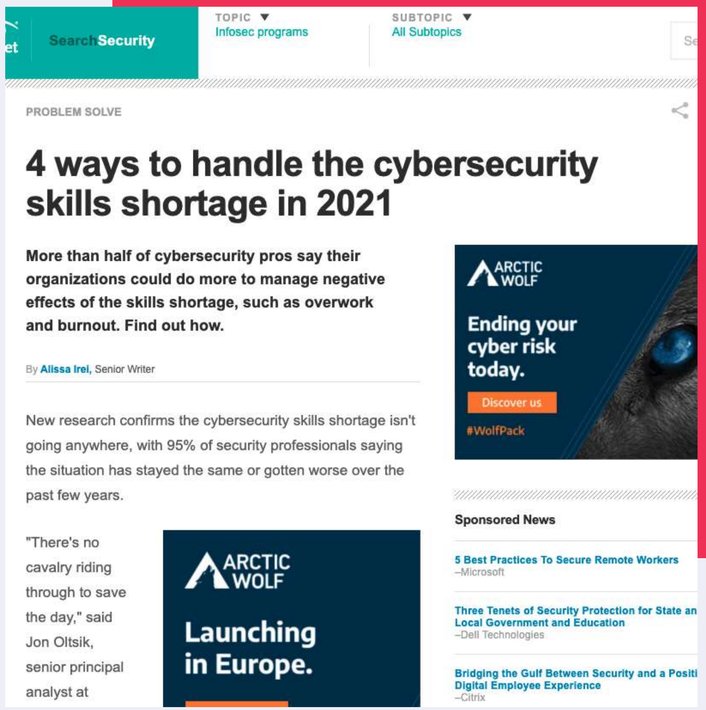
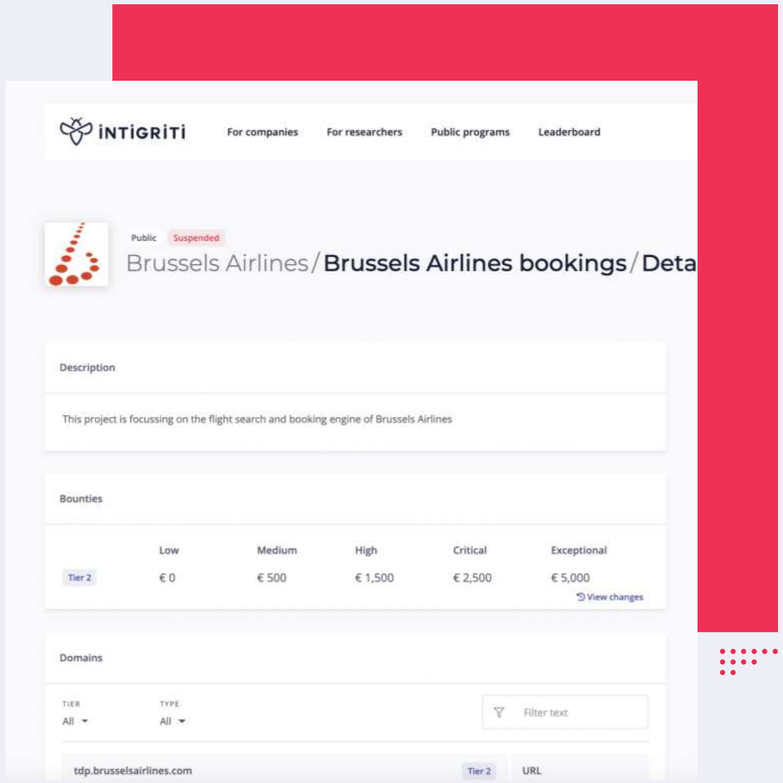
Einführung in Bug Bounty für Unternehmen



