

4) Enter the interface to operate related functions of the external application cloud platform

4.2.2.4 Data return function

Supports the transmission of result files, cloud notes and other data obtained from the task cloud host to the private network management platform. The transmission is point-to-point transmission,

that is, from the external network file server to the private network file server. This transmission channel can only be transmitted in one direction and is irreversible.

External network/private network file server used for file transfer, and the received files are encrypted and stored. File transmission and storage are

isolated in the directory structure, from single user to single user, and from log file to log file in order to prevent third parties from snooping and tampering,

and ensure the security of data transmission.

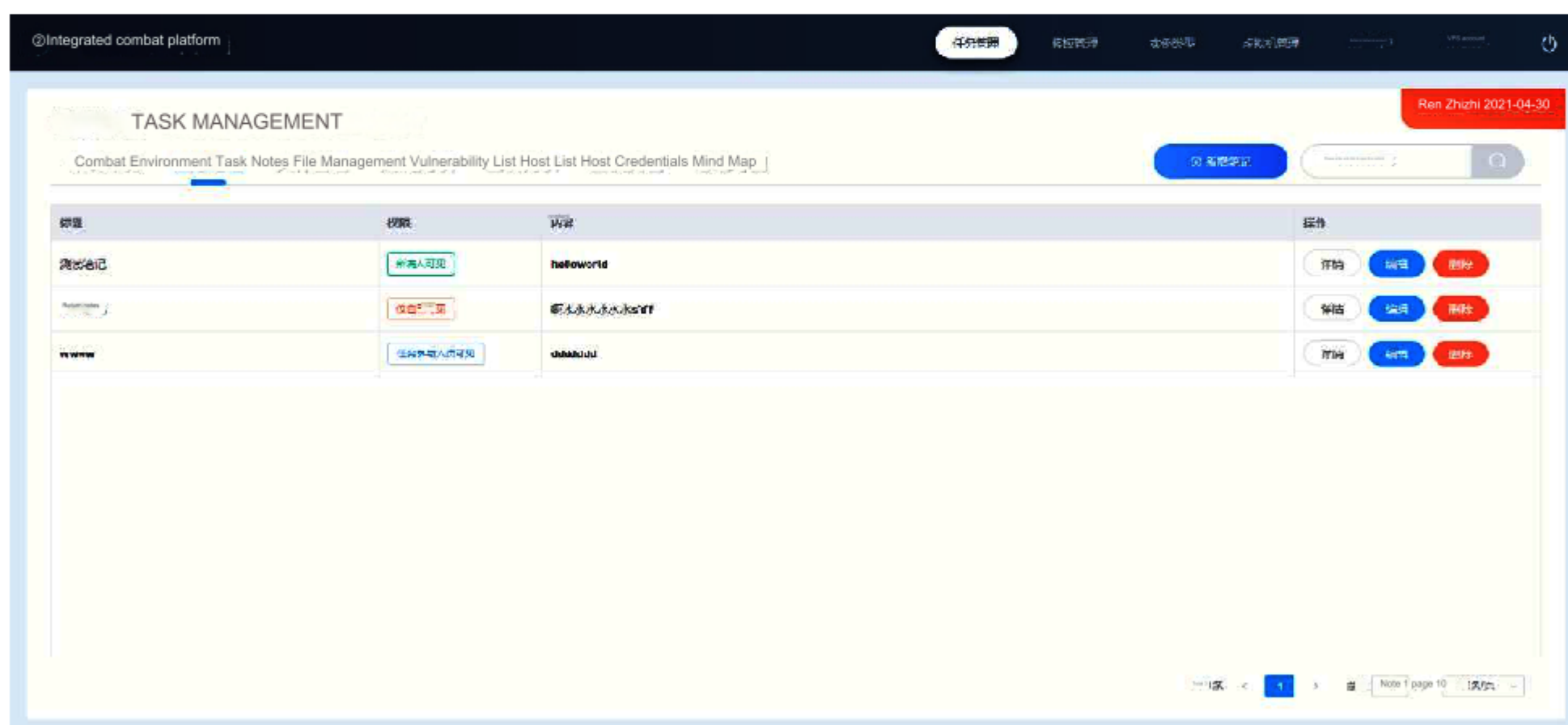
The external private network information synchronization function includes file synchronization, cloud note synchronization and task cloud host information synchronization.

4.2.2.5 Task note function

The task note component supports collecting, organizing and writing various types of information. It supports the creation of folders for classified storage, supports the

insertion of pictures and attachments, supports automatic saving, etc., making it easy to organize and summarize fragmented records such as new techniques and tactics and

usage experience formed during actual operations, and quickly synchronize to Private network and display.

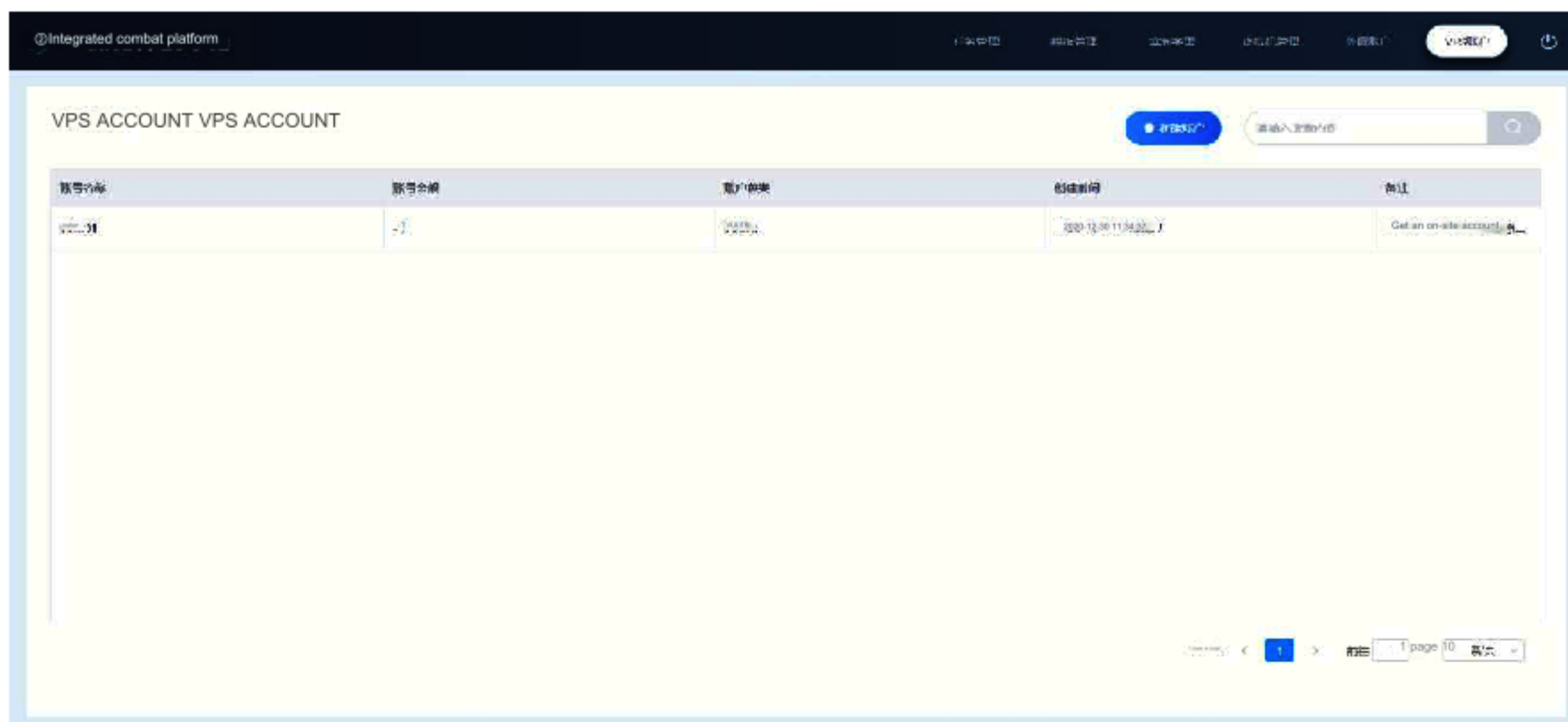


(Task note management)

4.2.2.6 Virtual machine management function

Supports management of virtual machines included in the platform, viewing corresponding IP or virtual machine status and time information, turning on or off virtual

machines and other operations.



(vps account management)

4.2.3 Link resource management function

In principle, there are no less than 3 access links to the external network platform, 2 TZ cover links and 1 scientific Internet link. The TZ cover link is used for daily network combat environments; the scientific Internet link is used for daily access. use. Whether you purchase third-party link resources or build your own links, all links must be in fully anonymous mode.

4.3 Security protection system

Security is the foundation and prerequisite for the application of integrated combat platforms. On the basis of building a basic security system, we design security strategies, build security barriers, and create security mechanisms from multiple dimensions such as identity authentication, data security, link security, anti-reconnaissance security, and security management to ensure that TZ business actual work is highly concealed and Highly safe and highly reliable.

4.3.1 Basic security system

The intranet platform should be deployed in the computer room in the user's jurisdiction, and the external network platform should be deployed in a safe and controllable computer room. A special security area should be set up in the computer room, and non-related personnel should not be allowed to contact to ensure the physical safety of the machine.

The internal and external networks of the platform are physically isolated. The security of the internal network relies on the protection system of the network security private network (such as deployed on the network security private network). If there is no

Deployment, then create a new protection system. External network security, in addition to the necessary security protection equipment, according to different application modules of the external network,

Set up different security zones for fine-grained security protection. Safety protection equipment, including but not limited to the security of each host system on the platform

Reinforcement, firewall, traffic auditing, intrusion detection equipment, APT attack detection equipment, honeypots, etc. Where conditions permit, please refer to etc.

Carry out safe construction according to the standards of Level 3 or above.

You can consider using masked identities to carry out the above-mentioned basic security system construction work.

4.3.2 Data security design

Data security refers to the technical and management protection measures adopted for the storage and transmission security of platform data. It is used to protect

computer hardware, operating systems, software and data from being damaged, tampered with and leaked due to malicious reasons.

One is data storage security. The storage device has an industrial-grade high-reliability design, supports concurrent access, and ensures that all cloud services on the cloud platform

It ensures uninterrupted business for customers and prevents unauthorized access. Security measures include:

1) Protect the integrity and confidentiality of key information such as user identification information and audit logs.

2) Effectively isolate the storage data of different cloud service customers in the cloud platform.

3) Take corresponding technical measures to monitor storage hardware resources and storage software resources in real time, provide timely alarms for abnormal

situations, and notify relevant responsible persons.

4) There are corresponding measures at the physical and software levels, such as disk redundancy queues, regular backups, redundant storage, encrypted

storage and isolated storage, etc., to prevent data loss or illegal access.

The second is data transmission security. Data transmission security means that data can be transmitted safely and completely from the external network to the internal network,

without leakage of data and data sources during the process. Data transmission security is achieved from three dimensions: access security, data security and transmission channel security.

1) The data recipient can use the whitelist method to control the source of the data, and use network security equipment to monitor and warn the

data in real time.

2) Data must be encrypted before transmission. Data cannot be encrypted or decrypted during the transmission process. Data encryption must be one-time

encryption. After the transmission is completed, the recipient must verify the integrity of the data.

3) The transmission channel needs to use a covert link to hide both the sender and the receiver to prevent traceability. The transmission channel needs to strictly control the source

and destination of data, and adhere to the principle of minimizing access.

The third is the safety of the combat environment. Combat environment security is to ensure the security of the cloud host environment during the execution of tasks and meet the

following requirements:

1) Supports firewall enablement and configuration of the host operating system.

2) Ability to conduct regular vulnerability monitoring on cloud hosts and perform patch updates in a timely manner.

3) Able to monitor the use of tools in the host, the opening of ports, etc., and provide early warning for abnormal situations to ensure the security of the

cloud host.

