Shrikrishna Khambe

Cyber Security Analyst

OBJECTIVE

Cyber Security Analyst with over 3 years of successful experience in identifying, assessing, and responding to cyber threats and able to collect and analyze data from various sources, such as logs, network traffic, malware samples, and threat intelligence reports, to find patterns, anomalies, and indicators of compromise. Recognized consistently for performance excellence and contributions to success in Wipro Limited industry. I explore new trends to develop effective solutions and am dedicated to teamwork to achieve organizational goals.

EXPERIENCE

Cyber Security Analyst at Wipro
March 2022 - Present

Incident Monitoring and Security Analysis in Shared domain (Working with 3 clients)

- **Incident Monitoring and Analysis:** Vigilantly monitor and analyze security incidents to protect sensitive data and critical systems, ensuring compliance with organizational and regulatory standards.
- **Working in SOC (24x7)**, monitoring SOC events, detecting and preventing intrusion attempts.
- **SIEM Tools Utilization:** Leverage advanced SIEM tools such as Splunk , QRadar and Securonix for real-time threat detection and incident response, enabling proactive identification of security threats.
- **Log Analysis and Incident Investigation:** Conduct thorough log analysis and incident investigations to identify potential threats and vulnerabilities, determining root causes and impacts to facilitate effective remediation.
- **Root Cause Analysis Reporting:** Prepare detailed root cause analysis reports that document findings and insights from security incidents, contributing to the continuous improvement of security measures

CONTACT

khambeshrikrishna@gmail.com
(+91)7756855356
www.linkedin.com/in/shrikrishna-khambe
Pune.

EDUCATION

-2017 - 2021 B.TECH IN COMPUTER ENGINEERING at **RAJARAMBAPU INSTITUTE OF TECHNOLOGY** (GPA:7.49)

-2017 Class 12th (80%)

-2015 Class 10th (91.80%)

SKILLS

- Environment:SOC(Security Operation Center)
- SIEM Tools: Splunk, Qradar, Securonix, Sentinel
- Primary SIEM: Splunk and Qradar
- Firewall: Checkpoint
- Ticketing Tool: Service Now
- Endpoint Security: Crowd Strike
- SOAR
- Proxy- Zscaler
- Communication
- KQL
- Python, C

CERTIFICATIONS and COURSES

- **Metrics Review:** Analyze daily, weekly, and monthly security reports for trends and anomalies, informing strategic decisions to enhance security posture
- **Ticket Management:** Create and manage tickets in ServiceNow for effective incident tracking, ensuring timely resolution and communication with relevant teams.
- **SOC Operations Engagement:** Participate actively in SOC operations, performing log and event analysis to improve incident response capabilities and enhance overall security operations.

- **Incident Remediation:** Track and follow up on incidents to ensure timely resolution, collaborating with cross functional teams to uphold security best practices
- **Security Tools Expertise:** Utilize a comprehensive understanding of security tools, including anti-virus solutions, IDS/IPS, firewalls, and vulnerability management systems
- **IOC Management:** Manage Indicators of Compromise (IOCs) using CrowdStrike EDR, facilitating swift incident response and threat management.
- **Cross-Functional Collaboration:** Collaborate with various teams to ensure effective incident response and adherence to security best practices across departments. (Like Firewall, Admin or Client Team)
- **Continuous Improvement Initiatives:** Contribute to the enhancement of security processes and procedures, fostering a culture of security awareness and resilience.
- **Documentation and Training:** Develop and document comprehensive user guides and training materials to empower team members and new joiners in effectively utilizing security features(SOP, Playbook,Trackers and Analyzing daily ,weekly and monthly reports on incident metrics update and close).

- SC-900
- Sentinel Training
- Microsoft Security Operations Analyst.
- 300 Certified SNYPR Security Analyst .
- Cortex XSOAR: SOAR,Analyst Training.
- Junior Cyber Security Analyst Path
- The Fundamentals of SOC.
- C
- Python