



GOVINDARAJULU BARATAM



 Hyderabad, Telangana
500098

 +918374625923

 govindarajuluwasblue@
gmail.com

A result-oriented professional with 16.6 years of Information Security Operations, Firewall implementation/operations/support, Endpoint Security implementation/operations/support, and Infrastructure Management.

Work History

2018-04 - 2025-03

• Senior Consultant (Techno Functional)

Infosys

- Played role Offshore Cybersecurity Operations Manager for two clients period from Jan2021 to Sep2023
- Playing role as Subject Matter Expert in TrendMicro Products like OfficeScan 11/XG, Apex, CrowdStrike Antivirus Portal Protect, Deep Security for Linux, Server Protect for Storage Filers, Portable Security
- Involving Security Operations/Functional Activities at Offshore
- Handling team size of 100 including Offshore/Onsite members
- Involving Quality Audit internally
- Managing the team
- Attending Daily Sync Up calls/Scrum
- Weekly/bi-weekly/monthly meeting with the team
- Attending calls Weekly with client
- Involving Technical troubleshooting when there is my involvement, planning and suggesting the team to fix the issues
- Have knowledge on SIEM(Splunk), Vulnerability Management (Nexpose, Rapid7)
- Have experience in ProofPoint (Email Security), Mobile Iron(Mobile Device Management)
- Involving Certificate management of internal/external(Digicert)
- Experience in ticketing tool ServiceNow
- Attending Ticket Quality Review
- Attending Change Advisory Boarding meetings
- Played role Offshore Cybersecurity Operations Manager for two clients
- Handled Complex/Major technical issues
- Experience in Firewall, Panorama
- Tracking the firewall auditing AV/patch updates

- Involving monthly SLA/Inventory activities monthly
- Involving Incident/Service handling meetings
- Coordinating cross towers if there is any need/requirement
- Involving Offboarding/Onboarding related requests
- Preparing Dashboards in ServiceNow
- Working on configuring scheduled reports in ServiceNow
- Configuring Kanban Visual Task boarding for easy tracking/monitoring purpose
- Having experience in preparing SOPS/MOPs/KB articles
- Working on virus/malware/suspicious investigation to remediate
- Involving on preventive actions of suspicious traffic/malicious infections
- Following incident following procedures
- Taking proactive measures for Ransomware/Embargo countries logs
- Checking and investigating brute force attacks
- Analyzing/Investigating threat logs
- Whitelisting various various legitimate applications in TrendMicro
- Preparing shift rosters for the team
- Involving security Audit and Forensic investigation
- Experience in Infrastructure Security Operations
- Operations Support for Fortigate, PaloAlto Firewall/IPS, Cisco FTD, CheckPoint, F5 and Forcepoint firewalls, Pulse SSL VPN, Cisco ISE, Imperva, Zscaler(ZPA and ZIA)
- Working on the KPIs
- Preparing WSR and MSRs
- Experience in Hybrid Setup of Firewall/IPS
- IOS up gradation in Firewalls/IPS devices
- Preparing KB articles for the team
- Configuring splunk searching and reporting modules, knowledge objects, administration, Add-ons, Dashboards, Clustering and forwarder management
- Designing and maintaining production-quality splunk dashboards
- Developed splunk dashboards, searches and reporting to support various internal clients in Security IT operations and application development
- Splunk enterprise deployments and enabled continuous integration on as part of configuration management
- Involving SOC operations, working on SIEM
- Worked on security solutions (SIEM) that enable organizations to detect, respond and prevent these threats by providing valuable context and visual insights to help you make faster and smarter security decisions
- Configured and developed complex dashboards and reports in Splunk
- Involving Zero Trust Network Security Assessment, working on the proposals, Reviewing the artifacts and NIST assessment as well
- PKI Certificate Management
- Hands on experience in Azure Cloud Security
- Hands on experience in threat hunting
- Aware of GRC process
- Having basic knowledge Arbour DDOS tool
- Hands on experience in Algosec (firewall Implementation/Planning automated task) tool

Objectwin Technologies

- Endpoint Security Operations
- Cybersecurity Operations
- Project Management Activities
- Internal Quality Audit
- Infrastructure Security operations
- PKI support and operations
- Interaction with client
- Reviewing SOWs
- Documentation Review

