NOVARTIS

Defensive Security Researcher

Job ID
REQ-10020027
Sep 04, 2024
Israel

Summary

Job title: Defensive Cyber Security Researcher

Location: Tel-Aviv, Israel

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. To execute this mission, the Defensive Cyber Security Researcher will use data analysis, threat intelligence, and cutting-edge security technologies.

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 behavioural 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.
- Leverage threat intelligence and analysis of anomalous log data to detect threat actors.
- 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.
- Analyze network traffic protocols and cryptographic algorithms leveraged by malware

- Produce detailed technical reports in support of malware / other hunting investigations.
- Continuously improve processes for use across multiple detection sets for more efficient IT Security operations.
- Document best practices with the Cyber Security staff using available collaboration tools and workspaces.
- 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.
- In alignment and collaboration with the Forensics team: Provide forensic analysis of network packet captures, DNS, proxy, Netflow, malware, host-based security and application logs, as well as logs from various types of security sensors.

Essential Requirements:

- BA or BSc in Computer Science or a related field experience
- 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 with Security, specifically Azure;
- High familiarity and experience with ENDTRA ID / Azure AD security and Conditional Access Policies
- 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.
- Advanced understanding of cyber threat vectors and countermeasures.
- Familiarity with the current nation-state (“APT”) threat landscape and the various actors and groups.
- In depth knowledge with analyzing disassembly of x86 and x64 binaries.
- Expert in dynamic and static analysis and tools such as IDAPro and Ollydbg.
- Skilled in performing kernel-mode debugging on rookit malware.
- Capable of identifying and defeating malware defense mechanism such as anti-reverse, anti-debug, and anti-virtual machine.
- Possess strong understanding of Windows Operating System Internals and Windows APIs.
- Experience with memory forensics to identify and understand memory resident malware.
- Demonstrated knowledge of Linux/UNIX operating systems.
- Familiarity with YARA, OpenIOC, and STIX frameworks.
- Experience with Snort, Bro or other network intrusion detection tools.
- Detailed understanding of the TCP/IP networking stack & network technologies.
- Very strong team and interpersonal skills along with the ability to work independently and achieve individual goals, with effective oral and written communication skills.
- Coordinate with other team members to achieve the specified objectives, have a high level of documentation and organizational skills, produce detailed technical reports in support of malware / other investigations.

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

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-10020027

Defensive Security Researcher

Apply to Job

Source URL: *https://qa1.novartis.us/careers/career-search/job/details/req-10020027-defensive-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://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Israel/Defensive-Security-Resarcher_REQ-10020027
4. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Israel/Defensive-Security-Resarcher_REQ-10020027