Table of Contents

JR00018039 - InfoSec L2 Security Engineer - IST Hours

Candidate Name	Candidate ID	Attachments
1. Pulla Surendra	C2000000562846	
2. Raja Kusuma	C2000000561439	
3. Vivek Thatikonda	C2000000561614	
4. Shweta Gupta (Shweta)	C2000000561512	
5. Ashutosh Pati (Ashutosh Pati)	C2000000560596	
6. kishan agarwal	C2000000451401	
7. Akshara M	C2000000450381	
8. venkatesh verimella	C2000000449865	
9. Ajay B	C2000000449611	
10. Ishita Paul	C2000000449396	
11. Nagaraj Cheruku	C2000000448952	
12. Archeshma Bodhanapu	C2000000448937	
13. Veerendra Jeelakarra	C2000000448850	
14. Anurag Akula	C2000000448776	
15. Sree vynathey reddy Mallepalli	C2000000448757	
16. Nehal Limje	C2000000448631	
17. Sai Raavi (Sai Raavi)	C2000000448446	
18. Sikkander Batcha k	C2000000448192	
19. Shaik Dilshad	C2000000448157	
20. sumanth gopu	C2000000448132	
21. M Sri Shailesh	C2000000448038	
22. Vivek Sugee	C2000000448029	
23. Sai Prakash Gundala	C2000000447981	
24. Naga Mohan Kolli	C2000000447987	
25. Mounika Pendem	C2000000447990	
26. Irfan Mohammad (Irfan Mohammad)	C2000000447984	
27. Afsal Shereef	C2000000447915	
28. Rutvik Shah (Rutvik Shah)	C2000000447858	
29. Krishna chaithanya varma Nampelli	C2000000447875	
30. Sowmya Lakkavajjala	C2000000447855	
31. CHEVULA SUNIL	C2000000447859	
32. Santosh Annapuraju	C2000000447853	

Pulla Surendra

Security Engineer

+91 9494298023 suri250519@gmail.com

SUMMARY

Experienced cybersecurity professional with 7+ years in VAPT and security assessments across web, mobile (Android & iOS), APIs, networks, and cloud environments. Skilled in identifying critical vulnerabilities and delivering remediation aligned with OWASP Top 10 and industry best practices. Strong expertise in application and cloud security, with a proactive approach to risk management and strengthening overall security posture.

EXPERIENCE

Security Engineer

Bangalore, India

KPMG

02/2018 - Present

Penetration Testing & Security Assessments

- Conducted thorough penetration testing across cloud, network, API, web, and mobile (Android/iOS) platforms
- Utilized both manual and automated techniques, including SAST, DAST, IAST, and SCA, to identify and mitigate vulnerabilities in languages such as Java, Python, JavaScript, C#, and C/C++
- Employed a wide range of tools including Burp Suite, OWASP ZAP, Postman, MobSF, Frida, Drozer, Objection, and apktool to uncover vulnerabilities such as Broken Authentication, IDOR, Insecure Data Storage, API Abuse, and Root/Jailbreak Detection Bypass
- Delivered actionable remediation strategies and collaborated closely with developers to embed security into the SDLC

Cloud Security & Compliance

- Extensive experience securing public cloud platforms including AWS (EC2, VPC, IAM, S3, RDS, WAF, Guard Duty, Route 53) and Azure (NSG/ASG, Firewalls, VPN)
- Implemented and managed security configurations, access controls, logging, and monitoring for secure cloud governance and compliance
- Hands-on with CSPM and CNAPP tools for continuous cloud posture management and risk mitigation
- Proficient in Docker, Kubernetes, and micro services architecture security, integrating protection throughout cloud-native environments
- Automated infrastructure provisioning and policy enforcement through Infrastructure as Code (Terraform) and embedded security into CI/CD pipelines
- Create S3 buckets with required configuration
- Create IAM rules with required policies, Configure SNS, SQS as per requirements
- Instances, configure and maintain route table, internet gateway within the VPC

Cybersecurity Solutions Development

- Designed and executed large-scale cybersecurity initiatives to protect Visa's brand, networks, assets, and products, implementing advanced detection, prevention, and response mechanisms
- Collaborated with cross-functional teams to develop innovative security solutions, ensuring the organization's cybersecurity posture remained resilient against emerging threats and vulnerabilities

DevSecOps & Automation

- Integrated security into DevOps workflows using CI/CD tools such as GitHub Actions, GitLab CI, and Jenkins
- Implemented automated security testing in CI/CD pipelines using SAST and DAST tools
- Built and optimized cloud-native security automation in Python and Bash, reducing time-to-detect and time-to-remediate for incidents
- Secured API interactions and enabled secure integrations through API-based security automation frameworks
- Skilled in programming languages such as Java, Python, and Bash

Threat Modeling, Risk Management & Governance

- Conducted threat modeling using STRIDE, MITRE ATT&CK, and PASTA methodologies, enabling proactive risk identification during design and development phases
- Participated in security architecture reviews and internal risk assessments for critical applications and cloud infrastructure
- Ensured ongoing alignment with NIST, ISO 27001/27701, SOC2, HIPAA, HITRUST, GDPR, CCPA, and PCI-DSS compliance frameworks

Network Security Assessment

- Protocols: Familiarity with web application security standards and protocols (SSL/TLS, OAuth, SAML, SSO)
- Reduced breach impact by 45% by implementing network segmentation strategies to limit lateral movement.
- IDS/IPS Implementation: Implemented IDS/IPS solutions that detected and prevented multiple network-based attacks, enhancing overall network security

Security Testing & Vulnerability Management

- Conducted comprehensive role-based security testing to validate that configurations met business, compliance, and security requirements
- Performed security vulnerability assessments and penetration testing across Oracle Cloud ERP and mobile platforms, ensuring secure and compliant systems

Security Monitoring, SIEM & Intelligence

- Managed security event monitoring and log analysis using Splunk, Sumo Logic, and QRadar for real-time threat detection and response
- Worked with malware analysis, container security, and attack simulation platforms like SafeBreach, AttackIQ, and Penter
- Integrated threat intelligence feeds into SIEM and security tools, enhancing visibility and response capabilities

EXPERIENCE

Endpoint Security

- EDR, Device control, Antivirus Protection, Application whitelisting
- Continuously contributed to fine-tuning detection rules, minimizing noise, and aligning use cases with current threat landscape
- Participated in team knowledge-sharing sessions and played a key role in onboarding and mentoring new team members

Security Incident Response & Coordination

- Acted as the primary coordinator for high-severity security incidents, ensuring timely response, containment, and resolution across global environments
- Led cross-functional incident response teams, including SOC, IT, and legal, during critical cybersecurity events, minimizing business disruption
- Oversaw end-to-end incident lifecycle management, from detection and triage to RCA (Root Cause Analysis) and post-incident review

Threat Investigation & Analysis

- Conducted in-depth investigations into security breaches, malware outbreaks, policy violations, and unauthorized access incidents
- Utilized forensic techniques and tools (e.g., EDR, SIEM, log analysis) to identify indicators of compromise (IOCs) and determine root causes
- Prepared detailed incident documentation, including timelines, evidence, impacted assets, and lessons learned

Endpoint & Malware Response

- Hands-on experience with Endpoint Detection & Response (EDR) and antivirus solutions (e.g., Crowd Strike, Defender ATP, McAfee) to analyze, isolate, and remediate infected systems
- Developed and enforced endpoint security policies and procedures, reducing malware infection rates and enhancing overall endpoint resilience
- Performed threat hunting and IOC sweeps across enterprise endpoints to detect hidden threats and lateral movement

Continuous Improvement & Preparedness

- Participated in and led incident response tabletop exercises and simulations to improve readiness and response time
- Regularly updated and optimized the Incident Response Plan (IRP) based on lessons learned and evolving threat landscapes
- Worked closely with security governance teams to enhance policies, procedures, and compliance controls

Security Knowledge & Framework Alignment

- Strong working knowledge of security standards and frameworks such as NIST CSF, ISO 27001, and CIS Controls
- Integrated best practices into incident response playbooks, ensuring alignment with industry regulations (e.g., GDPR, HIPAA)
- Actively tracked emerging threats and incorporated threat intelligence into detection and response strategies

Operational Excellence & Continuous Improvement

- Managed lifecycle activities for perimeter security systems, ensuring ongoing compliance with engineering standards and best practices
- Championed efficient asset tracking and database management practices, improving overall project timelines and asset inventory systems

Leadership & Strategic Impact

- Spearheaded cloud security initiatives that increased compliance coverage by **25%**, reducing risk exposure across multi-cloud environments
- Led vulnerability management programs, bridging technical teams with business stakeholders to drive timely remediation and policy enforcement
- Mentored junior security engineers, fostering a collaborative and security-first culture within cross-functional teams
- Acted as a security subject matter expert, communicating security risks and concepts to both technical and non-technical stakeholders

EDUCATION

Bachelors in Electrical

Kakinada, India

JNTU Kakinada University

2016

SKILLS

SIEM, SOC, Threat-Hunting, Security-Operations, Incident-Lifecycle, Risk-Mitigation, Mentoring, Linux-Basics, OSINT, IDS, Azure-Identity-Protection, Network-Monitoring, Azure-Sentinel, Log-Analysis, Root-Cause-Analysis, Alert-Triage, SOPs, XDR, EDR, Incident-Response, AWS, Bash, DevSecops, FileZilla, GCP,, OWASP, Kubernetes, Service Now, GitHub,

Raja Venkatesh Kusuma

Information Security Analyst

Hyderabad, India | +91 9154509336 | rajavenkateshkk@gmail.com | Raja Kusuma

SUMMARY

- Results-driven Information Security Analyst with **5.9 years of overall IT experience**, including **3.9 years of focused expertise in cybersecurity engineering** and operations.
- Proven expertise in **24/7 Security Operations Center (SOC)** environments for monitoring, investigating, and triaging security incidents.
- Adept at incident response, including the development of effective triage playbooks and workflows.
- Skilled in implementing and managing security tools and controls to enhance the organization's security posture.
- Hands-on experience **with Endpoint Detection and Response (EDR),** including **Microsoft Defender for Endpoint** and Intune integration.
- Conducts phishing simulation campaigns to evaluate and train users on phishing awareness.
- Experience in **vulnerability management**—tracking, reporting, and coordinating remediation efforts.
- Proficient in **Privileged Access Management (PAM),** including monitoring and resolving privileged account issues.
- Experienced **in email security analysis, phishing email investigations**, and user communication/reporting.
- Strong understanding of networking concepts such as OSI model, TCP/IP, DNS, DHCP, firewalls, content filtering, and checkpoint technologies.
- Skilled in writing detailed incident reports and maintaining comprehensive documentation.
- **Conducts daily threat hunting based on Indicators of Compromise (IOCs)**.
- Regularly creates and analyzes security reports (daily, weekly, and monthly) for trends and actionable insights.

TECHNICAL SKILLS

- **Programming**: Kusto Query Language (KQL), HTML
- **Endpoint Security**: CrowdStrike, Defender for Endpoint, Cisco AMP
- **SIEM**: MS Sentinel, BluSapphire, IBM Qradar
- **Email Security**: Defender for O365
- **Privileged Identity Management**: BeyondTrust Password Safe
- **Phishing Campaign**: Defender Attack Simulation, Knowbe4
- **Vulnerability management**: Tenable.io

CERTIFICATIONS

- Zscaler for Users – **Essentials** (EDU-200)
- Zscaler for Users – **Advanced** (EDU-202)

EXPERIENCE

Birla Soft, Hyderabad
Technical Specialist – Cyber Security *Aug' 2021 - Present*

- Monitored and **analysed security alerts from SIEM tools** to identify potential threats and incidents.
- Performed **log analysis and incident investigation** across security devices including firewalls, IDS/IPS, databases, and web servers.
- Conducted detailed analysis of security events using data from various sources such as firewalls, routers, operating systems, and intrusion detection/prevention systems.
- Created and delivered detailed incident reports and documentation for stakeholders and clients.

Executed **real-time monitoring, triage, escalation, and reporting of security incidents** from multiple log sources.
- Maintained up-to-date knowledge of emerging cyber threats to enhance incident detection and prevention strategies.
- Acted as a **primary point of contact for customers during high-priority incidents**, assisting with containment and mitigation efforts.
- Troubleshot **SIEM dashboard issues**, ensuring accurate and timely data reporting.
- **Engaged with clients to validate findings**, collect additional context, and ensure effective resolution.
- Assessed the scope and potential impact of security incidents, providing actionable remediation steps with supporting evidence.
- Demonstrated strong understanding of **OWASP Top 10 vulnerabilities, threat modelling, and common attack vectors** (e.g., DoS, DDoS, MITM, SQL Injection, XSS, CSRF).
- Investigated log source communication issues as part of initial troubleshooting.
- Generated alerts and **conducted in-depth analysis of anomalies found in live traffic** data.
- Compiled RCA documents and prepared routine reports (daily, weekly, monthly) for internal and client review.
- Supported global clients by continuously monitoring their environments for signs of malicious activity.
- Contributed to **incident response procedures during security breaches**, ensuring timely reporting and containment.
- **Conducted vulnerability assessments in production**, pre-production, and on-prem environments; coordinated with Windows teams for remediation.
- Performed daily threat hunting based on active IOCs from **threat intelligence** feeds **using SIEM, Zscaler, and EDR tools**; communicated findings with clients.
- Prepared and shared comprehensive SOC reports including **weekly metrics, bi-monthly adhoc reports, monthly KPIs, SLA reports, and quarterly/yearly summaries**.

Cognizant, Chennai
Security specialist *Sep' 2020 – Dec' 2020*

- Operated in a **24x7 Security Operations Center (SOC)** environment, leveraging multiple SIEM platforms and the ManageEngine ticketing system for effective incident management.
- Adhered to **standard operating procedures (SOPs) and playbooks to ensure consistent and efficient incident response**.
- Maintained accurate ticket documentation by updating trackers with detailed records of incidents, investigations, and resolutions.
- Compiled and submitted daily and weekly security incident reports along with operational performance summaries.
- Collaborated with Level 2 analysts in preparing monthly reports and conducting health checks on client infrastructure and security devices.

Supreme NetSoft, Hyderabad
IT Support Engineer *Aug' 2018 – Sep' 2020*

- Acted as the **first point of contact for IT support** via phone, email, and ticketing system, ensuring timely resolution of user issues.
- Logged, tracked, and prioritized incidents and service requests using ITSM tools to meet SLAs.
- Managed user account tasks including creation, password resets, and access provisioning.
- Provided technical support for Windows, macOS, and Linux operating systems.
- Assisted with basic network troubleshooting such as VPN connectivity and Wi-Fi issues.
- Installed, configured, and updated software applications in compliance with company policies.
- Maintained detailed records of resolved incidents, contributing to the internal knowledge base.
- Documented step-by-step troubleshooting procedures for recurring technical issues to streamline support.

EDUCATION

B-Tech – Computer Science Engineering
Kakinada Institute of college of Engineering and Technology, JNTU – Kakinada *2008-2012*

Vivek Thatikonda

+91 9059655105 | Vivekthatikonda9141@gmail.com | Hyderabad, Telangana 500035

PROFESSIONAL SUMMARY

Accomplished Security Analyst with over Five years of specialized experience in Information Security, focusing on security operations, incident response, and threat intelligence.
My expertise encompasses a deep understanding of SIEM solutions, including Splunk and XSOAR, complemented by practical skills in vulnerability assessments and endpoint security management.
I have a track record of efficiently dissecting security incidents, engaging cross-functional teams, and deploying effective security protocols.
I am eager to apply my capabilities to enhance the cybersecurity posture of a forward-thinking organization.

OWAS | Network | TCP/UD | Incident Response | Security | Incident | Threat | Effective | SIEM Architecture | Vulnerability Assessment | Log Analysis | Endpoint Security | Root Cause Analysis | Security Policies & Procedures | Encryption Techniques | Access Control | Training & Awareness | Complian | Emerging | Antivirus | Information Security | Intrusion Detection | SIEM | Malware | SPLUN

EXPERIENCE

INFORMATION SECURITY ANALYST, Hyderabad

Wipro, June 2020 - Present

- Orchestrated operations within a 24x7 SOC team, overseeing log monitoring, security information management, and threat analysis.
- Leveraged expertise in SIEM tools such as Splunk, XSOAR to analyze alerts and discern between true positives and false positives.
- Conducted root cause analysis for critical security incidents, documenting findings and proposing remediation strategies to mitigate risks.
- Facilitated incident remediation by communicating with end-users, ensuring swift resolution of reported incidents.
- Implemented access control measures and encryption techniques, fortifying data confidentiality and integrity.
- Contributed to the development and implementation of security policies, ensuring adherence to established guidelines.
- Maintained vigilance on emerging security trends, participating in meetings to discuss the current cyber threats landscape and provide strategic recommendations.

- Collaborated with technical staff to conduct threat assessments and enhance overall cybersecurity posture.
- Played a key role in investigating security incidents and recommending remediation steps, bolstering organizational resilience against cyber threats.
- Analyze Log events and protection from Database Injection (SQL) attacks and XSS attacks.
- Conducted training sessions on technology safety and security awareness, promoting good privacy practices.
- Participated in the deployment of intrusion detection systems to monitor for suspicious behavior, enhancing the organization's detection capabilities.
- Contributed to the creation of disaster recovery plans, including backup strategies for mission-critical systems and data, ensuring business continuity in the event of security breaches or other emergencies.
- Demonstrated expertise in analyzing system log files regularly to detect suspicious patterns indicative of potential
  security breaches, enabling proactive threat mitigation measures.
- Documented computer security policies, procedures, and tests, ensuring clarity and adherence to established protocols while facilitating continuous improvement in cybersecurity practices.

TECHNICAL ASSOICATE, Hyderabad
Tech Mahindra, Nov 2018 – Feb 2020

- Facilitated Technical Support for Telstra Customers in Australia regarding hardware, peripherals, network connections and Mail issues.
- Managed 30+ support tickets daily with a 99.8% success rate, and implemented ticket management best practices which slashed resolution time by 30%.
- Ensured 100% customer satisfaction by implementing effective strategies and eliminating the root causes of customer's technical issues.
- Achieved weekly productivity and quality targets by effectively prioritizing tasks, managing workload, and meeting established performance metrics.

EDUCATION

BACHELOR OF TECHNOLOGY
Jawaharlal Nehru Technological University,2018.

TOOLS

Operating System Known: Windows,
Linux. SIEM Tools: Splunk, IBM Qradar.
EDR: MDATP, TrendMicro, Carbon Black.
Exploitation Frameworks: CyberKill Chain, MITRE ATT&CK®.
Test Methodologies: OWASP TOP 10.
Security Tools: Palo alto, Microsoft Suite, SEPM
Antivirus. Ticketing Tool & SOAR: XSOAR, JIRA, SERVICE
NOW.

PERSONAL INFORMATION

Date of Birth: 05Th Nov 1996.
Languages Known : English, Hindi, Telugu.
Preferred Location : Hyderabad, Bangalore, Pune,
Remote. Marital Status: Single.

