

# Associate Director Threat Detection & Response

Job ID

REQ-10075330

Apr 21, 2026

LOC\_MX

## About the Role

### Key Responsibilities:

- Lead and support complex cyber incident investigations across endpoints, identity, email, cloud, network, and data environments.
- Coordinate incident response activities, including triage, scoping, containment, eradication, recovery, and post-incident analysis.
- Serve as a senior escalation point for high-severity security incidents and provide expert guidance during active response efforts.
- Drive CSOC optimization initiatives focused on improving incident handling, analyst effectiveness, operational consistency, and overall response speed and quality.
- Identify opportunities to enhance detection coverage, reduce alert fatigue, improve investigation fidelity, and streamline response processes.
- Partner with threat hunting, detection engineering, threat intelligence, vulnerability management, and other cyber teams to improve CSOC outcomes.
- Develop and refine incident response playbooks, standard operating procedures, and investigation guidance.
- Perform deep technical analysis of attacker behavior, tactics, techniques, and procedures to support effective response and lessons learned.
- Translate incident trends and operational insights into recommendations for security improvements, control enhancements, and process changes.
- Contribute to CSOC metrics, performance reporting, and maturity assessments to help leadership understand operational effectiveness and risk trends.
- Mentor analysts and responders through technical guidance, incident coaching, and knowledge sharing, while remaining an individual contributor.
- Support tabletop exercises, readiness activities, and continuous improvement efforts across cyber operations.

### Essential Requirements:

- Bachelor's degree in Cybersecurity, Computer Science, Information Technology, or a related field, or equivalent practical experience.
- 8+ years of experience in cybersecurity, with significant experience in incident response, threat detection, or security operations.
- Strong hands-on experience investigating and responding to security incidents in enterprise environments.
- Deep understanding of attacker techniques across endpoint, identity, network, cloud, and email attack surfaces.
- Experience working in a CSOC, SOC, or incident response function in a large, complex organization.
- Strong knowledge of security operations workflows, alert triage, escalation management, and response coordination.
- Experience with SIEM, EDR/XDR, email security, identity monitoring, case management, and other security operations technologies.
- Ability to analyze logs, alerts, and forensic artifacts to determine scope, impact, and response actions.
- Strong written and verbal communication skills, with the ability to clearly brief both technical teams and senior stakeholders.
- Proven ability to identify operational improvement opportunities and drive meaningful enhancements without direct people management responsibility.

### Desirable Requirements:

- Experience leading or supporting major incident response efforts in a global enterprise environment.
- Familiarity with frameworks such as MITRE ATT&CK, NIST, and incident response lifecycle best practices.
- Experience improving SOC or CSOC operating models, workflows, metrics, or tooling.
- Background in threat hunting, detection engineering, digital forensics, or adversary emulation.
- Relevant certifications such as GCIH, GCFA, GCIA, GNFA, CISSP, or equivalent.
- Experience working cross-functionally with security engineering, infrastructure, legal, privacy, and business stakeholders

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.

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>

Join our Novartis Network: If this role is not suitable to your experience or career goals but you wish to stay connected to learn more about Novartis and our career opportunities, join the Novartis Network here:

<https://talentnetwork.novartis.com/network>

**Role Requirements**

**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>

**Benefits and Rewards:** Learn about all the ways we’ll help you thrive personally and professionally.

[Read our handbook \(PDF 30 MB\)](#)

Division

DIV\_TO

Business Unit

Information Technology

Location

LOC\_MX

Site

INSURGENTES

Company / Legal Entity

MX06 (FCRS = MX006) Novartis Farmacéutica S.A. de C.V.

Functional Area

FCT\_TT

Job Type

Full time

Employment Type

Regular

Shift Work

No

[Apply to Job](#)

Job ID

REQ-10075330

## Associate Director Threat Detection & Response

[Apply to Job](#)

---

**Source URL:** <https://prod1.jobapi.novartis.com.cn/req-10075330-associate-director-threat-detection-response>

### List of links present in page

1. <https://prod1.jobapi.novartis.com.cn/req-10075330-associate-director-threat-detection-response>
2. <https://www.novartis.com/about/strategy/people-and-culture>
3. <https://talentnetwork.novartis.com/network>
4. <https://www.novartis.com/about/strategy/people-and-culture>
5. [https://www.novartis.com/sites/novartis\\_com/files/novartis-life-handbook.pdf](https://www.novartis.com/sites/novartis_com/files/novartis-life-handbook.pdf)
6. [https://novartis.wd3.myworkdayjobs.com/en-US/Novartis\\_Careers/job/INSURGENTES/Associate-Director-Threat-Detection---Response\\_REQ-10075330-1](https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/INSURGENTES/Associate-Director-Threat-Detection---Response_REQ-10075330-1)
7. [https://novartis.wd3.myworkdayjobs.com/en-US/Novartis\\_Careers/job/INSURGENTES/Associate-Director-Threat-Detection---Response\\_REQ-10075330-1](https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/INSURGENTES/Associate-Director-Threat-Detection---Response_REQ-10075330-1)