Shayan Jagan Mathew

Address: 58 Heather Way, Romford, London, RM1 4TA
Mobile: 07918 295385 **Email:** shayan.jagan@gmail.com
Linkedin: linkedin.com/in/shayan-jagan

PERSONAL DETAILS

Date of Birth	: 01/10/1991
Nationality	: Indian
Passport details	: U 3352599 issued at Trivandrum on 27/01/2020, Expires – 26/01/2030, holding UK Dependant visa

PROFILE

An ardent computer enthusiast who has worked as Cyber Security Engineer skilled in Cyber Security and Windows administration with expertise in Incident Response, threat and vulnerability management, used SIEM tools like Rapid7, SentinelOne and Manageengine Desktop Central for documentation.

Graduated in Computer Science & Engineering and have done EC-Council Certifications in CEH & ECSA, also CCNA & MCSA networking & Microsoft Server certifications.

EDUCATION

06/10 - 04/14 — **Bachelor of Engineering (BE):**
Computer Science and Engineering (Anna University, Chennai)
CSI Institute of Technology, Thovalai, Kanyakumari District, Tamil Nadu, India.

CERTIFICATIONS

04/16 - 09/16 — **DIPLOMA IN INFORMATION SECURITY**
(ATL Education Foundation) USDLA Student ID: FRP-IS-15-1676

09/16 - 10/16 — **CEH (Certified Ethical Hacker)**
***EC Council** Certificate No: ECC44954864177*

11/16 - 07/17 — **ECSA (EC Council Certified Security Analyst)**
***EC Council** Certificate No: ECC33262126141*

04/18 - 07/18 — **CCNA(Cisco Certified Network Associate)**
Certificate No: CSCO13350569

05/18 - 08/18 — **MCSA (Microsoft Certified Solutions Associate)**

12/22 – 02/23 — **Certificate in Advanced Python**
Certificate No: INETPS519

EMPLOYMENT HISTORY

ENGINEER – IT SECURITY
Orion Innovation
Lulu Cyber Tower I, Infopark, Kakkanad, Kochi, Kerala, India **(July 2021 – March 2023)**

- Managing incident response processes - detection, triage, incident analysis, remediation and reporting.

- Remediating incidents by analysing the data, evaluating and identifying the root cause of the incident and implementing required security actions within SLAs and working as per ISO and SOC2 compliance to remediate incidents and Reduce downtime and ensure business continuity.
- Monitoring the Incident alerts from SIEM tool (Rapid7) to identify malicious activity, modify and manage the detection rules to analyse User Behaviour. Making custom alert vectors to tailor according to company policies. Research for community threats to include them in SIEM using tailor made queries for bulk log search and data retrieval.
- Monitoring the Incident alerts from XDR tools like SentinelOne, mitigate and document them and identify false-positive cases.
- Working towards mitigating the vulnerabilities detected in the organization network and devices, remedy them via Desktop Central.
- Working to complete monthly patching and verifying assets are complying the security standards with company policies.
- Managing and monitor software control tool, Investigate on unauthorized software installations and quarter wise patch update on third party softwares using Desktop Central tool.

SYSTEMS ADMINISTRATOR & TECHNICAL SUPPORT

Believers Church Medical College Hospital

St. Thomas Nagar, Kuttapuzha P.O, Thiruvalla, Kerala, India. **(Aug 2018 – June 2021)**

- Managing 800+ Desktops, Installation, support and maintenance with different OS Versions
- Troubleshooting network related issues, also performing regular System and Network Monitoring.
- Managing Active Directory, adding, removing, or updating user account information, setting up security policies for users, in addition to handling SQL Servers and VM Host Servers.
- Install, configure, and maintain all virtual environment implementations as well as taking backup of MSSQL Databases of application servers PACS, HIS for offsite recovery
- Providing remote infrastructure support delivery and performing problem cause analysis.
- Perform Detailed Documentation, ensuring that all phases of support are properly logged, tracked and resolved.

TRAINER FOR CYBER SECURITY

CATS (Centre for Advanced Training in Security)

Trivandrum, Kerala, India. **(Nov 2016 – Sept 2017)**

- Delivering training on CEHv9 (Certified Ethical Hacker) Certificate.
- Rendered assistance to Cyberdome as voluntary work in carrying out vulnerability assessment, network scanning and penetration testing – Backtrack, W3af and Acunetix.
- Responsible for social engineering vulnerability analysis and security advisory services.
- Accountable for incident management and computer fraud investigations.
- Consulted in information security domain, including experience and domain knowledge of corporate aspects of security.
- Responsible for consultancy and implementation of security aspects especially in government and financial sector

TECHNICAL EXPERTISE

SIEM Tools Used	**:**	Rapid7 IDR, IVM
XDR Tools Used	**:**	SentinelOne
Documentation Tools	**:**	Manageengine Desktop Central
Network Monitoring Tools	**:**	Nagios, Auvik
Programming Skills	**:**	Python, Shell Scripting, Java Scripting for Penetration Testing
Operating Systems	**:**	Windows, Linux, Kali Linux, CentOS, Ubuntu
Servers	**:**	Microsoft 2012R2,2016, Apache, Mysql

Hardware	**:**	Lenovo, HP, Dell desktops and laptops, HP, Canon Printers, Canon, Fujitsu Scanners, CISCO, HP Switches & Routers, NAS Storage.
Software Applications	**:**	Microsoft Office Suite (Word, Excel, Outlook, PowerPoint), Active Directory, ManageEngine ServiceDesk
Database	**:**	MySQL, MS SQL, PostGreSQL
Pen-Testing Tools	**:**	Nessus, Acunetix, GFI Languard, Nexpose, Tcpdump, NMAP, IBM Appscan, Nessus, Qualysguard, WTF, Burpsuite, Retina, Wireshark
Pen-Testing Frameworks:		Metasploit, Armitage, Setoolkit, BeeF

SKILLS

Cyber Security:

- SOC (Security Operations Centre), Incident Response, Security Monitoring.
- Threat and Vulnerability Management.
- SIEM (Security Information and Event Management), Rapid7 InsightIDR (IDR), Log Analysis,Rapid7 InsightVM Vulnerability Management (IVM)
- XDR, SentinelOne.
- ManageEngine Desktop Central.
- Network defence.
- Ethical hacking.
- Reverse engineering.
- Information Security technologies – including firewall technologies, VPN, intrusion detection, log analysis, IP Tables, vulnerability assessment.
- Knowledge in cryptographic algorithms (encryption, hashing, signing etc)
- Web Application Penetration Testing (OWASP).

System Administrator:

- Windows, Linux, Ubuntu, Kali Linux.
- Ms Excel, MS PowerPoint, Apache, Mysql servers.
- Windows server 2012/R2, 2016, Active directory management, File Server, Windows Server Clustering, VM Host servers backup.
- Fortinet Firewall Management.
- Installing, managing and monitoring in Nagios.
- LAN/WAN Administration.
- Workflow Planning.
- Productivity Improvement.
- Technical Support.
- Training & Mentoring.

Programming languages known:

- Python,
- C++,
- Core Java.

PROFESSIONAL MEMBERSHIP AND ACHIEVEMENTS

- OWASP
  Community
- Runner-up: Kerala Police Cyber Dome Hack Fest

References available upon request