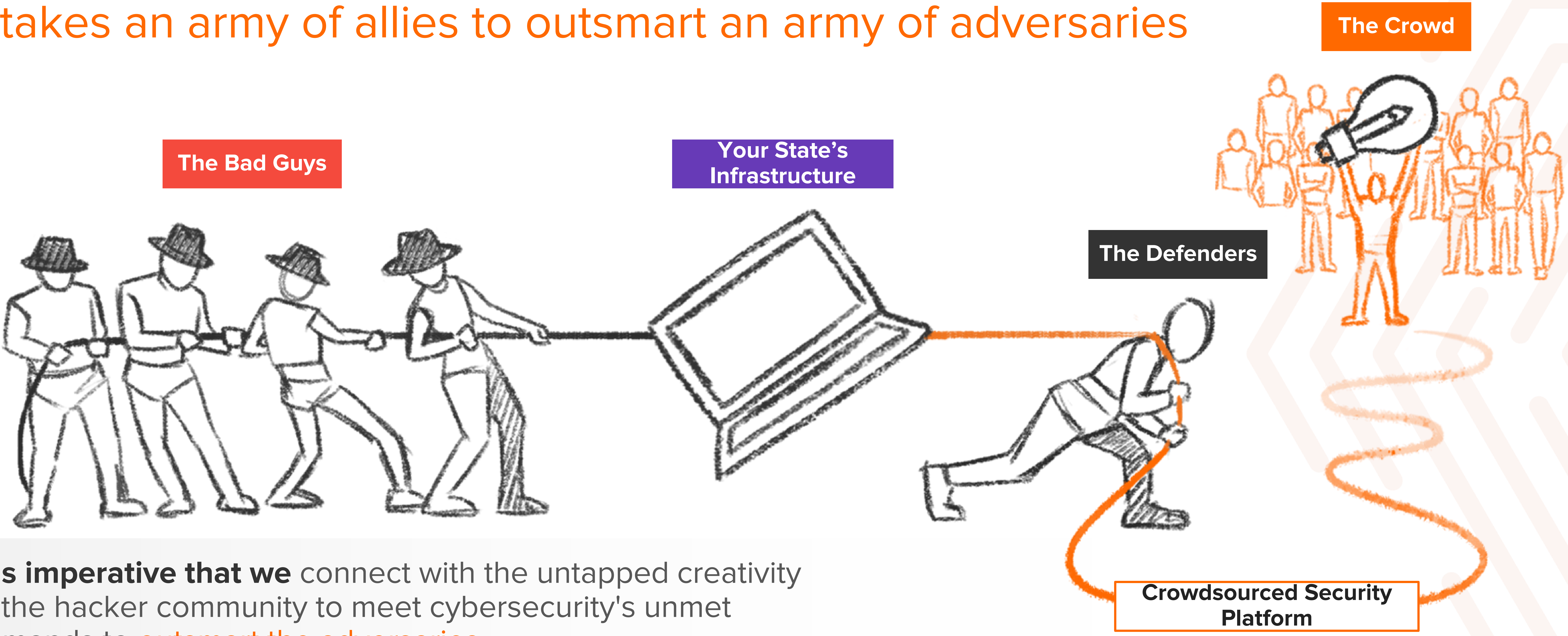
Iowa
Secretary of State Program: The Crowd as a Force Multiplier

Why are we here?

