Associate Director DDIT ISC Detection & Response

Job ID
REQ-10022170
Sep 26, 2024
Mexico

About the Role

MAJOR ACCOUNTABILITIES

In addition to accountabilities listed above in Job Purpose:

- Security Monitoring and Triage
  - Monitor in real time security controls and consoles from across the Novartis IT ecosystem
  - Communicate with technical and non-technical end users who report suspicious activity
- Forensics and Incident Response
  - Conduct initial investigations into security incidents involving a variety of threats
  - Gather live evidence from endpoint devices and log sources from a variety of systems and applications
  - Support incident response activities including scoping, communication, reporting, and long term remediation planning
  - Review technical reports and escalations for completeness and accuracy
- 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
  - 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

Minimum Requirements:
Work Experience:

- 5+ years of experience in Incident Response / Computer Forensics / CSOC team / Threat Hunting or related fields
- Experience in reporting to and communicating with senior level management (with and without IT background, with and without in depth risk management background) on incident response topics
- 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
- Excellent understanding and knowledge of general IT infrastructure technology and systems
- Proven experience to initiate and manage projects that will affect CSOC services and technologies
- Experienced IT administration with broad and in-depth technical, analytical and conceptual skills

Skills:

- Good mediation and facilitation skills
- Good knowledge of IT Security Project Management
- Experience with security incident monitoring and response related to medical devices
- 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
- Proficient 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.
- Effective oral and written communication skills

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
Mexico
Site
INSURGENTES
Company / Legal Entity
MX06 (FCRS = MX006) Novartis Farmacéutica S.A. de C.V.
Functional Area
Technology Transformation
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job

Job ID
REQ-10022170

Associate Director DDIT ISC Detection & Response

Apply to Job

Source URL: *https://jobapi.novartis.com/req-10022170-associate-director-ddit-isc-detection-response*

List of links present in page

1. https://jobapi.novartis.com/req-10022170-associate-director-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/INSURGENTES/Associate-Director-DDIT-ISC-Detection---Response_REQ-10022170-2
6. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/INSURGENTES/Associate-Director-DDIT-ISC-Detection---Response_REQ-10022170-2