

{retrospect_labs}

Gauntlet

Deliver realistic and meaningful cyber exercises on-demand with Gauntlet, our modern cyber security exercise platform

Sales deck
info@retrospectlabs.com



**Build Readiness.
Respond Effectively.**





The problem

Organisations not ready to respond to cyber incidents will experience **significant negative impacts** that should have been avoided.

Frequent cyber exercises prepare organisations but are a **high burden** to design and execute. Actions and decisions are hard to capture, resulting in **loss of insights** and **subjective evaluations**.

“

Data breach costs rose from USD 3.86 million to USD 4.24 million, the highest average total cost in the 17-year history of this report.

IBM Security
Cost of a Data Breach Report 2021

”

{retrospect_labs}

Meet Gauntlet

The solution - our modern cyber security exercise platform enabling organisations to continuously deliver meaningful cyber exercises

Gauntlet is a **Software-as-a-Service** application, meaning it's immediately accessible. Team members can participate in cyber exercises from any location.

The screenshot displays the Gauntlet interface for a team named 'APT 27001 Crouching Tiger Hidden Auditor'. A vertical sidebar on the left contains navigation icons, including a profile icon with the initials 'JP'. The main content area features a timeline of exercises:

- Sat 21 Nov 06:31: 1 Something phishy is going on...
- Mon 23 Nov 15:45: 2 Fake News! (highlighted)
- Tue 24 Nov 16:22: 3 Stolen Data
- Wed 25 Nov 18:16: 4 Build the picture
- Thu 26 Nov 08:55: 5 Exercise Completed

The detailed view of the 'Fake News!' exercise shows a tweet from AusCyberNews (@AustralianCyberNews) posted on 10 Nov 2019 at 10:05PM. The tweet text reads: 'Someone is selling @intergalactic web... #spacehacked'. Below the text is a redacted image with the text 'TOP SECRET // PROJECT B' and a logo for 'INTERGALACTIC AERONAUTICS'. The tweet has 320,367 retweets and 93,729 likes.

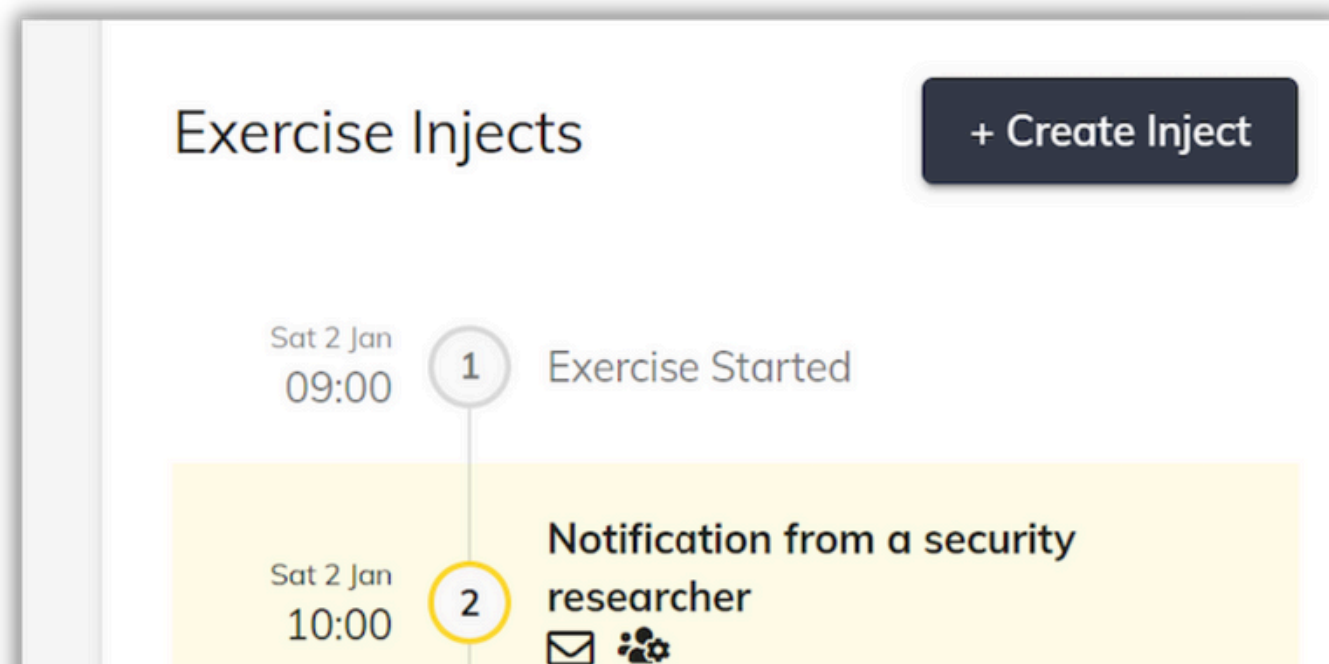
The image in the report appears real and extremely s

{retrospect_labs}

Gauntlet overview

Gauntlet has successfully delivered thousands of cyber exercises for Governments and critical infrastructure providers.

There are only three steps needed to deliver an effective cyber exercise from start to finish.



1. Design

Create the exercise from scratch or use a template. Set the objectives and once ready, send out the invites.

2. Execute

Start the exercise. Participants respond to the scenario with Gauntlet capturing their actions and decisions.

