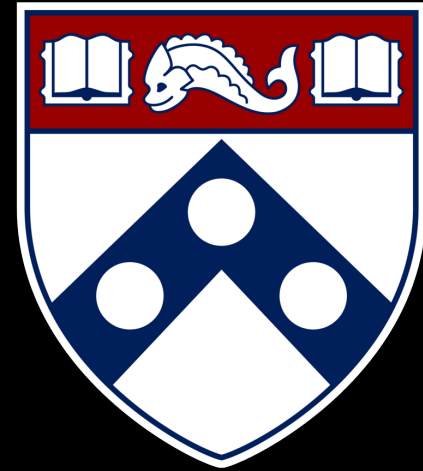


Empirical Security & Privacy, for Humans



UPenn CIS 7000-010
9/16/2025



The Cyberattack business

Readings



Systematically Understanding the Cyber Attack Business: A Survey

KEMAN HUANG, MICHAEL SIEGEL, and STUART MADNICK,
Massachusetts Institute of Technology

Cyber attacks are increasingly menacing businesses. Based on the literature review and publicly available reports, this article conducts an extensive and consistent survey of the services used by the cybercrime business, organized using the value chain perspective, to understand cyber attack in a systematic way. Understanding the specialization, commercialization, and cooperation for cyber attacks helps us to identify 24 key value-added activities and their relations. These can be offered "as a service" for use in a cyber attack. This framework helps to understand the cybercriminal service ecosystem and hacking innovations. Finally, a few examples are provided showing how this framework can help to build a more cyber immune system, like targeting cybercrime control-points and assigning defense responsibilities to encourage collaboration.

CCS Concepts: • **Social and professional topics** → **Computing and business; Socio-technical systems; Computer crime; • Security and privacy** → **Social aspects of security and privacy; Systems security; Social network security and privacy;**

Additional Key Words and Phrases: Cyber attack business, cyber crime, value chain model, cyber-crime-as-a-service, hacking innovation, control point, sharing responsibility

ACM Reference format:

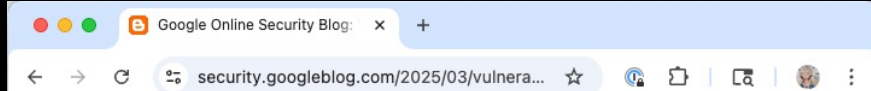
Keman Huang, Michael Siegel, and Stuart Madnick. 2018. Systematically Understanding the Cyber Attack Business: A Survey. *ACM Comput. Surv.* 51, 4, Article 70 (July 2018), 36 pages.
<https://doi.org/10.1145/3199674>

1 INTRODUCTION

"Where there is commerce, there is also the risk for cybercrime" [131].

Cybercrime is a tremendous threat to today's digital society. It is estimated that the cost of cybercrime will grow from an annual sum of \$3 trillion in 2015 to \$6 trillion by the year 2021 [109]. Nearly one-third of companies are affected by cybercrime (32%). Indeed, 61% of CEOs are concerned with the state of the cyber security of their company [124]. It has become generally accepted that, "there are only two types of companies: those that have been hacked and those that

70



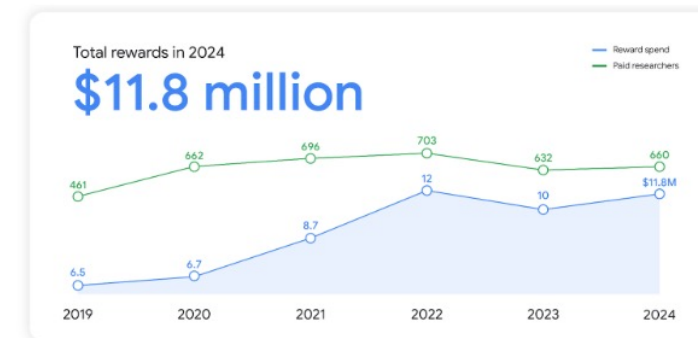
Vulnerability Reward Program: 2024 in Review

March 7, 2025

Posted by Dirk Göhmann

In 2024, our Vulnerability Reward Program confirmed the ongoing value of engaging with the security research community to make Google and its products safer. This was evident as we awarded just shy of \$12 million to over 600 researchers based in countries around the globe across all of our programs.

Vulnerability Reward Program 2024 in Numbers



Readings



Systematically Understanding the Cyber Attack Business: A Survey

KEMAN HUANG, MICHAEL SIEGEL, and STUART MADNICK,
Massachusetts Institute of Technology

Cyber attacks are increasingly menacing businesses. Based on the literature review and publicly available reports, this article conducts an extensive and consistent survey of the services used by the cybercrime business, organized using the value chain perspective, to understand cyber attack in a systematic way. Understanding the specialization, commercialization, and cooperation for cyber attacks helps us to identify 24 key value-added activities and their relations. These can be offered "as a service" for use in a cyber attack. This framework helps to understand the cybercriminal service ecosystem and hacking innovations. Finally, a few examples are provided showing how this framework can help to build a more cyber immune system, like targeting cybercrime control-points and assigning defense responsibilities to encourage collaboration.

CCS Concepts: • **Social and professional topics** → **Computing and business**; **Socio-technical systems**; **Computer crime**; • **Security and privacy** → **Social aspects of security and privacy**; **Systems security**; **Social network security and privacy**;

Additional Key Words and Phrases: Cyber attack business, cyber crime, value chain model, cyber-crime-as-a-service, hacking innovation, control point, sharing responsibility

ACM Reference format:

Keman Huang, Michael Siegel, and Stuart Madnick. 2018. Systematically Understanding the Cyber Attack Business: A Survey. *ACM Comput. Surv.* 51, 4, Article 70 (July 2018), 36 pages.
<https://doi.org/10.1145/3199674>

1 INTRODUCTION

"Where there is commerce, there is also the risk for cybercrime" [131].

Cybercrime is a tremendous threat to today's digital society. It is estimated that the cost of cybercrime will grow from an annual sum of \$3 trillion in 2015 to \$6 trillion by the year 2021 [109]. Nearly one-third of companies are affected by cybercrime (32%). Indeed, 61% of CEOs are concerned with the state of the cyber security of their company [124]. It has become generally accepted that, "there are only two types of companies: those that have been hacked and those that

Cybercrime: Big \$\$

- Paper: “It is estimated that the cost of cybercrime will grow from an annual sum of **\$3 trillion in 2015 to \$6 trillion in 2021**” – cited 2016 report by Cybersecurity Ventures
- Evolve Security blog post (written 2023?) agrees with those numbers, estimates **\$20 trillion cost by 2026**

The screenshot shows a web browser displaying the Evolve Security blog post. The URL in the address bar is evolvesecurity.com/blog-posts/actual-cost-of-cybercrime. The page has a dark blue header with the Evolve Security logo and navigation links: Penetration Testing, Platform, Attack Surface Management, Strategic Advisory, Partners, and Co. A light blue banner at the top right says "Register for your complimentary CTEM Fast Track Assessment". The main content area has a light blue background. On the left, there is a "Contents" sidebar with links: "What Is the Impact of Cybercrime on Organizations?", "Statistics of Cybercrime Costs" (highlighted), and "Protect Your Organization's Financial Health from Cybercrime with Evolve Security". The main article title is "The Cost of Cybercrime in the U.S". The text discusses statistics from NIST and the FBI, noting that cybercrime costs the U.S. hundreds of billions, potentially 1-4% of GDP. It mentions a 2021 FBI report where losses amounted to nearly \$7 billion, with BEC schemes causing nearly \$2.4 billion in losses. The article also mentions that this figure skyrockets if unreported incidents are factored in. Below this, there is a section titled "The Global Cost of Cybercrime" which states that the global cost was estimated to surpass \$8 trillion in 2022 and is expected to go beyond \$11 trillion in 2023. It predicts that cybercrime will cost the global economy more than 20 trillion U.S. dollars by 2026, a 1.5 times increase compared to 2022. The final paragraph states that the cybercrime industry is growing year after year, with global damages costing \$6 trillion in 2021, expected to grow by 15% annually, reaching \$10.5 trillion by 2025, up from \$3 trillion in 2015.

