Sai Vikas Batchu

SOC ANALYST

CONTACT

- +91 939-717-8993
- saivikas888@gmail.com
- linkedin.com/in/sai-vikas-batchu-37605aaa

TOOLS & TECHNOLOGIES

- Splunk Enterprise
- Phantom
- Palo Alto IPS/IDS
- CrowdStrike
- Proofpoint
- Symantec DLP
- Threat Grid
- Palo URL Filtering
- Cisco Talos
- IPVOID
- Virus Total
- MX Toolbox
- Abuse IPDB
- TCP/IP Protocols
- Phishing Email Analysis
- Malware Analysis
- Active Directory
- SQL Database
- SailPoint IdentityNow
- Service Now
- BMC Remedy

CERTIFICATIONS

- SPLUNK Core Certified User
- Fortinet NSE 2

EDUCATION

- B.Sc. in Computer Science at MG University, Nalgonda - 2017

Career Objective

- Looking for a role to further my Cybersecurity technical career, where my acquired skills will be utilized for the growth of the organization as well as to enhance my knowledge about new and emerging trends in the Cyber World.

SUMMARY

- Overall 5+ years of experience in Information Security with 2.8 years of experience as SOC Analyst at Infosys.
- Working level knowledge on security solutions like Antivirus, Firewall, IPS, Email Gateway, Proxy, IAM, TI, VA Scanners, DLP etc.
- Strong hands-on experience in security management tools like Splunk Security Incident and Event Management (SIEM)
- Good knowledge on skills like Malware Analysis, Threat Hunting.
- Exposure to using frameworks and compliances like MITRE ATT&CK. CIS Critical Controls, OWASP, PCI-DSS, ISO 27001 etc.
- Solid understanding of common network services and protocols.
- Good knowledge on cyberattacks and attack vectors.
- Maintain up-to-date documentation of designs/configurations.
- Good experience in working/communicating with cross-functional IT infrastructure.
- Co-ordinate with auditing and compliance team by providing requested report and data
- Perform root case analysis of incidents/breaches.
- Intermediatory knowledge on Python and Regular Expressions.
- Capable of independently learning new technology by utilizing available documentation and vendor support resources.
- Have good communication to effectively communicate with team and to customers.
- Proactive security search in network, endpoints to hunt malicious and suspicious activities that have evaded detection from existing tools using Threat Hunting techniques.
- Collecting evidence based information on the malicious activities and reporting them to various Threat Intelligence tools in blocking the IOC's.

Work History

INFOSYS

SOC Analyst | (2 Years 8 Months) March 2020 – Till Date

- Deep dive analysis of triggered alerts from SIEM, SOAR, Network, Endpoint security tools.
- Investigating incidents, remediation, tracking and follow-up for incident closure with concerned teams, stakeholders
- Advise incident responders on the steps to take to investigate and resolve computer security incidents.
- Analysis of CrowdStrike EDR Alerts by validating Command line executions and deep dive analysis of executing process/files/scripts and validating file paths.
- Analysis of Palo Alto alerts in analyzing packet captures of the traffic if it contains any malicious URLs/Scripts/IP Address and blocking the indicators at signature/network level.
- Hands on experience in Phishing Email Analysis (Tap and Trap alerts) and Conducting dynamic analysis with the sandbox tool.
- Build weekly and monthly reports as per SOC Manager requirements and walk through the handled incidents to peers and management.
- Develop the Splunk correlation rules by fine tuning and creation of dashboards, reports and alerts.
- Analyze for more information on observed indicators in various Threat Intelligence tools.
- Involved in threat hunting activities by assisting with support data from building hypothesis to finding evidence and enhancing security controls and detection logic
- Periodic upgradation/creation of correlation rules based on emerging threats and requirement following MITRE Attack and other TTP sources.
- Have knowledge on Playbook creation for use cases.
- Monitor health of SIEM components and reports to Admin.

INFOSYS

Identity Management Analyst | (2 Years 2 Months) January 2018 – February 2020

- Responsible for maintaining real time sync of identity information across multiple Identity systems like SailPoint, Active Directory and Identity Database (SQL Database).
- Managing lifecycle state changes of user accounts.
- Performing user management activities in SailPoint IDN like enabling /disabling /aggregating user accounts and synchronizing user attributes across applications.
- Creation of User accounts, Vendor accounts, DL Groups- Adding/Removing members and Renewal of groups in Active Directory.
- Managing password resets and Account active status in Active Directory
- Updating records in Identity Database (IDDB) using SQL queries.