

Sr. Specialist CSOC/SIEM/DLP Engineer

Job ID

REQ-10023688

nov 14, 2024

République tchèque

Résumé

Location: Prague, Czech Republic; Barcelona, Spain

CSOC Engineering 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 main objective of the CSOC Engineering is to design, develop, implement, and manage dataflow pipelines and integrate them with SIEM platforms such as Sentinel and Splunk. The Data onboarded to SIEM will be Crucial for CSOC Analysts and the content development and SOAR Engineers to develop monitoring alerts and automation playbooks.

Collaboration with internal and external stakeholders, including Novartis' internal teams, external vendors, and Product/Platform engineers, will be a crucial aspect of this role. The CSOC Engineer will work closely with Application owners to understand and integrate various datasources. This may involve utilizing services such as Cribl, Syslog NG, Azure Monitoring Agent, Universal Forwarder etc. to list a few.

Furthermore, the CSOC Engineer will work in close partnership with the CSOC stakeholders, including TDR, THR, Forensic, Content Development, and SOAR teams. Their expertise and collaboration will be instrumental in quickly resolving any Data onboarding requests or issues that arise.

Overall, the CSOC Engineering role is pivotal in ensuring the proactive defense of Novartis' critical assets, systems, and infrastructure against the ever-evolving landscape of cyber threats.

About the Role

Your key responsibilities:

- Evaluate and onboard new data sources, performing data analysis for identifying anomalies and trends, and developing dashboards and visualizations for data reporting.
- Collaborate with CSOC engineers, Threat Hunters, and CSOC Analysts to gather requirements and develop solutions.
- Troubleshoot and provide support for onboarding issues with platforms like Sentinel, Splunk, and Cribl.
- 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.

- Identify opportunities for automation in data onboarding and proactively detect parsing/missing-data issues.

What you'll bring to the role:

- University working and thinking level, degree in business/technical/scientific area or comparable education/experience
- 4+ Years work experience.
- Understanding of Splunk, Sentinel and Cribl architecture.
- Good general security knowledge, with security tools knowledge and understanding of security systems (such as AV, IPS, Proxy, FWs etc.).
- Understanding of CSOC use-case designing
- Understanding of Scripting and Development
- Understanding of network protocols and topologies.
- Strong technical troubleshooting and analytical skill and an understanding of error messages and logs displayed by various software.
- Strong communication skills.
- Experienced IT administration with broad and in-depth technical, analytical and conceptual skills.
- 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.
- Excellent understanding and knowledge of general IT infrastructure technology and systems.

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
- Preferably one or more Splunk certification.
- A knowledge of the MITRE ATT&CK framework is a beneficial .

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); public transportation 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>

Division

Operations

Business Unit

CTS

Emplacement

République tchèque

Site

Prague

Company / Legal Entity

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

Alternative Location 1

Barcelona Gran Vía, Espagne

Functional Area

Technology Transformation

Job Type

Full time

Employment Type

Regular

Shift Work

No

[Apply to Job](#)

Job ID

REQ-10023688

Sr. Specialist CSOC/SIEM/DLP Engineer

[Apply to Job](#)

Source URL: <https://prod1.adacap.com/careers/career-search/job/details/req-10023688-sr-specialist-csocsiemdlp-engineer>

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/Sr-Specialist-DDIT-ISC-CSOC-Engineering_REQ-10023688-1
7. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Prague/Sr-Specialist-DDIT-ISC-CSOC-Engineering_REQ-10023688-1