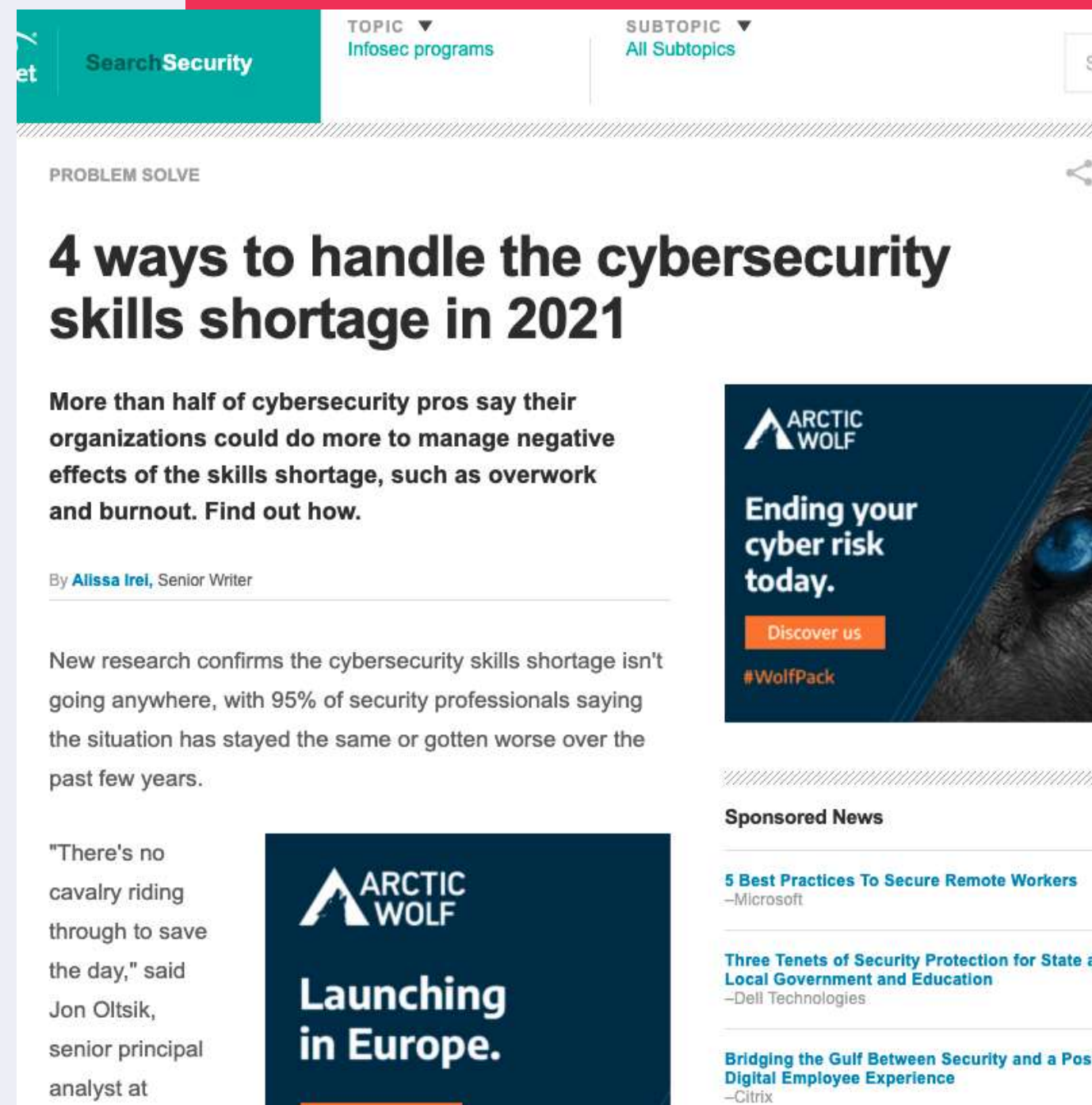


Einführung in Bug Bounty für Unternehmen





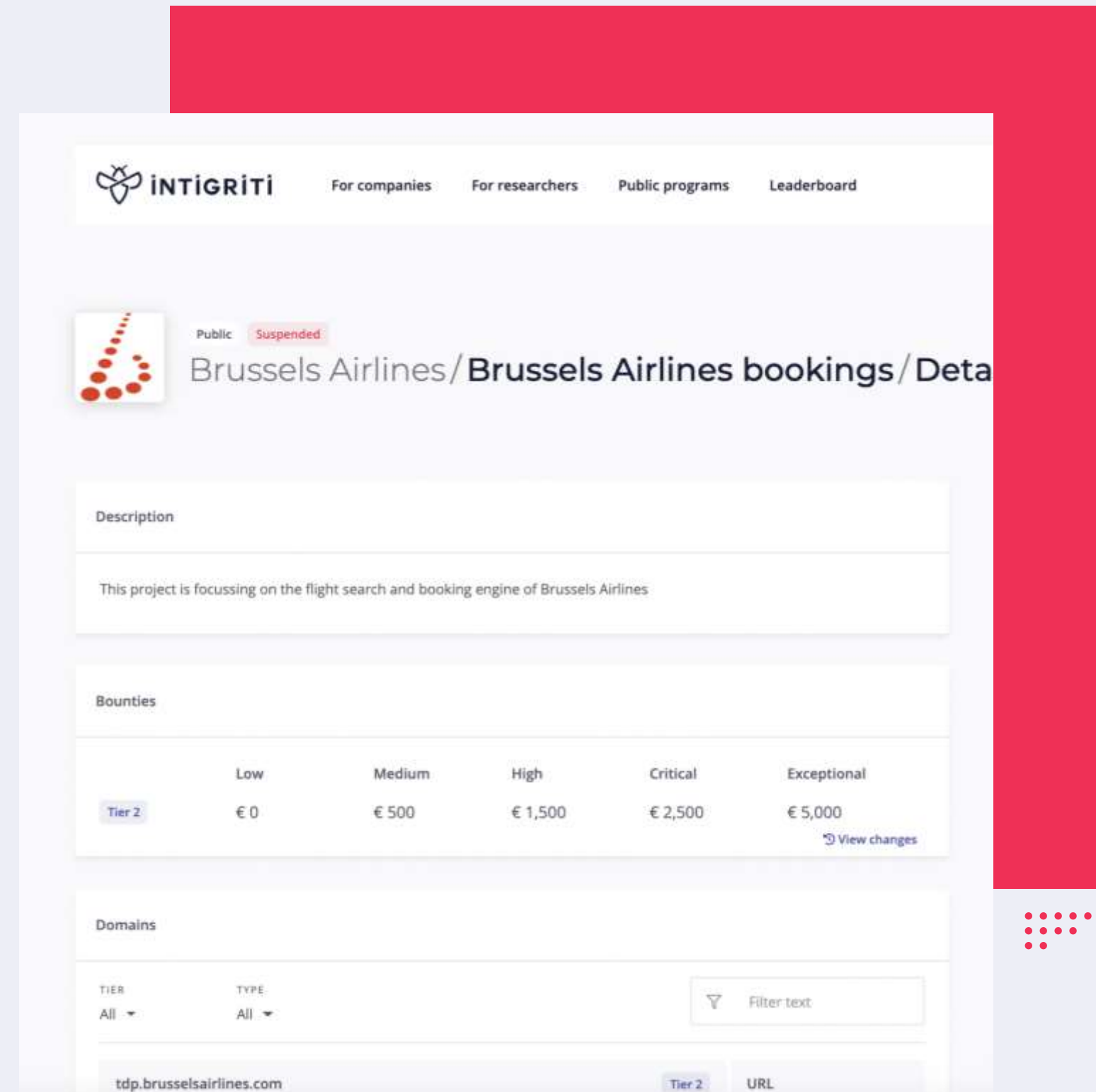
The screenshot shows a webpage from 'Search Security' with a teal header. It features a dropdown menu for 'TOPIC' set to 'Infosec programs' and a 'SUBTOPIC' dropdown set to 'All Subtopics'. The main article is titled '4 ways to handle the cybersecurity skills shortage in 2021' and is categorized under 'PROBLEM SOLVE'. The article text states that more than half of cybersecurity professionals say their organizations could do more to manage negative effects of the skills shortage, such as overwork and burnout. It is written by Alissa Irel, Senior Writer. To the right of the article is an advertisement for 'ARCTIC WOLF' with the text 'Ending your cyber risk today.' and a 'Discover us' button. Below the article is another advertisement for 'ARCTIC WOLF' with the text 'Launching in Europe.' and a 'Discover us' button. At the bottom right, there is a 'Sponsored News' section with three items: '5 Best Practices To Secure Remote Workers' by Microsoft, 'Three Tenets of Security Protection for State and Local Government and Education' by Dell Technologies, and 'Bridging the Gulf Between Security and a Positive Digital Employee Experience' by Citrix.



