Why Crowdsourced Security?

Crowdsourced Security is a powerful tool – used by leading edge firms such as Google, Apple and Facebook – to decrease risk. However crowdsourced security is not yet well understood across the enterprise security community. This brief will define crowdsourced security and describe why it's a key element of any viable security architecture.

There is a fundamental imbalance between the creativity and motivations of cyber attackers, and those of enterprise security defenders.

Crowdsourced security eliminates this imbalance by harnessing whitehat security researchers to find and eliminate vulnerabilities.

Crowdsourced security provides focused results to support rapid risk reduction, cost control, and lower operational overhead.

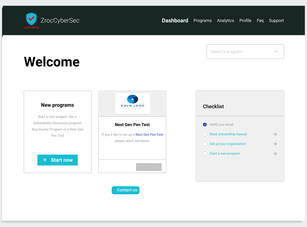
Partnering with an established crowdsourced security platform largely eliminates overhead and maximizes risk reduction.

Crowdsourced security supports the most critical attack surfaces: web and APIs interfaces on server/cloud, mobile and IoT platforms.

Highly vetted, trusted security researchers and private programs diffuse concerns of risk associated with crowdsourced security.

How it works

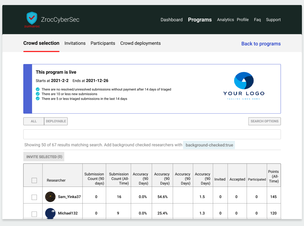
Crowdsourced Security: A Human-Based Approach to Risk Reduction



Define

Design Your Program

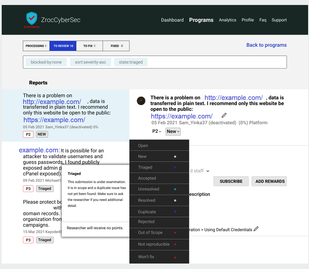
You define the attack surfaces you need to harden, for example web application front ends or a mobile application.



PUBLISH

Connect to The Crowd

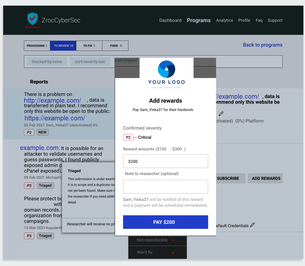
Depending on the type of program, you either publish the program broadly to the researcher community, or engage a more limited set of researchers in a private "invite only" program.



TRIAGE

Find Vulnerabilities

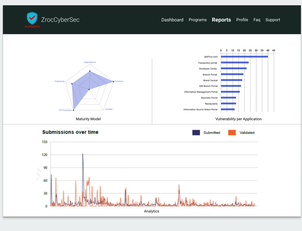
As vulnerabilities are uncovered by the researchers, they are triaged to determine validity and severity.



REWARD

Incentivize Results

You pay a reward (or grant public "kudos") to the researcher for finding the problem, patch the vulnerability, and verify that the attack vector has been closed.



Analytics

Measure KPIs

Zumaroc analytics and key performance indicators can be used to help measure your organization's vulnerability coordination & manage bug bounty programs.

WHY IT WORKS

True Risk Reduction

Rewards are tied to successful outcomes — finding vulnerabilities you need to know about.

Speed

The first hacker to find a vulnerability is rewarded, encouraging hackers to work quickly.

Value

The more critical the vulnerability found, the bigger the reward to the hacker, driving better value.

WHERE IT WORKS

Web Front-End · API · X86 Server /Cloud · Mobile · IoT

Crowdsourced security supports today's key attack surfaces, on all key platforms, as well as "the unknown." As organizations move to cloud architectures and applications, the biggest concerns are web application front ends and APIs, which may be deployed on IoT devices, mobile apps, or on-prem/cloud. All of these can be evaluated for risk by crowdsourced security. Furthermore, a public crowd program can uncover risk in areas unknown to the security organization, such as shadow IT applications or exposed perimeter interfaces.

Using crowdsourced security lowers security costs and operational overhead. There is no agent software on applications or clients, and no software instrumentation to support. There are no network devices or virtual appliances to install and manage. There is also little to no operational waste caused by false positives or low-priority events. As security budgets come under increasing scrutiny, crowdsourcing becomes an obvious choice for simultaneously controlling costs while still aggressively protecting the business.

EXPLORE OUR OFFERINGS

Penetration Testing

Crowdsource human intelligence at scale to discover high-risk vulnerabilities faster.

Bug Bounty

Take a proactive, pay-for-results approach by actively engaging with the Crowd.

Vulnerability Disclosure

Meet compliance and reduce risk with a framework to receive vulnerabilities.