It takes an army of allies to outsmart an army of adversaries



The Crowd

The Bad Guys

Your State's Infrastructure

The Defenders

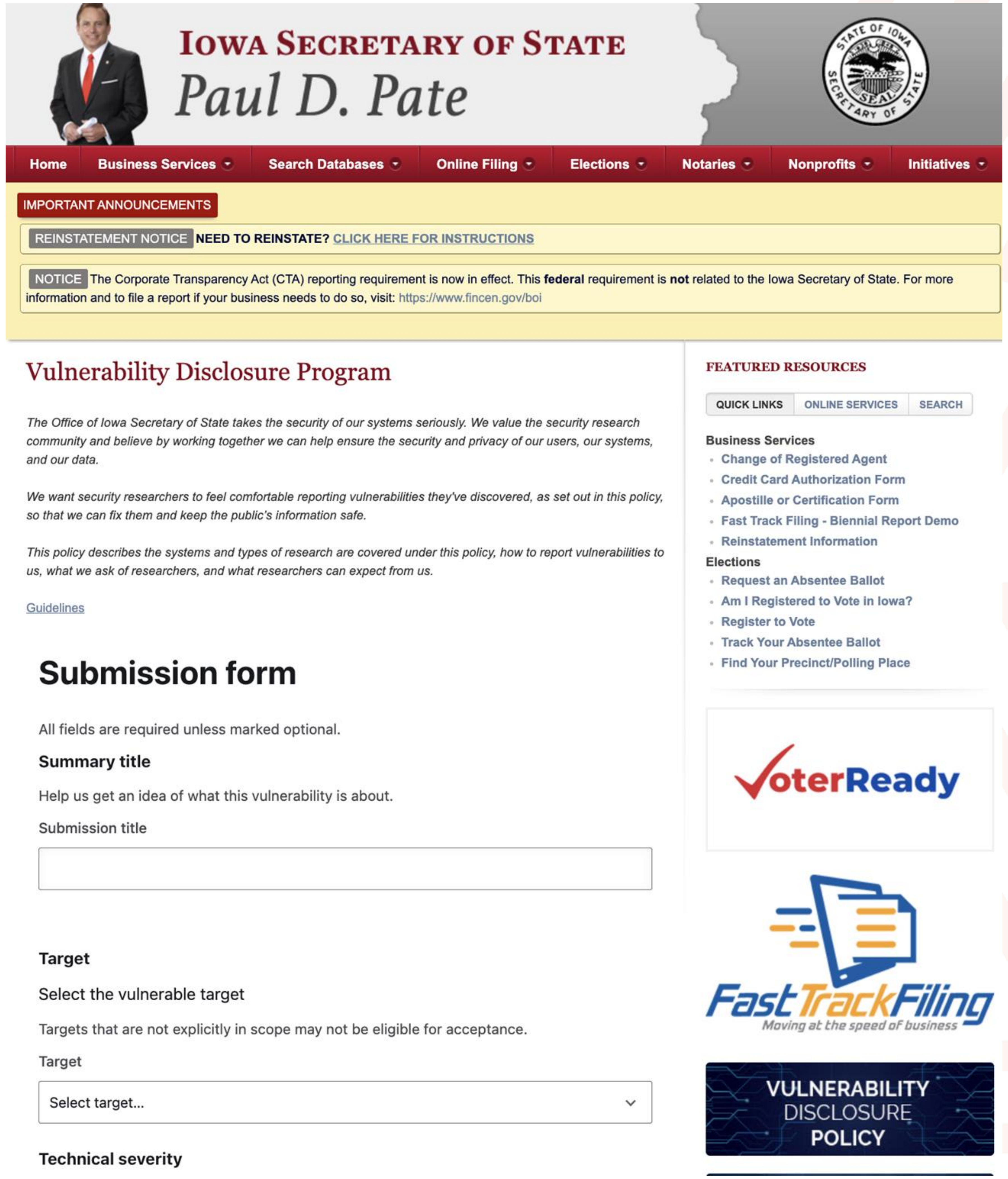
Crowdsourced Security Platform

It is imperative that we connect with the untapped creativity of the hacker community to meet cybersecurity's unmet demands to outsmart the adversaries

Iowa SoS Journey

Crowdsourced Security

- What is a Vulnerability Disclosure Program?
  - Internet's "Neighborhood Watch"
    - See Something, Say Something!
  - Structured Framework for organizations that allows ethical hackers, security researchers, and the general public to report vulnerabilities discovered in their systems, websites and applications



IMPORTANT ANNOUNCEMENTS

REINSTATEMENT NOTICE **NEED TO REINSTATE?** CLICK HERE FOR INSTRUCTIONS

NOTICE The Corporate Transparency Act (CTA) reporting requirement is now in effect. This **federal** requirement is **not** related to the Iowa Secretary of State. For more information and to file a report if your business needs to do so, visit: https://www.fincen.gov/boi

Vulnerability Disclosure Program

The Office of Iowa Secretary of State takes the security of our systems seriously. We value the security research community and believe by working together we can help ensure the security and privacy of our users, our systems, and our data.

We want security researchers to feel comfortable reporting vulnerabilities they've discovered, as set out in this policy, so that we can fix them and keep the public's information safe.

This policy describes the systems and types of research are covered under this policy, how to report vulnerabilities to us, what we ask of researchers, and what researchers can expect from us.

Guidelines

Submission form

All fields are required unless marked optional.

Summary title

Help us get an idea of what this vulnerability is about.

Submission title

Target

Select the vulnerable target

Targets that are not explicitly in scope may not be eligible for acceptance.

Target

Select target...

Technical severity

FEATURED RESOURCES

Business Services

- Change of Registered Agent
- Credit Card Authorization Form
- Apostille or Certification Form
- Fast Track Filing - Biennial Report Demo
- Reinstatement Information

Elections

- Request an Absentee Ballot
- Am I Registered to Vote in Iowa?
- Register to Vote
- Track Your Absentee Ballot
- Find Your Precinct/Polling Place

VoterReady
FastTrackFiling
Moving at the speed of business
VULNERABILITY DISCLOSURE POLICY