← → ↺ 🔍 evolvesecurity.com/blog-posts/actual-cost-of-cybercrime ☆ ⓘ 🗖

Register for your complimentary CTEM Fast Track Assessment →

EVOLVE SECURITY Penetration Testing Platform Attack Surface Management Strategic Advisory Partners Co

Contents

- What Is the Impact of Cybercrime on Organizations?
- Statistics of Cybercrime Costs**
- Protect Your Organization's Financial Health from Cybercrime with Evolve Security

The Cost of Cybercrime in the U.S

Statistics from the National Institute of Standards and Technology (NIST) suggests that cybercrime costs the United States hundreds of billions, potentially as much as 1–4% of America's annual GDP (Source: [NIST](#)).

A 2021 FBI report says that out of 847,376 cybercrime cases reported in 2021, the losses amounted to nearly \$7 billion. Among the reported cases, business e-mail compromise (BEC) schemes, ransomware, and cryptocurrency scams were among the reported incidents. Out of the amount, BEC caused losses of nearly \$2.4 billion. This figures skyrockets quickly if you factor in unreported incidents (Source: [FBI Internet Crime Report 2021](#)).

The Global Cost of Cybercrime

The global cost of cybercrime was estimated to surpass \$8 trillion in 2022. The figure is expected to go beyond \$11 trillion in 2023. Statistics predict that cybercrime will cost the global economy more than 20 trillion U.S dollars by 2026, a 1.5 times increase compared to figures in 2022 (Source: [Statista](#)).

The cybercrime industry is growing year after year. In 2021, it caused global damages that costed \$6 trillion. The value is expected to grow by 15% annually over the next five years. By 2025, experts predict that the number will reach (and surpass) \$10.5 trillion, up from \$3 trillion in 2015 (Source: [Cybersecurity Ventures](#)).

Understanding cyber criminals

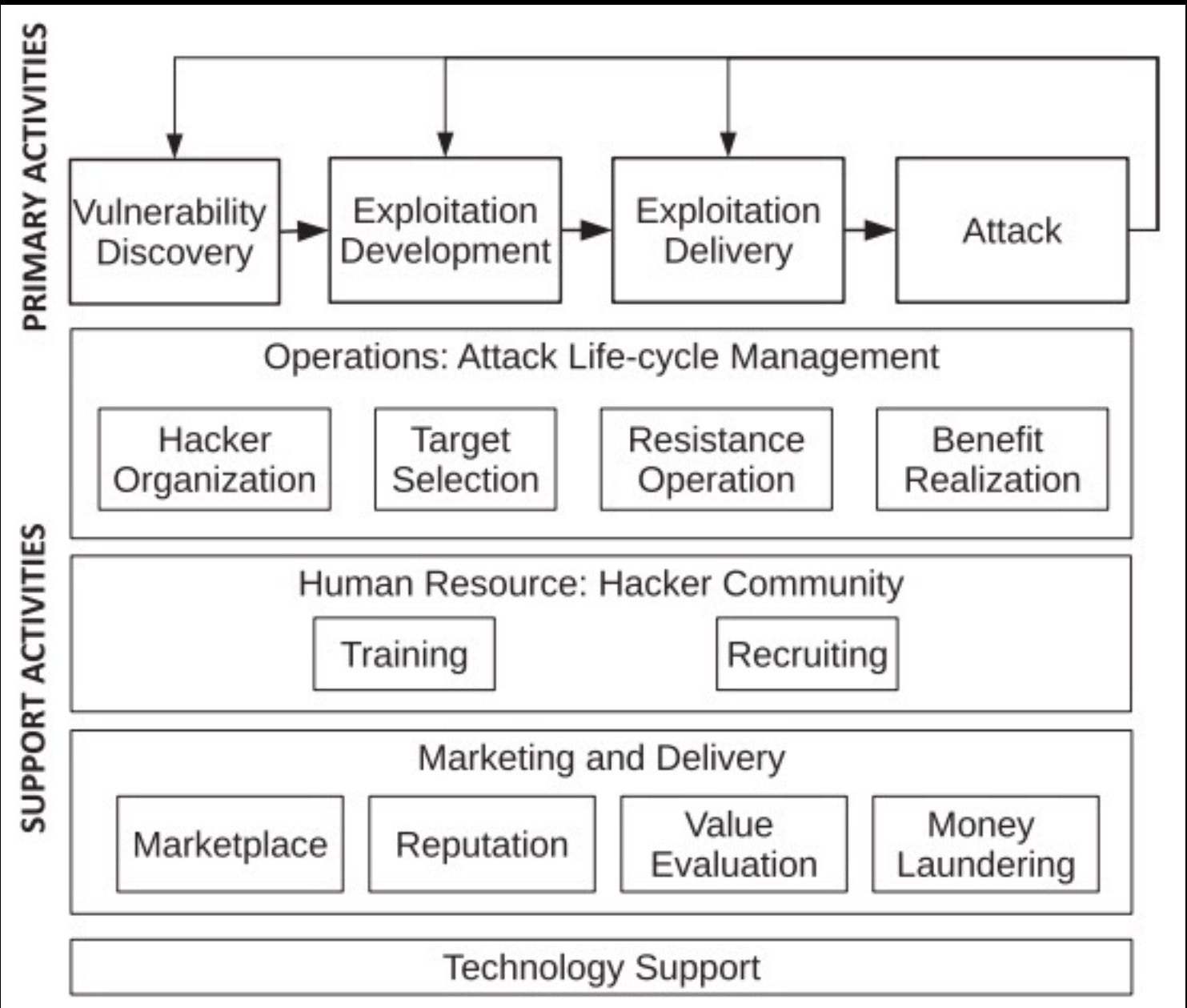
- Cybersecurity landscape has three main actors: **victims** (users), **attackers**, and **defenders** (cybersecurity product sellers)
- Grigg models victims and defenders, but **ignores attackers** (treated like “nature” in safety assessments)
- Hypothesis of Huang et al. paper: Understanding attackers and the business of cybercrime offers **opportunities for better defense**



Approach

- Survey the literature that reveals the various practices of the cybercrime business
- Develop a framework in which to categorize and group these practices: The **cybercriminal value chain model**
 - Vulnerability discovery, exploitation development & delivery, attack, and underlying supports
- Model an observed trend: Cybercrime is organized into **services**
 - Enables specialization, commercialization, and cooperation among actors with different skillsets
- All of this may reveal opportunities for disruption

