Management (BeyondTrust).
Vulnerability Management: Qualys Guard (Prioritization & Remediation).
Threat Defense: Malware Analysis, Threat Hunting, Root Cause Analysis (RCA).
Frameworks & Tools: MITRE ATT&CK, ITIL v4, ServiceNow ITSM, SQL (Basic).

PROFESSIONAL EXPERIENCE

Senior Analyst – Cybersecurity
Capgemini Technology Services India Limited | Oct 2022 – Present

- **Incident Response & Investigation:** Led Level 2 investigations for complex security breaches, achieving 100% SLA compliance and reducing system downtime by **30%** through rapid containment strategies.
- **Advanced Threat Hunting:** Engineered custom **KQL queries** within Microsoft Sentinel to proactively hunt for persistence and lateral movement techniques across 1,000+ enterprise systems.
- **Process Optimization:** Conducted deep-dive **Root Cause Analysis (RCA)** and malware investigations that decreased recurring security incidents by **25%**.
- **Log Correlation:** Developed correlation rules across diverse telemetry (Firewall, AD, Endpoint) to detect sophisticated phishing and credential theft attempts.
- **Vulnerability Governance:** Coordinated vulnerability remediation using **Qualys**, collaborating with infrastructure teams to patch critical-rated assets and reduce organizational risk.
- **Leadership & Mentoring:** Upskilled a team of Level 1 analysts on advanced investigation workflows, resulting in a **40% improvement** in overall team operational efficiency.

CERTIFICATIONS

SC-200: Microsoft Certified: Security Operations Analyst Associate.
SC-300: Microsoft Certified: Identity and Access Administrator Associate.
SC-900: Microsoft Security, Compliance, and Identity Fundamentals.
ITIL 4 Foundation: IT Service Management

EDUCATION

Bachelor of Technology (B. Tech) – Computer Science and Engineering
DRIEMS Autonomous Engineering College | 2022

LANGUAGES

English | Hindi | Odia