# Assoc. Dir. DDIT ISC Threat Hunting

Job ID
REQ-10044437
Mar 28, 2025
Mexico

## 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 Responsewill 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:

- 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
- Threat Hunting:
  - Review incident and intelligence reports from a variety of internal and external sources and teams
  - Develop hypotheses, analyze techniques, and execute hunts to identify threats across the environment
  - 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 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
  - 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
  - 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-10044437

## Assoc. Dir. DDIT ISC Threat Hunting

Apply to Job

---

**Source URL:** *https://prod1.novartis.com/careers/career-search/job/details/req-10044437-assoc-dir-ddit-isc-threat-hunting*

**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-Threat-Hunting_REQ-10044437
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/INSURGENTES/Assoc-Dir-DDIT-ISC-Threat-Hunting_REQ-10044437