Associate Director DDIT ISC Detection & Response

Job ID
REQ-10023083
Oct 09, 2024
India

Summary

JOB PURPOSE
The Detection and Response Associate Director will be an integral part of the Novartis Cyber Security Operations Center (CSOC). The Novartis CSOC is an advanced security team that has reinvented Security Operations. It is comprised of a global team passionate about defending Novartis against modern and sophisticated IT security threats and attacks. The Detection and Response Associate Director will leverage a variety of tools and resources to detect, investigate, and mitigate threats impacting Novartis' networks, systems, users, and applications. This role will involve coordination and communication with technical and nontechnical teams, including security leadership and business stakeholders. This is a position intended for an experienced professional, and will challenge and grow their technical investigation, IT security, and leadership skillsets.

About the Role

Major Accountabilities:

In addition to accountabilities listed above in Job Purpose:

- Technical Team Manager
  - 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 monitoring and incident response
- 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
- 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
- Big Data analysis and reporting:
  - Utilizing SIEM/Big data to identify abnormal activity and extract meaningful insights.
  - Research, develop, and enhance content within SIEM and other tools

- Technologies and Automation:
  - Interface with engineering teams to design, test, and implement playbooks, orchestration workflows and automations
  - Research and test new technologies and platforms; develop recommendations and improvement plans
- Day to day:
  - Perform host based analysis, artifact analysis, network packet analysis, and malware analysis in support of security investigations and incident response
  - Coordinate investigation, containment, and other response activities with business stakeholders and groups
  - Develop and maintain effective documentation; including 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 junior staff and serve as point of escalation for higher difficulty 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

KEY PERFORMANCE INDICATORS / MEASURES OF SUCCESS

- Effectively investigate to identify root cause, including attack vector, exploitation, and other techniques utilized to bypass security controls
- Accurately diagnose impact, damage, and mitigation techniques needed to restore business operations and minimize reoccurrence
- Identify technology and process gaps that affect CSOC services; develop solutions and make recommendations for continuous improvement
- Provide oversight and support for first level monitoring and triage to ensure effective operations and mitigation of lower impact incidents
- Good cultural orientation and strong influencer of information risk management, information security, IT security, to be embedded across IT, OT and Medical Technologies

JOB DIMENSIONS (Job Scope)

Number of associates:

Management responsibility

Financial responsibility

No direct

PERSONAL CONSIDERATIONS

As the role is part of a global organization, willingness for required traveling and flexible work hours is important.

EDUCATION / EXPERIENCE

EDUCATION

- University working and thinking level, degree in business/technical/scientific area or comparable education/experience
- Professional information security certification, such as CISSP, CISM or ISO 27001 auditor / practitioner is preferred. Professional (information system) risk or audit certification such as CIA, CISA or CRISC is preferred

EXPERIENCE

- 6+ years of experience in Incident Response / Computer Forensics / CSOC team / Threat Hunting or related fields
- Experienced IT administration with broad and in-depth technical, analytical and conceptual skills
- Experience in reporting to and communicating with senior level management (with and without IT background, with and without in depth risk management background) on incident response topics
- Excellent written and verbal communication and presentation skills; interpersonal and collaborative skills; and the ability to communicate information risk-related and incident response concepts to technical as well as nontechnical audiences
- Excellent understanding and knowledge of general IT infrastructure technology and systems
- Proven experience to initiate and manage projects that will affect CSOC services and technologies

PRODUCT/MARKET/CUSTOMER KNOWLEDGE

- Good understanding of pharmaceutical industry. Good understanding and knowledge of business processes in a global pharmaceutical industry

SKILLS/JOB RELATED KNOWLEDGE

- Good mediation and facilitation skills
- Good knowledge of IT Security Project Management
- Experience with security incident monitoring and response related to medical devices
- Knowledge of (information) risk management related standards or frameworks such as COSO, ISO 2700x, CobiT, ISO 24762, BS 25999, NIST, ISF Standard of Good Practice and ITIL
- Knowledge of security frameworks such as Hitrust
- Host and network based forensic collection and analysis
- Dynamic malware analysis, reverse engineering, and/or scripting abilities
- Proficient with Encase, Responder, X-Ways, Volatility, FTK, Axiom, Splunk, Wireshark, and other forensic tools
- Understanding of Advanced Persistent Threat (APT) and associated tactics.
- Research, enrichment, and searching of indicators of compromise
- Very strong team and interpersonal skills along with the ability to work independently and achieve individual goals.
- Coordinate with other team members to achieve the specified objectives.
- Effective oral and written communication skills

NETWORKS

- High level of personal integrity, and the ability to professionally handle confidential matters and exude the appropriate level of judgment and maturity

- Ability to handle competing priorities, and seeking consensus when stakeholders have different or even contradicting opinions

OTHER

- Fluency (written and spoken) in English

CORE COMPETENCIES

Leadership

Establishes clear direction and sets stretch objectives. Aligns and energizes Associates behind common objectives. Champions the Novartis Values and Behaviors. Rewards/encourages the right behaviors and corrects others.

- Establishes clear directives and objectives.
- Communicates positive expectations for others on the team.
- Integrates and applies learning to achieve business goals.

Customer/Quality Focus

Assigns highest priority to customer satisfaction. Listens to customer and creates solutions for unmet customer needs. Established effective relationships with customers and gains their trust and respect.

- Defines quality standards to ensure customer satisfaction.
- Creates and supports world-class quality standards to ensure customer satisfaction.

Fast, Action-Oriented

Is action-oriented and full of energy to face challenging situations. Is decisive, seizes opportunities and ensures fast implementation. Strives for simplicity and clarity. Avoids 'bureaucracy'.

- Alerts others to potential risks and opportunities.
- Keeps organizational processes simple and efficient.
- Takes acceptable/calculated risks by adopting new or unknown directions.

Results Driven

Can be relied upon to succeed targets successfully. Does better than the competition. Pushes self and others for results.

- Anticipates potential barriers to achievement of shared goals.
- Pushes self and others to see new ways of achieving results (e.g., better business model).
- Uses feasibility and ROI analyses to ensure results.

Keeps pace with new developments in the industry

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-10023083

Associate Director DDIT ISC Detection & Response

Apply to Job

Source URL: *https://prod1.id.novartis.com/careers/career-search/job/details/req-10023083-associate-director-ddit-isc-detection-response*

List of links present in page

1. https://www.novartis.com/about/strategy/people-and-culture
2. https://talentnetwork.novartis.com/network
3. https://www.novartis.com/careers/benefits-rewards
4. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Associate-Director-DDIT-ISC-Detection---Response_REQ-10023083
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Associate-Director-DDIT-ISC-Detection---Response_REQ-10023083