Cybercriminal Value Chain Model



Cyberattack target selection rule

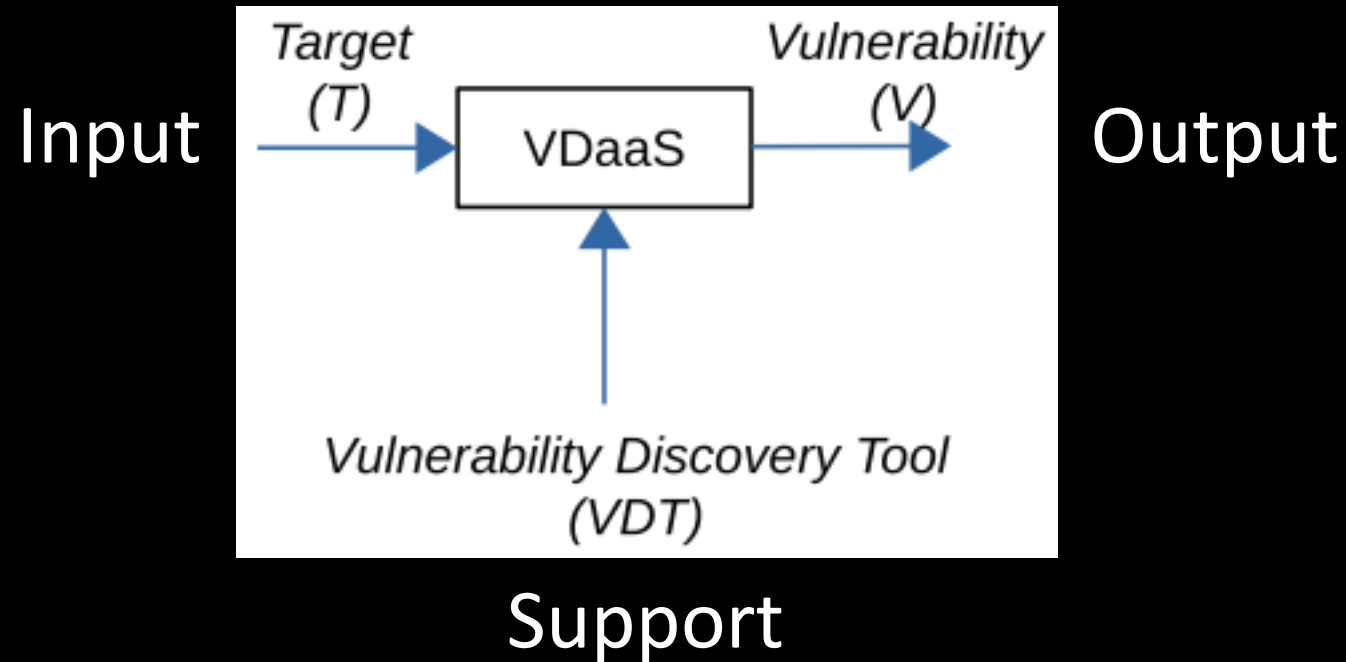
$$P_e \times (B_{pm} + B_{pp}) \times E_r > C_{ps} + (P_a \times P_c \times C_c) + (C_{im} + C_{om})$$

Expected benefit

Expected cost

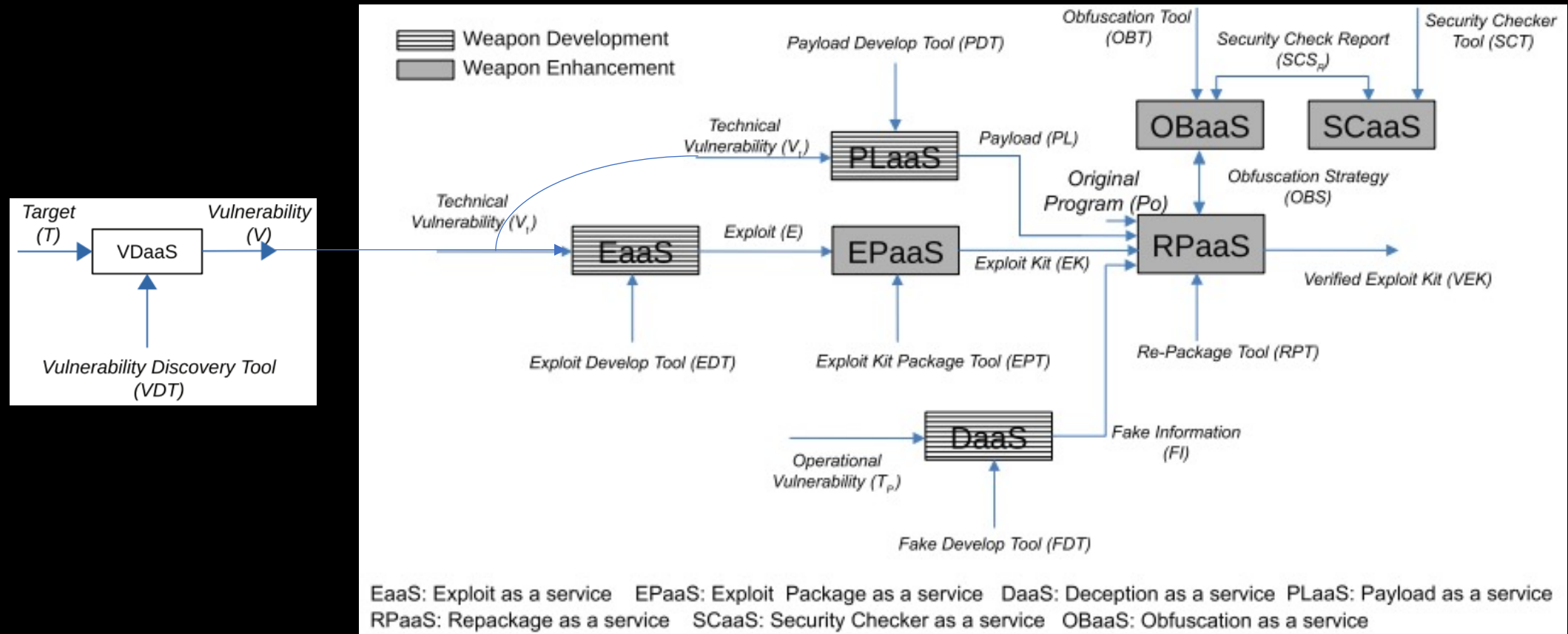
Cybercriminal service model

An application of “service science”



Smaller services can compose into larger ones, including with iteration-based refinement

Composition: Exploit kit development service



Ukraine power grid attack

For example, in the Ukraine power grid cyber attack,

- *the **spear-fishing emails** from **DaaS** (fake information),*
- *the **exploit kit targeting vulnerabilities**, ... from **EPaaS** (exploit kit),*
- *the KillDisk, a destructive **data-wiping utility**, and the **SSH backdoor** to maintain persistent access from **PLaaS** (payload),*

were used in tandem to successfully break into the Ukrainian power grid system.

