Akshay patalbansi

SOC Analyst Techowl Infosec

KEY HIGHLIGHTS

Proactively detected threats through continuous event monitoring and Triage.
Investigated and classified security alerts for rapid response.
Mitigated intrusion attempts, ensuring a secure environment.
Monitored events from various sources for comprehensive threat analysis.
Responded swiftly to suspicious emails, enhancing security measures.
Collected and reviewed threat intelligence for proactive defense.
Optimized SIEM rules for accurate threat identification.
Contributed to maintaining a 24x7 security operations center for continuous vigilance.

CERTIFICATIONS

EC-Council-Network Defense Essentials

Incident Response Lifecycle

EDUCATION

Bsc. Completd from Gadge baba Amravati university.Maharashtra

Pursuing MSCCS cybersecuirity

Email Id: Patalbansiakshay6@gmail.com
Contact No:7020148227

Professional Summary

Results-driven SOC Analyst with a proven track record in monitoring, triage, analysis, and swift response to security incidents. Proficient in leveraging industry-leading tools like SIEM, IDS/IPS, Firewall, AV/EDR, Email Gateway, and Web Proxy for effective cyber threat detection and mitigation. Notable expertise in conducting in-depth investigations, implementing robust security measures, and collaborating with cross-functional teams to fortify organizational defenses. Known for fostering collaboration, I excel in working with fellow security professionals to elevate the overall security posture of organizations. Adept at preserving the integrity of networks and systems, I am committed to staying abreast of emerging security trends.
Seeking to apply my skills and experience in a challenging SOC Analyst role within a dynamic cybersecurity team.

SKILLS

- **SIEM**-Splunk, Fortisiem,ELA event log analyzer
- **EDR**- Crowdstrike,
- **Firewall**- Palo alto
- **Email Gateway**-Symantec
- **Web Proxy**- BlueCoat,
- **Web Application Firewall**- Imperva,
- **Anti-Malware** - Symantec Endpoint, McAfee
- **IDS/IPS**- Tipping point, McAfee
- **Ticketing Tools**-Remedy Smart IT
- **Malware Analysis**-Wireshark, McAfee ATD, Anyrun, Hybrid Analysis
- **Threat intelligence**-Recorded Future, Anomali

Experience

SOC Analyst Techowl Infosec 2022 june- Present

- Conduct proactive monitoring and efficient triage of security events.
- Investigate all security alerts, utilizing tools and log files to differentiate whether the event is a false positive or a security incident.
- Recognize potential, successful, and unsuccessful intrusion attempts and compromises through reviews and analyses of relevant event details and summary information.
- Monitor diverse security events and logs (Proxy, IPS/IDS, Firewall, Email, Anti-Malware, Endpoints, Web Application Firewall) for situational awareness.
- Investigate reported suspicious emails, categorize them, and respond to users with findings and recommendations.
- Collect and analyze threat intelligence feeds, investigating potential Indicators of Compromise (IOCs).
- Identify, ingest, and manage IOCs in applicable security controls.
- Review and enhance detection coverage of IOCs, collaborating with vendors or internal teams.
  Develop SOC monitoring use cases to proactively detect emerging threats.
- Fine-tune SIEM rules to minimize false positives and eliminate false negatives.
- Update incident response playbook for effective cybersecurity readiness.
- Monitor the health of security sensors and SIEM infrastructure.