2017-01 - 2017-06

Lead Systems

Software Paradigms InfoTech (SPI), Mysore, India

- Endpoint Security
- Infrastructure Security Operations
- Firewall support and operations
- Email Security
- Proxy support and operations

2014-05 - 2016-04

IT Support Engineer

National Bank Of Abu Dhabi, Abu Dhabi, UAE

- Role played IT support
- Print Security Management service
- Project Management activities
- Endpoint Security
- Firewall support (L1)

2007-05 - 2014-05

System/Network Administrator

St. John's Research Institute, Bangalore

- System/Network administration
- Endpoint security
- Server Administration
- Desktop support
- Documentation
- Lead role played



Education

2011-01

MBA: Information Systems

Sikkim Manipal University - Bangalore

2005-01

B.Sc.: Computer Science

Andhra University - AP

2001-01

Intermediate (+2): Maths, Physics and Chemistry

Board of Intermediate Education - Andhra Pradesh

Advanced Diploma: Computer Hardware, Networking



Certifications

Professional Development Program, St. John's Emmaus Tuberculosis Research Initiatives (SETRI Project), Basic Clinical Research, MCSE (Microsoft Certified Systems Engineer), Microsoft Windows Server 2003, ITIL Foundation Course, HP Sales Certified - Printing and Computing Services in 2015, AZ-

900: Microsoft Certified, Azure Fundamentals, AZ-500: Microsoft Certified, Azure Security Engineer Associate, Palo Alto EDU-010, Palo Alto Networks Certified Network Security Engineer (PCNSE), Symantec Sales Expert, Symantec Sales Expert+, Kanban Certification, Infosys Internal Certification- Cyber Security Professionals, Checkpoint Certified Security Administrator R80 (156-215.80), Cloud Security services, Networking Fundamentals Security, Infrasecurity Fundamentals, Splunk Power User Certification, Pursuing Certified Information Security Manager Certification (CISM)



Languages

- English (Read, Write, Speak)
- Hindi (Read, Write, Speak)
- Telugu (Read, Write, Speak)
- Tamil (Speak)
- Kannada (Speak, Read)
- Malayalam (Speak)



Personal Details

- **Date of Birth:** 1983-06-01
- **Religion:** Hindu
- **Marital Status:** Married
- **Other:** Marital Status: Married



Ticketing Tools

- Freshdesk admin
- ServiceNow
- ITSM Hp
- Jira (IRR)
- Archer (RCSA)
- Tenable (Nessus), Rapid 7 Insight VM



Onsite Experience

- 2.5 years, National Bank Of Abu Dhabi, Abu Dhabi, UAE



Clients Industries

- Semiconductor
- Cars
- Wind Power Manufacturing
- Banking
- Finance
- Dairy



Personal Information


- Passport Number: Z6118508
- Date of Birth: 06/01/83

- Marital Status: Married
- Religion: Hindu



Skills

- Endpoint security operations
- Infrastructure support
- Firewall operations/support/implementation
- Offshore security Operations
- Functional management
- Project management activities
- Preparing monthly reports
- SIEM Operations
- Vulnerability Management Operations
- Ticketing management
- Security Zero Trust assessment
- Interaction with clients
- Knowledge on Information Security/Cybersecurity Design/Architecture
- Conducting daily/weekly/monthly meetings with the offshore teams
- Involving Zscaler Private/Internet access, part of Operations
- Involving DLP support/operations
- Involving VPN support/operations
- Project Management Activities in Security Operations
- Problem and Change Management
- Issue solving/investigation/analysis
- Root Cause Analysis of issues
- Experience in EDR(Crowdstrike, MS Defender), IPS and IDS
- Work on KPIs, SLAs
- Involvement in recruitment
- Experience in Cybersecurity Architecture/Design/Implementation/Support
- Firewall support and operations L2.5 level in Cisco FTD, Checkpoint, Paloalto, Forcepoint, F5 and Fortigate products
- Knowledge in DDOS
- Knowledge in Threat modeling

- 
- Threat hunting
 - GRC policies
 - Information security governance
 - Experience in VAPT
 - Knowledge in Red and Blue teams