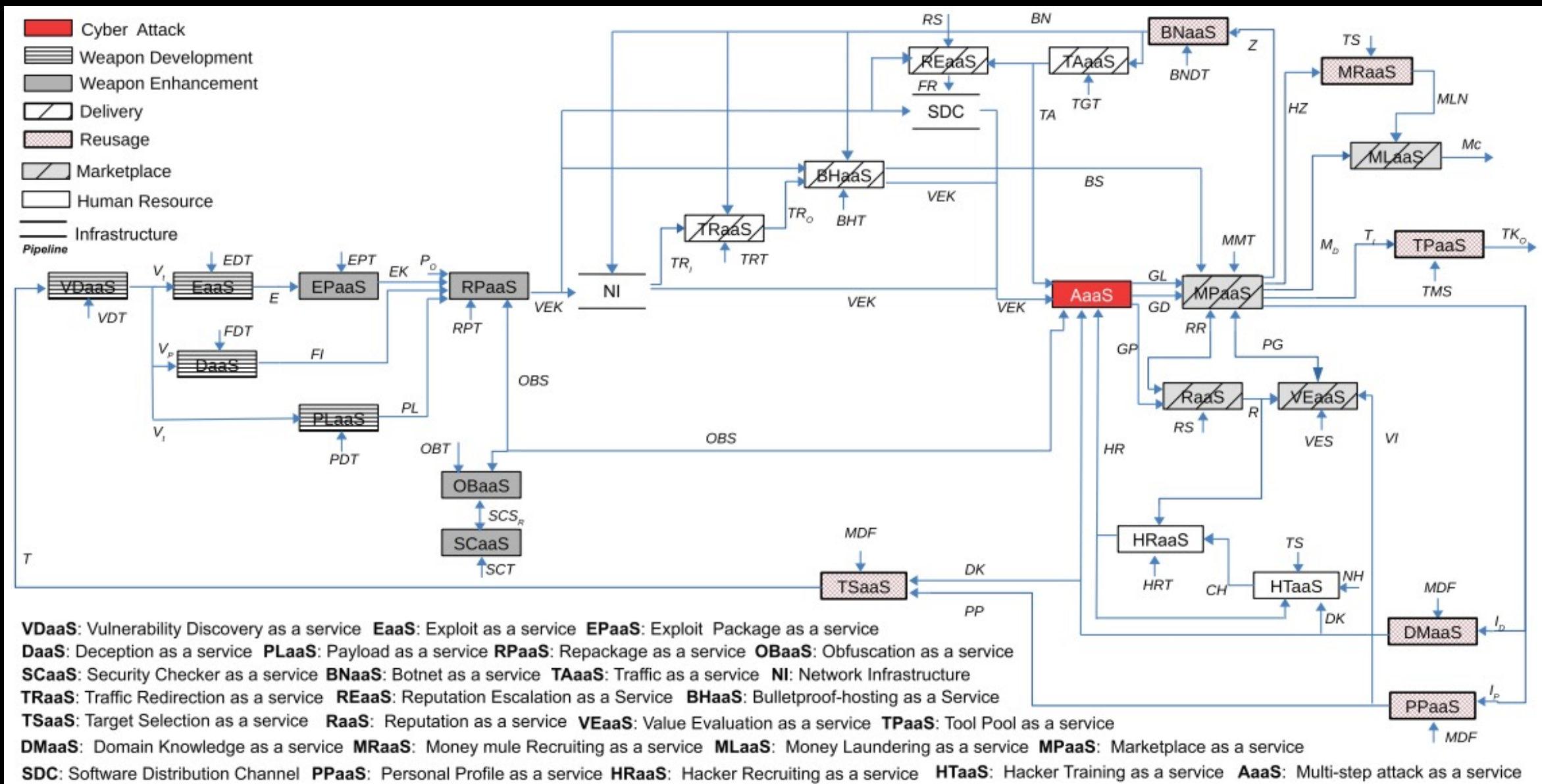
*In the second step of the same attack, **malicious firmware** (from **PLaaS**) developed based on domain knowledge collected from the distribution management system,*

*which was tested by the **simulated power grid system** (from **SCaaS**), was uploaded to the system and to attack the ICS components.*

Status and typical pricing of cybercrime services

Service	Status	Pricing Model	Example Case	Estimated Price
EaaS	Existing	License	Exploit Trading [71]	up to more than \$250,000
		Subscription	Up-to-date Zero-day Exploits [151]	\$150,000 per month
PLaaS	Existing	Pay-per-install Commission	Payload Renting [10, 16]	\$0.02–0.10 per install 40%
DaaS	Existing	Subscription	Phishing Service [145]	\$85–\$115 per month 40%
		Commission	Fake Anti-virus [97]	
OBaaS	Existing	Subscription	Obfuscation Platform [50]	\$50–150 per month
SCaaS	Existing	Subscription	Scan4you [72]	\$25 per month
TRaaS	Existing	Pay-per-click	Traffic Redirection [50]	\$7–\$15 per 1,000 visitors
BNaaS	Existing	Subscription	Botnet Shops [145]	\$40 per month
BHaaS	Existing	Subscription	Cloud Bulletproof Servers [100]	\$300 per month
TAaaS	Existing	Subscription	DDoS Attack Service [134]	\$999 per month
REaaS	Existing	Pay-per-record	Reputation Escalation Markets [170]	\$0.4–0.7 per record
MPaaS	Existing	License	Market Framework [35]	\$4,500 per licence
		Commission	Marketplace [34]	2%–10%
MRaaS	Existing	License	Money Laundering Recruitment Package [99]	\$1,700 per licence
MLaaS	Existing	Commission	Money Laundering Service [127]	2%–30%
HTaaS	Existing	License	Hacker Training Courses [138]	\$250–\$800 per person
PPaaS	Evolving	License	Personal Profile Investigator [59]	\$4–\$20 per record
TPaaS	Evolving	Subscription	“One-stop-shop” Platform [2, 73]	\$4,000 per month
RaaS	Evolving	Subscription	Smart Contract [79]	/
HRaaS	Evolving	Subscription	Online Hacker Recruiting Market [105]	/
VDaaS	Emerging	Subscription	Bug Bounty Program [132]	\$542.04–\$1810.31 per vulnerability
TSaaS	Emerging	Subscription	Targets Ranking based on Value [101]	/
EPaaS,RPaaS	Emerging	Subscription	Repackaging Platform [143, 151]	\$4,000 per month
DMaaS	Emerging	Subscription	“How-to” Knowledge Systems [27]	/
VEaaS	Emerging	Subscription	Comparison “Shopping” Service [57]	/

Services are defined and explained in the following sections. Examples for existing services are actual, emerging, and evolving services are based on offensive versions of actual legitimate services. Prices listed here are intended to be representative of current prices and are constantly evolving.



Putting it all together: Multi-step attack as a service

Example Costs: Ransomware

To run a ransomware attack as a business, a cybercriminal can

- *buy **BNaaS (botnet)** for \$999 per month,*
- *a **traffic redirection protocol** for \$600,*
- *six servers as a part of **BHaaS (bulletproof server)** for \$1,800 per month,*
- *access to the **Neutrino exploit kit in EPaaS (exploit package)** for \$4,000,*
- *a **ransomware payload with customer support in PLaaS (payload)** for \$3,000 and*
- *the **traffic redirection service TRaaS** to redirect victims to servers for \$600 per month.*

To further increase the effectiveness of an attack, a cybercriminal can

- *hire a **qualified hacker from HRaaS** for \$2,000 per month, and*
- *employ an **obfuscation service from OBaaS** to repackage the exploit kit and payload for \$600 per month.*

*Finally, to reduce risk of arrest, services to monetize benefits in the wake of a cyber attack as a part of **MLaaS (money laundering)** can be accessed for a fee of \$400 and 40% commission on processed funds.*

Ransomware Benefits and ROI

Assume **30,000 people** are redirected **per day**, of which **10% are victims** of a ransomware attack where **0.5% of victims pay a \$300 ransom**.

