# Senior Specialist DDIT ISC Detection & Response

Job ID
REQ-10023403
Sep 26, 2024
Mexico

## About the Role

MAJOR ACCOUNTABILITIES

In addition to accountabilities listed above in Job Description:

· Security Monitoring and Triage

o Monitor in real time security controls and consoles from across the Novartis IT ecosystem

o Communicate with technical and non-technical end users who report suspicious activity

· Forensics and Incident Response

o Conduct initial investigations into security incidents involving a variety of threats

o Gather live evidence from endpoint devices and log sources from a variety of systems and applications

o Support incident response activities including scoping, communication, reporting, and long term remediation planning

o Prepare technical reports for business stakeholders and IT leadership

· Big Data analysis and reporting:

o Utilizing SIEM/Big data to identify abnormal activity and extract meaningful insights.

o Research, develop, and enhance content within SIEM and other tools

· Technologies and Automation:

o Interface with engineering teams to design, test, and implement playbooks, orchestration workflows and automations

o Research and test new technologies and platforms; develop recommendations and improvement plans

· Day to day:

o Perform host based analysis, artifact analysis, network packet analysis, and malware analysis in support of security investigations and incident response

o Coordinate investigation, containment, and other response activities with business stakeholders and groups

o Develop and maintain effective documentation; including response playbooks, processes, and other

supporting operational material

o Perform quality assurance review of analyst investigations and work product; develop feedback and development reports

o Provide mentoring of junior staff and serve as point of escalation for higher severity incidents

o Develop incident analysis and findings reports for management, including gap identification and recommendations for improvement

o Recommend or develop new detection logic and tune existing sensors / security controls

o Work with security solutions owners to assess existing security solutions array ability to detect / mitigate the abovementioned TTPs

o Creating custom SIEM queries and dashboards to support the monitoring and detection of advanced TTPs against Novartis 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

**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-10023403

## Senior Specialist DDIT ISC Detection & Response

Apply to Job

---

**Source URL:** *https://prod1.jobapi.novartis.com/req-10023403-senior-specialist-ddit-isc-detection-response*

**List of links present in page**

1. https://prod1.jobapi.novartis.com/req-10023403-senior-specialist-ddit-isc-detection-response
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/INSURGENTES/Senior-Specialist-DDIT-ISC-Detection---Response_REQ-10023403-1
6. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/INSURGENTES/Senior-Specialist-DDIT-ISC-Detection---Response_REQ-10023403-1