NOVARTIS

Threat Detection & Response Senior Specialist

Job ID
REQ-10076479
May 13, 2026
LOC_MX

About the Role

Key Responsibilities:

- Security Monitoring and Triage: monitor in real time security controls and consoles from across the Novartis IT ecosystem
- Forensics and Incident Response: support incident response activities including scoping, communication, reporting, and long term remediation planning, conduct initial investigations into security incidents involving a variety of threats
- Communicate with technical and non-technical end users who report suspicious activity, prepare technical reports for business stakeholders and IT leadership
- Gather live evidence from endpoint devices and log sources from a variety of systems and applications
- Big Data analysis and reporting: Utilizing SIEM/Big data to identify abnormal activity and extract meaningful insights; Research, develop, and enhance content within SIEM and other tools
- Technologies and Automation: Interface with engineering teams to design, test, and implement playbooks, orchestration workflows and automations; Research and test new technologies and platforms; develop recommendations and improvement plans
- Day to day: Perform host based analysis, artifact analysis, network packet analysis, and malware analysis in support of security investigations and incident response; Coordinate investigation, containment, and other response activities with business stakeholders and groups; Develop and maintain effective documentation; including response playbooks, processes, and other supporting operational material
- Perform quality assurance review of analyst investigations and work product; develop feedback and development reports; Develop incident analysis and findings reports for management, including gap identification and recommendations for improvement; Recommend or develop new detection logic and tune existing sensors / security controls
- Provide mentoring of junior staff and serve as point of escalation for higher severity incidents
- Work with security solutions owners to assess existing security solutions array ability to detect / mitigate the abovementioned TTPs

Essential Requirements:

- Bachelor’s degree in Cybersecurity, Computer Science, Information Technology, or a related field, or equivalent practical experience.
- 3+ years of experience in cybersecurity, with significant experience in incident response, threat detection, or security operations.
- Strong hands-on experience investigating and responding to security incidents in enterprise environments.
- Deep understanding of attacker techniques across endpoint, identity, network, cloud, and email attack surfaces.
- Experience working in a CSOC, SOC, or incident response function in a large, complex organization.
- Strong knowledge of security operations workflows, alert triage, escalation management, and response coordination.
- Experience with SIEM, EDR/XDR, email security, identity monitoring, case management, and other security operations technologies.
- Ability to analyze logs, alerts, and forensic artifacts to determine scope, impact, and response actions.
- Strong written and verbal communication skills, with the ability to clearly brief both technical teams and senior stakeholders.
- Proven ability to identify operational improvement opportunities and drive meaningful enhancements without direct people management responsibility.

Desirable Requirements:

- Scripting experience with Python, PowerShell, Bash, or similar languages
- Experience with malware analysis or basic reverse

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

Role Requirements

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

Benefits and Rewards: Learn about all the ways we'll help you thrive personally and professionally.
Read our handbook (PDF 30 MB)

Division
DIV_TO
Business Unit
Information Technology
Location
LOC_MX
Site
INSURGENTES
Company / Legal Entity
MX06 (FCRS = MX006) Novartis Farmacéutica S.A. de C.V.
Functional Area
FCT_TT
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job

Job ID
REQ-10076479

Threat Detection & Response Senior Specialist

Apply to Job

Source URL: *https://prod1.jobapi.novartis.com.cn/req-10076479-threat-detection-response-senior-specialist*

List of links present in page

1. https://prod1.jobapi.novartis.com.cn/req-10076479-threat-detection-response-senior-specialist
2. https://www.novartis.com/about/strategy/people-and-culture
3. https://talentnetwork.novartis.com/network
4. https://www.novartis.com/about/strategy/people-and-culture
5. https://www.novartis.com/sites/novartis_com/files/novartis-life-handbook.pdf
6. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/INSURGENTES/Threat-Detection---Response-Senior-Specialist_REQ-10076479-1
7. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/INSURGENTES/Threat-Detection---Response-Senior-Specialist_REQ-10076479-1