3. Assess

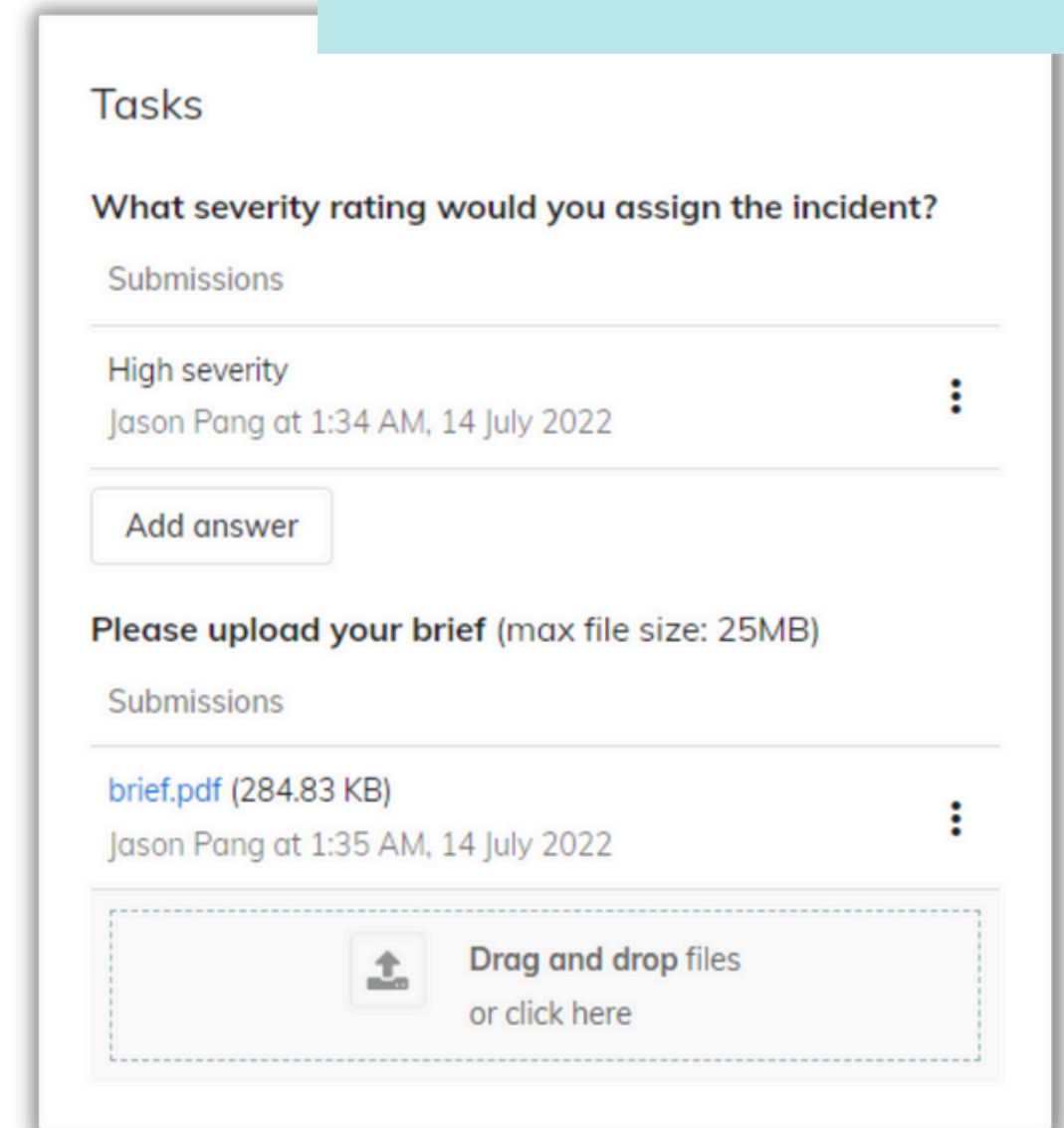
After the exercise has ended, view all the collected data to see how the team performed against the objectives.

{retrospect_labs}

Key features

- **Exercise mode** - Facilitate or let participants drive exercises independently
- **Tasks** - Give tasks to participants like questions to answer or files to upload
- **Objectives** - Set objectives per exercise, and mark them off when completed
- **Templates** - Use our templates to quickly create and run exercises
- **Collect emails** - Capture relevant emails by cc'ing the exercise's inbox
- **Personas** - Practice communicating with external entities like regulators
- **Exercise summary** - Understand everything that happened during the exercise

Use task submissions to uncover why certain decisions were made



Tasks

What severity rating would you assign the incident?

Submissions

High severity
Jason Pang at 1:34 AM, 14 July 2022

Add answer

Please upload your brief (max file size: 25MB)

Submissions

brief.pdf (284.83 KB)
Jason Pang at 1:35 AM, 14 July 2022

Drag and drop files
or click here

Key roadmap items



Case management integration

Starting with Jira, capture case data created during the exercise.

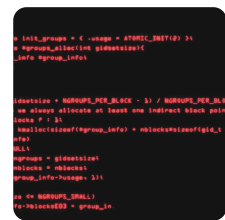
Other planned case management integrations include: TheHive, ServiceNow, Cydarm



Dashboard and visualisations

Creation of dashboard and visualisations to gain better insights.

Metrics and statistics at the organisation, team, and individual level.



Purple team capability

Enable purple team style exercises by capturing both red and blue team activities.

Understand actions of blue team in response to the red team's activities.



Virtualised applications

Spin up virtualised application that complements the scenario or supports the participants.

This can include forensic workstations, case management tools, and phishing sites.

{retrospect_labs}

Thank You!

We are passionate about cyber security exercises and helping organisations build their incident response readiness and minimise the damage incidents can cause.

Please reach out if you are interested in learning more about Gauntlet or cyber security exercises.

✉ Contact

info@retrospectlabs.com

🌐 Website

retrospectlabs.com

🌐 LinkedIn

linkedin.com/company/retrospectlabs