EXTRA CIRCULLAR ACTIVITIES

Binge Watching Netflix.

Tech Enthusiast & Avid Reader. Badminton.

SHWETA GUPTA

(91)8860066857 ◇ India
shwetag2511@gmail.com ◇ LinkedIn

OBJECTIVE

Cyber Security Operations Engineer with 4 years of experience in securing networks, systems, and cloud environments. Skilled in threat detection, incident response, vulnerability management, and leveraging SIEM and EDR tools to ensure optimal security posture.

SKILLS

SIEM and Cloud Security	ArcSight, LogRhythm, Wazuh, Cloudguard, AWS, Microsoft Azure
Endpoint Security and Other tools	Cisco AMP, ARCON PAM, Lansweeper, Nessus, Datadog
Technical Skills	Log Analysis, Malware Investigations, Vulnerability Management, Threat Intelligence, Incident Response, Privileged access management

EXPERIENCE

Thales (Avionics Domain) May 2023 - Present
Cyber Security Operations Engineer *Noida, U.P*

- Monitored and secured 400+ critical assets across Data Center and Airport sites, analyzing security logs to detect unusual authentication attempts, brute-force attacks, and privilege escalation events.
- Conducted log analysis of on-premise assets using LogRhythm, Cisco AMP and cloud environments with CloudGuard, Wazuh, Azure, and AWS to detect and mitigate potential threats.
- Hands-on experience responding to a real-world phishing and remote access attack, involving social engineering, PowerShell payloads, EDR evasion, and rapid containment through endpoint isolation, session revocation, and C2 block.
- Performed endpoint security investigations with Cisco AMP, correlating malicious file executions with user activity logs to prevent Trojan infections and credential theft improving operational efficiency by 20%.
- Identified vulnerabilities using Cyber Threat Intelligence, analyzing daily Avionics ISAC Memo reports to proactively detect threats.
- Conducted quarterly vulnerability assessments on systems and networks, identifying critical vulnerabilities such as missing patches and misconfigurations, leading to a 25% reduction in overall risk exposure.
- Collaborated with Product Owners to present detailed reports, including identified vulnerabilities, severity levels, and remediation recommendations, resulting in a 25% improvement in security posture in key systems.

DXC Technology (Health Care and Banking Domain) June 2021 - May 2023
Security Analyst *Noida, U.P*

- Worked as a Cyber Security Analyst at a 24x7 SOC, managing relationships with over five international clients utilizing ArcSight SIEM for threat detection.
- Created and fine-tuned filters, reports, and correlation rules in ArcSight to detect targeted attacks such as unauthorized access and unusual login behavior.
- Monitored the health status of SmartConnectors via ArcSight Logger and performed proactive troubleshooting for devices not sending logs.
- Led monthly security audits with clients and the CISO, strengthening security governance across environments.
- Managed privileged access using ARCON, overseeing creation, modification, and deactivation of privileged accounts.

CERTIFICATIONS

- CompTIA Security+ (SY0-701) **[August, 2024]**

EDUCATION

Bachelor of Technology in Information Technology, GGSIPU 2017-2021
CGPA: 8.6

Ashutosh Kumar Pati

Rourkela | ashutoshpati87@outlook.com | 8763944032

linkedin.com/in/ashutosh-kumar-pati-467b96184/

Professional Summary

Security Analyst with 3+ years of experience in security operations, cloud security, and Microsoft security products. Proficient in SIEM platforms like Azure Sentinel, with expertise in alert triage, fine-tuning, KQL-based rule creation, and building hunting queries and workbooks. Skilled in Microsoft 365 Defender, Defender for Cloud, Microsoft Intune, EDR, WAF, and Azure Firewall. Experienced with Zscaler, Abnormal Security and Vali mail. Strong collaboration skills in working with cross-functional teams to ensure prompt resolution of security incidents..

Education

Government College of Engineering ,Kalahandi, B.Tech in Electrical Engineering with minor in Computer Science and Engineering — Aug 2016 – Dec 2020

Experience

Security Delivery Analyst, Accenture – Pune, IND — Feb 2022 – Current

- Responsible for real-time security monitoring and incident response within a shared SOC environment. Identified and reduced false positive alerts by 50 percent within the first quarter, optimizing security event analysis and reducing noisy alerts, hence improving detection accuracy.
- Fine-tuned 5 use cases and developed 2 automation rules in Microsoft Sentinel and Microsoft Defender, automating 20 percent of routine security tasks and improving response times.
- Monitored security logs, identified, and investigated security incidents, and generated detailed reports. Collaborated with support teams to resolve incidents within SLA and achieved a 100 percent SLA compliance rate.
- Vigilantly monitored endpoint security posture, strengthened compliance gaps, and applied remediation strategies to maintain security standards. Secured the overall security compliance of workstation and servers to 90 percent.
- Managed email security by analyzing emails flagged by Defender, reported by users, or submitted directly by clients. Maintained a 100 percent secure environment against phishing attempts by identifying and blocking threats. Assisted clients by providing investigation reports when phishing link clicks were detected, reviewing logs, taking appropriate remediation actions, and delivering post-remediation reports. Reduction in spam and phishing emails reported by users up to 40 percent by proactive blocking and filtering.
- Conducted in-depth malware analysis on workstations and servers. Collaborated with end users and internal teams to determine the root cause of infections and carried out effective remediation measures.
- Enhanced cloud security posture by reviewing and implementing security recommendations from Microsoft Defender. Collaborated with cross-functional teams to address compliance issues and work on recommendations from the tools, resulting in a 92 percent compliance score.
- Developed and implemented detailed incident response plans, reducing the overall incident response time and efficiency by 30 percent. Documented and analyzed processes, identified and implemented more than 10 process improvements. Documented and maintained knowledge base for recurring incidents with resolution steps.
- Created firewall rules to enhance network security in Azure Firewall. Monitored network traffic flows to detect and respond to suspicious activity.
- Leveraged Zscaler security solutions (ZIA, ZPA) to enhance network security. Monitored Zscaler logs and alerts, responded to security incidents, and provided technical support to ensure optimal performance and security.
- Configured and Streamlined Zscaler policies to enforce security best practices and improve security and user experience.
- Actively helped in migration of 2 tenants to the existing Zscaler cloud for better user experience and security.

- Good knowledge of document creation. Have worked on weekly and monthly service reports.
- Conducted proactive threat hunting and contributed to the development of detection content
- Actively participated in daily stand-up calls to discuss ongoing incidents, trends and process improvements.
- Provided on-call support for high-severity security incidents, collaborating with incident managers to ensure swift mitigation.
- Managed end-to-end incident life cycle, ensuring timely resolution and documentation.

Certifications

- Microsoft Azure Fundamentals - AZ900
- Microsoft Security, Compliance, and Identity Fundamentals - SC900
- Microsoft Certified: Security Operations Analyst Associate- SC 200
- ZIA Admin Certification – Zscaler
- Microsoft Applied Skills: Configure SIEM security operations using Microsoft Sentinel- Applied Skill Badge

Tools Proficiency

- **Threat Detection and Response**: Microsoft Sentinel, Microsoft Defender for cloud, Sentinel One
- **Email Security**: Microsoft Defender for O365, Abnormal Security, Vali Mail
- **Endpoint Detection:** Microsoft Defender for Endpoint, Microsoft Intune, MCAS
- **Firewall**: Azure Firewall, Zscaler
- **CSPM:** Microsoft Defender for Cloud
- **Ticketing tool**: ServiceNow

Awards and Recognition

Skills Star Award, Recognized as an ACE Winner in FY24 Q3, 2024

Recognized by the team for Client Value creation, 2024

Kishan Agarwal

OT/IT Security Analyst & Specialist

Detail-oriented & Enthusiastic OT/IT Security Specialist with almost 8 years of expertise in managing vulnerabilities and implementing security controls. Aiming to assist organisations in achieving compliance and data integrity. Ability & Knowledge to utilize security controls to mitigate risk to achieve confidentiality and availability of OT systems.

kishanagrawala@gmail.com

+91 9826047577

Indore, India

linkedin.com/in/kishan-agarwal-787224b1

SKILLS

- OT Security
- IEC 62443
- NERC CIP
- NIS Directive
- Vulnerability Managment
- Patch Management
- Antivirus Software Deployment
- Whitelisting Software Deployment
- Backup and Disaster recovery tool
- Factory Security Audits
- MS PowerBI
- MS Power Automate
- SQL Queries
- Risk Management
- Security Controls Implmentation

LANGUAGES

English
Full Professional Proficiency

WORK EXPERIENCE

Information Security Analyst
American Express India Private Limited

07/2022 - Present — *Bengaluru - India*

Achievements/Tasks

- Contribute to the successful delivery of large scale company projects to enhance the security infrastructure by eliminating the risk and vulnerabilities with the help of automation within the specified timeline by collaborating with different team members.
- Research, identify and appraise emerging technologies, hardware and software to provide strategic recommendations for continuous improvements.
- IBM RACF Mainframe Database support and Security compliance monitoring using the help of automation.ITSM ticket support and CAB management for new requirement.
- BMC AMI administration and creation of use cases for security alerts, SIEM management.

OT Security Specialist
Siemens Gamesa Renewable Energy

02/2022 - 07/2022 — *Bengaluru - India*

Achievements/Tasks

- Execute the planning, design, development, and implementation of technical controls, procedures, and policies associated with cybersecurity compliance and /or regulatory standards.
- Maintain the highest level of integrity, protecting the confidentiality and security of all clients and project information.
- Perform detailed, post-event analysis of unusual events, and direct needed procedure or process changes in response. Resolve technical issues, analyse implications to the client's business, and be able to communicate them with applicable stakeholders within the business.
- IEC 62443 Requirement Analysis, Review of Sales Contract, NERC CIP, ISO 27001 Implementations.

OT Security Analyst
Tetra Pak India Private Limited

10/2018 - 06/2022 — *Bengaluru - India*

Achievements/Tasks

- Operational Technology systems end to end Compliance Management in terms of security controls. High level monitoring of all the security controls installed on an OT systems and servers.
- Implement processes and manage tools used to identify vulnerabilities and track their remediation within the OT environment.
- Responsible for security patch management and upgradation of virus definitions with latest software upgrades.
- Conducting and performing Factory Audits to determine security posture of the systems and the factory and using that data developing security assessment reports for factory directors and factory stakeholders.
- PowerBI report support, management, and creation of new reports according to requirements. Power Automate (MS Flow) hands on experience for Automation.

CERTIFICATES

CompTia Security plus (01/2025 - Present)

CompTia Cyber Security (11/2024 - Present)

Dear Hiring Managers,

I am writing to express my interest InfoSec L2 Security Engineer with Zoetis. With a bachelor's degree in computer science and 8 years of experience as an OT/IT Security Specialist, I have developed a strong background in handling security threats, managing data access, and leading security initiatives at my previous employer.

My professional experience involves proactively identifying and addressing security threats, as well as implementing effective security solutions for clients. I believe that my skills and experience align well with the requirements of the position at Zoetis.

Below are some of my most relevant accomplishments and experiences:

In my current organization i.e., **American Express India Pvt Ltd**., I am responsible for the IT security implementation which is IBM RACF Security and Database monitoring and making sure we are always up to date with latest security trends and software. I am also working on creating a security metrics to identify and analyze the security gaps proactively. I am working on the automation using SQL queries, SQL jobs, SQL procedures and using SQL functions, cursors etc. Furthermore, I am working on creating a security document for the entire team and setting up the timeline for the new project considering the priority of the project.

Working at **Siemens Gamesa Renewable Energy**, I was responsible for the OT security implementation and making sure they were compliant with the various country standards like IEC 62443, NERC CIP, NIS directive etc. I was also reviewing the sales contract in terms of cybersecurity. I was also performing test cases in a test environment to make sure products are up to date with the functionalities. Likewise, I was also working on Cybersecurity/SAT documents to ensure the assets are compliant with that.

Working at **Tetra Pak India Pvt Ltd**, I was responsible for overall security compliance of all the factory OT assets, servers, and workstations around the world which consist of 5000 assets. Developed regular security reports and presented findings to senior decision makers. I have implemented various OT projects which includes different security specifications/products. During these times, I have conducted various security audits around the Tetra Pak factories to determine security posture of the systems and the factory and using that data developing security assessment reports for factory directors and factory stakeholders. I was also responsible for security patch management and upgrade of virus definitions with latest software upgrades. Implemented processes and manage tools used to identify vulnerabilities and track their remediation within the OT environment.

Please feel free to contact me at **+91-9826047577** or via email at **kishanagrawala@gmail.com** for any further information. Thank you for considering my application. I look forward to the opportunity to discuss how my background, skills, and experiences align with the needs of Zoetis.

Sincerely,

Kishan Agarwal

AKSHARA M

CYBERSECURITY VULNERABILITY MANAGEMENT LEAD ANALYST

CONTACT

+91 80893 93893
akshararadhakrishnanclt@gmail.com
linkedin.com/in/Akshara
Kochi, Kerala, India

SKILLS

- Infrastructure vulnerability scanning
- DAST, SAST
- Policy compliance scanning
- Cloud & On-Prem Security
- Change Management
- Incident Resolution
- Automation (Python, C, C++)
- Reporting & Documentation
- Operating System (Windows, Linux)

TOOLS KNOWN

- Qualys
- Tenable (Security Center, VM, Nessus)
- CrowdStrike
- Rapid7 InsightVM
- Microsoft Defender
- Invicti
- Hadrian
- Snyk
- JFrog
- JIRA, ServiceNow, Fresh service

EDUCATION

College of Engineering, Vadakara
2018-2022
B. Tech CSE (Honors) – 8.3 CGPA

CERTIFICATIONS

Microsoft certified: Security Operations Analyst Associate (SC-200)

Qualys Guard Certified Specialist (VMDR)

REFERENCES

Sreejith K
Senior Technical Consultant
Sreejith.061@wipro.com
+91 94477 12627

PROFILE

Cybersecurity Analyst with 3 years of experience in vulnerability management, risk assessment and security compliance across cloud and on-prem environments. Skilled in threat detection, web application security, policy compliance scanning and automation. Proven ability to lead team, optimize security operations and enhance organizational security posture. Currently serving notice period.

EXPERIENCE

Vulnerability Management Lead Analyst

Wipro Limited (May 2022 – Present)

- Leading a 6-member team, successfully delivering security assessments across cloud and on-premises environment, for 10000+ Ips and 20+ applications per month, maintaining 95% on-time project delivery rate.
- Experience in deploying, configuring and managing vulnerability assessment tools.
- Conducted Dynamic Application Security Testing (DAST) using Tenable VM and Invicti, identifying vulnerabilities based on OWASP top 10 & SANS top 25.
- Executed Static Application Security Testing (SAST) using Snyk, to identify vulnerabilities in source code.
- Leveraged JFrog to scan and manage vulnerabilities in software artifacts.
- Engaged agent-based scanning in Qualys and InsightVM.
- Worked on Policy compliance, enhancing adherence of security benchmarks.
- Knowledge in change management process, including raising, assessing and implementing change requests.
- Migrated EOS vulnerability scanners from CentOS to Oracle Linux, upgraded scanners, and migrated RHEL servers to maintain compliance.
- Troubleshot and resolved scan and server level issues related to TVM tools.
- Proficiency in Python to automate reporting tasks, reducing manual report generation time by 50%.
- Acted as Transition SME, leading smooth KT and transfer of process, tools and responsibilities.
- Managed the remediation process by prioritizing vulnerabilities and coordinating with relevant teams to implement timely fixes.
- Analyzed threat intelligence feeds to author comprehensive vulnerability advisories, notifying threats and recommending remedial actions.
- Prepared customized reports, summaries, SOPs and status report decks.
- Experienced in handling various customers across different geographies.
- Resolution of requests and incidents within SLA.
- Mentored Junior analysts by providing guidance, training and support.

ACHEIVEMENTS

- Wipro Beyond Boundaries award for excellent client feedback.
- Wipro Habit Flagbearer award for due diligence and proactive approach.
- Wipro Inspiring performance award for team leadership and positive attitude.

VENKATESH VERIMELLA
Mobile: +91-8712403945
E-Mail: venkatesh.verimella94@gmail.com

Objective :

To be a continuous value addition to the organization to work in an innovative and competitive world, intend to build a career with a leading corporate with committed and dedicated people, which will help me to explore myself and realize my potential to the fullest

Career Record

Job summary :

Experienced SOC Analyst with a demonstrated history of working in the Computer & Network Security industry with an overall experience of 5 years in a SOC team, performing real-time monitoring, investigation, Incident Management, analysis, reporting, and escalations of Security events.

Experience:

Pegasystems India Worldwide PVT Ltd
June 2021 to Present

Roles and Responsibilities:

- Investigate escalated SIEM (Splunk & CS Nextgen) and EDR (Crowdstrike) alerts from our MSSP.
- Triage alerts, take appropriate actions, and contain endpoints if abnormal activity is detected via Crowdstrike Real-Time Response (RTR).
- Perform Threat hunting using various tools.
- Handle service requests and incident tickets using the ticketing tool.
- Perform DMZ scans in Tenable and respond to user queries.
- Check and Approve the IAM Sailpoint requests.
- Conduct monthly and weekly vulnerability scans using Tenable.
- Collaborate with respective teams to patch vulnerabilities and prevent potential security breaches.
- Conduct web application scans as well as AWS vulnerabilities.
- Generate HEC tokens in Splunk upon team requests and share the key via a secret password manager.
- Install the Splunk UF on the required servers with the help of the IT support team & reboot the machines if any updates are released.
- Install CS EDR sensors on servers that have not been installed and address challenges through communication with the support team.
- Schedule phishing campaigns and send simulated phishing emails to organization-level employees using the KnowBe4 platform.
- Conduct phishing awareness meetings with users who failed phishing tests.
- Review malicious flagged emails and address user queries about emails using the abnormal security platform.
- Handle Carblock Alerts to manage applications and remove unapproved software from endpoints.
- Perform mobile application scanning in MobSF and share scan results with remediation recommendations.

- Manage KnowBe4 security training and ensure compliance by following up with employees to complete assigned training.
- Configure Cribl Edge on servers to optimize data ingestion and streamline processing capabilities.
- Continuously monitor, assess, and manage our security posture to improve the organization's security score through BitSight/security scorecard remediation activities.
- Git guardian alerts monitoring.

