NOVARTIS

Assoc. Dir. DDIT ISC SecOps VulnSvcs

Job ID
REQ-10018655
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 with major focus on high risk, theme based and 0-day vulnerabilities emergency response and remediation. Flexibility with work schedule is critical.
Analyze ongoing security vulnerabilities risk posture, perform technical vulnerability/mitigations tests, collaborate with finding owners/support teams for managing resolutions, act as SME to assess discovered vulnerabilities and provide pragmatic solutions and flexibly support emergency vulnerability remediations. Collaboration with cross functional teams for threat intel, incident response, security architecture, remediation and security operations are 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:

- Act as a Technical Security SME and point of contact for responding to ongoing high-risk vulnerability exposure
- Continuously monitor and prioritize security vulnerabilities, missing controls, mitigations and defenses through risk analysis to understand potential impact and translate vulnerability severity as security risk.
- Identify problem areas, root causes and solution to prevent/reduce vulnerabilities.
- Support vulnerability assessments and penetration testing of infrastructure, applications, and services where needed to verify false positives or remediations.
- Ensure that vulnerability remediation plans are delivered to the agreed SLA, engage application managers and asset owners to carry out corrective actions.
- Identify potential improvement areas for vulnerability response and shared learned lessons with teams and stakeholders.
- Take accountability to ensure adherence with Security and Compliance policies and procedures.
- Stay up to date with the latest security threats and vulnerabilities, proactively recommending mitigation strategies.
- Develop and maintain documentation of related process and best practices.
- Implement security policies, procedures, and standards to ensure the confidentiality, integrity, and availability of cloud resources from technical vulnerabilities.
- Provide security awareness and training to teams on security practices and vulnerability related processes.
- Be flexible with work schedules (including support outside standard business days/hours) to coordinate emergency response for high-risk vulnerability remediation with relevant stakeholders. Drive identification

of root causes and prevention of recurrences.
- Collaborate with various stakeholders from security operations, architecture, cyber, SOC, and application teams to achieve technical risk reduction 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
- Flexibility to support vulnerability response remediation with sense of urgency.
- Technical expertise proven in identifying, reviewing, and improving vulnerabilities.
- 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:

- 8+ years of overall working experience in information security preferably in Application Security and Vulnerability management domain.
- At least 3+ years in handling security vulnerability response and remediation or SOC, coordinating with relevant stakeholders, and implementing corrective/preventive actions.
- Experience performing passive discovery and active testing of network or application vulnerabilities for validating external threat landscape to Novartis assets.
- 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.
- Vulnerability management, response and technical assessments
- Threat research and correlation with vulnerabilities

Skills:

- Strong security knowledge top security vulnerabilities, threat correlation, host/NW controls, mitigations, leading vulnerability scoring standards, such as CVSS, and ability to translate vulnerability severity as security risk.
- Understanding of relevant industry technology environments and their in-depth information including operating system, protocols, services, applications, configurations, and firmware to review and consult on vulnerabilities.
- Experience with security vulnerability detection tools for network, applications, web services, databases, containers, code security, cloud services, NW devices, etc.

- Hands-on experience monitoring threat intel for high-risk vulnerabilities, finding ownerships, handling shadow IT asset scenarios, sensitizing teams for security remediation, performing tests for technical vulnerability confirmation, etc.
- Knowledge of security patching, technical debt, SW patching, and relevant domains.
- Escalation.
- Information Security Audit.
- Information Security Risk Management.
- Quality Management.
- Root Cause Analysis (Rca).
- Sec Ops (Security Operations).
- Vendor Management.
- Persuasive communication skills

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-10018655

Assoc. Dir. DDIT ISC SecOps VulnSvcs

Apply to Job

Source URL: *https://prod1.id.novartis.com/id-en/careers/career-search/job/details/req-10018655-assoc-dir-ddit-isc-secops-vulnsvcs*

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-SecOps-VulnSvcs_REQ-10018655
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Assoc-Dir-DDIT-ISC-SecOps-VulnSvcs_REQ-10018655