Abishkar Bharat Singh

CYBERSECURITY ANALYST

Phone: +91-8600658527 **Address:** Mumbai, Maharashtra, India **Website:** www.abishkarbharatsingh.com
Email: abishkarbharatsingh@gmail.com **LinkedIn:** https://www.linkedin.com/in/abishkar-bharat-singh/

Professional Summary

I am a cybersecurity Analysist with 4+ years of hands-on experience in SOC environments, specializing in incident detection, investigation, and response across diverse platforms, including Azure, AWS, and GCP. My expertise lies across XDR & EDR technologies such as Taegis, Microsoft Defender, Cybereason, CrowStrick, Trellix, Cisco Meraki.

Work Experience

UNHCR| FEB 2025 - Present

Phishing Email Analysis Workflow

When a user reports a suspicious email, we perform a comprehensive investigation that includes:

- **Sender Analysis:** Validate sender domain, email address, and originating IP.
- **Content Review:** Examine email body for malicious indicators, phishing language, or social engineering tactics.
- **Artifact Inspection:** Analyze embedded URLs, attachments, and QR codes for malicious behavior.
- **Header Analysis:** Check for anomalies in email headers such as spoofing or relay inconsistencies.

If the email is confirmed as suspicious or malicious:

- Block the sender's email ID and domain.
- Block identified malicious URLs.
- Delete the reported email from the user's mailbox.
- Escalate the email to Microsoft for further review.
- Apply protective measures on the user account, including forced password reset and MFA review.

Additional Steps for Lookalike Domains:

- If a cloned or impersonating website mimicking the organization's domain is detected, we apply the same investigative process and mitigation steps.

User Remediation Recommendations:

- Delete temporary files.
- Clear browser cache and cookies.
- Review MFA settings.
- Check for unauthorized browser extensions.
- Perform a full system malware scan.
- Change all stored passwords in browsers.

Post-Incident Account Audit:

- Review Azure AD sign-in logs and audit logs for suspicious IP activity.
- Investigate mailbox and account changes:
- Folder permission modifications.
- Inbox rule updates.
- User and application management activities.
- Check SharePoint, OneDrive, and Teams for unauthorized actions.
- Identify any suspicious outbound email activity, including bulk sends from user or shared mailboxes.

Cloud Security Checks

- **AWS:** Review GuardDuty and CloudTrail alerts to determine the nature of triggered events and validate user authorization.
- **Azure AD:** Analyze sign-in logs, audit logs, device codes, and MFA alerts for anomalies.
- **Microsoft Defender for Cloud:** Investigate alerts related to:
  - Role assignment changes.
  - VM, server, and database creation/deletion.
  - Load balancer, Storage account creation.
  - Network & Virtual security rules creation.
  - Network and firewall rule creation/deletion.
  - SQL injection attempts and other defender for cloud alerts.

Network Security (Meraki)

- Monitor traffic from corporate devices.
- Block unauthorized devices.
- Investigate inbound/outbound traffic anomalies.

Threat Detection (Taegis)

- Perform end-to-end alert analysis using normalized and raw data.
- Use advanced queries for deeper investigation.

Endpoint Management (Intune)

- Validate device ownership and enrollment details.
- Check installed applications and security posture:
- Malware status.
- Encryption (BitLocker).
- Secure Boot and Code Integrity settings.
- Take appropriate action on lost or compromised devices.

Takedown Requests

- For impersonation or fraud cases:
- **Email/Domain:** Coordinate with internal teams for takedown.
- **Websites:** Engage Digital Security Team for fraudulent site removal.
- **Social Media:** Work with Social Media Team to remove fake profiles.
- **Recruitment Fraud:** Notify HR for job-related impersonation cases.

Credential Theft Response

- When credentials are exposed:
- Notify affected users.
- Advise immediate password reset for all corporate and personal accounts.
- Provide guidance on securing accounts and monitoring for misuse.

Metro | March 2024 - Jan 2025

- Monitored real-time security across endpoints, networks and email systems to detect suspicious behaviours and potential threats and vulnerabilities.
- Configured and managed EDR and XDR tools and policies for malware detection, endpoint security, threat mitigation.
- In CrowdStrike, conducted root cause analysis on security incidents using process trees & tables, Events timelines, Graph, file executions, and network connections.
- Integrated threat intelligence to enrich alerts and enhance the detection of IOC, IOA and TTPs (Tactics, Techniques, Procedures).
- Implemented Data Loss Prevention (DLP) policies to prevent unauthorized exfiltration of sensitive data.
- In Cybereason, utilized timeline, process, communication, Threat Graph, Attack story, Evidence and response to track and visualize attack for comprehensive incident analysis and remediation.
- In Microsoft Defender 365, conducted in-depth security investigations using advanced querying tools like KQL for efficient correlation of multiple alerts.
- Conducted through investigations to evaluate and categorize security alerts, differentiating between true and false positives to ensure precise threat analysis.
- Managed whitelisting/blacklisting of applications to enhance endpoint and network security.
- Blocked malicious indicators (IPs, URLs, files) and isolating compromised system to prevent lateral movement and credential exploitation.