Ernst & Young Global Delivery Services (GDS)
June 2020 to June 2021

Project Roles and Responsibilities:

- Monitoring Security Information and Event Management (SIEM) platform for security alerts. Integrate and work with the firm's Managed Security Services Provider (MSSP) services.
- Capable of working independently and involving senior analysts as necessary.
- performs monitoring, research, assessment and analysis on Intrusion Detection and Prevention tools as well as Anomaly Detection. currently dealing with SIEM Platforms: Splunk, LogR. EDR Tools: Carbon black, Crowd strike & Fidelis.
- Perform incident response activities such as host triage and retrieval, malware analysis, remote system analysis, end-user interviews, Performing monthly Threat hunting activities and remediation efforts.
- Follow detailed processes and procedures to analyze, escalate, and assist in remediation of critical information security incidents with respective with SLA.
- Raising Tickets, assigning tickets to concern teams and take follow ups on respective SLA's
- Produce situational reports from both SIEM and other service reporting tool

NETMAGIC IT SOLUTIONS PVT LMTD (NTT ONE)
MAY 2019 to June 2020

Project Roles and Responsibilities:

- Monitoring Mcafee SIEM , Mcafee epo ,Mcafee trusted sources and Smoke screen alerts.
- Perform incident response activities such as host triage and retrieval, malware analysis, remote system analysis and remediation efforts.
- Raising Tickets, assigning tickets to concern teams and take follow ups on respective SLA's.
- Provide network intrusion detection to support timely and effective decision making of when to declare an incident.
- Analysis multiple sources including events like: Email gateway events, Firewall logs. Proxy logs.
- Checking day to day integrated devices logs health status of critical devices and making reports, updating incident management day to day trackers.
- Analyze a variety of network and host-based security appliance logs (Firewalls, SWIFT server, WAF, IPS, NIDS etc.) to detect any threats and provide the correct remediation actions.
- Collect New/Existing Threat Feeds from various open source Threat Intelligence Platforms and Provide advisory reports, Working on Cert Advisory IOC Reports.

Technical Skills:

SIEM Tools
EDR Tools
Email security
Vulnerability management
GitGaurdian
Network security

Education:

Bachelors of Technology (E.C.E) – 2018
Sreyas Institute of Engineering and TechnologyHyderabad.

Declaration:

I declare that the above particulars are true, correct and complete to the best of my knowledge. I am also confident of my ability to work in a team

V. Venkatesh

ajay.baby@outlook.com
+91 9633910044
Bengaluru, India

Ajay B

Sr. System Security Administrator

SUMMARY

Cybersecurity professional transitioned from a successful 4-year career as an electrical project engineer, bringing valuable interdisciplinary insights to the cybersecurity field. My collaborative and coordination skills are empowering assets in my journey.

PROFESSIONAL EXPERIENCE

Sr. System Security Administrator - L1 Jan '23 - Present

Claysys Technologies Infopark,Kochi

- Secured digital banking websites by conducting in-depth vulnerability assessments, penetration tests, and providing expert consultation to developers. Identified and remediated critical vulnerabilities, ensuring robust protection of sensitive financial data.
- Led comprehensive weekly vulnerability assessments for servers and web applications, promptly addressing security issues to maintain a secure environment.
- Conducted advanced penetration testing on APIs, uncovering security weaknesses and implementing measures to ensure secure API communications.
- Performed thorough mobile penetration testing to identify and mitigate vulnerabilities in mobile applications, enhancing app security.
- Simulated Distributed Denial of Service (DDoS) attacks and conducted Web Application Firewall (WAF) tests to evaluate and strengthen firewall and front-end defenses.
- Prepared detailed penetration testing reports, including findings, risk assessments, and tailored mitigation strategies to address identified risks effectively.
- Managed security configurations and monitoring of firewalls, Cloudflare CDN, endpoint systems, and other security technologies such as 0365 Defenders and NETGEAR, ensuring swift incident response.

CERTIFICATIONS

- Certified Cybersecurity -ISC2
- Certified Associate Cybersecurity -Fortinet
- API Penetration Testing -APIsec University
- Python for Data Science -IBM

TECHNICAL SKILLS

- Skilled using Burpsuite,Qualys Postman, Nessus & Veracode for web penetration tests and infrastructure testing.
- Experience in using Kali Linux to do web application assessment and other attacks.
- Skilled in using ADB, MobSF, Drozer, and APKTool for mobile application security testing.
- Excellent at identifying business logic and other logic-level vulnerabilities in applications.
- Proficient in SAST & DAST utilizing various tools and techniques to analyze source code and detect potential security flaws.

EDUCATION

B.Tech - Electrical & Electronics Engineering Aug '13 - Jun '17

Nehru College of Engineering & Research Centre Thrissur,Kerala

One of the leading engineering colleges in kerala Accreated by NAAC

Second Class with 6.5 CGPU (Passed out in 2019)

Ishita Paul

9082209582 | ishitapaulip@gmail.com | https://www.linkedin.com/in/ishita-paul/ - Mumbai, India

SUMMARY

Enterprise Cloud Security Engineer with 2.5+ years of experience, working closely with cross-functional teams to follow security best practices. This helps to minimize risks, enhance compliance, and ensure business continuity and aids in securing cloud applications, network infrastructure, and data

EXPERIENCE

Revvity (FKA PerkinElmer, Inc.) - Mumbai, India (May 2023 - Present)

Enterprise Cloud Security Engineer, IT

- Created conditional purging rule in Qualys to streamline asset management and monthly removal of over 300 stale assets on average, reducing human time and effort.
- Reduced vulnerabilities in lab machines to 0, coordinating with the patch management team for CE+ certification.
- Scheduled daily Zero-Day vulnerability reports for every month and work with Patch Management team to bring down vulnerability count by 80%.
- Analyze and resolve on average 15 incident tickets per month on ReliaQuest ServiceNow with a Mean Time to Resolve rate of 3 days, leveraging KQL in Microsoft Sentinel.
- Applied least privilege access principles by providing Role-Based Access Control to users in platforms such as AWS, Wiz.io and Qualys.
- Drafted policy for enforcing exclusively HTTPS requests for S3 buckets to ensure encryption at rest and in transit in AWS.
- Created security-centric visualizations in Power BI and Spotfire for 70 projects, fetching data from Wiz API.
- Created POCs for project teams for container image scanning using GitHub Actions and Wiz CLI for detection and remediation of vulnerabilities, reducing vulnerabilities by 98%.
- Established asset inventory for lab assets, based on 18 locations; each location list comprised on average 225 IP addresses, DNS hostnames and asset type, fetching data from Qualys Map Scans and Microsoft CASB

Honors: *Making a Difference*

PerkinElmer, Inc. - Mumbai, India (July 2022 – May 2023)

Enterprise Cloud Security Engineer, IT **(January 2023 – May 2023**)

- Created security audit reports for each cloud subscription in the organization for ISO 27001 certification.
- Implemented controls pertaining to CIS and STIG security standards by hardening Linux/Unix images AWS Image Builder, increasing compliance score to 87%.
- Developed POC for 5 cloud project teams to allow federated access to AWS resources using OpenID Connect in GitHub Actions for secure deployment of resources.
- Shifted sensitive healthcare data from personal to corporate Google Drive and performed security assessment for project to implement security controls, such as encryption-in-rest (AES-256) and transit (TLS).

Management Trainee - Cyber and Information Security, IT **(July 2022 – January 2023)**

- Implemented Security Best Practice of restricting access to unauthorized ports in AWS by creating Lambda functions to automatically delete security group rules created using ports such as port 22 and 3389.
- Performed static and dynamic application security testing in Veracode and Snyk for projects to prioritize and mitigate vulnerabilities.

CERTIFICATIONS

International Information System Security Certification Consortium (ISC2) – Certified in Cybersecurity
Certification Cycle: Dec 2023 - Nov 2026

EDUCATION

Mumbai University – Bachelor of Engineering (B.E.) in Computer Engineering – Graduated: May 2022: CGPA: 9.23/10

SKILLS:

KQL | Microsoft Sentinel | Qualys | Power Platform | AWS | Wiz.io | Python | GitHub Actions| Threat Modelling | ReliaQuest ServiceNow | Spotfire | Microsoft CASB | Snyk | Veracode| Jenkins

Nagaraj
Ph: 9908393449
Email: cherukunagaraj01@gmail.com

OBJECTIVE

To excel in the field of Information Technology as a Cloud Engineer by contributing continuously towards organizational growth by providing database support and to utilize every opportunity to achieve both personal and professional development.

PROFESSIONAL SUMMARY

- Having 10 years of IT experience.
- Proficient in AWS services like VPC, EC2, S3, ELB, Autoscaling Groups (ASG), EBS, RDS, IAM, Cloud Formation, Route 53, CloudWatch, Cloud Trail, SES, SNS.
- Experience of Cloud Security Tools (e.g., AWS Security Hub, Azure Security Centre)
- Created NAT gateways and instances to allow communication from the private Instances to the internet through bastion hosts.
- Installed and Setup Web Servers (Apache Tomcat), DB Server (ORACLE/SQL SERVER).
- Creating/Managing AMI/Snapshots/Volumes, Upgrade/downgrade AWS resources (CPU, Memory, EBS)
- Extensive experience in Provisioning, Installation and Configuration of Oracle Server 11g, 10g on different flavors of UNIX (OEL, RHEL, Windows) operating systems.
- Experienced in Performance Tuning and Query Optimization in ORACLE Database
- Implementation and maintaining Database Security by creating users, grant/revoke roles, privileges, creating and assigning Profiles to the users.
- Experience on Azure cloud platform
- Knowledge on AWS Inspector for Vulnerability management
- Experience in Migrating On-Premises DB to AWS RDS using AWS DMS.
- Experience of Cloud Security Tools (e.g., AWS Security Hub, Azure Security Centre)
- Experience in Trend micro deployment and configuration
- Hands on experience in Vulnerability Management,
- Implementing security policy changes
- Performing daily, weekly, and monthly checks
- Monitoring the availability of systems and responding to alerts
- Monitor the capacity of systems & supporting infrastructure and project future capacity.
- Setup/Managing VPC, Subnets make connection between different zones, Blocking suspicious Ip/subnet via ACL.
- Knowledge with provisioning, implementing, and maintaining Microsoft Azure Platform as a Service (PaaS) services.
- Experience with creating and managing subscriptions and resource groups.
- Experience in Windows AZURE(IaaS) migrating like creating AZURE VMs, storage accounts, VHDs, and creating availability sets in AZURE.
- Experience in configuring Application Gateway

Educational Qualifications:

- Master of Computer Applications from Osmania University.
- B.Sc. (computer Science) from Osmania University.

Professional Experience:

- Worked for eTEAM Info services Private Limited from July 2013 to Feb 2016
- Worked for Cognizant Technology Solutions from May 2016 to Nov2021
- Working for Wipro LTD from Dec 2021 to Till date.

TECHNICAL SKILLS

Operating System	Red Hat Linux, Window server 2012,2016,2019
Release Management	Patching, Updates of Application and Version.
AWS /Azure	VPC, EC2, S3, ELB, Autoscaling Groups (ASG), EBS, RDS, IAM, Cloud Formation, Route 53, CloudWatch, Azure Storage, Azure App services, Azure Virtual Network, Resource Groups, Application Gateway, Azure DMS, Security Center, Guard Duty
	• Security event and log analysis • Security control implementation • Risk analysis and mitigation. • Cloud security technologies and tools • MS Defender AV & EDR /Trend Micro EDR & AV • Vulnerability Management

Professional Experience:

Project : AWS/Azure Infra support
Client : Philips Healthcare
Role : Cloud Engineer
Environment : AWS Cloud and Azure Cloud

Roles and Responsibilities:

Cloud Admin:

- Setup/Managing Linux Servers on Amazon (EC2, EBS, ELB, SSL, Security Groups, RDS and IAM).
- Setup/Managing VPC, Subnets make connection between different zones, Blocking suspicious Ip/subnet via ACL.
- Knowledge with provisioning, implementing, and maintaining Microsoft Azure Platform as a Service (PaaS) services.
- Experience with creating and managing subscriptions and resource Groups.

- Experience in Windows AZURE(IaaS) migrating like creating AZURE VMs, storage accounts, VHDs, and creating availability sets in AZURE.
- Experience in configuring Application Gateway.
- Knowledge on Azure DMS.
- Knowledge on Azure Storage services
- Develop PowerShell scripts and ARM templates to automate the provisioning and deployment process.
- Setup/Managing Databases on Amazon RDS. Monitoring servers thorough Amazon CloudWatch, SNS.
- Creating/Managing DNS records on Amazon Route 53.
- Creating/Managing AMI/Snapshots/Volumes, Upgrade/downgrade AWS resources (CPU, Memory, EBS)
- Configured AWS Identity Access Management (IAM) Group and users for improved login authentication.
- Maintained the monitoring and alerting of production and corporate servers using Cloud Watch service.
- Created EBS volumes for storing application files for use with EC2 instances whenever they are mounted to them.
- Implemented Amazon RDS multi-AZ for automatic failover and high availability at the database tier.
- SFTP server configuration for user to upload and download files to AWS servers.
- Bastion (Guacamole) server configuration on Docker container for accessing AWS/Azure Instances.
- Windows Remote desktop licensing server configuration.
- Interacting with Application support team, other vendor and customers for planning and implementation of new changes in environment on daily basis.
- Knowledge with provisioning, implementing, and maintaining Microsoft Azure Platform as a Service (PaaS) services.
- Implemented Amazon RDS multi-AZ for automatic failover and high availability at the database tier.
-

Database Admin

- Installed and Setup Web Server (Apache and Tomcat), DB Server (Oracle/SQL Server)
- Oracle Database backup (Hot/Cold) and recovery, repair and optimize tables,
- Oracle Database security, creating users and managing permissions.
- Server's, Domain’s, and Database's migration on Amazon Web Services.
- Setting up a new DNS and a corresponding VHOST to make the website functional.
- Log Analysis, Maintaining documents of Production server error log's reports.
- Monitor Production Server Health of different parameters (System Load, Swap Memory, Hard disk, Apache requests) via Nagios and CloudWatch.

Security Admin

- Cloud Security Deep AWS knowledge Security Services (Guard Duty, CloudTrail, Security Hub, AWS Inspector, etc.)
- Strong knowledge on Azure Sentinel, Defender for Identity, Defender for office, Defender for Cloud, M365 Defender, Intune, Azure Information protection

- Manage operations within a cloud solution environment such as operations tasks, using cloud native tools, like Log Analytics, Azure Monitor and Azure Security Center or other monitoring tooling.
- Design and implement security solutions for Azure-based applications, systems, and networks.
- Experience in analyzing infrastructure implementations from a security perspective.
- Configure and manage Azure security services, including Azure Active Directory, Azure Information Protection, Azure DDoS protection, and Azure Firewall
- Monitor Azure resources for security issues and investigate potential threats.
- Good Experience on Azure Monitor and Application Insights.
- Good Experience on Configuring Network Security Groups (NSG) in Azure as Firewall.
- Good Understanding of Risk, Threat and Vulnerability.
- Knowledge of cloud infrastructure security controls such as Identity & Access Management (e.g., Oauth, AD) and network security (e.g., Application Gateway, Web Application Firewalls)
- In-depth understanding of Azure Security components/services like Azure firewall, Azure firewall manager, Azure front door, WAF, NSG, Internet analyzer, Bastion, Defender, Key Vault, Sentinel, etc.
- Strong understanding of how to securely interconnect multiple cloud accounts, on-prem servers, etc.
- Vulnerability Remediation for Windows servers and creating reports & Dashboards.
- Hardening Windows OS as per the CIS Benchmark Standards to create Golden Images.
- AWS NACL & Azure NSG Rules review & mitigation
- Managing Servers hosted in AWS/Azure/On-prem via TrendMicro & MS Defender AV Solutions
- CSPM For AWS & Azure detection and mitigations
- Create and execute PowerShell scripts for remediating CIS Benchmark fixes

ARCHESHMA BODHANAPU

INFORMATION SECURITY ENGINEER

+91-9618402315 | archeshmabodhanapu@gmail.com | linkedin.com/in/archeshma-bodhanapu-7a74bb230

Proactive Cloud Security Engineer with deep expertise in securing multi-cloud environments across AWS, GCP, and Azure. Skilled in Cloud Security Posture Management (CSPM), Cloud Workload Protection Platform (CWPP), database security controls audit, and firewall audits. Adept at investigating and responding to SOC-related alerts and cloud security incidents, ensuring compliance with industry security standards. Experienced in implementing and evaluating security controls, collaborating with cross-functional teams like techops to enhance cloud security posture, and mitigating potential threats. Passionate about securing cloud infrastructure and optimizing security frameworks for enterprise environments.

PROFESSIONAL EXPERIENCE

Gainsight Solutions Private Limited

- *Information Security Engineer* *Feb 2025 - Present*
    - Securing multi-cloud environments (AWS, GCP, Azure) with expertise in CSPM, CWPP, database security controls audits, firewall audits, and infrastructure security.
    - Investigating and responding to SOC-related cloud security alerts and incidents, ensuring rapid mitigation and compliance with security standards.
    - Conducting security assessments, enforcing cloud security best practices, and collaborating with cross-functional teams like techops to strengthen security posture.
    - Implementing and evaluating security controls to detect vulnerabilities, mitigate risks, and enhance cloud security frameworks.
    - Driving security automation and continuous monitoring initiatives to improve threat detection and response.

- *Associate Information Security Engineer* *June 2023 - Jan 2025*
    - Conducted CIS Benchmark assessments for AWS, GCP, and Azure, ensuring cloud environments adhered to industry security best practices.
    - Worked on ISO 27001 compliance implementation and audits across AWS, GCP, and Azure, strengthening cloud security governance.

- Performed database security controls audits in AWS, GCP, and Azure to identify vulnerabilities and enforce security policies.
- Assisted in securing multi-cloud infrastructures by evaluating security configurations and recommending improvements.
- Collaborated with internal teams to enhance cloud security posture and align with regulatory compliance requirements.

- *Intern - Information Security* *Nov 2022 - May 2023*
  - Conducted penetration testing for major and minor product releases to identify security vulnerabilities.
  - Discovered and reported security bugs, working closely with development teams to ensure timely fixes.
  - Assisted in improving secure coding practices by providing insights from security assessments.
  - Contributed to enhancing the overall product security posture through continuous testing and risk analysis.

WeSecureApp

- *Junior Security Analyst* *May 2022 - Aug 2022*
  - Conducted penetration testing across multiple projects to identify security vulnerabilities.
  - Discovered and reported critical security issues, including an account takeover vulnerability, leading to enhanced security measures.
  - Performed web and application security assessments, ensuring compliance with security best practices.

ERSegment Solutions Pvt Ltd

- *Cyber Security Analyst* *Feb 2021 - March 2022*
  - Trained 500+ students in Cybersecurity, Ethical Hacking (CEH), and Networking.
  - Conducted sessions on penetration testing, network security, and vulnerability assessment.
  - Mentored students in security best practices and industry certifications.

EDUCATION QUALIFICATION

- Bachelor's of Technology — 2017-2021
  St. Martin's Engineering College — *Hyderabad*
- Higher Secondary School (CBSE) — 2015-2017
  St. Andrew's School — *Hyderabad*
- Secondary School (SSC) — -2015
  St. Peter's Grammar School — *Hyderabad*

CERTIFICATIONS

- AWS Certified Solutions Architect
- SY0-701 - CompTIA Security+
- AWS Certified Cloud Practitioner
- ISC2 - Certified in Cybersecurity
- Google Cloud Digital Leader
- Certified Ethical Hacker (CEH v11) - EC-Council

TOOLS

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure
- Lacework
- Qualys
- Burpsuite
- Crowdstrike
- Optiv
- Securonix
- Kali Linux

PROJECTS

- Integrating AWS, Azure with Lacework for CSPM and CWPP – Configured and onboarded cloud accounts to Lacework for continuous security posture and workload protection monitoring.

