

Can You Find The Panda?

hackerone

HackerOne and Attack Resistance Management

IT-SA Expo&Congress 2022

Chris Dickens
Solutions Engineer @ HackerOne



Who Am I



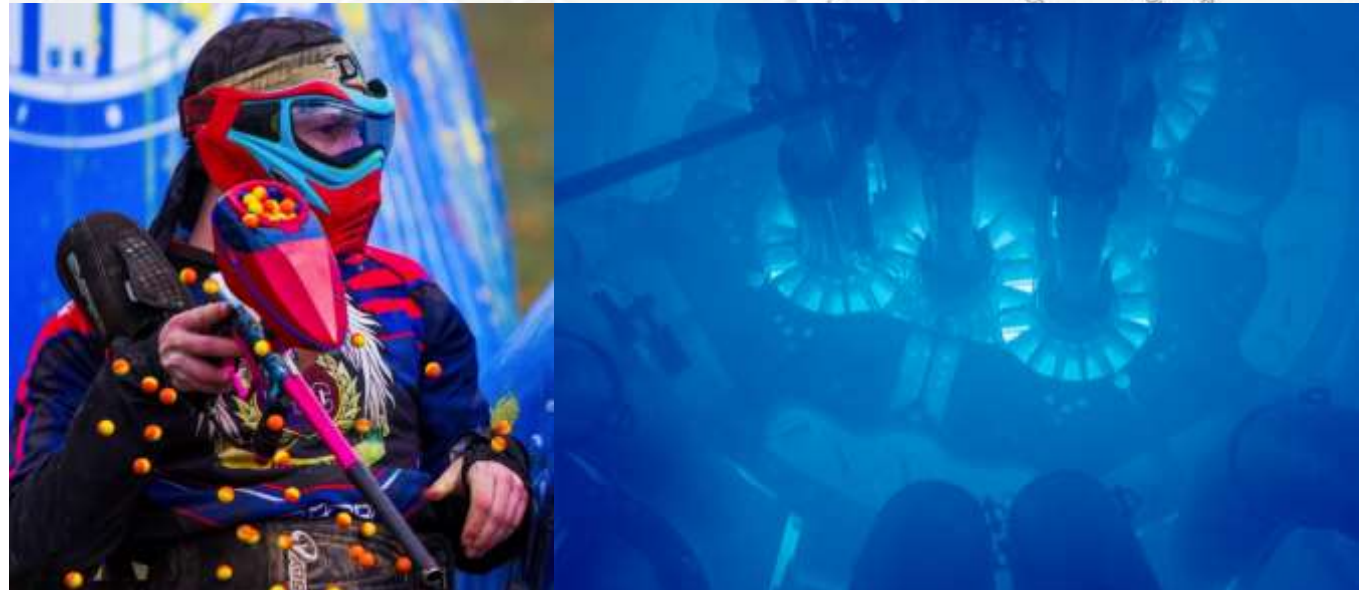
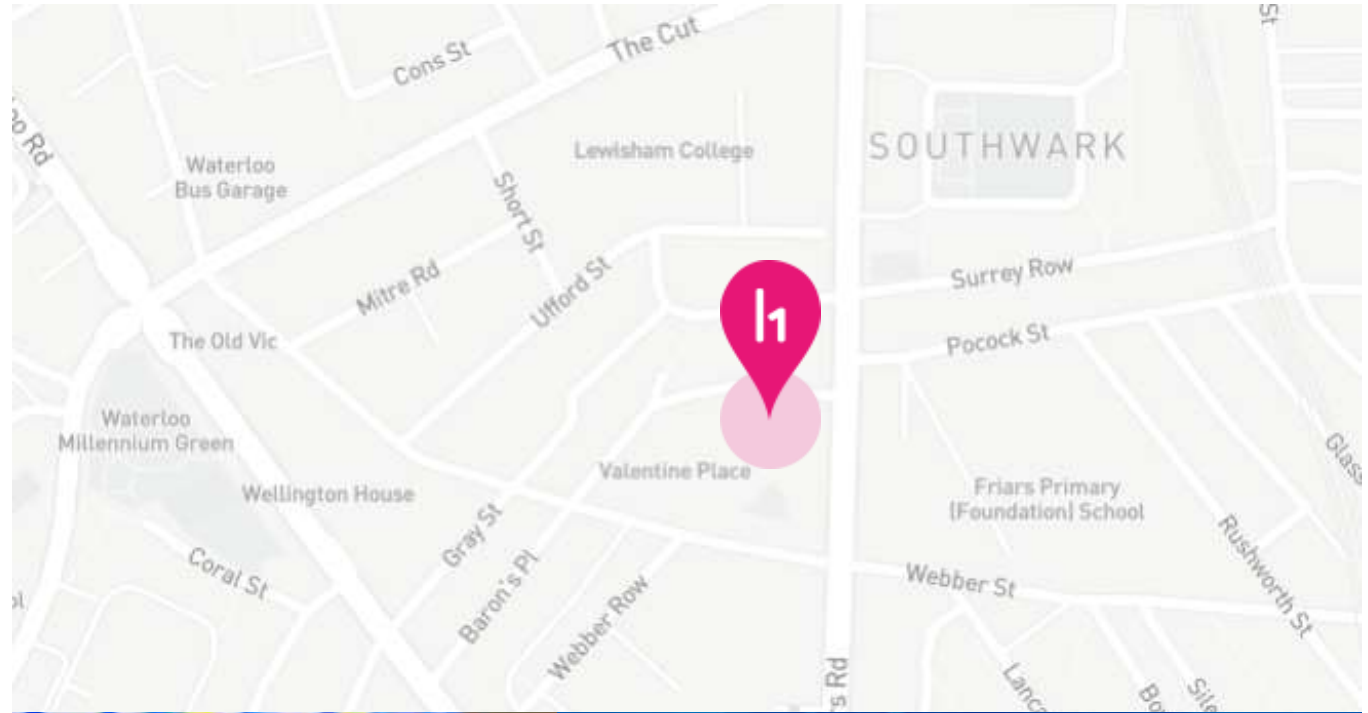
cdickens@hackerone.com



[Hackerone.com](https://hackerone.com)