The fourth is tool platform security. Ensure the security of the tool platform through identity authentication and multi-dimensional access control, and ensure the security of the

tool itself through security testing and encrypted storage to meet the following requirements:

1) The tool platform can only be accessed within the private network and has no Internet access channel.

2) The tool platform has identity authentication to minimize access rights and ensure that only those with designated special permissions can use the tool platform.

3) The tool platform restricts access to source IP.

4) Conduct a comprehensive security test on the tool itself to ensure that there are no loopholes in the test and prevent the safe operation of the cloud host from being affected after uploading.

5) Conduct security training for those with access rights, securely upload the toolkit through special encryption, and use a one-time

password.

6) Authorize the use of tools, and they cannot be used without authorization.

4.3.3 Identity authentication security

No real personal information (including but not limited to WeChat, email, phone number, police number, etc.), task information (including but not

limited to task content, etc.) will appear in any part of the external platform (including account number, user name, new content, etc.) Task number, participants,

etc.), and no confidential information shall appear.

The external network platform uses two-factor strong authentication and needs to use dynamic passwords, QR code authentication and other methods for two-factor authentication to prevent others

from maliciously logging in.

The platform uses high-intensity security policies to prevent brute-force cracking of platform usernames and passwords through blacklists, connection limit limits,

password error limits and other methods.

4.3.4 Security link design

The first is access link security: the intranet platform is in an isolated secure network and is not connected to the Internet. Host creation for the external network platform requires that

the resource configuration information and tool authorization information in the intranet be transmitted to the external network platform using offline encryption.

The second is the security of the combat link: the external network platform does not directly conduct operations against the target, but must access the secure hidden link to conduct

work on the target. If the combat link is interrupted, the cloud host needs to be disconnected from the network to avoid IP address leakage caused by direct connection to MB.

The third is access link security: platform users need to access the combat host through a special access link.

Fourth, backhaul link security: In order to ensure the security of the intranet platform, when data from the external network is transmitted to the intranet platform, the transmission channel

is one-way and irreversible. And the transmission link is isolated from the access link. When there is no one-way data import channel between the external network and the internal network, the internal

network will actively capture the task data and notes transmitted to the secure data cloud center. When there is no one-way data import channel between the external network and the internal network, a

secure data cloud center must be established and deployed in a secure network domain (connected to the Internet, but with two-way access control and protection), and the internal network platform

must also be deployed in another Within the secure network domain (connected to the secure data cloud center, but with two-way access control and protection). Task data and notes are encrypted

and transmitted to the secure data cloud center and stored encrypted. The intranet actively initiates an application to the secure data cloud center. After passing the certification, the data and notes

are encrypted and transmitted to the intranet.

4.3.5 Anti-reconnaissance design

The first is covert camouflage: The external platform uses ultra-long random strings to set login addresses and uses non-related name naming systems to covertly

camouflage the platform to prevent others from guessing the address.

The second is content desensitization: the external platform uses desensitized text, logo naming related functions, and tab pages. All information on the external platform must be

Nothing to do with business.

The third is platform code security: developer information cannot exist in the platform code, and information related to developers and platform functions cannot exist in

the annotation information. Code audits and security tests are required before the platform is released to prevent it from being exploited by attackers.

Fourth, trace removal: the platform will not store any user-related information or usage trace information.

The fifth is security cover: Platform development, line rental, computer room rental and other businesses need to be handled using a cover identity to prevent

Stop being traced and located. The system, language, time zone, font, system environment, input method, etc. used by the external platform must all be in non-Chinese languages. all

The configuration information is configured according to the protected identity.

The sixth is self-destruction processing: after detecting a system intrusion on the external network platform, the network connection is first blocked, and then the level of harm is assessed.

When the hazard level reaches a certain level, the self-destruction process is initiated.

4.3.6 Managing security design

The first is the management system: organizations at all levels formulate corresponding management regulations, form a dedicated, authoritarian, and dedicated management model, improve the management system, conduct strict review of personnel entering and exiting the computer room, conduct regular inspections of the environmental safety of the computer room, and pass the system. Ensure people and environment are reliable.

The second is safe operation specifications: through long-term actual combat accumulation and summary, safe operation requirements for daily work are gradually formed. The operations of relevant personnel must comply with security regulations. Any attack operations are based on tasks and will not attack targets privately.

The third is daily security management: Platform managers need to regularly audit the operations of platform users so that problems can be discovered and resolved early.

4.3.7 Application security design

First, non-administrator permissions: The combat cloud host can only be logged in through non-administrator accounts, and corresponding group policies are configured, such as prohibiting modification of registry entries, prohibiting access to system directories, prohibiting modification of network configurations, etc.

The second is the black/white list control mechanism: black/white list configuration can be performed on the network resources that the combat cloud host is allowed to access, such as restricting the resources that the cloud host can access based on domain names, IPs, ports, etc.

5

Product parameters

（一）Intranet platform	
category	Parameter index
Architecture	B/S architecture
Deployment method	local deployment
Intranet business management module	
Task management function	support
Personnel management function	support
User management function	support
Points management function	support
Skills and tactics sharing function	support
Task statistics function	support
Log management function	support
Intranet resource management module	
Data resource management function	support
Template resource management function	support
Link resource management function	support
Weapon resource management function	support
Security sandbox module	
File import analysis function	support
API detection function	support
Behavior analysis function	support

Process image analysis function	support
PACP packet capture analysis function	support
Malicious behavior screenshot function	support
(二) External network platform	
category	Parameter index
Architecture	B/S architecture
Deployment method	local deployment
External network task management module	
Task list display	support
View cloud host information	support
Weapons resource management module	
File import analysis function	support
API detection function	support
Behavior analysis function	support
Process image analysis function	support
PACP packet capture analysis function	support
Malicious behavior screenshot function	support
Weapon storage management function	support
Weapon storage management function	support
Weapon information annotation function	support
Weapon classification encrypted storage function	support
Weapon download logging	support
Weapons resource management module	

Weapon authorization update function	support
Weapon upgrade update function	support
Historical version tracing function	support
Weapon update logging function	support
Combat environment management module	
Cloud host management function	support
Template management function	support
Terminal access function	support
Data return function	support
Task note function	support

6 Product Deployment

6.1 Applicable environment

The integrated combat platform is a set of professional system platforms that can achieve a high degree of business integration, efficient and intensive resources, efficient and practical collaboration, and build a complete security system. It is suitable for network TZ teams to conduct collaborative and efficient operations to achieve full integration of various resources, Create safe and concealed technical measures, scientifically manage TZ weapons and equipment usage mechanisms, establish and improve TZ task process specifications and other TZ comprehensive business scenarios.

6.2 Deployment method

The integrated combat platform is mainly divided into two parts, namely the intranet business comprehensive management platform and the external network combat application management platform. The intranet business comprehensive management platform is deployed in the absolute intranet (can be deployed in the network security private network), and the external network combat application management platform is deployed in a secure computer room that can connect to the Internet. In order to fully ensure the security of interaction between the internal and external networks of the platform, when the internal network transmits instructions to the external network, offline encrypted transmission (non-physical connection) is used. When the external network platform returns data to the internal network platform, the data is transmitted in one direction and is in the link. Add light gates to securely control data transmission.

(1) Integrated intranet business management platform

The intranet business comprehensive management platform is deployed in the intranet computer room where the user is located. In order to meet the functional needs of the intranet

platform and the basic operating environment, the platform deployment requires a high-performance server for resource monitoring, calling and data storage. Server-related The configuration

is as follows:

Configuration Environment	Device parameters
Intranet server configuration	1. Control nodes and storage nodes support monitoring and calling the resource usage of slave devices, and storing related data.
	2. CPU: Intel 5218*2
	3. Memory: 128G
	4. Network card: 4*GE
	5. Disk controller: 6/12G RAID card supporting RAID5
	6. Hard drive: 960GSSD+6TSATA*5
	7. Quantity: 1 unit

(2) External network combat application management platform

The external network combat application management platform is deployed in a secure computer room that can be connected to the Internet. In order to meet the basic functional applications

and basic operating environment of the external network platform, the platform deployment needs to be equipped with a total of 6 servers of various types such as control nodes, computing nodes,

and storage nodes. , At the same time, in order to meet the needs of the combat environment, anonymous purchase kits are used to purchase VPS servers to build VPS clusters, in which the

number of concurrent VPS servers is no less than 30, fully ensuring multi-task execution needs. The server related configuration parameters are as follows:

Configuration Environment	Device parameters
Control node server configuration	1. Control node supports monitoring and calling the resource usage of slave devices.
	2. CPU: Intel 4216*2
	3. Memory: 128G
	4. Network card: 4*GE

	5. Disk controller: 6/12G RAID card supporting RAID5
	6. Hard drive: 480GSSD+4TSATA*4
	7. Quantity: 2 units
Compute node server configuration	1. Computing nodes provide computing resources and virtualization capabilities.
	2. CPU: Intel 5218*2
	3. Memory: 128G
	4. Network card: 4*GE
	5. Disk controller: 6/12G RAID card supporting RAID5
	6. Hard drive: 480GSSD+4TSATA*4
	7. Quantity: 2 units
Storage node server configuration	1. Storage nodes provide storage capabilities.
	2. CPU: Intel 5218*2
	3. Memory: 128G
	4. Network card: 4*GE
	5. Disk controller: 6/12G RAID card supporting RAID5
	6. Hard drive: 480GSSD+6TSATA*6
	7. Quantity: 2 units
VPS server cluster	1. Single cloud host hard disk $\geq 100G$
	2. Cloud host concurrency ≥ 30 units
	3. VPS are purchased using anonymous packages
	4. IP addresses are all overseas addresses

7 product advantages

> Highly integrated business

The integrated platform fully combines the characteristics of network TZ business, establishes a standardized task-oriented management mechanism, and builds a complete set of business processes from task release, reception, pre-start, mid-control, and post-processing, and combines the business processes to form an integrated standardization.

An integrated working environment, solidified covert secure access links, flexible task release and approval management, and strict weapon use all-promote the highly integrated and standardized development of business work in an all-round way.

> Efficient and intensive resource utilization

The integrated platform fully combines the actual business direction of TZ, makes full use of virtualization technology and multi-interface collaboration technology, integrates various combat environment resources such as links, weapons, techniques and tactics required for TZ work, and provides combat resources, combat environment, The unified management and application of combat weapons and combat methods has created a comprehensive, centralized and efficient management and use platform that integrates various resources such as environmental management, weapons management, and data management.