- CIS Benchmark, ISO/IEC 27001-2022 - AWS, GCP, Azure – Assessed cloud environments against CIS and ISO 27001 standards, identifying compliance gaps and recommending security improvements.

- Database Security Controls Audit – Evaluated database security configurations across AWS, GCP, and Azure to ensure compliance with security best practices and regulatory requirements.

- Security Group, Firewall Audit - AWS, GCP, Azure – Analyzed security group and firewall rules to detect misconfigurations, enforce least privilege access, and enhance network security.

LANGUAGES KNOWN

- English
- Hindi
- Telugu

VEERENDRA JEELAKARRA

+918106479465 · veerendraj.0111@gmail.com · www.linkedin.com/in/veerendra-veeru-061565355/

Efficient and result oriented security professional with experience in Vulnerability Management, Threat Management, Endpoint Protection, EDR, XDR, MS365, Threat Hunting, Incident Response and ATP.

PROFILE SUMMARY

- Information Security professional with around 3.5 years of experience in Endpoint Protection.
- Effective handling of major stake holders and partners/clients with large environments, troubleshooting and providing with best practices.
- Experience with Endpoint security, Endpoint detection and response (EDR), Network security with the products like Microsoft Defender for Endpoint and Secure score.
- Hands-on experience using tools like Windbg, Procmon (Process monitor), Windows Event viewer, Wireshark, diagnostic data for Linux, mac.

PROFESSIONAL SKILLS

- Endpoint Protection
- Microsoft Defender for Endpoint
- Endpoint Detection and response (EDR)
- Extended Detection and Response (XDR)
- Security Architecture management
- Vulnerability management
- Endpoint configuration management
- Incident management
- Endpoint Compliance and coverage
- Attack surface Reduction
- Cyber Kill chain model
- TTP's and MITRE ATTCK Techniques
- Web Content Filtering

EXPERIENCE

Dec 2023 – Present (Microsoft (Ushta Te Consultancy Services llp)
Technical support Engineer (Microsoft Defender for Endpoint),

Key responsibilities and Expertise

- Providing technical support and troubleshooting for Microsoft Defender for Endpoint.
- Assisting customers with the installation, configuration, and maintenance of Microsoft Defender for Endpoint.
- Investigating and resolving security incidents and vulnerabilities.
- Collaborating with other teams to ensure seamless integration and operation of security solutions.
- Conducting workshops and training sessions for customers to enhance their understanding and usage of Microsoft Defender for Endpoint.
- Proficiency in endpoint security solutions, particularly Microsoft Defender for Endpoint.
- Strong understanding of cybersecurity principles and practices.

- Experience with troubleshooting and resolving technical issues related to endpoint security.
- Knowledge of various operating systems, including Windows, macOS, Linux, and mobile platforms.
- Familiarity with security incident response and vulnerability management
- Employed advanced Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Security Information and Event Management (SIEM) tools to proactively safeguard environments from security vulnerabilities.
- Played a pivotal role in incident management, resolution, documentation by preparing RCA. overseeing resolutions and providing strategic insights through comprehensive incident reports. • Fostered seamless collaboration with internal teams, clients, and vendors to deliver tailored security solutions in adherence to strict SLA standards.
- Facilitated client onboarding and offboarding, mass deployments processes within Microsoft Defender for Endpoint.
- Implemented and managed Group Policy Object (GPO) configurations, including scheduling daily and weekly scans and handling exceptions via SCCM and MECM portals.
- Orchestrated proxy configurations and endpoint deployment and management through the Defender console.
- Executed whitelisting file submissions and oversaw alert management procedures.
- Participated in migrations from Microsoft Monitoring Agent to a unified solution.
- Managed Defender platform upgrades, engine connectivity with the MDE portal, and customized reporting using advanced hunting techniques.
- Involved in isolation of devices, detect, analyze and respond to security threats via SIEM.
- Monitored incidents and warnings in the MDE portal, ensuring timely security intelligence updates.
- Troubleshooted issues related to security intelligence updates, client onboarding, and exception policy configurations by analyzing security client analyzer logs.
- Conducted internal triage calls to review customer-driven DCRs (Design Change Requests) focused on continuous feature improvements, in collaboration with the Microsoft product team.
- Collaborated internally with the product and development teams to address bugs, implement continuous feature changes, and analyze issue fluctuations, ensuring seamless support and resolution for customers.
- Worked on and tested Intune configurations, deploying policies via the Microsoft Intune portal for both Microsoft Defender for Endpoint and Mobile Device Management (MDM).
- Seamlessly collaborated with Purview, Sentinel, Intune, and Messaging Protection teams to ensure customer queries were addressed on priority, while consistently maintaining high SLA standards

Dec 2021 to Oct 2023 (Tata Consultancy Services)
Assistant System Engineer

Key responsibilities and Expertise

- Successfully monitored and responded to security incidents, minimizing potential risks and impacts.
- Conducted thorough investigations into security alerts, providing valuable insights and recommendations.
- Collaborated with cross-functional teams to develop and implement security solutions tailored to organizational needs.
- Participated in security awareness training sessions to educate employees on best practices and potential threats.

Domain Expertise

Domain	Specific area in domain	Experience (yrs/months)
End Point Security	Security	3+ years
Security Incident management	Security	3+ years

Technical Expertise

Primary skills	Experience (yrs/months)	Secondary skills	Experience (yrs/months)
MS 365 Defender	3	Defender AV	2
Endpoint detection and response	3	XDR	3
Security Incident & Change Management	3		1.5

EDUCATION

B. TECH IN CIVIL ENGINEERING (2018 to 2021)
GIET Engineering College

Anurag Suresh Akula

7093525063 • anurag.suresh17@gmail.com • Hyderabad, India 500026

Summary

Assistant System Engineer at Tata Consultancy Services with strong expertise in Unix and PL/SQL. Achieved significant improvements in server reliability and successfully executed system upgrades on schedule. Skilled in using PL/SQL to optimize operations, complemented by robust analytical capabilities and effective communication. Committed to delivering high-quality solutions in dynamic environments while continuously learning new technologies such as AWS, Python, Networking, and Cybersecurity.

Skills

- Amazon Web Services (AWS)
- Cybersecurity: CIA Triad, NIST CSF, PASTA, OSI Model, protocols, ports
- Network Security: Vulnerability Scanning, Router Management, Firewalls, Network Architecture, Network Monitoring, DHCP, NAT, DMZ
- Work with hashes (MD4, MD5, SHA-256)
- Tools and software: Nmap, Zenmap, Microsoft Baseline Security Analyzer, PuTTY, ServiceNow, VS Code, Jira, PostgreSQL, Microsoft Word, Microsoft Excel, Debian, and Kali
- PL/SQL
- Linux
- Python (intermediate level)

Experience

03/2022 - 03/2024
Assistant System Engineer, **Tata Consultancy Services**, Hyderabad, India

- Managed telecom data and services by analyzing call data and retrieving information for government authorities when required.
- Ensured continuous server uptime and reliability by managing and maintaining server operations 24/7.
- Implemented system upgrades in production environment and conducted testing of deployments within the development environment.

Relevant Experience (06/2024 - Present)

- Working on the Hospital Information Management System (HIMS), where my team and I manage the workflows of each data flow (PuTTY, PostgreSQL)
- Monitoring and safeguarding the log sources and security access
- Planning for disaster recovery in the event of any security breaches (chain of custody, CIA triad, PASTA)
- Monitor for intrusions and unusual, unauthorized, or illegal activity, including log monitoring
- Create necessary documentation (SOP) in case of any future events (NIST CSF)

Education And Training

07/2021
Bachelor Of Engineering, Civil Engineering
Maturi Venkata Subba Rao Engineering College, Telangana, India

Activities

- Very much into resistance training and calisthenics.
- I love playing cricket, snooker, and table tennis.

Certifications

- Amazon Web Services (AWS) Certified Cloud Practitioner (CLF-CO2)
- Google Cybersecurity Professional Certificate V2!

SREE VYNATHEY REDDY MALLEPALLI

+919790092254 | sreevynathey.reddy@gmail.com | linkedin.com/in/sree-vynathey-reddy/

Professional Summary

- A result-oriented professional with 6+ years of experience highly dedicated in the domain of Security administration, Security Operations, Endpoint Security and Vulnerability Management.
- Qualified in evaluating end-user requirements and troubleshooting for complex problems.
- Reviewed new security policies, drafted and implemented security procedures and work instructions.
- Solid understanding of networking concepts.
- Good knowledge on cyberattacks and attack vectors.
- Working level knowledge on security solutions like Antivirus, EDR, SIEM etc.
- Basic knowledge on skills like Ethical hacking, Threat Hunting.
- Exposure to frameworks and compliances like MITRE ATTCK, HIPAA etc.
- Good understanding of various SOC processes like monitoring, analysis, playbooks, escalation, issue documentation, SLAs, client meetings, bridge calls etc.
- Hands on expertise in administering windows servers and VMware virtualized infrastructure.
- Good experience in working/communicating with cross-functional IT infrastructure teams like network, system, database, application, security to build and manage effective security operations.
- A team player with strong communication, analytical, logical and problem-solving skills.

Skills

Antivirus/EDR: CrowdStrike Falcon, McAfee, Cylance, TrendMicro

SIEM/SOAR: QRadar on Cloud, Splunk, Cortex XSOAR

Vulnerability Management: Qualys, Rapid7 Nexpose

Network Segmentation: Illumio

Certificate Management: Venafi

ITSM Tools: Service Now, Salesforce (OneEMS and ServiceMax), Rally

Operating Systems: Windows, Linux

Additional Skills: VMware virtualization, Wireshark

Core Competencies: Security Operations, Security Administration, Endpoint Security, Vulnerability Management, Team Management

Work Experience

Invesco, Hyderabad

Advanced Engineer (Security SME) **Dec 2023 - Present**

- Approved ***300+*** new software installations/upgrades across the organization.
- Performed upgrades of CrowdStrike Falcon sensor and Illumio VEN agent.
- Worked with respective support teams to install/upgrade CrowdStrike sensor and Illumio VEN agents to latest version as part of reconciliation .
- Handled user access management tasks for various security tools like CrowdStrike, Cylance and QROC.
- Assisted in Qualys New Appliance deployment/appliance migration.
- Supported validation of security tools as part of post checks for DC related activities.
- Provided use cases for automation using XSOAR.
- Reviewed the Power BI Security dashboard to identify repetitive tasks and successfully delegated them to the CSS team.
- Streamlined workflows by transitioning ***90%*** of requests and incidents from the Power BI report to the CSS team, reducing manual effort and increasing efficiency.
- Acted as a reliable escalation point for NOC and L1 teams, ensuring prompt issue resolution.
- Gathered feedback from L1 and NOC teams to refine processes and address challenges.

- Enhanced efficiency by reviewing and updating SOPs and KB articles to align with current practices.
- Spearheaded as team's representative in meetings, presentations or discussions with other departments or stakeholders.

Infosys, Hyderabad
Senior Associate Consultant (Cyber Security) **Jun 2022 - Dec 2023**

- Performed health checks of TrendMicro, Rapid7 Nexpose and Splunk dashboards.
- Troubleshot the issues if health checks are not normal.
- Worked with vendors to fix the errors related to the application.
- Product version upgrades of servers in TrendMicro and Splunk.
- Reset passwords of Swift HSM boxes.
- Managed user access by approving the requests based on their role in IAM tool.
- Renewed certificates which are about to expire and creating new certificates in Venafi.
- Managed vulnerabilities i.e., exporting report, segregating VITs based on OS and application and tracking them on weekly basis.
- Coordinated with internal and VM teams to mitigate vulnerabilities.
- Created service requests, changes in ServiceNow and working on incidents getting assigned to our security group.
- Assisted in creation of user stories in Rally, as a part of Sprint planning for 2-week iterations.

Philips, Bangalore
Security Engineer **Jun 2019 - Jun 2022**

- Managed McAfee, Cylance and TrendMicro central dashboards.
- Deployed endpoint security solutions across the field (AV/EDR, Firewall and STIGS)
- Regularly patched all servers in install base based on Nessus scan report.
- Regular product version upgrade of all components.
- Complex and sophisticated troubleshooting of security related field issues.
- Worked with vendors and internal partners to resolve complex field issues.
- Worked with RnD team on the security solutions implementation and bug fixes.
- Created tickets in salesforce and analysed the cases which are assigned to security queue.
- Incident responder which includes first level of investigation for security incidents.
- Escalated Security incidents to incident response team.
- Administered Thycotic secret server and DLP server.
- Generated Compliance reports on weekly, monthly data and present it to management to define the compliance and coverage.

Philips, Bangalore
Intern **Jan 2019 - Jun 2019**

- Saved manual work hours by automating the tasks.
- Created scripts for Antivirus installation/removal on remote servers using Powershell.
- Developed Python Script to merge Antivirus servers export data for Compliance reports.
- Performed encryption on the PACS (picture archiving and communication system) servers using Bloombase store safe and ESKM (Enterprise Secure Key Management).

Education

Vellore Institute of Technology Vellore, Tamil Nadu
Bachelor's Degree in Electronics and Communications Engineering, CGPA: ***9.59*** ***2019***

Narayana Junior College Hyderabad, Telangana
Grade 11 and 12 Education, Percentage: ***97*** ***2015***

Narayana E-Techno High School Anantapur, Andhra Pradesh
Class 10th Education, GPA: ***9.7*** ***2013***

Certifications

- CrowdStrike Certified Falcon Adminstrator
- Splunk Enterprise Certified Admin
- Splunk Core Certified Power User
- Certified Ethical Hacker v11 (EC Council)
- CompTIA Security+ SY0-501 (Udemy)
- Certified Network Security Specialist by ICSI (International Cybersecurity Institute), UK
- AZ-900: Microsoft Azure Fundamentals

Achievements

- Infosys ***Client Certificate of Recognition*** from Head of Technology for mitigating the vulnerabilities from 12000+ to 500 in 9 months.
- Infosys ***Insta awards*** appreciation for excellent work done on antimalware installation on production servers.
- Philips ***behavior (Customers first) recognition*** as a part of team which delivered ESU deployed Netlogon patches for entire PACS install base in just 3 weeks.
- ***Merit Certificate and Top 10 Rank holder*** - Awarded Merit Certificate Scholarship ***consecutively for three years*** for outstanding academic excellence in B.Tech.
- Secured ***5th rank*** out of around ***700 students*** in the ECE department.

NEHAL LIMJE

https://www.linkedin.com/in/nehal-limje-373811120/
Nagpur, Maharashtra, India | (+91) 8149787961 | limjenehal@gmail.com

PROFILE SUMMARY

A detail-oriented security professional with 5.2 years of experience working in Cloud Security and SOC domain, protecting infrastructures and enterprise data across cloud environments. Skilled in integrating the Cloud infrastructure and assessing security risk. Experienced in automating security controls and developing security policies. Specialized in Security Operations, Vulnerability Management, Security Monitoring and Incident Response leveraging tools such as SIEM, EDR and Defender suite. Proven track record of improving the security posture, committed to delivering secure, scalable and resilient cloud environments.

WORK EXPERIENCE

Litera Technologies, India (Remote) May 2023 – Present

Security Operations Analyst – Cloud Security & SOC

- Secure cloud environments and check for security misconfigurations.
- Develop and enforce cloud security policies using Microsoft Intune, Entra Admin center, MS Purview, Defender etc.
- Manage user access controls, MFA and IAM policies to ensure secure access to cloud resources.
- Address vulnerability issues and take care of third-party risk assessments.
- Assist in integrating and migrating services within the cloud.
- Help in the implementation of security controls and measures across cloud environments.
- Hands-on experience with SIEM fine-tuning, automation workflows and log integration.
- Ensure compliance with industry standards & regulations such as ISO 27001, NIST, CIS, PCI DSS, HIPAA, GDPR & SOC 2.
- Monitor cloud environments for threats. Respond to and investigate security incidents using tools such as Sentinel, Defender and Dark Web for threat detection.
- Run phishing campaigns using MS Defender to check organizational receptivity to defend against phishing attacks.

Accenture, Pune, India May 2022 – May 2023

Cloud Security Analyst – Managed Security Services

- Helped to develop a stronger cloud security environment in line with regulation and/or current standards, such as ISO27001, NIST, CIS etc.
- Supported the migration and integration of cloud security infrastructure.
- Built platform security policies such as Conditional access, Email, Intune, Information protection and Mobile device management (MDM) policies tailored for each cloud environment.
- Created and deployed analytics rules and logic apps within Sentinel to enhance security monitoring and response.
- Responded to and remediated security incidents, threats and phishing attacks, leveraging tools like Sentinel, Microsoft Defender and Splunk for detection and analysis.
- Integrated Windows and Linux devices with Microsoft Sentinel for log ingestion.
- Managed and configured DNS records, email records and WAF rules within Cloudflare.
- Automated security controls and processes to enhance operational support.

Capgemini, Mumbai, India Feb 2020 – May 2022

SOC Analyst

- Monitored and responded to security incidents on a 24/7 basis utilizing Qradar, Defender, Symantec and Crowd strike EDRs for detection.
- Triaged, investigated security incidents and coordinated incident response with detailed post-incident reports.
- Managed lifecycle of incidents from detection to analysis, containment, eradication and recovery within a defined SLA.
- Assessed vulnerabilities using Qualys, scanned critical devices and worked with the relevant teams to fix the identified weaknesses.
- Integrated Windows and Linux devices with Qradar for log collection.
- Worked in collaboration with cross-functional teams to research and resolve complex security issues.

KEY SKILLS

Cloud Security Architecture, Threat and Platform protection, Email Security, Vulnerability Management, Log Analysis, Security Monitoring and Incident Response, Endpoint Security, Network Security, Vulnerability Assessment, Identity Access Management systems, Security Operations, Threat Hunting, URL filtering and Security Automation.

HANDS ON TOOLS

Microsoft suite tools: Entra ID, Entra ID Security, Defender for Endpoint, Defender for O365, Defender for Cloud Apps, Intune, Sentinel, Exchange Admin Center, MS 365 Admin Center and Microsoft Purview.

SIEMs: IBM-Qradar and Splunk. **Firewalls:** Cisco FW and Palo Alto FW. **EDRs:** SEP-EDR and Crowd strike falcon.

ITSM: ServiceNow, Freshservice and Jira.

Other tools: Mimecast, Cloudflare, Qualys, Symantec endpoint protection and management (SEPM), Infoblox, Cisco ISE, FireEye HX, Confluence and Prisma Cloud.

