Divya Parkala

Hyderabad, Telangana
-Email me on Indeed: http://www.indeed.com/r/Divya-Parkala/fd32bed94c9dcac2

• Overall 4+ years of experience into Information Security as Security Analyst (SOC)
• Good understanding of security solutions like Anti-virus, DLP, Proxy, Firewall filtering/monitoring, IPS, Email Security, EPO etc.
• Hands on experience with QRadar, Splunk & SIEM tool for logs monitoring and analysis, Service now ticketing tool.
• Good knowledge on networking concepts including OSI layers, subnet, TCP/IP ports, DNS, DHCP, firewall monitoring, content filtering, check point etc.
• Hands-on experience into creating and updating event-based rules in Splunk.
• Good experience in creating & updating Incident response runbooks.

Willing to relocate to: Bengaluru, Karnataka - -

Personal Details

Date of Birth: 1990-09-01
Eligible to work in: India
Highest Career Level: 2-5 years experience
Industry: IT Operations & Helpdesk
Total years of experience: 4

Work Experience

Security Analyst

Mindtree - Hyderabad, Telangana
January 2018 to Present

ROLES & RESPONSIBILITIES:
• Responsible for first level incident response and incident management in managed SOC for different industries.
• Investigate and triage various CyberSecurity related events to determine risks and potential impact using SIEM solutions (Splunk).
• This also include escalating to senior level analysts if the event is beyond the initial scope of resolution.
• Capable of performing in depth research and analysis to identify if reported suspicious activity is due to malicious intent or expected behavior.
• Examine information security incidents to determine the scope of compromise to data and employees.
• Capable of using various security tools such as Security Information and Event Management (SIEM), endpoint, and open-source threat intelligence to execute security controls and defense/counter measures to prevent internal or external attacks or attempts to infiltrate company email, data, e-commerce and web-based systems.

• Evaluate new methodologies to support investigating CyberSecurity incidents and provide reviews and recommendations.
• Understand and utilize Cyber threat intelligence sources.
• Utilize the SIEM and CrowdStrike Falcon to correlate events and identify indicators of threat activity.
• Perform endpoint detection and response.
• Conduct analysis of multiple data sources to identify indicators of compromise.
• Communicate cyber events to internal and external stakeholders.
• Provide information and updates to shift leads.
• Create turnovers for next shift while working closely with supporting teams.
• Research, gather and compile the appropriate metrics to accurately update the weekly threat report, and daily turnover report in a relatable fashion to executive level committees.
• Participate in several tabletop exercises as a means of reinforcing incident response training.
• Creating weekly reports, monthly reports & Ad-hoc reports as per client requirements.
• Good experience in handling various types of incidents across multiple security solutions such as Firewall, IDS/IPS, End point, Servers, Windows related.
• Good experience in handling health alerts and closely working with engineering team for troubleshooting.
• Investigating and creating case for the security threats and forwarding it to Onsite SOC team for further investigation and action.
• Closely working with Senior analysts & Client SOC team in performing/identifying Root cause analysis.
• Preparing documents & templates for escalations.
• Performing Log analysis & analyzing the crucial alerts at immediate basis.
• Filling the Daily health checklist.
• Responsible for monitoring, analyzing and reporting multiple security events from devices like IDS/IPS, firewall etc. using the ArcSight and other Security Information & Event Management (SIEM) tools to detect IT security incidents.
• Reporting weekly / monthly dashboards to customer.
• Recognizing attacks based on their signatures
• Monitoring and carrying out second level analysis incidents.
• Responsible for performing investigation of the incidents captured in the SIEM and notifying clients with all the findings.
• Creating/Updating Runbooks.
• Being SPOC, handling client queries and resolving if any clarification required.
• Active participant in Buddy programs and Brownbag sessions.
• Collaborating with Engineering team, Hunt Team, Threat Intel team for ticket/process improvements.
• Experience in creating incidents in various ticketing tools like ServiceNow, Jira.
• Identifying multiple threats while Cyber Drills.
• Hands-on experience in handling incidents and ensuring SLA's to be met.
• POC for the shifts, managing shift roster, client bridging, managing shifts as per requirement.
• Work closely with clients for the follow-ups and understanding client requirements and updating the same with analysts.
• Performing peer reviews of the investigation on incidents before notifying the clients.
• Responsible for performing daily health checks of SIEM (Splunk).

• Responsible for performing investigation of the incidents captured in the SIEM and notifying clients with all the findings.
• Good experience in handling various variants of incidents across multiple clients.
• Good experience in handling Phishing emails, performing Header analysis to identify the integrity of the email & body analysis for any IOC presence.
• Good experience in handling IOC's by performing malware analysis.
• Good experience in handling EDR detections (both file based, and process based) from Crowd strike & Carbon Black.
• Good understanding of MITRE ATT&CK® framework.
• Knowledge in understanding TTP's detected by EDR solutions.
• Good understanding of OWASP Top 10, IDS, IPS, Threat modeling and Cyber Attacks like DOS, DDOS, MITM, SQL Injection, XSS and CSRF.
• Experience in performing Ad-hoc AV scans on hosts whenever required.
• Closely working with Hunt team, identifying latest attack vectors, latest IOC's and performing IOC sweep activities across various clients.
• Responsible for client calls & their request like IOC sweep, Ad-hoc request or Hunting.
• Hands-on experience in handling incidents and ensuring SLA's to be met.
• POC for the shifts, managing shift roster, client bridging, managing and updating client updates and managing shifts as per requirement.
• Work closely with clients for the follow-ups and understanding client requirements and updating the same with analysts.
• Performing peer reviews of the investigation on incidents before notifying the clients.
• Responsible for responding and managing the intrusions for multiple clients using respective SIEM solutions in managed SOC environment.
• Performing Trend analysis of the Use Cases to identify the aspects for high count of False positives and performing fine tuning of Use Cases.
• Collaborating with Engineering team, Hunt Team, Threat Intel team for ticket/process improvements.
• Experience in creating incidents in various ticketing tools like ServiceNow, Jira.
• Creating weekly reports for client reference.

Education

B.Tech in Engineering
JNTU - Hyderabad, Telangana
2008 to 2012

Higher Secondary(12th Pass) in MPC
Vikas vidyaniketan Jr. College (Board of Intermediate Education) - Hyderabad, Telangana
2006 to 2008

SSC
Martinet High school
2006

Skills / IT Skills

- IBM QRadar, Splunk, Trained on ArcSight
- CrowdStrike, Carbon Black, Proofpoint, G-suite, Panorama Firewall, IDS Firepower, TrendMicro Deep Security etc
- OSINT tools like, Threat connect, Virus total, IBM X-Force, Cisco Talos, Hybrid Analysis, App any run, Browser ling etc.
- Ticketing tools like, ServiceNow, Jira etc.
- O365 Security & Compliance

Languages

- English - Expert