> Full platform virtualization

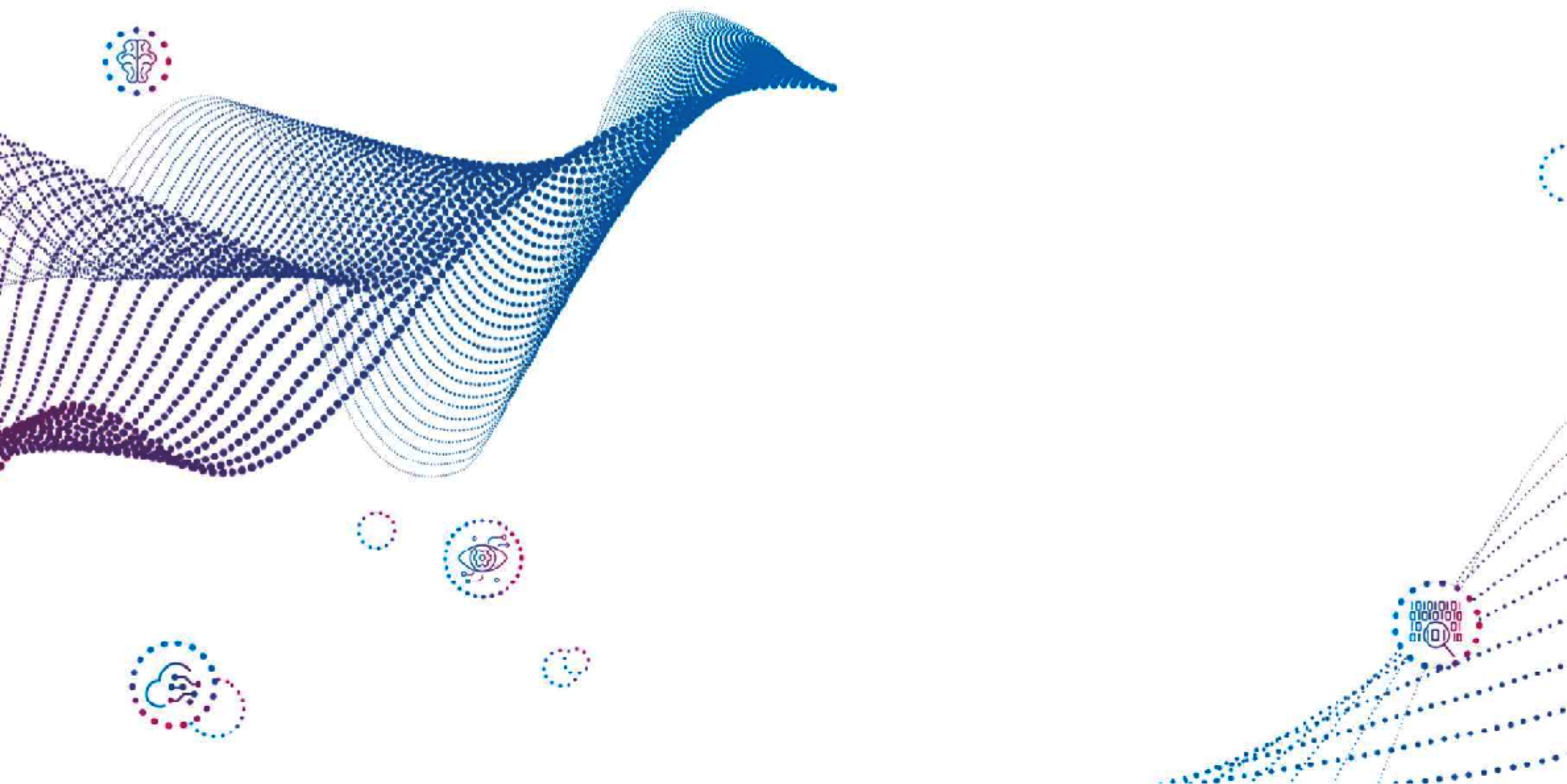
The entire platform uses iSoonStack technology to provide resource optimization and virtualization, which includes storage services, image management, With network management, virtual machine management and other functions, users can simulate real network topology and build their own network according to their own needs.

The network environment is configured through a virtual host and a visual operation interface, which simplifies the tedious configuration and does not require the user terminal to type commands.

Moreover, the operation logic is reasonably designed to be simple, efficient, and easy to expand. It is suitable for different network topology environments and does not require Repeat configuration is required.

> Deep security system

The integrated platform construction focuses on TZ's business environment needs and combat environment needs, and carries out a safe and reliable security protection system design, formulating a high-intensity security protection strategy. According to various requirements such as safety regulations and safety standards, from physical security to equipment security Carry out comprehensive and detailed planning and scientific design from multiple dimensions such as application security, data security and management security, so as to protect the entire platform and prevent damage and attacks.



Integrated combat platform

Product white paper

(V1.0 version in 2022)

1	Introduction	1
2	demand analysis	1
3	Product Introduction	2
3.1	Product introduction.	2
3.2	Product composition.	3
3.3	System architecture.	3
3.4	Network architecture.	4
4	product features	6
4.1	Intranet platform functions	6
4.1.1	Intranet business management module.	6
4.1.2	Intranet resource management module.	16
4.1.3	Security sandbox module,	18
4.2	External network platform functions	22
4.2.1	External network task management module.	22
4.2.2	Weapons resource management module.	19
4.2.3	Combat environment management module.	26
4.2.4	Link resource management function.	31
4.3	Safety protection system... ..	31
4.3.1	Basic security system..	31
4.3.2	Data security design	32

4.3.3 Identity authentication security.	33
4.3.4 Security link design.	33
4.3.5 Anti-reconnaissance design:	34
4.3.6 Managing security design	35
4.3.7 Application security design	35
5 product parameters	36
6 Product Deployment	38
6.1 Applicable environment.	38
6.2 Deployment method.	38
7 product advantages	41

1 Introduction

In recent years, with the continuous development and construction of network TZ teams and TZ laboratories at all levels, the level of technical personnel reserves and equipment construction of public security network TZ teams at all levels has reached a certain level. The professional network TZ laboratory team focusing on "team building, capacity building, infrastructure construction, and equipment construction" has achieved good results in combating various network illegal and criminal activities, obtaining key clues and intelligence to protect national security, and has also demonstrated its The network TZ team will play a decisive role in the future work of guarding, governing, and maintaining cyberspace.

However, with the development of the Internet and 5G and other mobile networks, network TZ work has begun to have characteristics such as diversity, randomness, complexity, and cumbersomeness. In the daily development of network TZ work, improper collaboration, improper cover, and lack of preparation are prone to occur. , Insufficient response, which often leads to unclear tasks, slow implementation, and low efficiency in TZ work.

Therefore, based on the current development trend and business direction of network TZ business, it is necessary to carry out overall planning and build a professional TZ business comprehensive combat management platform to solve the problems of security, concealment, collaboration, mobility and flexibility in daily TZ work, and through the establishment of mission-oriented A comprehensive combat management platform that integrates , environment, resources and security protection to fully integrate various resources, create safe and concealed technical measures, scientifically manage the use mechanism of TZ weapons and equipment, and establish and improve task process specifications.

2 Requirements analysis

The integrated combat platform should be able to solve the related problems encountered by network TZ services. It is a set of professional system platforms that can achieve high degree of business integration, efficient and intensive resources, efficient and practical collaboration, and build a security system.

The construction of the entire platform needs to meet the following requirements:

(1) High degree of business integration

The integrated combat platform should be able to fully combine the characteristics of network TZ business, establish a standardized task-oriented management mechanism, and build a complete set of business processes from task release, reception, pre-start, mid-control, and post-processing, and combine with business processes to form a centralized A platform that integrates a standardized working environment, solidified covert secure access links, flexible task release and approval management, and strict weapons use Taiwan, comprehensively promote the highly integrated and standardized development of business work.

(2) Efficient and intensive resource utilization

The integrated combat platform should be able to fully integrate the actual business direction of TZ, make full use of virtualization technology and multi-interface collaboration

technology, integrate various combat environment resources such as links, weapons, techniques and tactics required for TZ work, and provide combat resources, combat Unified management and

application of the environment, combat weapons, and combat methods to create a comprehensive, centralized and efficient management and use platform that integrates environmental management,

weapons management, data management and other resources.

(3) Collaboration is efficient and practical

The integrated combat platform should be able to provide a cross-time, cross-space, and cross-task collaborative working mechanism. Combined with the collaborative model of TZ business

work, various collaborative models in actual combat should be reflected on the platform, which can facilitate the technical personnel of the special investigation team in Collaborative operations,

combined operations, and team sharing of techniques, tools, equipment, and results are carried out on the platform to give full play to the advantages of collective operations. And the entire platform takes

practicality, ease of use, and ease of use as its fundamental goals, and achieves the overall construction purpose of being based on needs, serving the process, and improving combat effectiveness.

(4) Build a safety system

The integrated combat platform should be able to provide a safe and reliable security protection system design around the TZ's business environment needs and combat

environment needs, and formulate high-intensity security protection strategies. According to various requirements such as safety regulations and safety standards, from physical

security, Comprehensive and detailed planning and scientific design are carried out from multiple dimensions such as equipment security, application security, data security and

management security, so as to protect the entire platform from damage and attacks.

3 Product Introduction

3.1 Product introduction

The integrated combat platform is a dedicated system platform based on solving actual combat problems. Under the entire business system, it belongs to the category

of combat units and is mainly used to organize and implement combat tasks. The integrated combat platform adopts physical isolation of internal and external networks. All combat

resources and combat environments are concentrated in the cloud with high-strength protection. Actual combat tasks are released through the intranet to ensure the security of

internal and external network data. Actual combat team members can safely and covertly access the combat platform at any time, anywhere, through any network, and using any terminal

to carry out actual combat work.

Based on this platform, combat team members can achieve collaborative operations in the same combat scenario for common tasks and goals, share resources,

intelligence and weapons and equipment, coordinate the progress, process and goals of combat tasks, and maximize the use of the team combat power. At the same time, the

cloud platform generates an assembled combat environment, solidifies security links, standardized security protection measures, and strict task process approval management to

constrain the behavior of combat team members, strictly control and prevent external attacks, and ensure operational security.

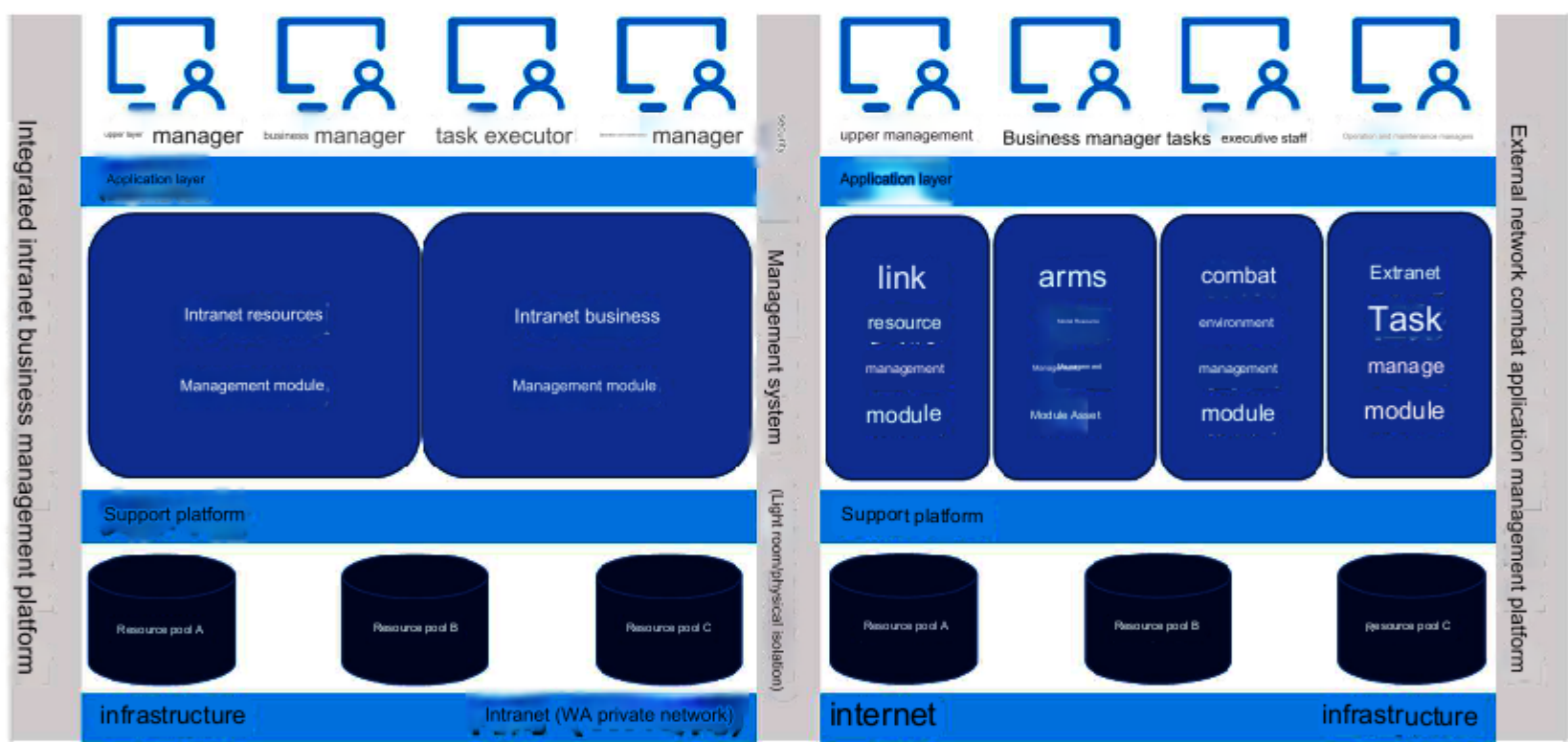
3.2 Product composition

The platform can be set up in a local deployment mode. Users can use server clusters of corresponding sizes according to their own needs. The platform can be

used after being deployed in the cluster. The product composition list is mainly as follows:

- 1. Integrated combat platform: 1 set
- 2. Integrated combat platform user manual: 1 copy

3.3 System architecture



(system architecture diagram)

The integrated combat platform system is designed based on the overall network topology, which is divided from bottom to top: infrastructure, support platform

and application layer.