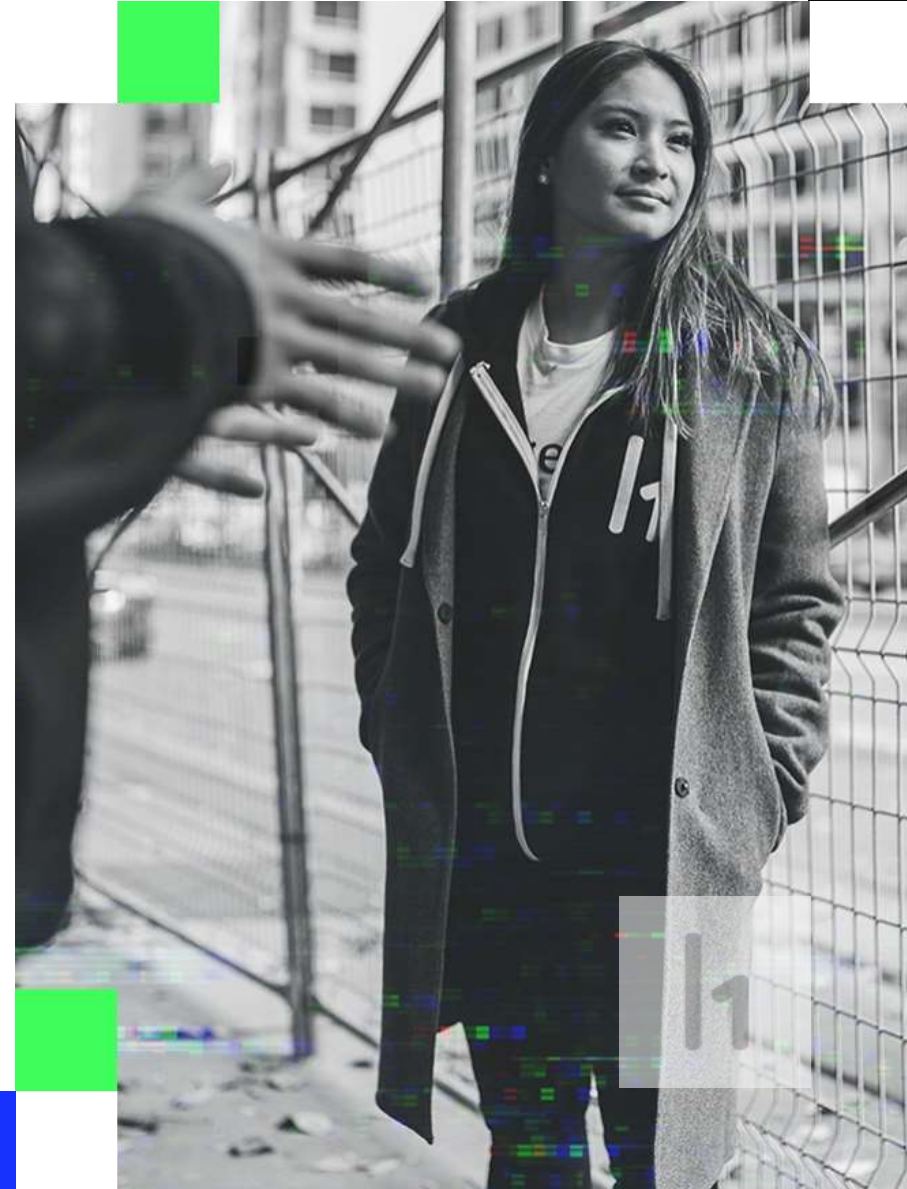


github.com/chrisdicken



Agenda

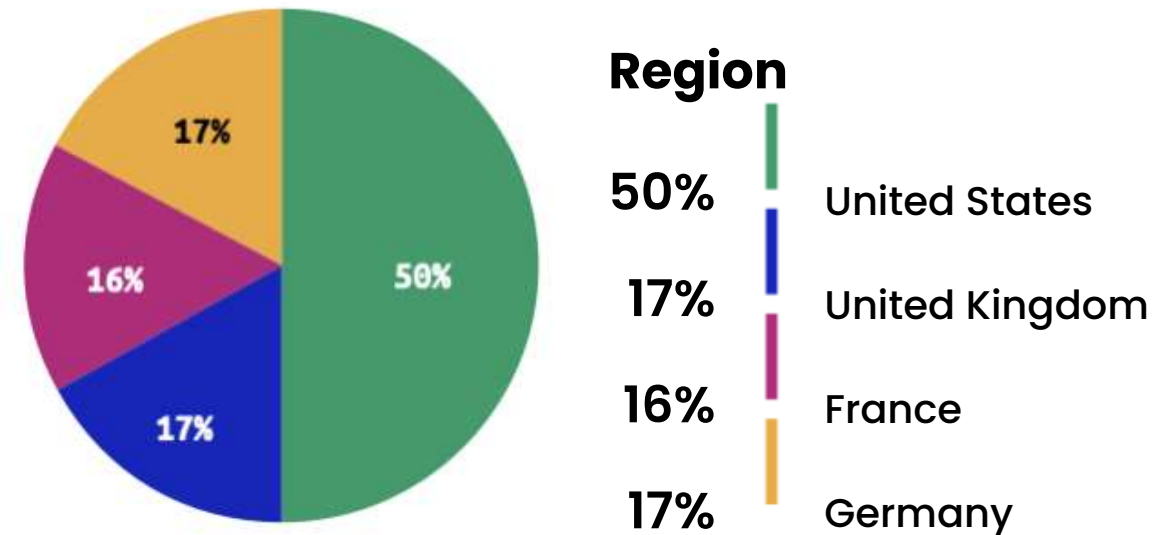
- Part I: Challenge
- Part II: HackerOne Solution



Part I: Challenge

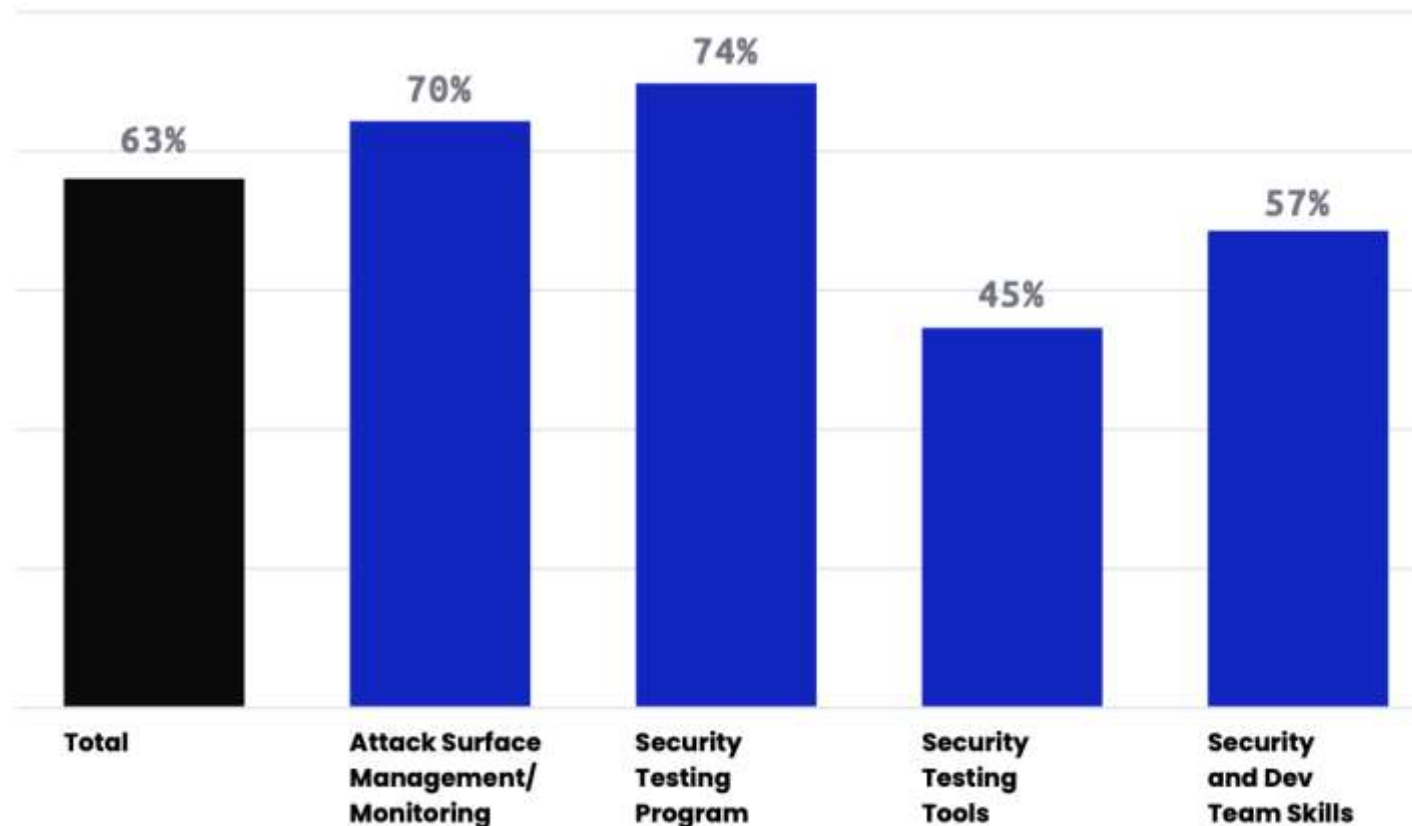
HackerOne 2022 Attack Resistance Research