- Though only 450 victims (0.05% of total users redirected) will end up paying the ransom over a period of one month (30 days), this brings the cybercriminal's **monthly earnings to \$135,000**.

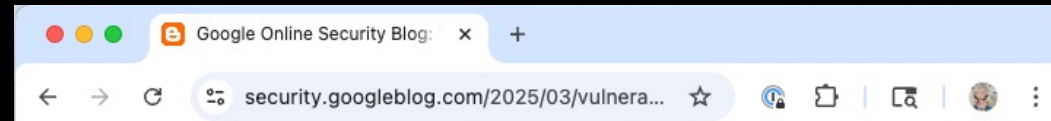
We can see that the **Return-On-Investment (ROI)**, even when only a small proportion of people end up paying a ransom, **is as high as 504.52%**, an impressive ROI for a business.

- The highest industrial ROI, which is from the Tobacco industry, is only 50.63% in August 2017

Discussion points

- General: What does all of this teach us?
- This paper was from 2016. What's happened in the meantime that might have changed things?
- How would we decide where is to disrupt this network, if we wanted to try?
- How do nation-state actors fit into this framework?
- What is the implication of “two way” services like vulnerability discovery training?
- Attacker motivations (“psychological”) might sometimes differ from defenders (reduce loss). Ramifications?

Readings



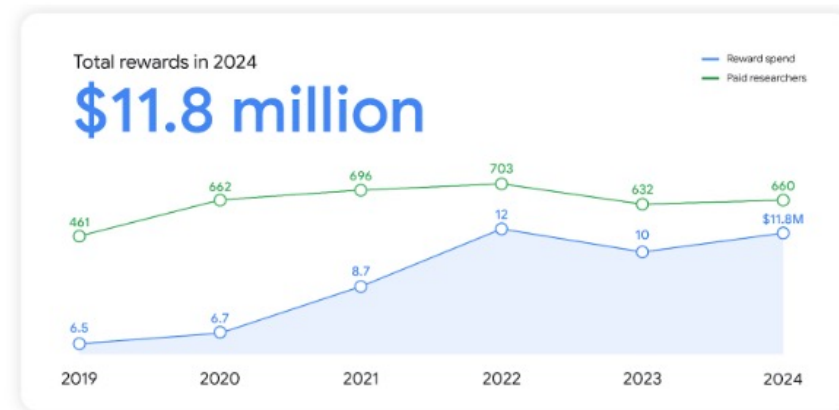
Vulnerability Reward Program: 2024 in Review

March 7, 2025

Posted by Dirk Göhmann

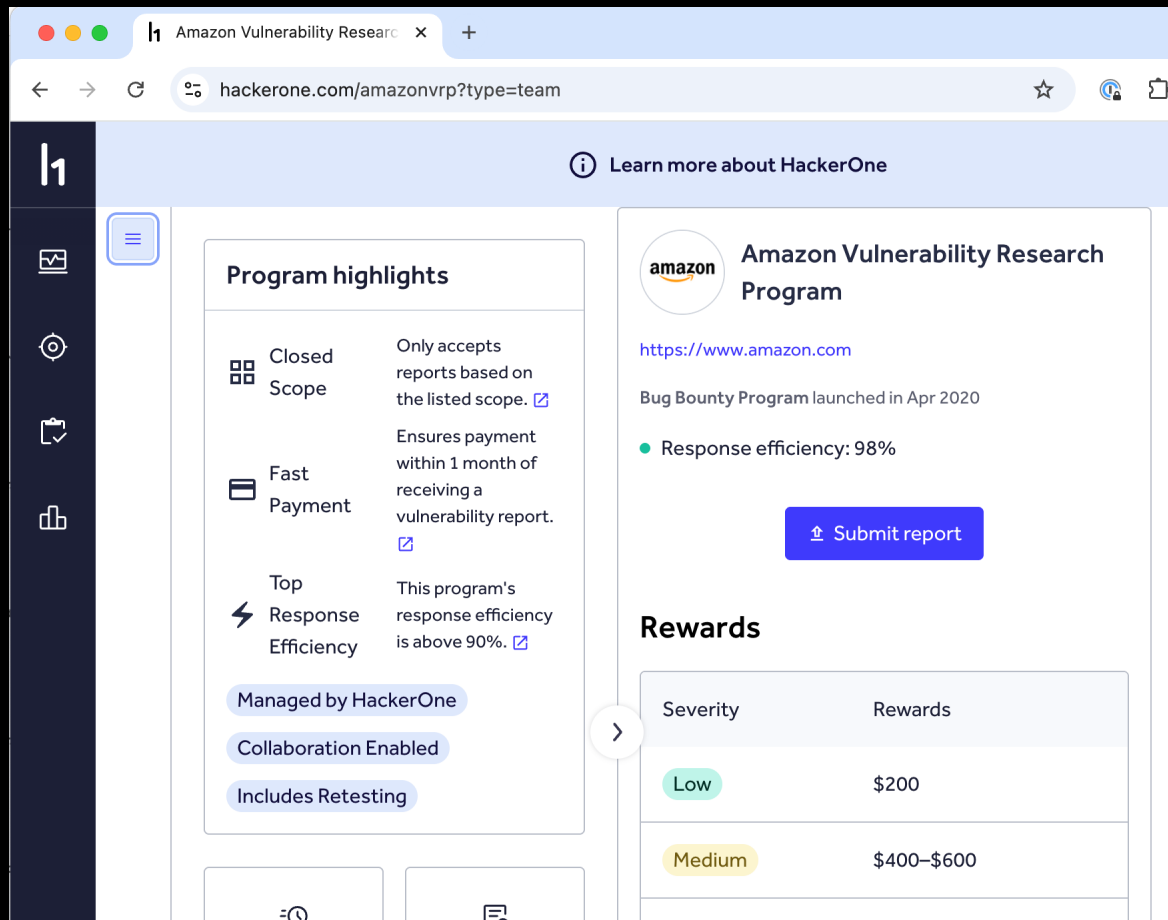
In 2024, our Vulnerability Reward Program confirmed the ongoing value of engaging with the security research community to make Google and its products safer. This was evident as we awarded just shy of \$12 million to over 600 researchers based in countries around the globe across all of our programs.

