bugcrowd

Live hacking events

Everything you need to know

What is a live hacking event?

Live hacking events are multiday virtual or in-person events that bring hackers together to find priority vulnerabilities for our customers.

Live hacking events attract and engage some of the best hackers in the world. They foster positive, real-time engagement that benefits everybody involved.

Eight benefits of hosting a live hacking event

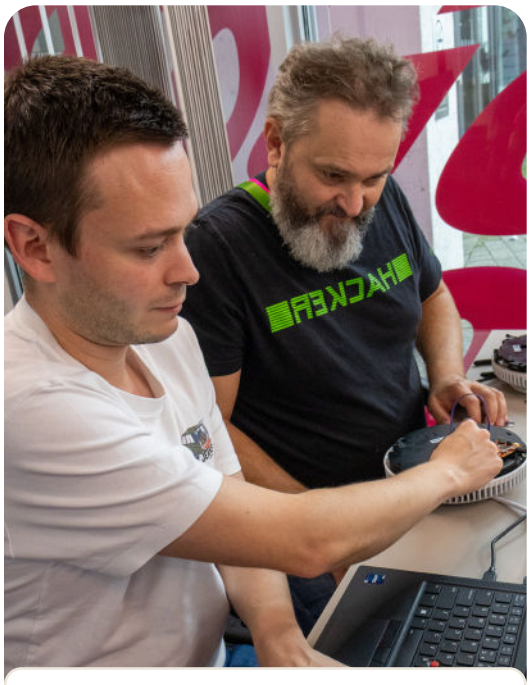
Live hacking events give organizations a concentrated, high-intensity burst of expert testing that's hard to replicate any other way. The main benefits are as follows:

1 Faster, higher-quality vulnerability discovery

A single live hacking event typically generates 200+ reports, with 85% being valid submissions and roughly 30% rated as critical or high impact. Organizations have also seen a 50% increase in critical findings in the six months following an event, suggesting that an event has a lasting effect on program quality.

2 Access to vulnerabilities a standard program might miss

At Indeed's first live hacking event, over 63% of the vulnerabilities found were net new, even though Indeed had already been running a bug bounty program for some time. For the State of Maryland's Department of Information Technology, the diversity of hackers at its live event surfaced findings that a traditional penetration test—which tends to use the same testers and techniques year after year—would be unlikely to catch.



3 Coverage for assets that can't be tested remotely

In-person events let hackers get hands-on with hardware, physical infrastructure, and other assets hackers can't access remotely. T-Mobile has specifically cited this as a reason for hosting Bug Bashes at facilities like its Tech Experience 5G Hub. Deutsche Telekom's Bug Bash similarly let hackers physically test 5G equipment in a controlled, closed-network environment.

4

Stronger relationships with elite hackers

In-person collaboration lets hackers work side by side with internal teams, share techniques, and chain vulnerabilities in ways that are difficult to accomplish asynchronously. T-Mobile has asserted that "in-person collaboration yields optimal results." Hackers at Maryland's first live event began combining specialized skills together by day two, despite arriving independently.

5

A proof point for leadership

Live events give security teams a concrete, visible way to demonstrate program value and build internal support for continued investment in preemptive security testing.

6

Community and hacker loyalty

An invitation to a live hacking event is seen as a significant achievement by many hackers, which helps companies attract and retain top talent for their ongoing programs. The hackers who attend often become experts in that company's attack surface, making them an incredibly valuable resource for future testing and complex bug discovery.

7

Coverage for assets that can't be tested remotely

Deutsche Telekom's Bug Bash brought T-Mobile US and Ericsson on-site specifically because these companies share similar equipment and infrastructure. This kind of event creates a chance to collaborate on shared challenges across an industry, not just a single company's assets.

8

Learning opportunities for internal teams

nternal blue teams or defensive teams often join live hacking events as an opportunity to see beyond an alert. It's a great chance for them to see the attacker mindset up close, ask questions, and understand hacker workflows.

What are the different types of live hacking events?

There are four types of live hacking events, each suited to a different scale, sensitivity level, and goal.

Event type	Best for	Typical scope
Virtual	An introductory, lower-cost way to prove out live testing or a lead-up to an in-person event or hacker workshop	Web, AI, crypto
Live in the Loop	Sensitive business units or highly specialized skill sets (like social engineering) where a smaller, curated hacker group and tighter access controls matter more than scale	Web, crypto, hardware, AI, social engineering
Bug Bash	A flashier combination of a marketing moment and on-site test, with a larger, more open scope to draw the maximum number of hackers	Web, hardware
ReCON	Large-scale, community-focused events with multiple tracks, talks, and deep collaboration between the customer, Bugcrowd, hackers, and sometimes other vendors	Web, hardware, AI

A few notes on how these differ in practice:

Virtual events don't require an open scope. They're a good way to let top hackers test a specific new feature or product line before it's added to your main program scope.

Bug Bash events default to a larger, more open scope specifically to maximize the number of hackers who can participate (generally 10 or more and up to roughly 50).

