Position Description

Designation:	Head – Managed Detection & Response (MDR)
Business Unit:	Managed Security Services
Department:	Managed Detection & Response (MDR)
Location:	Ahmedabad, India
Reporting:	CEO/CTO

Tribastion Technologies Pvt Ltd
4th floor, Commercial Tower 1,
Inspire Business Park, Adani Shantigram,
Ahmedabad 382421, Gujarat, India

Phone: +91 79 4773-3001
Email: info@tribastion.com
CIN: U62099GJ2024PTC149820

Company Overview

Tribastion Technologies Private Limited is an emerging cybersecurity company headquartered in Ahmedabad, India. We specialize in delivering comprehensive cyber security consulting and managed security services to individuals and organizations.

Our services include proactive threat detection, swift incident response, continuous monitoring, and expertly designed security solutions to protect your digital environment from cyber threats. We cater to the broader cyber landscape, encompassing IT, OT, and Cloud environments.

Our long-term vision is to establish Tribastion as an Indian multinational, recognized globally as the preferred partner for quality cybersecurity solutions.

Position Summary

The Head of Managed Detection and Response (MDR) will oversee the MDR function within Tribastion and will be responsible for overseeing all aspects of cybersecurity operations and defense practices. This includes Next-Generation SOC, security analytics, threat hunting, incident response/automation, threat intelligence, malware analysis, SIEM use case engineering, MIRTE, SOC design and implementation related to NIST or other frameworks, security data lake management for structured and unstructured data, and other emerging technical security aspects of the SOC.

The individual will also advise client leadership on complex and often unique cyber threat issues within IT/Cloud and OT infrastructure. Responsibilities include recommending mitigation strategies and supporting customers and partners in implementing these strategies. This role encompasses project management, service delivery and quality assurance, customer management, and maintaining relationships with vendors and technology partners.

Key General Responsibilities:

- Lead and drive the Security Operations Management function, focusing on new project acquisition, project delivery, and operational support.
- Demonstrate strong leadership skills, with the capability to lead the department and manage functional teams effectively.
- Build and enhance team competency through strategic hiring and development initiatives.
- Provide robust technical leadership to the delivery team, partners, and customers.

- Be results-oriented with the ability to think strategically and work backward from customer needs.
- Oversee project management, service management, customer handling, and quality assurance.
- Communicate effectively and work cross-functionally, with a proven track record of delivering results and demonstrating strong ownership.
- Manage people-related functions, including hiring, talent development, performance management, succession planning, coaching direct reports, and fostering team engagement.
- Exhibit excellent communication and interpersonal skills, with the ability to influence and engage stakeholders at all levels within the organization, as well as with customers and partners/vendors.
- Support sales strategies to achieve business revenue goals through pre-sales activities and appropriate solutions.
- Identify and develop new opportunities with existing customers, ensuring high levels of customer satisfaction and retention.

Key Technical Responsibilities:

- As a technical leader, drive the future strategy for cybersecurity operations, including threat intelligence and analytics, threat monitoring, incident response, threat hunting, and forensic investigation.
- Establish and manage a large security operations and engineering team to support 24/7 SOC and infrastructure security operations.
- Design and implement enterprise security solutions, including Next-Generation SOC, threat and incident management services, and malware analysis.
- Conduct periodic reviews of the overall security posture, including server security, network security, application security, vulnerability management, cloud security, Active Directory, and common vulnerabilities and misconfigurations, along with their associated exploitation techniques.
- Develop use cases and hunting models based on a detailed study and mapping of TTPs, using the MITRE Framework to enhance enterprise security.

- Manage EDR/XDR, threat intelligence, security analytics technologies and tools, and SIEM tools (both commercial and open source), as well as TIP/SOAR platforms.
- Lead complex and diverse cybersecurity projects and implementation programs.
- Oversee incident response, digital forensics, breach investigations, and cyber crisis management programs.
- Supervise 24/7 security operations and threat monitoring, and security engineering for IT, cloud, and OT environments.
- Perform security architectural reviews, control assessments, and threat modeling to develop use cases for automated alerts and threat hunting.
- Complete project work with high quality and within deadlines, analyzing data, drawing comprehensive conclusions, and providing appropriate recommendations and mitigation plans.
- Communicate the technical impact and business risk to non-technical stakeholders post-project.
- Provide expert advice on the selection and implementation of SOC tools and technologies, following best practices and relevant frameworks such as NIST and MITRE.
- Adhere to security standards and frameworks, implementing best practice methodologies.
- Collaborate closely with customer security and IT teams to ensure secure practices are implemented.
- Educate customers, technical teams, IT and security teams, and application developers about emerging threats and vulnerabilities, raising awareness and building a Security Champion program.

