H^4: Key Techniques and Equipments of Guard Model based Sensing High-hidden Threats in Electric Power Network

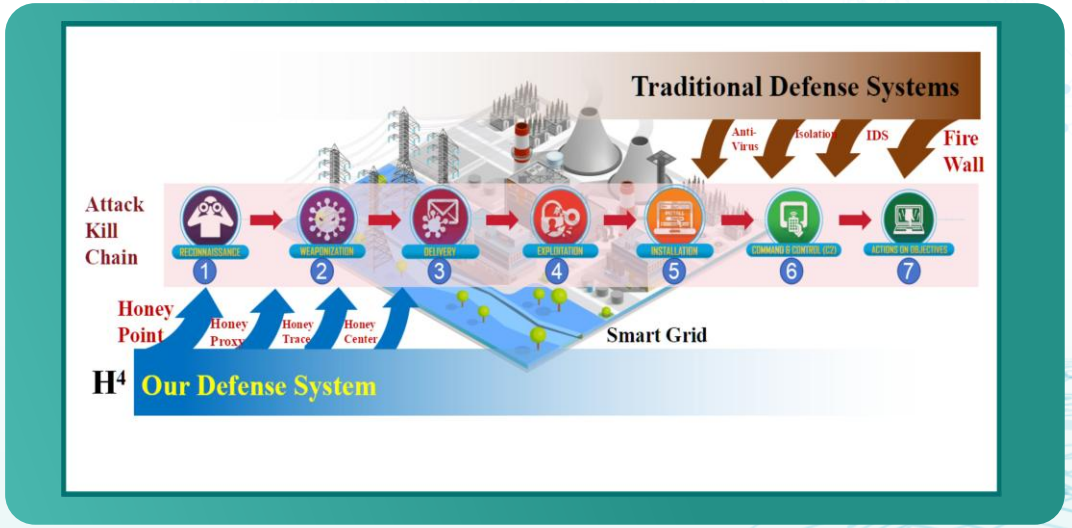
国家电网
STATE GRID

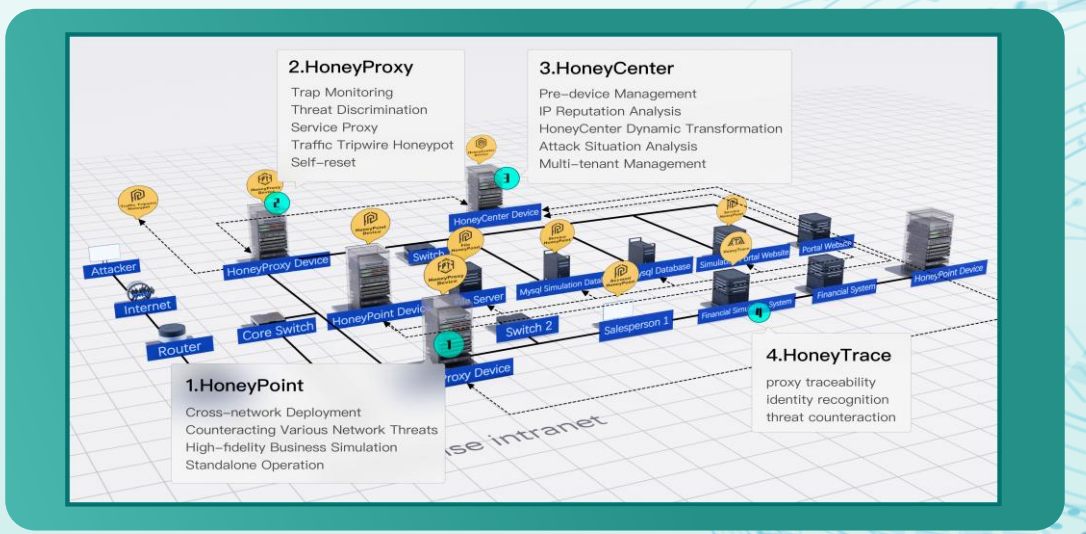
江西神舟

软极网络
RANGE·SOFT

Context and Introduction

Traditional defense mechanisms struggle against APT attacks. We innovatively proposed the "Safeguard Mode," which enables precise early-stage identification within the attack kill chain. Breakthrough technologies include trap-based probing, preemptive threat observation, collaborative transformation, and hunting deception. These innovations have been successfully commercialized into market-ready products: HoneyPoint, HoneyProxy, HoneyTrace, and HoneyCenter. The H⁴ system has been validated and widely applied in protecting national critical information infrastructure and safeguarding cybersecurity missions, generating over 5.7 billion RMB in direct sales revenue over the past three years.





