



A digital marketplace where you can

Unzip a BUG, Earn the TRUST

What is Bug Bounty?

A **basic and initial step** to explore cyber vulnerabilities



A crowdsourcing initiative **connects** like-minded cybersecurity talents (“bounty hunters”) to facilitate sharing **high quality** cyber advice for enterprises



A **reward** to bounty hunters who can find security loopholes (“bugs”)



Allow to discover and resolve bugs **before** the public aware the threat

Why Cyberbay Bug Bounty is safe & reliable?

Build trust among bounty hunters and enterprises through **governance**



Enforcement of **Know Your Client ("KYC")** in sign up process to verify bounty hunters' identity



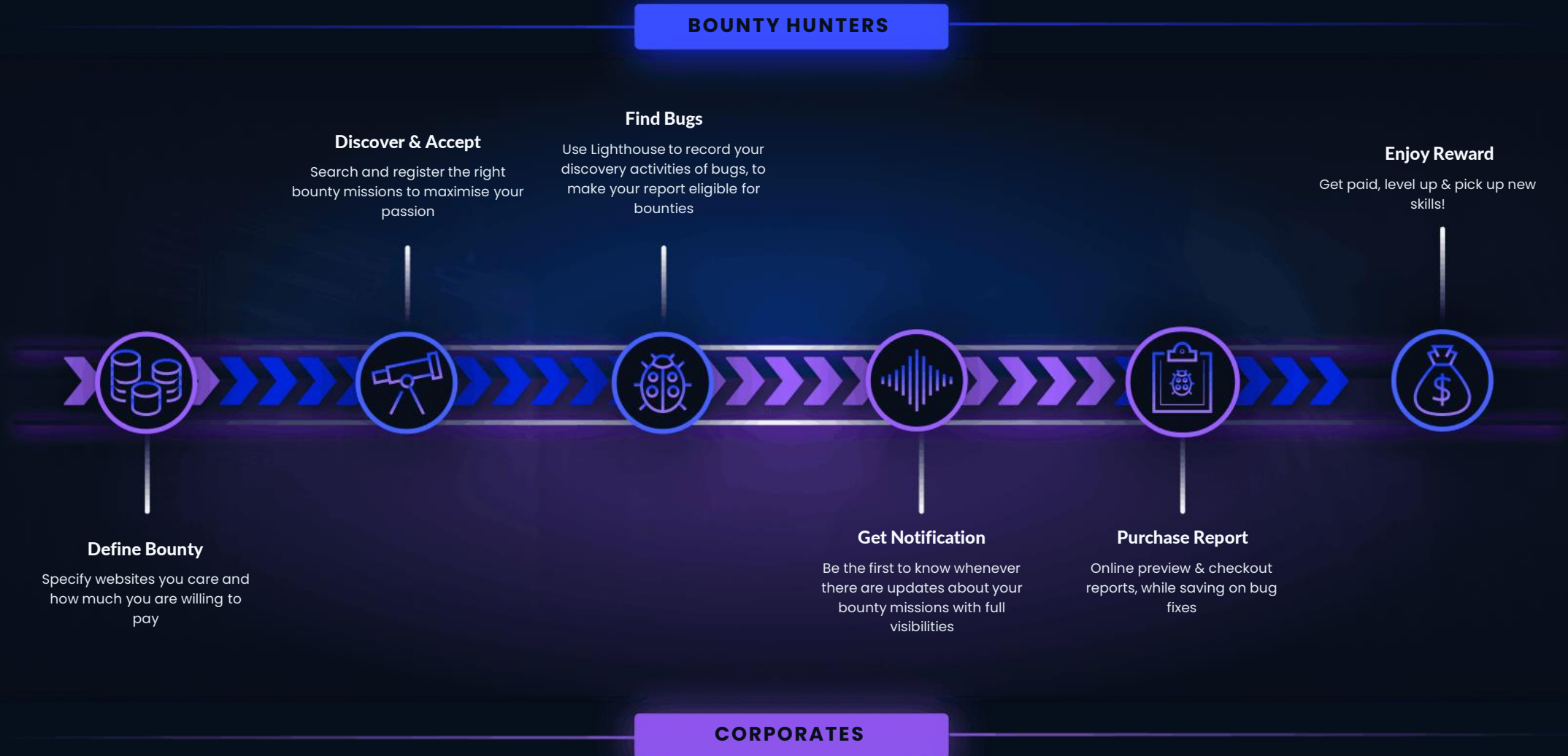
Inspection can only be conducted **after enterprise acknowledgement**



Intelligence "Lighthouse" technology to **24/7 monitor** bounty hunter activities in assessment process

