NOVARTIS

Sr. Specialist SOC Engineering (Sentinel, Cribl, SIEM)

Job ID
REQ-10054479

6月 19, 2025

Czech Republic

摘要

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

Internal job title: Sr. Specialist DDIT ISC CSOC Engineering

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

About the Role:
This role 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. By leveraging various tools and resources, the CSOC Engineer will help to proactively detect, investigate, and mitigate both emerging and persistent threats that pose a risk to Novartis' networks, systems, users, and applications.
The Sr. Specialist SOC Engineering (Sentinel, Cribl, SIEM) will be responsible to design, develop, implement, and manage dataflow pipelines and integrate them with SIEM platforms such as Sentinel, playing a pivotal in ensuring the proactive defence of Novartis' critical assets, systems, and infrastructure against the ever-evolving landscape of cyber threats.

About the Role

Please note, this role will require flexibility to provide on-call support on a rotational basis, including weekends, to ensure system stability and incident response readiness.

Key Responsibilities:

Data Onboarding

- Evaluate and onboard new data sources, performing data analysis for identifying anomalies and trends, and developing dashboards and visualizations for data reporting; troubleshoot and provide support for onboarding issues with platforms like Sentinel, and Cribl.
- Collaborate with CSOC engineers, Threat Hunters, and CSOC Analysts to gather requirements and develop solutions, working with cross-functional teams to understand risks and develop effective detection strategies that align with organizational security goals.
- Validate and ensure proper configuration and implementation of new logics with security system and application owners; perform data normalization, establish datasets, and develop data models; Manage backlog of customer requests for onboarding new data sources.
- Detect and resolve issues in various data sources, implementing health monitoring for data sources and feeds.
- Provide 24x7 on-call support on a rotational basis, including weekends, to ensure system stability and incident response readiness.

Content Development and Automation

- Design and create security detection rules, alerts, and Use Cases utilizing platforms such as SIEM, DLP, EDR, and WAF.
- Develop robust detection mechanisms to identify and respond to potential security threats across various security technologies.
- Regularly review and enhance existing detection rules and Use Cases to ensure their effectiveness and alignment with emerging threats and vulnerabilities.
- Automation CSOC Engineering workload

Essential Requirements:

- University working and thinking level, degree in business/technical/scientific area or comparable education/experience.
- 3-5 years experience in the field, with good general security knowledge.
- Strong expertise in Sentinel and Direct experience managing Data ingestion pipeline through Cribl.
- Hands on experience and knowledge of security tools (DLP, XDR, SIEM, Firewalls) and experience in Security Engineering tasks such as SIEM alert creation, SOAR playbook development

- Experience in IT administration with broad and in-depth technical, analytical and conceptual skills, and exceptional understanding and knowledge of general IT infrastructure technology and systems.
- Experience in configuring Data collection Endpoints, connectors and parsers.
- Good knowledge of collectors/forwarder components, integrating Security tools using API, syslog, cloud etc.
- Experience in scripting and Automation for Security tools, with development experience in Python (SDKs)
- Excellent communication and collaborative skills cross functionally and in global teams, with good 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.

Desirable requirements

- Advanced training/certification on Security tools like Sentinel, XDR, DLP
- SANS certifications (for security analyst/SIEM)
- Cloud Security Engineering certification (Azure/AWS)
- Knowledge of the MITRE ATT&CK framework is 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-10054479

Sr. Specialist SOC Engineering (Sentinel, Cribl, SIEM)

Apply to Job

Source URL:
https://www.novartis.com.cn/careers/career-search/job/details/req-10054479-sr-specialist-soc-engineering-sentinel-cribl-siem

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/Sr-Specialist-SOC-Engineering--Sentinel--Cribl--SIEM-REQ-10054479-1
6. https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/Prague/Sr-Specialist-SOC-Engineering--Sentinel--Cribl--SIEM-REQ-10054479-1