We surveyed 800+ IT executives to investigate the attack resistance gap

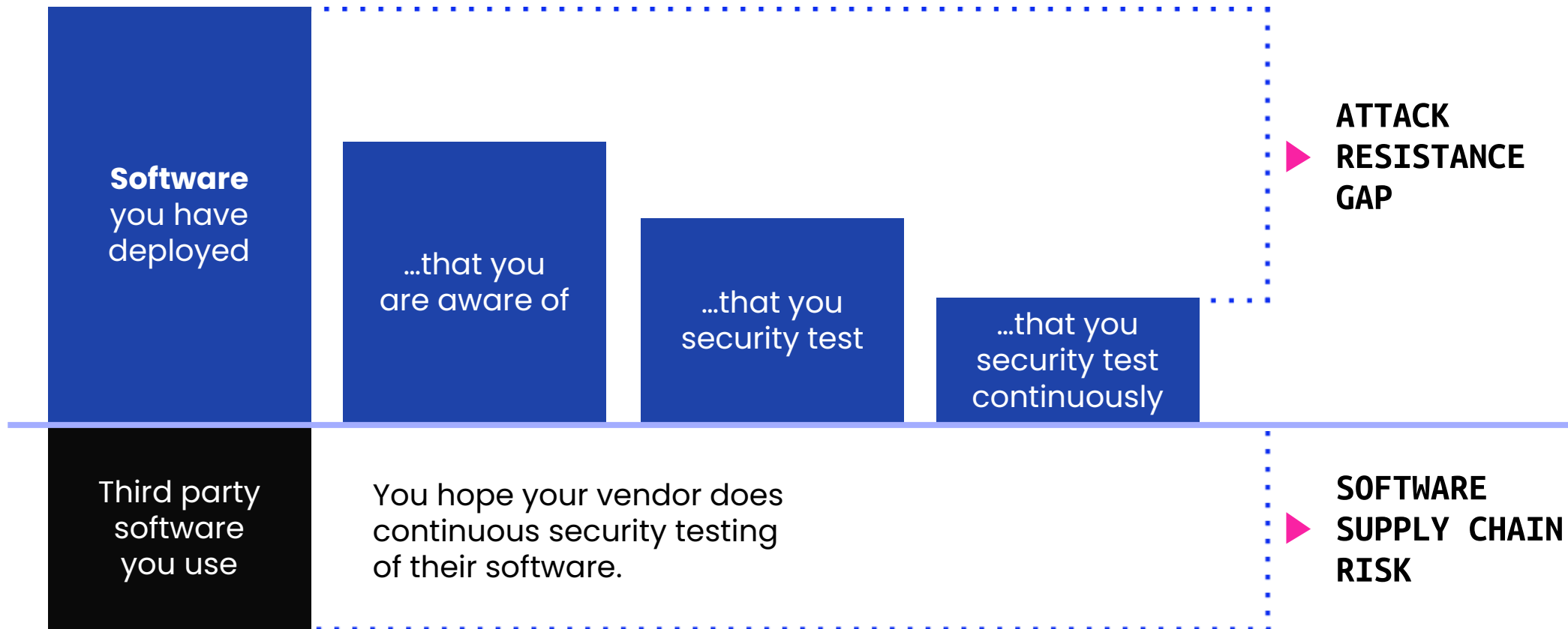


Key Components of Attack Resistance

- Together, respondents believe that **63%** of their entire attack surface is ready to resist attack
- This leaves an attack resistance gap of **37%**



