ROD VIAL
Technical Account Manager
Managed Cloud Enterprise Hosting (IaaS, SaaS, PaaS) Software & Network Solutions
| Managed Security Service Provider (MSSP)

**Task Description**

As a Technical Account Manager (TAM) role in the Managed Cloud Enterprise Software and Network Solutions based on Cybersecurity Managed Security Service Provider (MSSP) with a focus on Endpoint Protection and Cloud Architecture involves in providing dedicated highly technical support and guidance to key customers in the context of their cybersecurity needs. This position demands a strong understanding of cybersecurity principles, endpoint protection technologies, and cloud architecture to assist customers in safeguarding their digital assets and environments effectively.

- Customer Relationship Management: Develop and maintain strong relationships with key customers, understanding their unique requirements, objectives, and pain points related to cybersecurity, endpoint protection, and cloud architecture.
- Technical Guidance: Provide expert technical advice and best practices to customers on cybersecurity strategies, endpoint protection solutions, and the design and implementation of secure cloud architectures.
- Solution Customization: Collaborate with customers to tailor cybersecurity solutions, endpoint protection strategies, and cloud architecture designs to align with their specific business needs and security objectives.
- Incident Management: Act as a point of escalation for critical cybersecurity incidents, helping customers to rapidly respond and mitigate threats in their environments.
- Technical Support: Offer ongoing technical support and assistance, addressing customer inquiries, troubleshooting issues, and ensuring the efficient operation of cybersecurity and endpoint protection solutions.
- Training and Education: Conduct training sessions and workshops to educate customers on the proper use and optimization of cybersecurity tools, endpoint protection technologies, and cloud security practices.
- Risk Assessment and Compliance: Conduct security risk assessments and compliance reviews to identify potential vulnerabilities, ensuring that customers maintain compliance with relevant regulations and industry standards.
- Continuous Improvement: Proactively identify areas for improvement in cybersecurity strategies, endpoint protection measures, and cloud architecture designs, striving to enhance the overall security posture of the customers.
- Cross-functional Collaboration: Work closely with internal teams, such as sales, engineering, and product development, to communicate customer needs, feedback, and feature requests, ensuring a seamless customer experience.
- Account Growth and Expansion: Identify opportunities for account growth and expansion by understanding customers' evolving security requirements and recommending additional services or upgrades.
- Guidance Level Agreement – Providing guidance and best practices to customers and users of their product and services, performance in cloud computing and software-as-a-service (Saas) environments, assist customers in optimizing their usage and achieving customer’s desired outcomes, it includes guidance on best practices, cost optimization, security measures, scalability, tips, and recommendations based on expertise.
- Network Engineering and Cybersecurity Engineering - Design and Maintain Network Topologies Maps and Diagrams – Network Traffic Analysis, Tunneling, TCP-IP, Network segmentation security zones, DMZ cyber security, TCP-IP, DNS, Gateways, and replicas.
- Health and Optimization Analysis: Secure Operations Technology best practices, Advanced Protection and Responses against known threats and external cyberattacks such as DDoS and ransomware.

In addition to the strong technical expertise required for this role, effective communication and interpersonal skills are essential for building and maintaining strong relationships with customers. TAMs in this context act as trusted advisors, helping customers navigate the complexities of cybersecurity and effectively protect their digital assets and data from evolving threats.

## Key Full-Stack Security Applications and Tools

### PROTECTION

- Identity and Access Management – AWS Identity and Access Management (IAM), Azure AD, Okta, RSA Identity Governance and Lifecycle, Auth0, CyberArk Privileged Access Security Solution, SailPoint IdentityNow, ForgeRock Identity Platform
- Vulnerability Identification & Scanning – Nessus, OpenVAS, Qualys, Rapid7, Burp Suite, Acunetix, OpenSCAP, Retina Network Security Scanner, Nmap, Metasploit
- Access Point Identification – Rogue Aps AirDefence, AirMagnet, Wi-Fi Scanners, Wireless Site Survey Tools, Wi-Fi Analyzer Apps, Wireless Network Monitoring Software, Command-Line
- Managed Data Encryption – Microsoft BitLocker, Symantec Endpoint Encryption, McAfee Endpoint Encryption, VeraCrypt, Sophos SafeGuard, ESET Endpoint Encryption, Boxcryptor, Fortinet FortiCrypt, Trend Micro Endpoint Encryption, CipherShed
- Managed Firewall Service – Cisco ASA (Adaptive Security Appliance), Fortinet FortiGate, Palo Alto Networks, Juniper Networks SRX Series, Check Point, SonicWall, Sophos XG Firewall, WatchGuard Firebox, Cyberoam
- Managed Security – Security Information and Event Management (SIEM), Intrusion Detection and Prevention Systems (IDPS), Antivirus and Endpoint Protection, Firewall Solutions, Vulnerability Management, Data Loss Prevention (DLP), Security Orchestration, Automation, and Response (SOAR), Identity and Access Management (IAM), Encryption Software, Network Traffic Analysis (NTA)
- Managed Detection and Responses (MDR) Service – Security Information and Event Management (SIEM) Platforms, Endpoint Detection and Responses (EDR) solutions, Network Traffic Analysis (MDR), Behavioral Analytics, Incident Response Playbooks, Automation and Orchestration, Machine Learning and Artificial Intelligence, Forensics, and Investigation Tools, 24/7 Security Operations Center (SOC)
- Managed Security Patching – Microsoft System Center Configuration Manager (SCCM), WSUS (Windows Server Update Services), IBM BigFix, SolarWinds Patch Manager, ManageEngine Patch Manager Plus, Ivanti Patch for Windows, Shavlik Patch (VMware vCenter Protect), Qualys Patch Management, Kaseya VSA, Automox
- Malware Detection – Antivirus Software, Endpoint Protection Platforms (EPP), Malwarebytes, Microsoft Defender, ESET NOD32, Sophos Endpoint Protection, Bitdefender GravityZone, Avast Business Antivirus, Kaspersky Endpoint Security, Trend Micro Worry-Free Services, FireEye Endpoint Security, Cisco AMP for Endpoints, McAfee Endpoint Security
- Training and Education – One-Click Phishing Reporting, Security, Risk and Compliance Training, CloudGuru, Khan Academy, Udemy, Coursera, Microsoft PowerPoint, Canva, Piktochart, Zoom, Microsoft Teams, Cisco Webex
- Network Diagrams Topology – Microsoft Visio, LucidSpark, Lucidchart, Cisco Visio Stencils, Draw.io, Gliffy, Dia, NetBrain, yEd Graph Editor