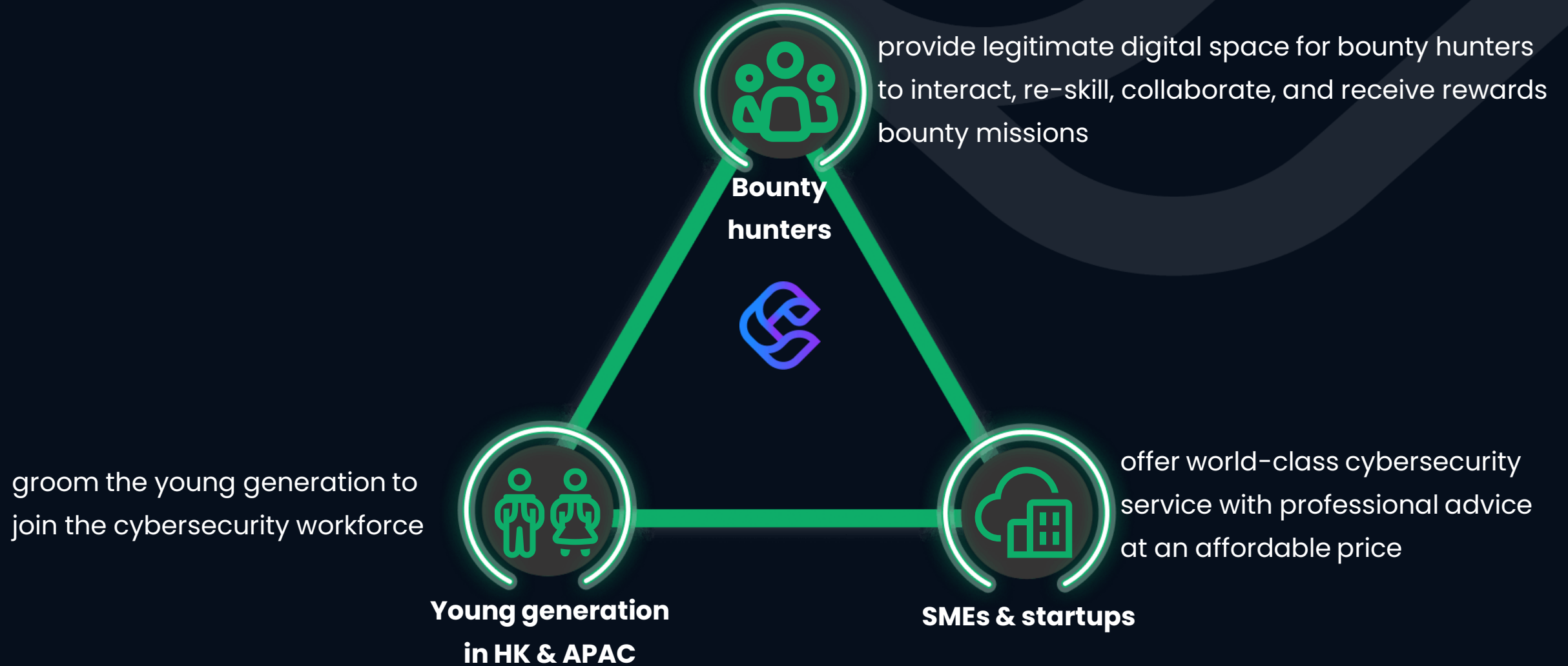
How we work?

Create a **transparent and high quality cyber advice** between bounty hunters and enterprises with mutual trust



