

Mokshal Mehta

✉ mokshalmehta8@gmail.com

☎ +91 9152552390

📍 Mumbai

🌐 <https://github.com/mokshal007>

🌐 <https://www.linkedin.com/in/mokshalmehta>

Career Objective

Aspiring cybersecurity professional with expertise in (SOC) security operations, incident response, and threat detection. Committed to leveraging advanced technologies to safeguard critical systems and data against evolving cyber threats.

Professional Experience

Investigation, Incident Response and management (IT Officer)

HDFC Bank (Jun 2024 - Present)

As an IT Officer specializing in Incident Response at HDFC Bank, I play a pivotal role in safeguarding the bank's critical infrastructure and ensuring the seamless operation of vital banking services. My responsibilities encompass:

Incident Response and Management:

- Led the resolution of nationwide P1 and P2 major incidents, minimizing disruptions to critical banking services, including UPI, Payment Gateways, Cloud, Databases, Servers, Networks, APIs, and SOA middleware
- Reported outcomes directly to the CIO, ensuring top-level visibility of incident management efforts.

Infrastructure Monitoring:

- Maintained continuous oversight of the bank's infrastructure and critical applications using advanced tools like Grafana, OEM, Elastic, Dynatrace, NewRelic, SPLUNK, Microsoft XDR, Network Node, AppDynamics, and Oracle Enterprise Management.
- Ensured the health and security of systems across India, proactively detecting and mitigating potential threats

Automation and Process Efficiency:

- Automated the periodic status reporting process with Power Automate, replacing a manual task conducted every 30 minutes.
- Significantly reduced manual workload, allowing the team to focus on strategic initiatives.

Collaboration and Process Improvement:

- Worked closely with cross-functional teams to enhance system monitoring capabilities and optimize performance.
- Contributed to the continuous improvement of incident response procedures, aligning them with industry best practices and regulatory standards.

Threat Mitigation:

- Deployed proactive security measures to protect against risks and downtime, ensuring uninterrupted banking operations.

Team Coordination and Preparedness:

- Conducted a comprehensive mock drill, effectively simulating a serious incident scenario to assess team readiness and response efficiency.
- Aligned team members, fostering collaboration and quick decision-making in high-pressure situations.

This role has enhanced my expertise in incident response, infrastructure monitoring, automation, and team coordination, preparing me to excel in challenging IT and cybersecurity environments.

Technical Skills

Programming Languages

Python, Java, SQL, Bash, HTML, CSS

Tools and Technologies

SIEM(Splunk), Microsoft Defender XDR, Firewalls, IDS/IPS(Snort), GCP, AWS, Maltego, nMap, Wireshark, BurpSuite,linux CMD , VM ware, VScode, Android Studios, Metasploit, Outlook, ServiceNow,Teams

Other skills

Raspberry pi, Linux OS, Windows OS, Networking, Network Security Protocols,Intrusion Detection, CIA traids, NIST, Compliance and Regulations, Risk Assessment and Management, Incident Response and Forensics, Cloud computing

Soft Skills

Adaptability, Teamwork, Continuous Learning, Business Acumen

Languages

English (IELTS 7.5 Bands), Hindi, Marathi, Gujarati

Projects

HoneyPot_with_SIEM_integration

- **Developed** a Python-based honeypot simulating SSH, HTTP, and FTP services to attract and monitor potential attackers.
- **Integrated** geolocation tracking to identify the geographical origin of incoming connections, enhancing threat intelligence and security analysis.
- **Implemented** logging, alerting, and notification features, including automated alerts to Discord for real-time incident response.
- **Successfully integrated** the honeypot with Splunk Enterprise Security (ES) for centralized log management, correlation, and analysis of security events.
- **Demonstrated** proficiency in cybersecurity, network monitoring, and threat detection techniques.

Spam Analysis Tool

- **Designed** and developed Sentinel, a command-line threat analysis tool utilizing machine learning models.
- **Supported** three main types of analysis: Malware Analysis, Email Spam Analysis, and URL Spam Analysis using ML algorithms.
- **Enabled** prediction of threats based on given inputs, providing insights into different types of cyber threats.

Keylogger



AutomatedKeylogger

- **Created** AutomatedKeylogger, an undetectable software application that captures and stores keystrokes,screenshots and webcam shots.
- **Implemented** advanced techniques to evade detection from security measures, ensuring the keylogger remains hidden within the operating system.
- **Automated** sending captured data to a Discord server for remote monitoring.

Education

2021 – 2024	Bachelors in Information Technology(BSC.IT)
Mumbai, India	<i>Jai Hind College/Mumbai University</i>
	Aggregate CGPA : 8.4

Certificates

- | | |
|---|--|
| • DefenceSOC_Splunk - SPLUNK ES  | • Cybersecurity foundations, network security, incidence response and threat detection, automation by Google  |
| • Working Towards CISSP and CCSP | |

extra-curricular

Completed SOC-L1 - Try Hack Me Active member of AntisyphonInfosec community