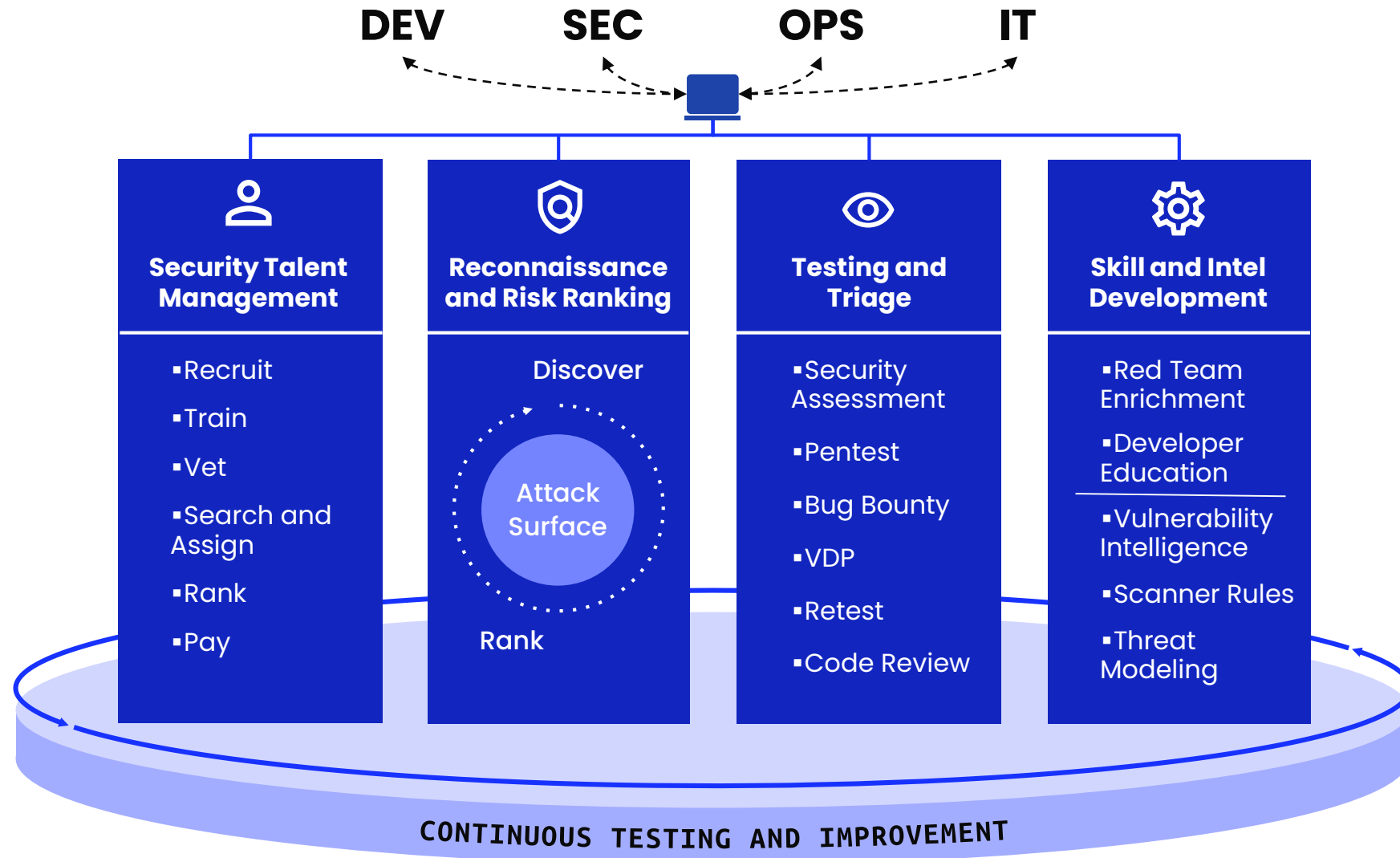
The Modern Attack Surface



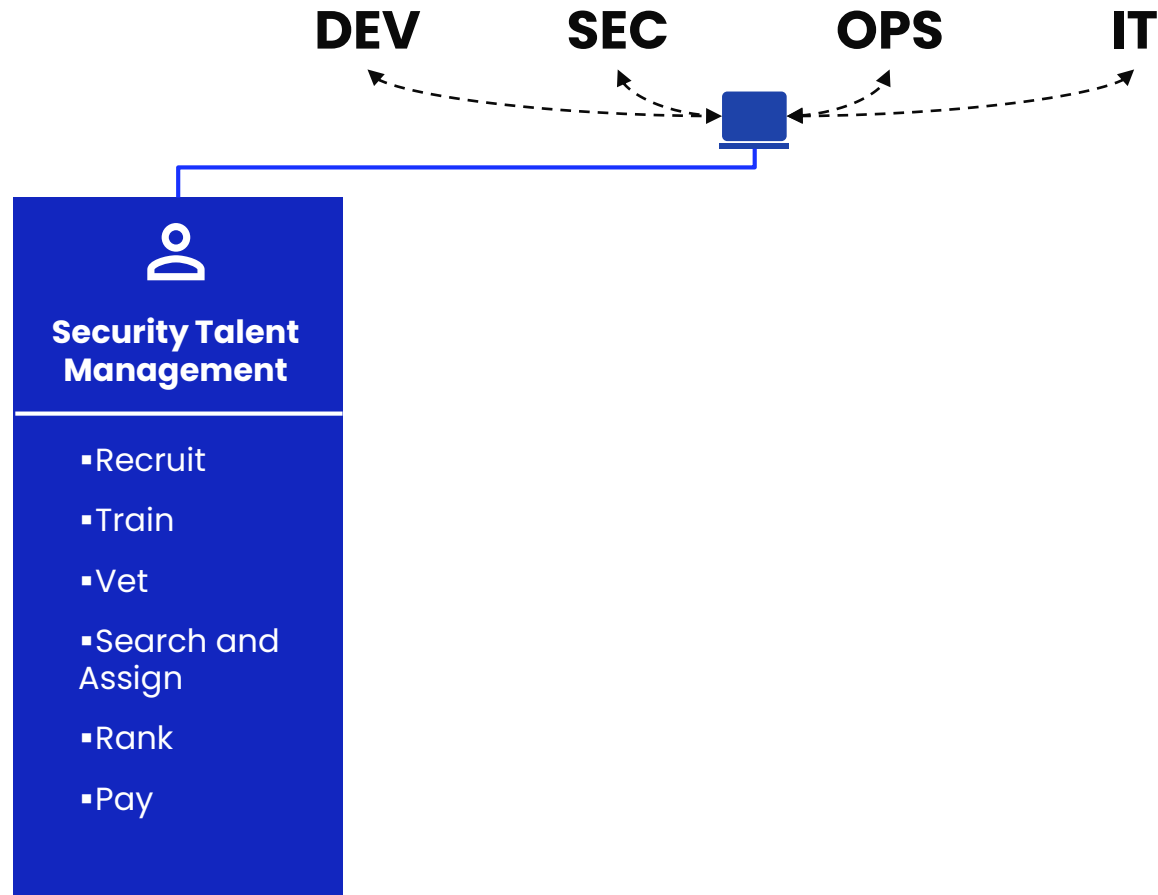
Part II:

HackerOne Solution

How Attack Resistance Management Works



How Attack Resistance Management Works



Security and Talent Management

The Security Team



The Attack Surface



Manoel Abreu
(manoelt)

Brazil
Joined July 2014



About Manoel Abreu

<https://www.hackerone.com/resources/hackerone/hacker-spotlight-interview-with-manoelt>

Master in Software Engineering. OSWE, GCPN.

I have won three HackerOne Capture The Flag:

2018 H1-5411 - <https://hackerone.com/reports/415682>

2019 H1-702 - <https://hackerone.com/reports/514664>

2020 H1-415 - <https://hackerone.com/reports/776634>

Stats All Time

7.00 96th
Signal Percentile

28.90 97th
Impact Percentile

2492 -
Reputation Rank

Hacktivity

All

100 [H1-415 2020] CTF Writeup
By manoelt to h1-ctf Resolved Critical bounty awarded 2 years ago

100 \$50 million CTF Writeup
By manoelt to 50m-ctf Resolved Critical disclosed 3 years ago

83 Remote Code Execution (RCE) in a DoD website
By manoelt to U.S. Dept Of Defense Resolved Critical disclosed 3 years ago

Certifications

GIAC Cloud Penetration Tester (GCPN)

Issued May 2022 / Expires May 2026

AWS Certified Cloud Practitioner (AWS Certified Cloud Practitioner)

Issued August 2021 / Expires August 2024 / Certification ID: 838M5TSBEJRQ1JG1

Offensive Security Web Expert (OSWE)

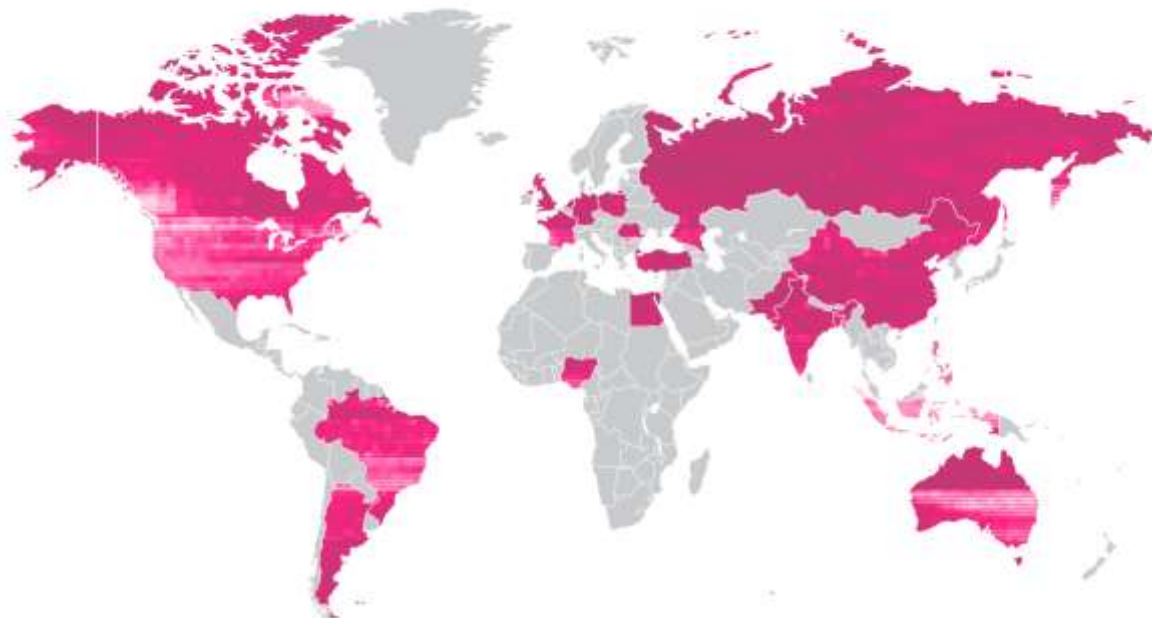
Issued July 2021 / Certification ID: OS-AWAE-40307

EC-Council Certified Ethical Hacker (CEH)

