Hyderabad , India 500016 | 8919055669 | divyasrinivasarao789@gmail.com

DIVYALAXMI SRINIVASARAO

SUMMARY

Proactive and detail-oriented SOC Analyst with 3+ years of experience monitoring, analyzing, and mitigating cybersecurity threats.
Skilled in using Splunk SIEM and SentinelOne EDR/XDR to detect and respond to security incidents. Proficient in investigating firewall, IDS/IPS, and proxy logs, focusing on identifying lateral movement, command-and-control activities, and persistence. Strong communicator with a passion for enhancing an organization's security posture.

EXPERIENCE

SOC ANALYST 12/2022 to Current
CA Technologies

• Monitored and analysed security alerts using Splunk SIEM and Azure. Sentinel, ensuring swift incident detection and response.

• Investigated firewall, IDS/IPS, and proxy logs for suspicious activities. including lateral movement and unauthorised data access attempts.

• Handled endpoint threats with SentinelOne EDR/XDR and Microsoft. Defender, mitigating ransomware, malware, and phishing attacks.

• Responded to advanced threat alerts, such as scheduled task creations, new. Process executions**,** and registry modifications.

• Conducted vulnerability assessments using industry-standard tools. Collaborating with IT teams to remediate risks.

• Coordinated with incident response teams to contain and resolve cloud-related issues. security threats via Defender for Cloud and O365 Defender.

• Analysed endpoint activity, detecting unauthorised persistence techniques. and malware activity.

• Provided first-level triage for security incidents, escalating complex cases to senior analysts.
• Track activities such as PowerShell commands, registry changes, and fireless. Malware behaviour.

• Monitor Windows, Active Directory, and Linux authentication logs for failures. Logins, privilege escalations, or lateral movement attempts.

• Monitor web proxy logs for unauthorised web access, malware-hosting. Domains, and anomalous outbound traffic.

• Identify and block access to malicious websites, and suspicious IPs.
• Analysed PowerShell-related alerts, new process creation, and unauthorised access. Lateral movement attempts.

• Investigate traffic patterns in firewall logs to identify unauthorised. Access, port scans, and unexpected data exfiltration attempts.

JUNIOR SECURITY ANALYST 10/2021 to 11/2022
Cybage Software Private Ltd

• I monitored and analysed security events using Splunk SIEM.
Identify potential threats.

• We investigated and mitigated endpoint security incidents with SentinelOne.
EDR, including malware containment and lateral movement prevention.

• Performed advanced threat detection and response using O365 Defender.
Addressing phishing, spam, and ransomware incidents.

• Conducted proactive log analysis of firewalls, IDS/IPS, and proxy logs to.
Identify suspicious activities and potential breaches.

• Continuously monitor and analyse logs from multiple sources, including.
firewalls, IDS/IPS, proxy servers, antivirus, email gateways, and DLP solutions.

• Responded to phishing and business email incidents using O365 Defender.
Reducing email-based attacks.

• Proactively analysed firewall, IDS/IPS, and proxy logs to identify anomalies.
and suspicious activities.

• Investigate traffic patterns in firewall logs to identify unauthorised access, port.
Scans, and unexpected data exfiltration attempts.

• Analyse intrusion detection and prevention system logs for potential threats.

SKILLS

- **SIEM Tools:** Splunk SIEM, Azure Sentinel, SOAR, and Qradar
- **Cloud Security:** Microsoft Defender for Cloud, O365 Defender for Emails
- **Threat Analysis:** Lateral Movement, Command and Control, Persistence detection
- **Endpoint Security:** SentinelOne EDR/XDR, Microsoft Defender for Endpoints
- **Log analysis:** firewall, proxy, IDS/IPS logs, AV logs, and database logs
- **Tools & Frameworks:** MITRE ATT&CK, Vulnerability Management tools like Tenable.io, & Rapid7

EDUCATION

Rayalaseema University , Kurnool
Bachelor Degree, Computers

LANGUAGES

English: C1
Advanced

Hindi: C1
Advanced

Telugu: C1
Advanced

CERTIFICATIONS

- CompTIA Security+
- SentinelOne Certified Engineer (S1CE)
- Microsoft Certified: Security Operations Analyst Associate