# Synack Managed VDP

## Synack's Managed Vulnerability Disclosure Program

### Why a Managed Vulnerability Disclosure Program?

A Vulnerability Disclosure Program (VDP) has become a basic layer of security infrastructure, allowing organizations to receive vulnerability submissions from the general public. Although VDP is a basic provision, receiving vulnerabilities from public researchers outside of the Synack Red Team (SRT) requires thoughtful implementation and management. Good ethics and security expertise are a critical part of any VDP and you need a trusted partner that can give you the best advice.

## Vulnerability disclosure on your site

Synack will set up responsible disclosure program pages for you so that you can easily create one link to them from your site. Once the link is published anyone can report a vulnerability or issue found on your site or in an application. That submission will go straight to Synack so we can review it and determine if it's a valid vulnerability. If it is valid, it will be reported to you through the platform for review. By default, all researchers who submit valid vulnerability reports through our Managed Vulnerability Disclosure Program will receive public recognition for their findings at client.responsiblediscloure.com. This acknowledgement does not include details about the vulnerabilities, only the names of researchers who wish to be recognized. This recognition can be omitted if the customer so chooses.

## The Synack Difference

High efficiency and ethical standards are built into the core of the Synack model. Synack's managed approach gives the same thorough triage and analysis to every submission and ensures that they are handled promptly and professionally.

## Process Overview

1. Should researchers identify a vulnerability on one of your internet-facing assets, they can learn about your managed vulnerability disclosure program at your VDP web page and submit their vulnerability on client.responsiblediscloure.com. Synack will provide a template to customize and host on your public facing website.
2. Upon submission of the vulnerability, the Synack Mission Ops team will triage it for validity, collaborating with the researcher as necessary. If deemed to be valid, the vulnerability will be submitted through the Synack Managed VDP program and will be made available to you in the Synack Client Portal.
3. Synack will direct the researcher not to disclose the details of the vulnerability publicly until it has been remediated; however, we highly recommend that these vulnerabilities are acted upon with priority in order to reduce the risk of unauthorized disclosure of open vulnerabilities.
4. Once the vulnerability is remediated, Synack will confirm the fix and close the loop with the researcher, thanking them for their submission and authorizing them to disclose the vulnerability publicly. Researchers can track the status of all their submissions at client.responsiblediscloure.com.
5. The researcher will then be listed on the client. responsiblediscloure.com acknowledgments page along with the vulnerability category and CVSS score. No monetary compensation will be provided to the researcher.

**Synack's Managed VDP solution is included as part of Synack security testing engagements.*

## Benefits

Synack strives to provide the highest level of quality possible without inconveniencing clients. We take on the end-to-end management of the program to alleviate your security team's operational burden:

**TRIAGE SERVICES & NOISE REMOVAL**
Complete triage for every vulnerability submission (including validation and thorough analysis) and vulnerability remediation

**END-TO-END OVERSIGHT**
Partner to help make sure that the full life cycle of the vulnerability is taken care of from discovery to remediation.

**RESEARCHER MANAGEMENT**
Managed researcher communications, support, report acknowledgement, and recognition

**VULNERABILITY MANAGEMENT**
Oversee your penetration testing and vulnerability disclosure programs in Synack's integrated platform

**RESEARCHER EXPERTISE**
Harness the security community's global and specialized expertise through providing a means for them to test publicly accessible targets.

**CLIENT WILL:**

- Develop and host content which directs researchers to client. responsibledisclosure.com and covers the program scope
- Review vulnerabilities that Synack has determined to be valid
- Patch and confirm fixes with Synack

**RESEARCHER WILL:**

- Perform testing activities within legal terms and program scope
- Input submissions to responsibledisclosure.com
- Disclose only when given confirmation from Synack
- Provide a customizable VDP template to host on the client's public-facing website

**SYNACK WILL:**

- Assist client in program implementation and scoping
- Manage registration and ongoing communication with researchers
- Triage and hand off valid vulnerabilities to client
- Verify vulnerability remediation after the client has confirmed patching
- Maintain the researcher recognition program

To learn more, please speak with your Synack Security Testing Specialist, or visit https://www.synack.com/contact/ and submit a contact request.