NOVARTIS

Associate Director, DDIT ISC Vulnerability Response (SecOps Vulnerability Services)

Job ID
REQ-10041246
Feb 21, 2025
Spain

Summary

Location: Barcelona, Tel Aviv

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.

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 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.

Please note this position will require flexibility with work schedules (including support outside standard business days/hours) to coordinate emergency response for high-risk vulnerability remediation with relevant stakeholders.

About the Role

Major responsibilities:

- 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.
- Collaborate with various stakeholders from security operations, architecture, cyber, SOC, and application teams to achieve technical risk reduction goals.

What you will bring to the role:

- University working and thinking level, degree in technical computer science or information security area or comparable education/experience
- 8+ years of experience in information security, preferably in Application Security and Vulnerability management domain.
- 3+ years in handling security vulnerability response and remediation or SOC, coordinating with relevant stakeholders, and implementing corrective actions.
- Experience performing passive discovery and active testing of network or application vulnerabilities for validating external threat landscape to Novartis assets.
- 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.
- Hands-on ability to perform vulnerability analysis, test based technical validation, and guiding remediation using varied set of tools and referenced learning as needed.
- Knowledge of security patching, technical debt, SW patching, and relevant domains.
- Demonstrated leadership skills, through experience as people manager and/or engagement with large security/development program stakeholders; excellent communication skills to effectively convey security risks and vulnerabilities to both technical and non-technical stakeholders, and the ability to collaborate with cross-functional teams.
- Strong problem-solving skills, ability to work independently, continuous learning attitude and a commitment to staying up to date with the latest security updates, vulnerability disclosures, and industry best practices.
- Strong understanding of metrics, KPI/KRI, SLAs, and dashboards for vulnerability management and providing executive reporting.

Desirable:

- Experience in vulnerability response and technical analysis.
- Relevant certifications: Offensive Security Certified Professional (OSCP), GIAC Penetration Tester (GPEN); Certified Information Systems Security Professional (CISSP), 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
Spain
Site
Barcelona Provincial
Company / Legal Entity
ES06 (FCRS = ES006) Novartis Farmacéutica, S.A.
Alternative Location 1
Israel, Israel
Functional Area
Technology Transformation
Job Type
Full time
Employment Type
Regular
Shift Work

No
Apply to Job
Job ID
REQ-10041246

Associate Director, DDIT ISC Vulnerability Response (SecOps Vulnerability Services)

Apply to Job

Source URL: *https://prod1.novartis.com/careers/career-search/job/details/req-10041246-associate-director-ddit-isc-vulnerability-response-secops-vulnerability-services*

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/Barcelona-Provincial/Associate-Director--DDIT-ISC-Vulnerability-Response--SecOps-Vulnerability-Services-_REQ-10041246-1
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Barcelona-Provincial/Associate-Director--DDIT-ISC-Vulnerability-Response--SecOps-Vulnerability-Services-_REQ-10041246-1