NOVARTIS

Cyber Threat Intelligence Researcher

Job ID
REQ-10009758
Jun 05, 2024
Israel

Summary

Cyber Threat Intelligence Researcher Location: Tel-Aviv, Israel About the role: The Cyber Threat Intelligence Researcher will be an integral part of the Threat Intelligence Team and the Novartis Cyber Center, providing leadership the most advanced analysis of cyber threats to the company, alongside with practical measures and controls to protect against them. The Cyber Threat Intelligence Researcher will use a variety of tools and resources to proactively collect and analyze threat intelligence, implement in-depth research about threats to the organization and the industry, and work with multiple teams to alert on threats to the organization, as well as to generate and deploy security controls to address them.

About the Role

Key Responsibilities:

- Analyze data logs from different security controls to identify cyber threats and patterns, and generate relevant intelligence and recommendations to the operation teams
- Effectively monitor, collect and report Intelligence relevant to the company and the industry
- Accurately analyze the impact / potential impact of an incident or vulnerability
- Implement in-depth research on threat actors, TTPs and vulnerabilities, and generate reports and white papers to relevant stakeholders
- Support and enrich internal security incidents with valuable threat intelligence concepts
- Define use cases to connect between Threat Intelligence indicators to the organization’s security controls
- Work with the Cyber and the Threat Hunting teams to create monitoring tools for highly sophisticated hacking technique

Essential Requirements:

- 3+ years of experience in Threat Intelligence / technical Intelligence analysis / Threat Hunting / SOC or related fields
- University working and thinking level. Degree in technical/scientific/business area or comparable education/experience
- Experience in reporting to and communicating with senior level management
- Experience in reviewing security controls data logs
- Knowledge of APT campaigns, attack Tactics, Techniques and Procedures (TTPs) and clear understanding and implementation of MITRE ATT&CK framework
- Experience with threat feed research; collect, prioritize, organize and research
- Hands on experience with SIEM (as Splunk)
- 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 in English
- Experience in leading projects end-to-end
- Strong collaboration and team-work skills, and ability to work independently
- Creative and proactive approach
- High technical aptitude; quickly learns new skills
- Scripting experience with Python, PowerShell – Big advantage

Desirable requirements:

- 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

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

Accessibility and accommodation:
Novartis is committed to working with and providing reasonable accommodation to all individuals. If, because of a medical condition or disability, you need a reasonable accommodation for any part of the recruitment process, or in order to receive more detailed information about the essential functions of a position, please send an e-mail to and let us know the nature of your request and your contact information. Please include the job requisition number in your message.

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

Division
Operations
Business Unit
CTS
Location
Israel
Site
Israel
Company / Legal Entity
IL04 (FCRS = IL004) Novartis Israel
Job Type

Full time
Employment Type
Regular
Shift Work
No
Apply to Job
Job ID
REQ-10009758

Cyber Threat Intelligence Researcher

Apply to Job

Source URL: *https://www.adacap.com/careers/career-search/job/details/req-10009758-cyber-threat-intelligence-researcher*

List of links present in page

1. https://www.novartis.com/about/strategy/people-and-culture
2. https://talentnetwork.novartis.com/network
3. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Israel/Assoc--Dir-DDIT-ISC--Threat-Intel-Research_REQ-10009758
4. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Israel/Assoc--Dir-DDIT-ISC--Threat-Intel-Research_REQ-10009758