Associate Director of Forensics DDIT ISC

Job ID
REQ-10039880
Feb 17, 2025
Malaysia

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

Your key responsibilities:

- 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
  - Provide mentoring and coaching of other CSOC team members

- 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

What you'll bring to the role:

- 4+ years of experience in Digital Forensics
- Experience with digital forensics related to medical/manufacturing devices
- Host and network based forensic collection and analysis
- Experienced IT administration with broad and in-depth technical, analytical and conceptual skills
- Excellent understanding and knowledge of general IT infrastructure technology and systems
- Good knowledge of IT Security Project Management, with proven experience to initiate and manage projects that will affect CSOC services and technologies
- 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
- Proficient with Encase, Responder, X-Ways, Volatility, FTK, Axiom, Splunk, Wireshark, and other forensic tools
- Research, enrichment, and searching of indicators of compromise
- 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
- Good mediation and facilitation skills
- Very strong team and interpersonal skills along with the ability to work independently and achieve individual goals; ability to coordinate with other team members to achieve the specified objectives.

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
Malaysia
Site
Selangor
Company / Legal Entity
MY01 (FCRS = MY001) Novartis Corporation (Malaysia) Sdn. Bhd. (19710100054)
Functional Area
Technology Transformation

Job Type
Full time
Employment Type
Regulär
Shift Work
No
Apply to Job
Job ID
REQ-10039880

Associate Director of Forensics DDIT ISC

Apply to Job

Source URL: *https://prod1.adacap.com/careers/career-search/job/details/req-10039880-associate-director-forensics-ddit-isc-de-de*

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/de-DE/Novartis_Careers/job/Selangor/Associate-Director-of-Forensics-DDIT-ISC_REQ-10039880-2
5. https://novartis.wd3.myworkdayjobs.com/de-DE/Novartis_Careers/job/Selangor/Associate-Director-of-Forensics-DDIT-ISC_REQ-10039880-2