NOVARTIS

Associate Director Threat Detection & Response

Job ID
REQ-10075330

4月 21, 2026

Mexico

摘要

Location: Mexico City, Mexico; #LI-HYBRID 12 days/month in office

Internal job title: Assoc. Dir. DDIT ISC Threat Detection & Response

The Associate Director of Threat Detection and Response is a senior individual contributor within the Cyber Security Operations Center (CSOC), responsible for leading high-impact incident response activities and driving continuous optimization of CSOC capabilities, processes, and detection effectiveness. This role serves as a senior technical expert and strategic operator, helping the organization rapidly identify, investigate, contain, and remediate cyber threats while improving the overall maturity and performance of security operations.

This position is ideal for a hands-on security leader who combines strong incident response expertise with the ability to identify operational gaps, improve workflows, strengthen detection and response capabilities, and influence teams across the broader security organization.

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

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)

部门
Operations

Business Unit
Information Technology

地点
Mexico

站点
INSURGENTES

Company / Legal Entity
MX06 (FCRS = MX006) Novartis Farmac é utica S.A. de C.V.

Functional Area
Technology Transformation

Job Type
Full time

Employment Type
Regular

Shift Work
No

Job ID
REQ-10075330

Associate Director Threat Detection & Response

Apply to Job

Job ID
REQ-10075330

Associate Director Threat Detection & Response

Apply to Job

Source URL:
https://www.novartis.com.cn/careers/career-search/job/details/req-10075330-associate-director-threat-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/about/strategy/people-and-culture
4. https://www.novartis.com/sites/novartiscom/files/novartis-life-handbook.pdf
5. https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/INSURGENTES/Associate-Director-Threat-Detection---ResponseREQ-10075330-1
6. https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/INSURGENTES/Associate-Director-Threat-Detection---ResponseREQ-10075330-1