NOVARTIS

Assoc. Dir. DDIT ISC VulnSvcs role

Job ID
REQ-10018657
Aug 20, 2024
India

Summary

The role is part of DDIT ISC Security Operations in Vulnerability Services team. The person will focus on reducing risk exposure from security vulnerabilities through design, implementation and operations of VulnSvcs products that implement the VulnSvcs processes. Plays an active role in analyzing vulnerabilities for reduction and management.
Objective of this role is to implement VulnSvcs processes through technology engineering, operations and ensuring effective use for wide array of stakeholders and users. Actively engage and work with VM team to analyze vulnerabilities posture and reduction. Role requires experience with vulnerability management/remediation solutions setup, end user focused product mgmt. and operations through strong collaboration with cross functional teams. Acumen with vulnerabilities/configuration issues, remediation/mitigation analysis, risk assessment, influencing stakeholders for timely mgmt., and operating security service is key.
-Oversees security operations service line, technology governance and external/internal interfaces in accordance with service operations and management processes.

About the Role

Major accountabilities:

- As a lead, own the design, implementation, roadmap, and operational oversight for VulnSvcs products to centralize and or operate the related processes:
- Ownership of VulnSvcs business requirements, translating to technical solution requirements, working with cross functional teams to manage implementation.
- Proactively monitor and govern engineering and support operations of the VulnSvcs solutions such as ServiceNow (SecOps module, custom modules), exposure mgmt. independently and aligned external/internal individuals.
- Identify problem areas and drive identification of root causes as well as sufficient prevention of recurrences.
- Lead product vendor/CSM connects to address Novartis requirements/issues.
- Plan, influence and deliver VulnSvcs products roadmap and maturity.
- Stay up to date with latest product features, perform POCs, finalize implementation requirements, ensure planned production.
- Develop and maintain documentation of related process and best practices.
- Provide security awareness and training to teams on VulnSvcs solutions and Mgmt.
- Implement security policies, procedures, and standards to ensure the confidentiality, integrity, and availability of solutions from technical vulnerabilities.
- Identify potential improvement areas for vulnerability remediation and shared learned lessons with

application/development teams.
- Monitor and prioritize security vulnerabilities through risk analysis to understand potential impact and translate vulnerability severity as security risk.
- Flexibly support emergency response for 0-day vulnerability remediation.
- Collaborate with various stakeholders from security operations, architecture, cyber, platform and application teams to achieve goals.
- Defines remediation activities for security assessment gaps as they pertain to IT Security Management

Key performance indicators:

- Stable, compliant, secure, and cost-effective operations measured by Availability, Performance, Capacity, Security Metrics -Responsiveness and Recovery Speed of critical incidents/issues in business -Learning Agility, ability to evaluate and launch new services and capabilities -Productivity gains and defect reduction through continuous improvement -Automation led Security Operations Services -Integration of Applications and Infrastructure into Centralized Security Platforms
- Adequacy and maturity of VulnSvcs technology and processes.
- Technical expertise proven in identifying, reviewing, and improving risk posture.
- Ensure Application/project satisfied with the risk, security, and remediation advisory.
- Reducing the number of vulnerabilities by adapting remediation wherever possible
- Cross skill collaboration and feedback from the various stake holders

Minimum Requirements:
Work Experience:

- 10+ years of overall working experience in information security preferably in Vulnerability Management, Security Patching and Security Operations domain.
- At least 5+ years of relevant experience in security domain dealing majorly with vulnerability analysis, remediations, and assessments.
- Experience with centralizing threat vulnerability management process & technologies.
- Experience of sourcing complex IT services, product management and working closely with vendors for effective use of capabilities.
- Demonstrated leadership skills through experience in middle management and/or engagement with large security/development program stakeholders.
- Risk.
- Accountability.
- Strong cross functional leadership.
- Relationship Management.
- Strategy Development.
- Operations Management and Execution.
- Collaborating across boundaries.
- Project Management.
- Interactions with senior management.
- People Leadership.

Skills:

- SNOW SecOps and related vulnerability products integration.
- Strong knowledge of security vulnerabilities in software and infrastructure, OWASP, SAMM, security frameworks, application architecture principles, security risk analysis and relevant domain areas.
- Acumen in designing and guiding implementation of vulnerability management solution workflows,

integration design of vuln detection tools, hands-on testing and ideation of related product features, product security operations.
- Persuasive communication skills to effectively convey to both technical and non-technical stakeholders, and the ability to collaborate with cross-functional teams.
- Strong problem-solving skills and the ability to work independently.
- Strong understanding of metrics, KPI/KRI, SLAs, and dashboards for vulnerability management and providing executive reporting.
- Escalation.
- Information Security Audit.
- Information Security Risk Management.
- Quality Management.
- Root Cause Analysis (Rca).
- Sec Ops (Security Operations).
- Vendor Management.

Languages :

- 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

Division
Operations
Business Unit
CTS
Location
India
Site
Hyderabad (Office)
Company / Legal Entity
IN10 (FCRS = IN010) Novartis Healthcare Private Limited
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job
Job ID
REQ-10018657

Assoc. Dir. DDIT ISC VulnSvcs role

Apply to Job

Source URL: *https://prod1.adacap.com/careers/career-search/job/details/req-10018657-assoc-dir-ddit-isc-vulnsvcs-role*

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/Assoc-Dir-DDIT-ISC-VulnSvcs-role_REQ-10018657
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Assoc-Dir-DDIT-ISC-VulnSvcs-role_REQ-10018657