KUMAR REDDY

SR CYBER SECURITY ANALYST

DETAILS

PHONE
512-669-8459

EMAIL
kumarwhitehatcybersecure@gmail.com

LINKS

Linkedin

SKILLS

- Penetration Testing
- INFRASTRUCTURE SECURITY
- WEB APPLICATION SECURITY
- THREAT MODELLING & HUNTING
- VULNERABILITY / RISK ASSESSMENT
- Forensic Analysis
- POLICY & GOVERNANCE
- INCIDENT RESPONSE
- PENETRATION TESTING
- C++ & Java
- Python
- SOC & SIEM
- Cisco Networking
- Computer Networking

PROFILE

7 years of experience specialized in Cyber Security services on Web Application, Network Security, Infrastructure Security, Social Engineering, Cloud Security on AWS & GCP, Threat Modeling, Risk Assessments, Forensic, Incident Response, IOT.

Framework understanding and followed from Department of Defense (DoDAF), NIST, CIS, PCI-DSS, HIPAA, HITRUST CSF, ISO, SANS, SOX, Zero Trust Policy architectural for Risk Management.

Created centralized platform for monitoring analyzing security events by **Threat Hunting** aggregating with **SIEM**, **SOC** standard **Splunk** and other monitoring tools**.**

Experience on **OWASP** TOP 10, **SANS/CWE**TOP 25 and **OSI** defense model.

Dynamic & **STATIC** Application Security Testing (**DAST**, **SAST)** scanner, Hardware protection, software protection and security testing platform **SDLC** & **Verification**, **DevSecOps** with Fortify WebInspect, Nmap, Tenable Nessus, Rapid 7.

Sandbox-Testing / ith Nessus, Fortify WebInspect for Network Administration, **White** & **Black Box** testing for analysis and documenting. **Red** & **Blue** team **CTF** for Authentication, Authorization, Logging, Encryption, Decryption VPN protocols.

Performed **Risk Assessment** / **System Security Plan** essentials for authentication operational control, documenting, security implementation in enterprise with **Proofpoint**.

Experienced in intelligence Threat **Forensic** Analysis with **Autopsy**, **X-Ways**, **FTK** with imaging, data carving, keyword searching to find root cause.

Vulnerability Assessment and **Penetration testing** (VAPT) – on network infrastructure, identify, exploit vulnerabilities, Data breaches, DLP, Data theft, Data integrity, Firewall.

Pen Testing on Infrastructure, cloud, Web Application, IOT, Networking for remediation of attacks, recording **IOC** indicators for Malware, Digital Forensics.

SOFT and **HARD Skills** to Manage, Budget, Leadership, Collaboration, interpersonal skills in creating IT strategies.

Program Coding in **Python, Java, C, C++** programming language for Code analysis, assessments on Microsoft Windows Server, Linux server, Managment tools Jira, Confluence.

Patch Managements, Driver interactions, Microsoft System Security Management (SCCM), Information Technology Infrastructure Libraries (ITIL).

Detection and secured from **Man-in-The-Middle**, **Denial-Of-Service** attacks (DOS).

Deployed **Honeypots** protecting, experience with API endpoint, Active Directory Troubleshooting, automated scans and Compliance Requirements Checks.

ISO 27001 standard for Information Security Management System develops standards to ensure the quality, safety and efficiency of products, services, and systems.

Experience in **Data Security Standards** (DSS), payment application data security standards, Point-to-Point encryption standard (P2PE).

Network security testing

Endpoint protection and Zero trust

wireless

SAST – DAST

IDS & IPS

Worked on **Social Engineering** in operating the security culture and educating employees.

Patched IP- spoofing, **Domain Name System** (DNS) attack on servers**.** Cloud Protection on Amazon Web Services (**AWS**), **GCP** IAM, PAM, 2-FA, Multi-Factor Authentication.

Deployed Scheduled, Automated **Intrusion Detection, Prevention Systems** for Clickjacking, to avoid cyber-attacks on enterprise networks, Cloud, Applications.

Scripting, Programming languages, and tools include

MITRE ATT&CK, **Trend Micro**, **Recorded Future**

Burp, **Nessus**, **Fortify**, PAM suites activities on server port, protocol, port scan, **BitNinja**, **SonicWall**, **Wireshark**

EMPLOYMENT HISTORY

Sr Cyber Security Analyst , Capital One

Mclean, Virginia

Sep 2021 — Present

· Deployed **Intrusion Detection** IDS Migration, IDS Routing**. Intrusion Prevention System** on Infrastructure, application, Network.

· Developed and managed pipeline internal channel with **Spring boot**, **Aws**, **Java 1.8** Concurrency API to manage the **RESTful Web Services**, Spring Boot Framework.

· Used Regulatory Governance **NIST** SP 800-53, 800-63, 800-79, 800-171 for guidelines.

· **PCI DSS**, **ISO 27001** guidance framework understanding and management for governance, Legal regulatory on Risk assessments, monitoring, and remediation.