Infrastructure: Infrastructure is mainly the hardware resources required to deploy the support platform, including various network hardware equipment resources. The infrastructure

of the intranet business comprehensive management platform and the external network combat application management platform adopts virtualization technology and private cloud storage

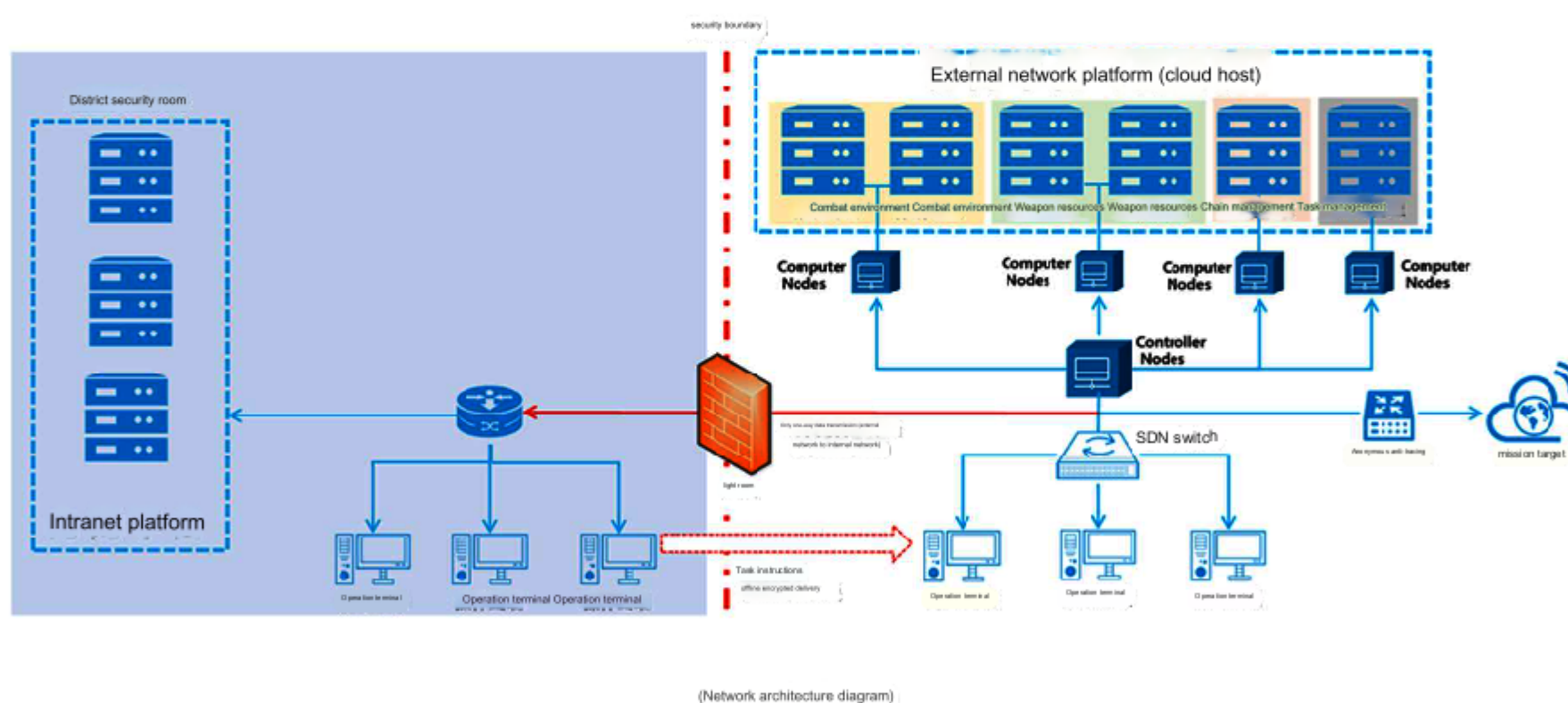
technology. Realize cluster allocation and resource scheduling of hardware resources to maximize the performance of platform infrastructure resources.

Support platform: The intranet business comprehensive management platform mainly deploys intranet resource management modules and intranet business management modules to meet daily needs.

Delivery of TZ services, comprehensive application management and evaluation of services, and comprehensive management and maintenance of data returned by daily TZ tasks. The external network combat application management platform mainly deploys the external network task management module, combat environment management module, weapon resource management module and link resource management module. The task management management module is mainly used for task status tracking and progress viewing on the external network platform; combat The environment management module mainly includes functions such as daily TZ mission environment issuance, environment generation, and environment destruction; the weapon resource management module mainly includes centralized management of various weapons and equipment required for daily mission execution, and issuing weapons according to mission requirements. For use, the link resource management module mainly provides comprehensive management functions for security cover links required for task execution, network links for daily use, and other network link resources.

Application layer: Mainly provides the login interface of the intranet business comprehensive management platform and the external network combat application management platform. Users can log in to the intranet business comprehensive management platform and the external network combat application management platform respectively through multiple security authentication and verification mechanisms. The two platforms provide different operating permissions and application interfaces based on user roles and identities. Further ensure the standardization and security of platform use.

3.4 Network architecture



The integrated combat platform is designed around the TZ business management idea. The intranet platform is deployed in the secure computer room in the user's jurisdiction, and the external network platform is deployed in the operator's computer room rented with a cover identity or the user's own cover base computer room, thus forming an entire Network architecture of integrated combat platform. The network architecture diagram mainly consists of three parts: the network environment of the internal network platform, the network environment of deploying the external network platform, and the interaction between the internal and external network environments.

Intranet platform network environment: In principle, the intranet platform is deployed in a secure computer room in the user's jurisdiction to build a private network (with the Internet The network is completely isolated and has no Internet access rights) or it can be deployed in the WA private network according to user needs to achieve control of the entire intranet platform.

Private network only.

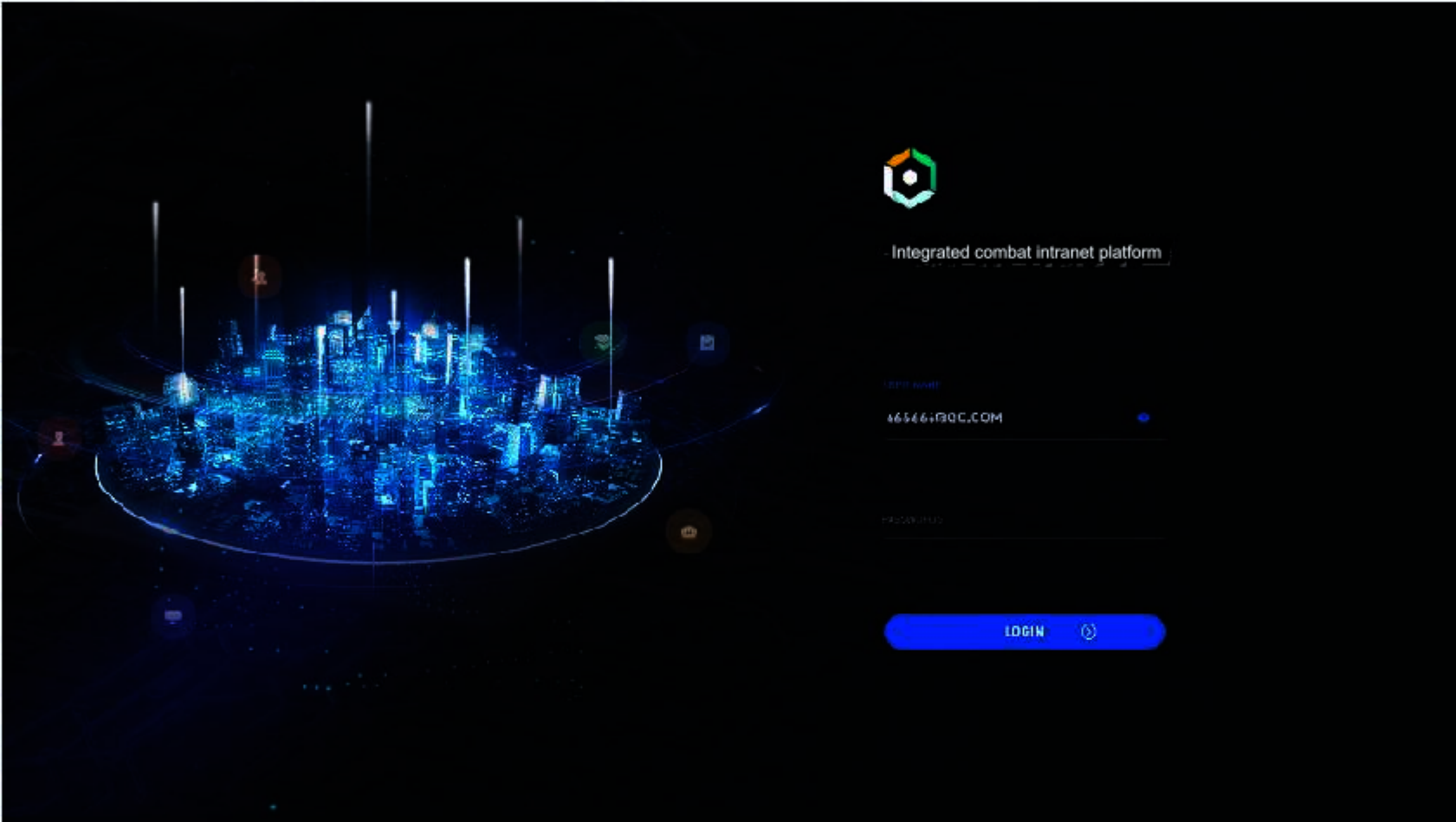
External network platform network environment: The hardware resources of various platforms that carry the external network's combat environment, weapon resources, link management, task management, etc. are deployed in a private cloud and deployed in the operator's computer room rented with a cover identity or the user's own cover base. In the computer room, combined with the particularity of each module and the network complexity of the external network platform, the external network platform is protected and isolated from the Internet through a firewall. The four management modules within the external network also adopt corresponding protection strategies to achieve mutual isolation. Only open necessary ports to achieve compliant use and operation of various resources.

Network interaction in the internal and external network environment: mainly includes two directions. One is to transfer instructions from the internal network to the external network. The transmission method must be offline and cannot be transmitted through any physical connection method. The instructions must be encrypted and transmitted, and the instructions should be in accordance with the agreed Data format and value specifications are written and transmitted. The second is to return the data collected by the task from the external network to the internal network. The return must be one-way and can only be transmitted from the external network to the internal network. The return data must be encrypted before it can be transmitted. The return must be through a separate cover link.

