Director DDIT Detection & Response

Job ID
REQ-10043330
Apr 03, 2025
Malaysia

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

Director DDIT Detection & Response

Location – Malaysia #LI Hybrid

About the Role:

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.

Key Responsibilities:

- Plan and implement technical and nontechnical development strategies for continuous development of CSOC analysts and leaders.
- Accountable for regional delivery around incident detection and response activities.
- Monitor in real time security controls and consoles from across the Novartis IT ecosystem.
- 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.
- 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.

Commitment to Diversity & Inclusion: :

We are committed to building an outstanding, inclusive work environment and diverse teams representative of the patients and communities we serve.

Essential Requirements:

- 10+ 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 leading and building highly motivated and technical global teams.
- 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.

Desirable Requirements:

- Excellent stakeholder management skills.
- Excellent communication, people management, stakeholder’s management and leadership skills.
- Good understanding of pharmaceutical industry. Good understanding and knowledge of business processes in a global pharmaceutical industry

Why Novartis: Our purpose is to reimagine medicine to improve and extend people’s lives and our vision is to become the most valued and trusted medicines company in the world. How can we achieve this? With our people. It is our associates that drive us each day to reach our ambitions. Be a part of this mission and join us! Learn more here: https://www.novartis.com/about/strategy/people-and-culture

You’ll receive: You can find everything you need to know about our benefits and rewards in the Novartis Life Handbook. https://www.novartis.com/careers/benefits-rewards

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.
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
Universal Hierarchy Node
Location
Malaysia
Site
Selangor
Company / Legal Entity
MY01 (FCRS = MY001) Novartis Corporation (Malaysia) Sdn. Bhd. (19710100054)
Functional Area
Technology Transformation
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job
Job ID
REQ-10043330

Director DDIT Detection & Response

Apply to Job

Source URL: *https://prod1.novartis.com/uk-en/careers/career-search/job/details/req-10043330-director-ddit-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/Selangor/Director-DDIT-Detection---Response_REQ-10043330-3
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Selangor/Director-DDIT-Detection---Response_REQ-10043330-3