Herausforderungen

- Fachkräftemangel
- Größer werdende Angriffsfläche durch Digitalisierung
- Agile Entwicklung macht klassische Methoden weniger effektiv

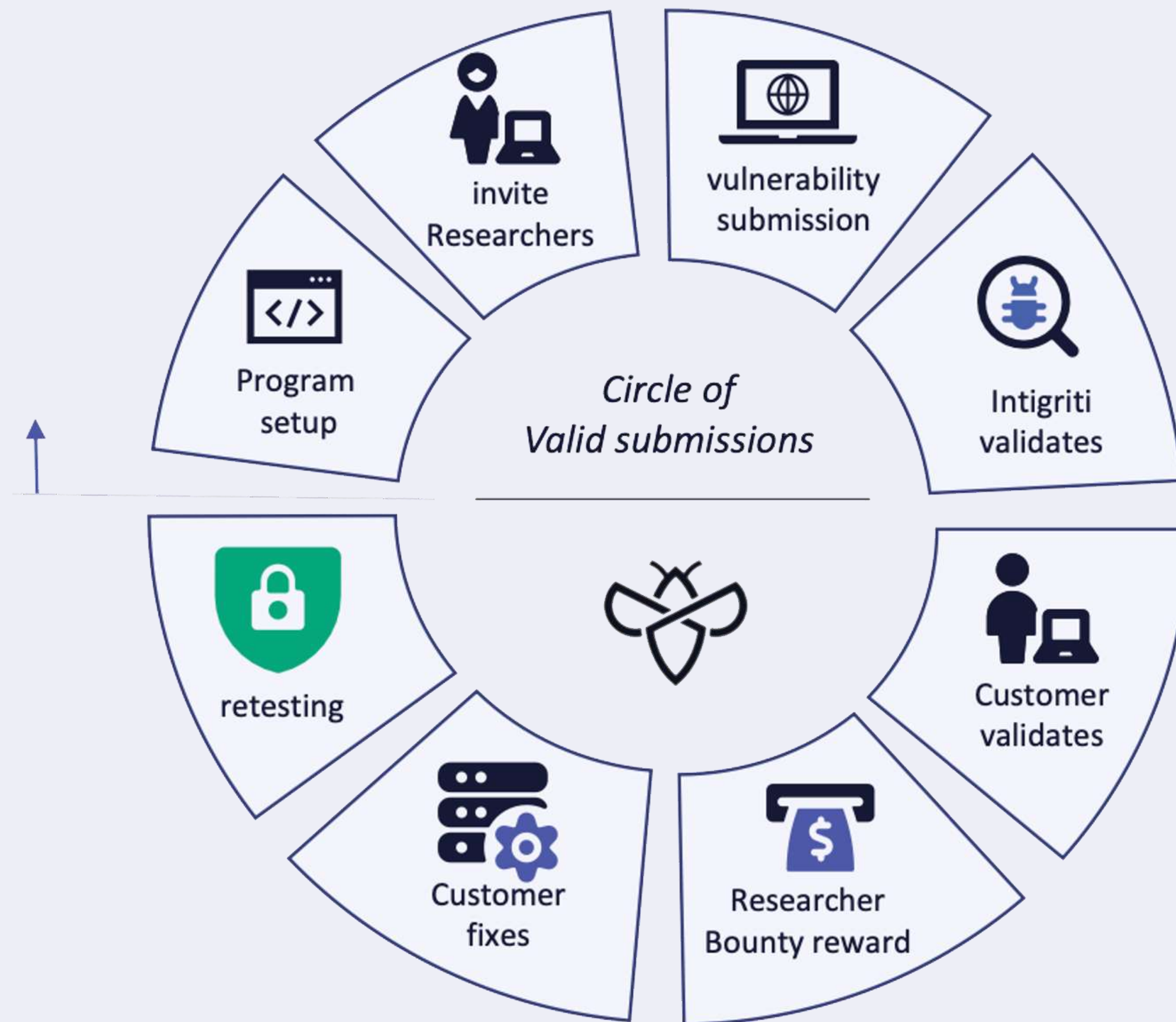




Was ist ein Bug Bounty Programm?

