Synack Managed Responsible Disclosure

Why Managed Responsible Disclosure?

Responsible Disclosure (RD) is a process for researchers to submit security vulnerabilities to companies, with clear expectations on both sides. At a minimum, the researcher will not be accused of illegal activity and the receiving company will be responsive in communications. Although RD can be set up in minutes with a web page, an ongoing program that receives vulnerabilities from public researchers requires thoughtful implementation and management. Despite its seeming simplicity, many components of a RD program can lead to reputation loss, financial risk, or worse...

Synack offers Managed Responsible Disclosure (MRD) to best protect our customers from the risks of hidden vulnerabilities lurking in their systems and from the risks of engaging with public researchers to find those vulnerabilities.

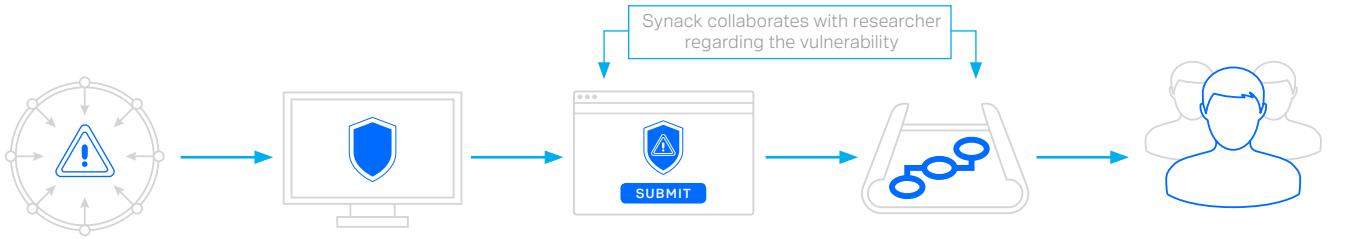
What is MRD and Why Use It?

MRD removes many of the real-world problems RD programs have had in implementation, by managing the researcher-company interaction. Synack protects researchers from inexperienced companies and protects companies from demands from researchers. Synack's managed approach seeks to avoid any and all moral hazard by clearly offering no bounties and setting clear, simple expectations. No Synack MRD client awards money themselves, or even interacts directly with the researchers—keeping them safe from blackmail attempts. Every vulnerability submitted through a Synack MRD program receives the same attention and goes through the same professional process as those submitted by the Synack Red Team.

How Does MRD Work?

Synack will set up responsible disclosure program pages for you that can be easily linked to 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 on the Synack Client Portal for review. All researchers who submit valid vulnerability reports through our Responsible Disclosure program will receive public recognition for their findings at client.responsibledisclosure.com.

Process Overview



Researcher discovers vuln on client public site

Researcher visits client's Responsible Disclosure Page

Researcher is directed to client.responsible disclosure.com to submit vulnerability

Vulnerability is triaged by Synack and submitted to client through Synack Client Portal

Vuln is addressed by client and researcher is recognized on client.responsibledisclosure.com

Benefits

Synack strives to provide the highest level of quality possible without inconveniencing clients:

- **Program Setup & Maintenance:** Full program implementation, including content for your disclosure website, asset scoping, and researcher recognition.
- **Protection:** Synack handles all communication with researchers and determines the value of each responsible disclosure report. The buck stops at Synack.
- **Researcher Management:** Managed researcher communications, support, report acknowledgement, and recognition. *Note: Synack clients can always communicate with researchers directly for clarification.*
- **Triage Services:** Complete triage for every vulnerability submission (including validation and thorough analysis) and vulnerability remediation.
- **Centralized Reporting:** Notification of valid vulnerability reports in the Synack Client Portal

Roles and Responsibilities

Synack will:

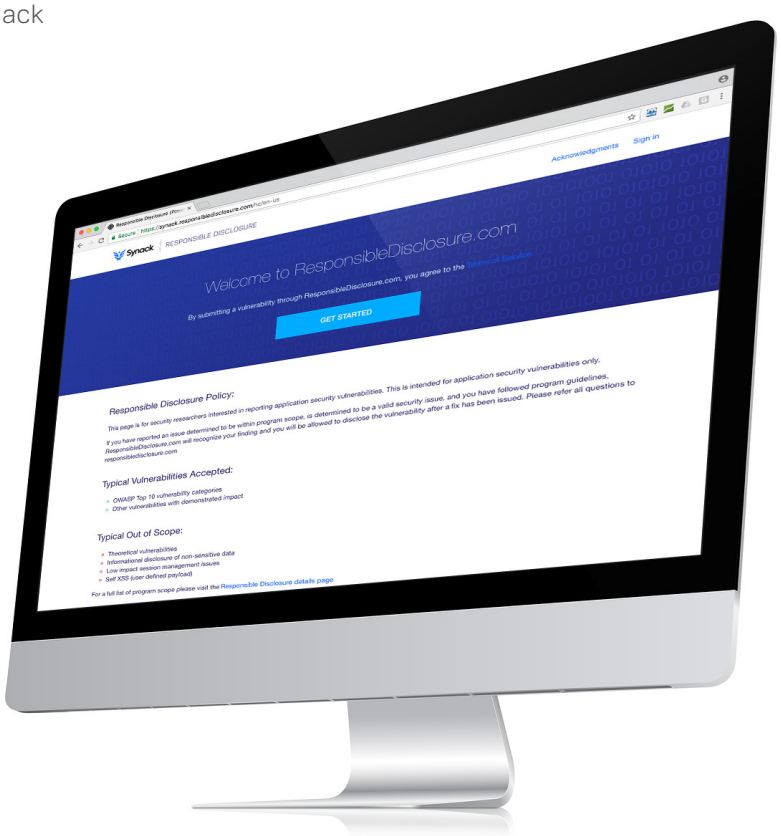
- Provide a customizable Responsible Disclosure template to host on the client's public-facing website
- Assist client in program implementation and scoping
- Manage registration and ongoing communication with researchers
- Triage and hand off valid vulnerabilities to client
- Verify vulnerability remediation after the client has confirmed patching
- Maintain the researcher recognition program

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



Synack, Inc.

855.796.2251 | www.synack.com | info@synack.com