

# Senior Specialist DDIT ISC Detection & Response

Job ID

REQ-10023406

Sep 24, 2024

República Checa

## Resumen

The Detection and Response Analyst will be an integral part of the Novartis Cyber Security Operations Center (CSOC). The CSOC is an advanced global Location: Prague, Czech Republic; Barcelona, Spain

The Detection and Response Analyst 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 modern and sophisticated IT security threats and attacks. The Detection and Response Analyst 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 to challenge and grow technical investigation and IT security skillsets

## About the Role

### Your key responsibilities:

- Security Monitoring and Triage: Monitor in real time security controls and consoles from across the Novartis IT ecosystem, and communicate with technical and non-technical end users who report suspicious activity
- Forensics and Incident Response: Conduct initial investigations into security incidents involving a variety of threats; Gather live evidence from endpoint devices and log sources from a variety of systems and applications; Support incident response activities including scoping, communication, reporting, and long term remediation planning; Prepare technical reports for business stakeholders and IT leadership
- Big Data analysis and reporting: Utilizing SIEM/Big data to identify abnormal activity and extract meaningful insights, and research, develop, and enhance content within SIEM and other tools
- Technologies and Automation: Interface with engineering teams to design, test, and implement playbooks, orchestration workflows and automations; research and test new technologies and platforms; develop recommendations and improvement plans
- Day to day: Perform host based analysis, artifact analysis, network packet 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
- Perform quality assurance review of analyst investigations and work product; develop feedback and development reports
- Develop incident analysis and findings reports for management, including gap identification and recommendations for improvement
- 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

### **What you'll bring to the role:**

- University working and thinking level, degree in business/technical/scientific area or comparable education/experience
- 2+ years of experience in Information Technology / Analytical role preferred
- Experience in IT administration with technical, analytical and conceptual skills
- Understanding and knowledge of general IT infrastructure technology and systems
- Good knowledge of IT Security Project Management
- Experience with security incident monitoring and response related to medical 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; 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
  
- Experience in reporting to and communicating technical and non-technical business stakeholders
- Excellent written and verbal communication and presentation skills; Good mediation and facilitation skills; interpersonal and collaborative skills; and the ability to communicate information risk-related and incident response concepts to technical as well as nontechnical audiences
- 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

### **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

### **You'll receive (Prague only):**

Monthly pension contribution matching your individual contribution up to 3% of your gross monthly base salary; Risk Life Insurance (full cost covered by Novartis); 5-week holiday per year; (1 week above the Labour Law requirement) ; 4 paid sick days within one calendar year in case of absence due to sickness without a medical sickness report; Cafeteria employee benefit program – choice of benefits from Benefit Plus Cafeteria in the amount of 12,500 CZK per year; Meal vouchers in amount of 90 CZK for each working day (full tax covered by company); car allowance; MultiSport Card. Find out more about Novartis Business Services:

<https://www.novartis.cz/>

### **Why consider 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>Imagine what you could do here at Novartis!

### **Imagine what you could do here at Novartis!**

**Join our Novartis Network:** If this role is not suitable to your experience or career goals but you wish to stay connected to learn more about Novartis and our career opportunities, join the Novartis Network here:

<https://talentnetwork.novartis.com/network>

### **Accessibility and accommodation:**

Novartis is committed to working with and providing reasonable accommodation to all individuals. If, because of a medical condition or disability, you need a reasonable accommodation for any part of the recruitment process, or in order to receive more detailed information about the essential functions of a position, please send an e-mail to <di.cz@novartis.com> and let us know the nature of your request and your contact information. Please include the job requisition number in your message.

**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>

División

Operations

Business Unit

CTS

Ubicación

República Checa

Sitio

Prague

Company / Legal Entity

CZ02 (FCRS = CZ002) Novartis s.r.o

Alternative Location 1

Barcelona Gran Vía, España

Functional Area

Technology Transformation

Job Type

Full time

Employment Type

Regular

Shift Work

No

[Apply to Job](#)

Job ID

REQ-10023406

## Senior Specialist DDIT ISC Detection & Response

[Apply to Job](#)

---

**Source URL:** <https://www.adacap.com/careers/career-search/job/details/req-10023406-senior-specialist-ddit-isc-detection-response>

### List of links present in page

1. <https://www.novartis.cz/>
2. <https://talentnetwork.novartis.com/network>
3. <https://www.novartis.com/about/strategy/people-and-culture>
4. <https://talentnetwork.novartis.com/network>
5. <https://www.novartis.com/careers/benefits-rewards>
6. [https://novartis.wd3.myworkdayjobs.com/en-US/Novartis\\_Careers/job/Prague/Senior-Specialist-DDIT-ISC-Detection---Response\\_REQ-10023406](https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Prague/Senior-Specialist-DDIT-ISC-Detection---Response_REQ-10023406)
7. [https://novartis.wd3.myworkdayjobs.com/en-US/Novartis\\_Careers/job/Prague/Senior-Specialist-DDIT-ISC-Detection---Response\\_REQ-10023406](https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Prague/Senior-Specialist-DDIT-ISC-Detection---Response_REQ-10023406)