Assoc. Dir. DDIT ISC Detection & Response

Job ID
REQ-10044110
May 02, 2025
Mexico

Summary

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 Lead
  - 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
  - Respond to major incidents as part of larger major incident response team
- 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
  - Participate in weekend/after hour on-call rotation to triage and/or respond to major incidents

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
Mexico
Site
INSURGENTES
Company / Legal Entity
MX06 (FCRS = MX006) Novartis Farmacéutica S.A. de C.V.
Functional Area
Technology Transformation
Job Type

Full time
Employment Type
Regular
Shift Work
No
Apply to Job
Job ID
REQ-10044110

Assoc. Dir. DDIT ISC Detection & Response

Apply to Job

Source URL: *https://prod1.novartis.com/us-en/careers/career-search/job/details/req-10044110-assoc-dir-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/INSURGENTES/Assoc-Dir-DDIT-ISC-Detection---Response_REQ-10044110-1
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/INSURGENTES/Assoc-Dir-DDIT-ISC-Detection---Response_REQ-10044110-1