Director DDIT Detection & Response

Job ID
REQ-10043340
Mar 18, 2025
India

Summary

The Threat Detection & Response Director will be an integral leader within the Novartis Cyber Security Operations Center (CSOC). The CSOC is an advanced global team passionate about the active defense against the most sophisticated cyber threats and attacks. The Threat Detection & Response Director will assist the Global Head of CSOC to provide leadership and oversight over integral operational services including continuous security monitoring, triage, and incident response.

The Threat Detection & Response Director will contribute to the implementation of the overall Novartis information security strategy related to cyber security defense and operations. They will manage associated programs, develop and implement required processes, procedures and tools. They will actively encourage a positive culture and cohesiveness within the CSOC, while reporting qualified information about actual cyber threats to the senior management and stakeholders. In this role they will enable informed and consistent risk decisions and establish sustainable security capabilities to support business strategies in an efficient and effective way.

About the Role

Key Responsibilities:

In addition to accountabilities listed above in Job Purpose:

- Technical Team Leader
  - Supervise and manage a team of diverse skillsets and personalities
  - Evaluate and review performance; provide coaching and mentoring; develop and track career improvement goals
  - Instill and maintain cohesiveness and positive working culture
  - Accountable for regional delivery around incident detection and response activities
- Talent & Growth
  - Manage and mentor junior and senior associates and team leaders.
  - Plan and implement technical and nontechnical development strategies for continuous development of CSOC analysts and leaders.
- Security Monitoring and Triage
  - Monitor in real time security controls and consoles from across the Novartis IT ecosystem
  - Communicate with technical and non-technical end users who report suspicious activity
- Tooling & Capabilities
  - Ensure security detection, protection, response, and recovery standards, processes and procedures are up-to-date, maintained and followed.

    - Responsible for recommending, configuring, operating, maintaining and enhancing relevant security systems and tools globally, based on contextual information and current threat landscape.
- Forensics and Incident Response
    - Serve as escalation point for conducting investigations into security incidents involving advanced and sophisticated threat actors and TTPs
    - Perform forensic collection and analysis of electronic assets and devices, scripts and malicious software, and log sources from a variety of systems and applications
    - Manage incident response activities including scoping, communication, reporting, and long term remediation planning
    - Respond to major incidents as part of larger major incident response team
- Performance & KPIs
    - Establish key security performance indicators that ensure proper service delivery and continuous CSOC service improvements.
    - Define metrics, gather and regularly report to CISO, ITLT and identified stakeholders on risks and cyber security threats, as well as state, maturity and value derived from the CSOC services.
    - Perform analyses against large data sets to identify potential deficiencies in information security.
- Day to day:
    - Perform host based analysis, artifact analysis, network packet analysis, and malware analysis in support of security investigations and incident response
    - Coordinate monitoring, hunting, investigation, containment, and other response activities with business stakeholders and groups
    - Develop and maintain effective documentation; including monitoring, hunting, and response playbooks, processes, and other supporting operational material
    - Perform quality assurance review of analyst investigations and work product; develop feedback and development reports
    - Provide mentoring of associates and managers and serve as point of escalation for higher severity incidents
    - Develop incident analysis and findings reports for management, including gap identification and recommendations for improvement
    - Recommend or develop new detection logic and tune existing sensors / security controls
    - Work with security solutions owners to assess existing security solutions array ability to detect / mitigate the abovementioned TTPs
    - Creating custom SIEM queries and dashboards to support the monitoring and detection of advanced TTPs against Novartis network
    - Participate in weekend/after hour on-call rotation to triage and/or respond to major incidents

Commitment to Diversity and Inclusion:
Novartis is committed to building an outstanding, inclusive work environment and diverse teams' representative of the patients and communities we serve.

Accessibility and accommodation
Novartis is committed to working with and providing reasonable accommodation to individuals with disabilities. If, because of a medical condition or disability, you need a reasonable accommodation for any part of the recruitment process, or in order to perform the essential functions of a position, please send an e-mail to diversityandincl.india@novartis.com and let us know the nature of your request and your contact information. Please include the job requisition number in your message

Join our Novartis Network: If this role is not suitable to your experience or career goals but you wish to stay connected to hear more about Novartis and our career opportunities, join the Novartis Network here: https://talentnetwork.novartis.com/network

Why Novartis: Helping people with disease and their families takes more than innovative science. It takes a community of smart, passionate people like you. Collaborating, supporting and inspiring each other. Combining to achieve breakthroughs that change patients' lives. Ready to create a brighter future together? https://www.novartis.com/about/strategy/people-and-culture

Join our Novartis Network: Not the right Novartis role for you? Sign up to our talent community to stay connected and learn about suitable career opportunities as soon as they come up: https://talentnetwork.novartis.com/network

Benefits and Rewards: Read our handbook to learn about all the ways we'll help you thrive personally and professionally: https://www.novartis.com/careers/benefits-rewards

Division
Operations
Business Unit
CTS
Location
India
Site
Hyderabad (Office)
Company / Legal Entity
IN10 (FCRS = IN010) Novartis Healthcare Private Limited
Functional Area
Technology Transformation
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job
Job ID
REQ-10043340

Director DDIT Detection & Response

Apply to Job

Source URL: *https://prod1.novartis.com/careers/career-search/job/details/req-10043340-director-ddit-detection-response*

List of links present in page

1. https://talentnetwork.novartis.com/network
2. https://www.novartis.com/about/strategy/people-and-culture
3. https://talentnetwork.novartis.com/network
4. https://www.novartis.com/careers/benefits-rewards

5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Director-DDIT-Detection---Response_REQ-10043340
6. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Director-DDIT-Detection---Response_REQ-10043340