# Specialist DDIT ISC Detection & Response

Job ID
REQ-10039818
Feb 24, 2025
Malaysia

## Summary

The Detection and Response Specialist will be an integral part of the Novartis Cyber Security Operations Center (CSOC). The Novartis CSOC is an advanced security team that has reinvented Security Operations. It is comprised of a global team passionate about defending Novartis against modern and sophisticated IT security threats and attacks. The Detection and Response Specialist will leverage a variety of tools and resources to detect, investigate, and mitigate threats impacting Novartis' networks, systems, users, and applications. This role will involve coordination and communication with technical and nontechnical teams, including security leadership and business stakeholders. This is an entry level position intended for a professional with minimal of experience that will challenge and grow their technical investigation and IT security skillsets

## About the Role

### MAJOR ACCOUNTABILITIES

In addition to accountabilities listed above in Job Purpose:

- Security Monitoring and Triage
  - Monitor in real time security controls and alerts originating from the Novartis IT ecosystem
  - Communicate with technical and non-technical end users who report suspicious activity
- Forensics and Incident Response
  - Conduct initial investigations into suspicious events and activity
  - Gather live evidence and logs from a variety of devices and applications
  - Support incident response activities including scoping, communication, reporting, and long term remediation planning
  - Prepare technical reports for business stakeholders and IT leadership
  - Support response to major incidents as part of larger major incident response team
- Big Data analysis and reporting:
  - Utilizing SIEM/Big data to identify abnormal activity and extract meaningful insights.
  - Research, develop, and enhance content within SIEM and other tools
- Technologies and Automation:
  - Interface with engineering teams to propose new automation and orchestration concepts
  - Research and test new technologies and platforms; develop recommendations and improvement plans
- Day to day:
  - Perform host based analysis, artifact analysis, network analysis, and malware analysis in support of security investigations and incident response

- Coordinate investigation, containment, and other response activities with business stakeholders and groups
- Develop and maintain effective documentation; including response playbooks, processes, and other supporting operational material
- Provide mentoring of junior staff and serve as point of escalation for higher severity incidents
- Develop incident analysis and findings reports for management, including gap identification and recommendations for improvement
- Recommend or develop new detection logic and tune existing sensors / security controls
- Work with security solutions owners to assess existing security solutions array ability to detect / mitigate the abovementioned TTPs
- Creating custom SIEM queries and dashboards to support the monitoring and detection of advanced TTPs against Novartis network
- Participate in weekend/after hour on-call rotation to triage and/or respond to major incidents

**EDUCATION**

- University working and thinking level, degree in business/technical/scientific area or comparable education/experience
- 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**

- 3+ years experience in cybersecurity / security operations
- Experience in Information Technology / Analytical role preferred
- Experience in IT administration with technical, analytical and conceptual skills
- Experience in reporting to and communicating technical and non-technical business stakeholders
- 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

**SKILLS/JOB RELATED KNOWLEDGE**

- Good mediation and facilitation skills
- Good knowledge of IT Security Project Management
- Understanding and knowledge of general IT infrastructure technology and systems
- 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
- Knowledge of security frameworks such as Hitrust
- Host and network based forensic collection and analysis
- Dynamic malware analysis, reverse engineering, and/or scripting abilities
- Familiarity with Encase, Responder, X-Ways, Volatility, FTK, Axiom, Splunk, Wireshark, and other forensic tools
- Understanding of Advanced Persistent Threat (APT) and associated tactics.
- 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.
- Effective oral and written communication skills

**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:** 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
Universal Hierarchy Node
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
Regular
Shift Work
No
Apply to Job
Job ID
REQ-10039818

## Specialist DDIT ISC Detection & Response

Apply to Job

---

**Source URL:** *https://prod1.novartis.com/uk-en/careers/career-search/job/details/req-10039818-specialist-ddit-isc-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/careers/benefits-rewards
4. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Selangor/Specialist-DDIT-ISC-Detection---Response_REQ-10039818-1
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Selangor/Specialist-DDIT-ISC-Detection---Response_REQ-10039818-1