Iowa SoS Journey

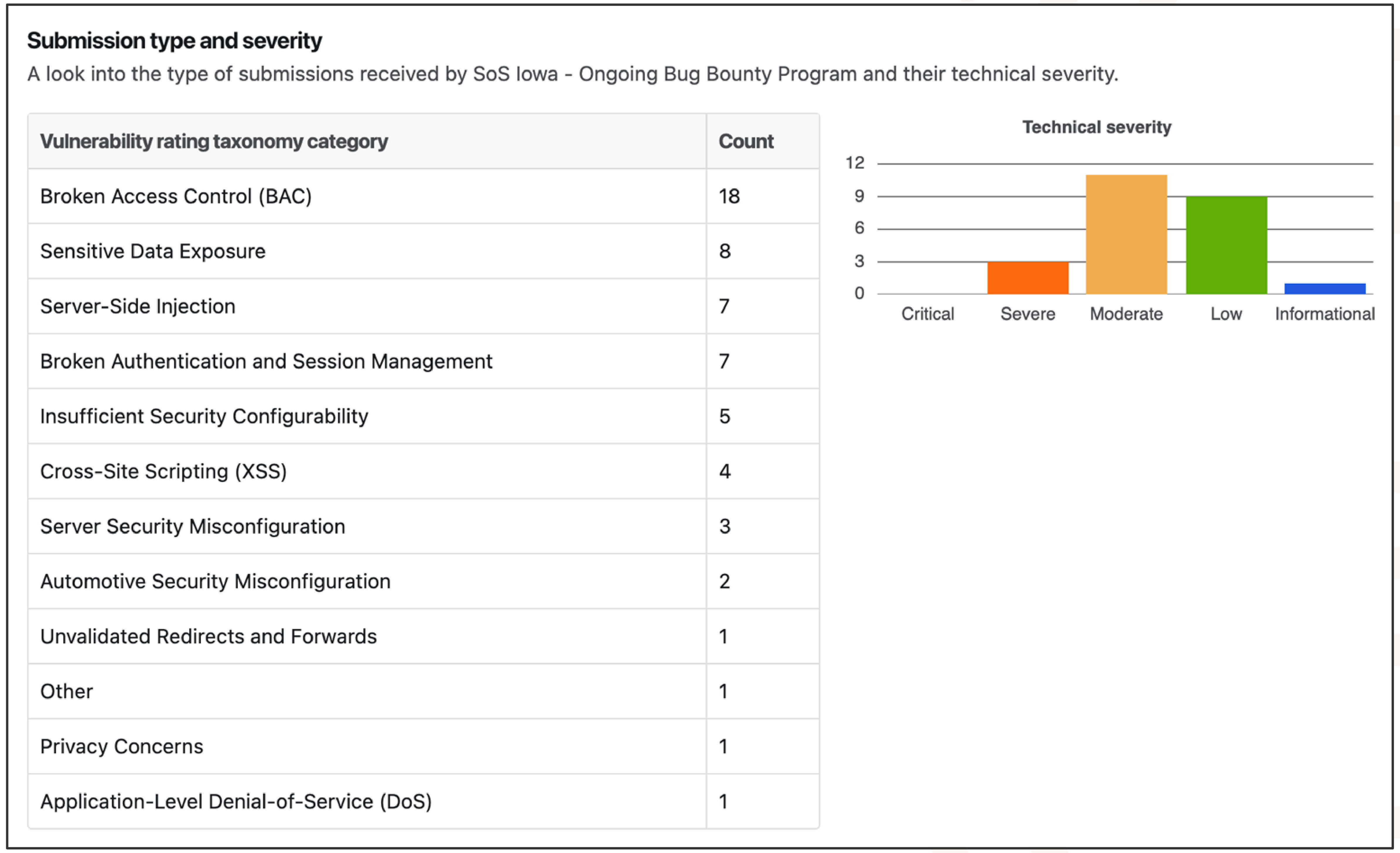
Starting Small and Adapting

- Using Penetration Tests
  - Great for specific point-in-time assessments / not continuous
  - Methodology based and compliance specific

- Incentivizing researchers to do more with Managed Bug Bounty Programs
  - Private and continuous in nature
  - Increased interest - stronger researchers
  - Pay for impact - reward researchers

- Challenges
  - Out of scope findings
  - When the researchers do the unexpected

Bug Bounty Program Results



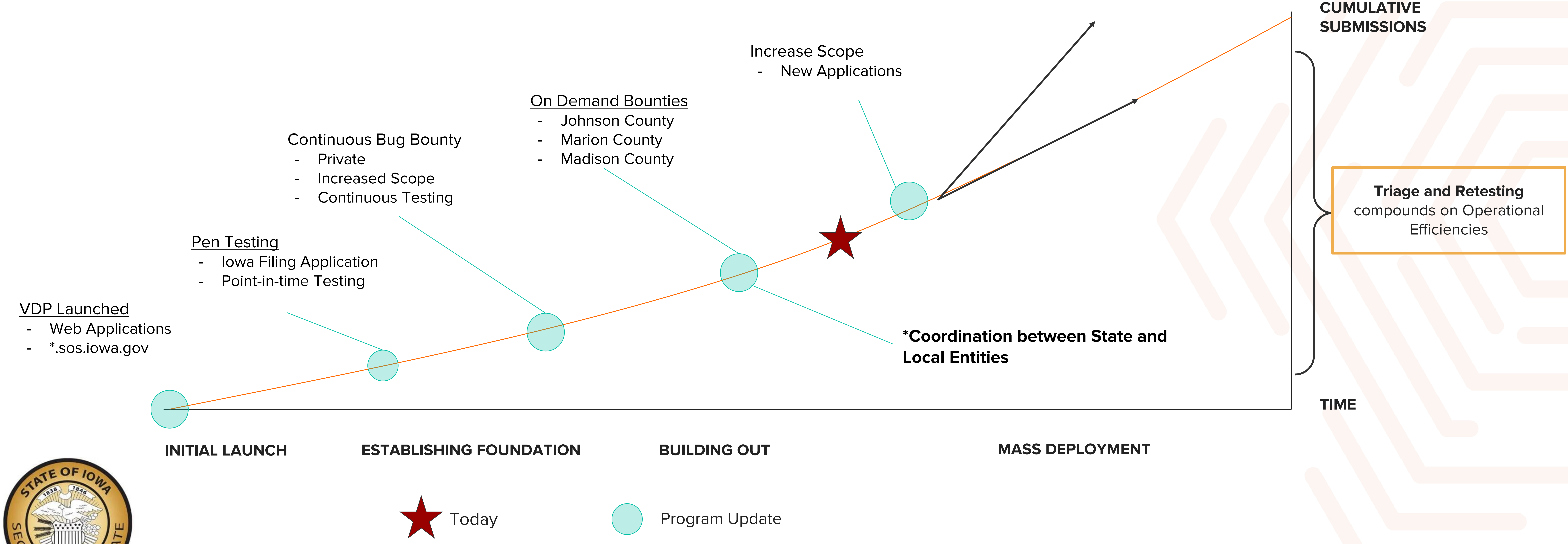
Submission type and severity

A look into the type of submissions received by SoS Iowa - Ongoing Bug Bounty Program and their technical severity.

