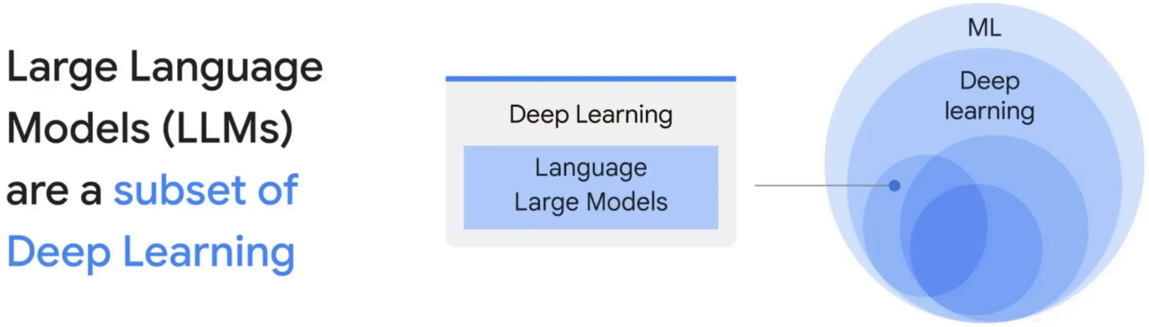
Vulnerability Management & The Commoditization of Security Research

Pioneering Bug Bounty Hunting Agency with Otacon

Otacon Core Development Team—core@otacon.ai
Submitted April 7th, 2024

Abstract

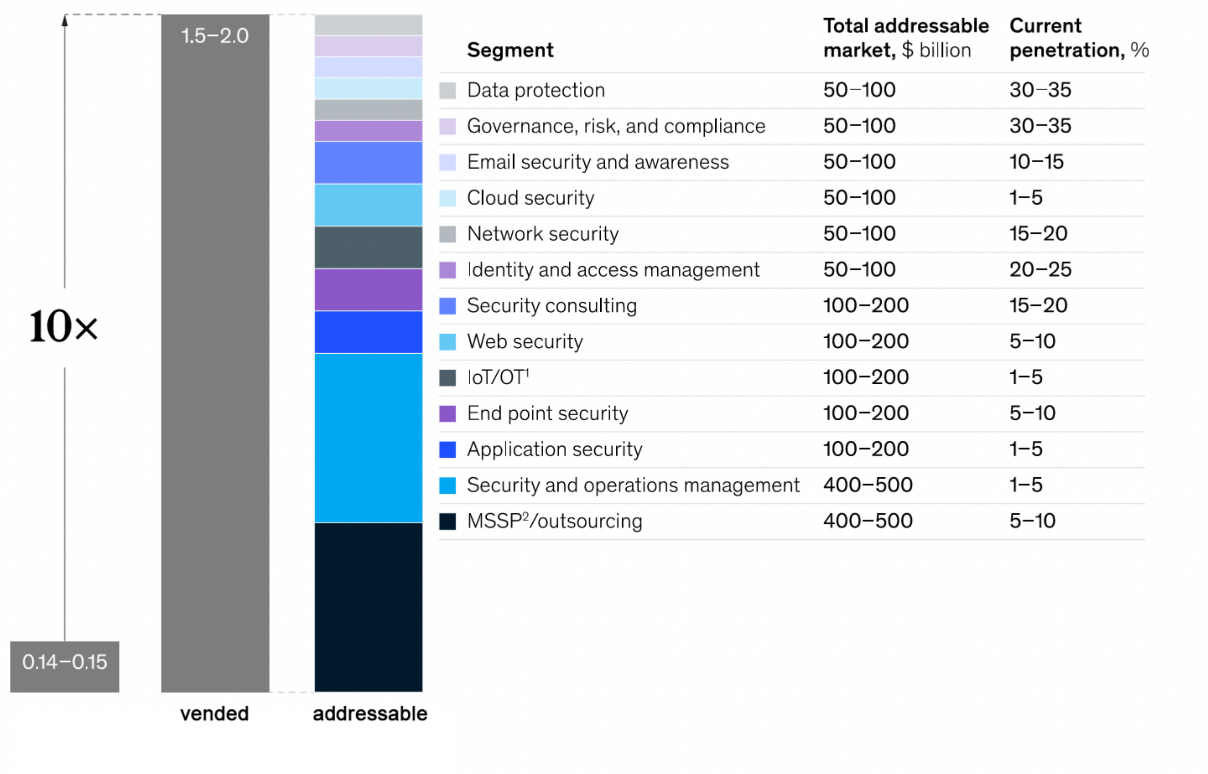
Vulnerability Management (VM) is the cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating software vulnerabilities. This paper explores the application of Artificial Intelligence (AI) foundation models to the Software Vulnerability Management workflow, with a focus on Large Language Models (LLM)—a new class of neural network architecture developed by Google by improving Natural Language Processing (NLP) technologies.



