JAGRUTI GADEKAR

1jagrutigadekar@gmail.com

7767896558

Pune, India 411045

EDUCATION

Bachelor of Engineering

Pune University, Pune, May 2020

LANGUAGES

English

Advanced (C1)

Hindi

Advanced (C1)

Marathi

Advanced (C1)

PROFESSIONAL SUMMARY

I have overall 3 years of experience in IT as a Security Researcher and Analyst. I would love to work in a company where I can utilize my skills and improve my career path.

Specialized in proactive network monitoring of SIEM (Splunk)/Azure Sentinel and EDR Carbon Black. Have a deep knowledge of identifying and analyzing suspicious events.

Proven track record of improving security posture through incident response, threat hunting, and continuous process enhancement. Seeking to contribute expertise in a dynamic cyber security team.

SKILLS

- SIEM - Splunk Es, Azure Sentinel
- Incident response, Detection, and Investigations
- EDR - Carbon Black, Crowd Strike, Microsoft 365 Defender.
- Firewall - Cisco ASA, Palo Alto, FortiGate & Cloud Flare WAF.
- Knowledge of MITTRE ATTACK Framework and attack trends
- Open Source Intelligent Tools: VirusTotal. IPvoid, AbuseIP, URLsc Cisco Talos, URLvoid
- Security operations | Endpoint Security - McAfee ePO | Symantec
- Familiarity with security technologies, including firewalls, IDS/IPS, and endpoint protection.
- Knowledgeable about cyber securi frameworks, compliance standard and best practices.

WORK HISTORY

June 2021 - Current
Birlasoft Limited - SOC Analyst, Pune, India

- Working in Security Operation Centre (24x7), monitoring SOC events, detecting and preventing intrusion attempts.
- Splunk ES / Azure Sentinel & Carbon Black EDR, Working on monitoring of alerts, analyzing, coordinating with concerned teams with remediation steps and triaging them as True positive and False Positive .
- Monitoring, analyzing, and responding to infrastructure threats and vulnerabilities. Collecting the logs of all the network devices and analyze the logs to find the suspicious activities.
- Monitored and analyzed security events using SIEM tools, detecting and responding to potential security incidents promptly and effectively.
- Investigate malicious phishing emails, domains and IPs using Open Source tools and recommend proper blocking based on analysis. Continuously

monitoring and interpreting threats using the IDS and SIEM tools.

- Perform Malware Analysis by Static and Dynamic methods to identify the malicious IOCs-indicator of compromise, taking action around IOCs identified.
- Performing real-time Monitoring, Analyzing, and Investigating of logs with Reporting, Escalation and resolve of various Incidents/Events/Security Alerts triggered in SIEM tool from multiple log sources.
- Conducted thorough investigations of security incidents, identifying root causes, and implementing preventive measures to avoid future occurrences.
- Collaborated with cross-functional teams to develop and refine incident response procedures, ensuring efficient handling of security breaches.
- Participated in regular security assessments and vulnerability scans to identify potential weaknesses in the infrastructure, taking proactive steps to remediate vulnerabilities.
- Led threat hunting activities, proactively seeking out hidden threats and suspicious patterns in network and system data, enhancing overall threat detection capabilities.
- Assisted in the implementation and tuning of security tools, such as intrusion detection/prevention systems and firewall rules, to enhance the organization's defense mechanisms.
- Generated comprehensive incident reports detailing incident analysis, containment, eradication, and lessons learned for continuous improvement.
- Mentored junior analysts, providing training on incident analysis, threat intelligence, and response best practices.
- Collaborated with external incident response teams to manage and mitigate high-impact security incidents, minimizing the potential damage and financial losses.
- Participated in after-action reviews and debriefings to identify areas for improvement in incident response processes and communication.
- Assisted in the development and maintenance of security policies, procedures, and guidelines, ensuring compliance with industry standards and regulations.
- Contributed to the development of custom correlation rules and signatures to enhance detection capabilities specific to the organization's environment.
  - Actively monitored threat intelligence sources to stay informed about the latest attack vectors, vulnerabilities, and emerging threats.
  - Worked closely with network and system administrators to implement security controls and configurations that aligned with best practices.
  - Conducted periodic security awareness training for employees to educate them about common threats, phishing attacks, and security best practices.
- Actively monitored threat intelligence sources to stay informed about the latest attack vectors, vulnerabilities, and emerging threats.

CERTIFICATIONS

Qualys- Certified Endpoint Detection & Response
SC-200 - Microsoft Security Operations Analyst