Vulnerability rating taxonomy category	Count
Broken Access Control (BAC)	18
Sensitive Data Exposure	8
Server-Side Injection	7
Broken Authentication and Session Management	7
Insufficient Security Configurability	5
Cross-Site Scripting (XSS)	4
Server Security Misconfiguration	3
Automotive Security Misconfiguration	2
Unvalidated Redirects and Forwards	1
Other	1
Privacy Concerns	1
Application-Level Denial-of-Service (DoS)	1

What the Journey Looked Like

A strong focus on building trust between **Security** > **Engineering** > **Leadership**, but also between **Iowa SoS** and the researcher community.



CUMULATIVE SUBMISSIONS

VDP Launched
- Web Applications
- *.sos.iowa.gov

Pen Testing
- Iowa Filing Application
- Point-in-time Testing

Continuous Bug Bounty
- Private
- Increased Scope
- Continuous Testing

On Demand Bounties
- Johnson County
- Marion County
- Madison County

Increase Scope
- New Applications

***Coordination between State and Local Entities**

Triage and Retesting compounds on Operational Efficiencies

TIME

INITIAL LAUNCH

ESTABLISHING FOUNDATION

BUILDING OUT

MASS DEPLOYMENT

★ Today

● Program Update

Outcome: Increased security & trust with the Iowa constituency through a pay for impact vulnerability discovery program

Interesting Findings from Hackers

Potential spam and DoS misconfiguration

Vulnerability / “Bug” : Server Side Misconfiguration- No Rate Limiting (P4)

No rate limiting on a form triggering emails/submissions

↓

Spamming of e-mails to Iowa citizens

↓

Denial of Service to County Payment Application

Overview of the Vulnerability

- Rate Limiting prevents an application from becoming unresponsive or unavailable

Business Impact

- Business outage
- Financial cost
- Reputational damage

Why is this significant?
This vulnerability was fixed in multiple web applications across other counties in Iowa as a result of this single finding in a bug bounty.

Level the Playing Field

Accelerate Vuln Discovery

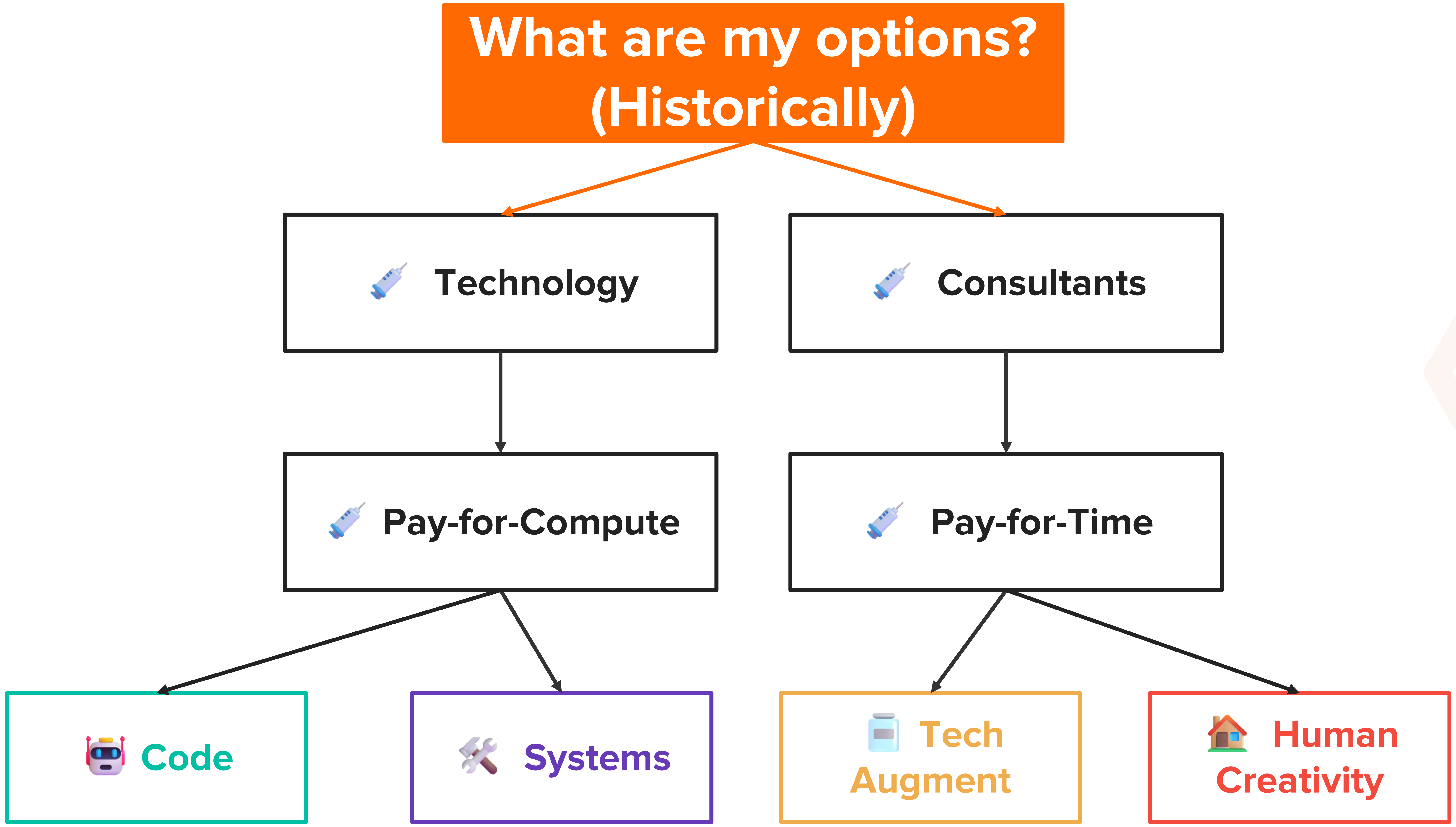
Use of Vulnerability Disclosure Programs and Bug Bounties