Issued October 2021 / Expires September 2024 / Certification ID: ECC1705269348

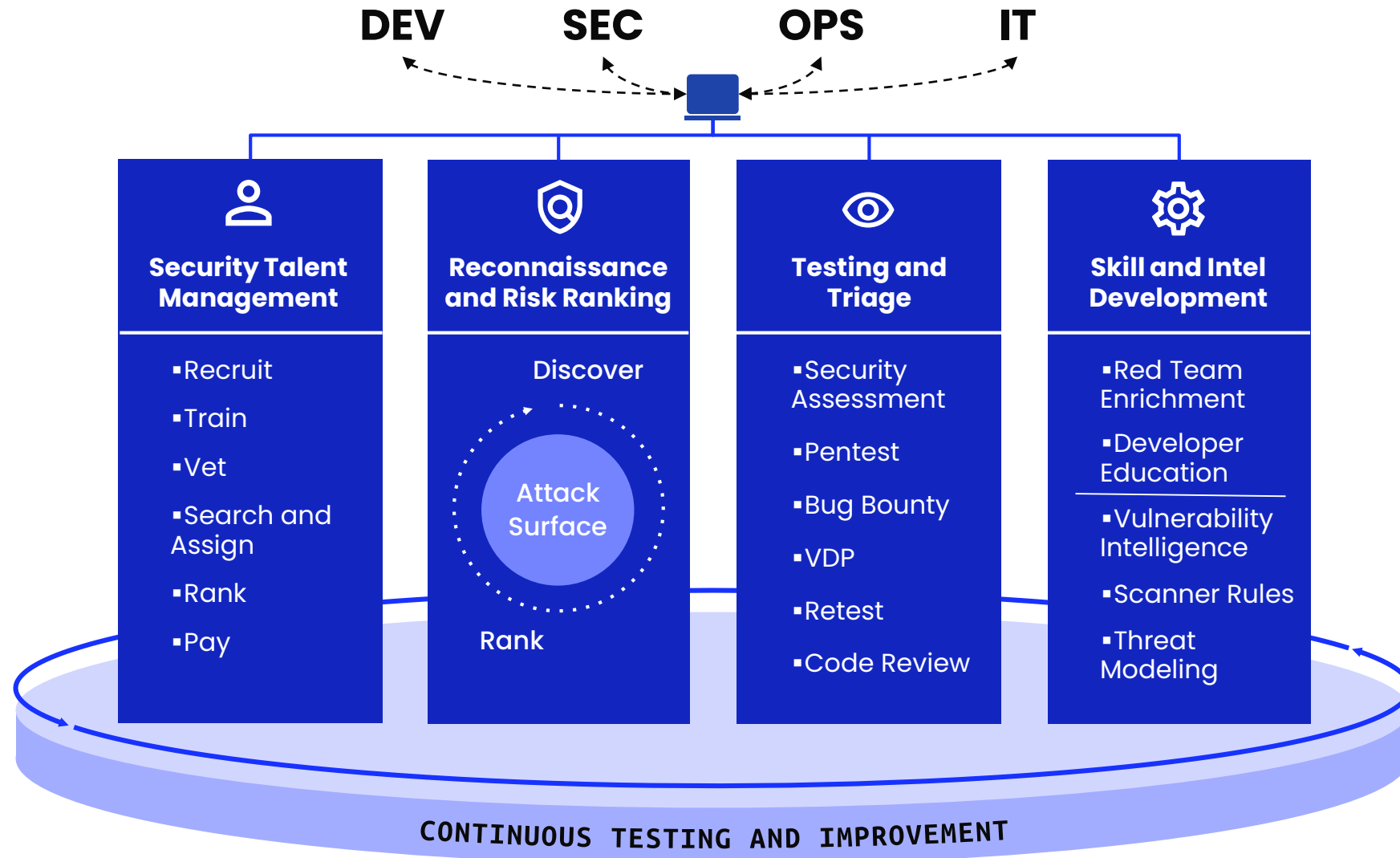
HACKERS AROUND THE GLOBE

TOP COUNTRIES
REPRESENTED ON HACKERONE

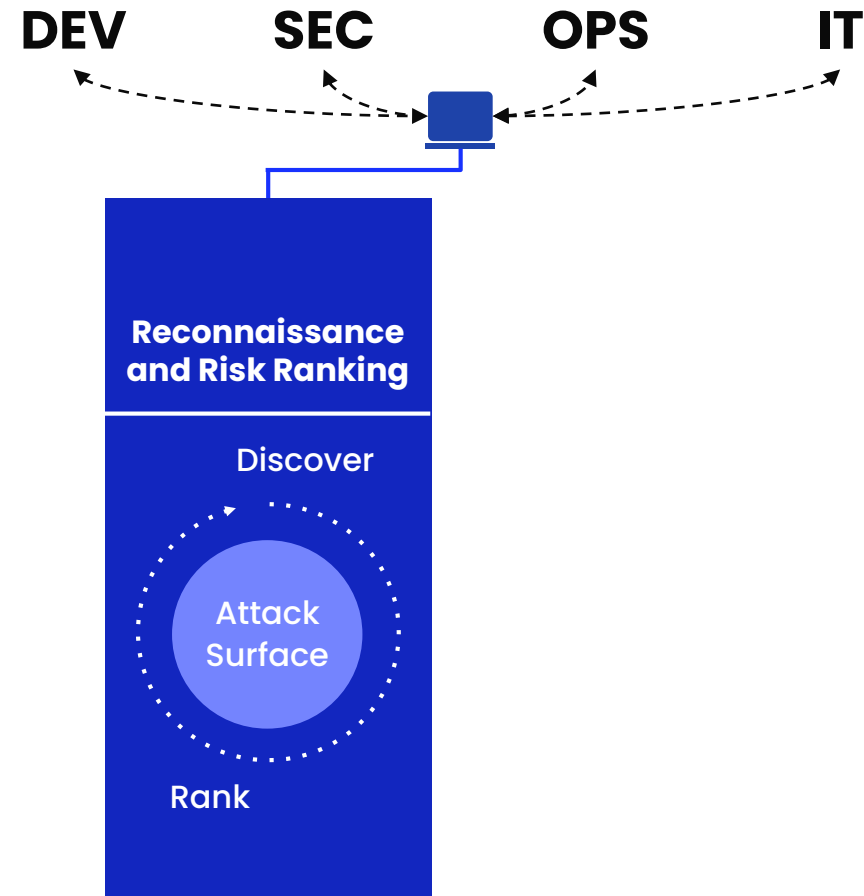


hackerone

How Attack Resistance Management Works



How Attack Resistance Management Works



Attack surface coverage

Export [PDF](#) | [CSV](#)

Filter results by

Select an organisation / company

Select a region / country

Last 30 days

By Tags

Asset Coverage Overview

Last 6 months

21 642

+8%

Assets at risk

[View list](#)

301

+8%

New assets

[View list](#)

7034

+8%

Untested assets

[View list](#)

352

+8%

Tested assets

[View list](#)

Risk score

↑ 83/100

+2%

Overall risk score

[Improve score](#)

Tested attack surface

Asset coverage by month

☒ Tested assets

☒ Known assets

Last 6 months



Known assets

Tested assets (scope)

| Submit Month | Coverage % | Risk |
|--------------|------------|----------|
| August '20 | +8% | Healthy |
| July '20 | +2% | Risk |
| June '20 | +1% | Risk |
| May '20 | +4% | Risk |
| Apr '20 | -2% | Risk |
| Mar '20 | -2% | Critical |

Tomnomnom – The King of Recon




 **[Pre-Submission][H1-4420-2019] API access to Phabricator on code.uberinternal.com** disclosed about 1 year ago
from leaked certificate in git repo
By [tomnomnom](#) to [Uber](#) Resolved Critical **\$39,999.99**

Live Recon and Automation on Shopify's Bug Bounty Program with [@TomNomNom](#)

52,006 views • Apr 19, 2021

 1.7K  DISLIKE  SHARE  DOWNLOAD  CLIP  SAVE ...

 **Tom Hudson**
[tomnomnom](#)

[Follow](#) [Sponsor](#)

Open-source tool maker, trainer, talker, fixer, eater, not really a sheep. He/him.