### RECOVERY

- Disaster Recovery-as-a-Service – Zerto, Veeam, Druva, Acronis, Carbonite, IBM Resiliency Orchestration, Microsoft Azure Site Recovery, Datto, Unitrends, Infrascale

### ASSURANCE

- vCISO Service – Cybersecurity Assessment Tools, Security Information and Event Management (SIEM) Systems, Threat Intelligence Platforms – ThreatX, ThreatConnect, Anomali ThreatStream, Recorded Future, IBM X-Force Exchange, ThreatQ, FireEye iSIGHT, ThreatMiner, ThreatConnect Intelligence Platform (TIP), ThreatQuotient

  Penetration Testing Tools – Metasploit, Burp Suite, Nmap (Network Mapper), Wireshark, Aircrack-ng, Nikto, OWASP Zap, SQLMap, BeEF, Hydra, Empire, Cobalt Strike
- Caas – Compliance-as-a-Service – Regulatory Compliance Monitoring, Policy Management, Risk Assessment and Management, Audit and Reporting Tools, Data Privacy and Security, Automated Compliance Checks, Compliance Dashboards, Vendor Compliance Management, Document Management, Alerts and Notifications, Integration with Other Systems like Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP)
- Security Assessments – Vulnerability Assessment Scanners, Penetration Testing Tools, Security Information and Event Management (SIEM), Intrusion Detection and Prevention Systems (IDPS), Endpoint Security, Network Security Monitoring, Web Application Security Scanners, Compliance and Policy Management, Threat Intelligence Feeds, Reporting and Analytics
- Alerts Monitoring – Nagios, Zabbix, Prometheus, Grafana, Datadog, Splunk, New Relic, SolarWinds, Dynatrace, PagerDuty, Opsgenie, Fortra Alert Logic (MDR), eSentire, ScienceLogic.

**Secure Cloud Service**

- Managed Private Cloud
- Managed Public Cloud
- Managed Hybrid Cloud
- Managed Colocation
- Managed Off Premises
- Managed Cloud Enterprise
- Well-Architected Review for AWS
- Monitoring Insights
- Managed Databases
- Cloud Desktop (VDI)

- All Managed Architecture and Infrastructure platforms are based on Clustering, Nodes and Hosts Windows and Linux RedHat, Ubuntu, CentOs Servers through Virtualizations tools.
- VMWare vSphere/ESXi, Microsoft Hyper-V, Oracle VM VirtualBox, KVM (Kernel-based Virtual Machine), Xen, Proxmox Virtual Environment, Docker, Kubernetes, OpenStack, QEMU (Quick Emulator), Vagrant
- Network, Firewall, Load Balancer, Switches and Routers, WAF –
    - Palo Alto Networks: Palo Alto Networks Next-Generation Firewalls (NGFW), Panorama, Cortex XDR, Prisma Cloud, WildFire, AutoFocus, GlobalProtect, Traps, IoT Security, DNS Security
    - Juniper Networks – Junos OS, Junos Space, Juniper Contrail, Juniper NorthStar, Juniper Security Director, Juniper AppFormix, Juniper Sky Enterprise, Juniper MX Series Routers, Juniper SRX Series Firewalls, Juniper EX Series Switches
    - F5 Networks – Big-IP, NGINX, Silverline, Advanced WAF (Web Application Firewall), DNS Load Balancer, SSL Orchestrator, Access Policy Manager (APM), Application Security Manager (ASM), Shape Security
    - KEMP Technologies – KEMP LoadMaster, KEMP 360 Vision, KEMP 360 Application Experience (AX) Fabric, KEMP 360 GEO, KEM 360 Secure, KEMP 360 Application Firewall Pack (AFP), KEMP 360 Certificate Manager, KEMP 360 Service Delivery Guardian.
    - Fortinet – FortiGate, FortiManager, FortiAnalyzer, FortiClient, FortiWeb, FortiSIEM, FortiSandbox, FortiEDR, FortiNAC, FortiGate Cloud
- Exclusive sandbox testing labs: Microsoft Windows Server and Linux Server with Software Development Sandboxes, Application Sandboxes, Security Sandbox Tools, Web Application Sandboxing, Cloud Sandboxes, Testing Sandboxes, Mobile App Sandboxing