NOVARTIS

Assoc. Dir. DDIT ISC SecOps VulnSvcs

Job ID
REQ-10006730
Oct 09, 2024
India

Summary

-Oversees security operations service line, technology governance and external/internal interfaces in accordance with service operations and management processes.
- Objective of the role is to continuously reducing risk exposure from security vulnerabilities with major focus on cloud services and technologies posture.
- This role is part of a pool of security vulnerability experts, with the objective of analyzing ongoing security vulnerabilities risk posture, collaborate with stakeholders/finding owners for managing resolutions, act as SME to assess discovered vulnerabilities, provide pragmatic solutions and flexibly support emergency vulnerability remediations. Collaboration with cross functional teams for threat intel, incident response, security architecture, engineering, remediation and security operations are key.

About the Role

Major accountabilities:

- Act as a Cloud Security SME and Vulnerability Management point of contact for responding to ongoing vulnerability exposure with major focus in cloud services (AWS and Azure).
- Monitor and prioritize security vulnerabilities through risk analysis to understand potential impact and translate vulnerability severity as security risk.
- 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 customers.
- Take accountability to ensure alignment 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 standard methodologies.
- 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.
- Support vulnerability assessments and penetration testing of infrastructure, applications, and services.
- Be flexible with work schedules (including support outside standard business days/hours) to coordinate emergency response for high-risk vulnerability remediation with relevant customers. Drive identification of root causes and prevention of recurrences.
- Collaborate with various customers from cloud engineering, 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
- Flexibility to support vulnerability response remediation with sense of urgency for 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
- 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:

- 10+ years of overall working experience in IT/Security
- 5+ years in Cloud services security area with at least 2 years handling cloud security posture and vulnerability management operations, coordinating with relevant customers, and implementing corrective actions.
- Expertise with top cloud security vulnerabilities, leading vulnerability scoring standards, such as CVSS, and ability to translate vulnerability severity as security risk.
- Strong knowledge of cloud technology environments and their in-depth information including operating system, protocols, services, applications, and configurations to review and consult on vulnerabilities.
- Experience with cloud security vulnerability detection tools and CSPM (preferrable Wiz)
- Hands-on experience monitoring threat intel feeds, high-risk vulnerabilities, finding ownerships, handling shadow IT asset scenarios, sensitizing teams for security remediation, performing quick tests for technical vulnerability confirmation, etc.

Relevant Certifications: AWS Certified Security - Specialty, Azure Security Engineer Associate, Certified Cloud Security Professional (CCSP), or equivalent.

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

Division
Operations
Business Unit
CTS
Location
India
Site
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-10006730

Assoc. Dir. DDIT ISC SecOps VulnSvcs

Apply to Job

Source URL: *https://prod1.id.novartis.com/careers/career-search/job/details/req-10006730-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-10006730
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Assoc-Dir-DDIT-ISC-SecOps-VulnSvcs_REQ-10006730