CERTIFICATIONS & TRAININGS

- ISC2: Certified in Cybersecurity — Feb 2025
- Security Blue Team: Blue Team Junior Analyst — Feb 2023
- Qualys Certified Specialist: PCI Compliance — Jan 2023
- EC-Council: Certified SOC Analyst v1 Training — Aug 2022
- Zscaler: Zscaler Internet Access (ZIA) Administrator — July 2022
- Qualys Certified Specialist: Vulnerability Management — Mar 2022
- Qualys Certified Specialist: Vulnerability Management Detection & Response — Feb 2022

EDUCATION

G.H. Raisoni College of Engineering, Nagpur, Maharashtra — July 2015 – June 2019

Bachelor of Engineering in Electronics & Telecommunication Engineering — CGPA: 9.31/10

PROJECT BASED INTERNSHIP

CSIR-National Environmental Engineering Research Institute, Government of India, Nagpur — Nov 2018 – May 2019

Project Title: Study of Air ions and magnetic field in macro-environment for urban management.

PUBLICATION

Co-authored and published Research article “Time-Dependent Study of Air Ions in Multiple Zones of Urban Environment”. European Journal of Sustainable Development Research, vol. 6, no. 2, 2022, em0186.

RAAVI SAI YASWITHA

Profile

Cloud Security Engineer with 4+ years of experience specializing in AWS, GCP with expertise in cloud architecture, security controls, automation, and Terraform. Certified in multiple cloud technologies including AWS, GCP, and Azure. Strong problem-solving abilities and a reliable, innovative team player committed to delivering secure and scalable cloud solutions.

Contact

PHONE:
(+91) – 789-331-7641
LINKEDIN:
www.linkedin.com/in/raavi-sai-yaswitha/
EMAIL
saiyaswitha@gmail.com

CERTIFICATIONS

AWS Solution Architect Associate
AWS Certified Security Specialty
AWS Certified SysOps Associate
AWS Certified Developer Associate
AZ-900, AZ-500
GCP - Associate Cloud Engineer
GCP - Professional Cloud Security Engineer
GCP - Professional Cloud Architect
GCP - Professional DevOps Engineer
Terraform Associate - 002
Certified in CyberSecurity – ISC2
CCSK v.4
PMCC

VOLUNTEER EXPERIENCE

Managed the official webpage of NIT Patna.
Campus Ambassador for TECHNEX-IIT (BHU) at NIT Patna (2017).
Active member of the sports committee at NIT Patna.

KEY ACHIEVEMENTS

Received 2 ACE awards, 3 project recognitions,3 MyCompetency awards (9 P4 skills, 26 P3 skills), Multi-Skill Champion, Global recognition for automating AWS security processes, improving efficiency by 75% along with other internal recognitions.

WORK EXPERIENCE

SECURITY DELIVERY SR. ANALYST — *ACCENTURE | 1st DEC'21 – Present*

- Identified cloud security gaps (AWS,GCP) using automation wherever possible and mitigated them in the client environments by applying best practices, including Prisma scan remediations and TFSec scans.
- Basic understanding of DevSecOps and CI/CD principles
- Posses basic knowledge on AI applications like Aws Bedrock, Sagemaker, Q.
- AWS and GCP integrations with Google SecOps, Prisma Cloud and internal MxDR platforms.
- Familiarity with cloud-native security tools such as CNAPP (Cloud Native Application Protection Platform) and CSPM (Cloud Security Posture Management).
- Automated Security Hub, Inventory reports and implemented Just-In-Time (JIT) access in AWS using Python and AWS Lambda.
- Led AWS security architecture design team for migration projects, collaborating with AWS teams to enhance security controls using cloudfprmation,Lambda,Terraform.

SECURITY DELIVERY ANALYST — *ACCENTURE | 1st SEP'20 – 30th NOV'21*

- Defined and implemented cloud security strategies, monitoring, and integration with Security Operations.
- Managed cloud security posture for AWS and GCP environments, and supported clients in adopting secure cloud frameworks.
- Worked with OKTA and Palo Alto Firewalls (basic), enhancing security measures for cloud infrastructures.

ADVANCED APP Engg Analyst — *ACCENTURE | 19th Aug'19-31th Aug'20*

- Developed and supported MuleSoft APIs, integrating MySQL databases and manipulating data for client applications.
- Delivered POCs and solutions related to MuleSoft platform for enterprise-level applications.

EDUCATION

B.TECH(IT) | June'19 | NIT Patna	**8.4** CGPA
Intermediate | Mar'15 | Sri Chaitanya Junior Kalasala	**98.1**%
Matriculation | Mar'13 | DR.KKR's Gowtham Concept School	**9.3** CGPA

TECHNICAL SKILLS

Cloud Platforms:

- **AWS:** EC2, S3, CloudTrail, CloudFront, WAF, IAM, Security Hub, GuardDuty, SCP, Guard Rails, Control Tower, Config, VPC, Detective,CloudWatch, Lambda, Change Manager
- **GCP:** SCC, IAM, Google SecOps, Org constraints, Logging, Access Context Manager,Cloud Functions,Cloud Storage

Security Tools:

- OKTA, Palo Alto Firewalls (Basic), Prisma Cloud, TFSec

Languages & Automation:

- Python, Terraform, MySQL, XML, JSON, HTML

Other Tools:

- PowerBI, MuleSoft CloudHub

Sikkander Batcha

DEVOPS ENGINEER

+91 9786468255
sulthanbatcha1@gmail.com
www.linkedin.com/in/sikkander-batcha95/

OBJECTIVE

DevOps & Network Security Engineer with 3+ years of experience in cloud infrastructure, CI/CD automation, and network security. Proficient in Azure DevOps, Azure networking, and Palo Alto firewalls, with hands-on expertise in Hub-and-Spoke topology and VPN solutions. Recently completed an Advanced Executive Program in Cybersecurity, further enhancing knowledge of modern security frameworks and best practices.

TECHNICAL SKILLS

- Azure Cloud & Networking
- Azure DevOps & CI/CD Pipelines
- Azure Kubernetes Service
- Network Security
- Palo Alto VM series NGFW
- Panoroma & HA firewalls
- Global Protect
- TCP/IP & SSL
- Hub and Spoke
- Azure VWAN
- Express Route & VPN
- Azure Firewall

PROFESSIONAL EXPERIENCE

CloudIQ Solutions Pvt Ltd **Jan 2022 - Present**
DevOps Engineer

- Managed change requests and tenant migrations across Azure and Palo Alto environments, ensuring 99.9% uptime and minimal disruption.
- Designed and automated CI/CD pipelines using Azure DevOps, reducing release cycles by 30% and streamlining deployments.
- Optimized Azure infrastructure (VMs, VNets, AKS, VWAN, Load Balancers) to enhance scalability, efficiency, and cost-effectiveness.
- Configured and managed Palo Alto firewalls in HA mode with Panorama, implementing customized security policies to strengthen network protection.
- Improved network performance by 40% through optimized traffic routing and connectivity using Azure VWAN and VPN solutions.
- Strengthened security posture by reducing attack surfaces by 30% via well-structured NSGs, firewall rules, and secure network designs.
- Implemented centralized management of Palo Alto firewalls using Panorama, streamlining policy administration and reducing configuration errors.
- Enhanced deployment processes by integrating automated testing into CI/CD pipelines, leading to a 25% decrease in post-release issues.

EDUCATION

- **Advanced Executive Program - Cybersecurity**
  IIT Bangalore in Collaboration
  with NPCI
  JUN 2023 - DEC 2023

- **Bachelor of Engineering (Electronics and Communication Engineering)**
  Vickram College of Engineering
  AUG 2012 - APR 2016

COURSES & CERTIFICATIONS

- Microsoft Certified: Azure Network Engineer Associate
- CCNA

SHAIK DILSHAD

Vulnerability Management Analyst

Bengaluru, Karnataka | +91-9606402429 | dilshad1998dil@gmail.com@gmail.com

Professional Summary

Cybersecurity Analyst with over 5 years of experience in vulnerability management at Tata Consultancy Services. Proficient in risk management, patch management, attack surface management and web application scanning. Skilled in using Nessus, Tenable.SC, Rapid7, and Burp Suite to identify and mitigate vulnerabilities, ensuring compliance with Symantec CCS. Adept at scripting in Python and SQL to streamline processes and deliver actionable security insights. Certified in CEH and AZ-900, with a proven track record of collaborating with teams to enhance organizational security.

Technical Skills

Vulnerability Management Tools: Nessus, Tenable.SC, Rapid7, Burp Suite, Nmap, Qualys

Web Application Scanning (WAS) Tools: Burp Suite, Rapid7

Patch Management Tools: SCCM, Qualys Patch Management

Attack Surface Management Tools: Tenable.io, Rapid7 InsightVM

Risk Management Tools: Tenable.sc,Qualys Vulnerability Management, ServiceNow

Areas of Expertise: Risk Management, Patch Management, Attack Surface Management, Web Application Scanning (OWASP Top 10)

Scripting & Coding: Python, SQL

Cloud Platforms: Azure (Certified AZ-900)

Networking: Network Scanning, Configuration Review

Compliance: Symantec CCS, Baseline Assessment

Other Tools: Splunk, Crowdstrike,Microsoft Office Suite, Microsoft Excel

Professional Experience

Tata Consultancy Services, Bengaluru, Karnataka

Cyber Security Analyst (Vulnerability Management Analyst)

July 2020 – December 2024

Conducted vulnerability assessments using Nessus, Tenable.SC, and Rapid7, identifying and prioritizing risks across infrastructure and web applications, reducing critical vulnerabilities through targeted remediation.

Performed web application scanning with Burp Suite and Rapid7, detecting OWASP Top 10 vulnerabilities and recommending mitigations

Managed patch management processes with Qualys Patch Management, collaborating with IT teams to deploy timely updates, minimizing patch-related vulnerabilities.

Executed attack surface management using Tenable.io and Rapid7 InsightVM, identifying exposed assets via Nmap scans and reducing attack vectors through configuration hardening.

Utilized risk management tools like Tenable.sc and Qualys Vulnerability Management to assess vulnerabilities based on CVSS scores and business impact, generating detailed reports for stakeholders.

Automated vulnerability scanning and reporting with Python scripts, streamlining workflows and improving operational efficiency

Supported compliance audits for ISO 27001, aligning vulnerability management processes with regulatory standards and ensuring audit readiness.

Analyzed security logs in Splunk using SQL queries, creating dashboards to track vulnerability trends and compliance metrics for senior leadership.

Monitor cybersecurity threats using Tenable.io and Splunk, applying preventive measures to protect organizational data and infrastructure.

Manage patch management with SCCM and Qualys Patch Management, ensuring timely deployment of updates to mitigate vulnerabilities.

Conduct web application scanning with Burp Suite, identifying and mitigating OWASP Top 10 vulnerabilities to enhance application security.

Perform attack surface management with Microsoft Defender External Attack Surface Management, recommending configurations to minimize exposure

Develop reports with Python and SQL to track vulnerability management metrics, identifying process improvements and supporting compliance with ISO 27001.

Troubleshoot hardware and software issues, ensuring system integrity and supporting vulnerability remediation efforts.

Education

Bachelor of Engineering, Computer Science

R.L. Jalappa Institute of Technology, Doddaballapur, Karnataka

August 2016 – May 2020 | CGPA: 7.01Class 12th, MPC

Sri Chaitanya Co-ed Junior College, Vijayawada, Andhra Pradesh

April 2014 – March 2016 | Grade: 87.8%Class 10th, SSC

Navodaya Public School, Vijayawada, Andhra Pradesh

May 2014 | GPA: 9.7/10

Certifications

Certified Ethical Hacker (CEH) |Microsoft Azure Fundamentals (AZ-900)|VMDR by Qualys

Languages

English (Fluent)Telugu (Native)Hindi (Proficient)Kannada (Basic)

Personal Skills

Risk Assessment

Problem-Solving

Attention to Detail

Multitasking

Time Management

Declaration

I hereby declare that the above details are true to the best of my knowledge

SUMANTH GOPU

HYDERABAD ✆ +91 9700146060 ✉ SGOPU@PROTONMAIL.COM WWW.LINKEDIN.COM/IN/SUMANTHGOPU

Career Summary

Proactive and analytical Incident responder with 2 years' experience in security analysis, incident response, and threat management. Adept at leveraging advanced security tools and techniques to detect and mitigate security threats, ensuring the integrity and confidentiality of critical information systems. Proven track record in managing complex incidents, conducting root cause analysis, and collaborating with cross-functional teams to effectively contain and remediate security incidents. Proficient in malware analysis, vulnerability assessments, and developing tailored incident response playbooks to enhance response efficiency. A motivational leader and collaborative team player with a strong work ethic, committed to driving excellence in security operations. Holds a Master's in Applied Information Technology with a focus on Networking and Cybersecurity, and committed to staying ahead of emerging cyber threats through continuous learning and professional certifications. An Innovative thinker who leverages new technologies and methodologies to improve organizational security posture and exceed expectations.

SKILLS & EXPERTISE

Security Analysis / Incident Response / Vulnerability Assessments / Project Management / Leadership & Collaboration
Escalations / Documentation / Networking / Virtualization / Malware Analysis / Threat Intelligence / Endpoint Security

TECHNICAL SKILLS

Security Tools: Microsoft Sentinel, Splunk, Microsoft Defender, Tanium, Abnormal AI, Forescout, CarbonBlack, Symantec DCS, ZeroFox, Varonis, Thinkst Canary, Rubrik, Verizon NDR, ORCA, Palo Alto, Trend Vision One, Cortex XSOAR, Cortex Xpanse
Programming & Scripting: SQL, Bash
Networking: TCP/IP, HTTP/S, DNS, VPN, IPsec
Operating Systems: Linux (Kali, Parrot, Tails, Ubuntu, RedHat), Windows, Unix (Mac OS X)
Virtualization: VMware, VirtualBox, Hyper-V
Frameworks & Methodologies: OWASP Top 10, SDLC, NIST CSF, ISO/IEC 27001, Kill Chain, MITRE ATT&CK
Tools & Platforms: GIT, Office 365

PROFESSIONAL EXPERIENCE

Ultraviolet Cyber (ACSIPL – Metmox)

Security Analyst — July23-July24

- Conducted in-depth security analysis to identify and mitigate potential threats, ensuring the integrity and confidentiality of sensitive data.
- Managed and responded to security incidents, efficiently triaging and escalating issues to appropriate teams.
- Monitored network traffic and system logs using SIEM tools to detect and respond to intrusions and anomalous activities.
- Provided ongoing education on emerging security threats and best practices, fostering a vigilant and security-conscious workforce.
- Spearheaded the development of an internal cyber range, enabling hands-on training through real-world security challenges and enhancing team preparedness.

Incident Responder — July24-Present

- Investigated and responded to security incidents, collaborating with cross-functional teams to contain and remediate threats effectively.
- Performed root cause analysis of security incidents, documenting findings and providing actionable recommendations to prevent recurrence.
- Developed and maintained incident response playbooks, ensuring consistent and efficient handling of security incidents.
- Prepared comprehensive incident reports and post-incident summaries, providing actionable insights to improve security measures.
- Conducted malware analysis, utilizing threat intelligence to stay ahead of emerging threats and vulnerabilities.
- Actively participated in incident response exercises and tabletop simulations to refine response capabilities.
- Identified and implemented process enhancements that streamlined incident response workflows and increased overall efficiency.
- Collaborated with SOC teams to fine-tune alerting rules in Microsoft Sentinel, reducing false positives.
- Trained and mentored junior analysts on incident handling best practices, SIEM querying and malware analysis techniques.

EDUCATION & QUALIFICATIONS

- **Victoria University**, 2020
  Master of Applied Information Technology, Networking and Cybersecurity
- **JNTUH**, 2018
  Bachelor of Computer Science and Engineering
- **Certifications:**
  - Microsoft Security Operations Analyst Associate
  - Splunk Enterprise Certified Admin
  - Splunk Core Certified Power User
  - Linux Professional Institute LPIC-1
  - Privacy OPS

PROJECTS & ADDITIONAL LEARNING

- Cyber Range Development – Spearheaded the development of an internal cyber range, providing hands-on security training through simulated real-world security scenarios to enhance incident response skills and team preparedness.
- Malware Analysis Lab – Developed a secure virtual environment for malware analysis, utilizing both dynamic and static analysis techniques to improve threat detection capabilities and response accuracy.
- **Additional Learning:**
  - Palo Alto Networks Cybersecurity Foundation
  - CompTIA Security+
  - Fundamentals of Red Hat Enterprise Linux
  - Experience Program Cyber@ANZ - Forage
  - TATA Cybersecurity Analyst – Forage

M Sri Shailesh *Security Engineer*

srishaileshm1998@gmail.com

7448326918

No 30 and 31 Koushik Avenue Ext 2 VGP Nagar South Rajakilpakkam Chennai 600073

11/08/1998

linkedin.com/in/m-sri-shailesh-748088187

Profile

- Skilled Security Engineer with 3.5 years of experience, specializing in **Incident Response**, **SOC**, **VAPT**, **DLP**, **EDR** and **Threat Intelligence**.
- Adept at threat analysis, risk assessment, Vulnerability Management and Security Operations, with hands-on expertise in **SIEM tools (QRadar, ArcSight, Tenable Nessus)**, **Firewall (IDS, IPS)** and **VAPT (Kali Linux)**.
- Certified in **CompTIA Security+**, demonstrating a strong foundation in **Risk Management, Cryptography, PKI and Threat Detection**.
- Adept at enforcing security policies, conducting risk assessments and ensuring compliance with industry standards such as **ISO 27001 and GDPR** and committed to staying ahead of emerging threats in a rapidly evolving cybersecurity landscape.
- Skilled in leveraging **SIEM** tools, **Intrusion Detection System(IDS)** and **Threat Intelligence** platforms to identify and mitigate security incidents and analyze logs, investigate alerts to implement remediation strategies.

Professional Experience

12/2021 – present

Security Engineer

Tata Consultancy Services

- Reduced security incidents by **50%** through the implementation of advanced **Threat Detection** tools and Proactive Monitoring.
- Successfully conducted **Vulnerability Assessments(Nessus)** and **penetration tests(Kali Linux, WireShark, MetaSploit, Nmap)** and generating reports for identifying and remediating critical, high risk vulnerabilities
- Involved in regular patching of appliances**(Physical)**, servers**(Windows, Linux)** as part of vulnerability mitigation and collaborated with development teams for mitigation strategies.
- Successfully responded to security incidents, including **malware infections, phishing attacks** and unauthorized access attempts.
- Performed **URL blacklisting and whitelisting** using **Forcepoint** at DC and DR level to restrict privilege escalations.
- Maintained Security Compliance Framework**(ISO 27001, GDPR)** as per security policy & directives.
- Leveraged **SIEM tools(ArcSight, QRadar)** to monitor for security events and logs and creating security alerts and incidents.
- Conducted Dynamic Application Security testing using **OWASP Zap, Burpsuite** to check for vulnerabilities in web applications and collaborated with development teams for remediation methods.

12/2020 – 12/2021

Customer Service Representative

HCL Technologies Ltd

- Successfully executed the payor change outbound dialing process, maintaining high levels of customer satisfaction.
- Engaged in productive interactions with customers, addressing inquiries and resolving issues promptly.
- Demonstrated exceptional multitasking abilities by efficiently managing diverse customer requests.
- Developed strong problem-solving skills through proactive troubleshooting of customer concerns.