Live in the Loop applies the principle of least privilege; smaller, more specialized hacker groups get access to more sensitive targets, which keeps the signal-to-noise ratio high and minimizes incidents.

ReCON events can also be run across multiple customers as shared, sponsored functions and are typically treated as annual flagship events rather than recurring products.

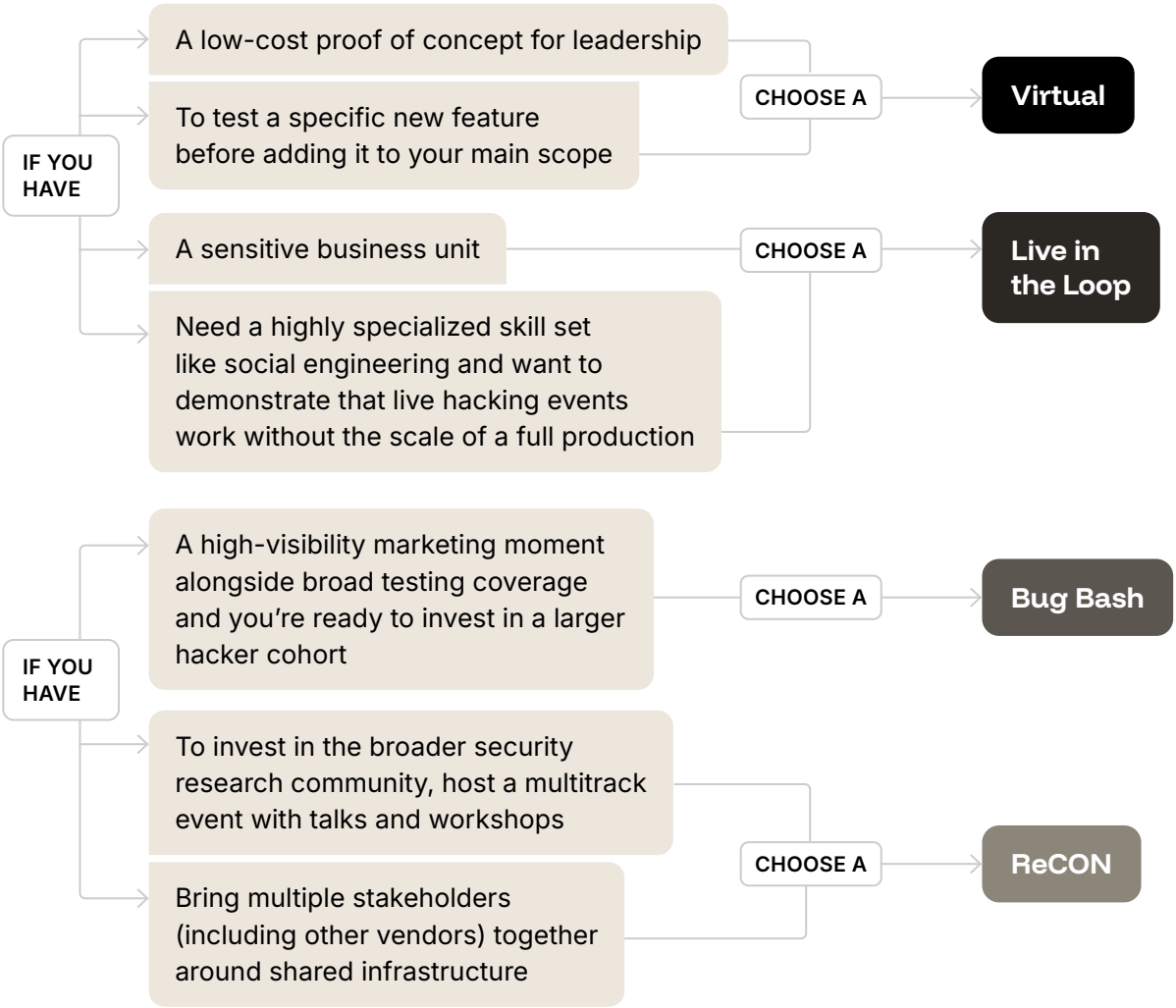
How do I know what type of live hacking event is right for me?

The right event type depends on three things: your customer segment/tier, the maturity of your existing bug bounty program, and your specific goal for the event.

Program maturity requirements:

- **Virtual:** No existing program required.
- **Live in the Loop:** Existing bug bounty program for at least 6 months.
- **Bug Bash:** Existing bug bounty program for at least 1 year.
- **ReCON:** Existing bug bounty program for at least 1 year.

Match the event to your goal



How do I determine the scope for the event?

Experts at Bugcrowd will help your team determine the scope for your live hacking event. Scope should be driven by two factors: **what you actually need tested and how sensitive that target is.**

→ Match your scope to the right event format

Web, AI, and crypto targets are well suited to Virtual events. Hardware, operational technology (OT), and social engineering require a Live in the Loop or Bug Bash, since hackers need physical or in-person access. ReCON events typically cover web, hardware, and AI targets, given their scale.

