

# Associate Director Threat Hunting & Response

Job ID  
REQ-10045919  
Jun 29, 2025  
Malaysia

## Summary

The Associate Director Threat Hunting and Response will be an integral part of 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 Associate Director Threat Hunting and Response is a principal engineer who will leverage a variety of tools and resources to proactively detect, investigate, and mitigate emerging and persistent 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. As an experienced skilled engineer, this role will also involve coaching and mentoring of more junior members of the CSOC.

## About the Role

### MAJOR ACCOUNTABILITIES

In addition to accountabilities listed above in Job Purpose:

- Network Forensics and Incident response
  - Serve as escalation point for conducting investigations into security incidents involving advanced and sophisticated threat actors and TTPs
  - Leverage expertise in network analysis to analyze packet captures, ID/PS and firewall logs, and log sources from a variety of systems and applications
  - Manage incident response activities including scoping, communication, reporting, and long term remediation planning
- Threat Hunting:
  - Serve as a subject matter expert in Network Security, including common attack types, network-based detection methodologies, and threat hunting trailheads
  - Review incident and intelligence reports from a variety of internal and external sources and teams
  - Lead the identification and validation of security threats across network traffic and endpoint activity to support proactive defense efforts.
  - Interface with security teams and business stakeholders to implement countermeasures and improve defenses
  - 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 network packet analysis, host based analysis, artifact 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
  - Provide mentoring of junior staff 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
  - Continuously refine and develop new detection logic, while optimizing existing security sensors, network monitoring technologies, and 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](mailto: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

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-10045919

## **Associate Director Threat Hunting & Response**

[Apply to Job](#)

---

**Source URL:** <https://prod1.id.novartis.com/id-en/careers/career-search/job/details/req-10045919-associate-director-threat-hunting-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/Selangor/Associate-Director-Threat-Hunting---Response\\_REQ-10045919-1](https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Selangor/Associate-Director-Threat-Hunting---Response_REQ-10045919-1)
6. [https://novartis.wd3.myworkdayjobs.com/en-US/Novartis\\_Careers/job/Selangor/Associate-Director-Threat-Hunting---Response\\_REQ-10045919-1](https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Selangor/Associate-Director-Threat-Hunting---Response_REQ-10045919-1)