

# Associate Director of Forensics

Job ID

REQ-10022259

Jan 16, 2025

Indien

## Summary

The Associate Director of Forensics 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 of Forensics is a seasoned and skilled professional who will leverage a variety of tools and resources to provide complete digital forensic services for the CSOC/ISC as well as for other functions including (but not limited to) Global Security, Human Resources, Internal Audit, and Legal. This role will involve coordination and communication with technical and nontechnical teams, including security leadership and business stakeholders.

## About the Role

### MAJOR ACCOUNTABILITIES

In addition to accountabilities listed above in Job Purpose:

- Digital Forensics and Incident Response
  - Support specific IT forensic investigations and operations, including
    - The extraction of data and electronic evidence from information technology in a way that ensures that the data is seized in compliance with computer forensic standards and in compliance with chain of custody guidelines.
    - The subsequent analysis of this electronic evidence where allowed and relevant.
  - Work with Group Legal department on forensic litigation support by providing expert advice, performing acquisition and discovery work, and writing summary reports
  - Actively participate in incident response team and efforts; perform evidence collection and root cause analysis of compromised devices
  - Create forensic images of electronic media and devices; including but not limited to servers, laptops, mobile phones, and portable storage devices
  - Continually keep current with emerging IT forensics trends, technologies and software.
  - Conduct investigations into security alerts and coordinate root cause analysis of IT Security incidents
- Technologies and Automation:
  - Interface with engineering teams to design, test, and implement playbooks, orchestration workflows and automations that support forensic activities
  - Research and test new technologies and platforms; develop recommendations and improvement plans
- Day to Day
  - Manage the development of tools, policies and processes to support the digital forensic program

- Develop metrics and KPI reports for management, including gap identification and recommendations for improvement
- Recommend or develop new forensic tools and techniques
- Provide mentoring and coaching of other CSOC team members

## **KEY PERFORMANCE INDICATORS / MEASURES OF SUCCESS**

- Demonstration of efficiency and effectiveness in forensic procedures (based on feedback from stakeholders involved)
- Timeliness of service delivery and customer satisfaction
- Good cultural orientation and strong influencer of information risk management, information security, IT security, to be embedded across IT, OT and Medical Technologies

## **JOB DIMENSIONS (Job Scope)**

### **Number of associates:**

Potentially external resources when relevant and required

### **Management responsibility**

### **Financial responsibility**

## **PERSONAL CONSIDERATIONS**

As the role is part of a global organization, willingness for required traveling and flexible work hours is important.

## **EDUCATION / EXPERIENCE**

### **EDUCATION**

- **Essential:**
  - University working and thinking level, degree in business/technical/scientific area or comparable education/experience.
- **Desirable:**
  - Professional information security certification, such as CISSP, CISM or ISO 27001 auditor / practitioner is preferred. Professional (information system) risk or audit certification such as CIA, CISA or CRISC is preferred.

### **EXPERIENCE**

- 4+ years of experience in Digital Forensics
- Experienced IT administration with broad and in-depth technical, analytical and conceptual skills
- Experience in reporting to and communicating with senior level management (with and without IT background, with and without in-depth risk management background) on incident response topics.
- Excellent written and verbal communication and presentation skills; interpersonal and collaborative skills; and the ability to communicate information risk-related and incident response concepts to technical as well as nontechnical audiences.
- Excellent understanding and knowledge of general IT infrastructure technology and systems
- Proven experience to initiate and manage projects that will affect CSOC services and technologies.

## PRODUCT/MARKET/CUSTOMER KNOWLEDGE

- Good understanding of pharmaceutical industry. Good understanding and knowledge of business processes in a global pharmaceutical industry

## SKILLS/JOB RELATED KNOWLEDGE

- Good mediation and facilitation skills
- Good knowledge of IT Security Project Management
- Experience with digital forensics related to medical/manufacturing devices.
- Knowledge of (information) risk management related standards or frameworks such as COSO, ISO 2700x, CobiT, ISO 24762, BS 25999, NIST, ISF Standard of Good Practice and ITIL
- Host and network based forensic collection and analysis
- Proficient with Encase, Responder, X-Ways, Volatility, FTK, Axiom, Splunk, Wireshark, and other forensic tools
- Research, enrichment, and searching of indicators of compromise
- Very strong team and interpersonal skills along with the ability to work independently and achieve individual goals.
- Coordinate with other team members to achieve the specified objectives.
- Excellent written and verbal communication skills; interpersonal and collaborative skills; and the ability to communicate IT security and IT Security risk-related concepts to technical and nontechnical audiences.

## NETWORKS

- High level of personal integrity, and the ability to professionally handle confidential matters and exude the appropriate level of judgment and maturity.
- Ability to handle competing priorities, and seeking consensus when stakeholders have different or even contradicting opinions.

## OTHER

- Fluency (written and spoken) in English.

**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>

**You'll receive:** You can find everything you need to know about our benefits and rewards in the Novartis Life Handbook. <https://www.novartis.com/careers/benefits-rewards>

**Commitment to Diversity and Inclusion:** Novartis is committed to building an outstanding, inclusive work environment and diverse teams' representative of the patients and communities we serve.

**Join our Novartis Network:** If this role is not suitable to your experience or career goals but you wish to stay connected to hear 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>

**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

Standort

Indien

Site

Hyderabad (Office)

Company / Legal Entity

IN10 (FCRS = IN010) Novartis Healthcare Private Limited

Functional Area

Technology Transformation

Job Type

Full time

Employment Type

Regular

Shift Work

No

[Apply to Job](#)

Job ID

REQ-10022259

## **Associate Director of Forensics**

[Apply to Job](#)

---

**Source URL:** <https://uat2.novartis.de/de-de/careers/career-search/job/details/req-10022259-associate-director-forensics>

### **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/Hyderabad-Office/Associate-Director-DDIT-ISC-Forensics\\_REQ-10022259-1](https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Associate-Director-DDIT-ISC-Forensics_REQ-10022259-1)
5. [https://novartis.wd3.myworkdayjobs.com/en-US/Novartis\\_Careers/job/Hyderabad-Office/Associate-Director-DDIT-ISC-Forensics\\_REQ-10022259-1](https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Associate-Director-DDIT-ISC-Forensics_REQ-10022259-1)