Herausforderungen

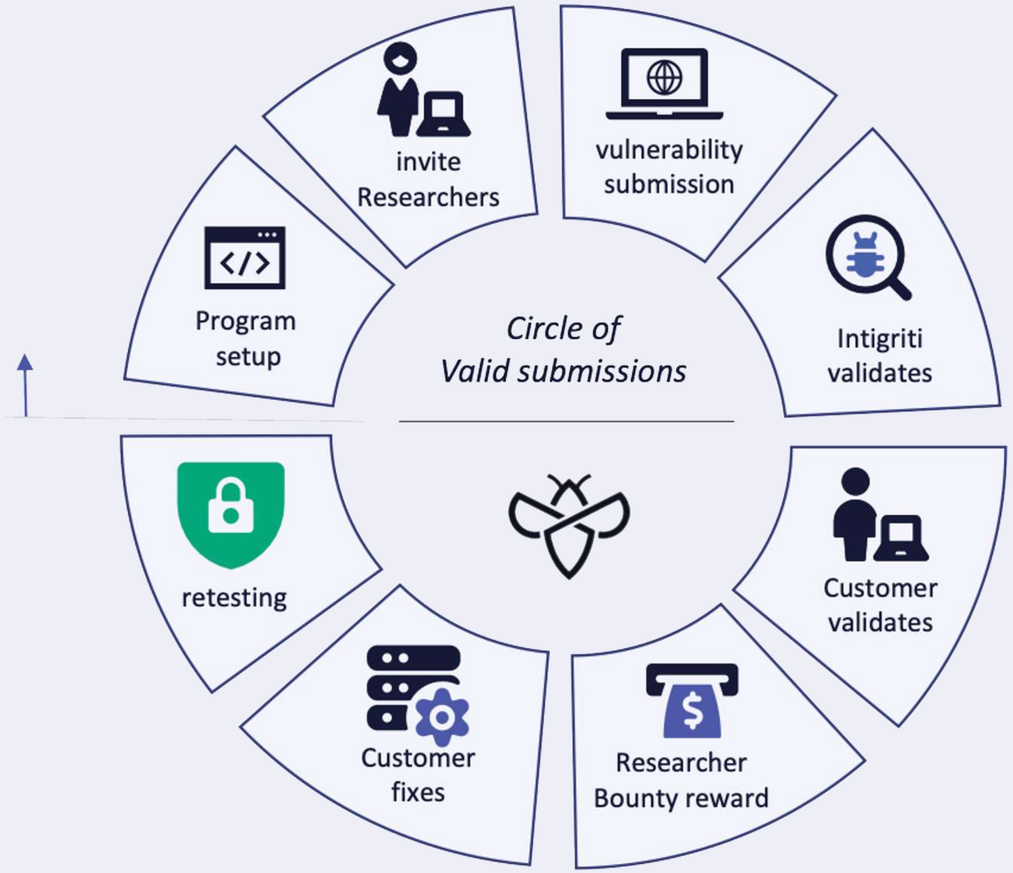
- **Fachkräftemangel**
- **Größer werdende Angriffsfläche durch Digitalisierung**
- **Agile Entwicklung macht klassische Methoden weniger effektiv**



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.

Wie funktioniert Bug Bounty?



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

Vergleich mit Penetrationtests

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

Community

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

53

ist die **durchschnittliche Anzahl Sicherheits-lücken**, 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 %

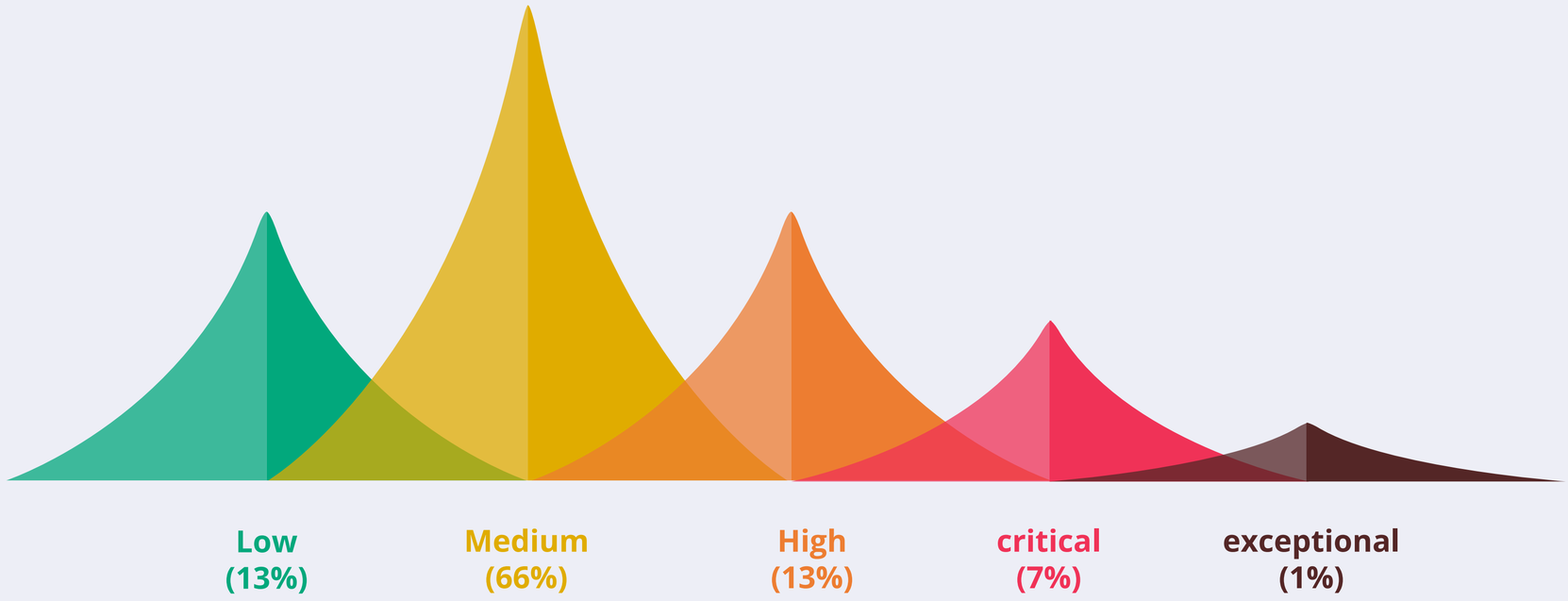
unserer registrierten ethischen Hacker/-innen reichen **mindestens einen Report pro Monat** ein.

