Associate Director DDIT ISC CSOC Engineering

Job ID
REQ-10022260
Sep 30, 2024
Indien

Zusammenfassung

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 Lead 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 Lead 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 Engineering Lead will work closely with these stakeholders 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 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 issues that arise.
Overall, the CSOC Engineering Lead 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:

- **Onboarding Lead**
  - Lead and manage a geographically distributed team of Skilled Engineers, providing guidance and support while leveraging their diverse skillsets and personalities.
  - Evaluate and review performance metrics and KPIs to ensure the Onboarding team is meeting targets and delivering efficient and effective results.
  - Take accountability for the team's performance in various areas, including but not limited to data onboarding to:
    - SIEM platforms such as Sentinel and Splunk

        - Supporting audit requests and reports
        - Engaging with product teams to address technical challenges
        - Managing stakeholders' commitments
    - Act as the primary point of contact for first-level escalations, addressing any issues or concerns that arise and ensuring timely resolution.
    - Develop and maintain comprehensive documentation to facilitate knowledge sharing and ensure quality outcomes are consistently achieved.
    - Drive a culture of continuous improvement and innovation within the team, identifying opportunities to optimize processes and enhance efficiency.
    - Serve as a subject matter expert in onboarding processes and play an active role in guiding the team and providing expertise whenever needed.

- Data Onboarding and Technical Management
    - 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.

KEY PERFORMANCE INDICATORS / MEASURES OF SUCCESS

- Maintaining and Improving Data Onboarding team perforemence according set KPIs.
- Evaluate and review Team performance.
- Identify technology and process gaps that affect CSOC services; propose solutions and make recommendations for continuous improvement.

JOB DIMENSIONS (Job Scope)

Number of associates:

~20 Associates

Financial responsibility

1-3 millions USD

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:**
  - 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.

EXPERIENCE

- 8+ Years work experience..
- Strong managing skills.
- Good general security knowledge.
- Strong knowladge ot security tools.
- 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.
- Proven experience to initiate and manage projects that will affect CSOC services and technologies.

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

- Understanding of Splunk, Sentinel and Cribl architecture.
- Understanding of security systems (such as AV, IPS, Proxy, FWs etc.).
- Understanding of CSOC use-case designing
- Understanding of Scripting and Development
- 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 a beneficial .
- Ability to prioritise workload.
- 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 handle 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? 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

You'll receive: You can find everything you need to know about our benefits and

rewards in the Novartis Life Handbook. https://www.novartis.com/careers/benefits-rewards

Commitment to Diversity and Inclusion: Novartis is committed to building an outstanding, inclusive work environment and diverse teams' representative of the patients and communities we serve.

Join our Novartis Network: If this role is not suitable to your experience or career goals but you wish to stay connected to hear more about Novartis and our career opportunities, join the Novartis Network here: https://talentnetwork.novartis.com/network

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

Abteilung
Operations
Business Unit
CTS
Ort
Indien
Website
Hyderabad (Office)
Company / Legal Entity
IN10 (FCRS = IN010) Novartis Healthcare Private Limited
Functional Area
Technology Transformation
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job
Job ID
REQ-10022260

Associate Director DDIT ISC CSOC Engineering

Apply to Job

Source URL: *https://prod1.adacap.com/careers/career-search/job/details/req-10022260-associate-director-ddit-isc-csoc-engineering*

List of links present in page

1. https://www.novartis.com/about/strategy/people-and-culture
2. https://www.novartis.com/careers/benefits-rewards
3. https://talentnetwork.novartis.com/network
4. https://www.novartis.com/about/strategy/people-and-culture
5. https://talentnetwork.novartis.com/network
6. https://www.novartis.com/careers/benefits-rewards
7. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Associate-Director-DDIT-ISC--CSOC-Onboarding_REQ-10022260
8. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Associate-Director-DDIT-ISC--CSOC-Onboarding_REQ-10022260