[8.3k](#) followers • [137](#) following

[sbtUK](#)
Yorkshire, UK
<http://tomnomnom.com>

[Overview](#) [Repositories 97](#) [Projects](#) [Packages](#) [Stars 290](#) [Sponsoring 3](#)

Find a repository...

[Type](#) [Language](#) [Sort](#)

hacks Public
A collection of hacks and one-off scripts
[Go](#) [1,562](#) [562](#) Updated 2 days ago

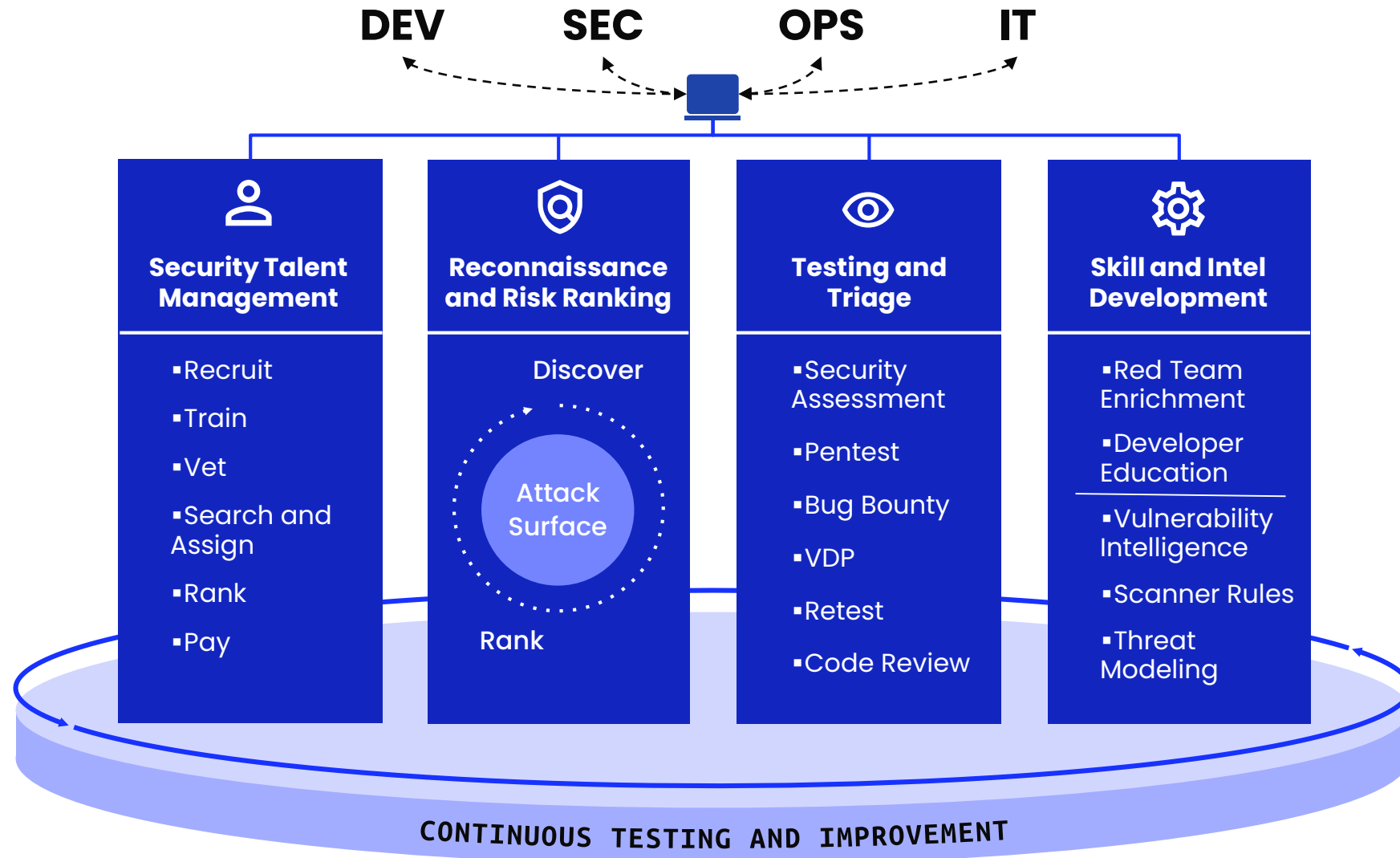
assetfinder Public
Find domains and subdomains related to a given domain
[Go](#) [1,933](#) [358](#) [MIT License](#) Updated 3 days ago

unfurl Public
Pull out bits of URLs provided on stdin
[Go](#) [842](#) [77](#) [MIT License](#) Updated 8 days ago

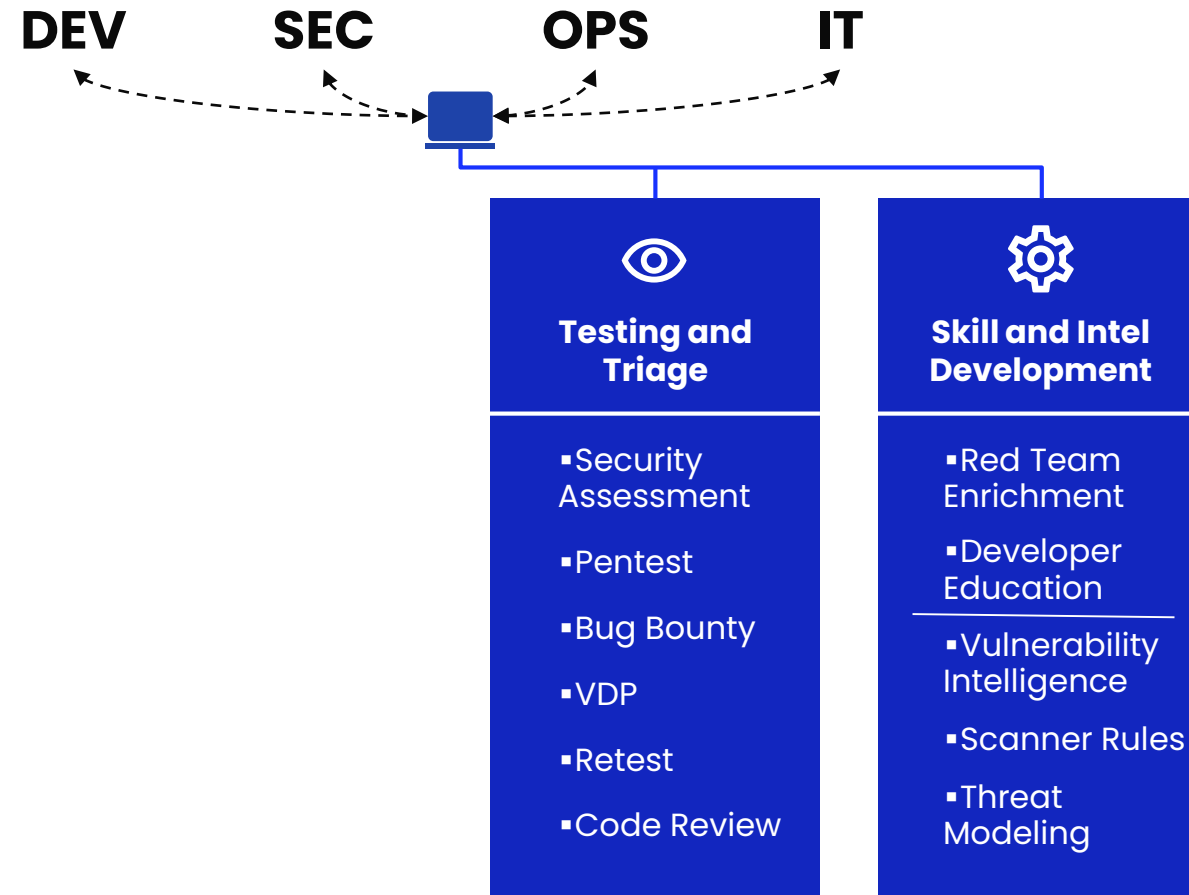
gf Public
A wrapper around grep, to help you grep for things
[Go](#) [1,113](#) [232](#) [MIT License](#) Updated 13 days ago



