

OPSWAT.

GRADUATE FELLOWSHIP PROGRAM

OPSWAT's Critical Infrastructure Cybersecurity

Program Overview

This immersive and hands-on program provides a unique opportunity for graduate students to study and mitigate real-world cybersecurity vulnerabilities affecting critical infrastructure systems.

As a participant, you will:



Identify and replicate known vulnerabilities in a controlled lab environment, leveraging our OPSWAT Critical Infrastructure Lab's resources.



Develop and test exploits related to these vulnerabilities, gaining insight into hacker tactics and methods.



Produce comprehensive written reports and visual content (video and images) detailing the vulnerabilities, the reasons behind their occurrence, and their potential impact on critical infrastructure.



Scan identified malware and vulnerabilities using OPSWAT's suite of tools, such as the MultiScanner, Deep CDR, Proactive DLP, Sandbox, Neuralyzer, and Vulnerability Scanners, and document your findings.



Create a defense strategy that outlines protective measures against identified vulnerabilities and similar future threats, backed by your hands-on experience and testing results.

Program Structure

The program consists of 6 modules as below:

1 Vulnerability Identification and Replication

- Start with a known vulnerability [to be provided during the program].
- Replicate the vulnerability in OPSWAT Critical Infrastructure Lab.

2 Exploit Development

- Develop an exploit for the identified vulnerability.
- Test and refine the exploit.

3 Analysis and Documentation

- Investigate and document the reasons the vulnerability occurred and its potential effects on critical infrastructure.
- Capture your process and findings through video/ images, and written reports.

4 Scanning and Identification

- Use OPSWAT's MultiScanner, Sandbox, Neuralyzer, and Vulnerability Scanners to scan and identify the malware and vulnerabilities.
- Document your scanning results and analysis.

5 Defense Strategy

- Based on your findings, formulate a strategy to defend against the identified vulnerabilities and similar future threats.
- Write a detailed report and create visual content [diagrams, flowcharts, etc.] to illustrate the defense strategy.

6 Final Presentation

- Compile all your findings, reports, and strategies into a comprehensive document and presentation.
- Present your work to a panel of cybersecurity experts from OPSWAT for feedback and further learning.
- Create video and online material to be published on OPSWAT's and your university's website.

What we offer you?

- By the end of this program, you will gain an in-depth understanding of vulnerability analysis, exploit development, and cybersecurity defense strategies within the context of critical infrastructure. This hands-on experience will be invaluable in helping you build and develop your future career in Cybersecurity. You can include this practical exercise in future Master's and Doctoral Research projects.
- You will have the opportunity to expose and work on OPSWAT's Critical Infrastructure Labs.
- Opportunities to become Intern/FTE of OPSWAT after the program.

Other benefits:

- Monthly allowance (for 3 day working week): gross VND 6,000,000
- Award for individual/team with excellence performance.
- Parking at the office building.
- Enjoy full office facilities, with breakfast & afternoon snacks, as well as other people activities.



What we need from you?

- Final year student or fresh graduate, major in Cybersecurity, IT or Computer Science who have special interest in Cybersecurity.
- Good English communication.
- Quantity: 4-6 members/batch.
- Ability to work in the office at least 3 days/week [Mon-Wed-Fri] for a period of 6 weeks in a row.

Batch 1

from 2 Oct 2023 to 10 Nov 2023

Batch 2

from 4 Dec 2023 to 19 Jan 2024

Batch 3

from 4 Mar 2024 to 12 Apr 2024

Registration

- Application is open from now until 15 September 2023
- Please send your application to recvietnam@opswat.com
- Only shortlisted candidates will be contacted.

Work location

OPSWAT Vietnam Office, 17th Floor, Saigon Giai Phong Building, 436-438 Nguyen Thi Minh Khai Street, Ward 5, District 3, HCMC.



Protecting the World's Critical Infrastructure

OPSWAT is a global cyber security company providing solutions for enterprises since 2002 to identify, detect, and remediate advanced security threats from data and devices coming into and out their networks.

Trusted by over 1,500 organizations worldwide and with over 30 anti-malware engines, 100+ data sanitization engines and more than 25 technology integration partners, OPSWAT is a pioneer and leader in data sanitization, vulnerability detection, multi-scanning, device compliance, and cloud access control.

OPSWAT. Protecting the World's Critical Infrastructure.