Large Language Models (LLMs) are a subset of Deep Learning

As the infrastructure of human activity, communication networks have become the backbone of our economy. Thus, protecting the flow of information and value against malevolent actors is an essential prerogative of software and network engineers.

But despite an exponential demand for security products and service, in an increasingly favorable regulatory environment, **security professionals still only manage to capture a mere 10% of an estimated $2 trillion market opportunity**. The below-target adoption of security products and services suggest that we must collectively rethink the go-to-market strategy of the Vulnerability Management stack, the value proposition of its architectural components, and the nurturing of the security talents that enable security workflows to deliver on their objectives.



Segment	**Total addressable market,** $ billion	**Current penetration,** %
Data protection	50–100	30–35
Governance, risk, and compliance	50–100	30–35
Email security and awareness	50–100	10–15
Cloud security	50–100	1–5
Network security	50–100	15–20
Identity and access management	50–100	20–25
Security consulting	100–200	15–20
Web security	100–200	5–10
IoT/OT[1]	100–200	1–5
End point security	100–200	5–10
Application security	100–200	1–5
Security and operations management	400–500	1–5
MSSP[2]/outsourcing	400–500	5–10

Otacon is a cybersecurity protocol that **bridges the gap between cybersecurity demand and supply**, by enabling anyone with a computer to become a Bug Bounty Hunter using Artificial Intelligence (AI) and Mechanism Design (MD).

After establishing the state of security research, and the size of the security problem humanity is facing, we describe how Otacon—a peer-to-peer security protocol—is a strong departure from traditional approaches to Vulnerability Management, that democratizes access to network, application, endpoint, data and asset security through Bug Bounty Hunting Artificial Intelligence (AI) agency and Bug Bounty crypto-economics that encourage global participation.

Keywords: Security, Software, Network, Engineering, Vulnerability Management, Bug Bounty, Artificial Intelligence, AI, Foundation Models, Large Language Model, LLM, Natural Language Processing, NLP, Smart Contracts

The Cybersecurity Landscape

In the ever-evolving, always-on, technological world that we live in, security research stands as a rampart against a rising tide of security threats.

As we step into 2024 and the era of threat automation, individuals, business and governmental participation in online activities represent both an extraordinary domain of opportunity, and a series of security disasters waiting to happen, as risk looms larger than ever before.

Expanding Attack Surface

The trajectory of security threats extends beyond mere numbers; it is a profound transformation in the very nature of these threats.

The attack surface—the sum of vulnerabilities that malevolent actors can leverage to access networks and softwares—has expanded dramatically, with the proliferation of interconnected devices, the increased reliance on third-party online services, and the advent of cryptocurrency.

An always-on world presents a multifaceted challenge for security professionals, individuals, businesses and states.

All Time High Damage

Security threats represent a significant financial burden to industries worldwide, with the costs associated with breaches escalating in recent years.

According to IBM's 2023 Cost of a Data Breach Report, the average total cost of a data breach now exceeds $4 million, the highest average in the history of the report.

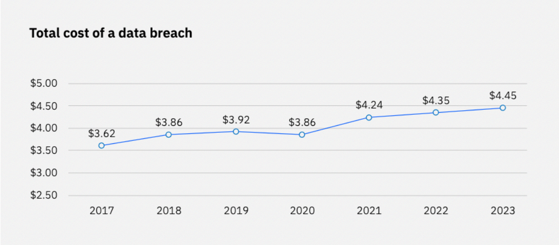


Figure 1. Measured in USD millions

This figure underscores the extensive financial impact of security incidents, which include direct expenses such as ransom payments, system repairs, legal fees, as well as indirect costs like reputational damage and lost customer trust.