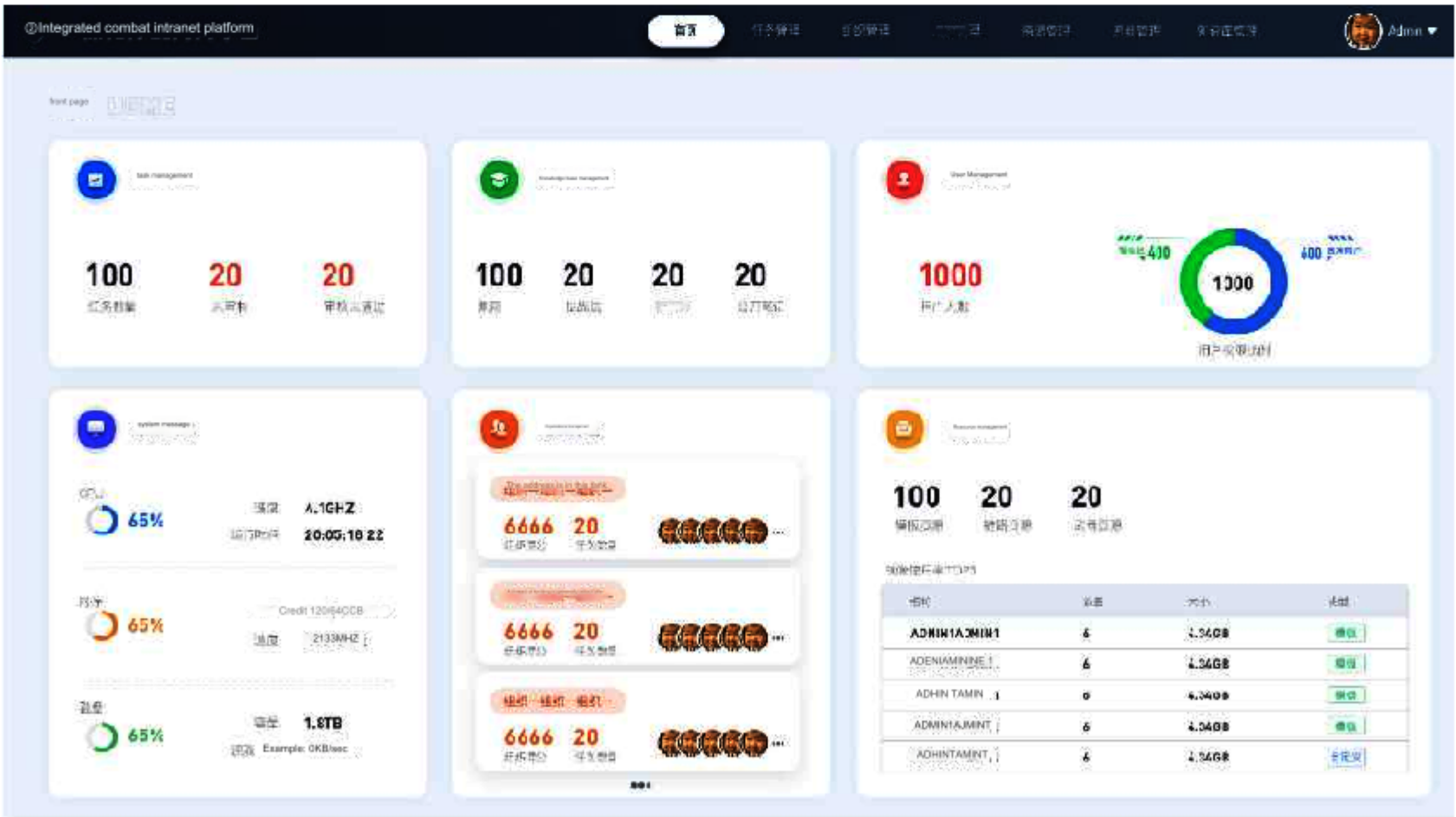
4 product features

4.1 Intranet platform functions

The intranet platform mainly includes an intranet business management module and an intranet resource management module. The intranet business management module is a component of the intranet business comprehensive management platform and an important link in realizing a complete closed-loop process; the intranet resource module is mainly responsible for comprehensive management of various intranet resources and external network backhaul resources. To ensure the security of the intranet, a security sandbox module will be deployed on the front end of the intranet resource management module.



(Intranet platform login interface)



(Intranet platform home page)

4.1.1 Intranet business management module

The intranet business management module mainly includes task management function, personnel management function, user management function, points management function,

technology and strategy sharing function, task statistics function, and log management function.

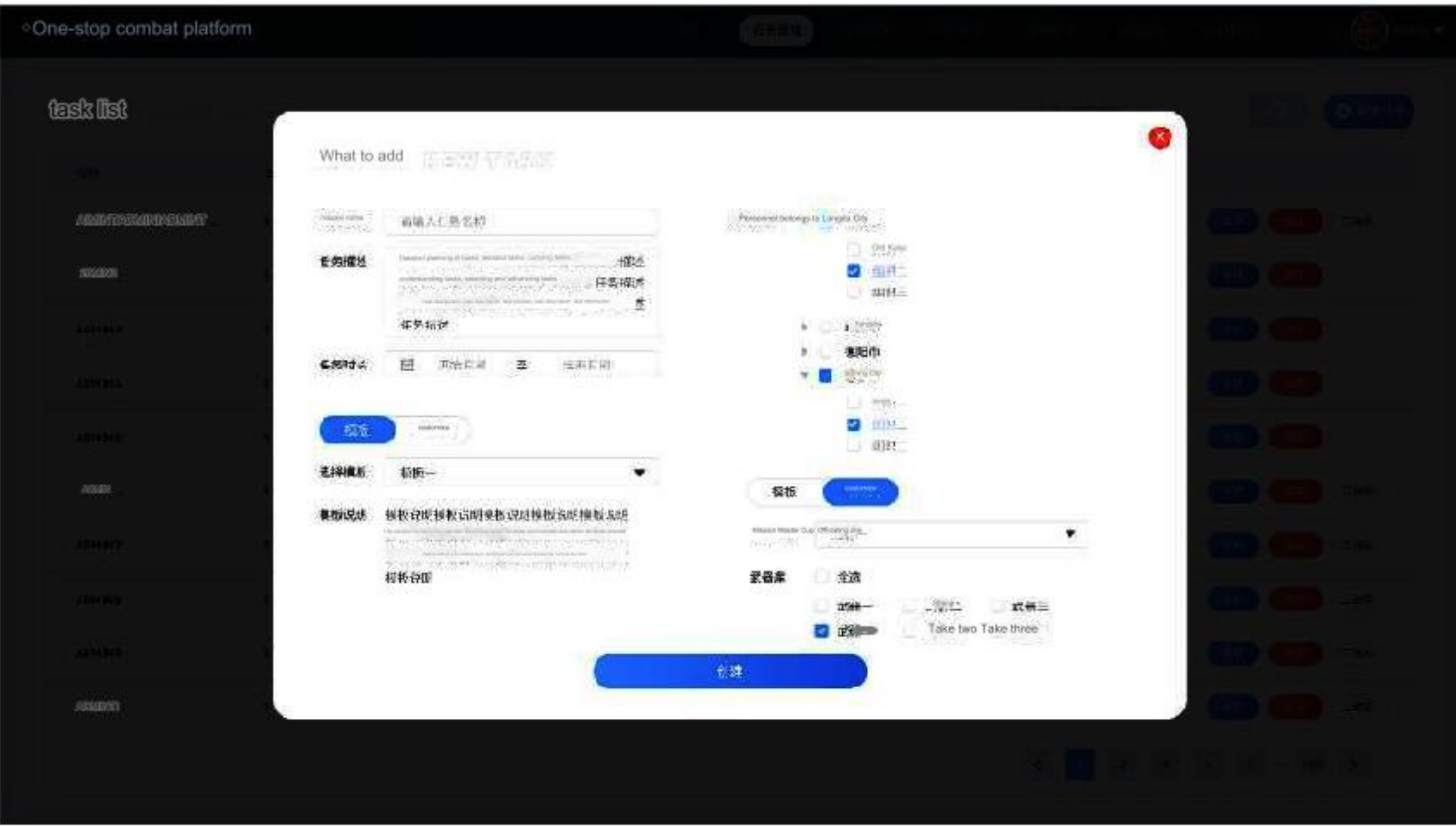
1) Task management function: Task management is the core function of the intranet business management platform. Authorized users

publish tasks through the task management module, assign specific subtasks to subordinate team members, and review and comment on

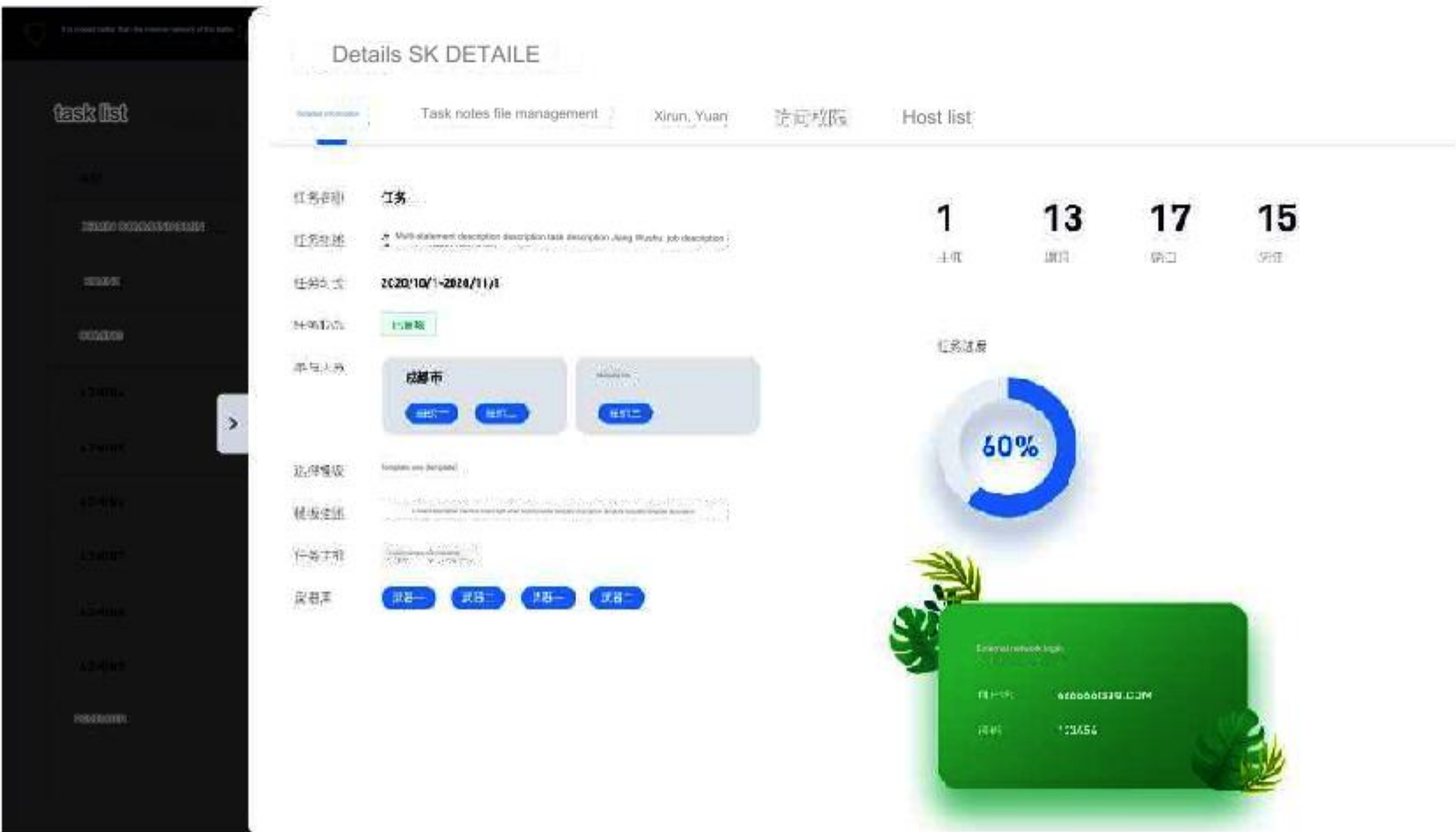
the submitted task results. , as the basis for performance appraisal; team members can view assigned tasks through task management,

and can apply for new tasks as needed, or perform task transfer and other operations. Mainly include: task release, task viewing, task