Tools

OWASP Zap	Forcepoint DLP
Tenable Nessus	Kali Linux, Wireshark
ArcSight	Linux, UNIX
Symantec Endpoint Protection	BurpSuite
QRadar	Trend Micro

Education

07/2016 – 09/2020 **Electronics and Communication Engineering**
Dhanalakshmi College of Engineering
CGPA - 7.4

Certifications

- CompTIA Security+
- Vulnerability Management with Nessus
- Web Application Security Testing (Udemy)
- Penetration Testing, Threat Hunting and Cryotography
- Kali Linux

RESUME

MR.VIVEK V SUGEE
E-mail: sugeevivek@gmail.com
Mobile: +918553735755
LinkedIn: https://www.linkedin.com/in/vivek-sugee-9b621116b
Residing Address: Bangalore

CAREER OBJECTIVE:

To obtain a challenging position with a growth oriented company and to significantly contribute to the success of the organization utilizing my knowledge and skills want to be a part in every success of the organization, which will be helpful in increasing my responsibilities and dedication towards work.

Global Certification:

- Red Hat Certified System Administrator (EX200) on Linux
- Jamf Certified Associate Exam 100
- Udemy Certification on Linux Security & Hardening
- CEH - Trained (EC - council)
- Powershell / Python Language

WORK EXPERINCE: (Overall Experience: 6+ years with IT Domain)

1] : Vistas Technolabs Private Limited (ZET)

Organization. : **Vistas Technolabs Private Limited (ZET), Bangalore**
Duration : **Sep'24 – till date**

Role description:

Designation: Information Security Engineer

- Review, update and maintain all the policies related to information security, disaster recovery and other relevant areas.
- Ensure compliance with ISO 27001 and CICRA provisions in all policies and standards.
- Conduct regular Appsec security assessments to identify vulnerabilities and risks in
- our mobile applications.
- Ensure compliance with data localization regulations by implementing measures to securely store and process data with specified geographic boundaries, mitigating legal and regulatory risks associated with data sovereignty.
- Develop and deliver information security training programs for all employees to

enhance awareness and compliance.

- Coordinate with various teams to ensure information security checks and verifications are carried out effectively.
- Generate and maintain evidence for all information security checks and verifications.
- Ensure completion of annual ISO, CICRA, and system audits, including coordination with audit teams and addressing any audit findings promptly.
- Own the information security process during the onboarding of new brands, ensuring adherence to security standards and protocols.
- Experienced on MDM, DLP, EDR,Identity access tool, SIEM
- Perform vendor information security assessments as needed, ensuring third-party vendors meet our security requirements.

2] Junglee Games Pvt.Ltd.

Organization : Junglee Games Pvt. Ltd. Bangalore
Duration : Jun'22 - July'24

Role description:

Designation: Security Engineer

- Develop and implement security policies, procedures, and technical measures to safeguard company assets and information systems, ensuring alignment with the ISMS ISO27001 framework.
- Implement, Onboarding and manage SIEM (Coralogix) solutions to centralize and correlate security event logs for proactive threat detection and incident response.
- Utilize SAST (OX Security) and DAST (Edge Scan) tools to identify and remediate vulnerabilities in software code during the development lifecycle
- Manage enterprise security tools including antivirus software (Trendmicro),Web proxy and DLP (Forcepoint) solutions, and Endpoint management tools (Jamf and Intune).
- Conduct regular security assessments and penetration testing to identify vulnerabilities and mitigate risks

- Experienced in Google Workspace administration, adept at overseeing user management, group settings, device policies, and security configurations within the Google Admin console.
- Skilled in OKTA administration, proficiently managing user authentication, access policies, application integrations, and security configurations within the OKTA Admin dashboard.
- Managing, Monitoring, and implementing New policies in Firewall (FortiGate 400E and Checkpoint 5200)
- Experienced in administering Microsoft Active Directory for streamlined user management and policies
- Creating and Maintaining Server (AWS Cloud and Virtualization) with Hardening Process Std.
- Implementation and Handling of Zabbix Monitoring tool for Monitoring Infrastructure (Network/ Server)
- Managing wireless network (Aruba access point) for the premises, managing DHCP,DNS service.

3] Blue Dart Express Ltd. Mumbai

Organization : Blue Dart Express Ltd. (HO)
Designation : Executive (Corporate – IT)
Duration : Aug'20 – May'22

Role description:

Managing and Handling Web Security / Email Security / Anti-Virus security / Firewall operation.

Firewall: Checkpoint R80 series
Web Security: Force point 8.5
Email Security: IMSVA (Trend Micro)
Network Security: McAfee IPS
Anti-Virus Security: McAfee ePO and Deep Security (Trend Micro)

- Monitoring all security device on daily and updating DAT/ signatures /Databases.
- Creating and implementation new rules and policies and VPN creation
- Reporting and analysis on daily / weekly basis
- Maintaining backup check on daily/weekly/monthly.
- Responsible for upgrade / patch / hotfixes updation.
- Responsible for the quick and appropriate action vulnerability risks.
- Security patches monthly on servers
- Experience on VMware infra server and Nutanix infra server.

4] UNIQUEE ENTERPRISES

Organization Payroll Employee Designation Duration : BLUEDART EXPRESS LTD
: Uniquee Enterprise
: System Administrator
: Apr'19 – Mar'20

Role description:

Client: BLUEDART EXPRESS LTD.

- Installation and management of Windows Server (2008 and 2012) and Linux
- Supporting Sever Hardware (Dell Power edge R630 & R740, Lenovo System X series)
- Setup and Managing VXL Thin Client devices
- Domain Knowledge (Group and Domain) and Monitoring the Health and performance of Servers
- User Support on Laptop and desktop level.
- Perform timely patch Management as per the schedule and deploying released patches through server
- Hardware Support and installation
- Support and Install required software

5] IDFC BANK

Organization : IDFC BANK
Payroll Employee : TeamLease Service Limited
Designation : Technical Support Engineer
Duration : Nov'17 – Feb'19

Role description:

- Manage Incident Request/Change Order in BMC remedy ticketing tool of Technical issue
- Follow-up with ticket and ensuring to be resolve in ETA
- Acknowledge the tickets, allocate appropriate category
- Recording, tracking, and updating incident ticket information in the service desk tool.
- Ensuring the respective support groups update activity details in the tool.
- Route service requests to the appropriate teams (viz. user mgmt. group, mail mgmt. group etc.)
- Coordinate with relevant internal service providers / functions for IT support

ACADEMIC CREDENTIAL:

2011-2016 **BACHELOR OF ENGINEERING**-(Electronic and Communication)

Government Engineering Colleges, Ramanagara

VTU UNIVERSITY, BELAGAM, KARNATAKA

Declaration: I hereby declare that the information furnished above is true to the best of my knowledge. I do hereby declare that above particulars of information and facts stated are true, correct and complete to the best of my knowledge and belief

Place: **Bangalore**
Date:

SAI PRAKASH GUNDALA

CYBERSECURITY ANALYST

saiprakashgundala@gmail.com

Phone: +91 7416955244

PROFILE SUMMARY

- Security Analyst with a run of 3.2+ years of professional experience in information security.
- Expertise in Vulnerability management, Web Application Security (SAST & DAST) & Network Penetration Testing, Cloud Security.
- Expertise in tracking vulnerabilities overseeing governance, ensuring compliance with vulnerability management frameworks
- Web Application Security Testing, Vulnerability Assessment and penetration testing conducted for wide range of business applications in financial/government /private sector domain against standards such as OWASP Top 10.
- Expertise in VMS to perform VA scans, proposing remediations and categorizing vulnerabilities.
- Good knowledge on networking concepts, cyber security concepts and cyber kill chain.

SKILL SET

- **Vulnerability Assessment & Pen Testing–Kali Linux, Nmap, Wireshark, Jok3r, testssl, Nessus, Metasploit Pro**
- **Vulnerability Management- QualysVMDR, Rapid7InsightVM**
- **Web application security - Burp suite, Acunetix, OWASP ZAP, HCL AppScan**
- **Cloud Security – Microsoft Defender for Cloud, CSPM for Azure, AWS**
- **Ticketing Tools – ServiceNow**
- **MS Office – MS Excel, Word, PowerPoint, Power BI**

EXPERIENCE

❖ **Infosys Limited - Hyderabad, India.**

❖ **Cybersecurity Analyst -27th Jan 2025 – Present.**

Client: Confidential (Retail Industry).
Vulnerability Management: Qualys VMDR, GRC

- Conducting vulnerability scans using Qualys and prioritizing vulnerabilities based on risk.
- Coordinate with Infra and Application teams to ensure timely remediation of finding security vulnerabilities.
- Providing technical guidance and assistance to the teams on vulnerability mitigation strategies.
- Define and vulnerability management policies, procedures and SLAs for mitigation.
- Maintain a formal process for risk exceptions, document justification and tracking compensating controls for vulnerabilities.
- Track and follow up on remediation progress ensuring compliance with internal and regulatory security standards.
- Develop and maintain dashboards using Excel and PowerBI to provide visibility into vulnerability trends, risk exposure and remediation status.
- Present security reports to the stakeholders including leadership.
- Regularly assessing and enhancing the security posture of organization by continuous improvement/monitoring.

❖ **Yash Technologies Pvt. Ltd. - Hyderabad, India.**

❖ **Cybersecurity Analyst - 8th Feb 2022 – 24th Jan 2025.**

Project 1
Client: Confidential (Health Care Sector)
Web & Network Penetration Testing:

- Performing network penetration testing on client's network infrastructure.
- Finding the open ports by using nmap.

- Performing PT on targets by using Burpsuite, Acunetix, OWASP ZAP and other CLI tools.
- Performing SAST &DAST testing on web applications to find known vulnerabilities like SQLI, XSS, CSRF etc.
- Participating in code review meetings to address potential security vulnerabilities.
- Performing automated scans on web applications by using different applications.
- Performing false positive analysis after automated scans and performing manual PT.
- Proposing mitigations for vulnerabilities.
- Report the which ports are opened and vulnerability findings in their infrastructure and applications.
- Creating customized reports about that which ports are opened and what are possibilities of vulnerabilities will be happen and proposing remediations.

Project 2

Client: Yash Technologies Pvt. Ltd.

Vulnerability Management: CyberCNS

- Onboarding assets into the tool.
- Onboarding the Authentication credentials to perform authentication scanning on different platforms.
- Responsible for conducting vulnerability assessments for networks, applications and operating systems using Rapid7 Insight VM and CyberCNS to find vulnerabilities.
- Proposing troubleshooting steps to the assets which are not alive and authentication failures.
- Identifying critical flaws in applications and systems that cyber attackers couldexploit.
- Manually validating report findings to reduce false positives.
- Preparing reports and working with respective teams and assist with the remediations of the identified vulnerabilities.

Project 3

Client: Confidential (Health Care Sector)

Vulnerability Management: Qualys VMDR

- Asset baselining and finalizing the assets to perform VA scans with the help of customer.
- Asset Onboarding.
- Scheduling discovery scans and producing report to the customer with the newly added assets in the scope.
- Scheduling VA scans for different platforms like Windows, Linux/Unix/CentOS, MacOS servers and Endpoints.
- Performing Ad-hoc scans based on customer requirement and for Zero Day Vulnerabilities.
- Creating alerts for different vulnerabilities.
- Creating different option profiles for different OS platforms.
- Asset tagging and grouping.
- Creating custom dashboards in Qualys VMDR by using QQL.
- Preparing custom report templates as per customer requirement.
- Producing VA reports to the different platform POC's and helping them to remediate those vulnerabilities.
- Categorizing and removing false positive vulnerabilities and proposing remediation.
- Troubleshooting the assets those are not alive and which are getting authentication errors.
- Performing CIS benchmark compliance scan on windows servers and endpoints.
- Responsible for conducting vulnerability assessments for different platforms and producing VA reports to the POC's.
- Responsible for creation of new users to the Qualys and removing unnecessary access (RBAC).
- Preparing custom reports as per custom requirement then help them to remediate vulnerabilities as per SLA.
- Performing rescan on ad-hoc basis for remediate assets.
- Helping to the customer to create auth credentials for different platforms by giving pre-requisites.
- Finding solutions for the issues getting in the solution i.e., Qualys by raising support case in the Qualys or getting in touch with TAM.
- Proposing troubleshooting steps to the assets which are not alive and authentication failures.
- Identifying critical flaws in applications and systems that cyber attackers could exploit.
- Risk analysis and prioritizing vulnerabilities as per SLA.
- Manually validating report findings to reduce false positives.
- Preparing reports and working with respective teams and assist with the remediations of the identified vulnerabilities.
- Preparing vulnerability trends and data points using Excel and Power BI.
- Presenting weekly data to the senior management by using PowerPoint presentations.

Project 4
Client: Confidential (Manufacturing Industry)
Cloud Security: Microsoft Defender for Cloud

- Implementing MDC for Azure based servers.
- Enabling required plans for the different resources to monitor cloud security posture management.
- Creating alerts by using Azure Monitor.
- Monitoring the critical alerts for all resources in the subscriptions as per the created alerts.
- Suppressing the alerts that are not required.
- Notifying the stakeholder regarding vulnerabilities that are found in VM's, Servers, Databases etc.
- Enabling Azure benchmark policy to the all subscriptions.
- Hardening the Azure based resources as per Azure benchmark policy.
- Proposing the recommendations for policy scans.
- Helping the customer to improve the cloud security posture.

❖ **Belcan India Pvt. Ltd. - Hyderabad, India.**

❖ **Junior Engineer – Dec 2021-Feb 2022.**

Client: Confidential (Aerospace Sector)

- Analyzing 2D drawings of Aero Engines
- Finding Hazardous materials in the Aero Engines.
- Report the Hazardous materials with composition to the customer.
- Preparing the tracker that have hazardous materials along with the part number,

CERTIFICATIONS

- CEH from EC-Council
  Validity: 12-12-2022 to 11-12-2025
- Computer Networks Security from EC-Council
- QUALYS VM Foundation
- Qualys VMDR

ACADEMIC DETAILS

- **2019:** B. Tech in Mechanical Engineering from G. Pullaiah College of Engineering & Technology. Kurnool, Andhra Pradesh.
- **2016**: Diploma in Mechanical Engineering from ESC Govt Polytechnic. Nandyal, Andhra Pradesh.
- **2013**: SSC from Shyam Vidya Vihar EM High School. Nandyal, Andhra Pradesh.

PERSONAL DETAILS

Date of Birth: 21st Jul1997
Languages Known: English, Telugu and Hindi
Present Address: H. No:28/1245 B12, Sri Sri Nivarthipuram, Noonepalli, Nandyal, Andhra Pradesh – 518501.

I hereby confirm that the above information is correct to the best of my knowledge.

Place: Hyderabad
Date:

Sai Prakash Gundala.

KOLLI NAGA MOHAN REDDY

India
+91 9573753975
mohan9573753975@live.com
LinkedIn: https://www.linkedin.com/in/k-nagamohan-reddy-aa482270

Personal Details

- **Date of Birth**: 05 June 1992
- **Languages Known:** English, Hindi, Telugu & Kannada
- **Address:** Nandyal, Andhra Pradesh,518502

Education

- **MBA (Operations and Marketing Management)** from M.S.Ramaiah Instiitute of Management in 2016
- **B.Tech. (Electrical and Electronics Engineering)** from G Pulla Reddy Engineering College in 2013

Skills/Tools

- SIEM Solutions
- Splunk Enterprise Security(ES)
- Microsoft Azure Sentinel
- SNYPR by Securonix
- Crowdstrike
- Cortex XDR
- Microsoft Defender
- Microsoft Purview
- Data Loss Prevention(DLP)
- Intrusion Prevention Systems(IPS)
- Intrusion Detection Systems(IDS)
- E-Discovery
- Zabbix
- Intermapper
- Zscalar
- Powershell
- SOAR

Profile Summary

- Focused, high-energy technocrat experienced in System & Security Operations Analysis, targeting assignments in System & Security Operations Analysis. Analytical, dedicated and detail-oriented Security Analyst with over 5 years of experience in monitoring and analyzing the security of critical systems such as e-mail servers, database servers, web servers and implementing changes to highly sensitive computer security controls to ensure appropriate system administrative actions, investigation, and preparation of reports on noted irregularities.
- Proficient in preparing **security incident reports** and communicating security information to people at all levels of the organization.
- Experienced in information security strategy, risk assessments, security architecture and governance, strategic outsourcing & co-sourcing, penetration testing (Web & Infra), regulatory audits, code reviews, malware analysis and forensics, threat management and so on.
- Expertise in conceptualizing & implementing security fundamentals, application protocols.
- Gained industry experience in integrating of new Data Sources such as Windows, Linux and networking devices likeFirewall, **IPS/IDS, DNS, Active Directory (AD), DLP to Splunk (SIEM)** and decommissioning.
- Key person in defining , planning, implementing, maintaining and upgrading security measures, policies and controls.
- Staying up to date on latest trends, issues and news related to information security and Knowledge on Cybersecurity Framework like MITRE ATT&CK and NIST.
- Highly skilled in conducting vulnerability testing and risk analyses to assess security and performing internal and external security audits.

Work Experience

November 2023 – May 2025 | Job Title: Technical Support Engineer | Company: Teamware Solutions (Microsoft - Payroll)

- Working as a technical support engineer to our premier customers assisting via phone chat and support tickets on
- issues related to compliance.
- Troubleshooting issues related to DLP, Online Archiving,E -Discovery and content search.
- Investigating issues related to Data life cycle management such as retention policy, adaptive scopes and PST import duties.
- Assisting issues related to labels and label policies, analyzing Auto-labeling issues on the server side.
- Troubleshooting issues related to DLP policies implemented, including rules and conditions for data protection.
- Analyzing the DLP logs for false positives alerts generated and addressing any false positives or negatives by refining policy rules and conditions.
- Addressing concerns related to information barrier policies and offering guidance on the creation and implementation of new DLP policies across various workload environments.

Core Competencies

- System & Security Operation
- Centre Analysis
- Malware Analysis, Email Phishing, Website Whitelisting
- SLA Metrics & Monthly Reports Generation
- Security Information & Event Management
- Weekly Ticket Reviewing
- In-house Process Training
- Incident Analysis & Resolution
- Adhoc Reporting & Documentation
- Cross-functional Coordination
- Compliance support engineer

- Collaborating with cross-functional teams to develop proactive solutions, identifying patterns in compliance issues to improve policy effectiveness and mitigate recurring incidents.