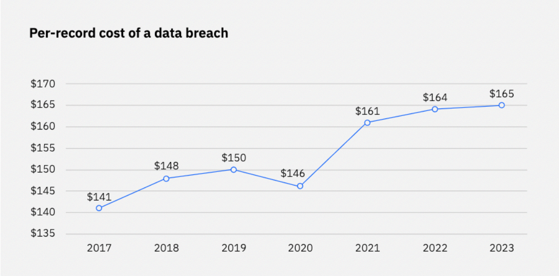


Figure 2. Measured in USD

The cryptocurrency industry is particularly susceptible to costly breaches.

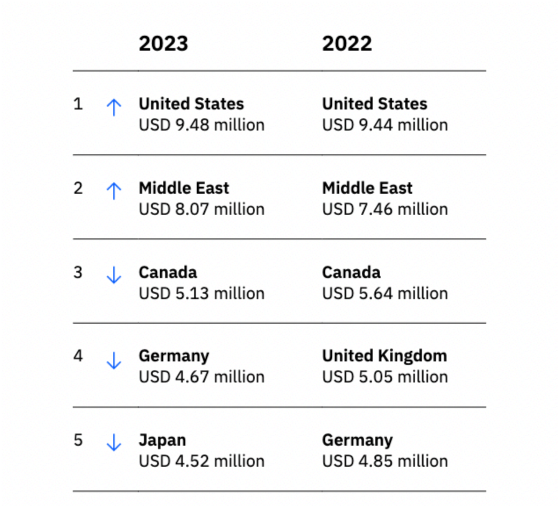
The 2014 Mt. Gox exchange hack led to the loss of approximately 850,000 bitcoins, valued at about $450 million at the time, and worth $60 billion today, changing the life trajectory of many early adopters of the electronic peer-to-peer cash system.

Over $3 billion worth of cryptocurrency was stolen from users in 2022, further highlighting that the demand for security products and service for the new asset class, and peer-to-peer networks, is still not met with working solutions.

Although they appear less costly, breaches in the legacy networks and financial systems are no less impactful.

The SolarWinds breach of 2020 also offers a stark reminder of the disruption associated with security failures in business environments, affecting upwards of 18,000 organizations and leading to an estimated hundreds of millions in global mitigation expenses.

The Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States, suffered a ransomware attack, which incurred direct costs of roughly $5 million in ransom payments, and additional millions in mitigation expenses.



		2023	2022
1	↑	**United States** USD 9.48 million	**United States** USD 9.44 million
2	↑	**Middle East** USD 8.07 million	**Middle East** USD 7.46 million
3	↓	**Canada** USD 5.13 million	**Canada** USD 5.64 million
4	↓	**Germany** USD 4.67 million	**United Kingdom** USD 5.05 million
5	↓	**Japan** USD 4.52 million	**Germany** USD 4.85 million

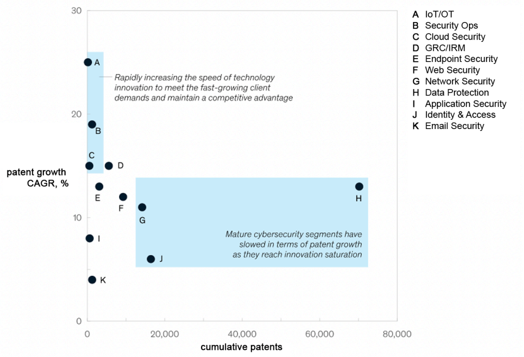
For the 13th consecutive year, the United States held the title for the highest data breach costs.—IBM's 2023 Cost of a Data Breach Report

More than ever, the security risk that individuals, businesses and states are exposed to must be mitigated.

Evolving Defense Strategies

In an inherently dynamic security landscape, the strategies adopted to defend against security threats must also be dynamic. Legacy approaches, relying solely on static analysis and manual Vulnerability Management workflows, are proving inadequate.

In response, a shift toward intelligence-driven security is imperative.



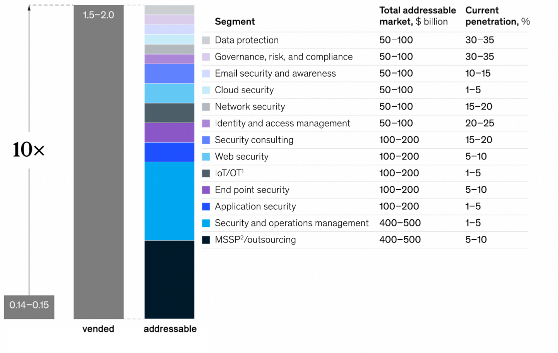
Increase in Security Patent Activity—Innography / McKinsey Survey (2022)

This entails the continuous monitoring of threats, the training of security stakeholders on documented and emerging threats, strong advocacy for a security culture at each and every layer of society, and higher throughput security products and services.

