Revanth **Bobba**

Information Security Engineer · Threat Hunter

1-483, Plot no:26, Dammaiguda, Hyderabad -500083

(+91) 93-9383-3019 | bobba.revanth@gmail.com | revanth543 | revanth-bobba-045086bb | @Revanth03896318

"If something sounds too good to be true… there's probably a scammer behind it.."

Professional Summary

Currently working as a Cyber Security Engineer, Threat Hunter at Sophos. Having 3+ years of professional experience specializing in incident response and management, OSINT, forensic investigation, vulnerability management, threat hunting and intelligence gathering. I aspire to serve an organization with sincerity and determination to succeed. I aim to occupy a responsible and challenging position in an organization by keeping abreast with the latest developments in Information Security.

Work Experience

Sophos Group plc.

Ahmedabad, India

Information Seurity Engineer - CIRT Team Member, Threat Researcher

Jul. 2018 - PRESENT

- **Blue Teaming, Incident Handling:**
  As part of internal GCIRT members will handles the critical cyber security alerts and incidents generated by SIEM/Proxy/AV/BRO/IDS and IPS using the standard operational documents/playbooks/flow-charts which designed based on the NIST, MITRE, Cyber Kill Chain frameworks.The SOP's will vary with the Industry(SOX, PCI, HIPPA.. etc
  –> *Splunk ES:* use-case design, building search queries and dashboard creation, implementation and fine-tuning.
  –> *Sophos Central:* end-point protection, malware events, agents monitoring, group policies, application control, web-proxy management
  –> *Sophos UTM:* IDS/IPS events related to external web-attacks, scanning and exploitation command and control/bot traffic
- **Threat Hunting, Google Dorking, Security Automation:**
  Hunting and Reducing the new threat and attack vectors that impacts the organization either Internal (or) Externally.
  –> *Wiki and Jira:* identifying the wiki directories with sensitive content.
  –> *Google Dorks,and Dark-Web:* by using open sources identifying the potential sensitive files, vulnerabilities of organization.
  –> *Digital Shadows:* third-party risk management tool which provides the parking domains, vulnerable certs, brand misuse, password dumps
  –> *Devops and Automation:* building custom python scripts to automate the intelligence gathering.Integrating IOC's to the SIEM which gathered from public and private intelligence source's
- **Phishing and Spam Automation:**
  handling phishing email submission from the end-users and taking containment steps. creating SPF, DKIM, DMARC records for the domains to protect from the spoofing.
  –> *Phish Threat:* phishing simulation, spear -phishing and purple-team simulation, quarterly campaign's and reporting to board members
  –> *Komand:* phishing automation, standard replies, e-mail banner implementation
- **Vulnerability Management and Patching**
  Performing scheduled vulnerability scans on web applications and network assets in the infrastructure to mitigate potential threat. Building and updating vulnerability knowledge base
  –> *Nexpose:* discovery scans and asset inventory management, scanner template creation, supporting development teams in the process of SDLC, patch management.

Metmox Software Solutions Pvt Ltd

Hyderabad, India

Information Security Sr. Analyst & IT security Analyst

Sept. 2015 - Jun. 2018

- **Incident Handler:**
  As part of L2 SOC team member, will handles, re-mediate, escalate the potential security incidents reported by L1 tier SOC members. Also worked on log sources integration and reports creation.
  –> *QRADAR:* offenses analysis, correlation searches creation, reporting, attending fine-tune and CIRT meetings.
- **Proxy Management:**
  Working with the network team on proxy installations, Region/Department policies, URL categorization, UBA events. Also working on the pedefing threat catgories in proxy such as Botnet Call back, Spyware Callback, Malicious Content, XSS, SQL, Cookie stealing.. etc.
  –> *Zscaler:* Working along with the network team and integrating ZEN/Proxy nodes to the Palo-alto and Juniper firewalls over ipsec/GRE tunnel.
- **Endpoint Detection and Response:**
  EDR tool identify and mitigates the potential ATP, Ransomware attacks.
  –> *Tanium:* Identifies and stops all ATP level attacks, power-shell executions and registry modifications, patch management, good source for inventory management
- **Third-Party Risk:**
  Third-Party risk tool provides the security rating for the organization based on the external threat vectors observed. This risk scores will calculated based on the industry type.
  –> *Bitsight:*Worked on third-part risk management tool which reports mis-configured a) SPF b) DKIM c) SSL/TLS certificate issues d) Potential open ports e) UBA events f) HTTP headers
  –> *SNR:* Creating Security Notification reports to the management for the external feeds.

Honors & Awards

Internal

2019	**CISO Security Award**, Identified potential Zero day attack in organization	*SOPHOS, U.K*
2018	**Quarterly Flyer**, Got best performer award for the Q3 2018	*SOPHOS, IT*
2017	**Security Specialist**, Received Security coin from the client	*Stryker, U.S.A*

External

2018	**HOF**, Received Hall Of Fame - https://www.vista.co/en/responsible-disclosure-policy/	*Bug-Bounty*
2013	**Hoodies**, Responsible Disclosures for multiple websites	*Bug-Bounty*

POC and SME

Sky-High — *Cloud Management*

DLP Management — *Jan. 2017 - Jul. 2017*

- Worked on the CASB infrastructure to mitigate the potential data theft from the internal systems and identifying the inside attackers. Created the regular expressions for the potential PII and sensitive information to track the users are uploading downloading/uploading externally

Carbon Black, Protect Wise - Endpoint Response — *Sensors and Agents*

EDR — *Oct. 2016 - May. 2017*

- Security End-point detection and monitoring tool to identify the ATP events and Torrent activity, TOR, Device Isolation

Security Training's and Certification

2019	**Trained and Certified**, EDR - Recloak certified specialist	*India*
2018	**Trained and Certified**, SOPHOS certified security engineer	*India*
2018	**Trained and Certified**, Splunk Fundamentals 1 and 2	*India*
2017	**Trained**, ECSA - EC-Council certified security analyst	*India*
2017	**Trained and Certified**, Cybrary - End-user PII and Security Fundamentals	*India*
2016	**Trained and Certified**, Qualys certified vulnerability specialist	*India*
2016	**Participated**, Finalist - Tech challenge 3.0 Capgemini	*India*
2016	**Trained and Certified**, IBM MSS Security Incident Response	*India*
2015	**Trained and Certified**, OCJP - Oracle Certified Java Programmer	*India*

Education

JNTU - Vaagdevi Eng. College — *Warangal, A.P*

B.tech. in Computer Science and Engineering — *Jun. 2011 - Exp. Jul. 2015*

–> Aggregated with CGPA of 7.6
–> Attended security related seminars
–> TL for the major and minor projects with team size of 4.

Extracurricular Activity

Participated several CTF's) — *India*

CTF Player — *Jun. 2017 - PRESENT*

- Got 112 Rank in NULL-CON - GOA, 2017
- Own CTF challenge in organization - conducted by client.

Blog Writer and Bug-Bounty) — *India*

Public Researcher — *Jun. 2017 - PRESENT*

- Blog/CTF writer
- Performing OSINT, exploitation on third-parties and reporting responsible disclosures

Sports and Games — *India*

Study and Sports and Games — *From Childhood*

- Playing and Watching cricket
- Playing and Watching chess
- Online Mobile and PC Gamer