Amey Vinay Kulkarni

Summary

Detail oriented and strategic professional with skilled expertise in Cybersecurity, Network Security and GRC. Outstanding planning, time management, communication and organization skills. Have supported big organizations by developing, implementing and maintaining complex projects.

Personal Details

Address: A803, Welworth Paradise, Baner, Pune - 411045
Contact: +917506484365
Email: ameyvkulkarni1990@gmail.com

Certifications

- **CEHv10 (License ECC36156068461)**
- **CompTIA Security + (License COMP001021384372)**
- **CCNA Security (License CSCO12991074)**
- **ISO 27001:2013 Lead Auditor**

Skills

- Footprint and Reconnaissance: Collection of information, Netdiscover
- Scanning of Network: Advance Port & IP scanner, NMAP/ZEMAP, Malware, Threat, Sniffing, DOS/DDOS attack, Phishing
- Cryptography and types, Vulnerability assessment, Enumeration
- Evading IPS, IDS, Firewall and Honeypots
- Security**:** Access Control List, AAA, DHCP snooping, Ip source guard, private VLAN, IP Security (IPsec), IPSEC VPN, SIEM.
- AWS Cloud: IAM, EC2, S3, VPC, Load-balancer, AWS WAF, CloudWatch & CloudTrail, Datadog

Experience

Deutsche Bank / Cyber Security Specialist

September 2023 - Present, Pune

- Proactively monitored the console for alerts using Google Chronicles, a robust SIEM solution.
- Conducted in-depth reviews and investigations of security incidents, including DOS/DDOS attacks, Malware, Phishing etc.
- Analyzed alerts from Rapid 7 InsightIDR, utilizing user behavior data analytics to identify and mitigate potential threats.
- Monitored EDR alerts on SentinelOne, implementing appropriate mitigation measures based on analysis.
- Implemented advanced methods for detecting and mitigating DDOS attacks, collaborating with Threat Management System Arbor for traffic cleaning during attacks.
- Conducted monthly vulnerability scans using Qualys VMDR to ensure PCI compliance.
- Prepared comprehensive Vulnerability Assessment reports and collaborated with relevant teams for timely remediation.
- Managed and fine-tuned threat prevention engines, including Anti-Malware, Anti-spyware, File block, and Vulnerability protection on firewalls.

- Administered AWS WAF to control web application requests based on IP addresses.
- Created, deleted, and modified firewall policies in response to customer requests.
- Managed network devices, including Juniper SRX, Palo Alto, and Checkpoint firewalls.
- Provided support for firewall-related requirements in various projects, ensuring end-to-end connectivity.
- Maintained meticulous documentation of network-related processes and configurations.
- Oversaw critical application, ensuring alignment with organizational goals.
- Provided detailed administrative information for IT Policies & Standards compliance.
- Managed application lifecycle gaps, addressing risks and ensuring compliance.
- Implemented swift responses to IT security incidents, mitigating risks effectively.
- Planned and managed application events, user access, and capacity for optimal performance.
- Coordinated infrastructure activities and upgrades, aligning with compliant platforms.

Accelya Kale Solutions Pvt Ltd/ Specialist - IT Security

January 2022 - September 2023, Pune

- Monitored console for alerts using SIEM Google Chronicles and carry out alert review.
- Reviewed Rapid 7 InsightIDR Alerts (User Behaviour data Analytic)
- Monitored EDR alerts on SentinelOne and taking appropriate mitigation measures.
- Performed monthly vulnerability scan via Qualys VMDR for PCI compliance
- Prepared Vulnerability Assessment reports and segregated to the concerned team for vulnerability remediation.
- Managed threat prevention engine like Anti- Malware, Anti-spyware, File block & Vulnerability on firewall
- Managed AWS WAF to allow or block web application requests via IP address.
- Created, deleted and modified firewall policy as per customer request.
- Managed network device like Juniper SRX, Palo Alto and checkpoint firewall on Gaia version R77 & R77.30

Cumulus Systems / Information Security Analyst (Security and Compliance)

August 2020 - August 2021, Pune

- Worked closely with key customers and design partners to understand their requirements. Suggest and implement solutions for improvement.
- Tracked of all these requirements and existing processes, offer solutions for implementation and improvement.
- Worked and supported the development team to implement these on the product.
- Understood the requirement for any logs monitoring and producing recommended cybersecurity use cases.
- Interpreted the raw logs from Security devices and interpret them as to what activity is going on in the logs.
- Defined Cybersecurity use cases for the Number of Security devices available in the Cybersecurity domain on different platforms for different customers.
- Monitored the detection and fine-tuning of use case conditions accordingly. Enhance the use cases by doing additional enrichment and correlation with cross data feeds.

Vodafone Intelligent Services (VOIS) / Cyber Security Analyst/ DDOS Protection

February 2019- August 2020, Pune

- Monitored offenses and take preventive measures to minimize threat over the environment using SIEM QRadar.
- Conducted security incident review and investigation for scenario/alert such as DOS/DDOS, Malware, Phishing etc
- Conducted DDOS detection and mitigation, and method used by Threat management system Arbor for cleaning traffic against DDOS attack.
- Created, deleted and modified firewall policy as per customer request.
- Performed firewall audits
- Performed risk assessment of various security devices
- Managed network device like Juniper SRX, Palo Alto and checkpoint firewall on Gaia version R77 & R77.30
- Managed threat prevention engine like Anti- Malware, Anti-spyware, File block & Vulnerability on firewall.
- Performed analysis of logs produced by network devices utilized within the infrastructure such as firewall, syslog from various sources/devices, directory services, DHCP logs.

GTT Communication / Tier 1 NOC Engineer

May 2017- January 2019, Pune

- Responded to tickets opened by routine alarms and network issues.
- Accessed specific customer process information to identify appropriate problem resolution procedure and contacts.
- Made initial outbound contact with customers to notify them of routine alarms and network.
- Worked with customers to perform troubleshooting of outages to determine if the issue is telecom, power, cabling, or equipment related.
- Assisted customers in identifying and resolving cabling and power issues.
- Updated ticket status in Network Operating Centre systems.
- Followed established internal escalation procedures to assign non-routine or equipment related tickets to higher-level customer support technicians
- Coordinated after-hours testing for customers. Arrange and communicate testing times to customer, NOC personnel and TELCO.
- Updated the NOC with temporary changes in customer notification procedure. Reports customer contact information errors to Lead Technician for customer.
- Displayed proficiency in the utilization of company systems and diagnostic tools.

Education

Auckland University of Technology, New Zealand/ PgDip in Electronic & Electrical Engineering (MAR-2015) - 65%

K.C College of Engineering, Thane/ B.E in Electronic and Telecommunication (May-2013) - 71%