Access to Skills Knowledge Transfer

Embrace the crowd and tap into a wellspring of knowledge

Discovering Vulnerabilities, A History

Scalable



What are my options? (Historically)

Technology

Consultants

Pay-for-Compute

Pay-for-Time

Code

Systems

Tech Augment

Human Creativity

Value-driven

Crowdsourcing + *pay-for-results* incentives reduce risk across defined targets

Extends your team

Increase bandwidth and capabilities via access to skill sets on demand

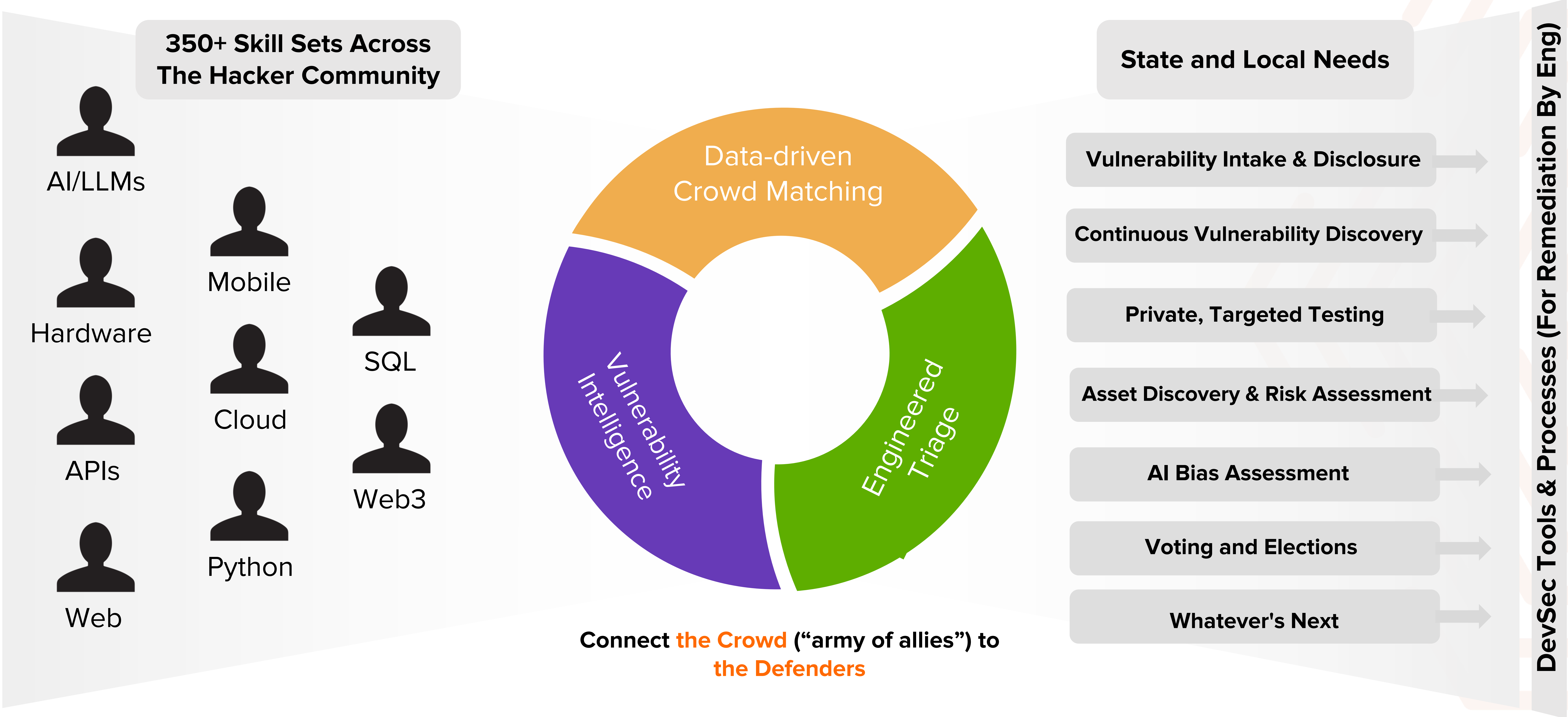
Finds more flaws

Reduce risk by finding 3x-5x more vulns prioritized by severity

Ties investments to results

Understand security Impact by paying rewards per vuln, not per hour

Unleashing human ingenuity for security



350+ Skill Sets Across The Hacker Community

AI/LLMs

Hardware

APIs

Web

Mobile

Cloud

Python

SQL

Web3

Data-driven Crowd Matching

Engineered Triage

