NOVARTIS

Sr. Specialist DDIT ISC CSOC Engineer

Job ID
REQ-10039796
Μαρ 28, 2025
Malaysia

Περίληψη

The Senior Specialist CSOC Engineer 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 security use cases and configure them with SIEM platforms such as Sentinel and Splunk. The use cases implemented on SIEM will be Crucial for CSOC Analysts to monitor/investigate and SOAR Engineers to develop 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 various alerting requirements. This may involve utilizing services such as Sentinel, MS DLP, MS Defender, Cortex XDR to list a few.
Furthermore, the CSOC Engineering Lead will work in close partnership with the CSOC stakeholders, including TDR, THR, Forensic, Data Onboarding, and SOAR teams. Their expertise and collaboration will be instrumental in quickly resolving any alerting issues with the detection rule on security tool such as SIEM, DLP, EDR.
Overall, the CSOC Engineering role is pivotal in ensuring the proactive defence of Novartis' critical assets, systems, and infrastructure against the ever-evolving landscape of cyber threats.

About the Role

MAJOR ACCOUNTABILITIES

In addition to accountabilities listed above in Job Purpose:

- 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.
  - Collaborate with cross-functional teams to understand risks and develop effective detection strategies that align with organizational security goals.
  - 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.

PERSONAL CONSIDERATIONS

- As the role is part of a global organization, willingness for required traveling and flexible work hours is important
- Provide 24x7 on-call support on a rotational basis, including weekends, to ensure system stability and incident response readiness

EDUCATION

- **Essential:**
  - University working and thinking level, degree in business/technical/scientific area or comparable education/experience.
- **Desirable:**
  - Advanced training/certification on Security tools like Splunk, Sentinel, XDR, DLP
  - SANS certifications (for security analyst/SIEM)
  - Cloud Security Engineering certification (Azure/AWS)

EXPERIENCE

- 4+ Years work experience.
- Effective communication skills.
- Good general security knowledge.
- Strong knowledge of security tools (DLP, XDR, SIEM, Firewalls).
- Experience in Security Engineering tasks such as SIEM alert creation, SOAR playbook development
- 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.
- Exceptional interpersonal and collaborative skills, fostering effective communication and cooperation with diverse individuals and teams.
- Exceptional understanding and knowledge of general IT infrastructure technology and systems.

PRODUCT/MARKET/CUSTOMER KNOWLEDGE

- Good understanding of pharmaceutical industry. Good understanding and knowledge of business processes in a global pharmaceutical industry.

SKILLS/JOB RELATED KNOWLEDGE

- Firsthand experience of Security tools like Splunk, Sentinel, DLP, XDR.
- Understanding of security systems (such as AV, IPS, Proxy, FWs).
- *Security use-case design and development*
- *Understanding of SOAR*
- Development experience in python (SDKs)
- A knowledge of the MITRE ATT&CK framework is beneficial.
- Excellent written and spoken English.
- Calm and logical approach.

OTHER

Fluency (written and spoken) in English

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

Τομέας
Operations
Business Unit
Universal Hierarchy Node
Τοποθεσία
Malaysia
Τοποθεσία
Selangor
Company / Legal Entity
MY01 (FCRS = MY001) Novartis Corporation (Malaysia) Sdn. Bhd. (19710100054)
Functional Area
Technology Transformation
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job
Job ID
REQ-10039796

Sr. Specialist DDIT ISC CSOC Engineer

Apply to Job

Source URL: *https://prod1.novartis.com/gr-el/careers/career-search/job/details/req-10039796-sr-specialist-ddit-isc-csoc-engineer*

List of links present in page

1. https://www.novartis.com/about/strategy/people-and-culture
2. https://talentnetwork.novartis.com/network
3. https://www.novartis.com/careers/benefits-rewards
4. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Selangor/Sr-Specialist-DDIT-ISC-CSOC-Engineering_REQ-10039796-1
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Selangor/Sr-Specialist-DDIT-ISC-CSOC-Engineering_REQ-10039796-1