Bug Bounty Program

Our security experts assist you in setting up, operating and organizing a Bug Bounty Program. We support you with our expertise - from the planning of the assessment scope to the review, examination and prioritization of incoming vulnerability reports.

Basics of the Bug Bounty Program

The goal of a Bug Bounty Program is to identify vulnerabilities before they can be exploited. The program allows your company to take advantage of the know-how and the inventiveness of a community of security experts. To this end, the community is invited to analyze a predefined area of your company for vulnerabilities. The rules to which the community must adhere during the program are defined in advance by your company. The discoverer of a vulnerability receives a reward that depends on the criticality of the vulnerability found.

Bug Bounty Platforms

A provider of Bug Bounty platforms provides the expertise of the connected community of security experts. The rules are clearly defined and vulnerability reports are only exchanged via the platform. This ensures that the vulnerabilities are communicated to the company in a coordinated and secure manner. Bug Bounty programs can also be implemented independently from platforms and without using a central platform. Communication and coordination with the security experts is carried out by the company itself.

How You Benefit from Our Service

In order for the Bug Bounty Program to be effective and free of unnecessary restrictions, it must be tailored to the needs of the company and take organizational structures into account. As a full service provider, we have the necessary expertise to determine the scope of the assessment together with you. We have experience in working with leading providers of Bug Bounty platforms and communicate with the community of security experts on your behalf. The vulnerability reports are reviewed and prioritized by our security experts. Upon request, we will support you in eliminating identified vulnerabilities.

Price

The scope of this service is determined individually. It depends, for example, on the desired support during the Bug Bounty Program. Please contact us. We will be happy to make you an individual offer.

How We Proceed - Phases

Our approach is individually tailored to your needs and adapted to the project phase. The procedure below can be regarded as exemplary.

Kick-Off

The preparation takes place during a kick-off meeting with your company's technical and organizational personnel. We will discuss your initial situation and your objectives as well as the type of reward you would like to offer. Together with you, we determine the next steps according to your requirements, resources and circumstances.

Concept Development

During the concept development phase, we clarify with you to what extent the internal specialist departments are involved and which interfaces are available. Together with you, we determine the scope of the assessment, the guidelines for Responsible Disclosure and the handling of incoming vulnerability reports from the community. We also define communicative processes and escalation channels. If desired, we integrate communication channels into your internal ticket system.

Optional Evaluation

If desired, our security experts analyze the defined testing scope using a pentest or code review before the bug bounty program launches.

Program Launch

Together with our security experts, the Bug Bounty Program is launched. Depending on the defined process, the incoming reports on identified vulnerabilities are validated and prioritized by our security experts. We take over the communication with the community and forward all identified vulnerabilities to the specialist department. The reward will be issued by your company's representative in charge of the program.

Vulnerability Elimination

Our security experts recommend measures to eliminate identified vulnerabilities and support you in executing those recommendations, if required. Optionally, we take over the communication with all involved specialist departments for you.

Please Note

A Bug Bounty Program does not replace implementing and executing a general IT security strategy.

This product sheet will be valid until a new version is released. *Creation date: 31.10.2018*

usd AG
Frankfurter Straße 233, Haus C1
63263 Neu-Isenburg, Germany | www.usd.de

Phone: +49 6102 8631-190 | E-mail: sales@usd.de
PGP or S/MIME for secure communication