Vulnerability Intelligence

Connect the Crowd ("army of allies") to the Defenders

State and Local Needs

Vulnerability Intake & Disclosure

Continuous Vulnerability Discovery

Private, Targeted Testing

Asset Discovery & Risk Assessment

AI Bias Assessment

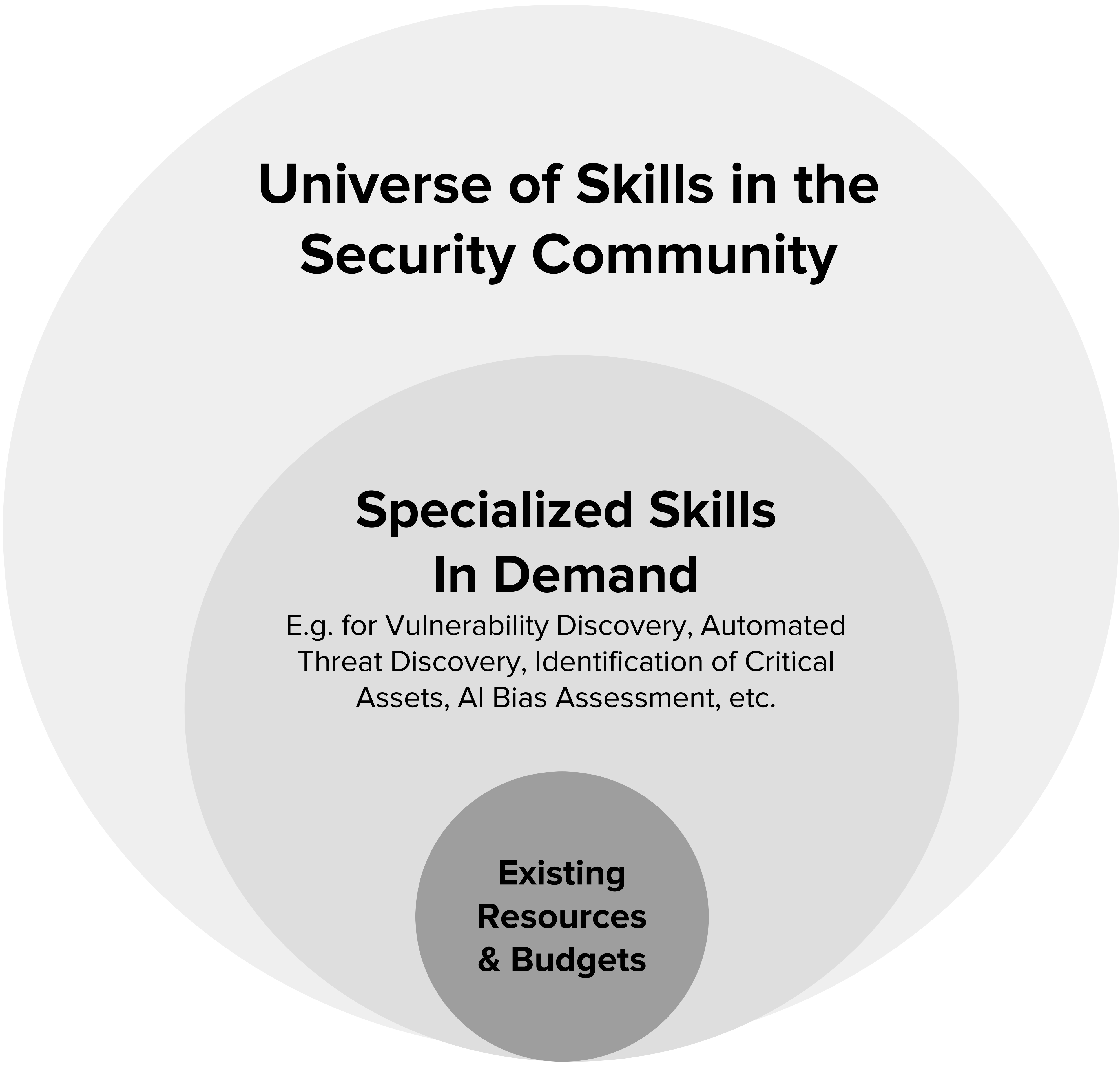
Voting and Elections

Whatever's Next

DevSec Tools & Processes (For Remediation By Eng)

The Force Multiplier

Demand for skills is growing, while access to them is shrinking



Universe of Skills in the Security Community

Specialized Skills In Demand

E.g. for Vulnerability Discovery, Automated Threat Discovery, Identification of Critical Assets, AI Bias Assessment, etc.

Existing Resources & Budgets

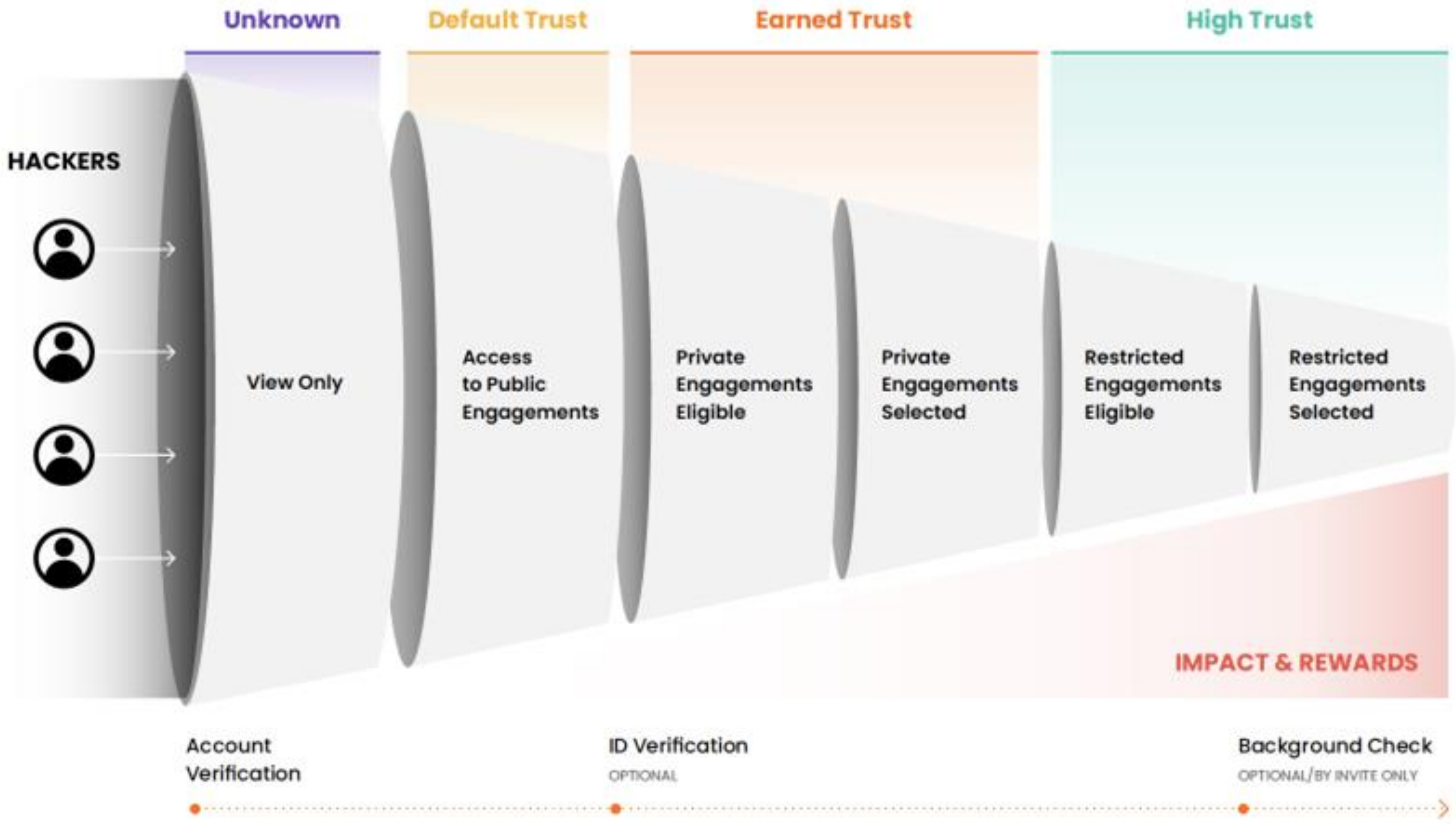
We don’t have a “cybersecurity hiring gap” in the Public Sector – we have an **“access-to-skills gap”** that is blocking progress

