Director, SOC Engineering SOAR

Job ID
REQ-10058511

7月 28, 2025

Czech Republic

摘要

Location: Prague, Czech Republic; Barcelona, Spain; #LI-Hybrid (12 days/month in office)

Internal job title: Director, DDIT ISC CSOC Engineering

The role is based in Prague/Barcelona. Novartis is unable to offer relocation support for this role: please only apply if this location is accessible for you.

About the Role:

The Director, SOC Engineering SOAR will be an integral part of the Novartis Cyber Security Operations Center (CSOC). The CSOC is an advanced global team passionate about actively defending against the most sophisticated cyber threats and attacks. The Director, SOC Engineering SOAR is a seasoned leader who will lead a team of skilled SOAR engineers and manage tools to support the proactive detection, investigation, and mitigation of emerging and persistent threats that impact Novartis’ networks, systems, users, and applications. This role will involve coordination and communication with technical and non-technical teams, including security leadership and business stakeholders. As an experienced and skilled manager, this role will also involve coaching and

mentoring talented Security Engineers with diverse backgrounds.

As the role is part of a global organization, some travel and flexible work hours may be required.

About the Role

Key Responsibilities:

- SOAR Manager
  - Lead and manage a geographically distributed team of skilled SOAR Engineers, providing guidance and support while leveraging their diverse skill sets and personalities, as well as evaluating and reviewing performance metrics and KPIs to ensure the SOAR team is meeting targets and delivering efficient and effective results.
  - Serve as a subject matter expert in SOAR processes and play an active role in guiding the team and providing expertise whenever needed.
  - Take accountability for the team's performance in various areas, including, but not limited to: Manage SOAR platforms; Support audit requests and reports; Engage with product teams to address technical challenges; Manage stakeholders' commitments
  - Act as the primary point of contact for first-level escalations, addressing any issues or concerns that arise and ensuring timely resolution.
- Workflow Orchestration and Process Automation
  - Define, design, evaluate, and improve business processes and playbooks integrating automation and orchestration; and develop and maintain effective documentation; including automation playbooks, processes, and other supporting operational material.
  - Develop custom integrations to support CSOC workflow automation and orchestration and integrate a variety of technology devices, applications, and datasets to support workflow orchestration and process automations.
  - Gather requirements, plan, design, implement, and test automations with SOAR platform and surrounding technologies.
- Case Management and Analytics
  - Interface with engineering teams to design, test, and implement case management with workflow orchestration and automation.
  - Define, design, evaluate, and enhance case management features including front end interface, backend data model, and technology integrations to support measurable, effective, and streamlined CSOC activities.
- Scripting and Development
  - Design, develop, and test scripts and other solutions to support CSOC mission and activities.
  - Research and test new technologies and platforms; develop recommendations and improvement plans.
- Cooperating with stakeholders
  - Periodically report to management the current status of sources and use cases in the system; and collaborate with operational stakeholders (CSOC analysts, Cyber Center), maintaining a good understanding of stakeholders ’ needs in regard to activities and requirements.

Essential Requirements:

- University working and thinking level, degree in business/technical/scientific area or comparable education/experience.
- 12+ years work experience in security, with 4+ years Python scripting or other similar coding experience.
- Experience planning, designing, developing, and testing automation solutions with SOAR platforms (Cortex, Phantom, FortiSOAR, etc), with good understanding of SOAR architecture components, including technology integrations, common automation scenarios and solutions.
- Experience developing solutions with SIEM tools (Splunk, QRadar, Sentinel, etc.).
- Experience with platform and application automated deployment and version control software e.g. (Ansible, Git, Bitbucket).
- Experienced IT administration with broad and in-depth technical, analytical and conceptual skills.
- Understanding of network protocols and topologies, as well as of error messages and logs displayed by various software and experience with software development lifecycle and user acceptance testing.
- 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, with good 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, and proven experience to initiate and manage projects that will affect CSOC services and technologies
- Prior people management experience leading a global teams

Desirable requirements

- Professional information security certification, such as CISSP, CISM or ISO 27001 auditor / practitioner.
- Professional (information system) risk or audit certification such as CIA, CISA or CRISC.
- Preferably one or more XSOAR, Phantom trainings/certifications.
- Knowledge of the MITRE ATT&CK framework is a beneficial.

Commitment to Diversity & Inclusion:

We are committed to building an outstanding, inclusive work environment and diverse teams representative of the patients and communities we serve.

You ' ll receive (CZ 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 105 CZK for each working day (full tax covered by company); MultiSport Card. Find out more about Novartis Business Services: https://www.novartis.cz/

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

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 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-10058511

Director, SOC Engineering SOAR

Apply to Job

Source URL:
https://www.novartis.com.cn/careers/career-search/job/details/req-10058511-director-soc-engineering-soar

List of links present in page

1. https://www.novartis.com/about/strategy/people-and-culture
2. https://www.novartis.com/about/strategy/people-and-culture
3. https://talentnetwork.novartis.com/network
4. https://www.novartis.com/careers/benefits-rewards
5. https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/Prague/Director--SOC-Engineering-SOARREQ-10058511-1
6. https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/Prague/Director--SOC-Engineering-SOARREQ-10058511-1