Unternehmen arbeiten in einem Bug Bounty Programm proaktiv mit ethischen Hackern zusammen. Die ethischen Hacker werden belohnt mit einer "Bounty", wenn sie eine valide Sicherheitslücke entdeckt und an das Unternehmen reportiert haben.





Ablauf

Kick-off

- Definition des Scopes
- Empfehlungen für Aufbau der internen Prozesse, um valide Reports zu verarbeiten (Bsp: Jira Integrationen)
- Definition der Höhe der Bounties
- Einladen der ethischen Hacker

Start

- Intigriti triage validiert alle Reports
- Kunde validiert Reports, die von Intigriti Triage kommen
- Intigriti bezahlt Bounty aus

Geltungsdauer		PENTEST	 BUG BOUNTY
 Teamgröße		KLEINE TEAMS ODER EINZELPERSONEN	TAUSENDE SICHERHEITSFORSCHER/-INNEN IN GESCHÜTZTEM RAHMEN
 Ansatz		TECHNIKORIENTIERT	KREATIVER ANSATZ
 Zeitliche Begrenzung		ZEITLICH BEFRISTET	KONTINUIERLICH
 Abrechnung		BEZAHLUNG NACH ZEIT	ERGEBNISBASIERTE ZAHLUNG
 Geltungsdauer		BEGRENZTER AUSSCHNITT	KONTINUIERLICHE TESTS
 Fachwissen		FACHWISSEN UND KOMPETENZEN EINZELNER ZUSTÄNDIGER	FACHWISSEN UND KOMPETENZEN DER GEMEINSCHAFT

- 1 **50.000** Hacker aus 140 Ländern
- 2 **KYC** and **Identitätsprüfung**
- 3 **Aktive** community:
35%+ aktiv im letzten Quartal
- 4 **12** Kategorien an Skills:
von Webapplikationen zu Mobile zu IoT
- 5 **Individuelle Zusammenstellung**
der Community für ihr Programm



Intigriti in Zahlen



FORSCHER
robin



53

ist die **durchschnittliche Anzahl Sicherheitslücken**, die in der ersten Woche **nach einer Programmeinführung** gemeldet werden.

37

ist die **durchschnittliche Anzahl Meldungen**, die in der ersten Woche **nach einer Programmeinführung** eingehen.

24 Std.

dauert im Durchschnitt die **Prüfung und Annahme oder Ablehnung eines Berichts** durch das Intigriti Triage-Team.

48 Std.

dauert im Durchschnitt die **Annahme oder Ablehnung des Reports (sofern eskaliert)** auf Kundenseite.

23 %

unserer registrierten ethischen Hacker/-innen reichen **mindestens einen Report pro Monat** ein.