Vulnerability Reward Program 2024 in Numbers



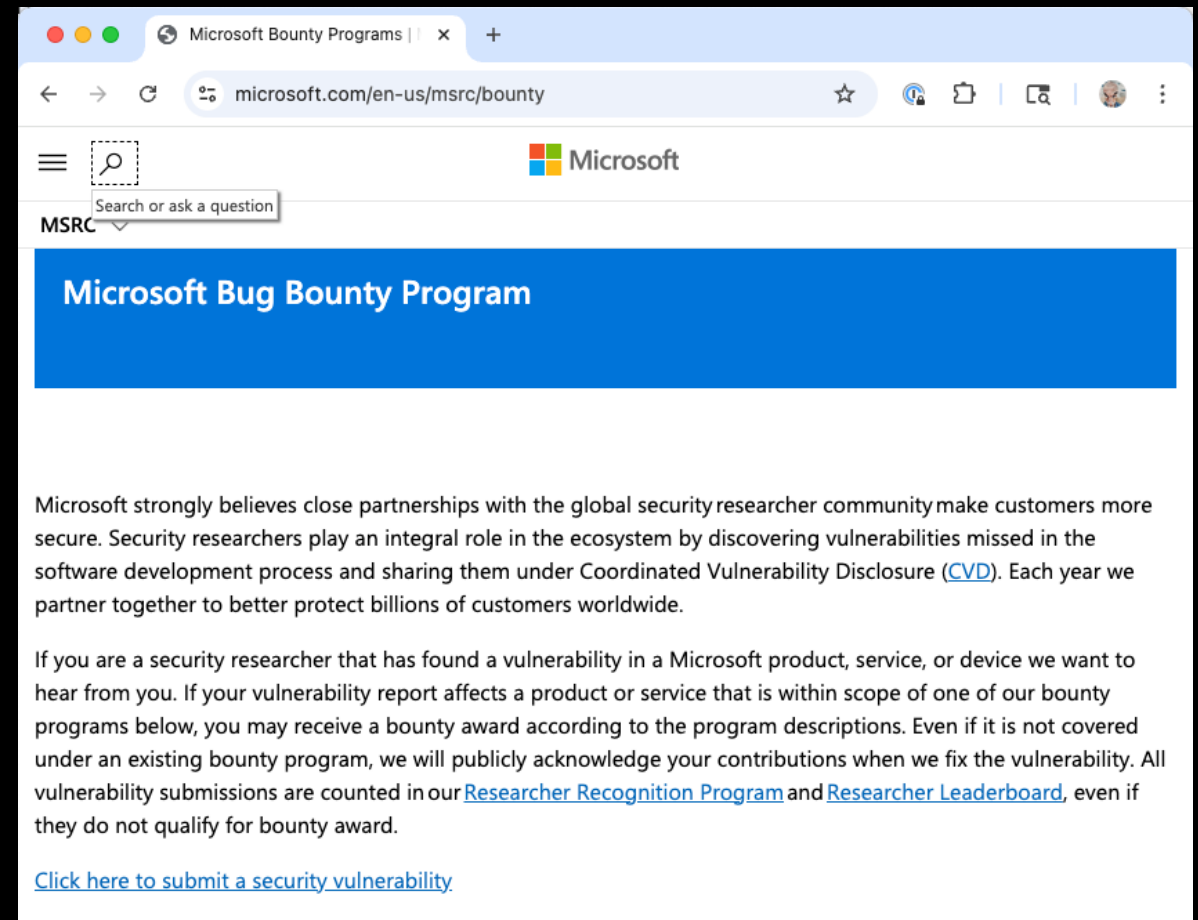
Bug bounty programs

Google has one, Microsoft too, and so does Amazon (via HackerOne)



The screenshot shows the Amazon Vulnerability Research Program page on the HackerOne platform. The page is titled "Amazon Vulnerability Research Program" and includes a link to <https://www.amazon.com>. It highlights the program's launch in April 2020 and a response efficiency of 98%. A "Submit report" button is visible. The "Program highlights" section lists: Closed Scope (Only accepts reports based on the listed scope), Fast Payment (Ensures payment within 1 month of receiving a vulnerability report), and Top Response Efficiency (This program's response efficiency is above 90%). It also mentions "Managed by HackerOne", "Collaboration Enabled", and "Includes Retesting". A "Rewards" table is partially visible at the bottom.

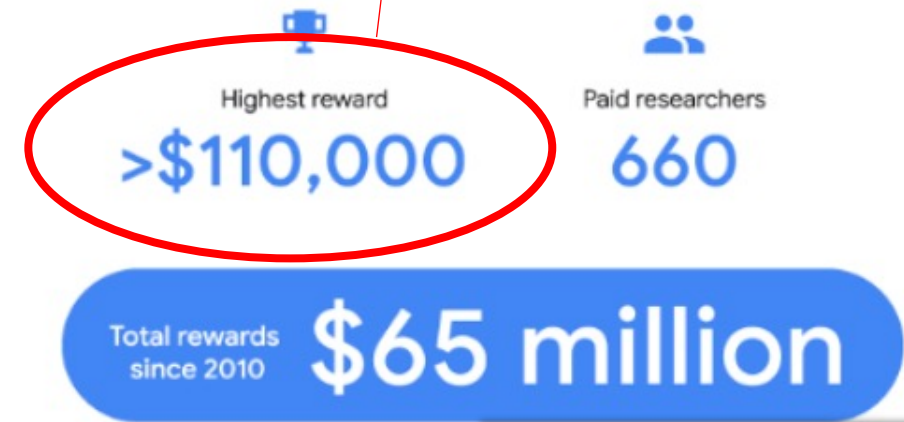
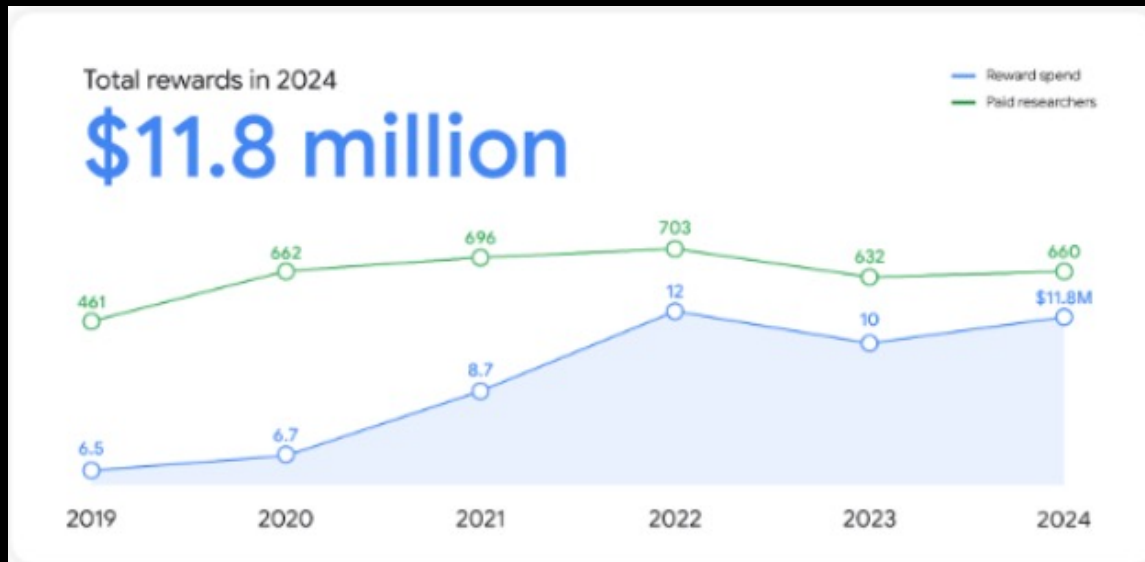
Severity	Rewards
Low	\$200
Medium	\$400-\$600



The screenshot shows the Microsoft Bug Bounty Program page. It features a search bar with the text "Search or ask a question" and a dropdown menu labeled "MSRC". The main heading is "Microsoft Bug Bounty Program". The text states: "Microsoft strongly believes close partnerships with the global security researcher community make customers more secure. Security researchers play an integral role in the ecosystem by discovering vulnerabilities missed in the software development process and sharing them under Coordinated Vulnerability Disclosure (CVD). Each year we partner together to better protect billions of customers worldwide." It also mentions that security researchers may receive a bounty award and that all vulnerability submissions are counted in the "Researcher Recognition Program" and "Researcher Leaderboard". A link "Click here to submit a security vulnerability" is provided at the bottom.