→ Understand the hacker and timeline commitment by asset type

Asset type	# of hackers	Recon time	Testing time
Web	50–100 (Virtual)	1 month	2 days
	5–10 (Live in the Loop)		
	30–50 (Bug Bash)		
AI	25+ (Virtual)	1–2 months	2 days
Crypto	10+ (Virtual)	1–2 months	2 days
Hardware	5–10 (Live in the Loop)	1–2 months	4 days
	10–15 (Bug Bash)		
Social engineering	3–5 (Live in the Loop or Bug Bash)	6 weeks	3–4 days
OT	5–10 (Live in the Loop)	2 months	4 days
	10 (Bug Bash)		

→ Weigh open scope against specialized scope

A wide-open scope lets you invite the maximum number of hackers, which is the default approach for a Bug Bash. A narrower, more specialized scope (used for sensitive business units or niche skill sets like social engineering) trades some scale for a better signal-to-noise ratio and tighter access control. As a rule, you can scale a Live in the Loop event up toward Bug Bash territory if needed, but a Bug Bash generally can't be scaled back down, since its cost and operational structure assume a larger footprint.

How much lead time do I need for a live hacking event?

EVENT TYPE	Virtual	Live in the Loop	Bug Bash	ReCON
LEAD TIME	4–6 weeks*	3+ months	3+ months	3+ months
TESTING TIME	2–4 weeks **for engagement building and hacker sourcing*	Varies by scope	Varies by scope	Varies by scope

How much should I budget for a live hacking event?

Live hacking events range in cost. The budget has two components:

The hacker reward pool + **The event production cost**

Event costs generally cover hacker and staff travel, food and beverage, venue, custom swag, on-site operational support, and priority triage. Costs scale up with the size of the hacker cohort and the complexity of on-site logistics (for example, hardware or OT testing requires more specialized setups than a standard web-focused event).

Event costs start at around $40,000 for **virtual** events.

Live in the Loop events range from $100K to $200K.

Bug Bashes range from $200K to $300K.

ReCON events start at $350K.

Live hacking event customer testimonials

"Having Bugcrowd's Platform and team behind us meant we could focus on building the right program for Maryland. The infrastructure and expertise were already there."

"There's a fear of, 'What happens when we do this? What happens when we find out?' But ignorance isn't bliss. You want to know where the problems are."

Steve Kain, Director of Adversary Emulation, Maryland Department of Information Technology

"The energy is super high, the researchers love it, and the targets are amazing. The Deutsche Telekom team especially has been out of this world, and I cannot wait to come back and do it again."

Alex Naranjo, Manager, Cybersecurity, T-Mobile

"Sure, we have pentesters, labs, and a red team that challenges our infrastructure and services every day of the week. In terms of technological leadership, we must not rest on our laurels. That's why we highly value external help based on Responsible Disclosure and treat security researchers from all countries with a lot of respect."

Thomas Tschersich, CSO, Deutsche Telekom & CEO, Deutsche Telekom Security GmbH

"The value of adding hacking into our security solution is the fact that we're doing offensive security and finding these vulnerabilities before a bad actor can exploit them."

Dominique DeVaux Jeffords, Sr. Manager of Cyber Resiliency and Portfolio Management, T-Mobile

"Ericsson is proud to support the T-Mobile Bug Bash event by providing our state-of-the-art 5G equipment. This initiative reflects our commitment to strengthening cybersecurity and driving innovation in the 5G ecosystem."

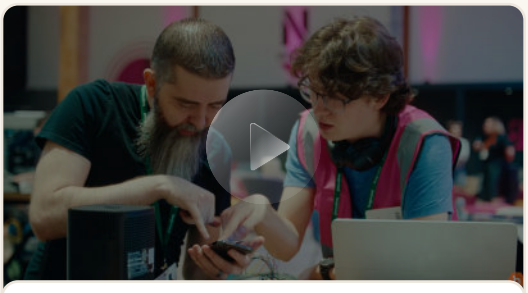
Andreas Blank, Head of Customer & Solution Security, Ericsson

"Indeed's Security and R&D teams were impressed by the results of our first Bug Bash event with Bugcrowd's global community of security researchers. With the help of the Bugcrowd community and platform, we've been able to continue strengthening our security posture and work together to protect the information of job seekers and employers."

Anthony Moisant, Chief Security Officer and Chief Information Officer, Indeed

See what Bug Bashes look like in action and meet the hackers in these recap videos!

Bugcrowd Live Hacking Event in Las Vegas ↗



Bugcrowd Live Hacking Event in Seattle ↗

Ready to host your own?

Live hacking events give you a concentrated, high-impact way to accelerate vulnerability discovery, build lasting relationships with elite hackers, and prove the value of your security program to leadership, all without replacing the bug bounty program or VDP you already rely on for continuous coverage.

Request a quote to find the right live hacking event for your organization and our team will help you scope, budget, and schedule an event tailored to your goals.

Request a demo