Defensive Cyber Security Researcher " >

Job ID
322964BR
Oct 06, 2021
Israel

Job Description

Defensive Cyber Security Researcher, Novartis, Tel Aviv, Israel

15 Petabyte of hosted data, 49 supported countries, 15000 servers and thousands of devices to connect locations and businesses.

Information is one of Novartis' most valuable assets and in our ISRM unit (Information Security and Risk Management), we implement and maintain solutions that secure the Novartis environment, protect our data, and provide the necessary control framework.

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. If you have what it takes, join our Tel Aviv Cyber Team.

Your key responsibilities:
Your responsibilities include, but are not limited to:

• Hunt through signals to identify threats, dissect them and extract meaningful insights and indicators of compromise.
• Demonstrate adversary tactics to recognize and analyze malicious activity
• 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.
• Analyze network traffic protocols and cryptographic algorithms leveraged by malware.
• Develop dashboards and reports to identify potential threats, suspicious/anomalous activity, malware in collaboration with the Security Operations Center
• Provide forensic analysis of network packet captures, DNS, proxy, NetFlow, malware, host-based security and application logs in alignment and collaboration with the Forensics team

Minimum Requirements

What you'll bring to the role:

• Critical understanding of the cyber attacker kills chain elements, with particular emphasis on attack objectives
• Advanced understanding of cyber threat vectors and countermeasures
• Software development experience/proficiency with scripting languages such as Python/Perl/Ruby
• In depth knowledge with analyzing disassembly of x86 and x64 binaries

• Expert in dynamic and static analysis and tools such as IDAPro and Ollydbg
• Experience with Snort, Bro or other network intrusion detection tools
• Skilled in performing kernel-mode debugging on rootkit malware
• Strong understanding of Windows Operating System Internals and Windows APIs as well as of Linux/UNIX operating systems
• Familiarity with YARA, OpenIOC, and STIX frameworks.

Desirable requirements:

• 5+ years of experience in Incident Response / CERT team and in Malware investigation
• Very strong team and interpersonal skills along with the ability to work independently and achieve individual goals

You'll receive:

- **Flexible working options – it's your choice with responsibility**
- **Global development opportunities**
- **Annual bonus, Pension fund, Study fund**
- **Company car and company phone**
- **Annual leave above the legal requirement**
- **Additional weeks of Paid parental leave**
- **Perks such as Holiday gift vouchers or birthday gifts**
- **Daily food allowance**

Why consider Novartis?
799 million. That's how many lives our products touched in 2019. And while we're proud of that fact, in this world of digital and technological transformation, we must also ask ourselves this: how can we continue to improve and extend even more people's lives?

We believe the answers are found when curious, courageous and collaborative people like you are brought together in an inspiring environment. Where you're given opportunities to explore the power of digital and data. Where you're empowered to risk failure by taking smart risks, and where you're surrounded by people who share your determination to tackle the world's toughest medical challenges.

Imagine what you could do at Novartis!

Commitment to Diversity & Inclusion:
Novartis embraces diversity, equal opportunity and inclusion. We are committed to building diverse teams, representative of the patients and communities we serve, and we strive to create an inclusive workplace that cultivates bold innovation through collaboration, and empowers our people to unleash their full potential.

Novartis are an equal opportunities employer and welcome applications from all suitably qualified persons.

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

Division
CTS
Business Unit
TT CTS
Location
Israel
Site
Tel Aviv
Company / Legal Entity
Novartis Israel
Functional Area
Information Technology
Job Type
Full Time
Employment Type
Regular
Shift Work
No

Apply to Job Access Job Account

Job ID
322964BR

Defensive Cyber Security Researcher

Apply to Job Access Job Account

Source URL: *https://www.novartis.com/careers/career-search/job-details/322964br/defensive-cyber-security-researcher*

List of links present in page

- https://www.novartis.com/careers/career-search/job-details/322964br/defensive-cyber-security-researcher
- https://sjobs.brassring.com/TGnewUI/Search/home/HomeWithPreLoad?PageType=JobDetails&partnerid=13617&siteid=5260&jobid=2739943&AL=1