AMAR SHRIMANTRAO KOKATE

CYBERSECUITY ENGINEER

Pune | kokateamar8@gmail.com | 9096989609 | https://www.linkedin.com/in/amar-kokate-9307a4227

SUMMARY

Dedicated Cyber Security Engineer with 2 years of hands-on experience in endpoint security solutions at Amazure Technology. Proven ability to implement and manage security measures to protect organizations from cyber threats. Possesses a Certified Ethical Hacker (CEH V12) certification that enhances technical expertise. Passionate about safeguarding sensitive information while optimizing security frameworks to meet business needs.

TECHNICAL SKILLS

- Security Incident Analysis & Reporting:
  - Incident investigation and analysis
  - Event log analysis and threat identification
  - Incident reporting and documentation
- Phishing & Threat Mitigation:
  - Phishing Email Analysis
  - Mitigation Strategies
  - Email Security Tools
- Endpoint Protection:
  - CrowdStrike
  - Trend Micro Apex One
  - Trend Micro Deep Security
  - Microsoft Defender for endpoint
- Compliance & Reporting:
  - Risk Mitigation,
  - Compliance Tracking
  - Vulnerability Management
- Security investigation Tool:
  - Virus Total for threat intelligence analysis
  - Cisco Talos Intelligence
  - AbuseIPDB for IP threat intelligence
- Security Concepts:
  - Endpoint Security
  - Firewall management
  - IDS and IPS (Intrusion Detection/Prevention Systems)
  - Cryptography
- Email Security Tool:
  - MX Toolbox,
  - Virus Total,
  - Hunter Mail Verify
  - Google Header Analysis
- Networking:
  - OSI Model
  - TCP/IP, UDP, SMTP, FTP
  - DNS
  - Network Topology

PROFESSIONAL EXPERIENCE

April 2023 - Oct 2023

Amazure Technology Pvt Ltd.
Balewadi, Pune
Cybersecurity Engineer Intern

- Assisted in the deployment and management of endpoint security solutions including CrowdStrike, Trend Micro Apex One, and Deep Security.
- Monitored and analyzed logs, events, and alerts to identify suspicious activity and respond to security incidents.
- Assisted with patch upgrade activities for various security solutions.
- Conducted initial investigations of phishing emails and provided recommendations for blocking suspicious domains and IP addresses.
- Collaborated with the IT and security teams to integrate security solutions with existing tools and processes.
- Provided support for application blacklisting and whitelisting efforts, blocking malicious URLs, IP addresses, and hashes.

Oct 2023 - Present

Amazure Technology Pvt Ltd.
Balewadi, Pune
Cybersecurity Engineer

- **Implemented and managed** endpoint security measures by deploying CrowdStrike, Trend Micro Apex One, Apex Central, and Deep Security to strengthen client security.
- **Monitored and analyzed logs,** events, and alerts detected in CrowdStrike, Trend Micro Apex One, DDI, DDAn, and Deep Security, proactively identifying suspicious activity and responding to security incidents.
- **Configured and troubleshoot** enterprise server & host security solutions including Deep Security, Trend Micro Apex One, Apex Central, and CrowdStrike.
- **Performed patch upgrad**e activities for Apex One, Apex Central, Deep Security Smart Protection Server.
- **Updated the latest agent versions** for CrowdStrike, Apex One, and Deep Security on a monthly basis to ensure enterprise security solutions are up to date.
- **Conducted detailed analysis of security incidents**, determining root cause analysis, impact, and appropriate remediation steps.
- Performed thorough analysis of endpoint data to detect anomalies, suspicious activity, and indicators of compromise (IOC).
- **Coordinated with local IT engineers**, providing guidance for installation, upgrades, uninstallation, and troubleshooting of security solutions.
- **Investigated phishing email** domains and IPs using open-source tools, providing recommendations for proper blocking based on analysis.
- **Applied device control policies** in CrowdStrike and Apex One, and maintained Mobile Device Management (MDM) including USB read and write execution lists.
- **Managed application blacklisting and whitelisting**, effectively blocking malicious URLs, IP addresses, and hashes.
- Escalated critical security incidents to technical leads.
- Uploaded and checked Indicators of Compromise (IOCs) in security solutions released by CERT-IN. Utilized Manage Engine as a ticketing tool to handle and track security incidents, ensuring efficient incident management and resolution.

EDUCATION

Bachelor of Science (B.Sc.)

Dr. Babasaheb Ambedkar Marathwada University, Aurangabad
2019

CERTIFICATIONS

Certified Ethical Hacking (CEH V12) – ECC4792851306

DECLARATION

I hereby declare that the information furnished above is true to my knowledge and record.

Place:
Date:

Signature
(Amar Kokate)