

Associate Director DDIT ISC CSOC Onboarding

Job ID
REQ-10023036
Sep 26, 2024
Mexico

About the Role

MAJOR ACCOUNTABILITIES

In addition to accountabilities listed above in Job Purpose:

- Onboarding Lead
 - Lead and manage a geographically distributed team of Skilled Engineers, providing guidance and support while leveraging their diverse skillsets and personalities.
 - Evaluate and review performance metrics and KPIs to ensure the Onboarding team is meeting targets and delivering efficient and effective results.
 - Take accountability for the team's performance in various areas, including but not limited to data onboarding to:
 - SIEM platforms such as Sentinel and Splunk
 - Supporting audit requests and reports
 - Engaging with product teams to address technical challenges
 - Managing stakeholders' commitments
 - Act as the primary point of contact for first-level escalations, addressing any issues or concerns that arise and ensuring timely resolution.
 - Develop and maintain comprehensive documentation to facilitate knowledge sharing and ensure quality outcomes are consistently achieved.
 - Drive a culture of continuous improvement and innovation within the team, identifying opportunities to optimize processes and enhance efficiency.
 - Serve as a subject matter expert in onboarding processes and play an active role in guiding the team and providing expertise whenever needed.
- Data Onboarding and Technical Management
 - Evaluate and onboard new data sources, performing data analysis for identifying anomalies and trends, and developing dashboards and visualizations for data reporting.
 - Collaborate with CSOC engineers, Threat Hunters, and CSOC Analysts to gather requirements and develop solutions.
 - Troubleshoot and provide support for onboarding issues with platforms like Sentinel, Splunk, and Cribl.
 - Validate and ensure proper configuration and implementation of new logics with security system and application owners.
 - Perform data normalization, establish datasets, and develop data models.
 - Manage backlog of customer requests for onboarding new data sources.
 - Detect and resolve issues in various data sources, implementing health monitoring for data sources

and feeds.

- Identify opportunities for automation in data onboarding and proactively detect parsing/missing-data issues.

Mandatory Requirements:

- Previous experience as a Team Leader
- Hands-on experience of SIEM tools with preferable certification of Splunk, Sentinel etc. , and experience managing Data ingestion pipeline through Cribl
- Understanding of security systems (such as AV, IPS, Proxy, FWs etc.).
- Solid understanding of error messages and logs displayed by various software.
- Understanding of network protocols and topologies.
- Excellent communications skills with written and spoken English

Desirable Requirements:

- Security use-case design and development
- Understanding of SOAR

CORE COMPETENCIES

Leadership

Customer/Quality Focus

Fast, Action-Oriented

Results Driven

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-10023036

Associate Director DDIT ISC CSOC Onboarding

[Apply to Job](#)

Source URL: <https://prod1.jobapi.novartis.com/req-10023036-associate-director-ddit-isc-csoc-onboarding>

List of links present in page

1. <https://prod1.jobapi.novartis.com/req-10023036-associate-director-ddit-isc-csoc-onboarding>
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/Associate-Director-DDIT-ISC--CSOC-Onboarding_REQ-10023036-1
6. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/INSURGENTES/Associate-Director-DDIT-ISC--CSOC-Onboarding_REQ-10023036-1