Associate Director Threat Hunting & Response

Job ID
REQ-10045919
Apr 04, 2025
Malaysia

Summary

Operations Center (CSOC). The CSOC is an advanced global team passionate about the active defense against the most sophisticated cyber threats and attacks. The Associate Director Threat Hunting and Responsewill is a principal engineer who 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 engineer, this role will also involve coaching and mentoring of more junior members of the CSOC.

About the Role

Associate Director Threat Hunting & Response

Location – Malaysia #LI Hybrid

About the Role:

The Associate Director Threat Hunting and Response 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 Associate Director Threat Hunting and Response will is a principal engineer who 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 engineer, this role will also involve coaching and mentoring of more junior members of the CSOC.

Key Responsibilities:

- 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, and log sources from a variety of systems and applications.
- Manage incident response activities including scoping, communication, reporting, and long term remediation planning.
- 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.
- Utilizing SIEM/Big data to identify abnormal activity and extract meaningful insights.
- Interface with engineering teams to design, test, and implement playbooks, orchestration workflows and automations.

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.

Essential Requirements:

- 8+ years of experience in Incident Response / Computer Forensics / CSOC team / Threat Hunting or related fields.
- Experienced IT administration with broad and in-depth technical, analytical and conceptual skills.
- 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.

Desirable Requirements:

- 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.

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

You'll receive: You can find everything you need to know about our benefits and rewards in the Novartis Life Handbook. https://www.novartis.com/careers/benefits-rewards

Commitment to Diversity and Inclusion:
Novartis is committed to building an outstanding, inclusive work environment and diverse teams' representative of the patients and communities we serve.
Join our Novartis Network: If this role is not suitable to your experience or career goals but you wish to stay connected to hear more about Novartis and our career opportunities, join the Novartis Network here: https://talentnetwork.novartis.com/network.

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
Universal Hierarchy Node
Location
Malaysia
Site
Selangor
Company / Legal Entity
MY01 (FCRS = MY001) Novartis Corporation (Malaysia) Sdn. Bhd. (19710100054)
Functional Area
Technology Transformation
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job
Job ID
REQ-10045919

Associate Director Threat Hunting & Response

Apply to Job

Source URL: *https://prod1.novartis.com/uk-en/careers/career-search/job/details/req-10045919-associate-director-threat-hunting-response*

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/Selangor/Associate-Director-Threat-Hunting---Response_REQ-10045919-1
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Selangor/Associate-Director-Threat-Hunting---Response_REQ-10045919-1