Technology Innovation

A new cyber security defense model for the power grid system has been proposed, Safeguard defense mode, which can identify attackers in early stages in their attack kill chain. The innovative technology breakthroughs include **trap-based probing, preemptive threat observation, collaborative transformation,** and **hunting deception.** Four types of market-ready equipment have been successfully developed correspondingly, namely HoneyPoint, HoneyProxy, HoneyTrace, and HoneyCenter. Its effectiveness has been validated and widely applied in protecting critical national information infrastructure and safeguarding national cybersecurity tasks.

HoneyPoint

HoneyPoint is proposed to entrap cyberattacks through trap-based probing technology, and we propose fast and diverse HonePoint construction methods based on vulnerability exploitation and large language models.

HoneyProxy

HoneyProxy is designed to preemptive observe and detect malicious traffic through preemptive threat observation technology, and the potential threats are identified by constructing a reputation system and then be redirected from the protected system.

HoneyTrace

HoneyTrace is proposed to proactively lure and mislead attackers through hunting deception technology, constructing a large scale simulated deceptive system and providing the advanced capabilities in threat response and protection.

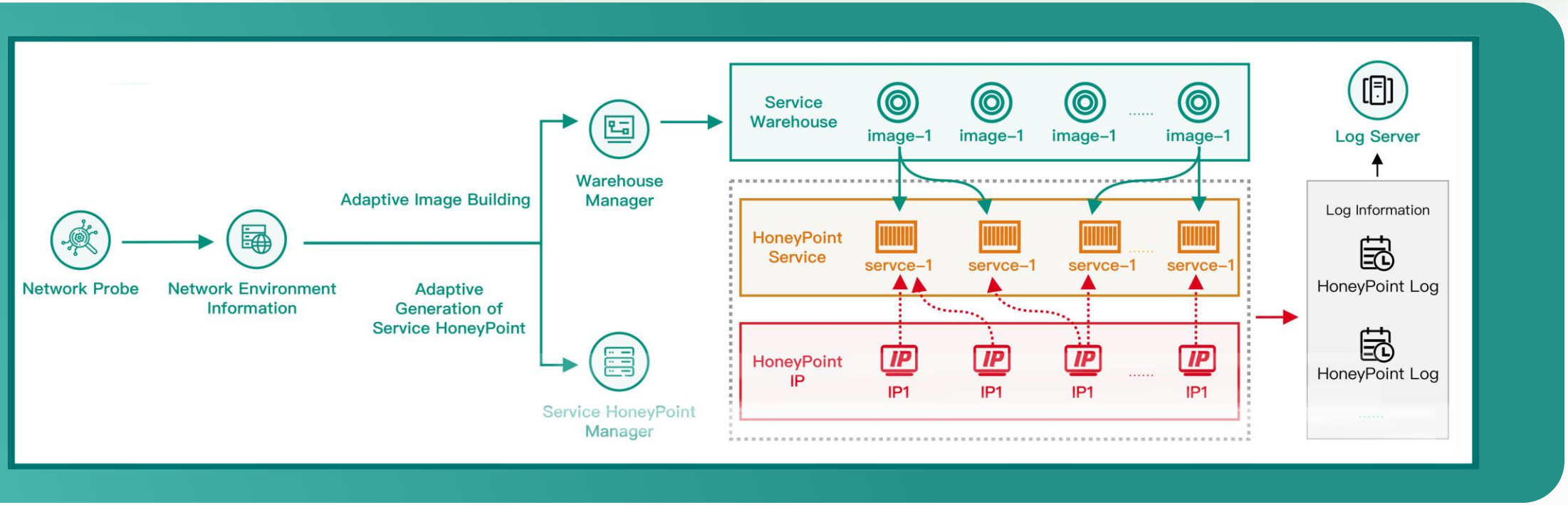
HoneyCenter

HoneyCenter is designed to collaboratively optimize the deployment strategy of HoneyPoint, HoneyProxy, HoneyTrace and other security devices, proposing collaborative transformation technology, which is based on game theoretical counteractions and dynamic transformations, offering an advanced defense mechanism for confronting evolving and persistent cyber threats.

Technology Innovation

HoneyPoint:

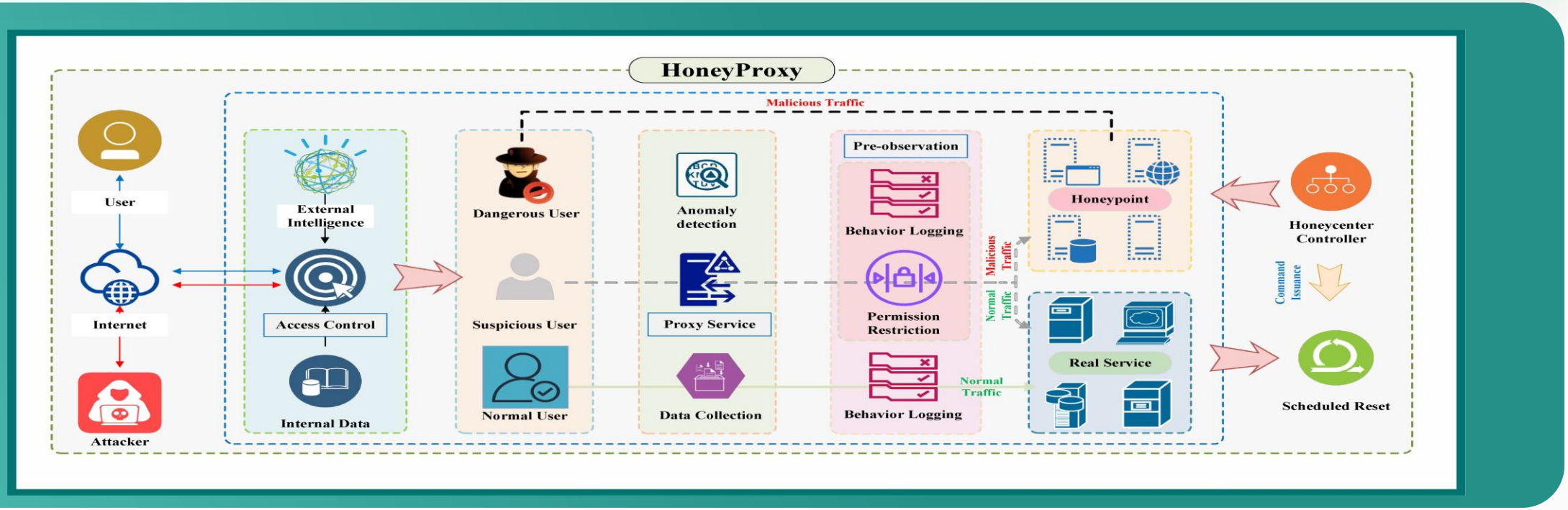
HoneyPoint is proposed to entrap cyberattacks through **trap-based probing technology,** and we propose fast and diverse HonePoint construction methods based on vulnerability exploitation and large language models.