For years, consumers have relied on on-demand platforms to tap an elastic supply of millions of workers for various tasks

Why can’t we make the cybersecurity talent pool work the same way for scale and agility?

Trust in the crowd

How to build the right trusted hacker team for your state and programs



Continuously assesses and scores every individual to provide quantitative and qualitative understanding of:

- Skills
- Motivation
- Trustworthiness
- Reliability
- Collaboration
- Engagement

Leverage clearances and enhanced background checks when needed, but remember there can be security built into larger numbers

Trending Across Industries

↑12%
increase in submissions
COMPUTER SOFTWARE

↓2%
decrease in submissions
COMPUTER HARDWARE

↑20%
increase in submissions
CORPORATE SERVICES

↑11%
increase in submissions
FINANCIAL SERVICES

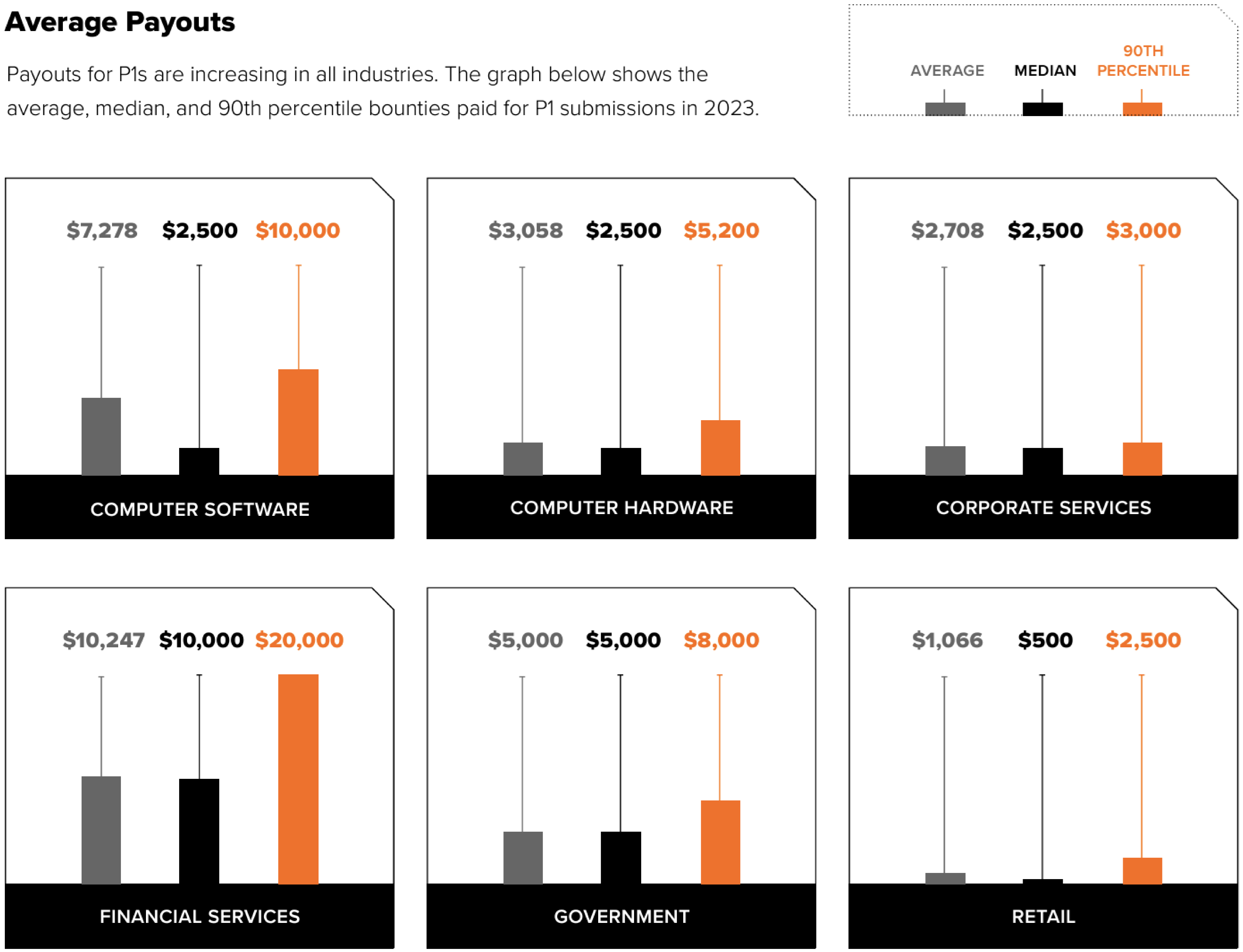
↑151%
increase in submissions
GOVERNMENT

