Abishkar Bharat Singh

CYBERSECURITY ANALSTS

+91-8600658527 | Mumbai, Maharashtra, India | www.abishkarbharatsingh.com
abishkarbharatsingh@gmail.com | https://www.linkedin.com/in/abishkar-bharat-singh/

Professional Summary

I am a cybersecurity analyst with over 4+ years of hands-on experience in Security Operations Center, Incident Response, and Infrastructure Security. Strong background in monitoring and analysing security events using EDR/XDR platforms, investigating phishing and malware incidents, managing endpoint and email security, and supporting network security operations.

Work Experience

Cybersecurity Analysts **UNHCR | Mar 2025 - Present**

Security Operations & Incident Response

- Investigated phishing and email-based threats using sender/domain validation, content and artifact analysis (URLs, attachments, QR codes), email header review, and sandbox detonation to identify spoofing, social engineering, and malicious infrastructure.
- Detected suspicious outbound email activity, including bulk or anomalous message sending.
- Additional, Cloned or impersonating website mimicking the organization's website & domain is detected follow the above same investigative and mitigation workflows.

Takedown for Fraud Response & Credential Theft Response

- Responded to credential exposure incidents by notifying users and application, enforcing password resets, and providing account-security guidance.
- Coordinated takedown efforts for phishing emails & domains, fraudulent websites, social media impersonation, and recruitment fraud.

Cloud Infrastructure Alerts & Network Security Monitoring

- **AWS:** Analyzed GuardDuty and CloudTrail logs to validate security events and determine the nature of triggered alerts and validate user authorization.
- **Azure AD:** Investigated sign-in anomalies, device code abuse, MFA alerts, and audit log irregularities.
- Reviewed Microsoft Defender for Cloud alerts covering role changes, VM/server/database lifecycle events, network and firewall rules, load balancers, storage accounts, and SQL injection attempts.
- Monitored Meraki network traffic, blocked unauthorized devices, and investigated anomalies indicating compromise or data exfiltration.

Threat Detection & Endpoint Security

- Conducted advanced threat analysis in Taegis using normalized/raw logs, process trees, timelines, and correlation queries to determine root cause.
- Validated endpoint security posture via Intune (enrollment, malware status, BitLocker, Secure Boot, code integrity) and took corrective action on lost, stolen, or compromised devices.
- Responded to Thread Hunt Report and take appropriate action on the affected machine.

Cybersecurity Analysts **Metro | Dec 2022 - Mar 2025**

- Monitored security alerts across endpoints, cloud, network, and email systems using tools like CrowdStrike, Microsoft Defender, Cybereason, and Trellix.
- Investigated and analyzed threats using process trees, timelines, threat graphs, and attack stories to identify root causes.
- Performed threat hunting and collaborated with SOC teams to improve detection capabilities and reduce false positives.
- Configured and managed EDR/XDR policies, firewall rules, and allow/deny lists to strengthen endpoint and network security.

- Blocked malicious indicators (IPs & URLs), contained compromised accounts, and implemented DLP controls to prevent data leakage and unauthorized access.
- Conducted in-depth security investigations using advanced querying tools like KQL for efficient correlation of multiple alerts.
- Managed whitelisting/blacklisting of applications and implemented firewall policies to enhance endpoint and network security.

ServiceNow Tester **TC Energy | Sep 2022 - Dec 2022**

- Created and maintained test documentation, including test plans and test cases for SAM Pro modules.
- Identified, reported, and tracked defects while collaborating with development teams for resolution.
- Tested Service Catalog forms, workflows, and multiple ServiceNow products to ensure functionality and performance.
- Worked with core ServiceNow components such as applications, modules, Service Catalog items, update sets, custom tables, and import sets.
- Developed and configured platform features including UI Policies, Data Policies, UI Actions, ACLs, workflows, business rules, script includes, client scripts, and notifications.

Asset Management **ABB | Dec 2021 - Sep 2022**

- Managed global asset and accessory inventories using Barscan and HPAM across 85+ countries (APAC, USA, Europe).
- Administered users, catalogs, assets, locations, Model and hardware models, maintaining accurate inventory and ownership records.
- Handled full device lifecycle management (allocation, repair, retirement) using manual and bulk updates, including warranty and retirement scheduling in HPAM.
- Executed asset and accessory migrations between tools, ensured data integrity, and generated daily exports, backups, and compliance reports.
- Managed asset purchasing workflows and resolved asset-related issues raised by OSS and FSM teams.

Citrix Administrator **ABB | Oct 2021 - Dec 2021**

- Managed Citrix Workspace user access by provisioning application and server permissions, troubleshooting access and VDI performance issues, and supporting the migration of dedicated VDIs to cloud infrastructure.

Academic History

Birla Institute of Technology and Science, Pilani | 2022-2025
Master of Technology - MTech, Computer System & Infrastructure | CGPA: 8.0

University of Mumbai | 2022-2025
Bachelor of Science - Information Technology, Information | CGPA: 8.70

Key Achievements

Best Team Award| 2022

Created 5 Automation to increased productivity | 2022

Key Skills

TAEGIS | MS DEFENDER | CYBEREASON | CROWSTRICK | TRELLIX | DEFENDER CLOUD | Azure | AWS | GCP | MERAKI | INTUNE | CANARY | SERVICENOW | JIRA | CITRIX | AZURE VDI | BARSCAN | HPAM | POWERSHELL | AWS WORKSPACE | OFFICE | for more details visit website .....
