Senior Specialist DDIT ISC Detection & Response

Job ID
REQ-10023350
Oct 17, 2024
India

About the Role

MAJOR ACCOUNTABILITIES:

- Security Monitoring and Triage
  - Monitor in real time security controls and alerts originating from the Novartis IT ecosystem
  - Communicate with technical and non-technical end users who report suspicious activity
- Forensics and Incident Response
  - Conduct initial investigations into suspicious events and activity
  - Gather live evidence and logs from a variety of devices and applications
  - Support incident response activities including scoping, communication, reporting, and long term remediation planning
  - Prepare technical reports for business stakeholders and IT leadership
- 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 propose new automation and orchestration concepts
  - Research and test new technologies and platforms; develop recommendations and improvement plans
- Day to day:
  - Perform host based analysis, artifact analysis, network 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
  - Provide mentoring of junior staff and serve as point of escalation for higher severity incidents
  - 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 / MEASURES OF SUCCESS:

- 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 first level monitoring and triage to ensure effective operations and mitigation of lower impact incidents
- Good cultural orientation and strong influencer of information risk management, information security, IT security, to be embedded across IT, OT and Medical Technologies.

EXPERIENCE:

- 3+ years experience in cybersecurity / security operations
- Experience in Information Technology / Analytical role preferred
- Experience in IT administration with technical, analytical and conceptual skills
- Experience in reporting to and communicating technical and non-technical business stakeholders
- Excellent written and verbal communication and presentation skills; interpersonal and collaborative skills; and the ability to communicate information risk-related and incident response concepts to technical as well as nontechnical audiences

SKILLS/JOB RELATED KNOWLEDGE:

- Good mediation and facilitation skills
- Good knowledge of IT Security Project Management
- Understanding and knowledge of general IT infrastructure technology and systems
- Knowledge of (information) risk management related standards or frameworks such as COSO, ISO 2700x, CobiT, ISO 24762, BS 25999, NIST, ISF Standard of Good Practice and ITIL
- Knowledge of security frameworks such as Hitrust
- Host and network based forensic collection and analysis
- Dynamic malware analysis, reverse engineering, and/or scripting abilities
- Familiarity with Encase, Responder, X-Ways, Volatility, FTK, Axiom, Splunk, Wireshark, and other forensic tools
- Understanding of Advanced Persistent Threat (APT) and associated tactics.
- Research, enrichment, and searching of indicators of compromise
- Very strong team and interpersonal skills along with the ability to work independently and achieve individual goals.
- Coordinate with other team members to achieve the specified objectives.

EDUCATION:

- University working and thinking level, degree in business/technical/scientific area or comparable education/experience
- Professional information security certification, such as CISSP, CISM or ISO 27001 auditor / practitioner is preferred. Professional (information system) risk or audit certification such as CIA, CISA or CRISC is preferred

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

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-10023350

Senior Specialist DDIT ISC Detection & Response

Apply to Job

Source URL: *https://jobapi.novartis.com/req-10023350-senior-specialist-ddit-isc-detection-response*

List of links present in page

1. https://jobapi.novartis.com/req-10023350-senior-specialist-ddit-isc-detection-response
2. https://www.novartis.com/about/strategy/people-and-culture
3. https://talentnetwork.novartis.com/network
4. https://www.novartis.com/careers/benefits-rewards
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Senior-Specialist-DDIT-ISC-Detection---Response_REQ-10023350
6. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Hyderabad-Office/Senior-Specialist-DDIT-ISC-Detection---Response_REQ-10023350