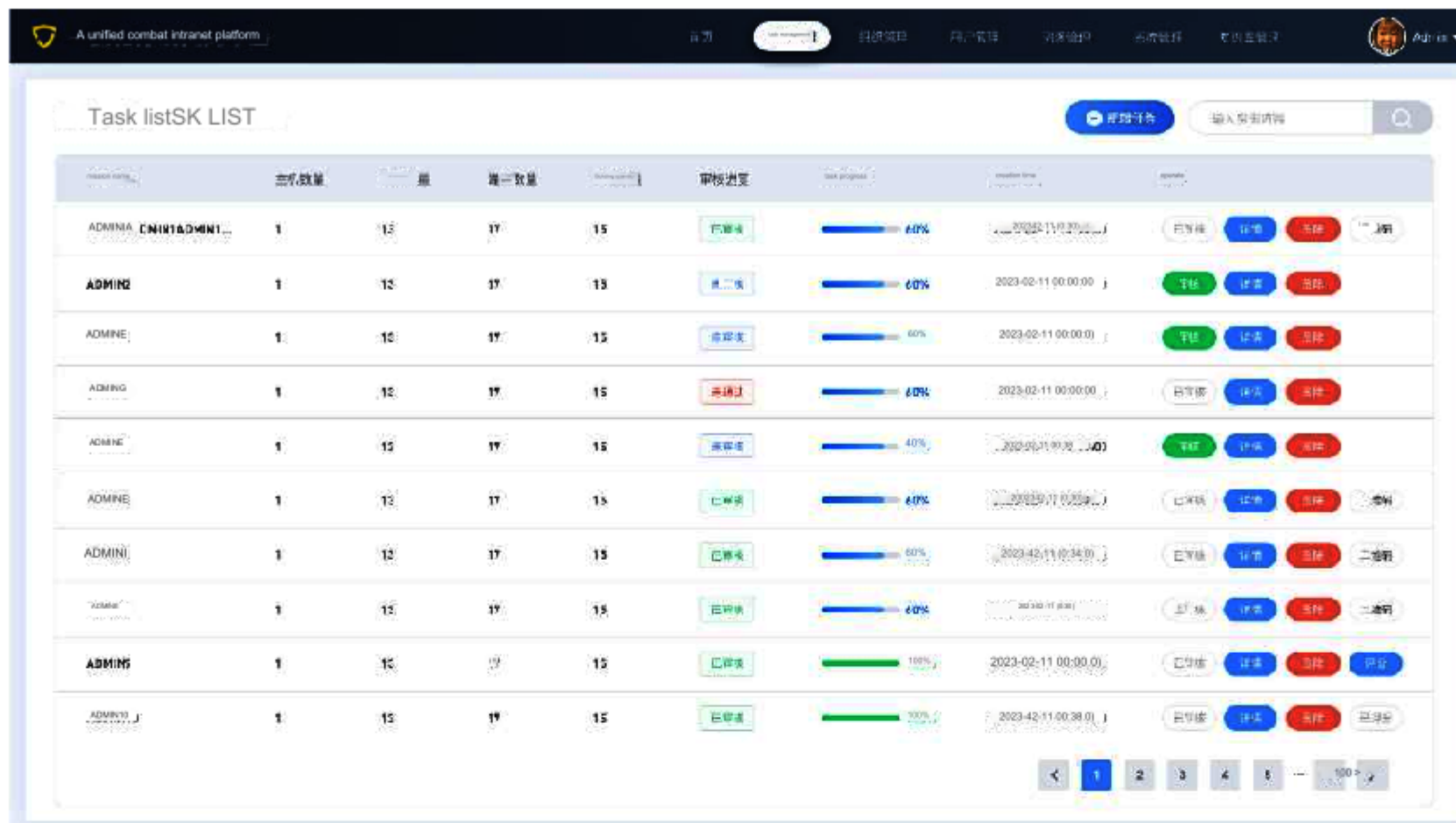
review, task application, task transfer and task review.



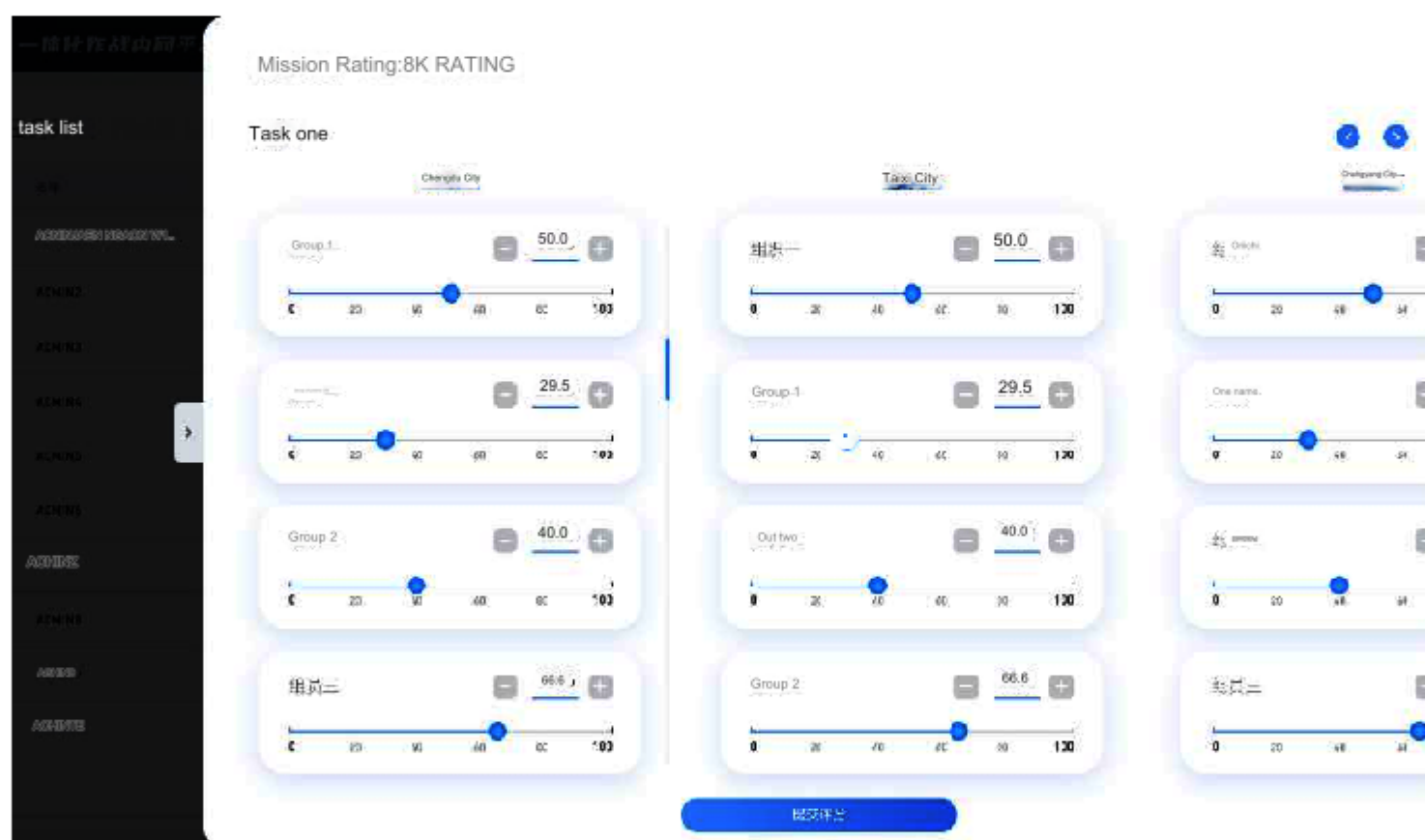
(task release)



(Task view)



(task list)



(mission review)

Integrated combat intranet platform

首页

任务管理

组织管理

用户管理

资源管理

系统管理

帮助与反馈

Admin

Organizational management

组织管理

组织列表

姓名	E-mail	contact number	所属单位	所属城市	操作
ADMIN1ADMIN1ADMIN1...	666664000.COM	13123456789	17	15	<div>修改</div> <div>删除</div>
ADMIN2	461444000.COM	13123456789	17	15	<div>修改</div> <div>删除</div>
ADMIN3	664644800.COM	13123456789	17	15	<div>修改</div> <div>删除</div>
ADMIN4	666665800.COM	13123456789	17	15	<div>修改</div> <div>删除</div>
ADMIN5	661664000.COM	13123456789	17	15	<div>修改</div> <div>删除</div>
ADMIN6	661665800.COM	13123456789	17	15	<div>修改</div> <div>删除</div>
ADMIN7	661666000.COM	13123456789	17	15	<div>修改</div> <div>删除</div>
ADMIN8	661444800.COM	13123456789	17	15	<div>修改</div> <div>删除</div>
ADMIN9	661666000.COM	13123456789	17	15	<div>修改</div> <div>删除</div>

<

1

2

3

4

5

...

100

>

(personnel list)

3) User management function: It mainly provides permission management for platform users, and divides different permissions according to the user's identity, including user creation, permission allocation, task viewing, task sharing and other functions.