Technology Innovation

HoneyProxy:

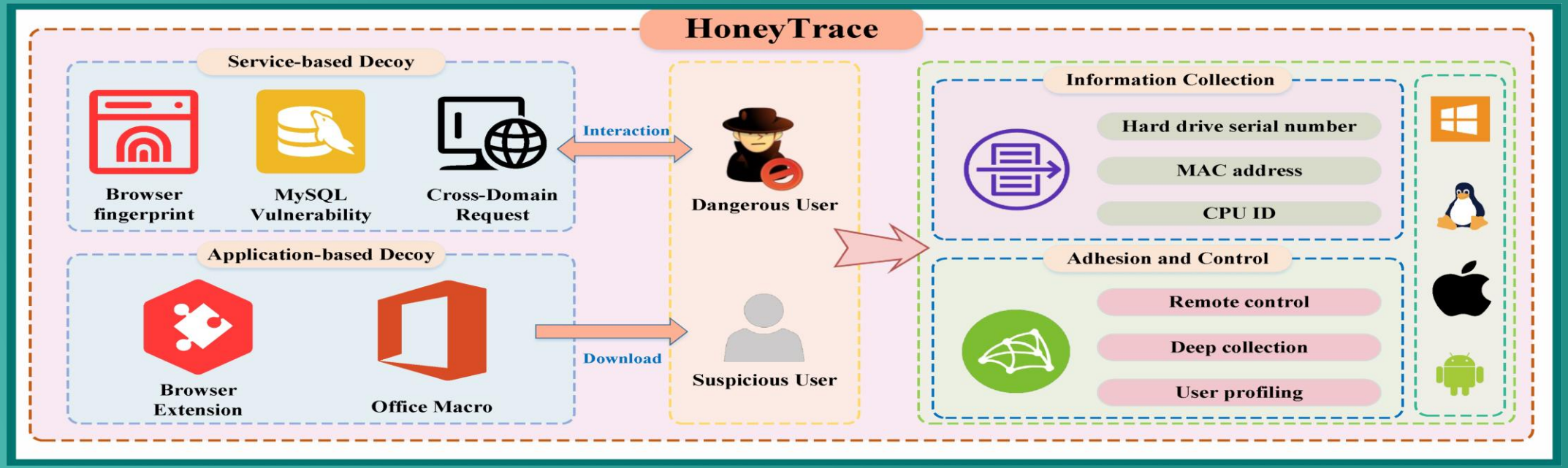
HoneyProxy is designed to preemptive observe and detect malicious traffic through **preemptive threat observation technology,** and the potential threats are identified by constructing a reputation system and then be redirected from the protected system.



Technology Innovation

HoneyTrace:

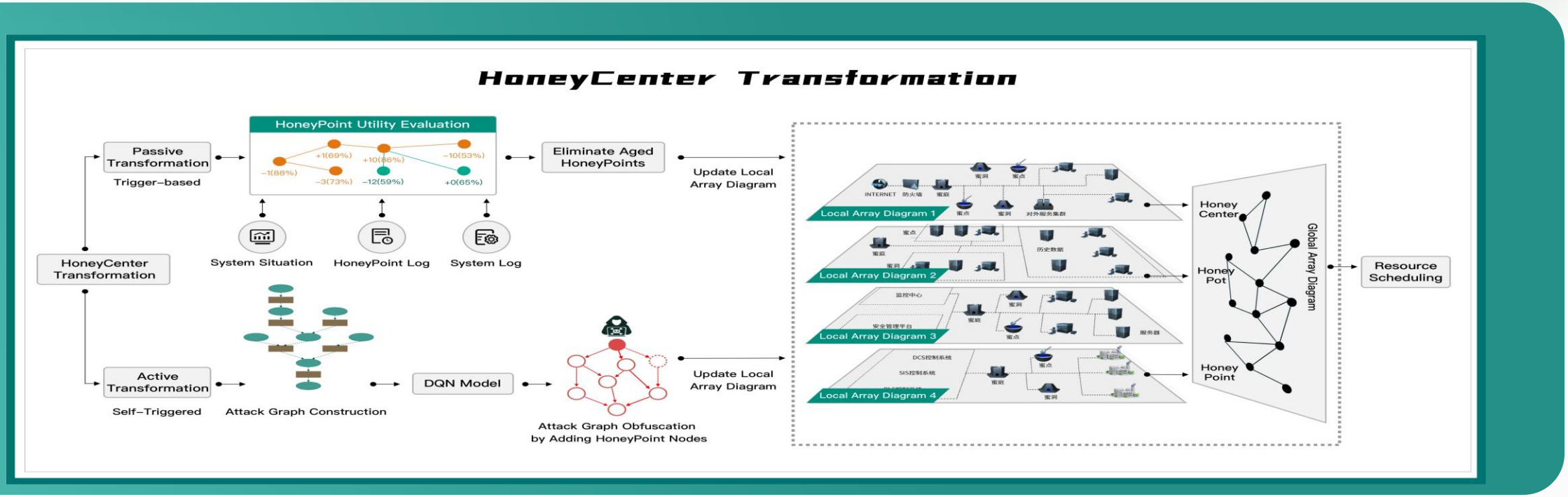
HoneyTrace is proposed to proactively lure and mislead attackers through **hunting deception technology,** constructing a large scale simulated deceptive system and providing the advanced capabilities in threat response and protection.



