

Assoc. Dir. DDIT ISC Ent Arch Digit Sec

Job ID

394168BR

Apr 16, 2024

India

Summary

-The Threat Hunting and Response Senior Analyst will be an integral part of the Novartis Cyber Security Operations Center (CSOC). -The CSOC is an advanced global team passionate about the active defense against the most sophisticated cyber threats and attacks. -The Threat Hunting and Response Senior Analyst will leverage a variety of tools and resources to proactively detect, investigate and mitigate emerging and persistent threats impacting Novartis networks, systems, users and applications. -This role will involve coordination and communication with technical and nontechnical teams including security leadership and business stakeholders. -As an experienced skilled analyst this role will also involve coaching and mentoring of more junior analysts.

About the Role

Major accountabilities:

- Forensics and Incident response -Serve as escalation point for conducting investigations into security incidents involving advanced and sophisticated threat actors and TTPs.
- Perform forensic collection and analysis of electronic assets and devices.
- Scripts and malicious software log sources from a variety of systems and applications.
- Manage incident response activities including scoping, communication, reporting and long term remediation planning.
- Threat Hunting, review incident and intelligence reports from a variety of internal and external sources and teams.
- Develop hypotheses, analyze techniques and execute hunts to identify threats across the environment.
- Interface with security teams and business stakeholders to implement countermeasures and improve defenses.
- Big Data analysis and reporting.
- Research and develop 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.
- 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.
- Utilizing SIEM/Big data to identify abnormal activity and extract meaningful insights.

- 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.
- Work with security solutions owners to assess existing security solutions array ability to detect / mitigate the abovementioned TTPs.
- Creating custom SIEM queries and dashboards to support the monitoring and detection of advanced TTPs against Novartis network.

Key performance indicators:

- Effectively investigate to identify root cause, including attack vector, exploitation and other techniques utilized to bypass security controls.
- Accurately diagnose impact, damage and mitigation techniques needed to restore business operations and minimize reoccurrence.
- Identify technology and process gaps that affect CSOC services.
- Develop solutions and make recommendations for continuous improvement.
- Provide oversight and support for monitoring, hunting and incident response activities to ensure effective operations and mitigation of cyber security threats and risks.

Minimum Requirements:

Work Experience:

- Relationship Management.
- Technical knowledge.
- Influencing without authority.
- Accountability.
- Process management.
- Experience working cross-functionally and trans-nationally.
- Interactions with senior management.
- Strategy Development.
- Collaborating across boundaries.

Skills:

- IT Governance.
- Compliance Risk Assessment and Remediation Protocols.
- Knowledge of all relevant policies and practices.
- Emerging Technology Monitoring.
- Regulatory Strategy.
- Strategic thinking and planning.
- Facilitation.
- Quality decision making.
- Creativity and visioning.
- Proactive thinking.
- Risk Management.
- Influencing and persuading.
- Effective communication.
- Synthesize insights to opportunities/challenges.

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

394168BR

Assoc. Dir. DDIT ISC Ent Arch Digit Sec

[Apply to Job](#)

Source URL: <https://prod1.adacap.com/careers/career-search/job/details/394168br-assoc-dir-ddit-isc-ent-arch-digit-sec-0>

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-Ent-Arch-Digit-Sec_394168BR
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Assoc-Dir-DDIT-ISC-Ent-Arch-Digit-Sec_394168BR