February 2023 – October 2023| Job Title: Lead Analyst Cyber Security | Company: Mphasis

- Monitoring & Detection use of **Splunk ES** and other security tools for continuous monitoring of network activity. Identifying and responding to suspicious activity and cyber-attacks. Ensuring proper log collection and analysis from indexers and forwarders.
- Monitor and analyze logs from network devices (like **IDS, IPS, firewalls**) to detect and respond to attacks. Create and track security incidents, ensuring they are resolved efficiently. Generate reports for stakeholders, including SLA metrics and CISO updates. Manage incident severity levels and escalate as needed.
- Performing deep-dive analysis into security incidents, including **malware analysis, phishing attempts, and website whitelisting**. Identifying and mitigating security breaches, and improving security posture by providing documentation for SOPs and future responses. Analyzing incidents to develop new security measures and improving response plans.
- Static and dynamic malware analysis using Sandbox or other available tools.
- Managing and configuring Splunk knowledge objects (e.g., Apps, Dashboards, Alerts).Evaluating security controls (e.g., **firewall, web proxies, DLP**) and approving/denying requests for exceptions or whitelisting. Ensuring all forwarders are correctly sending logs to indexers.
- Producing ad-hoc reports and metrics on use cases and incidents for business stakeholders. Preparing and providing insights on the effectiveness of security measures, incident response, and disaster recovery plans.
- Conducting regular security tests and identifying vulnerabilities in the network infrastructure. Proactively identifying potential threats and developing strategies to mitigate future incidents.
- Coordinating with external vendors for security-related services and integrations. Collaborating with other teams (L2, Business, stakeholders) to create and improve security policies and procedures. Leading efforts to mitigate security breaches and improving the overall security posture of the organization.

May 2020 – January 2023 | Job Title: Professional Engineer I | Company: Capgemini

- Extensive experience working in a 24x7 Security Operations Center(SOC) or Managed Security Services(MSS) environments by handling incident response and malware analysis using SIEM solutions such as **Splunk ES** and **Microsoft Azure Sentinel** and EDRs like **Cortex XDR by Palo Alto, Crowdstrike, Microsoft Defender**.
- Built and refine advanced threat detection mechanisms to identify and mitigate potential risks. Stay updated on emerging threats by researching attack methods, exploitation techniques, and adversary behaviors.
- Partners with incident response teams to analyze and address security incidents, which may occasionally require after-hours work.
- Continuously enhance detection tools and systems to improve threat identification capabilities.
- Develop and maintain comprehensive documentation outlining detection methodologies and procedures.
- Create automation workflows and playbooks to streamline processes within the Threat Analysis team.

MOUNIKA PENDEM **Email:**
mounikasoc27@gmail.com

Mobile: 91- **9347639546**

OBJECTIVE:

To work in a professional environment with committed and dedicated people where I can get the opportunity to expand my field of knowledge that will help me to explore myself and make a value addition to the growth of the company.

PROFFESIONAL SUMMARY:

- Over all **4.6** Years of experience and **3.3** years of Relevant experience as **Information Security Analyst in** large Security operations environment.
- Performing real time investigation analysis and, monitoring on event logs using **Microsoft Sentinel SIEM** for different network components and applications.
- Conduct in-depth analytical queries and investigations to identify areas needing attention, indicators of compromise (IOC), and events of interest (EOI) for development into the **Azure Sentinel SIEM** platform.
- Responsible for **security monitoring and investigation.**
- Providing support to customer on Incident Response related activities.
- Good understanding of network concepts and protocols, such as TCP/IP, LAN, WAN.
- Project involves **24x7x365** security monitoring and management of security infrastructure
- Quickly adapting to **new Technologies.**

EDUCATIONAL QUALIFICATION:

- **Bachelor of Technology** (Electronics and Communication Engineering) from **JNTU, HYDERBAD with 67.10% in 2015 Pass out.**
- **Board of Intermediate Education** in Gouthami Junior College, **NALGONDA with 71.80% in 2011 pass out.**
- **School of secondary Education** in Sri prathiba High school, **NALGONDA with 77.33% in 2009 pass out.**

TECHNICAL SKILLS:

- **Operating Systems-** Microsoft Windows Server, Windows 10, 11, Linux.
- **SIEM –** Microsoft Azure Sentinel
- **End Point Security (EDR)** –Microsoft Defender, Sentinel One.
- **Email Security** – Microsoft Defender for Office 365, Perception Point.
- **Data Loss Prevention –** Microsoft Purview, Netskope.
- **Host Intrusion Detection** - Trend Micro Deep Security, MCA Fee
- **Network Firewalls** – Panorama Firewalls, Checkpoint.
- **Next Generation Intrusion Prevention System**-- Source fire NIPS/NFirewall.
- **Vulnerability Assessment & Compliance** – Rapid 7, Nexpose, Critical Watch(FusionVM).
- **Packet Sniffers** – Wire Shark.
- **Database:** MS office, Oracle 10g.
- **Ticketing Tools –**Service Now, HP Service Manager 9.0.
- **Languages –** C#.NET, ASP.NET.
- Good knowledge in **ITIL.**

PROFESSIONAL EXPERIENCE:

- Working as **Information Security Analyst** with **Tech Mahindra, Hyderabad** since **October-2021** to Till Date.
- Worked as **Desktop Engineer** with **CYouTech IT Consulting Services, Hyderabad** since **June 2020 to Oct 2021**.

CERTIFICATIONS:

- **Certified Ethical Hacking.**
- Certified **AZ 900 Microsoft Azure Fundamental Courses.**
- Certified **SC -200 Microsoft Security Operation Center.**
- Trained & certified in **CCNA.**

WORK EXPERIENCE:

2. Organization : Tech Mahindra.
Project : Security Operation Center (SOC).
Client : MGM Resorts International.(USA)
Tools : Microsoft Azure Sentinel SIEM.
Role : Information Security Analyst.
Location : Hyderabad.
Duration : October-2021 to Till Date.

Roles and responsibilities:

- Monitoring SOC mail Box.
- Conduct in-depth analytical queries and investigations to identify areas needing attention, indicators of compromise (IOC), and events of interest (EOI) for development into the **Azure Sentinel SIEM** platform.
- Design and configure analytics for processing events and logs across multiple Microsoft Sentinel SIEM.
- Automate and orchestrate tasks (playbooks) within Microsoft Sentinel SOAR based on specific event triggers.
- Creating tickets as per the source, destination IP, Signature of the alert.
- Implement complex use cases in Azure Sentinel using **Kusto Query Language (KQL)** for correlation across diverse data sources.
- Create and manage **playbooks** and alerts for various endpoint security events using Microsoft 365 Defender XDR.
- Extensive experience in crafting Azure Sentinel analytics rules, incidents, playbooks, notebooks, workbooks, and threat hunting in the Azure Cloud.
- Robust understanding of cloud security and networking principles and practices.
- Collaborate with **SOC** personnel for event/detection triage and policy refinement as needed.
- Collaborate with the Tactical Use Case Development team to process complex use case development requests from customers.
- Configure, install, and provide technical support for all components related to Microsoft Defender for Endpoint.
- Configure security policies in compliance with best practices and industry standards for MDE using the Intune portal.
- Manage endpoint compliance, including definition updates, client version updates, and device activity using Intune.
- Responsible for implementing new features and requirements for 365 Defender.
- Coordinate with site administrators to track non-compliant platforms and maintain necessary exception documentation.
- Handle any issues related to 365 Defender XDR across the organization.
- Involved in creating, managing, and fine-tuning policies according to client requirements in MCAS.

- Implement Microsoft Cloud App Security MCAS and DLP standards for over 3,000 end users globally.
- Implement and manage a cloud security posture management solution, Microsoft Defender for Cloud.
- Conduct regular security assessments to identify vulnerabilities, misconfigurations, and compliance violations. Analyze and prioritize security findings and collaborate with stakeholders to remediate issues.
- Monitor cloud infrastructure and applications for security events, alerts, and indicators of compromise (IOCs).
- Extensive experience and working knowledge of Proof Point and Fire Eye Email Gateway Solutions.
- Manage, monitor, and administer the email security stack and policies for both OnPrem and cloud environments, including Microsoft Purview, Netskope and FireEye email security solutions.
- Implement email fraud defense and authentication mechanisms (DKIM, DMARC, and SPF).
- Analyze phishing emails reported by users to identify the type of attack and take immediate remediation.
- Create policies on email gateways to auto-quarantine emails from user mailboxes.
- Validate false positive emails and release them to users.
- Understanding of cyber security controls, as well as logging and monitoring tools.
- Thorough alert triage and endpoint investigations using EDR technologies.
- Provide support to the Security Operations Centre (SOC) during incident response, event monitoring, and threat hunting activities.
- Monitor and identify genuine security events from the Microsoft Azure Sentinel dashboard during shift hours and take necessary action for critical events.
- Work in the 24x7 Security Operation Centre (SOC) to monitor SOC events.

1. Organization : CYouTech IT Consulting Services.
Duration : June 2020 to Oct 2021.
Role : Desktop Engineer.
Project : InfraJini (Global Network Operation Centre)
Client : Hindustan Unilever.
Location : Hyderabad

- 24x7 rotational on-call support, including escalation to Emergency Response Team (ERT), driving Root Cause Analysis (RCA), Preventative action follow-though, and participation in weekly operations reviews.
- Interaction with 3rd party vendors, Client Teams and senior onsite Systems Engineers as necessary to optimally perform job responsibilities.
- Providing first level support on Desktops, Peripherals, and Office automation products.
- Logging Tickets (Incident / Service Request / Information Query) for every user interaction handled.
- Troubleshooting and Maintaining Laptops.
- Monitor, escalate and update trouble tickets using Service now Tool.
- Adding, removing, or updating user account information, resetting password.
- Performing system Tuning and increasing the performance.
- Responding to and Answering Calls, Emails and Web Tickets of end users in a cordial, professional manner.
- Troubleshooting Operating systems.
- Installing, configuring and Troubleshooting Outlook issues.
- Troubleshooting Network Issues.
- Able to handle IT Helpdesk tool. (Creating, closing Tickets and also able to Send Emails).
- Following Service Level Agreements.
- Trouble shooting scanners and printers.
- Handling US Clients on Calls/emails/Application Support.
- Installing and troubleshooting Antivirus application.
- Escalating server and network issues to L1 & L2 dept.

Personal Details:

Name : MOUNIKA PENDEM
Father's Name : Venkateshwarlu
Gender : Female
Marital Status : Married
Spouse Name : Harikrishna Shamala
Date of Birth : 27-May-1994
Languages Known : English, Hindi & Telugu.
Hobbies : Netsurfing, Listening music.
Address : 4-9-774/p17, East rajarajeshwari colony, road no 11, HayathNagar, 501505.

Declaration:

I declare the information and facts stated above are true and correct to the best of my knowledge and belief.

Place: Hyderabad Yours Faithfully,
Date:

(**Mounika Pendem)**

Md IRFAN

SOC Analyst

mdirfan05091986@gmail.com +91 9963014048

CAREER OBJECTIVE

Dynamic and results-oriented Security Analyst with over 5.4 years of experience in Information Security, aiming to contribute to organizational growth while advancing my expertise in a challenging environment.

PROFESSIONAL SUMMARY

- With 5.4 years of IT experience in securing network environments with expertise in monitoring and investigating security events.
- Experience in Monitoring & Investigating the incoming Events.
- Experience of working in 24x7 operations of SOC team, offering log monitoring, security information management, global threat monitoring.
- Experience in security operations, incident management, intrusion detection, and event analysis using SIEM tools such as IBM QRadar and Splunk.
- Experience in generating Daily, Weekly & Monthly Reports, and dashboards and rules fine tuning.
- Monitored and analyzed CrowdStrike Falcon alerts to identify potential threats, including phishing attempts.
- Responsible for monitoring the Phishing attempts.
- Good understanding of log formats of various devices such as Websense, Vulnerability Management Products, IDS/IPS, Firewalls, Routers, Switches, OS, DB Servers, and Antivirus
- Mostly worked on broken authentication, Sensitive data exposure, broken access control, XSS, using components with known vulnerabilities, Insufficient logging and monitoring.
- Exposure to Ticketing tool like Service Now.
- Strong knowledge on Event Life Cycle and Incident management life cycle.
- Good communication, problem solving skills and the ability to acquire new skills in a timely manner.

PROFESSIONAL EXPERIENCE

Company: Wipro (Bangalore)
Role: SOC Analyst
Duration: Oct 2021 to till date

- Working in Information Security on security operations, incident management, intrusion detection, and security event analysis using SIEM tool like IBM QRadar & Azure Sentinel
- Monitor and analyze security alerts generated by CrowdStrike Falcon to identify potential threats and incidents.
- Working in Offshore SOC team. Monitoring of SOC events, detecting and preventing the Intrusion attempts.
- Ad hoc report for various event sources customized reports and scheduled reports as per requirements.
- Collecting the logs of all the network devices and analyze the logs to find the suspicious activities.
- Monitor security alerts and logs generated by Zscaler to detect and respond to potential threats in real-time.
- Conduct in-depth analysis of suspicious activities, leveraging CrowdStrike's EDR capabilities to detect advanced threats such as malware, ransomware, and zero-day exploits.
- Proactively hunt for threats within the organization's network using CrowdStrike's threat hunting tools and techniques.

Company: Deloitte (Bangalore)
Role: System Analyst
Duration: Oct 2019 to Sept 2021

- Investigate the security logs, mitigation strategies and Responsible for preparing generic security incident report.
- Incident Investigation: Perform deep-dive analysis of security incidents, leveraging Zscaler's data to determine root causes and implement corrective actions.
- Track and report on user activity across the organization to identify and address any unusual or suspicious behavior.
- Worked directly with QRadar SIEM Tool for day-to-day operations.
- Skilled in Security advisory and Anti-malware And Investigating security threats (DDOS, IP Spoofing, SQL injection) on network (log Monitoring).
- Handling the different issues like Phishing, Spam, Scam and Malicious email.
- Using Service now to handle & track all kind of incidents.
- Actively participating in all the Security flash calls with Offshore & Clients.
- Coordinates with all the teams to Mitigate/Remediate the issue.
- Investigating the events based on particular criteria by creating an Active Channel.
- Handling the failed logins issues from the different systems.
- Working on security related threats and Incidents.

Technical skills

- Security Operation Center **(SOC)**
- **SIEM Tools**: Splunk and Q-radar
- **TICKETING TOOL:** Service Now
- **ENDPOINT SECURITY:** Symantec & Trend Micro.
- **DLP:** Crowd Strike, Carbon Black**.** Defender for end point
- **VULNERABILITY MANAGEMENT:** Nessus & Qualys
- **EMAIL SECURITY:** Proof point & Symantec

Education

B. Com in Computers, Acharya Nagarjuna University, Vijayawada, Andhra Pradesh (2009).

Declaration

I hereby declare that all information furnished above is correct to the best of my knowledge.

Mohammad Irfan

Afsal Shereef

+91-9495395861 | afsalshereefpta@gmail.com | LinkedIn | India

Summary

Experienced Associate Security Engineer at H&R Block, proficient in AWS and Azure Cloud Security, firewalls, Splunk, and DEVO. Passionate about protecting organizations from cyber threats and ensuring robust security measures.

Education

Digital University Kerala — Trivandrum, India
M.Sc. Computer Science (Cybersecurity); ***GPA: 7.75/10*** — *August 2021 – July 2023*

Jain University — Bengaluru, India
B.Sc. Forensic Science (Honours); ***GPA: 7.78/10*** — *June 2018 – July 2021*

Professional Experience

H&R Block India Pvt. Ltd. — Trivandrum, India
Associate Security Engineer — *November 2023 – Present*

- Administer, manage, and support enterprise security platforms, including but not limited to SIEM, Log source integrations, Cloud Security.
- Provide guidance and assistance with logging configurations for systems and applications to integrate logs with the SIEM tool, enabling near real-time alerting.
- Assist with incident response and system stability issues, including involvement outside regular work hours, with a focus on responsiveness.
- Research, validate, and deploy solutions that meet security and business needs.
- Develop security test plans from architectural design, identify deficiencies, and make enhancements to ensure production is not impacted.
- Create SIEM Use Cases and Standard Operating Procedures (SOPs) with thorough documentation.

AIRBUS India Pvt. Ltd. — Bengaluru, India
Cybersecurity Intern — *March 2023 – September 2023*

- Developed and enhanced Splunk-based SOC use cases, collaborating with cross-functional teams to fine-tune queries and dashboards for improved threat detection and incident response.
- Gained expertise in the MITRE ATT&CK Framework for understanding and analyzing adversary tactics, techniques, and procedures.
- Developed and improved Splunk-based SOC use cases to enhance threat detection and incident response.
- Engaged in AWS threat hunting, analyzing CloudTrail logs, VPC Flow Logs, and CloudWatch metrics to detect security anomalies and threats in AWS.
- Gained experience deploying and managing infrastructure in AWS using Infrasrtucture as a Code (IaC).
- Collaborated with the Cloud Security team to gain deep insights into Prisma Cloud Security Posture Management (CSPM) for AWS.

Skills

Languages: Python, Splunk Query Language (SPL), LINQ, Bash (Basics), HTML, CSS.

Technologies: Log Analysis, AWS (Core Services), PrismaCloud, Azure Cloud, Terraform (Basics), Cloud Security, Network Security, Terraform (IaC).

SIEM: Splunk (SIEM), DEVO

Operating Systems: Linux, Windows Server.

Database: SQL

Projects

Automated AWS-Splunk Integration for Enhanced Security and Efficiency

- Orchestrated AWS and Splunk integration, automating misconfiguration detection and remediation with the help of lambda service, leading to enhanced AWS security and operational efficiency.

Business Impact Analysis

- Utilized BPMN to prototype and assess the BPMN workflow with CVE and CVSS-based security.

SSH Honeypot and IDS in Raspberry Pi

- Implemented Raspberry Pi-based SSH honeypot and intrusion detection system, diverting attackers, swiftly detecting anomalies, and enhancing overall network security.

Snort IDS for Evidence Collection and Real-Time Notification For SQL Injection Attacks.

- Implemented Snort IDS for real-time detection and rapid alerting during SQL injection attacks, strengthening security and enabling post-event data analysis.

Certifications and Courses

Certified Network Security Practitioner (CNSP)

Microsoft Certified: Azure Fundamentals (AZ-900)

NSE 2 Network Security Associate (Fortinet)

Foundations of Operationalizing MITRE ATT&CK (AttackIq)

Foundations of Threat Hunting (Picus Security)

CompTIA Security+ (Course)

Network Defense Essential (EC Council)

Rutvik Shah

rutvikshah2412@gmail.com | 8490047099

EDUCATION

NATIONAL FORENSIC SCIENCE UNIVERSITY
M.Sc. Digital Forensics and Information Security
2021-2023 | Gandhinagar, Gujarat

A. D. PATEL INSTITUTE OF TECHNOLOGY
B. Tech Computer science and Engineering
2015-2019 | New Vallabh VidhyaNagar

RESEARCH JOURNAL

SMART BANNER ADVERTISEMENT USING DYNAMIC PRICING
International Research Journal of Engineering and Technology
Issued Aug 2019
Credential ID: Volume 6 Issue 8

LINKS

portfolio: /rutvikshah.vercel.com
LinkedIn: /rutvikshah2412
Github: /rutvikshah2412
Try Hack Me: /1azyc0d3r

SKILLS

TECHNICAL

• CNAPP • ASPM • VAPT
• DevSecOps • Secure SDLC
• Networking • OSINT
• SRE Practices - Security
• MS SharePoint/Power Apps/Power Automate
• Jira/ Confluence

Familiar:
GitHub • Jenkins • CI/ CD/ CT • AWS Cloud • BASH • Java • Python

MANAGERIAL

• Stakeholder Management & Cross-Functional Collaboration
• Security Product Evaluation & Procurement
• Budgeting & Resource Allocation
• Security Metrics and key Risk Indicators (KRIs)
• Vendor Management and Coordination.