2024 Google rewards

Much bigger than in 2013!



\$6.5M in 2019 for 461 researchers = \$14,100 per person
\$11.8M in 2024 for 660 researchers = \$16,939 per person

In early 2013, \$1,000 - \$3,133.7 (max) paid per vulnerability
per Finifter et al, "An Empirical Study of Vulnerability Rewards Programs," USENIX 2013.

An Empirical Study of Vulnerability Rewards Programs

Matthew Finifter, Devdatta Akhawe, and David Wagner
University of California, Berkeley
{finifter, devdatta, daw}@cs.berkeley.edu

Abstract

We perform an empirical study to better understand two well-known vulnerability rewards programs, or VRPs, which software vendors use to encourage community participation in finding and responsibly disclosing software vulnerabilities. The Chrome VRP has cost approximately \$580,000 over 3 years and has resulted in 501 bounties paid for the identification of security vulnerabilities. The Firefox VRP has cost approximately \$570,000 over the last 3 years and has yielded 190 bounties. 28% of Chrome's patched vulnerabilities appearing in security advisories over this period, and 24% of Firefox's, are the result of VRP contributions. Both programs appear economically efficient, comparing favorably to the cost of hiring full-time security researchers. The Chrome VRP features low expected payouts accompanied by high potential payouts, while the Firefox VRP features fixed payouts. Finding vulnerabilities for VRPs typically does not yield a salary comparable to a full-time job; the common case for recipients of rewards in either program is that they have received only one reward. Firefox has far more critical-severity vulnerabilities than Chrome, which we believe is attributable to an architectural difference between the two browsers.

1 Introduction

Some software vendors pay security researchers for the responsible disclosure of a security vulnerability. Programs

costly zero-day disclosures. Monetary rewards provide an incentive for security researchers not to sell their research results to malicious actors in the underground economy or the gray world of vulnerability markets. Third, VRPs may make it more difficult for black hats to find vulnerabilities to exploit. Patching vulnerabilities found through a VRP increases the difficulty and therefore cost for malicious actors to find zero-days because the pool of latent vulnerabilities has been diminished. Additionally, experience gained from VRPs (and exploit bounties [23, 28]) can yield improvements to mitigation techniques and help identify other related vulnerabilities and sources of bugs. Finally, VRPs often engender goodwill amongst the community of security researchers. Taken together, VRPs provide an attractive tool for increasing product security and protecting customers.

Despite their potential benefits, there is an active debate over the value and effectiveness of VRPs. A number of vendors, notably Microsoft, Adobe, and Oracle, do not maintain a VRP, with Microsoft arguing that VRPs do not represent the best return on investment on a per-bug basis [26]. Further, it is also not clear if the bounties awarded are a sufficient attraction for security researchers motivated by money—underground economy prices for vulnerabilities are far higher than those offered by VRPs [20, 37].

Given the emergence of VRPs as a component of the secure development lifecycle and the debate over the effi-

Chrome

- 337 reports of unique, valid security bugs
- Awarded \$3.4 million to 137 Chrome VRP researchers
- So: ~\$10K per bug

	High-quality report with demonstration of RCE	High-quality report demonstrating controlled write	High-quality report of demonstrated memory corruption	Baseline
Sandbox escape / Memory corruption / RCE in a non-sandboxed process [1], [2]	Up to \$250,000	Up to \$90,000	Up to \$35,000	Up to \$25,000
Memory Corruption / RCE in a highly privileged process (e.g. GPU or network processes) [2]	Up to \$85,000	Up to \$70,000	Up to \$15,000	Up to \$10,000
Renderer RCE / memory corruption in a sandboxed process	Up to \$55,000	Up to \$50,000	Up to \$10,000	Up to \$7,000 [3]

Android and devices

Code execution reward amounts

Description	Maximum Reward
Pixel Titan M with Persistence, Zero click	Up to \$1,000,000
Pixel Titan M without Persistence, Zero click	Up to \$500,000
Local App to Pixel Titan M without Persistence	Up to \$300,000
Secure Element	Up to \$250,000
Trusted Execution Environment	Up to \$250,000
Kernel	Up to \$250,000
Privileged Process	Up to \$100,000

Data exfiltration reward amounts

Description	Maximum Reward
High value data secured by Pixel Titan M	Up to \$500,000
High value data secured by a Secure Element	Up to \$250,000

