

Abishkar Bharat Singh

Cybersecurity Analyst | SOC & Incident Response Specialist

www.abishkarbharatsingh.com | abishkarbharatsingh@gmail.com | linkedin.com/in/abishkar-bharat-singh/

Professional Summary

Cybersecurity Analyst | SOC & Incident Response Specialist with 4+ years of cybersecurity experience and exposure across **enterprise, banking, UN, and large-scale environments**. Brings a strong combination of **SOC operations, incident response, security investigation, and cross-functional IT experience**, with a proven ability to adapt across diverse security environments and rapidly understand complex security incidents. **Recognized for strong analytical thinking, investigation skills, and a proactive approach to reducing cyber risk**. Passionate about threat detection, incident response, threat hunting, and continuously strengthening enterprise security posture.

Work Experience

Oct 2022 - Present

- Investigated and remediated phishing email based threats by analyzing email OR artifact inspection, sandbox detonation, and handled cloned or impersonating websites mimicking organizational domains and mitigation such threads.
- Led fraud, phishing and credential theft response efforts by notifying affected users and applications, enforcing password resets, providing security guidance, and coordinating takedowns of phishing domains, fraudulent websites, social-media impersonation, and recruitment scams.
- Analyzed and validated cloud security alerts across AWS and Azure by analyzing GuardDuty, CloudTrail, Azure AD sign-in, MFA/device code alerts, and audit log irregularities to confirm authorization and threat impact.
- Reviewed Microsoft Defender for Cloud alerts covering IAM role changes, Virtual machine lifecycle events, network and firewall configuration, load balances, storage accounts and SQL injection attempts.
- Performing advanced threat detection and root-cause analysis on malware alerts, leveraging raw/normalized logs, process trees, timelines and correlation queries to identify attack chains and containment actions.
- Ensured endpoint and network security posture through Intune and Meraki by validating device compliance (encryption, Secure boot, malware status), responding to lost or compromised endpoint, acting on threat-hunt reports, and blocking unauthorized network access.
- Strengthened security controls by configuring EDR/XDR/SIEM policies, firewall rules, allow/deny lists, application whitelisting/blacklisting, blocking malicious Ips and URLs, and implementing DLP controls to prevent data leakage.

Incident response

- Investigated suspicious web activity and identified malicious IP addresses, attack patterns, request paths, browser details, response codes, and policy violations, while supporting containment and blocking activities to mitigate threats.
- Analyzed deception and intrusion alerts to identify attacker behavior, unauthorized login attempts, exposed credentials, and indicators of compromise for further investigation and remediation.
- Triaged threat-intelligence alerts from Third Party and Regulatory by correlating malicious IPs, domains, URLs, hashes, vulnerabilities, and file paths & name, sender email id & Domain, CVE IDs to support incident investigation, threat validation, containment, and historical foot printing across enterprise environments.
- Investigated phishing campaigns, fake URLs, malicious domains, social media impersonation, fraudulent mobile applications, and brand abuse cases, while initiating takedown and remediation activities for confirmed threats.
- Supported fraud and social-engineering investigations involving fake call centers, impersonation attempts, malicious APKs, and credential-harvesting activities by collecting evidence, validating indicators, and supporting containment actions.

- Reviewed email security alerts, spam quarantine reports, suspicious email traffic, malware detections, and malicious attachments to identify potential threats, phishing indicators, and unauthorized communication attempts.
- Investigated data exposure and credential compromise incidents involving leaked credentials, API exposures, code repositories, compromised endpoints, personally identifiable information (PII), and payment-related data, while supporting password resets, session termination, endpoint scanning, and user-awareness activities to strengthen security posture and reduce organizational risk.

Key Achievements

- Demonstrated cross-functional IT expertise by successfully working across multiple roles, including **Citrix Administration**, **Asset Management Team Lead**, and **ServiceNow Testing**, developing strong expertise in infrastructure management, IT asset lifecycle management, and ITSM processes.
- Developed 5 **PowerShell** scripts to automate asset data extraction and centralize reporting, reducing manual effort by **15 hours** for a client and improving operational visibility. This contribution led to team recognition and my promotion as Asset Management tools lead.
- Developed automated **Microsoft Excel** solutions for client reporting and Asset Management inventory tracking, reducing manual effort by approximately **3.5 hours** and improving operational efficiency.
- Successfully developed an **Android application** as part of my MTech final-year project, demonstrating practical expertise in mobile application development.
- Designed and developed my personal portfolio website to showcase my professional experience, technical skills, blog and projects: **abishkarbharatsingh.com**
- Gained cybersecurity experience across diverse environments, including a **global enterprise**, **United Nations organization**, and **banking sector**, covering EDR operations, SOC monitoring, and Incident Response.
- Developed **AI-prompts** to streamline phishing email analysis and investigation, improving the efficiency and consistency of threat assessment.

Academic History

- Master of Technology – MTech, Computer System & Infrastructure | CGPA:6.89 | 2022-2025
- Bachelor of Science – Information Technology, Information | CGPA: 8.70 | 2018-2021

Certificate

SC-900, SC-300, SC-401, SC-200, AZ-500, CompTIA security+, CEH.

Key Skills

- **Cyber Skills:** CSIRT & SOC, Incident Detection, Analysis & Resolution.
- **Security tool:** Taegis, Microsoft Defender, CrowStrick, Cybereason, Trellix, SentinelOne, Qradar.
- **Cloud Infrastructure:** Azure, AWS, GCP, Defender for Cloud, Canary, Active Directory, Office 365.
- **Network Security:** Cisco Meraki, Firewalls, IDS/IPS, WAF.
- **Endpoint & Email:** Intune, Defender for Endpoint, Email & Web Security Gateways, Proxy & Entra.
- **ITSM:** ServiceNow, Jira, BMC Helix.
- **Digital Forensics:** Cloud Sek, RSA, iZoolabs.
- **Decoy:** Zscaler, F5.

to explore my background, profession, projects, and personal journey do visit my personal portfolio website and that is <https://abishkarbharatsingh.com/>