AMEY S KULKARNI

Email – ameysk1996@gmail.com
Phone No- +91 7738103999

Profile Summary

✞A professional with 6 years of experience in **IT Cybersecurity, IT Audits, GRC practices, SIEM management**, **OT Cybersecurity**
✞ **Core member of the OT Security Team** and managed Cyber Security against the OT security framework; monitored teams for compliance; formulated policies & procedures for implementation of security controls, limiting information risk and leakages.

Core Skills

- Information Security, IT Cyber Security IT Audits and GRC practices, Knowledge of ISO 27001, MITRE Framework
- OT Cyber Security - IEC 62443.
- SIEM Operations and Management, VAPT- Nessus, Nets parker, Acunetix, Qualys, QVM, Nessus for OT
- IPS- McAfee IPS
- Threat Intelligence- Open-Source Threat Intelligence Platform Such as IBM X Force
- Online search Engines- avoid, Virus total, IPabuseDB, shodan.io

Work Experience

SIEMENS LIMITED, Navi Mumbai **Senior Executive – OT Cyber Security** **03/2023 – Present**

- Conducted OT Network Architecture review, process review, Gap Assessment, VTR based on standard IEC 62443.
- Experienced in Creating Cyber Security Policies and Procedures for OT Industries based on IEC 62443.
- Conducted Cyber Security Training program to Internal BU's as well as for Clients.
- Point of contact from OT Security team for responding RFP against cyber-Security compliance requirements.
- Preparation of Checklists based on SL, Product Compliance Assessment based on SL.

Yotta Infrastructure LLP, Navi Mumbai **Assistant Manager - GRC** **01/2023 – 03/2023**

- Conducted Phishing Simulations, Sent IS Awareness mailers Maintained and Prepared VAPT Assessment Calendar, Internal Audit Calendar for financial Year.
- Prepared Monthly Security Dashboard and Presented to Management

QualityKiosk Technologies Pvt Ltd, Navi Mumbai **Executive** **10/2021 – 12/2022**

- SIEM Management – Responsible to maintain track, incident follow ups with internal teams/ stakeholders till SOC incident closure which are received from MSSP team.
- Responsible for Monthly activity tracking and its Updates, Review of device coverage and its integration with SIEM. Preparation of Customized Monthly SIEM reports and presentation for security threat posture.
- Policy and Procedure Reviews – For Qulaitykiosk and for QK Clients
- Co ordination with External Auditors to understands Audit requirements.
- Infosec GRC - ISO 27001 readiness and implementation for different clients, experienced in conducting Internal audits across all business units of QK. Participated in Information security RFP/ POC, Information Security KPI and KRI
- User Awareness- Cybersecurity awareness mailer, Posters, Phishing Awareness Program, Infosec Awareness session for New Joiners
- Experienced in information security risk assessments and gap analysis. Ability to interface with internal and external clients, Monthly System Audits
- Responsible to communicate audit report/ audit finding to all internal departments from Infosec Team, Tracking of remediation of audit findings, compliance governance.

IBM, Mumbai **Service Delivery Specialist** **04/2021 – 10/2021**

- SOC Operations- Worked as L2 Security analyst.
- Experienced in handling Qradar SIEM. Log Source Integration to SIEM Platform and its Troubleshooting
- SIEM Use case creation and Its Fine tuning such as Rule Creation, deletion, Modification, Reports and Dashboards, SLA Tracking, Backup Process, Worked on SOC Change requests and Its Tracking, OSINT (IBM X force), Daily Health Checkup of SIEM Components. Response for Forensic investigations, event Investigations, Reviewed incidents raised by L1 engineers, AD hoc SOC Requests. Conducted VA on servers, Network devices Qradar Vulnerability manager along with VA report Preparation. Monthly review meetings.

WNS, Mumbai **Sr. Executive- Risk Management** **09/2020 – 03/2021**

- SOC Operations-Log monitoring of real time alerts on Qradar, Incident creation, follow ups & Closure within defined SLA.
- Documentation of incident investigation and case analysis for P1 Incidents.
- Worked on Report review Antivirus Reports, DLP reports, User activity monitoring reports and responsible to create incident depending upon observed activity. Engaged in continuous monitoring of Risk and UEBA platform "GURUCUL" for detection of user behavior analytics as well as potential anomalies.
- Monitoring of IPS dashboards and responsible to highlight observed suspicious events to resp team for mitigation of the same.

Inspira Enterprise India Pvt Ltd, Mumbai **Security Analyst** **06/2019 – 09/2020**

- SOC Operations-Worked in MSSP SOC. Experienced in handling Qradar SIEM, McAfee ESM.
- Real - Time Log monitoring from different devices such as Firewalls, IDS, IPS, Operating Systems like Windows, Linux, Proxy Servers, Windows Servers, System Application, Databases, Web Servers, and Networking Devices. Responding to real time alerts based on its priority and raising incidents to concern team.

SIEM Use case creation and Its Fine tuning such as Rule Creation, deletion, Modification, Reports and Dashboards, SLA Tracking, Backup Process, Worked on SOC Change requests and Its Tracking, Daily Health Checkup of SIEM Components. Log Source Integration to SIEM Platform and its Troubleshooting. Mining IOC campaigns from various opensource threat intel platform

- Investigation of cyber security advisories with the help of open-source threat intelligence platform.
- Upgradation of existing content packs to its latest version, Health check monitoring of SIEM devices as well as data sources which are integrated with SIEM. Report Creation – Monthly, Weekly. Preparation of PPT for monthly review

BDO India LLP, Mumbai **Assistant- RAS IT** **01/2018 – 06/2019**

- Process Audits - ITGC audits, Vendor Risk Assessment audit
- Security Auditing- Vulnerability Assessment and penetration testing.
- Documentation and presentation of security testing result to technical team. Provided technical understanding on remedial actions to be taken on identified vulnerabilities.
- Performed ISO 27001 Readiness Pre-Checks for Different Clients

Certifications

- Certified Ethical Hacker V 10-EC Council.
- Certified CCNA
- Certified ISO 27001:2013 LA- BSI Training Academy
- IEC 62443- IC 32 Trained & Certified, IC 33 – Trained
- Certified "ZCCA-IA"(Zscaler Certified Cloud administrator- Internet Access) - Completed Through Zscaler Portal
- Next Milestone- CISA

Education

BE in Electronics and Telecommunication Engineering from B.R. Harne College of Engineering & Technology, Mumbai University with 6.53 CGPA in 2017

Certifications

Title: UNDERWATER SENSORNETWORK (Border alert system for boat using piezo sensor)
This project describes and explores underwater application and challenges for underwater sensor networks. This project helps to advance military application, allow or scientific data Collection to predict natural disaster and also will helps in scientific Research.

Personal Dossier

- Date of Birth : 12 April 1996
- Permanent Address: B-202, Yashodeep Apartment, Gopal Nagar Road no. 2 Dombivli
- Nationality: Indian
- Marital Status : Married