George David

georgedavid.work@gmail.com | 6383253202| /georgedavidd/ | George-1100/
| georgrdavid.netlify.app|

EDUCATION

BSc. Information security and digital forensics Coimbatore, TN | Jun 2023
KARUNYA UNIVERSITY

WORK EXPERIENCE

SKYSECURE | ASSOCIATE SECURITY ANALYST Coimbatore, TN | April 2024 – Present

- Azure Sentinel: Conduct incident handling and timely respond to tickets, providing remediation steps to clients.
- Microsoft Defender for Endpoint: Investigate suspicious activity and malware defections, running antivirus scans on infected systems to ensure network safety.
- Microsoft Defender for Office: Examine quarantined emails, releasing them to user mailboxes when deemed safe.
- Manage day-to-day security operations procedures.

ZOHO | WHITE BOX PEN-TESTING INTERN Chennai, TN | Jan 2023 - Mar 2023

- Worked in white box pen testing for Java-based web application code analysis for XSS and SQL injection.

PROJECTS

LIMACHARLIE EDR AND SOAR LIMACHARLIE EDR, TINES, VIRTUALBOX, WINDOWS SERVER , LAZAGNE
Set up a Windows Server virtual machine with LimaCharlie EDR to improve endpoint detection capabilities. Created custom detection rules for identifying the LaZagne password-cracking tool and used Tines for automated alerting and created a SOAR playbook using for machine isolation based on user confirmation

AZURE SENTINEL THREAT MONITORING SENTINEL, POWERSHELL, WORKBOOK, KQL, VIRTUAL MACHINE
Implemented Azure Sentinel for live threat monitoring on a honeypot, utilizing a custom PowerShell script to detect and geolocate RDP brute force attacks.

WAZUH LAB WAZUH, VIRTUALBOX, VIRTUAL MACHINE, VIRUSTOTAL
Installed and configured wazuh SIEM with Two clients with installed wazuh agent. And performed file integrity monitoring and thread detection using Virus Total.

NESSUS VULNERABILITY MANAGEMENT NESSUS,VIRTUAL MACHINE, DEPRECATED FIREFOX
Installed and confiured Nessus in the host machine, created a VM as a victim machine and connected with the host via NAT. Installed deprecated Firefox in the VM. Runes the credential scan to detect Firefox vulnerabilities.

DIGITAL FORENSICS ON WANNACRY RANSOMWARE WANNACRY RASOMWARE, VIRTUAL MACHINE, AUTOPSY, VOLATILITY
Conducted an in-depth digital forensics investigation on the WannaCry ransomware. This involved setting up an isolated Windows 10 virtual machine, disabling security protections, executing the ransomware, and performing comprehensive disk and memory forensics.

SKILLS

Networking, Linux, SIEM, EDR, Email security, web application attacks, azure sentinel, KQL,
Defender for Endpoint and office 365, Email analysis