Dir. DDIT ISC CSOC Engineering

Job ID
REQ-10058510

7月 27, 2025

India

摘要

The Director DDIT ISC CSOC Automation Engineering will be an integral part of the Novartis Cyber Security Operations Center (CSOC). The CSOC is an advanced global team passionate about actively defending against the most sophisticated cyber threats and attacks. The Director DDIT ISC CSOC Automation Engineering is a seasoned leader who will lead a team of skilled SOAR engineers and manage tools to support the proactive detection, investigation, and mitigation of emerging and persistent threats that impact Novartis’ networks, systems, users, and applications. This role will involve coordination and communication with technical and non-technical teams, including security leadership and business stakeholders. As an experienced and skilled manager, this role will also involve coaching and mentoring talented Security Engineers with diverse backgrounds.

About the Role

MAJOR ACCOUNTABILITIES

In addition to accountabilities listed above in Job Purpose:

- SOAR Manager
  - Lead and manage a geographically distributed team of skilled SOAR Engineers, providing guidance and support while leveraging their diverse skill sets and personalities.
  - Evaluate and review performance metrics and KPIs to ensure the SOAR 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:
    - Manage SOAR platforms
    - Support audit requests and reports
    - Engage with product teams to address technical challenges
    - Manage 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 consistently achieving quality outcomes.
  - 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 SOAR processes and play an active role in guiding the team and providing expertise whenever needed.
- Workflow Orchestration and Process Automation
  - Define, design, evaluate, and improve business processes and playbooks integrating automation and orchestration.
  - Integrate a variety of technology devices, applications, and datasets to support workflow orchestration and process automations.
  - Gather requirements, plan, design, implement, and test automations with SOAR platform and surrounding technologies.
  - Develop custom integrations to support CSOC workflow automation and orchestration.
  - Develop and maintain effective documentation; including automation playbooks, processes, and other supporting operational material.
- Case Management and Analytics
  - Interface with engineering teams to design, test, and implement case management with workflow orchestration and automation.
  - Define, design, evaluate, and enhance case management features including front end interface, backend data model, and technology integrations to support measurable, effective, and streamlined CSOC activities.
- Scripting and Development
  - Design, develop, and test scripts and other solutions to support CSOC mission and activities.
  - Research and test new technologies and platforms; develop recommendations and improvement plans.
- Cooperating with stakeholders
  - Management - Periodically report to management the current status of sources and use cases in the system.
  - Operational stakeholders (CSOC analysts, Cyber Center) - Maintain a good understanding of stakeholders ’ needs in regard to activities and requirements.

Essential Requirements:

- University working and thinking level, degree in business/technical/scientific area or comparable education/experience.

- **Desirable Requirements:**
    - 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 XSOAR, Phantom trainings/certifications.

EXPERIENCE

- 6+ Years work experience.
- 4+ Years Python scripting or other similar coding experience.
- Experience with Python and Splunk.
- Experience planning, designing, developing, and testing automation solutions with SOAR platforms (Cortex, Phantom, FortiSOAR, etc).
- Experience developing solutions with SIEM tools (Splunk, QRadar, Sentinel, etc.).
- 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.

SKILLS/JOB RELATED KNOWLEDGE

- Understanding of SOAR architecture components, including technology integrations, common automation scenarios and solutions.
- Understanding of configuration files and relationship between GUI configuration and backend configuration file impact.
- Experience with software development lifecycle and user acceptance testing.
- An understanding of error messages and logs displayed by various software.
- Ability to troubleshoot, diagnose and solve issues independently.
- Self-learner, ability to document learning as experience is gained.
- Understanding of network protocols and topologies.
- Strong technical troubleshooting and analytical skills.
- Experience with platform and application automated deployment and version control software e.g. (Ansible, Git, Bitbucket).
- 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.

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

部门
Operations

Business Unit
Universal Hierarchy Node

地点
India

站点
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-10058510

Dir. DDIT ISC CSOC Engineering

Apply to Job

Source URL:

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/Hyderabad-Office/Dir-DDIT-ISC-CSOC-Engineering_REQ-10058510-1
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Dir-DDIT-ISC-CSOC-Engineering_REQ-10058510-1