PAVAN KUMAR SHINDA

Bangalore, India 560066 • 8247512658 • Pavanshinde3548@gmail.com

PROFESSIONAL SUMMARY

I have overall 4+ 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 monitoring of SIEM (Splunk)/Azure Sentinel, SentinelOne EDR/XDR and Proof Point Email Gateway.. Have a deep knowledge of identifying and analyzing suspicious events.

EDUCATION

Bachelor Degree, 2019
Osmania University - Hyderabad, India

SKILLS

- SIEM - Splunk Es, Azure Sentinel & IBM Qradar
- EDR - SentinelOne ,Carbon Black & Defender for Endpoints
- XDR - Sentinelone
- Email Security - Proof Point TAP ,TRAP & 365 Defender.
- Cloud Security - Defender for Cloud | Defender for Cloud Apps.
- Vulnerability Management - Microsoft Defender for Vulnerability.
- DLP - Microsoft 365 for Data Loss Prevention
- Incident response, Detection, and Investigations
- Firewall - Cisco ASA, Palo Alto, FortiGate & CloudFlare WAF.
- Proxy - Zscaler | Cisco Umbrella
- Cloud - Azure Security | Microsoft Defender | Azure Monitor Logs
- Open Source Intelligent Tools: VirusTotal, IPvoid, AbuseIP, URLscan, Cisco Talos, URLvoid & IBM XForce.

WORK HISTORY

SOC Analyst, 01/2024 - Current

WNS Global Services -

Bangalore

- Working in the Security Operation Centre (24x7), monitoring SOC events, and detecting and preventing intrusion attempts.
- Investigate incidents using Dashboards/Events/Graphs /Annotations and reports Monitoring real-time security events on SIEM (Splunk ES).
- Monitoring and perform in-depth analysis of security alerts using the SentinelOne EDR & XDR platform .
- Monitoring and perform in-depth analysis of Cloud security alerts using Defender for cloud.
- Monitoring and perform in-depth analysis of Phishing alerts using Proof Point email security.
- Working on multiple tools to perform a day-to-day task, like having Azure Sentinel ,Sentinelone EDR , Carbon Black Response and Protect, DLP, and many more.
- Worked on monitoring of alerts, analyzing, coordinating with concerned teams with remediation steps and triaging them as True positive and False Positive and getting it resolved/closure in accordance with incident response process and procedure.
- Search firewall, email, web or DNS logs to identify and mitigate intrusion attempts. Identify and ingest indicators of compromise (IOCs), e.g malicious IPs/URLs, e.g. into network tools/applications.
- 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.
- Investigate all reported suspicious emails and determine whether the emails are malicious, non-malicious or legitimate and reply to the user who reported the suspicious email with a message reporting the findings and any recommendations.
- Identify and ingest indicators of compromise (IOCs), e.g. malicious IPs/URLs, e.g., into network tools/applications stay up to date with

current vulnerabilities attacks.

- Monitoring IOC (Indicators of Compromise) Making reports as per client requirements Generating and Making Daily, Weekly and Monthly reports and Dashboards and create annotations.
- Raising incident with concern teams, respond to the incidents and service requests and bring together additional information to either resolve or escalate the issue to the appropriate teams Take follow-ups and closing of the tickets based on the client response.
- Monitor user activity, network events, and signals from security tools to identify events. Tier 1 SOC Analyst is responsible for determining which alerts and other abnormal activity represent real threats.
- Evaluate the attacks, identify the root of the attack, implement required security actions to counter the attack, and restore system operations.
- Perform investigations and evaluations of network traffic, read and interpret logs, sniffer packets, and PCAP analysis with RSA Security analytics and Wireshark.
- Perform incident monitoring, response, triage and initiate investigations Create and track incidents and request using ticketing tool: (Service Now).

SOC Analyst, 06/2023 - 12/2023

Eli Lilly, Bengaluru, Karnataka - Bengaluru

- Working in Security Operation Centre (24x7), monitoring SOC events, detecting and preventing intrusion attempts.
- Splunk ES & SentinelOne 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 suspicious emails through Proof point TAP & TAP.
- Monitored and analyzed security events using Sentinelone XDR.
- Monitored and analyzed security events using SIEM tools to identify potential threats and anomalies.
- Monitored and analyzed Cloud related suspicious activities throgh Microsoft Defender.
- Perform incident monitoring, response, triage and initiate investigations Create and track incidents and request using ticketing tool: (Service Now).
- Perform Malware Analysis by Static and Dynamic methods to identify the malicious IOCs-indicator of compromise, taking action around IOCs identified.
- Investigate all reported suspicious emails and determine whether the emails are malicious, non-malicious or legitimate and reply to the user who reported the suspicious email with a message reporting the findings and any recommendations.
- Monitoring and perform in-depth analysis of security alerts using the SentinelOne platform.
- Investigated and triaged alerts, ensuring timely response and resolution of security incidents.
- 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.
- Conducted analysis of network traffic, logs, and alerts to identify signs of unauthorized activities.

Information Security Analyst, 09/2019 - 10/2022

Tata Consultancy Services - Hyderabad

- Monitored system performance and responded to alerts
- Investigate incidents using Dashboards/Events/Graphs /Annotations and reports

Monitoring real-time security events on SIEM (SplunkES).

- Monitoring, analyzing, and responding to infrastructure threats and vulnerabilities. Collecting the logs of all the network devices and analyzing the logs to find suspicious activities.
- Perform incident monitoring, response, triage, and initiate investigations Create and track incidents and requests using the ticketing tool: (Service Now).
- Perform Malware Analysis by Static and Dynamic methods to identify the malicious IOCs-indicator of compromise, taking action around the IOCs identified.
- Hands-on experience in monitoring events and Investigating incidents daily.

CERTIFICATIONS

- SC- 200 - Microsoft Security Operations Analyst
- SentinelOne EDR Certified Analyst
- CCNP (Routing & Switching) | CCNA, CCNP (Security)

LANGUAGES

English

■■■■■□

Advanced (C1)

Hindi

■■■■■□

Advanced (C1)