Integrated combat intranet platform

组织管理

用户管理

资源管理

系统管理

帮助与反馈

Admin

User Management

用户管理

用户列表

New users

新增用户

Username

张三

Contact number

Please enter your contact number

E-mail

请输入电子邮箱

用户权限

普通用户

管理员

普通用户

管理员

Personnel belonging to war city

选择一

选择二

选择三

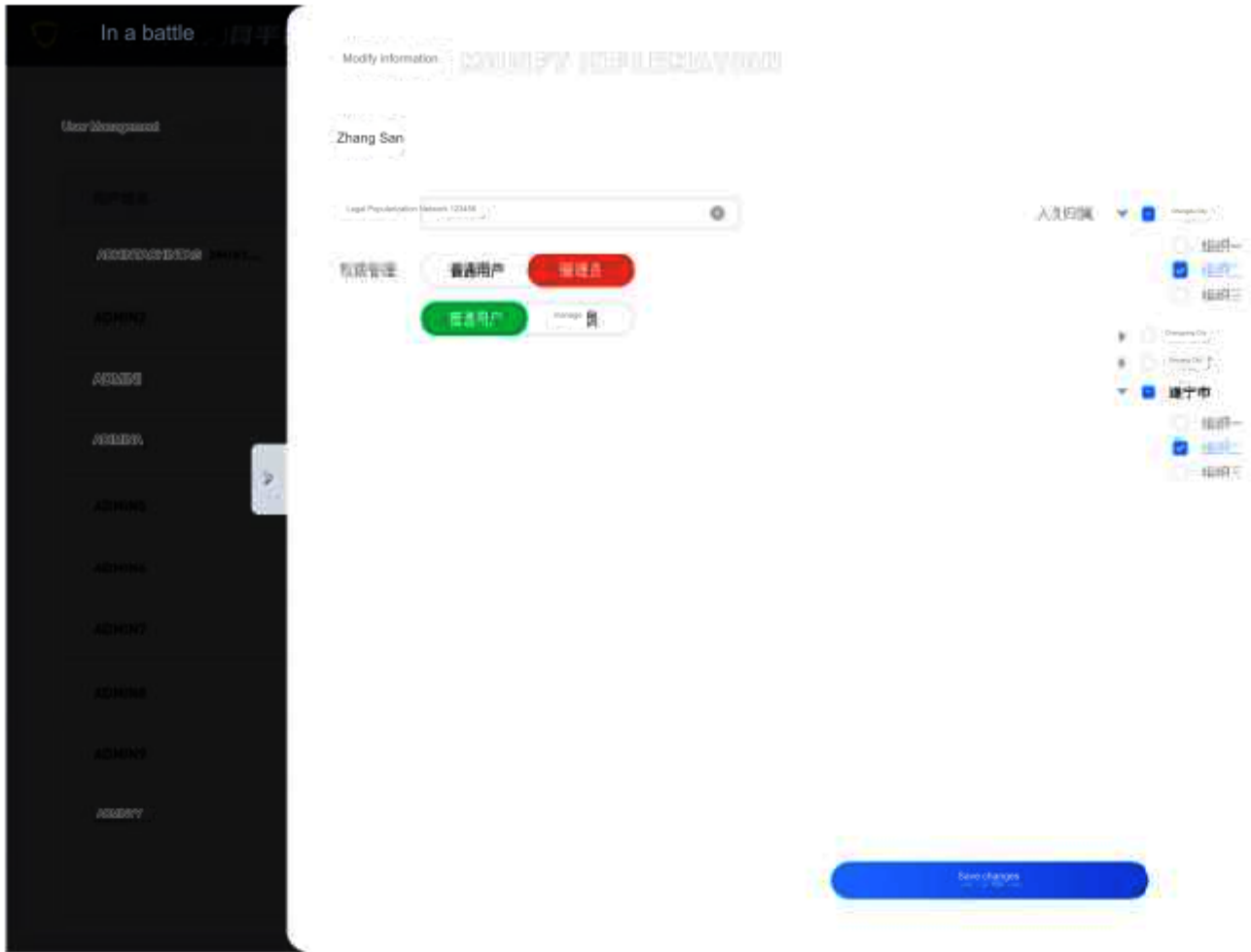
选择一

选择二

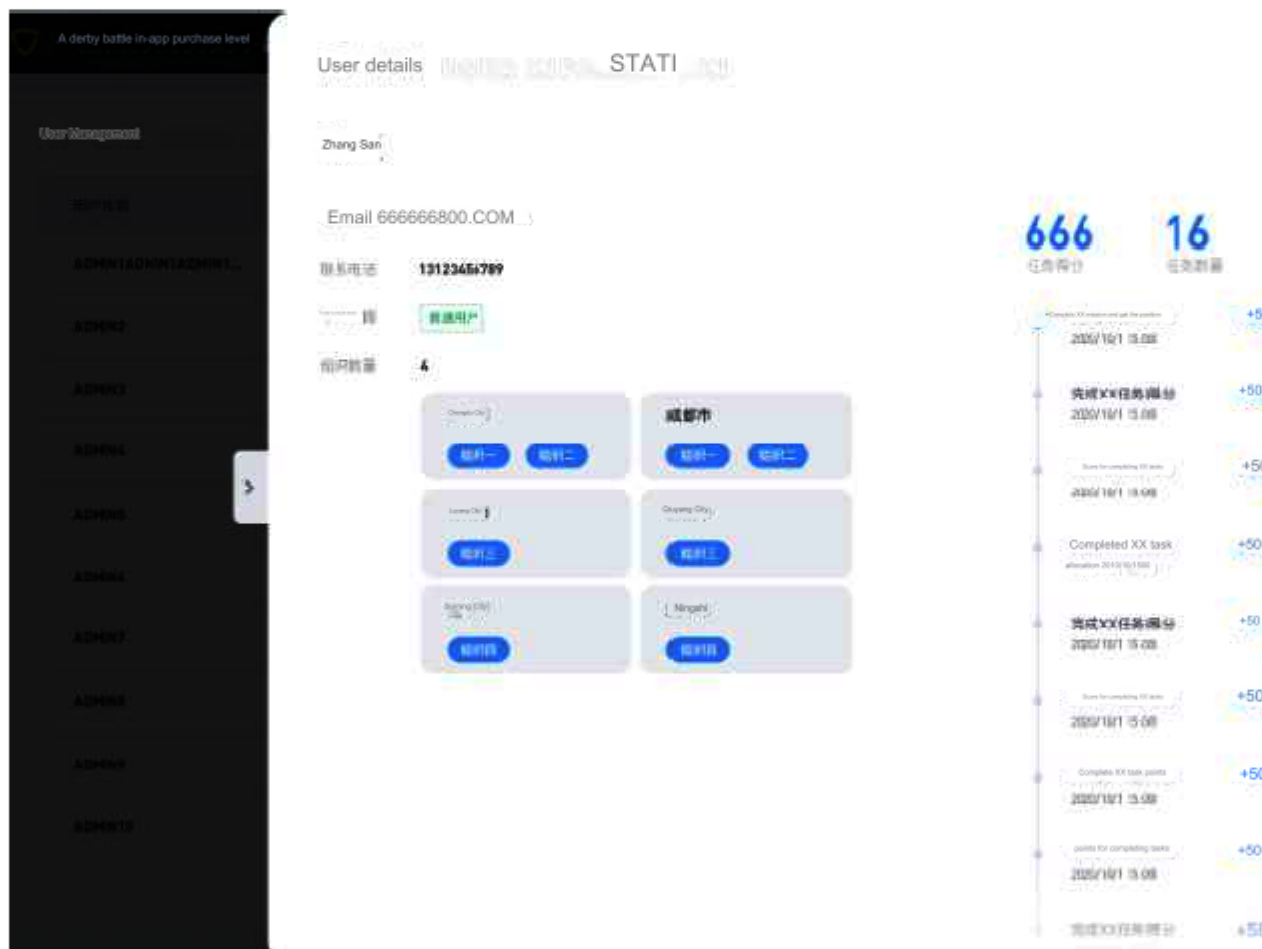
选择三

Create user

(Created by user)



(Permission allocation)



(personnel details)

4) Points management function: Provides assessment points records for each task. Each task will be set with different scores according to the difficulty of the task.

The background can conduct comprehensive evaluation and scoring based on task completion, completion efficiency, data results, etc. Points can be used in business

scenarios such as performance appraisal. Statistics and analysis of the tasks completed by the organization and personnel are carried out from two different dimensions,

showing managers the tasks completed by the organization and personnel and the areas they are good at, and use this as a data basis for managers to

consider performance. Organizational assessment is a statistical assessment of the completion of tasks by the superior organization on the subordinate organization. Select

the organization, start time, and end time, and the system will display statistical information on the organization's task completion within the selected time period.

The interest and time period (in months) can be selected independently according to needs. Statistical information includes the total number of tasks, the number of

completed tasks, task score distribution, etc., and the task score distribution displays the number and proportion of tasks in each score segment in the form of a chart.



5) Techniques and tactics sharing function: used to exchange and share information such as internal experiences, techniques and tactics within the private

network, as well as to acquire and learn cutting-edge technological knowledge. The knowledge management module supports multiple different dimensional

content sources, namely: sharing among group members, latest content push, result review analysis, etc. The knowledge management module is similar to building

a BBS forum for communication on a private network. Users can post freely and view all shared posts.

a) Users need to fill in the post content and set attributes when posting. Set the post type (including knowledge items, bookmarks,

discussion/study meetings, simple PPT, etc.); enter the title, edit the content, upload attachments (size limit 10MB), and

preview the post instantly. You also need to select the visibility range: private (visible only to yourself), public, protected (select

the visible range); set labels; select editable objects. When all content is completed, click Publish and the post can be

shared successfully.

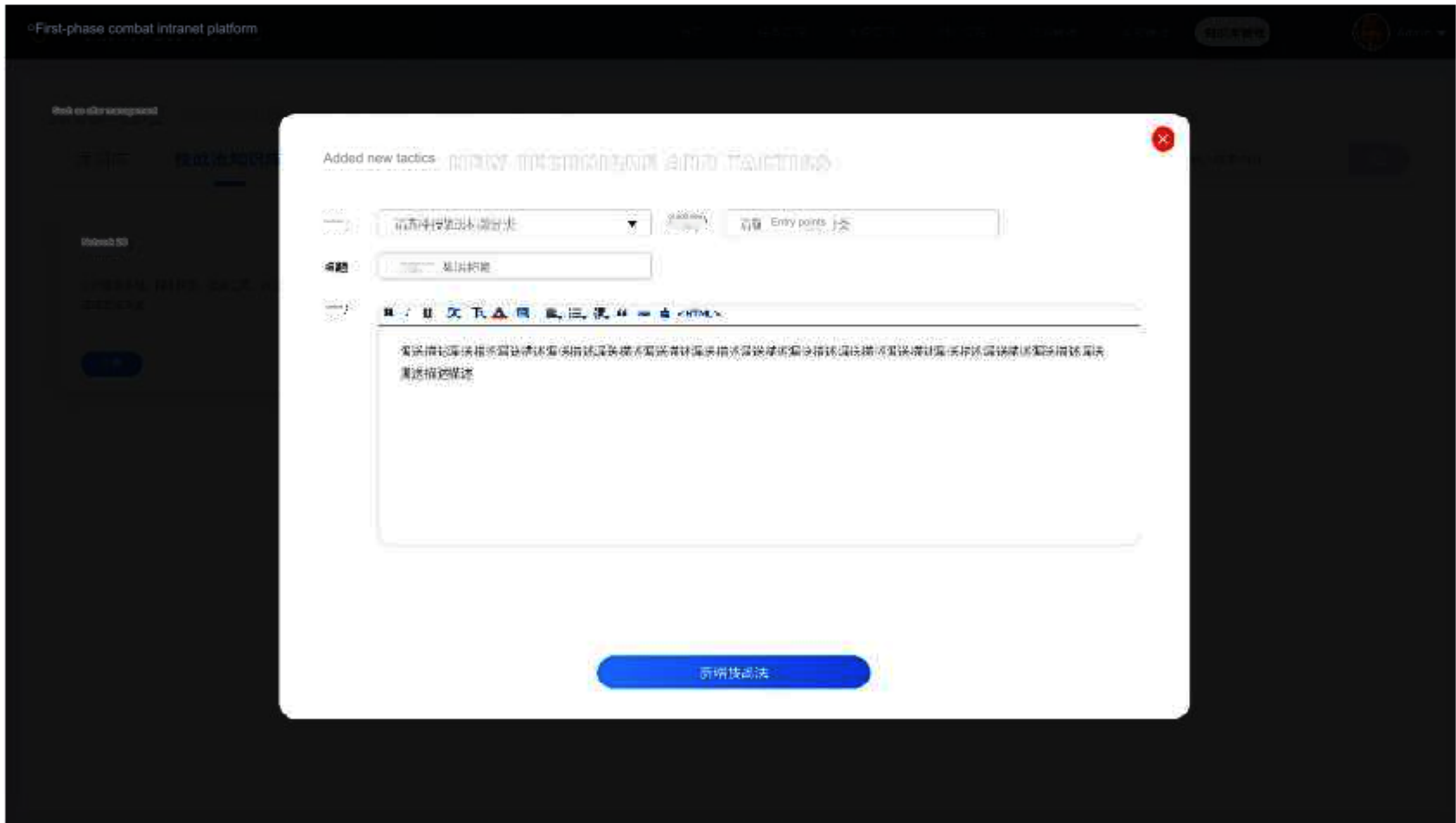
b) Users can see a list of posts shared by all people. The list display includes the post's title, publisher, editing

time, type, public scope, and the number of collections, likes, and replies; click Collection, Like, reply can