How Attack Resistance Management Works



How Attack Resistance Management Works



Attack Resistance Management Portfolio

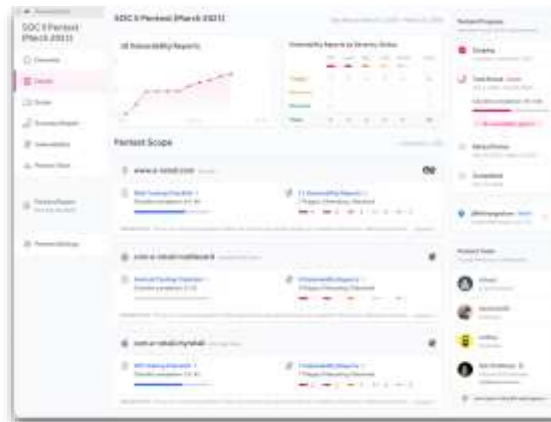
Bounty

Continuous Proactive
Security Testing



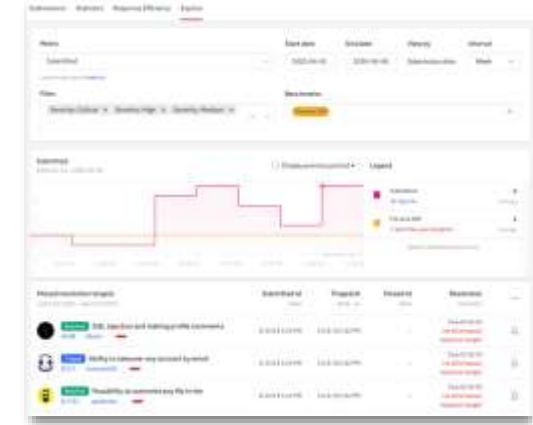
Assessments

On-Demand, Time-bound
Testing



Response

Continuous Vulnerability
Disclosure



Advisory Services

Code Review

Triage Services

Integrations








hackerone

Ethical Hackers Have Your Back


131

#1543159

Able to approve admin approval and change effective status without adding payment details .

Share:     

TIMELINE · EXPORT

 bisesh submitted a report to [Reddit](#).
Apr 17th (3 months ago)


Summary:




In <https://ads.reddit.com/> you can create campaign under which you can create ads , once you create new campaign , it is on pending stage and will not be delivered unless you add payment details and is reviewed by admin and approved according to what it says here <https://advertising.reddithelp.com/en/categories/ad-review/about-reddits-ad-review-process> . But changing the value of admin_approval to APPROVED and effective_status to ACTIVE , the ads is approved and thus we receive the confirmation email from reddit ads that our ads is approved .


Impact:

Can bypass the review process and change the ads status to approve and active without payment process .

Reported April 17, 2022 5:55pm +0100


 bisesh

Participants   

State  Resolved ()

Reported to [Reddit](#) Managed

Disclosed June 22, 2022 6:05am +0100

Severity  High (7 - 8.9)

Weakness Business Logic Errors

Bounty \$5,000

Time spent None

54

#419883

H1514 [beerify.shopifycloud.com] GraphQL discloses internal beer consumption

Share:     

