NOVARTIS

Offensive Cyber Security Researcher

Job ID
REQ-10066824

11月 17, 2025

Israel

摘要

Location: Tel Aviv, Israel; #LI-Hybrid (12 days/month in office)

The role is based in Tel Aviv. Novartis is unable to offer relocation support for this role: please only apply if this location is accessible for you.

About the Role:

The Offensive Cyber Security Researcher will join a newly established Think Tank of advanced security researchers responsible for continuously challenging Novartis ’ information security defenses, application security posture, and data protection capabilities.

In this role, the researcher will take a true attacker-focused perspective, analyzing Novartis ’ infrastructure, identity systems, and business applications as a sophisticated adversary would. This includes conducting deep vulnerability research, exploring innovative infiltration and exfiltration techniques, mapping attack paths, and developing realistic breach scenarios that reflect modern threat actor behavior.

The researcher will proactively identify and evaluate weaknesses, related exploits, and attack vectors, translating offensive insights into actionable defensive recommendations that improve Novartis ' overall security resilience.

About the Role

Key Responsibilities:

- Proactively identify gaps and vulnerabilities in Novartis systems and architectures, and validate possible exploitation by defining the most likely threat actors and required capabilities.
- Design and develop tools, frameworks, and the methods required for facilitating and executing complex attacks and emulating adversarial tactics, techniques and procedures (TTPs).
- Conduct deep-dive research into AD, Entra ID, and hybrid identity attack surfaces.
- Develop and maintain cutting-edge techniques for privilege escalation, credential compromise, session hijacking, lateral movement, and domain dominance.
- Track emerging identity-related threats, TTPs, attack paths, and novel exploitation techniques
- Provide in-depth technical analysis of computer networks applications and systems, culminating in the identification of existing potential vulnerabilities.
- Collaborate with engineering teams to test for and prevent threats to Novartis Networks infrastructure and data, and work closely with the Threat Hunters and Intelligence teams to help improve the team's abilities in Detection, Prevention and Response capabilities.
- Maintain up-to-date awareness of computer network exploitation and attack tools, threats and vulnerabilities and respective counter/mitigation measures.
- Assist with security investigations, root-cause analysis and corrective measures as required.
- Design and execute realistic attack simulations against enterprise identity systems to validate detection, controls, and architectural design.
- Compose Red Team test reports and record vulnerability data according to Governance, Risk, and Compliance processes.
- Deliver technical debriefs to engineers and developers as needed, and work with IS&RM managers to prioritize vulnerability findings for remediation.
- Mentor and train Novartis IS&RM employees in attack techniques, intelligence analysis and adversarial tactics

Essential Requirements:

- Education: BA or BSc in Computer Science or a related field, or comparable work experience
- 5+ Years experience in Security Research, Web-Application & Network Penetration Testing or adjacent fields.
- Experience in Software development with proficiency in multiple languages, mainly C/C++ and other object-oriented platforms. Experience with scripting languages such as Python/Perl/Ruby.
- Expertise with reverse engineering tools (e.g. disassemblers, debuggers, instrumentation frameworks, etc.).
- Ability to understand and apply attack and penetration concepts including the attack surface;

identification of system software and configuration vulnerabilities and critical information, data and processes that must be protected.
- Basic understanding of concepts in vulnerability research: Shellcode, ROP, ASLR, exploit types, and heap manipulation; Experience in IOT and Industrial Controls Systems.
- Ability to manage new and existing security requirements, help with training personnel, and implement control and risk procedures to ensure all operations are conducted in accordance of Novartis networks standards.
- Very strong team and interpersonal skills along with sense of ownership, and the ability to work independently and achieve individual goals; ability to collaborate and coordinate with other team members to achieve the specified objectives; excellent communication skills

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.

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-10066824

Offensive Cyber Security Researcher

Apply to Job

Job ID
REQ-10066824

Offensive Cyber Security Researcher

Apply to Job

Source URL:
https://prod1.novartis.com.cn/careers/career-search/job/details/req-10066824-offensive-cyber-security-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://www.novartis.com/about/strategy/people-and-culture
4. https://www.novartis.com/sites/novartiscom/files/novartis-life-handbook.pdf
5. https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/Israel/Offensive-Cyber-Security-ResearcherREQ-10066824-1
6. https://novartis.wd3.myworkdayjobs.com/en-US/NovartisCareers/job/Israel/Offensive-Cyber-Security-ResearcherREQ-10066824-1