71 %

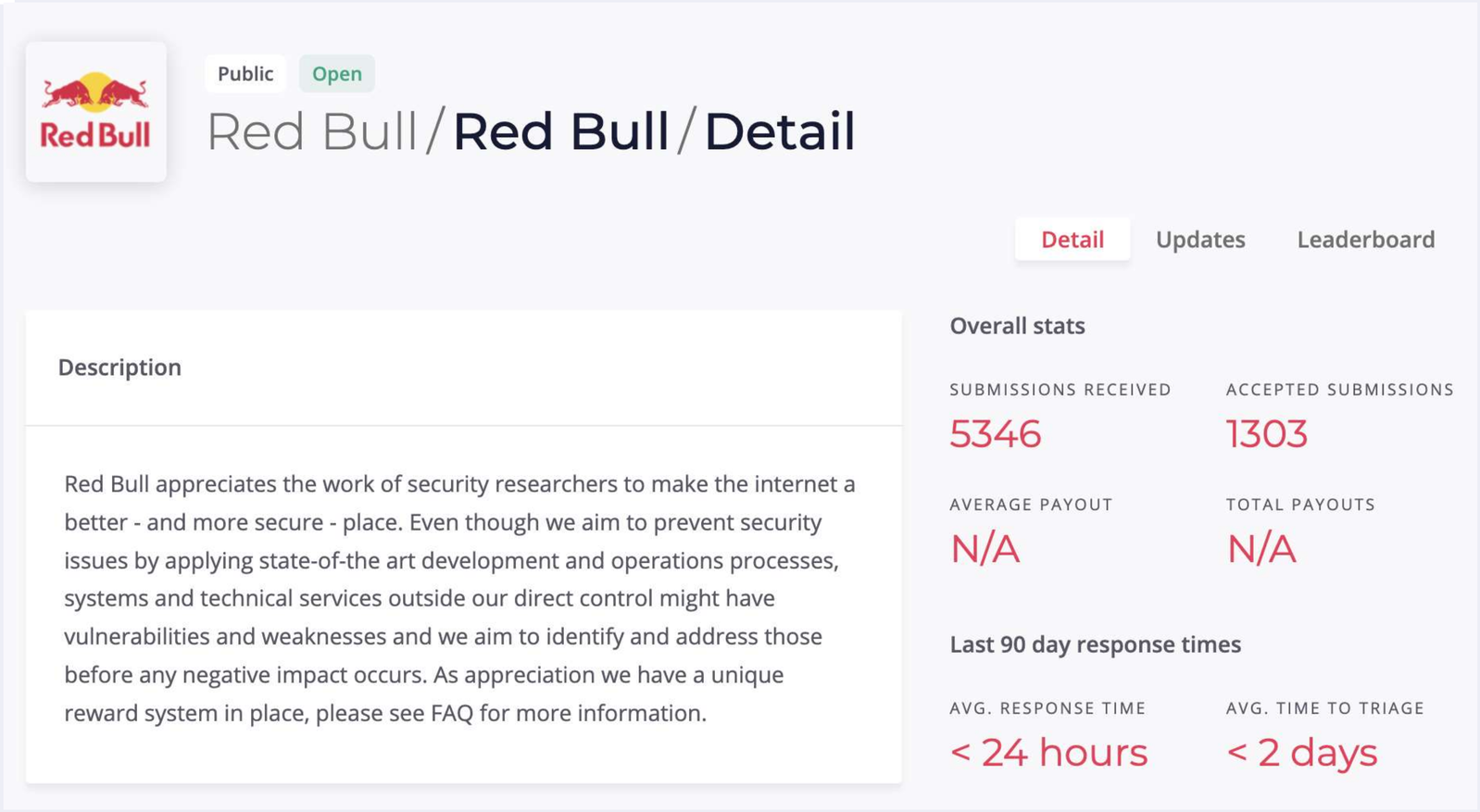
der Unternehmen erhalten nach dem Start ihres Programms über Intigriti **innerhalb der ersten 48 Stunden eine Sicherheitsmeldung, deren Bedeutung als hoch oder kritisch eingestuft wird**.

