Associate Director, Threat Hunting and Response

Job ID
REQ-10044438

3月 26, 2025

Czech Republic

摘要

Location: Prague, Czech Republic; Barcelona, Spain

The Associate Director Threat Hunting and Response 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 Threat Hunting and Responsewill is a principal engineer who will leverage a variety of tools and resources to proactively detect, investigate, and mitigate emerging and persistent 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. As an experienced skilled engineer, this role will also involve coaching and mentoring of more junior members of the CSOC.

About the Role

Please note, this role will require to participate in weekend/after hour on-call rotation to triage and/or respond to major incidents. Also, some travel may be required.

Your key responsibilities:

- Forensics and Incident response
  - Serve as escalation point for conducting investigations into security incidents involving advanced and sophisticated threat actors and TTPs
  - Perform forensic collection and analysis of electronic assets and devices, scripts and malicious software, and log sources from a variety of systems and applications
  - Manage incident response activities including scoping, communication, reporting, and long term remediation planning

- Threat Hunting:
  - Review incident and intelligence reports from a variety of internal and external sources and team, and respond to major incidents as part of larger major incident response team
  - Develop hypotheses, analyze techniques, and execute hunts to identify threats across the environment
  - Interface with security teams and business stakeholders to implement countermeasures and improve defenses

- 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 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
  - 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

What you ' ll bring to the role:

- University working and thinking level, degree in business/technical/scientific area or comparable education/experience
- 8+ years of experience in Incident Response / Computer Forensics / CSOC team / Threat Hunting or related fields
- Experience with security incident monitoring and response related to medical devices
- experience in host and network based forensic collection and analysis
- Dynamic malware analysis, reverse engineering, and/or scripting abilities
- Proficient with Encase, Responder, X-Ways, Volatility, FTK, Axiom, Splunk, Wireshark, and other forensic tools
- Understanding of Advanced Persistent Threat (APT) and associated tactics.
- 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, and knowledge of security frameworks such as Hitrust
- Experienced IT administration with broad and in-depth technical, analytical and conceptual skills, and excellent understanding and knowledge of general IT infrastructure technology and systems
- Good knowledge of IT Security Project Management, and proven experience to initiate and manage projects that will affect CSOC services and technologies
- Good understanding and knowledge of business processes in a global pharmaceutical industry
- 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
- 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.

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-cultureImagine 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

部门
Operations

Business Unit
CTS

地点
Czech Republic

站点
Prague

Company / Legal Entity
CZ02 (FCRS = CZ002) Novartis s.r.o

Alternative Location 1
Barcelona Gran V í a, Spain

Functional Area
Technology Transformation

Job Type
Full time

Employment Type
Regular

Shift Work
No

Apply to Job

Job ID
REQ-10044438

Associate Director, Threat Hunting and Response

Apply to Job

Source URL:
https://www.novartis.com.cn/careers/career-search/job/details/req-10044438-associate-director-threat-hunting-and-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/NovartisCareers/job/Prague/Associate-Director--Threat-Hunting-and-ResponseREQ-10044438
7. https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/Prague/Associate-Director--Threat-Hunting-and-ResponseREQ-10044438