Sr. Specialist DDIT ISC CSOC Engineering

Job ID
REQ-10023687
Sep 26, 2024
Mexico

Summary

JOB PURPOSE

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

MAJOR ACCOUNTABILITIES

In addition to accountabilities listed above in Job Purpose:

- Data Onboarding
  - 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.

PERSONAL CONSIDERATIONS

As the role is part of a global organization, willingness for required traveling and flexible work hours is important.

Mandatory Requirements:

- 4+ Years work experience, Good general security knowledge with hands on experience and certifications in Splunk, SIEM, SANS Sentinel
- Hands-on experience managing Data ingestion pipeline through Cribl
- Understanding of security systems (such as AV, IPS, Proxy, FWs etc.).
- An understanding of error messages and logs displayed by various software.
- Understanding of network protocols and topologies.
- Excellent communications skills with written and spoken English Fluency

Desirable Requirements:

- *Security use-case design and development*
- *Understanding of SOAR*

CORE COMPETENCIES

Leadership

Customer/Quality Focus

Fast, Action-Oriented

Results Driven

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
Location
Mexico
Site
INSURGENTES
Company / Legal Entity
MX06 (FCRS = MX006) Novartis Farmacéutica S.A. de C.V.
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job
Job ID
REQ-10023687

Sr. Specialist DDIT ISC CSOC Engineering

Apply to Job

Source URL: *https://prod1.id.novartis.com/careers/career-search/job/details/req-10023687-sr-specialist-ddit-isc-csoc-engineering*

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/INSURGENTES/Sr-Specialist-DDIT-ISC-CSOC-Engineering_REQ-10023687-1
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/INSURGENTES/Sr-Specialist-DDIT-ISC-CSOC-Engineering_REQ-10023687-1