↑34%
increase in submissions
RETAIL

Payouts Per Industry

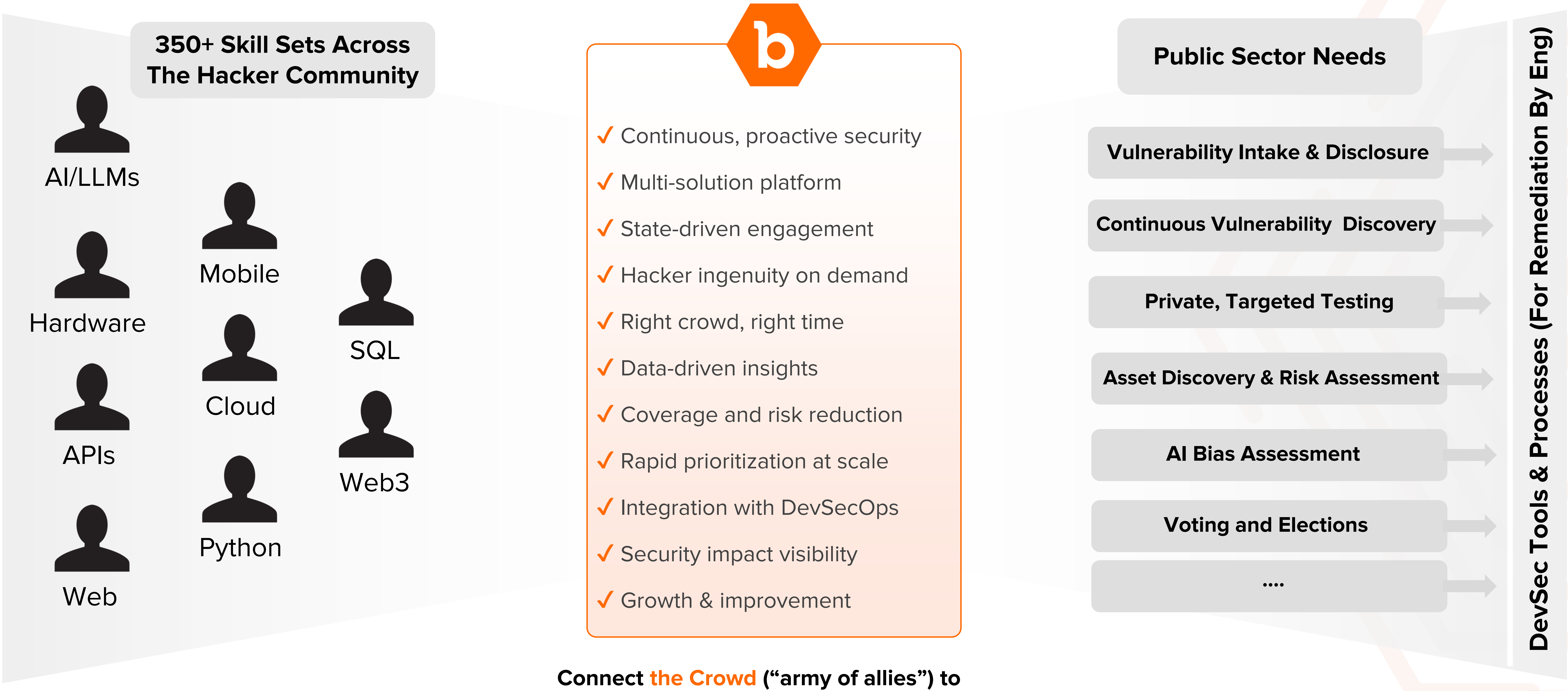
Average Payouts

Payouts for P1s are increasing in all industries. The graph below shows the average, median, and 90th percentile bounties paid for P1 submissions in 2023.



In 2023, programs with open scopes received 10x more P1 vulnerabilities than those with limited scopes.

Unleashing human ingenuity for security



350+ Skill Sets Across The Hacker Community

AI/LLMs

Mobile

Hardware

SQL

Cloud

APIs

Web3

Python

Web

✓ Continuous, proactive security

✓ Multi-solution platform

✓ State-driven engagement

✓ Hacker ingenuity on demand

✓ Right crowd, right time

✓ Data-driven insights

✓ Coverage and risk reduction

✓ Rapid prioritization at scale

✓ Integration with DevSecOps

✓ Security impact visibility

✓ Growth & improvement

Public Sector Needs

Vulnerability Intake & Disclosure

Continuous Vulnerability Discovery

Private, Targeted Testing

Asset Discovery & Risk Assessment

AI Bias Assessment

Voting and Elections

....

DevSec Tools & Processes (For Remediation By Eng)

Connect the Crowd (“army of allies”) to the Defenders

The Force Multiplier

Q&A

Contact:

Kent Wilson
kent.wilson@bugcrowd.com
https://www.linkedin.com/in/wkentwilson/