Market Outlook

Over the next decade, the security industry, already worth more than $2 trillion today, is anticipated to experience significant growth and transformation, primarily driven by escalating online threats across various sectors.

But the growth trajectory of the total addressable market for security products and services is undermined by the scalability of security professionals, as the vended market and target adoption has been stalling in the last decade.



Segment	Total addressable market, $ billion	Current penetration, %
■ Data protection	50–100	30–35
■ Governance, risk, and compliance	50–100	30–35
■ Email security and awareness	50–100	10–15
■ Cloud security	50–100	1–5
■ Network security	50–100	15–20
■ Identity and access management	50–100	20–25
■ Security consulting	100–200	15–20
■ Web security	100–200	5–10
■ IoT/OT[1]	100–200	1–5
■ End point security	100–200	5–10
■ Application security	100–200	1–5
■ Security and operations management	400–500	1–5
■ MSSP[2]/outsourcing	400–500	5–10

Innovations in Artificial Intelligence (AI) and Machine Learning (ML) will be crucial, as they provide the capabilities to keep pace with the speed of escalation.

From security risk prevention to remediation through continuous vulnerability management, security cannot afford to be an afterthought anymore, and embedding security frameworks directly into the design process of networks and softwares—known as "security by design"—will likely become a standard practice to mitigate risks from the onset.

The industry will also be shaped by stringent regulatory landscapes as governments are expected to implement tougher data protection and security laws to protect consumer data and maintain the integrity of systems.

Addressing the cybersecurity talent gap will also be a critical challenge over the next decade. While demand for skilled security researchers and professionals is growing rapidly, there remains a substantial deficit in qualified personnel, with millions of roles going unfilled worldwide.

This shortage is anticipated to expand unless there is a concerted effort from educational institutions and corporations to bolster training programs and career pathways in the field.

Bug Bounty Hunting

As a response to the complexity of Vulnerability Management processes, Bug Bounty Hunting has emerged as a pivotal way to fortify the security landscape, by encouraging ethical security researchers to discover and report vulnerabilities in networks and softwares in exchange for a reward.

Bug Bounty programs provide organizations with an external perspective on their security posture, and incentivizes the correction of vulnerabilities before malicious actors can exploit them.

Today, it is the most popular form of security practice for businesses. However, the demand for skilled bug bounty hunters has, yet again, far outstripped the supply of talent, and bottlenecks are forming as we are nearly capped in hunting capacity.

Stage I: Manual

Manual Bounty Programs are non-standardized ways for a third-party to reach out to a business, often through a security@company.com dedicated email address. Most, if not all steps of the Vulnerability Management workflow are handled through back-and-forth email communications until the settlement of the manual Bug Report submission.

Stage II: Computer-Assisted

Bounty Programs can by assisted by computers through the use of a third-party, centralized Bug Bounty platform.

Most steps of the Vulnerability Management workflow are handled by a software application that guides the Bounty Program stakeholders through a collaborative pipeline until the settlement of the Bug Report submission.

While doing some of the heavy lifting, Bug Bounty Hunting platforms do not automate Bug Scanning, Proof of Concept, and the other labor-intensive parts of the Bug Bounty Hunt, and are not immediately a good fit for novice enthusiasts.

Stage III: Human-Assisted

Bounty Programs can by assisted by humans through the use of a third-party, centralized AI Bug Bounty platform.

Since the Artificial Intelligence (AI) is responsible for most of the labor-intensive parts of the Bug Bounty Hunt, humans are relegated to control and administration tasks.
The paradigm shift of Artificial Intelligence (AI) is that virtually all networks and software will become human-assisted.

Otacon: A Revolutionary Approach to Vulnerability Management

This is where Otacon, and Artificial Intelligence (AI) are poised to revolutionize Bug Bounty Hunting.

Otacon is enabling not only experts but also novice security enthusiasts to participate in bug bounty programs. It can identify potential vulnerabilities, prioritize them based on severity, and even suggest remediation steps, democratizing the art of ethical security research.