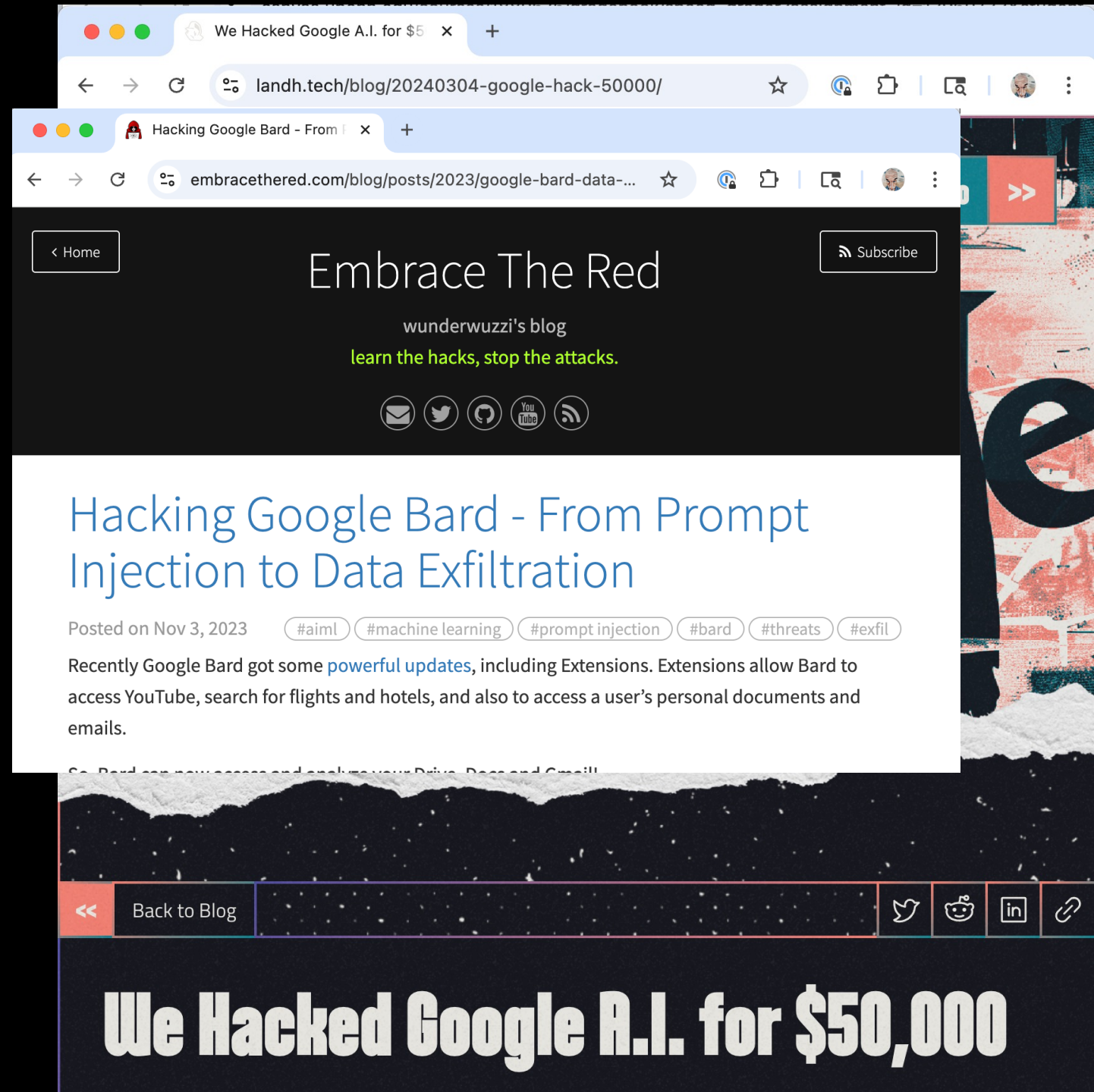
Bypass reward amounts

Description	Maximum Reward
Lockscreen bypass [1]	Up to \$100,000
Device Policy Controller bypass [2]	Up to \$75,000

- Awarded over \$3.3 million total
- 8% decrease in the total submissions
- 2% increase in the number of critical and high vulnerabilities

Generative AI

- Prompt attacks
 - Training Data Extraction
 - Manipulating Models
 - Adversarial Perturbation
 - Model Theft / Exfiltration
-
- 150 bug reports – over \$55,000 in rewards so far – with one-in-six leading to key improvements



Bugcrowd

- Bug bounties as a service (and other programs, too)
- Claimed benefits:

24/7

Response for critical issues

30%

Reduction in risk of a breach

7x

More critical vulnerabilities found

268%

Return on investment

The screenshot shows the Bugcrowd website homepage. At the top, there's a navigation bar with the Bugcrowd logo, a "Talk to an Expert" button, and a "Menu" icon. The main headline reads "Join forces with hackers and reduce risk". Below this, a sub-headline states: "Find and fix hidden vulnerabilities faster by accessing the world's best hackers and pentesters. Crowdsourced intelligence stops breaches before attackers can strike." A prominent purple button says "Take a 5-Min Tour". To the right, a diagram illustrates the Bugcrowd ecosystem, with a central "CODE" box connected to various technology categories: Cloud Services, Data Bias, Crypto, Web3, IoT, LLM Apps, and Reconnaissance. At the bottom, there's a Gartner Peer Insights rating of 4.9 / 5, represented by five stars. The footer features logos for OpenAI, Pinterest, T-Mobile, Indeed, Atlassian, and Mastercard.

bugcrowd

Talk to an Expert Menu

Join forces with hackers and reduce risk

Find and fix hidden vulnerabilities faster by accessing the world's best hackers and pentesters. Crowdsourced intelligence stops breaches before attackers can strike.

Take a 5-Min Tour

Gartner Peer Insights Rated 4.9 / 5

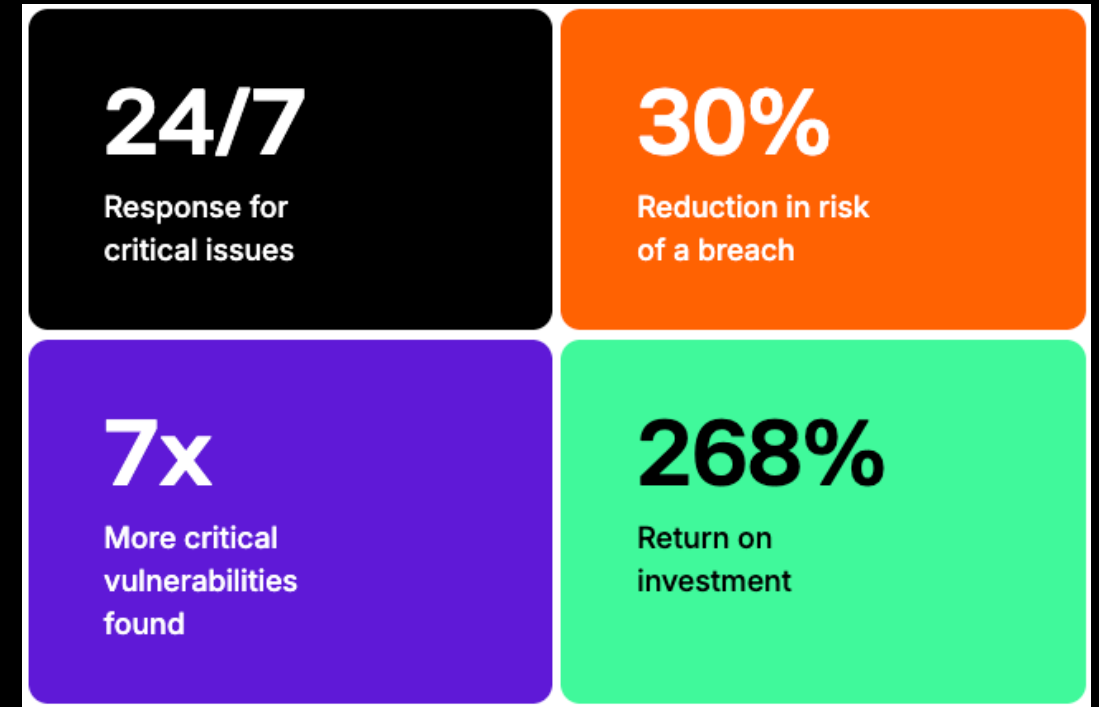
Cloud Services Data Bias Crypto Web3 IoT LLM Apps Reconnaissance

CODE

OpenAI Pinterest T-Mobile Indeed ATlassian mastercard

Return on investment?

- What is the calculation used to determine the benefits?
- What are the incentives to find and fix vulnerabilities in your systems
 - If you are a software provider
 - If you are a service provider
 - If you are a government agency



Worry: Hackers will sell your vulnerabilities on the dark web for more \$\$

Discussion points

- General takeaways?
- What can you glean from Google's results about their security?
 - How would you tell whether the program is really game-changing, i.e., significantly raising costs for attackers?
- Bug bounty programs:
 - When would you be motivated to start a bug bounty program?
 - Now that AI is becoming a big deal, how are these programs changing (or should change)?
 - How do these programs affect the attack ecosystem described in the other paper?
 - Concerns about how "security researchers" are compensated?