SHUBHAM RAJENDRA BIRARI

SOC ANALYST

+91 9527981464
shubham22birari@gmail.com
www.linkedin.com/shubham birari

OBJECTIVE

Dedicated and results-oriented professional with experience in monitoring security events, conducting investigations, and implementing proactive defense measures to mitigate risks. Pursuing a challenging role to leverage expertise in threat intelligence, automation, and continuous security improvement, aiming to contribute to a dynamic Security Team while enhancing organizational resilience against cyberattacks.

EDUCATION

2021
B.E. in **Information Technology** from **Zeal College of Engineering, Pune**

2018
Diploma in **Computer Technology** from **Sanjivani KPB Polytechnic, Kopargaon**

CORE COMPETENCIES

- Incident Management
- Phishing Detection
- Information Security Management
- Threat Detection & Analysis
- Endpoint & Network Security
- Cyber Threat Intelligence
- Risk Assessment and Mitigation

SOFT SKILLS

- Collaborator
- Communicator
- Planner
- Critical Thinker
- Problem Solver
- Team-oriented

PROFILE SUMMARY

- Possess **over 3 years** of rich experience in **cybersecurity**, focusing on **incident response and security operations to protect sensitive data.**
- Currently working as SOC Analyst at Allianz Technology, **leveraging threat detection, incident management, and forensic analysis to protect enterprise environments** from evolving cyber threats.
- Developed a profound understanding of various security tools and technologies including, but not limited to, **Proxy, EDR, SIEM, IDS, IPS, Email Security, Zerofox, Blueliv**.
- Displayed exceptional performance in the current role by **managing and resolving more than 50 security incidents each month**, ensuring robust security measures were upheld.
- Displayed expertise in managing **threat intelligence and conducting thorough security investigations**.
- Exhibited proficiency in leveraging a diverse array of security tools and technologies, including **FireEye and Bluecoat Proxy**, to conduct comprehensive investigations and analyses of security incidents.
- Passionate about continuous learning in the evolving landscape of **cyber threats, attack vectors, and defense mechanisms**.
- Skilled in **real-time threat monitoring, log correlation, and event analysis** to identify security incidents.
- Experience in **escalation management, incident lifecycle management, and root cause analysis** to minimize risks.

TECHNICAL SKILLS

- **SOC Services:** Cofense, Log Analysis, Bluecoat Proxy, ADC, IDS/IPS
- **FireEye (Advanced Malware Detection):** Callback, Malware Binary, Malware Object, Domain Match, Malicious URL Proxy/Firewall
- **Endpoint Security Tools (EDR):** Cynet, CrowdStrike Falcon
- **SIEM Tools:** ArcSight
- **Ticketing & Incident Response Tools:** ServiceNow, Archer, SOAR (Security Orchestration, Automation, and Response), JIRA

ACHIEVEMENTS

- Implemented measures **reducing data breaches by 40%,** enhancing cybersecurity.
- **Earned multiple awards (RNR, Bravo) for excellence** in cybersecurity operations.

CERTIFICATION

- Certified Ethical Hacker (CEH v12) from EC-Council

WORK EXPERIENCE

Feb 2022 – Present | SOC Analyst| Allianz Technology, Pune

Key Result Areas:

- Monitoring, analyzing, and responding to security incidents by investigating alerts from firewalls, intrusion detection systems, SIEM platforms, and antivirus tools.
- Conducting in-depth investigations of security breaches, phishing emails, suspicious domains, and malicious IPs using open-source intelligence tools, recommending appropriate mitigation strategies.
- Operating in a 24/7 Security Operations Center (SOC), ensuring continuous threat monitoring and rapid incident response.
- Identifying and analyzing suspicious/ malicious activities, providing recommendations for remediation to strengthen cybersecurity posture.
- Investigating and resolving incidents involving unauthorized access to sensitive data, mitigating potential risks.
- Collaborating effectively within a team environment, offering support, knowledge sharing, and guidance on security best practices.
- Maintaining efficiency in task management, ensuring timely completion of incident investigations and security analyses.
- Proactively identifying security issues, analyzing threats, and implementing solutions to enhance organizational cybersecurity defenses.
- Developing and fine-tuning custom detection rules to identify evolving threats and anomalies.
- Monitoring and analyzing DNS traffic, proxy logs, and endpoint behavior for hidden threats.
- Managing and optimizing threat intelligence feeds to enhance proactive defense.
- Documenting and maintaining detailed post-incident reports, lessons learned, and security playbooks.

PERSONAL DETAILS

Address	:	Pune-411014, Maharashtra, India
Date of Birth	:	22nd June 1998
Languages Known	:	English, Hindi, and Marathi