Qualifications

- **Education:**
  - Bachelor's degree in Cybersecurity, Information Technology, Computer Science, or a related field. A master's degree or relevant certifications (e.g., CISSP, CISM, CHFI) are preferred.
- **Experience:**
  - 10-12 years of experience leading and managing 24/7 cybersecurity operations centers, delivering Managed Threat Detection and Response (MDR), threat

intelligence services, security analytics, and overseeing projects and customer engagements.

- At least 5 years of experience managing and leading a diverse team of security professionals, including SOC analysts, threat hunting experts, incident responders, threat intelligence analysts, software developers, forensic analysts, and security infrastructure engineers.
- 5 years of hands-on experience in cybersecurity, including security standards, best practices, SOC design, and implementation.
- 3-4 years of experience in enterprise security management, security product/solution integration, and security operations, with a strong understanding of network and system security concepts and standards, as well as security best practices.
- Proven experience in building, leading, and managing security teams with expertise in cybersecurity practices, SOC, threat intelligence, vulnerability management, and infrastructure security.
- Excellent skills in project management, service management, and customer handling.
- Exceptional written, presentation, and verbal communication skills, essential for team coordination, partner support, and service discussions, along with strong organizational abilities.
- Strong analytical skills with the ability to think creatively to solve complex technical problems.
- Ability to work effectively with clients, management, staff members, vendors, and consultants.
- Good interpersonal skills for interacting and collaborating with senior management stakeholders, including IT, Network and Security teams, and CIO/CTO/business leadership.
- Ability to remain calm and patient in high-pressure situations within a dynamic environment.

- **Skills and Competencies**
  - Experience in managing large security operation centers, including 24/7 security monitoring operations, incident response, digital forensics, breach investigations, and crisis management.

- Solid understanding of SOC architecture, operational models, and the design and implementation of enterprise security solutions, including Next-Generation SOC, threat and incident management services.
- Comprehensive knowledge of server security, network security, application security, vulnerability management, cloud security, OS internals (Windows, Linux), Active Directory, and common vulnerabilities, misconfigurations, and exploitation techniques.
- Extensive experience and practical knowledge in applying TTPs and the MITRE Framework to secure enterprise environments.
- Proficient in using EDR, threat intelligence, security analytics technologies and tools, SIEM tools (commercial and open-source), and TIP/SOAR platforms.
- Expertise in leading complex and diverse cybersecurity projects and implementation programs.
- Strong background in network/infrastructure vulnerability assessment and penetration testing (PT) concepts, including OWASP Top 10 vulnerabilities, enterprise security architecture, and relevant best practices and frameworks.
- Skilled in malware analysis.
- Extensive expertise in web, API, Android mobile app, and AWS/Azure cloud security.
- In-depth knowledge of cloud security best practices, including experience with AWS and Azure cloud platforms, and the ability to configure security controls and monitor for cloud-based threats. Experience in conducting AWS/Azure cloud security assessments.
- Familiarity with common compliance requirements such as GDPR, PCI-DSS, and ISO 27001.
- Knowledgeable in Agile processes and ITIL service management, as well as security standards and frameworks like NIST and MITRE.
- Ability to assess alerts, intelligently identify false positives, and improve detection rates.

Why Tribastion?

- **Strategic Leadership:** Play a pivotal role in shaping Tribastion's growth strategy in one of the most competitive markets in the world.

- **Career Advancement:** Opportunities for professional growth within a dynamic and rapidly expanding organization.
- **Innovative Environment:** Contribute to a company that prioritizes excellence, innovation, and leadership in the cybersecurity industry.

How to Apply

Interested candidates are invited to submit their resume, cover letter, and any relevant certifications to careers@tribastion.com. Please include "Head – Managed Detection & Response" in the subject line.

Tribastion is an equal opportunity employer. We celebrate diversity and are committed to creating an inclusive environment for all employees.