71 %

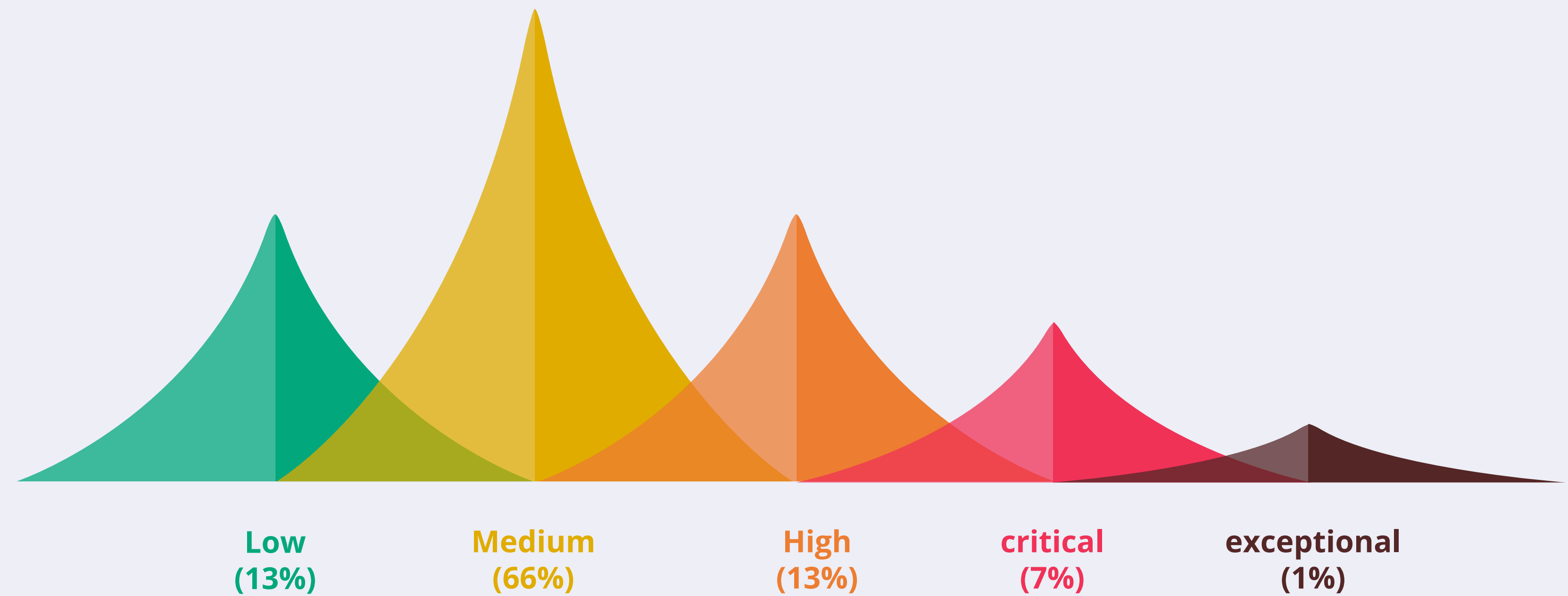
der Unternehmen erhalten nach dem Start ihres Programms über Intigriti **innerhalb der ersten 48 Stunden eine Sicherheitsmeldung, deren Bedeutung als hoch oder kritisch eingestuft wird.**





CVSSv3 5.27

Verteilung der
akzeptieren Reports auf
der Intigriti Plattform







Public

Open

Red Bull/Red Bull/Detail

Detail

Updates

Leaderboard

Description

Red Bull appreciates the work of security researchers to make the internet a better - and more secure - place. Even though we aim to prevent security issues by applying state-of-the art development and operations processes, systems and technical services outside our direct control might have vulnerabilities and weaknesses and we aim to identify and address those before any negative impact occurs. As appreciation we have a unique reward system in place, please see FAQ for more information.

Overall stats

SUBMISSIONS RECEIVED	ACCEPTED SUBMISSIONS
5346	1303
AVERAGE PAYOUT	TOTAL PAYOUTS
N/A	N/A

Last 90 day response times

AVG. RESPONSE TIME	AVG. TIME TO TRIAGE
< 24 hours	< 2 days

Aktives VDP: Red Bull





Aktives VDP: give **Red Bull**

2. Describe your assets:

Tier 1

🛡️ Maturity:

🎯 Risk:

📈 Curve:

