Intigriti's triage services explained

Intigriti's triage services explained

Intigriti leverages its experienced team of security analysts to validate and prioritize every finding that is submitted to our platform. With our focus on quality over quantity, we promise an extremely competitive triage lifecycle for clients.

Intigriti's triage team at a glance

1h

is the average amount of time it takes our triage team to respond to researcher questions, allowing them to continue their work and deliver reports to clients more quickly.

24h

is the time it takes on average for Intigriti to review, and accept or reject a vulnerability report.

41%

of ethical hackers who choose not to, or prefer not to, work with companies outside of a bug bounty platform cite the lack of a triage department as the biggest reason.

$**71.7**M

is the total cybercrime costs saved to date based on the average cost of a data breach (USD 4.24million, according to IBM) and total number of triaged reports by Intigriti.

9.2NPS

is the Net Promoter Score that reflects our triage team's swift, fair, and personal approach to triaging.
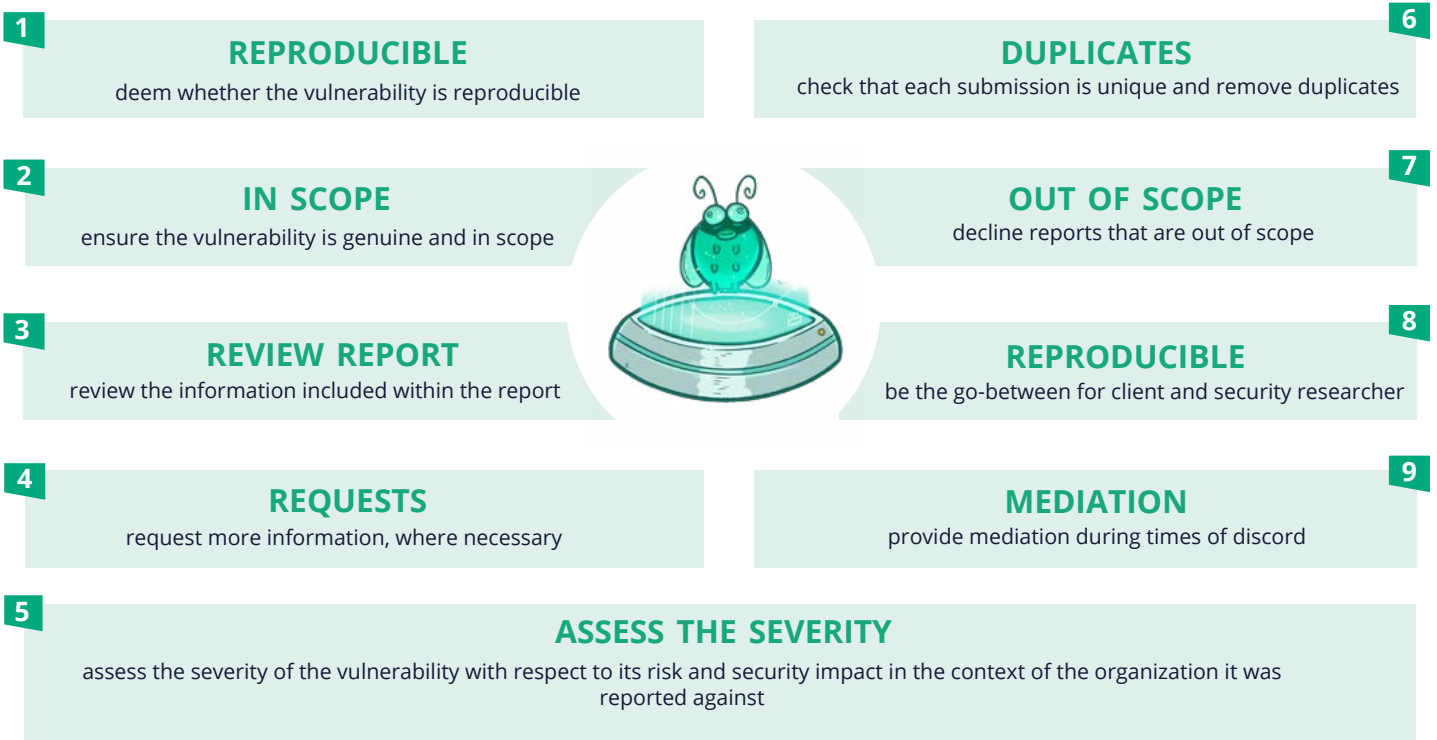
How Intigriti triaging services work

Intigriti bug bounty programs offer triage services by default. This security validation process is executed by our in-house security analysts and ensures clients only receive valid, unique and in scope vulnerability reports.

Steps Intigriti's triage department takes before escalating reports to clients:

1 REPRODUCIBLE
deem whether the vulnerability is reproducible

6 DUPLICATES
check that each submission is unique and remove duplicates

2 IN SCOPE
ensure the vulnerability is genuine and in scope

7 OUT OF SCOPE
decline reports that are out of scope

3 REVIEW REPORT
review the information included within the report

8 REPRODUCIBLE
be the go-between for client and security researcher

4 REQUESTS
request more information, where necessary

9 MEDIATION
provide mediation during times of discord

5 ASSESS THE SEVERITY
assess the severity of the vulnerability with respect to its risk and security impact in the context of the organization it was reported against

> I really like the method for submitting reports on Intigriti. First, it's Intigriti's triage team who test and approve the report before they send it to the client. This is important because I know that, if it is passed along to the client, I'm sending across a good vulnerability. From the client-side, this step is valuable because they know they aren't about to have their time wasted.

Kuromatae
Intigriti Cybersecurity Researcher

> The most impact we have experienced from working with Intigriti is the extra time that my security team gets back from not triaging reports. What I also appreciate about Intigriti is the feeling that the customer comes first — it is an open and collaborative relationship where we share a common goal to mitigate found vulnerabilities.

Thomas Colyn
CISO - DPG Media

About Intigriti

Agile testing powered by the crowd

Intigriti's bug bounty platform provides continuous, realistic security testing to help companies protect their assets and their brand. Our community of ethical hackers challenge our customers' security against realistic threats — we test in precisely the same way malicious hackers do.

50,000+ researchers
More than 50,000 security researchers use Intigriti to hunt for bugs — and we're growing!

400+ live bug bounty programs
Companies of all sizes, and across multiple industries, trust Intigriti to launch their bug bounty program.

GDPR compliant
We ensure compliance with the highest security standards.

Strong European presence
In terms of hacker pay-outs, 8 out of 10 of the best performing countries are European. However, Intigriti is very much a global business. In 2020, vulnerabilities were submitted from more than 140 countries.

TAKE YOUR FIRST STEPS

- Request a demo www.intigriti.com/demo
- Visit the website www.intigriti.com
- Get in touch hello@intigriti.com

How vulnerability management works on Intigriti

Researcher **searches** for a **vulnerability**

Researcher **submits** a **report** via Intigriti

Intigriti's **triage** begins **communication** with researcher

Intigriti's **triage** team applies **quality assurance** steps

In-scope, unique and well-written **reports** are **submitted** to client

Client accepts report, and **payment** is **automatically** processed

You're in good company

A vulnerability reported and fixed is one less opportunity for a cybercriminal to exploit. Ready to talk about launching your first bug bounty program? We're here to help you launch successfully.

Speak to our team today.