This not only scales our ability to secure networks and softwares to unprecedented levels but also diversifies the talent pool by lowering barriers to entry, ensuring a broader and more inclusive approach to Vulnerability Management.

Otacon leverages Artificial Intelligence and Mechanism Design to continuously analyze programs, seeking patterns indicative of potential vulnerabilities. By automating the initial stages of vulnerability detection, Otacon frees up human experts to focus on more complex, nuanced security challenges.

This fusion of human expertise and AI-driven automation not only accelerates the remediation of vulnerabilities but also reduces the burden on security teams by boosting the efficiency of Bug Bounty programs.

Launched in October 2023, Otacon is the culmination of the collaborative effort of Product Developers, Artificial Intelligence Engineers, and Security Researchers. It aims at empowering individuals, businesses and governments to actively participate in the fortification of networks, softwares and smart contracts, by capturing and orchestrating the distribution of the $2 trillion total addressable market for security products and services.

Scanning

Otacon employs Large Language Models (LLM) to scan Smart Contracts for vulnerabilities. Large Language Models are a new class of neural network architecture developed by Google by improving

Tokenization

Once vulnerabilities are detected, Otacon has the ability to log their details onto a blockchain network, ensuring the immutable record-keeping of security risk exposures.

But instead of simply documenting vulnerabilities, Otacon transforms them into “Proof of Bug” assets, with financial properties.

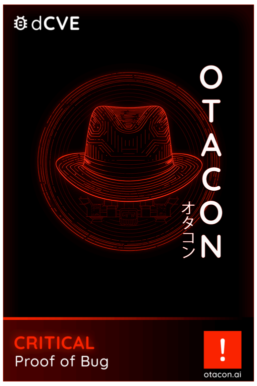
Represented by a non-fungible token (NFT) collectible on the blockchain, a Proof of Bug serves as an immutable and portable proof of discovery that can be traded for value in blockchain-based protocols. As such, they enhance security while fostering an active community of contributors.

Bug-to-Token Conversion

Once vulnerabilities are detected, Otacon has the ability to log their details onto a blockchain network, ensuring the immutable record-keeping of security risk exposures. But instead of simply documenting vulnerabilities, Otacon transforms them into “Proof of Bug” assets, with financial properties.

dCVE
OTACON
オタコン
LOW
Proof of Bug
otacon.ai

dCVE
OTACON
オタコン
MODERATE
Proof of Bug
otacon.ai



Represented by a non-fungible token (NFT) on the blockchain, a Proof of Bug serves as an immutable and portable proof of discovery that can be traded for value in blockchain-based protocols. As such, they enhance security while fostering an active community of contributors.

Prototyping

In certain bounty programs, a valid Proof of Bug submission will require a Proof of Concept (PoC), a program that reproduces the bug documented by the collectible.

This process begins with the extraction and analysis of the data encoded within the Proof of Bug, which includes comprehensive details about the bug such as its type, the affected code, its severity and potentially exploitable conditions.

The PoC code is then crafted by the prototyping component of Otacon, using the information derived from the collectible.

This code, or script, is designed to exploit the bug safely within a controlled environment, demonstrating the vulnerability's potential impact without causing actual harm. The creation of the PoC is a critical step as it transforms theoretical vulnerability information into tangible, actionable insight, confirming the existence and severity of the vulnerability through practical demonstration.

Once the PoC code is developed, it is deployed in a dedicated test environment. This environment is isolated from production systems to prevent any real-world damage and simulates the conditions under which the vulnerability exists, but within a secure sandbox. The execution of the PoC allows the Bounty Program owner to observe the vulnerability in action, providing clear evidence of how an attack could occur.

Submission

The most immediate utility of a Proof of Bug in the Otacon blockchain-based protocol is to report a vulnerability in an Otacon Bounty Program.

Otacon Bug Bounty Hunters are also required to stake OTACON utility tokens to prioritize and weigh Proof of Bug submissions.

Revenue Share

When a Proof of Bug and an optional Proof of Concept are validated, the bounty hunter who discovered and reported the bug is entitled to a reward.

