**SRUTHEEN UPPU (CISM)**

**(13 years in various domains of cybersecurity)**

**(Computer Science Graduate)**

**9419287831|usrutheen@gmail.com**

**OBJECTIVE**

Seeking a dynamic role to apply my expertise in formulating and implementing robust cybersecurity strategies, contributing to the enhancement of organizational security postures.

**TOOLS & TECHNOLOGIES**

CYBER SECURITY MONITORING: SIEM (Wazuh, Mcafee ESM), Packet analysis (Wireshark)

CYBERTHREAT INTELLIGENCE**:** MISP, Mandiant, VT Enterprise.

CLOUD SECURITY MONITORING: AWS Guard Duty, Cloudtrail

DIGITAL FORENSICS: SIFT, FTK, Autopsy, Windows Sysinternals).

MEMORY ANALYSIS**:** Volatility, Sysinternals.

EDR (CB Response, Crowd strike), Cylance

VAPT**:** Nessus, Nexpose, Netsparker, Metasploit, Nmap, WPscan, SQLmap, Burp Suite, OWASP ZAP, OWASP Dependency checker, Xray, Kali Linux, Cycognito

DLP: McAfee, Forcepoint

**PROFESSIONAL EXPERIENCE**

**E2open Inc.** (JAN ’18 to Present, **Senior Staff Security Engineer)**

1. Lead APAC security operations. (Incident response and monitoring teams)
2. Provide expert Investigative support (Highest point of Escalation) for incident response for critical security incidents.
3. Subject Matter Expert for Security engineering tools Architect design, Configuration, and deployment for Enterprise aligned to NIST 800 series.
4. Worked on implementation of Security Orchestration and Automation (SOAR) – workflow creations, written playbooks, actively working on improving process documents.
5. Configured and integrated MISP as our opensource threat intel.
6. Developed threat detection and created custom detections.
7. Performed incident response on true positive AWS GuardDuty events.
8. Performed dynamic malware analysis on the encountered incidents and taken steps to contain and remediate systems.
9. Expertise in implementations for Suricata (Open-source custom IDS/IPS) across multi-tenant DCs and corporate offices and involve troubleshooting when encountering issues.
10. Closely Working with infrastructure teams evaluating network rules providing reviewing and approving as necessary.
11. Identifying the latest TTP’s, by hunting known Command and Control Frameworks.
12. As part of regular threat intel activity identifying the IP's and domains used in malicious activities by using OSINT Methodologies and other professional services.
13. Actively hunting for threats on Layer 3 and Layer 7 devices, define Hypothesis & come up with detections (Lockheed Martin | MITRE ATT&CK Enterprise framework).
14. Actively working on improving the security scorecard of the organization with the help of infrastructure and operations teams for remediation of findings related to our vulnerability management program and other attack surface management tools.
15. Currently working on container security and devsecops.
16. Worked with software development teams for reviewing their design, approving their release by reviewing their third party, static and dynamic scan reports.

**Tata Consultancy Services.** (FEB ’17 to JAN ’18, **IT Analyst**)

1. SME in implementing & Configuring Cyber Security Solutions (SIEM, EDR)
2. Responsible in developing custom correlation rules and security use cases.
3. Provide expert Investigative support (Highest Point of Escalation) for incident response for critical security incidents.

**CYIENT Ltd.** (MAR ’14 to FEB ’17, **Senior Executive – Cyber Security**)

1. SIEM Implementation/ administration & Monitoring of SIEM, DLP, END POINT security solutions.
2. Digital Forensics & Incident Response/Incident Handling, Create process documentation and SOP(s).
3. Working along with compliance team in aligning CoE’s to the standard’s compliance requirements.
4. Facing external certification audits and customer audits.
5. Assisting compliance team in planning, designing, implementing and monitoring ISO 27001, ISO 27019 standards.
6. Providing support on security prospects to ISO 27001

**E2labs Information Security Pvt Ltd.** (NOV ’10 to MAR ’14, **Security Consultant**)

1. Handled security incidents, validating the legitimacy of the incident, identifying the source, the Indicators of Compromise & perform event correlation and timeline followed by reporting.
2. Penetration Testing, Vulnerability management
3. Examined and analyzed electronic media in support of computer intrusion. Analyzed media using a broad range of computer forensic tools.
4. Trained Government, Law Enforcement Agencies & Non-Government Professional on Cyber Security Methodologies.