NOVARTIS

Defensive Cyber Security Researcher

Job ID
REQ-10077584

5月 28, 2026

Israel

摘要

Location: Tel-Aviv, Israel
#LI-Hybrid 3 days/week in office

Internal job title: Assoc. Dir. DDIT ISC Security Research

About the role:

The Defensive Cyber Security Researcher will be part of a new Think Tank group of security researchers that will challenge Novartis information security defenses, application security and data protection.
The Defensive Cyber Security Researcher will be responsible for participating in threat actor based investigations, creating new detection methodology and providing expert support to incident response and monitoring functions.
The focus of the Defensive Cyber Security Researcher is to detect, disrupt and eradicate threat actors from enterprise networks, including emerging AI-driven and AI-assisted threats. To execute this mission, the Defensive Cyber Security Researcher will use data analysis, threat intelligence, and cutting-edge security technologies – with a growing emphasis on understanding how AI can be

weaponized against the organization and how it can be leveraged defensively.
The Defensive Cyber Security Researcher will identify and analyze patterns and changes in tactics, techniques and procedures used by attackers to attack Novartis IT infrastructure and management staff. The analysis will result in indicators of compromise, accurate understanding of the risk to Novartis IT infrastructure and prioritization of remediation efforts.

About the Role

Key Responsibilities:

- Hunt through huge number of signals to identify new emerging threats, dissect them and extract meaningful insights and indicators of compromise.
- Demonstrate adversary tactics to recognize and analyze malicious activity (techniques, tools and processes) based on a combination of behavioral activity and signature based analysis.
- Participate in "hunting missions" using threat intelligence, analysis of anomalous log data and results of brainstorming sessions to detect and eradicate threat actors on the Novartis network.
- Provide expert analytic investigative support of large scale and complex security incidents.
- Perform analysis of security incidents for further enhancement of alert catalog; perform in-depth static and dynamic malware reverse engineering; preform ad hoc memory and disk forensics.
- Produce detailed technical reports in support of malware / other hunting investigations.
- Review alerts generated by detection infrastructure for effectiveness and recommend improvements.
- In collaboration with the Security Operations Center: Develop dashboards and reports to identify potential threats, suspicious/anomalous activity, malware, etc.
- Research and assess AI-specific security risks to the organization, including adversarial use of AI models, prompt injection attacks, data poisoning, shadow AI adoption, and LLM-assisted threat actor operations; translate findings into actionable defensive guidance and detection rules.
- Collaborate with Cyber Threat Intelligence (CTI) teams to operationalize intelligence feeds, enrich hunting missions with external and internal threat data, and contribute research outputs (IOCs, TTPs, adversary profiles) back into intelligence pipelines.

Essential Requirements:

- 5+ years of experience in Incident Response / CERT team or 5+ years of experience with malware investigations.

- Critical understanding of the cyber attacker kills chain elements, with particular emphasis on attack objectives.
- High familiarity and experience with Active Directory (AD) and Entra ID / Azure AD security – including AD attack paths (Kerberoasting, pass-the-hash, DCSync, Golden/Silver Ticket), BloodHound-based graph analysis, AD tiering models, and Conditional Access Policies; ability to identify misconfigurations that lead to privilege escalation and lateral movement.
- Solid understanding of AI security risks and their organizational impact, including adversarial

machine learning, prompt injection, data poisoning, shadow AI risks, and the use of generative AI tools by threat actors; ability to advise the organization on AI-related threat exposure and contribute to AI governance from a security perspective.
- Proven ability to work effectively with Security Operations Center (SOC) teams: including joint detection engineering, alert tuning, escalation workflows, and acting as a subject matter expert during high-severity incident response; experience bridging the gap between research depth and SOC operational tempo.
- Experience working with Cyber Threat Intelligence (CTI) teams: consuming and operationalizing intelligence products, contributing research outputs as structured intelligence (IOCs, TTPs, adversary profiles), and participating in joint threat briefings and intelligence-driven hunting operations.
- Good familiarity with Red Teaming tools and operations, understanding of Wireshark, Cobalt Strike and more
- Advanced programming skills with scripting languages such as Python/Perl/Ruby.
- Familiarity with the current nation-state ("APT") threat landscape and the various actors and groups.

- Very strong team and interpersonal skills along with the ability to work independently and achieve individual goals, with effective oral and written communication skills.

Desirable requirements:

- Relevant Technical Security Certifications (GIAC, EC-Council, Offensive Security, etc.)

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

Benefits and Rewards: Learn about all the ways we ' ll help you thrive personally and professionally. Read our handbook (PDF 30 MB)

部门
Operations

Business Unit
Information Technology

地点
Israel

站点
Israel

Company / Legal Entity
IL04 (FCRS = IL004) Novartis Israel

Functional Area
Technology Transformation

Job Type
Full time

Employment Type
Regular

Shift Work
No

Job ID
REQ-10077584

Defensive Cyber Security Researcher

Apply to Job

Job ID
REQ-10077584

Defensive Cyber Security Researcher

Apply to Job

Source URL:
https://www.novartis.com.cn/careers/career-search/job/details/req-10077584-defensive-cyber-security-researcher

List of links present in page

1. https://www.novartis.com/about/strategy/people-and-culture
2. https://www.novartis.com/sites/novartiscom/files/novartis-life-handbook.pdf
3. https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/Israel/Defensive-Cyber-Security-ResearcherREQ-10077584
4. https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/Israel/Defensive-Cyber-Security-ResearcherREQ-10077584