PROFESSIONAL EXPERIENCE

CREDABLE – EQUENTIA SCF TECHNOLOGIES PRIVATE LIMITED
Senior Engineer - SRE — Feb 2023 - Present

- Managed Application Security Posture and CNAPP for continuous security monitoring and compliance across 10+ apps and Cloud Account.
- Conducted VAPT for web apps, APIs, cloud infrastructure to identify and mitigate threats.
- Optimized 5+ security tools for enhanced threat detection and proactive risk mitigation.
- Integrated security practices into DevSecOps, Achieved 90% automation of code scans and enforcing secure coding in CI/CD, leading to a 25% drop in critical vulnerabilities pre-deployment.
- Delivered security training to 15+ QA team members on vulnerability detection and remediation.
- Built security dashboards, offering real-time insights for informed decision-making.
- Authored 10+ remediation documentation with mitigation strategies and best practices.
- Led end-to-end security assessments, ensuring compliance with industry standards.

TATA CONSULTANCY SERVICES LIMITED (TCSL)
Assistant System Engineer (ASE) - Trainee — June 2019 - 2020

- Developed a scalable government sector application with robust architecture and design.
- Built and optimized 8 static and dynamic web interfaces for user interaction and performance.
- Developed a log management system with dynamic report generation and amendment tracking to enable monitoring of 100% user activities.
- Wrote secure, modular code, managed version control securely and enhanced UI responsiveness using the ZK (Ajax) framework improving overall user experience.

PROJECT UNDERTAKEN

- Smart Business Card.
- Smart advertisement display based on gender and age prediction.
- Exploratory study of DevSecOps (Development- Security- Operations).

PROFESSIONAL DEVELOPMENT AND ACTIVITY

- Character certificate of National Cadet Corps.
- Volunteer in the event "VFX" in SPECTRUM'18(A.D.I.T Techfest) in March, 2018.
- Participated in the "Can you root?", "ForSecCtf" in CTF'22(NFSU University) in July.
- Liaison officer responsibility in the event "7th Interpol DFEG Meeting" in October, 2022.
- Received ownership award for leading Vulnerability Assessment and Penetration Testing (VAPT) initiatives in January, 2024.

NAMPELLI KRISHNA CHAITHANYA VARMA

[8297760783|chaithanyanampelli55555@gmail.com|LINKEDIN-CHAITANYAVARMANAMPELLI|NIRMAL,504106]

PROFESSIONAL SUMMARY

Motivated and detail-oriented cybersecurity intern with hands-on experience in soc operations, vulnerability management, and threat analysis. Strong knowledge of security frameworks, network security, and incident response. Passionate about cybersecurity research and eager to apply skills in a professional setting.

TECHNICAL SKILLS

- SIEM & SOC : MDR,Splunk & alert logic, XSOAR, XDR
- Endpoint Security : Sophos MDR
- IDS/IPS/Firewall. : Sophos MDR
- System Security : Windows, Linux, Kali Linux
- Vulnerability Management: Qualys Guard, burpsuite, nmap.
- Ticketing tool : ServiceNow

- Threat Analysis ::Understanding of common threat vectors and attack methodologies.
- Incident Response ::Basic knowledge of incident response processes and protocols.

EDUCATION

Bachelor of Commerce / computer applications ,vashista degree college.
2021-2024

CERTIFICATION

[EC COUNCIL]EC-Council Certified Security Analyst (CSA)

CERTIFICATION NO: **ECC4391870265**

EXPERIENCE

Cybersecurity Intern

[PENTESTERZONE TECHNOLOGIES PVT LTD] | [04/ 2024] – [03/2025]

- Monitor security events and alerts using siem tools like splunk ,mdr,to identify potential threats.
- Conduct vulnerability scans using qualys, assisting in risk assessment and remediation planning.
- Assist in incident response, analyzing logs and investigating security incidents to support threat mitigation.
- Utilize network monitoring tools such as wireshark to detect anomalies and potential intrusions.
- Research emerging cybersecurity threats and trends to improve security posture.
- Ii have 1+ years of experience as a intern in soc analyst & vulnerability management analyst in the field of cyber security operations for 24*7 soc environment using the siem tools splunk enterprise, servicenow, sophos mdr, and qualys guard for vm
- Expertise in soc (security operations centre) operations methodology such as incident handling, network traffic monitoring, real time security event handling, log analysis, identifying and classifying attempted compromises to networks through heuristics identification of suspect traffic.
- Working with vulnerability management and patch management tasks and reachout to stakeholders on call if any urgent patching needed.
- Working with security protocols http, https, ssl, ipsec, and dhcp
- Experience in deployment of ca agent and de-install activities
- Experience in device configuration for various devices and applications including firewalls, ids, ips, windows servers, linux servers, database servers and other Applications as per the custom requirements.

PROJECT INVOLVEMENET

Client : NTT Data India
Payroll : PENTESTERZONE TECHNOLOGIES PVT LTD
Designation : SOC Analyst & VM Analyst
Duration : **APRIL/2024 TO MARCH/2025**

- Monitoring and analysis of events generated by various security and network tools like firewalls, proxy servers, av, ips/ids, system application, windows and linux servers e.t.c
- Working as vulnerability management tasks and deploy new agents.
- Security incident response: Responsible for monitoring of security alerts. Analysis of logs generated by appliances, investigation, and assessment on whether the incident is false positive or false negative.
- Use siem tools (splunk) to detect possible signs of security breaches and perform detailed investigation to confirm successful breach. Perform root cause analysis and appropriately handle the incident as per defined incident.
- Siem deployments (splunk), working with uf and hf
- Coordinating with network team, server team regarding activities and technical issues.
- Creating vulnerability and remedy reports and reporting them to users.
- Finding the critical servers and application inventory from respective business owners and scheduling the scan weekly, monthly and quarterly basis.
- Knowledge sharing session with the team members whenever complex incident issues are raised and also lessons learned from other team members.
- Scanning the environment using qualys tool and finding the vulnerabilities based on the business units and sending the report to respective business owners

PERSONAL INFORMATION

- Date of Birth : 14-04-2003
- Sex : Male

- Marital Status : Un-Married
- Languages Known : English, Telugu, Hindi
- Nationality : Indian

- **DECLARATION**

I hereby declare that the information furnished above is true to the best of my Knowledge.

Place: Hyderabad

(NAMPELLI KRISHNA CHAITHANYA VARMA)

Sowmya Lakkavajjala

Hyderabad
9182520626
sowmyalakkavajjala2000@gmail.com

Objective

Experienced Results-driven security engineer at Deloitte USI, having nearly 4 years of expertise in threat detection, SIEM engineering, and cloud security. Proficient in developing custom security content, advanced threat detection, and optimizing security architectures. Strong hands-on experience in Splunk, KQL, SPL, SOAR, MITRE ATT&CK, threat hunting, and cloud security (AWS & Azure). Certified in Splunk, Azure Security, and AWS Cloud Practitioner.

Experience

- **Deloitte** 2021 - Present
  Security engineer
  - Developed, tested, and deployed custom security detections in Splunk (SPL), Microsoft Defender (KQL) to enhance real-time threat visibility.
  - Created detection use cases for MITRE ATT&CK-aligned TTPs, increasing threat detection efficiency by 30% across SIEM and EDR platforms.
  - Engineered advanced threat detection rules and anomaly-based alerts to detect malicious activities, APT movements, and insider threats.
  - Onboarded and managed data sources to the SIEM platform (e.g., Beyond Trust, Fortigate, Palo Alto) to enhance log correlation and analysis.
  - Worked on applying patches to various vulnerabilities.
  - Conducted proactive threat hunting using the MITRE ATT&CK framework, leveraging network traffic analysis (PCAP, firewall logs, IDS logs) to detect unknown threats.
  - Analysed and processed security logs from multiple sources including Microsoft Defender, Carbon Black, and network logs, resulting in a 25% improvement in threat identification accuracy.
  - Performed root cause analysis (RCA) and fine-tuned detections based on post-incident findings, reducing false positives by 25%.
  - Handled the security incidents response and created incident response reports.
  - Led SIEM content development & tuning efforts, ensuring alignment with industry frameworks and compliance requirements.
  - Managed and optimized Linux-based SIEM infrastructure, improving log forwarding performance and reducing data ingestion latency by 20%.
  - Conducted deep log analysis and investigations to detect suspicious activities, improving visibility into lateral movements and persistence mechanisms.
  - Provided security expertise in customer-facing engagements, translating complex threat intelligence into actionable security controls.
  - Diagnosed and resolved log ingestion issues in Splunk, ensuring seamless data flow from diverse security sources (e.g., firewalls, EDR, proxy, and cloud platforms). Optimized log parsing, onboarding, and connector configurations, enhancing real-time threat visibility and detection.
  - Skilled in SOAR workflows and playbooks such as Resilient, enhancing incident response capabilities and streamlining security operations.
  - Utilized the MITRE Framework in hunting methodology, demonstrating a comprehensive understanding of the Cyber Kill Chain and Pyramid of Pain frameworks.

Education

- **Osmania University** 2021
  Stanley college of engineering and technology for women
  8.13

Skills

Splunk (Enterprise, Cloud, SOAR) ,MITRE ATT&CK Framework, SIEM Content Development ,Use Case Optimization , EDR (Carbon Black, Microsoft Defender), AWS (GuardDuty, CloudTrail), Azure (WAF, Risky Sign-ins), Python, PowerShell, Bash, Regex , Log Analysis, Log Forwarding & Parsing (Syslog-ng, rsyslog), Security Data Integration , Firewall, Proxy, IDS/IPS Log Analysis, API & Web Services Integration (SOAP, REST, JSON) ,KQL, SPL ,Threat Hunting & Incident Response , Cyber Kill Chain.

Artificial intelligence and Machine learning.

Projects

- **Medicinal herb identification using Deep learning**
  Published papers in Global Journal of Engineering Science and Research and JASC Journal.

Achievements & Awards

- Awards 2 Applause Awards – Deloitte India (Offices of the US) 1 Spot Award – Deloitte India (Offices of the US)

Certification

- Splunk Enterprise Certified Administrator
  Splunk Core Certified Power User
  Microsoft Certified: Security Operations Centre Associate (SC-200)
  AWS Certified: AWS Cloud Practitioner

CHEVULA SUNIL

Karimnagar, Telangana

chevulaasunil@gmail.com | +91 8688192227

https://www.linkedin.com/in/chevula-sunil-23977b338/

Professional Summary

Cybersecurity Analyst with **3+ years of experience** in Security Operations Center (SOC) environments, currently working as **L2 SOC Analyst**. Proficient in **Security Information and Event Management (SIEM) tools (Splunk, Microsoft Sentinel)**, **EDR solutions (CrowdStrike, Microsoft Defender)**, and **incident response methodologies**. Skilled in **threat hunting**, **log analysis**, **rule tuning**, and applying the **MITRE ATT&CK** framework for adversary behavior detection. Proven ability to reduce MTTD/MTTR and drive continuous improvements in security posture.

Technical Skills

- **SIEM & SOAR Tools**: Splunk, Microsoft Sentinel, IBM QRadar (basic), SOAR platforms
- **EDR & Endpoint Security**: CrowdStrike, Microsoft Defender, Carbon Black
- **Threat Intelligence & Analysis**: VirusTotal, Cisco Talos, IBM X-Force, Mx Toolbox
- **Security Concepts**: MITRE ATT&CK, TCP/IP, IDS/IPS, Phishing Detection, Malware Analysis
- **Tools & Platforms**: ServiceNow, JIRA, Wireshark

Work Experience

Winnow IT Services Pvt Ltd | SOC Analyst L2 | *Aug 2024 – Present*

- Monitored and analyzed **10,000+ security events per day** using **Splunk** and **Microsoft Sentinel**.
- Led high-impact **incident response efforts**, reducing **MTTD by 30%** and **MTTR by 40%**.
- Developed and tuned **20+ Security Information and Event Management (SIEM) use cases**, reducing false positives by **25%**.
- Conducted proactive **threat hunting** using Splunk and CrowdStrike EDR; detected **5+ critical incidents monthly**.
- Mentored L1 analysts and delivered training on SOC triage, malware analysis, and hunting.

- Integrated new data sources into Security Information and Event Management (SIEM) and automated alert correlation using APIs.
- Generated detailed incident reports and dashboards for management and audits.
- Supported **policy reviews**, **compliance checks**, and **patch validation efforts**.

Winnow IT Services Pvt Ltd | SOC Analyst L1 | *May 2022 – Aug 2024*

- Triaged **15,000+ logs/day** across firewalls, endpoints, and cloud assets.
- Investigated phishing attacks and achieved **95%+ resolution within SLA**.
- Created custom dashboards and alerts to enhance detection capabilities.
- Collaborated with vulnerability management teams to patch and remediate systems.
- Maintained SOC runbooks and developed SOPs to streamline L1 workflows.

Education

Bachelor of Technology (B.Tech)

JB Institute of Engineering and Technology, Hyderabad

Certifications

- Microsoft SC-200: Security Operations Analyst (In Progress)

Santosh Annapuraju

Phone number: (+91) 7569029991 (Mobile) | **Email address:** annapurajusantosh29@gmail.com | **LinkedIn:** https://www.linkedin.com/in/santosh-kumar-9666b82b5/

ABOUT ME

A dynamic and results-oriented IT professional with 4.7 years of experience, including over 3 years specializing in Information Security. Proficient in leveraging SIEM tools such as Splunk and QRadar to analyze and respond to security threats and intrusion attempts. Adept at working in fast-paced, challenging environments, I am committed to contributing to the growth of the organization while continuously advancing my career in cybersecurity.

PROFESSIONAL

Summary

A Competent professional with 4.7 years of experience in IT industry and 3+ year's Information Security as Security Analyst. Hands on experience with SIEM tool for logs monitoring and analysis on SOC (Security Monitoring and Operation) and SIEM (Security Information and Event Management) tools like Monitoring real-time events using Splunk, IBM Qradar and Azure Sentinel & Malware Analysis and good hands on experience on DLP, EDR, Email security.

- Knowledge on McAfee and LogRhytm, Crowdstrike (EDR, Malware Hunting), DLP–(Symantec), Email-Proofpoint Microsoft Advanced Threat Protection–ATP Microsoft O365 Security.
- Good knowledge on networking concepts including OSI layers, subnet, TCP/IP, ports, DNS, DHCP, firewall monitoring, content filtering, check point etc.
- Good understanding of security solutions like Anti-virus, DLP, proxy, Firewall filtering/monitoring, IPS, Email Security, Vulnerability Assessment.
- Hands-on experience on endpoint security.
- Trainings: SIEM (Splunk, Qradar, Azure Sentinel, Seceon) Malware Analysis, email security, DLP, Incident Lifecycle.

WORK EXPERIENCE

10/06/2024 – CURRENT Bengaluru

SENIOR SOC ENGINEER LIMINAL CUSTODY PVT LTD

- Monitor and respond to security alerts and incidents across custody operations using SIEM tools (Splunk, QRadar).
- Lead real-time monitoring and management of security events using SIEM tools (Splunk, IBM QRadar, Azure Sentinel) in a 24/7 Security Operations Center (SOC).
- Perform detailed analysis of security incidents, including phishing attempts, malware infections, and data breaches, to identify and mitigate threats.
- Collaborate with cross-functional teams to improve security incident response processes and reduce response times.
- Conduct vulnerability assessments and ensure remediation of security gaps using tools such as Qualys and Nessus.
- Provide detailed incident reports and trends to senior management for strategic decision-making.
- Ensure endpoint security and implement security policies related to antivirus (McAfee), endpoint detection (CrowdStrike Falcon), and firewall management (Palo Alto).
- Implement security measures to protect clients' financial assets, ensuring regulatory compliance and adherence to internal policies.
- Oversee secure processing of asset transfers, settlements, and corporate actions.
- Collaborate with cross-functional teams (custody operations, IT, compliance) to integrate security measures across all functions.
- Manage, configure, and troubleshoot security systems and custody platforms to ensure optimal operation.
- Lead the installation, configuration, and troubleshooting of security connectors in custody operations.
- Implement and maintain security protocols for the storage, transfer, and access of sensitive financial data (e.g., encryption of digital assets, secure transaction channels).
- Notify clients about upcoming corporate actions and provide them with information on their options and provide regular and ad-hoc reports to clients, summarizing asset positions, transaction history, and corporate actions.
- Maintain accurate and up-to-date records of all assets under custody, including documentation of transactions, contracts, and custodial agreements.

09/2020 – 07/06/2024

SECURITY ANALYST MICROLAND

- Monitored security alerts and events from various SIEM platforms (Splunk, QRadar) to detect and respond to security incidents.
- Analyzed phishing emails and spear-phishing attacks to detect and prevent email-based threats.
- Performed daily vulnerability scanning and patch management for systems and applications to reduce the attack surface.
- Managed and configured endpoint protection using CrowdStrike Falcon and Symantec to prevent malware and ransomware threats.
- Worked with the Incident Response team to analyze and remediate security incidents, including system compromises and unauthorized access.
- Managed service tickets using ServiceNow, ensuring timely resolution of security incidents and user-reported vulnerabilities.

08/2019 – 09/2020

SYSTEM ADMINISTRATOR

- Helped standardize and implement the scheduled maintenance plan documentation process.
- Monitored system performance and diagnosed software/hardware problems.
- Document and track issues via a ticketing system.
- Configured, troubleshot and maintained Windows 2003 and 2008 Servers.
- Ensured full and increment all data backups were successful.
- Performed data restore for users as needed.
- Responsible for applying security updates and patches on servers, desktops, and laptops.

TECHNICAL SKILLS

Key Skills

- Security Operations Center (SOC)
- SIEM Tools: Splunk, IBM QRadar, Azure Sentinel, Seceon
- Antivirus & Endpoint Security: McAfee, CrowdStrike Falcon, Symantec
- Threat Analysis: Phishing Email Analysis, Vulnerability Assessment (Qualys, Nessus)
- Email Security: Forcepoint, Email Logs from Forcepoint, Spam and Phishing Email Analysis
- Firewalls & Network Security: Palo Alto, DUO, IDS/IPS, VPNs
- Cybersecurity Tools: Carbon Black, Digital Garden USB/Print Logs
- Ticketing Tools: ServiceNow, FreshService
- Networking: TCP/IP, network configuration, segmentation, and firewalls
- Web Security: Forcepoint against viruses, malware, and phishing
- OS & System Administration: Linux, Windows Server, Mac
- Incident Response & Monitoring: Log analysis, malware analysis, alert triage

EDUCATION AND TRAINING

2012 – 2016

B.TECH (CSE) Geethanjali College of Engineering & Technology