Bended

↺

🗑️

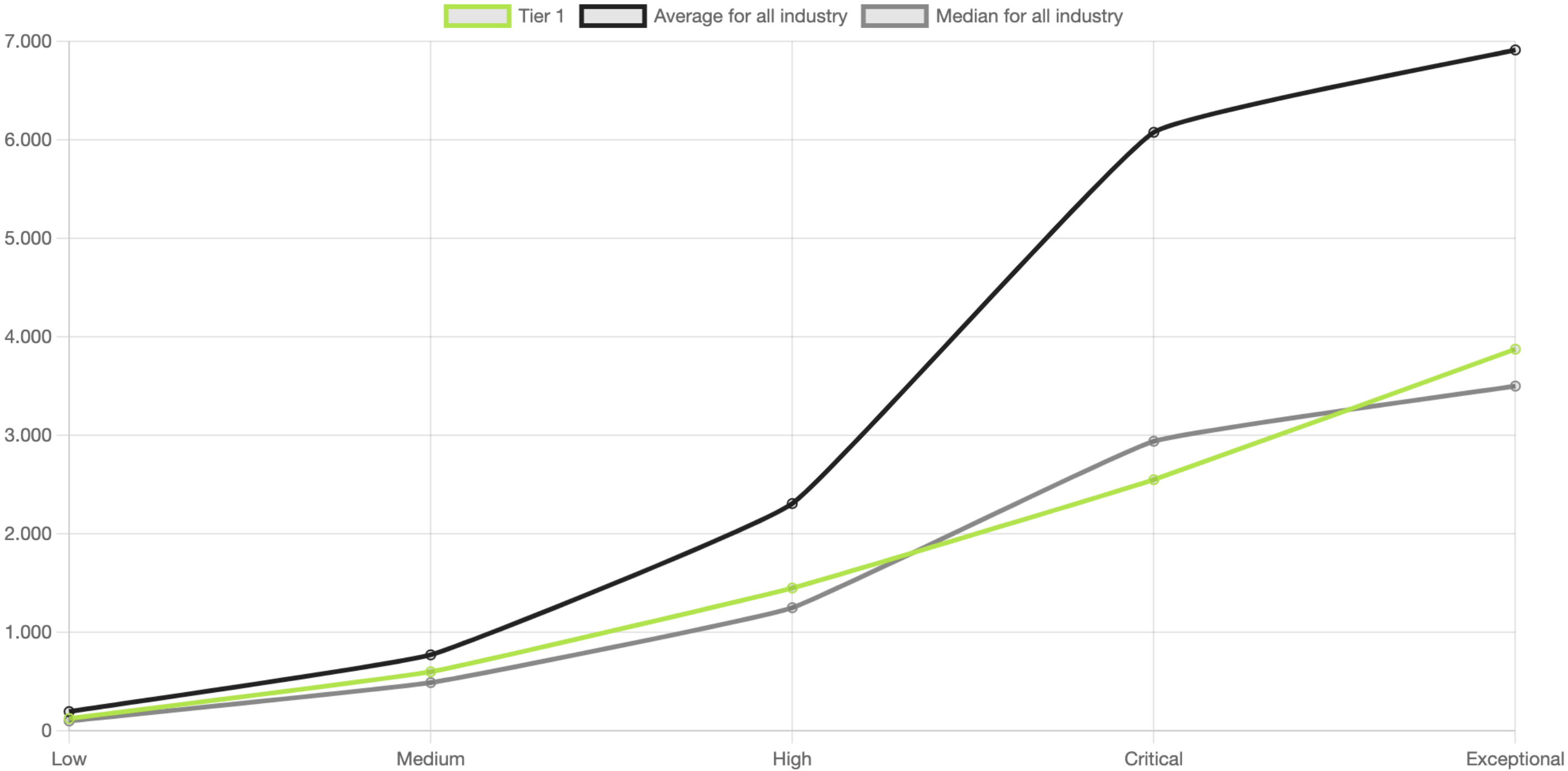
+

3. View your bounty table:

☒ Include exceptional category

CVSSv3 score:	Low (0.1 - 3.9)	Medium (4.0 - 6.9)	High (7.0 - 8.9)	Critical (9.0 - 9.4)	Exceptional (9.5 - 10)
Tier 1	€ 125	€ 600	€ 1.450	€ 2.550	€ 3.875
Industry average	€ 195	€ 771	€ 2.307	€ 6.076	€ 6.912
Industry median	€ 100	€ 490	€ 1.250	€ 2.940	€ 3.500

Your overall bounties are **47.1% below** the average and **3.9% above** the median for your industry.
Your bounty levels are estimated to attract **intermediate** hackers.



Über Intigriti



SaaS Plattform mit **50,000+** ethischen Hackern



90 Mitarbeiter global



2016 gegründet mit HQ in Antwerpen



Über **250 aktive Programme**

