NOVARTIS

Specialist DDIT ISC CSOC Engineering

Job ID
REQ-10028173
Jan 17, 2025
Mexico

Summary

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 defence 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 to list a few.
Furthermore, the CSOC Engineering Lead 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 resolve any issues with the detection rule on security tool such as SIEM, DLP, EDR.
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.

- 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.

KEY PERFORMANCE INDICATORS / MEASURES OF SUCCESS

- Improving Data Onboarding processes.
- Evaluate and review the Data quality in SIEM.
- Timely delivery of defect free onboarding services for CSOC.
- Identify technology and process gaps that affect CSOC services; propose solutions and make recommendations for continuous improvement.

PERSONAL CONSIDERATIONS

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

EDUCATION / EXPERIENCE

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

- 2+ Years work experience.
- Effective communication skills.
- Good general security knowledge.
- Strong knowledge of security tools (DLP, XDR, SIEM, Firewalls).
- Experienced IT administration with broad and in-depth technical, analytical and conceptual skills.
- 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.
- 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.
- Direct experience managing Data ingestion pipeline through Cribl.
- Understanding of security systems (such as AV, IPS, Proxy, FWs).
- *Security use-case design and development*
- *Understanding of SOAR*
- Development experience in python (SDKs)
- An understanding of error messages and logs displayed by various software.
- Understanding of network protocols and topologies.
- Strong technical troubleshooting and analytical skills.
- A knowledge of the MITRE ATT&CK framework is beneficial.
- Excellent written and spoken English.
- Calm and logical approach.

NETWORKS

- High level of personal integrity, and the ability to professionally handle confidential matters and exude the appropriate level of judgment and maturity.
- Ability to manage competing priorities, and seeking consensus when stakeholders have different or even contradicting opinions.

OTHER

- Fluency (written and spoken) in English

CORE COMPETENCIES

Leadership

Establishes clear direction and sets stretch objectives. Aligns and energizes Associates behind common objectives. Champions the Novartis Values and Behaviors. Rewards/encourages the right behaviors and corrects others.

- Establishes clear directives and objectives.
- Communicates positive expectations for others on the team.
- Integrates and applies learning to achieve business goals.

Customer/Quality Focus

Assigns highest priority to customer satisfaction. Listens to customer and creates solutions for unmet customer needs. Established effective relationships with customers and gains their trust and respect.

- Defines quality standards to ensure customer satisfaction.
- Creates and supports world-class quality standards to ensure customer satisfaction.

Fast, Action-Oriented

Is action-oriented and full of energy to face challenging situations. Is decisive, seizes opportunities and ensures fast implementation. Strives for simplicity and clarity. Avoids 'bureaucracy'.

- Alerts others to potential risks and opportunities.
- Keeps organizational processes simple and efficient.
- Takes acceptable/calculated risks by adopting new or unknown directions.

Results Driven

Can be relied upon to succeed targets successfully. Does better than the competition. Pushes self and others for results.

- Anticipates potential barriers to achievement of shared goals.
- Pushes self and others to see new ways of achieving results (e.g., better business model).
- Uses feasibility and ROI analyses to ensure results.
- Keeps pace with new developments in the industry.

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.
Functional Area
Technology Transformation
Job Type

Full time
Employment Type
Regular
Shift Work
No
Apply to Job
Job ID
REQ-10028173

Specialist DDIT ISC CSOC Engineering

Apply to Job

Source URL: *https://uat2.novartis.de/careers/career-search/job/details/req-10028173-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/Specialist-DDIT-ISC-CSOC-Engineering_REQ-10028173
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/INSURGENTES/Specialist-DDIT-ISC-CSOC-Engineering_REQ-10028173