· Performed **Manual Inspection**, **Code Review**, **Threat Modeling** on application, classify assets, exploring Threats and scenarios and working toward mitigation strategies.

· Performed versatile **Forensic**methods with **X-Ways**, **Autopsy** for data recovery analysis, encryption, Malware, phishing, Virus, VPN, spoofing, Worm, social-engineering. **FTK**for finding root cause with imaging, data carving and keyword searching.

· **Threat hunting**across disparate security tools monitoring for firewalls, routers, switches, wireless, with **VMWare Carbon Black Endpoint.**

· Performed **Threat Protection** with CISCO Prime, Physical & Virtual firewall.

· Worked in **patch management program**across CSPM, CIEM (**Cloud** infrastructure entitlement, **Security**posture management) Cloud network infrastructure & workload protection, Security offering, Detection & Response with **Trend Micro, CISCO**

Analyzing cybersecurity **Phishing**, **Vishing**, **Smishing** attacks via social engineering, **EDR** technology endpoint, workstations, servers, information security file activities.

Developed and implemented a complex network security system, reducing the risk of Cyber threats by 50%

Cybersecurity Analyst , Citibank

Edison, NJ

Jan 2021 — Sep 2021

· Configured and monitored Network IP logging with **Cisco IDS**, **Microsoft**,**Network Sniffers**, **Active Directory**, **WAN/LAN analyzer**.

· Remediated **ORM** (Object Relation Mapping) **injection** in SQL injection against data.

· **Vulnerability Scanner** on web application software via **Tenable Nessus** for Threats, malicious insiders, and human errors.

· Setting **Enterprise Risk Management** objectives**,** identification, Prioritizing-**,** Assessments**,** Measures and Reporting.

· Worked on **Static application code testing in Java and python**, CSS, JavaScript.

· Designed **Security architecture** & **Software Security** with mitigating JavaScript interaction attacks with continues monitoring and frequent testing. Secured server from **WEB Attacks** via Web application firewall (WAF) mitigated Cross-site Scripting (XSS).

· Performed Deep **Penetration Test** featured with NetSparker, for security for **SQL injection detection** (SQLI), Local file inclusion detection (LFI), Remote file inclusion detection (RFI), Reflected XSS detection (RXSS).

· Worked and improved defense with **Trend Micro, MITRE ATT&CK**, **CVE**, **CAPEC**, **CWE** for structure advisory behavior for threat intelligence, feeds.

· Monitored Compliance requirements for industry standards on regulatory with **ISO 27000.**

Information Security Analyst, ACORD Pearl River, NY

Jul 2020 — Dec 2020

· Security overall **SDLC**, integrating and maintaining security frameworks and standards.

· Knowledge of industry policies Governance, Compliance **NIST SP 800-53**. **SANS, SOX**.

· Maintained **cyber security documentation** including Business Continuity and Disaster Recovery Plans, facilitating **risk assessment** exercises, performed compliance and risk monitoring/validation, and other **compliance assurance exercises** as required.

· Designed environment in **Cryptography** algorithms, Ciphers, security measures.

· Conducted **Symmetric**, **Asymmetric Keys Data integrity**, password, **Hash** function testing for data manipulations and **SQL injection.**

· Implemented identity **Firewall Management**, **Security Program Strategy-**, **detection of Network anomaly**, unusual network, unusual server port activity, protocol activity, port scan / port sweep activities.

· Experienced with **Trend Micro** Data classification, Policy enforcement, Cloud Data protection, Loss Prevention solutions.

On Call response/ on premises response for security incidents in alerting **PCIA** (Protection, Confidentiality, Integrity, Availability).

Application Security Analyst , Molina healthcare Long Beach, CA

Nov 2015 — Nov 2018

· Developed **Cyber Security Web Application** with **Burp** Proxy, intruder, repeater, sequencer, decoder features and functionality usage to allow tests. Provide a strategic stop gap against common vulnerabilities like injection and **Cross-Site Scripting** (XSS).

· Expert Dynamic vulnerability scanning test, Web Application security with **WebInspect**.

· Defended system attacks with **VMWare, Linux servers, Microsoft windows server**. Controlled **USB** device control, disk encryption & host firewall.

· Guidance Volume 1 – Volume 4 of CMS, Minimum acceptance of Risk standards of exchange. Risk Security & Privacy control of exchange and **ASVS**, **MASVS**.

· Developed **Automation** with monitoring tools with **Java, Python, JavaScript** coding for representing, collecting user actions, version controlling with **GIT-**, **Jenkins** tool for continues integration and Monitoring.

· Performed **Manual Penetration Testing** analysis using Burp Suite, Zen map, Nessus.

· **Access control management**& central monitoring with cloud native technologies.

EDUCATION

Master degree, University of Mary-Hardin Baylor Belton

Graduated in Information System (Cyber Security)

Bachelor of Engineering, Jawaharlal Nehru technological University Hyderabad

Computer Science Engineering