MANU PRASADH

Cyber Security Consultant

Contact

Address
Abudabi UAE

Phone
+971 502270194
+91 8807401443

E-mail
manuprasadhmvs@gmail.com

Skills

Security Operation Center, Vulnerability Assessment, Penetration testing, Threat Hunting, Malware Analysis, DFIR

Web Application Security, Incident Response, Custom Log parsing (Flex and RegEx).

Languages

English, Tamil and Malayalam.

Programming Skills

C, C++, Java, .Net languages (VB, C#) & Python

Web Development (HTML, CSS, PHP and JS)

- Having with 9+ Years of core security experience with strong technical experience in SIEM, SOC, Vulnerability Assessment and Endpoint security.
- Experience of working in 24/7 Security Operations Center (SOC) responsible for providing Security Monitoring, Incident Response & Content Management.
- Technical knowledge in security-related hardware and software, security monitoring and other security systems and tools.

Work History

Jul 2023 - Current — **Core42 - G42 Cloud**

Jul 2023 - Current — **Cybersecurity Consultant (SOC & IR)**
UAE's Leading Cloud Service Provider, Abudhabi, UAE

Aug 2015 - Jun 2023 — **TATA Consultancy Services Limited**

Dec 2019 - Jun 2023 — **Senior Security Operations Centre Analyst**
Leading Bank of Abudhabi, Abu Dhabi, UAE

Sep 2017 - Nov 2019 — **SOC Specialist & SIEM administrator**
Government of India Entity, Bangalore, India

Aug 2015 - Aug 2017 — **Security Operations Centre Analyst**
Government of India Entity, Bangalore, India

Education

2016-06 - 2018-03 — **Master of Computer Applications (M.C.A)**
Bharathiar University - Coimbatore, India

2012-06 - 2015-03 — **Bachelor of Computer Applications (B.C.A)**
Dr.NGP.College - Coimbatore, India

Certifications

2019-02 — **CEH v10** - Certified Ethical Hacker (Version 10)

2022-12 — **SC100** - Microsoft Cyber Security Architect - Expert

2020-11 — **MS500** - Microsoft 365 Security Administration

2021-08 — **AZ500** - Microsoft Azure Security Technologies

2022-08 — **SC200** - Microsoft Security Operations Analyst

2021-03 — **NSE 1&2** - Network Security Expert – Fortinet

Achievements

- Received Star of the Month, On the Spot and Star team award in recognition for excellent performance.
- Created custom parsers for the event logs of various tools.
- Developed an analysis tool and multiple projects for Security Operations.

Tools

SIEM – Arcsight, Splunk, QRadar and Azure Sentinel

EDR – MS Defender, Symantec endpoint protection, Mcafee

SOAR – Cortex XSOAR,Forti SOAR **Vulnerability assessment tool** – Nessus & Rapid7,

Data Exfiltration Monitoring – Forcepoint, Fidelis Cyber Security & Mcafee DLP.

Host IDS/IPS – CISCO AMP, Symantec Data Center Security

NDR – Corelight, ExtraHop. **Patch management** – Symantec Altiris.

WAF (Web Application Firewall) – F5-ASM, Radware - AppWall

Email Security – Microsoft 365, Cisco ESA & Symantec MG,

RDBMS – Oracle, MS SQL Server, MS Access, MySQL.

DDOS – Arbor APS, Lancope - Stealth watch,

Others– Active Directory, Elastic Products (ELK Stack), NMAP, NIKTO

Roles and Responsibilities

Aug 2015 - Aug 2017

Security Operations Centre Analyst

Tata Consultancy Services, Project : Government of India Entity, Bangalore, India

- Analyse a variety of network and host-based security appliance logs (Firewalls, NIDS, HIDS,SysLogs, etc.) to determine the correct remediation actions and escalation paths for each incident.
- Monitor security solutions: SIEMs, firewall appliances, intrusion prevention systems, analysis tools, log aggregation tools.
- Investigate alerts created by IDS/IPS and WAF including malicious file uploads, compromised servers, SQL injections, and port scanning
- Create and maintain operational reports for Key Performance Indicators and weekly and Monthly Metrics.
- Analyse network flow data for anomalies and detect malicious network activity.
- Security events investigation, incident creation and response efforts. Provide daily monitoring and alerting of events that occur within the near real time environment.
- Develop and maintain standard operating procedure (SOPs) and incident response playbooks based on identified incidents and develop incident eradication plans
- Participate in the development of incident reports and update of lessons learnt
- Assist in data recovery procedures
- Participate in testing, deploying, and administering the infrastructure required to provide appropriate incident response