SUMMARY BY SHOPIFY

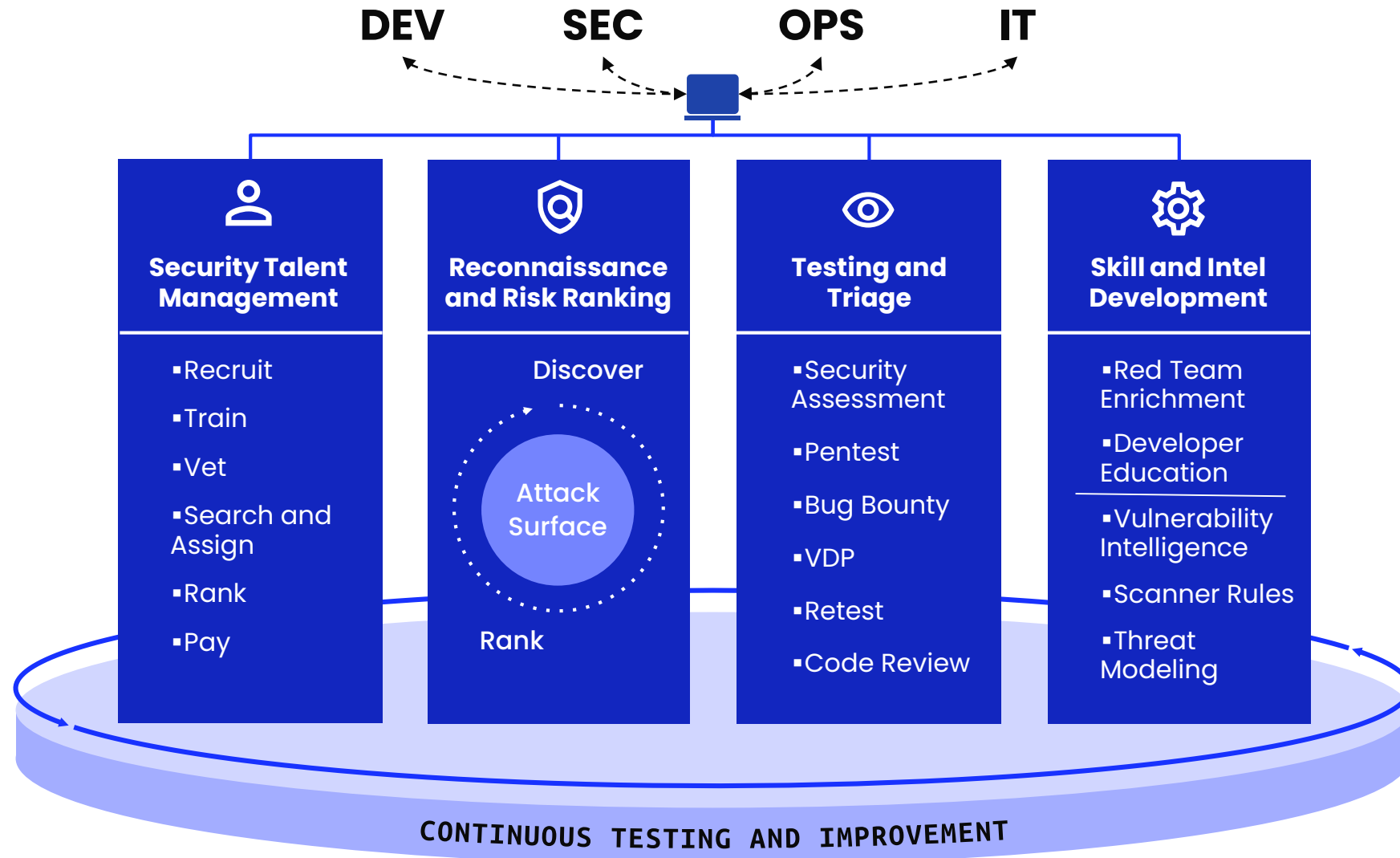
Reported October 6, 2018 12:33am +0100

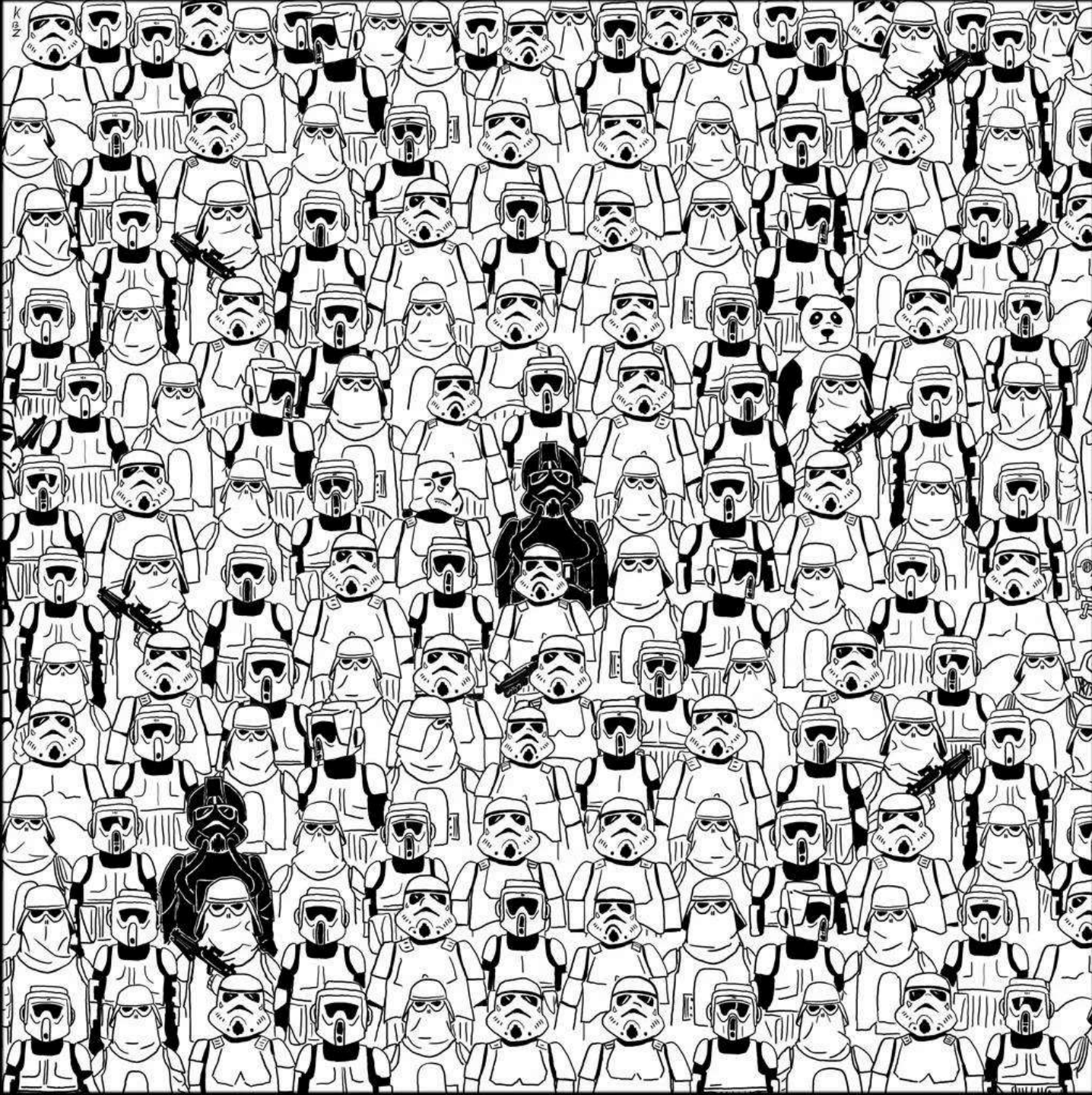
 emitrani

Participants     

220K+
Valid Reports

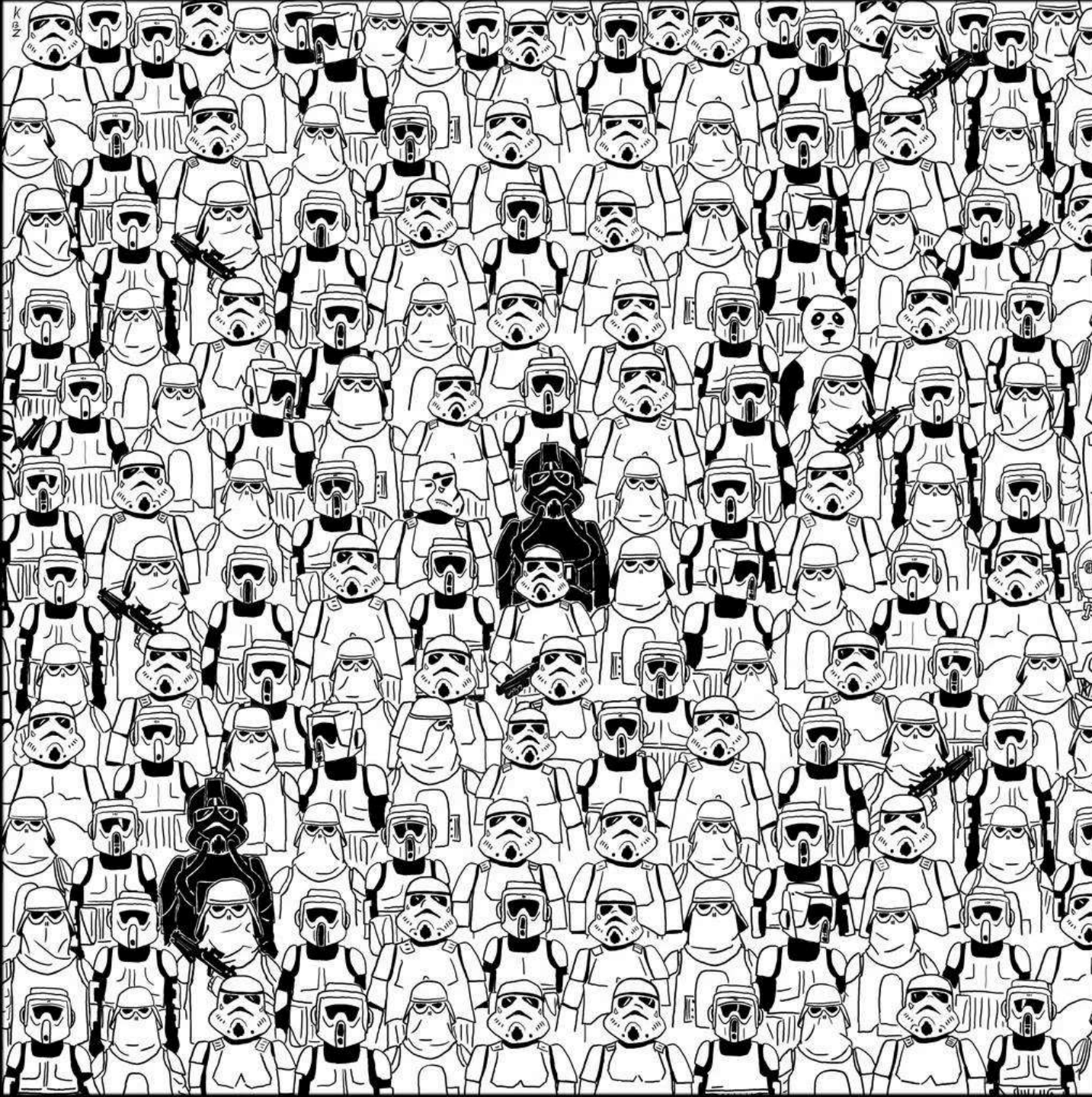
How Attack Resistance Management Works





**Use Hackers to help you
find the Pandas in your
company**

hackerone



Thank You!

Visit HackerOne's stand #7-514, Hall 7 to discuss your security program

Chris Dickens
Solutions Engineer



Learn more about
HackerOne solutions

hackerone