CVSSv3 5.27

Verteilung der
akzeptieren Reports auf
der Intigriti Plattform



Unsere Kunden



Aktives VDP: Red Bull

Aktives VDP: give Red Bull

2. Describe your assets:

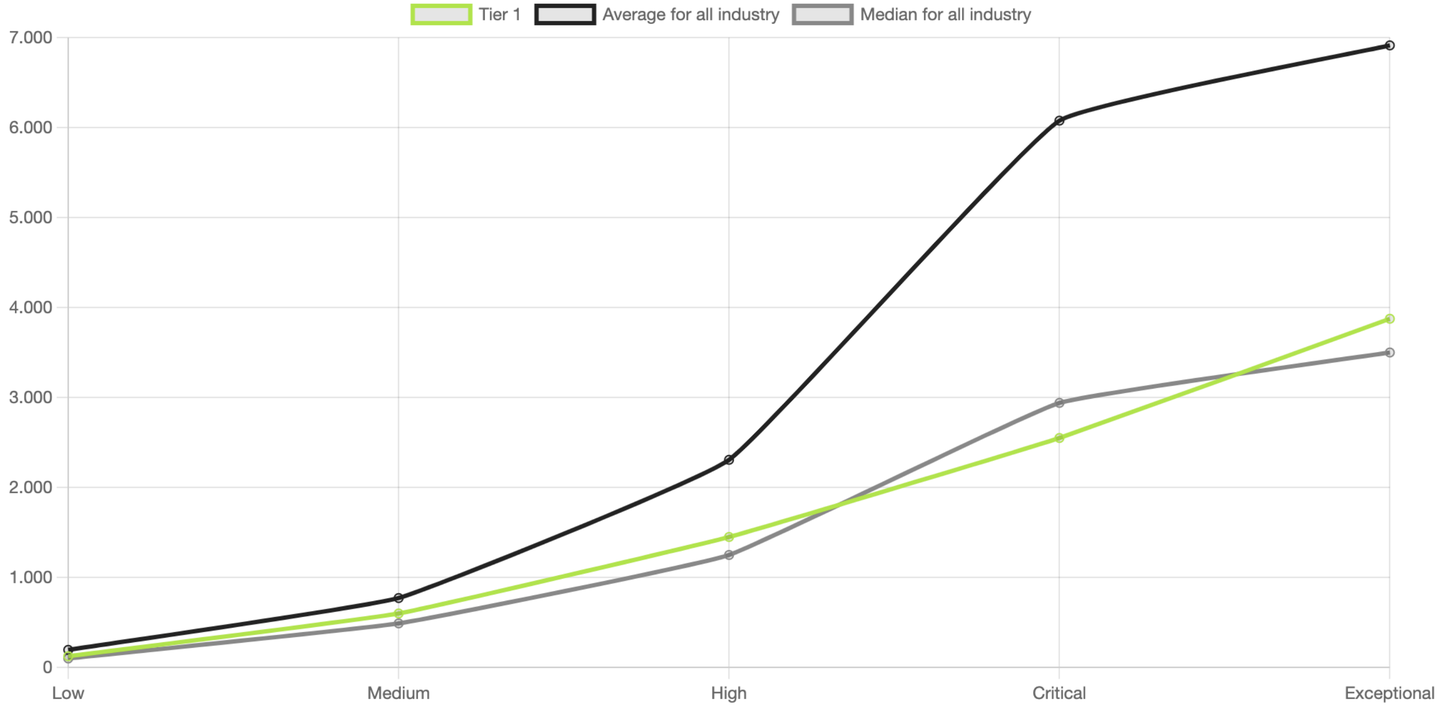
Tier 1 | Maturity: | Risk: | Curve: Bended

