TOUSIF PASHA

APPLICATION SECURITY SPECIALIST

CAREER SUMMARY

Highly competent and recognized security professional offering 8+ years of solid experience in information security holding a proven track record of surpassing client expectations. Seeking for a good position where I can utilize & enhance my skills in information security. Bringing ability to drive the successful delivery of exceptional support to clients while maintaining a positive corporate culture and reinforcingthe company's vision.

WORK EXPERIENCE

Application Security Specialist

Cognizant Technology Solutions India Pvt Ltd| May 2021 - Present

- Analyzing suspicious logs through a centralized log management tool SIEM - Arcsight
- ArcSight ESM, Logger, troubleshooting, installation setup.
- Hands on experience in real-time logs monitoring, analysis, investigation, incident handling, reporting and escalations of security events and its mitigation.
- Manage product performance and co-ordinate with team for smooth releases.
- Leading a team and serving as the main point of contact for administrating and supporting Endpoint Security solution like Antivirus, Vulnerability management, Information security compliance and SIEM solution.
- Share metrics periodically on security solutions handled by us to clients.
- To drive security incident management process for handling various real-time threats within the network.
- Follow risk management process and document and review the risk periodically with the customer

Senior Security Engineer

NTT Ltd. | May 2018 - May2021

- Monitoring and administrating Security operations and Security solutions like, Endpoint Security, Database security, Vulnerability management and Security operations.
- Handling prep calls with various engagement stakeholders to explain the requirement of changes before CAB meetings.
- Managing operations for various domains of security such as Endpoint security (McAfee ePO, Symantec Endpoint protection, Symantec DLP), Vulnerability assessment & Security patching(Tenable).
- Monitoring and performing analysis on high priority incident using various SIEM and User behavior based analytic tools
- IAM - Analyzing risk, strategy, threat intelligence, incident &response, application security, Conducting Research, Analyzing Data and Creating Reports
- Interacting with service providers, to ensure all technical tasks are closed on time with no impact on security operations.

PROFESSIONAL SKILLS

- Arcsight - SIEM
- Splunk
- Security Controls
- Endpoint security Solutions McAfee
- McAfee ePO, ENS, VSE, HIPS
- McAfee MVISION EDR and other McAfee supporting products
- Symantec End Point Protection - Manager(SEPM) 12 and 14
- Symantec email cloud security
- Symantec Data Loss Prevention
- Vulnerability Management - Tenable io
- Vulnerability Assessment
- Malware Analysis
- CYBER ARK, ARCON PAM
- IAM (Identification and Access Management)

HOW TO CONTACT ME

Phone No : +91 8147378375 /
+971 564842459
Email: tousif.iffath@gmail.com
PASSPORT No. : U6621513
LinkedIn: @/tousifpasha

WORK EXPERIENCE

Security Consultant

CAPGEMINI INDIA PVT LTD | May 2016 - Mar 2018

- Leading a team and serving as the main point of contact for administrating and supporting Endpoint Security solution like Antivirus, Vulnerability management, Information security compliance and SIEM solution.
- Undertake up-gradation task of Endpoint security solution such as McAfee, Symantec and aid in deploying new solution within the environment.
- Share metrics periodically on security solutions handled by us to clients.
- To drive security incident management process for handling various real-time threats within the network.
- Highlight the security gaps within the network and also provide solution to mitigate the risk.
- Follow risk management process and document and review therisk periodically with the customer

Security Analyst

CAPITA INDIA PVT LTD | Oct 2014 - May 2016

- Part of Platform-security team implementing and troubleshooting L2/L3 issues for infra- security tools like Symantec Endpoint Security and McAfee ePO.
- Created SOP documents as per the requirements. Also, created run/ play books on the latest attacks.
- Vulnerability management and risk assessment with MVM and Nessus. Part of L1 team monitoring SIEM alerts and endpoint protection.
- Server hardening and patch management for windows.
- Handled migration of machines from one ePO to other ePO server.
- Analyzing the Non-complaints end points which is communicated ePO server with current Date and not updating with latest DAT
- Task Management & Prioritization and timely delivery of Monthly reports to End Markets.
- IAM - Manage end user accounts, user access groups andentitlements using applicable tools and applications.

System Administrator

AST SOLUTIONS PVT LTD | Aug 2013 - Sep 2014

- Monitoring real time analysis of all network and security events through ArcSight monitoring tool.
- To monitor events generated by Symantec, McAfee and analyze and prioritize according to Criticality of the event.
- Preparing Knowledge base articles for technical issues.
- Communicate findings of all reports to all levels, i.e. from executive staff to working level. Coordinating with IT resources to effectively perform incident response tasks.

ACHIEVEMENTS

- Awarded with "TOP PERFORMER OF THE YEAR -2017" from CapGemini for continuous hard work and efforts towards the project.
- Have created a Test environment in CapGemini for McAfee ePO and Symantec with exact replica of Production (CLUSTER Based) to test Major ePO upgrades, Windows OS upgrades and SQL Upgrades prior rolling out to Production.
- Received Quarterly awards/certificates in CAPITA for completing the projects before the deadline.

TRAININGS & CERTIFICATIONS

- ITIL Foundation V4 training
- Specialized training of Symantec Endpoint protection, Symantec DLP and Symantec email cloud.
- Specialized training on McAfee ePO and its supporting products.
- Cyber ARK training and certification from vendor
- Splunk 7.x Fundamentals certification

EDUCATION

Bachelor of Engineering - VTU
Electronics and Communication - 2009-2013