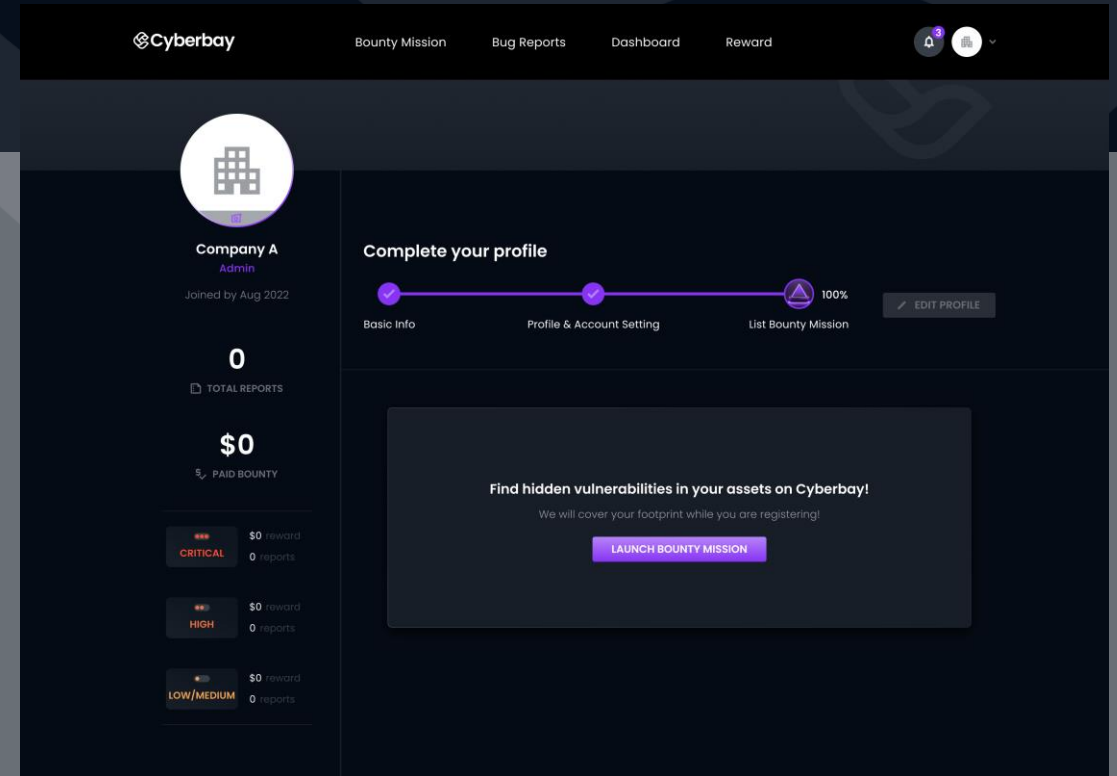
Creating a bug free cyber ecosystem

The 1st **digital crowdsourcing and C2B bug bounty marketplace** founded in Hong Kong and Asia Pacific



As a corporate user, you will experience...

Onboarding in 3 minutes



As a corporate user, you will experience...

Threat intelligence to define your bounty

The screenshot displays a web application interface for defining a bounty. At the top, a banner reads "Hello, Admin". Below this, a purple notification box states: "Verify your new website/app. Please return to the profile page to verify your new website/app."

The main section is titled "Bounty Details" and includes a sub-header: "The information you provide will help inform bounty scope and help us identify the right skills and experience among the bounty hunters to ensure maximum bounty value."

The form contains several input fields:

- Bounty Title**: A text input field.
- Date Range**: Two date input fields (DD/MM/YYYY) with a "to" separator.
- Time Range**: Two time input fields (00:00 in GMT+8 to 23:59 in GMT+8) with a "to" separator.
- Target URL**: A text input field containing "www.cyberbay.tech" and a "Select Asset Type" dropdown menu.

A list of target URLs is displayed below the input fields, with checkboxes for selection:

- ☐ Select All
- ☒ www.cyberbay.tech
- ☐ forum.community.cyberbay.tech
- ☒ career.cyberbay.tech
- ☐ about.cyberbay.tech

At the bottom, a summary shows "Currently Selected" (www.cyberbay.tech, career.cyberbay.tech, about.cyberbay.tech) and "Total Selected 3".

On the left side, there are two informational boxes:

- Bounty Title**: Descriptive name for the bounty program such as the name of your company or the application that is being tested.
- Looking for other service?**: We don't cater Internal App or IOT at this moment, if you are looking for other service, please contact us by hello@cyberbay.tech

On the right side, there is a box for **End Date**: The end date in date range field is optional.

As a corporate user, you will experience...

Full control on how / when for payments

2

❏ Spending Limit

Set a maximum reward that your organization would pay for an exceptional submission.

❏ Critical Reward

Critical error, flaw, fault, or problem impacting business with direct reputation, operation, finance and litigation damages.

❏ High Reward

High severity error, flaw, fault, or problem impacting system confidentiality, integrity, or availability.

❏ Low/Medium Reward

Generic error, flaw, fault, or problem that impacts one of functionality, performance, usability, or security.

Reward Setting

Guide to set amount.

Spending Limit

per bounty

\$100,000

CRITICAL

per bug

\$50,000

MAX HKD 1,000,000

AVG. \$5,000

HIGH

per bug

\$3,500

MAX HKD 1,000,000

AVG. \$3,000

LOW/MEDIUM

per bug

\$10,000

MAX HKD 1,000,000

AVG. \$1,000

CANCEL

SUBMIT

As a corporate user, you will experience...

Zero upfront cost: No bug, no pay

The screenshot displays the Cyberbay bug bounty platform interface. The top navigation bar includes the Cyberbay logo and links for Bounty Mission, Bug Reports, Dashboard, and Reward. The main section is titled 'Reports' and shows a list of bug reports. The reports are filtered by 'AVAILABLE' (10), 'PURCHASED' (6), 'RETEST' (2), and 'ALL' (18). A search bar is present with the text 'Search by website domain'. The reports are sorted by 'Severity: High to Low'. The list shows several 'Critical information disclosure' bugs, all with a 'NEW' status and a 'CRITICAL' severity. The bugs are listed with their URL (https://cyberbay.tech) and DATE (13 Oct 2022). On the right side, a summary table shows the total amount for the selected reports (3 report selected) and a 'PURCHASE' button.

Report Description	Amount
Critical information disclosure	HKD11,500
Search is not triggered when clicking the search button	HKD7,000
Bug capable of collapsing large parts of the system	HKD3,500
Total Amount:	HKD22,000

PURCHASE

Shaping the future of cybersecurity

Crowd sourcing model: **VDP (vulnerability disclosure programme)**



Eligibility of scope
& approach



Program declaration
& ownership



Recognition / Hall
of Fame



Gift / Rewards

Thank you!

Make digital transformation **easier and safer** for everyone