3. View your bounty table:

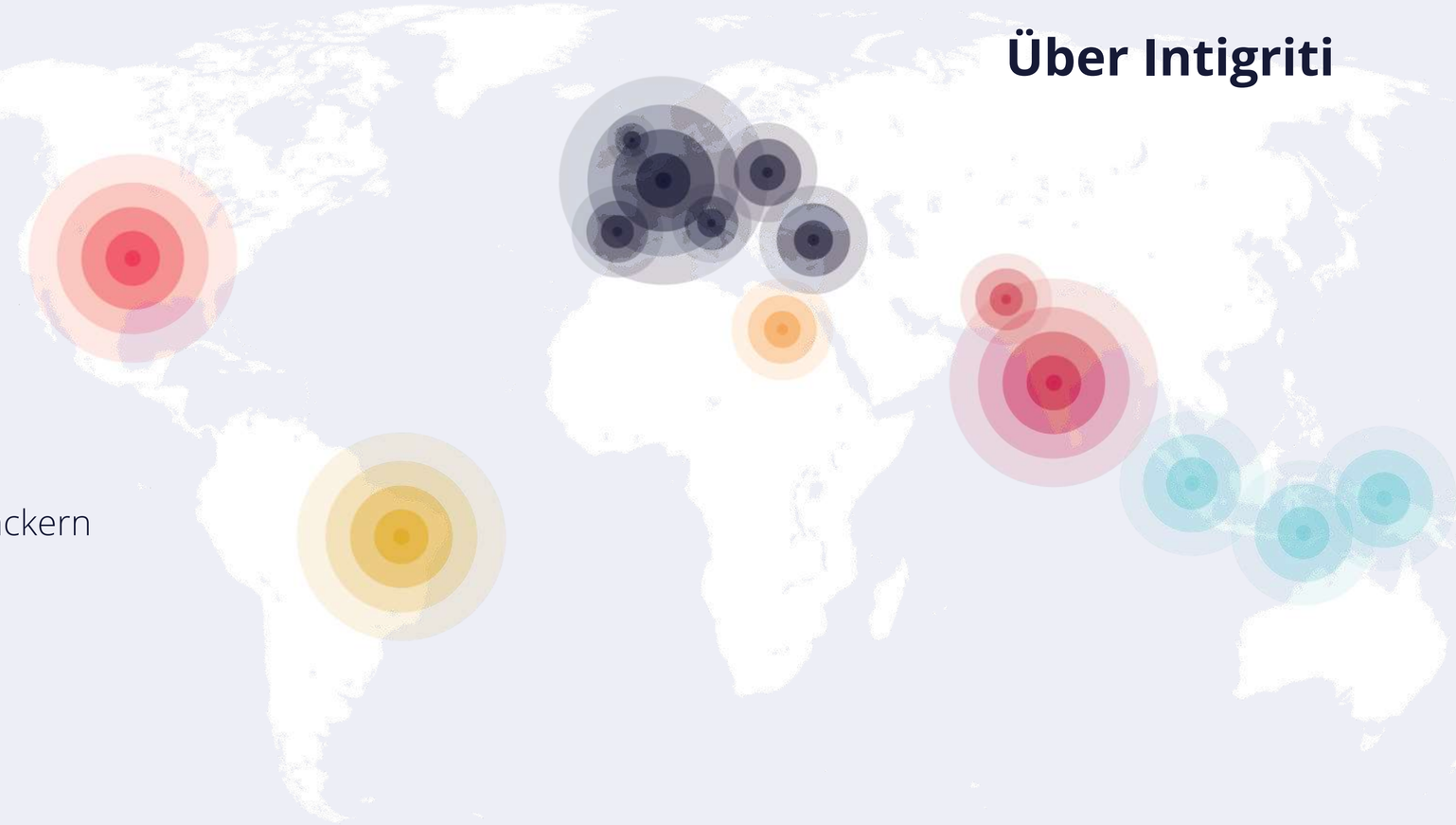
Include exceptional category

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**