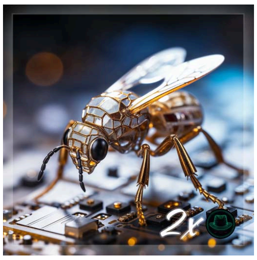
To promote a collaborative and inclusive community, a portion of this reward is shared among all participants of the bounty hunt, based on their OTACON utility token stake, and revenue modifiers.

The OTACON utility token plays a central role in this ecosystem, serving as a means of calculating Bounty Rewards, driving competition within the platform and ensuring the quality of submissions.

Participants who stake more OTACON utility tokens are considered to have a higher vested interest in the ecosystem's success and governance.

Revenue Modifiers

Ownership of Otacon Bugs collectibles also influences the reward distribution. These collectibles are unique non-fungible token (NFT) collectibles available for purchase on the Otacon Marketplace.



Owning a bug increases a hunter’s share of the communal bounty. This feature serves to deepen engagement within the platform, encouraging participants not only to invest in the ecosystem through OTACON utility token staking but also to participate in the marketplace and fund developments of a fully bootstrapped blockchain-based protocol.

Otacon: The Future

Scanning Accuracy

Improving the bug-finding accuracy of Otacon involves a robust strategy of fine-tuning its Large Language Models on a diverse and extensive dataset.

By utilizing a dataset of 9,000 vulnerable smart contracts, Otacon can deeply understand the patterns and commonalities associated with various types of vulnerabilities.

Otacon will also rely on 1,000 security audits from the top 50 smart contract security firms and independent Web 3.0 auditors, ensuring that the model learns from the highest standards of current security practices.

Additionally, integrating models trained on Graph Neural Networks (GNNs) could exploit the relational data between contract components, effectively detecting vulnerabilities arising from complex interactions within contracts. These models analyze the nodes (representing contract elements) and edges (representing interactions) in a graph, providing a sophisticated method for uncovering deep-seated and non-obvious vulnerabilities.

This approach ensures that Otacon remains at the forefront of cybersecurity technology, providing a robust, proactive defense mechanism against the increasingly sophisticated landscape of smart contract vulnerabilities, before tackling other classes of networks and software involving legacy technologies.

Bounty Hunting Agency

As the Otacon blockchain-based protocol evolves, the future appears particularly promising, especially with the integration of Autonomous Bug Bounty Hunting agents. These agents, designed by bug bounty hunters, will be capable of operating independently across various platforms, participating in both manual and automated bounty programs without the constraints of being tied exclusively to Otacon.

This development is expected to significantly expand the scope and effectiveness of Otacon’s Bug Bounty Hunting efforts beyond business development efforts to onboard smart contract developers to the protocol.

This capability not only increases the potential earning opportunities for hunters but also enhances the ability of Otacon to become the most important aggregation infrastructure of security solutions ever created.

Conclusion

Otacon represents a significant advancement in the field of cybersecurity, particularly within the burgeoning realm of blockchain technology and smart contracts. By integrating AI-driven approaches with blockchain's inherent transparency and security features, Otacon is poised to redefine how vulnerabilities are detected, reported, and mitigated. The use of "Proof of Bug" NFTs not only ensures that discoveries are documented and verifiable but also incentivizes participation through a transparent and fair reward system that benefits all contributors based on their engagement and investment in the ecosystem.

The deployment of autonomous bug-hunting agents that can operate across various platforms exemplifies Otacon's innovative approach to scaling cybersecurity efforts. These agents enhance the system's ability to monitor and respond to threats in real-time, democratizing cybersecurity by enabling a wider range of participants to contribute to and benefit from secure digital environments. This capability is supported by a robust financial model that utilizes marketplace proceeds and OTACON tokens to sustain and expand the platform's operations, ensuring ongoing development and refinement.

Future enhancements to Otacon's AI models, through extensive training on diverse and comprehensive datasets including thousands of vulnerable smart contracts and security audits, are set to improve the platform's accuracy and predictive capabilities. The incorporation of foundational AI models like large language models and graph neural networks will further sophisticate its analytical tools, enabling the detection of complex and subtle vulnerabilities. As a result, Otacon is not just a tool for today but a scalable solution for the future, continuously evolving to meet the challenges of an increasingly complex cybersecurity landscape. This holistic and forward-thinking approach marks Otacon as a pivotal development in securing digital assets and maintaining trust within the digital economy.

ABOUT US

🕷️ Otacon is the world's first #AI Bug Bounty Hunting and #SecFi experience.—https://otacon.ai