Associate Director, Security Patching (ISC SecOps Vulnerability Services)

Job ID
REQ-10063068

9月 30, 2025

Spain

摘要

Location: Barcelona, Spain; Hyderabad, India; #LI-Hybrid (12 days/month in office)

Internal job title: Assoc. Dir. DDIT ISC SecOps VulnSvcs

The role is based in Barcelona or Hyderabad. Novartis is unable to offer relocation support for this role: please only apply if this location is accessible for you.

About the Role:

The Associate Director, Security Patching will join the DDIT ISC Security Operations Vulnerability Services team. The role will focus on reducing risk exposure from security vulnerabilities with major focus on enabling, enforcing and operating scalable remediation through Security Patching process. Among the responsibilities, will be to analyze ongoing security vulnerabilities risk posture, align patch based remediations, collaborate with service lines and finding owners for managing resolutions for patch success, act as SME to assess discovered vulnerabilities, provide pragmatic solutions and

flexibly support emergency security patching. Collaboration with cross functional teams for patch infrastructure health, threat intel, security architecture, remediation and security operations are key.

Please note this position may 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

Key Responsibilities:

- Govern and operate the Security Patch Management process for technologies such as Windows servers, Unix servers, Windows clients, Mac clients, databases, and middleware.
- Assess daily risk exposure from security vulnerabilities, assess patch applicability and enable scalable remediations through centralized or decentralized patching.
- Monitor patching coverage and compliance using tools such as SNOW, INPAT, SCCM, Intune, JamF, Ansible.
- Generate regular reports on patching status, coverage, and risk metrics continuously engage with service lines and stakeholders to maintain the process and tools health.
- Assess, initiate and lead emergency patching activities to ensure timely responses to critical vulnerabilities; Perform root cause analysis for patching failures and implement corrective actions.
- Create and maintain documentation, including SOPs, work instructions knowledge articles, and training material. Ensure cross functional relevant documents are maintained/updated from time to time or upon changes to related working.
- Take accountability to ensure adherence with Security and Compliance policies and procedures; Implement security policies, procedures, and standards to ensure confidentiality, integrity, and availability of resources from technical vulnerabilities.
- Stay up to date with the latest security threats and vulnerabilities, proactively recommending mitigation strategies.
- Provide security awareness and training to teams and stakeholders.
- Collaborate with various stakeholders from cross functional service lines, security operations, architecture, cyber, SOC, and application/infra teams to achieve technical risk reduction goals.

Essential Requirements:

- University working and thinking level, degree in technical computer science or information security area or comparable education/experience.
- 8+ years of overall working experience in information security, preferably in Security patch management, vulnerability management and/or Infrastructure patching domain.
- 3+ years in handling security vulnerability analysis, remediation and response coordinating with relevant stakeholders, and implementing corrective actions.
- Experience with vulnerability management, scanning and patching tools: Qualys, ServiceNow, Wiz, MS Defender, SCCM, Intune, JamF, Ansible.
- Excellent hands-on analytical skills for vulnerability exposure analysis, remediation analysis,

mitigations and RCA. Strong understanding of metrics, KPI/KRI, SLAs, and dashboards for vulnerability management and providing executive reporting.
- Strong knowledge of automation/orchestration implementation in patch management, top security vulnerabilities, threat correlation, control mitigations, vulnerability scoring standards and ability to translate vulnerability severity as security risk.
- Knowledge of operating systems and platforms: Windows servers, Unix servers, Windows clients, Mac clients, databases, middleware technologies for patch analysis.
- Know how on handling shadow IT asset scenarios, sensitizing teams for security patching, technical debt, SW patching, maintenance windows, scalable remediations, and relevant domains.
- Demonstrated stakeholder management skills and leadership skills through engagement with large security/development program stakeholders.
- Excellent communication and cross-functional collaboration skills, ability to effectively convey security risks and vulnerabilities to both technical and non-technical stakeholders
- Strong problem-solving skills and the ability to work independently and ensuring external team deliverables and day to day outcomes; strong curiosity, staying up to date with the latest security updates, vulnerability disclosures, and industry best practices.

Desirable:

- Working experience in security patching domain, vulnerability patch analysis and automation/orchestration implementation in patch management.
- Relevant certifications: Certified Information Systems Security Professional (CISSP), Certified Cloud Security Professional (CCSP), or equivalent.
- Product certified knowledge like Microsoft or RHCE.

Commitment to Diversity & Inclusion:

We are committed to building an outstanding, inclusive work environment and diverse teams representative of the patients and communities we serve.

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

Join our Novartis Network: If this role is not suitable to your experience or career goals but you wish to stay connected to learn more about Novartis and our career opportunities, join the Novartis Network here: https://talentnetwork.novartis.com/network

Accessibility and accommodation:
Novartis is committed to working with and providing reasonable accommodation to all individuals. If, because of a medical condition or disability, you need a reasonable accommodation for any part of the recruitment process, or in order to receive more detailed information about the essential functions of a position, please send an e-mail to and let us know the nature of your request and your contact information. Please include the job requisition number in your message.

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
CTS

地点
Spain

站点
Barcelona Gran V í a

Company / Legal Entity
ES06 (FCRS = ES006) Novartis Farmac é utica, S.A.

Alternative Location 1
Hyderabad (Office), India

Functional Area
Technology Transformation

Job Type
Full time

Employment Type
Regular

Shift Work
No

Apply to Job

Job ID
REQ-10063068

Associate Director, Security Patching (ISC SecOps Vulnerability Services)

Apply to Job

Source URL:
https://www.novartis.com.cn/careers/career-search/job/details/req-10063068-associate-director-security-patching-isc-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/about/strategy/people-and-culture
4. https://talentnetwork.novartis.com/network
5. https://www.novartis.com/careers/benefits-rewards
6. https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/Barcelona-Gran-Va/Associate-Director--Security-Patching--ISC-SecOps-Vulnerability-Services-REQ-10063068-1
7. https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/Barcelona-Gran-Va/Associate-Director--Security-Patching--ISC-SecOps-Vulnerability-Services-REQ-10063068-1