Technology Innovation

HoneyCenter:

HoneyCenter is designed to collaboratively optimize the deployment strategy of HoneyPoint, HoneyProxy, HoneyTrace and other security devices, proposing **collaborative transformation technology,** which is based on game theoretical counteractions and dynamic transformations, offering an advanced defense mechanism for confronting evolving and persistent cyber threats.



Performance Metrics

HoneyPoint

171 types

We have developed 171 types of HoneyPoints in the context of power grid scenario.

100ms

The average startup time for a single vulnerability exploitation honeypoint is less than or equal to 100 milliseconds.

100%

The accuracy of unauthorized external connection detection is 100%.

HoneyProx

95%

The accuracy of redirecting malicious traffic is greater than 95%.

50ms

The latency of the redirection Service proxy is less than or equal to 50 milliseconds.

100%

The accuracy of first-time threat detection is 100%.

HoneyTrace

10K nodes

The system with 10 thousands nodes can be constructed within one hour.

50%

The construction time of the virtualized simulation network at the scale of tens of thousands is approximately 50% less than that of the existing methods.

HoneyCent

4.3 times

The time efficiency of strategy updation is improved by 4.3 times.

10 types

Supports remote collaborative deployment, compatible with 10 types of devices, 3 protocols, and 4 scheduling methods

50K units/device

The number of managed devices is greater than or equal to 50,000 units per device.

Innovation Achievements

·Published of two China standards: 《2024-2081T-YD-Data Analysis Requirements for Active Defense-Oriented H⁴ Systems》 and 《2024-2082T-YD-General Technical Requirements for Active Defense-Oriented H⁴ Systems》.
·Published **36** academic papers.
·**42** patents(40 China Patents and 2 Japan Patents).
·Innovation and Application Case, the World Intelligence Expo 2024,(Top 20 among 990 casesfrom 49 countries).

Applications and Promotion

As a national-level cybersecurity device and solution, H⁴ has established a mature application framework spanning multiple industries and scenarios.

1. Power Industry Coverage

·Deployed across **27** provincial power grids (covering 80% of China's electricity network), serving over 1.1 billion people.
·Case Study (Jiangxi Power Grid, 2024): Blocked over 4.8 million cyberattacks, patched 765 vulnerabilities, traced 58 hackers, and gained control of 112 bot-controlled devices, achieving full closed-loop management of attack chains.

2. Key Sector Adoption

·Adopted by **50** core organizations in public security, banking, finance, and government sectors.

Applications and Promotion

3. Major Event Safeguards

·Secured high-profile international events: Winter Olympics, Asian Games, Universiade, Asian Winter Games, and the Canton Fair.
·Provided decade-long protection for the Canton Fair with **zero security incidents.**
·Cumulative threat detection: Over **24.81 million** high-risk threats identified.

4. Technological Superiority

·Pioneered an active defense system featuring **"trap deployment, attack observation, collaborative conversion, and attack entrapment."**
·Recognized by **316 global experts** (including 158 IEEE Fellows and 62 members of the Chinese Academy of Engineering and Chinese Academy of Sciences).
·Submitted 67 zero-day vulnerabilities certified by both CVE and CNVD.

5. Economic Impact

·Generated over **5.7 billion CNY** (approximately 780 million USD) in revenue in the past three years.