Sep 2017 - Nov 2019

SOC Specialist & SIEM administrator

Tata Consultancy Services, Project : Government of India Entity, Bangalore, India

- Manage the Mail Gateway server, monitor and analyse the emails for threats including phishing and malware, and escalates per procedure.
- Customize and manage security solution for client setups including SIEM, HIPS, NIPS, Endpoint Security, Mailing Security and Web Application Firewall.
- Collect IOCs and other threat intel data and build logic within security tools to detect the presence of the IOCs in the organization.
- Collect Vulnerability details from the respective team and ensure that there is adequate monitoring on the exploitation of these vulnerabilities.
- Implementation and configuration of Flex-connector and writing custom parser for Syslog and Non-Syslog events.
- Doing Penetration testing for the client infrastructure using Kali Linux on a regular basis to identify the security gaps before an intruder finds it.
- Doing a Web Application Vulnerability analysis and Malware Analysis
- Maintaining Threat Intelligence by integrating reputed online security forums to keep update of bad reputation sources, and Knowledge on IOCs.
- Vulnerability assessment of the production network devices and servers using Scanning tool and Verify regular patches for the same.

Dec 2019 - Jun 2023

Senior Security Operations Centre Analyst

Tata Consultancy Services, Project : Leading Bank of Abudhabi, Abu Dhabi, UAE

- Malicious and Suspicious email investigation. Providing awareness to end-users about the risks of such emails.
- Creating and Suggesting real-time use cases for the SOC monitoring. Working along with TDO of Defence Team.
- Monitor security appliances: SIEMs, firewall, intrusion prevention systems, analysis tools, log aggregation tools.
- Triage the identified incidents and ensure that incidents are classified as per the criticality
- Liaise with Incident response team for coordinating the Incident response activities.
- Perform intrusion scope and root cause analysis
- Participate in the development of an incident containment plan to limit incident damage
- Participate in systems backup and forensic image capture to ensure the affected systems state is captured as it is during the incident with the objective of performing forensics investigation at a later stage
- Redirect events to appropriate parties (according to playbooks and standard operation procedures) while providing necessary context and details
- Participate in incident eradication and recovery activities to ensure compromised systems are no longer affected
- Identify existing eradication plan from existing documentation, or develop new one eradication plans
- Participate in incident recovery activities to ensure affected systems are fully operational
- Manage the proper turnover of security incidents and coordinate response efforts between the stakeholders involved in incident response activities
- Reporting intrusion events, security incidents, and other threat indications and warning information to clients and respective authorities.
- Create and maintain operational reports for Key Performance Indicators, daily and Monthly Metrics.

Jul 2023 - Current

Cybersecurity Consultant (SOC & IR)

Group 42 - Cloud (Contractor), Abu Dhabi, UAE

- Usecase suggestion and creation. Alerts finetuning and Suppresion.
- Implementation and configuration of Flex-connector and writing custom parser for Syslog and Non-Syslog events.
- Participate in threat hunting activities.
- SOAR playbook creation and SIEM engineering.
- Analyse a network logs, Cloud logs, System logs and security appliance logs (Firewalls,NDR NIDS, HIDS,NDR,SysLogs)
- Conducted in-depth log analysis, identifying patterns and anomalies that led to the swift resolution of potential security issues
- Monitor security solutions: SIEMs, firewall appliances, intrusion prevention systems, analysis tools, log aggregation tools.
- Analyse network flow data for anomalies and detect malicious network activity.
- Security events investigation, incident creation and response efforts. Provide daily monitoring and alerting of events that of cloud environment.
- Provide guidance on cloud security best practices to ensure a secure and compliant infrastructure.
- Coordinate incident response activities related to cloud security incidents
- Suggestion and Creation of new correlation rules (usecases), offering recommendations, and fine-tuning suggestions to enhance visibility into cloud intrusions