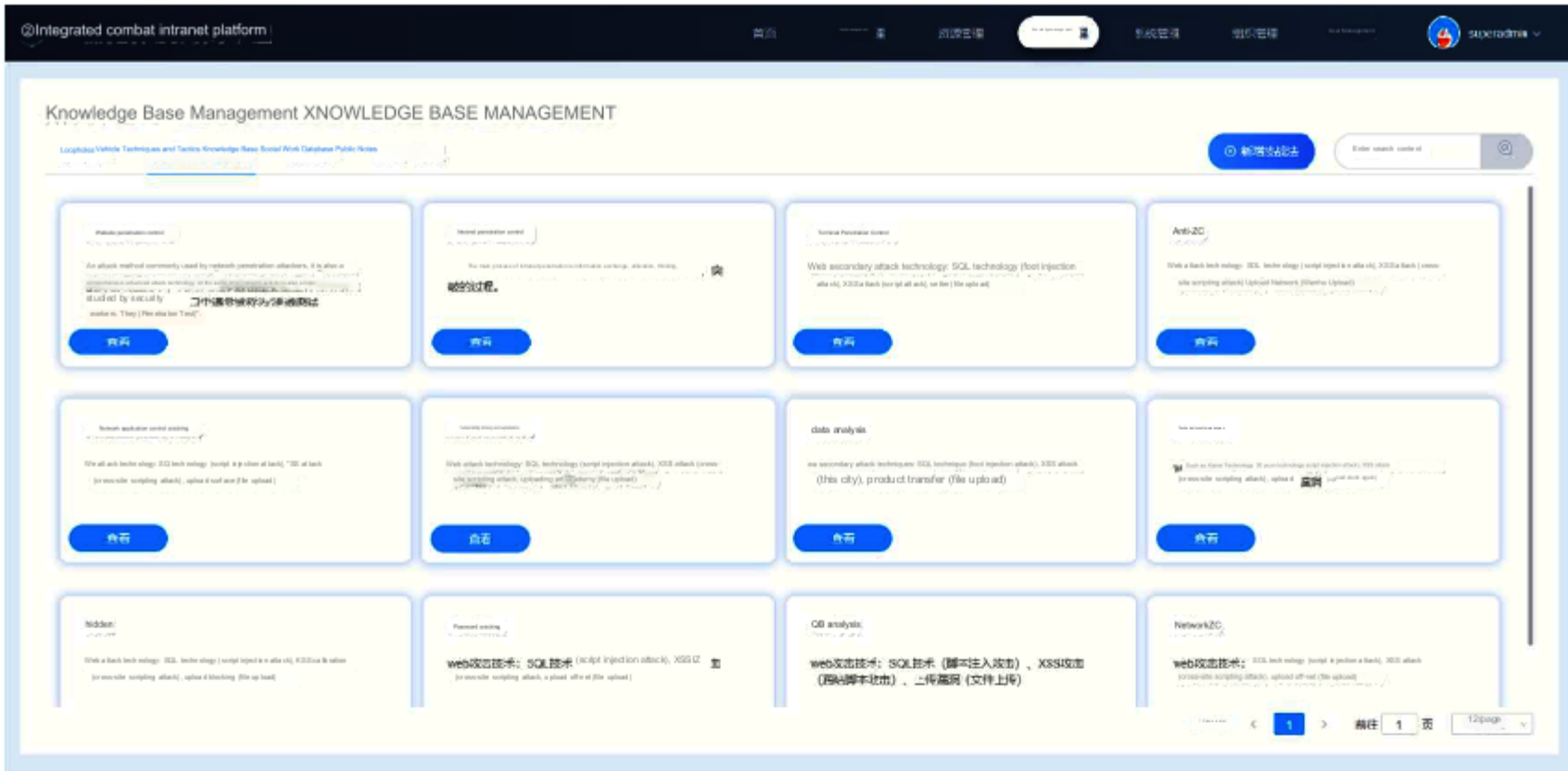
See a list of related people. Click on the title of the post to enter the detailed information interface of the post. You can see the complete content of the post, and you can reply to, favorite, and like the post. At the same time, the system will display the popularity of the article based on the click-through rate and so on.

c) Users can view posts of a certain type by filtering post types, and can also query posts published on a single day.

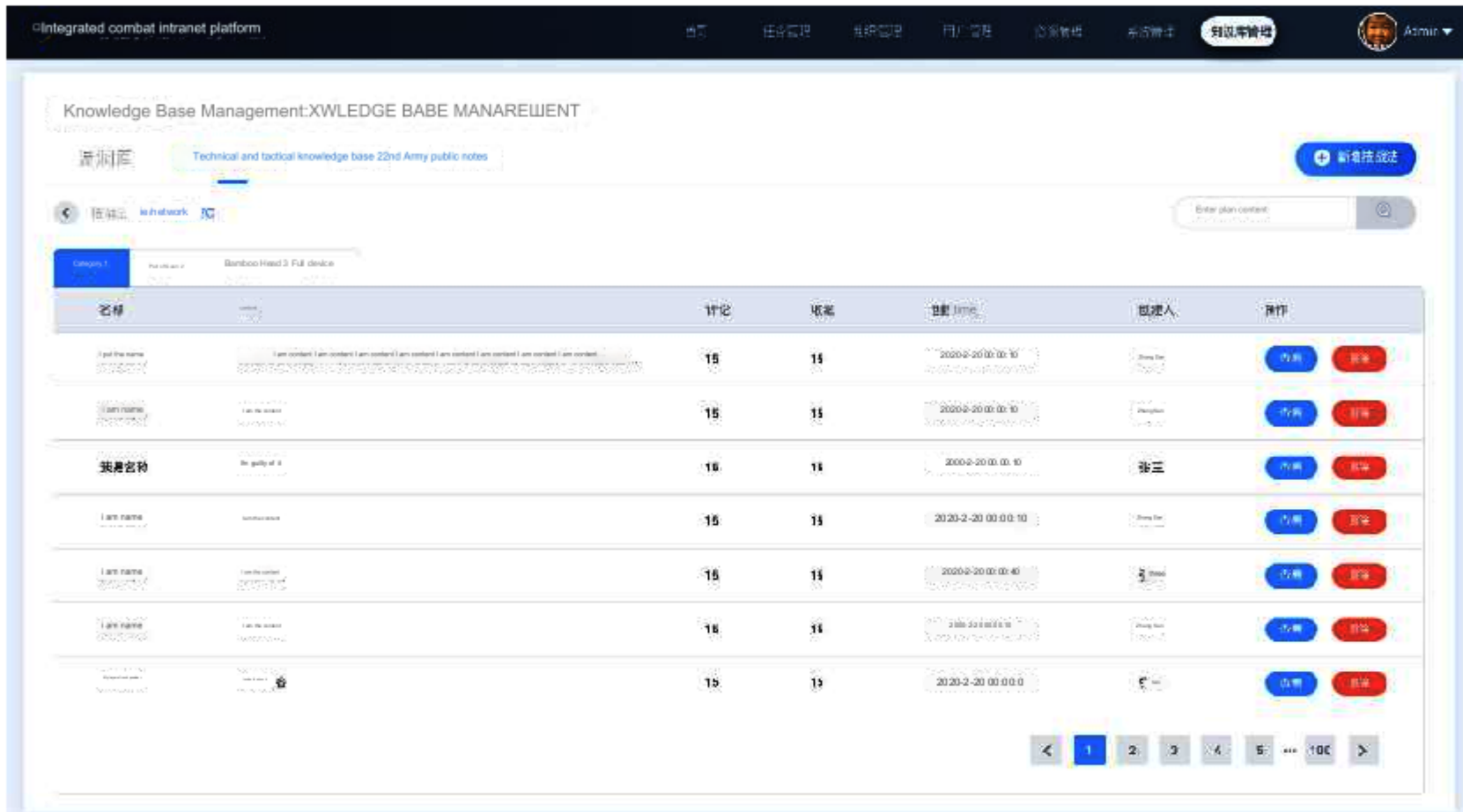
d) The sharing content of the knowledge management module can be the use of special technologies and tools, the sharing of practical cases, solutions to difficult problems or requests for help, etc. The establishment of the knowledge management module enables the ordering, digitization, and codification of technical information, technical means, and technical experience mastered by personnel within the organization, which is conducive to strengthening knowledge exchange and sharing, conducive to realizing collaboration and communication within the organization, and also helping It improves the professional skills of internal staff and provides good training materials for new employee training. The technical skills and technical experience shared by people within the organization can also be used as a supplement to performance appraisal.



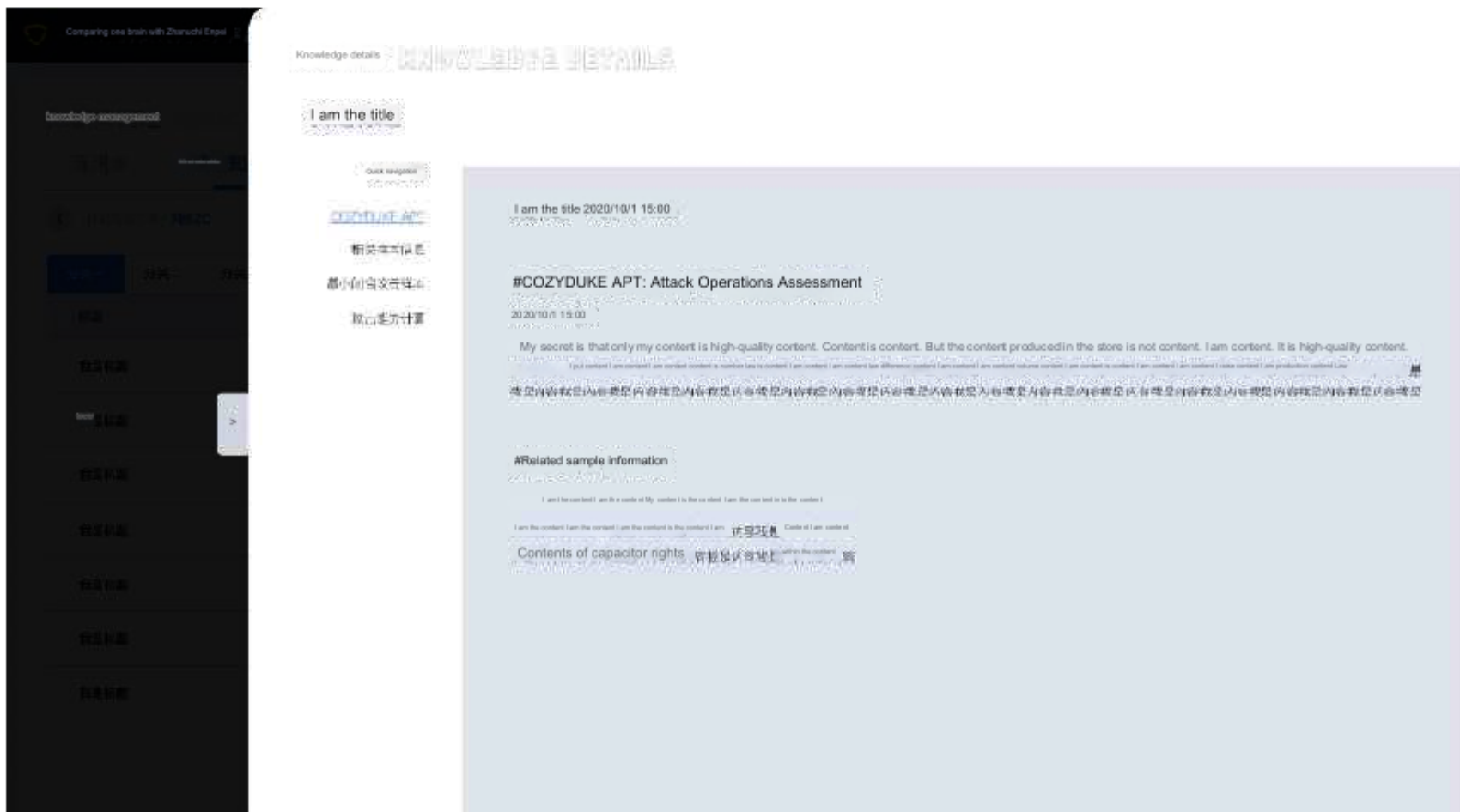
(Added new techniques and tactics)



(List of techniques and tactics)

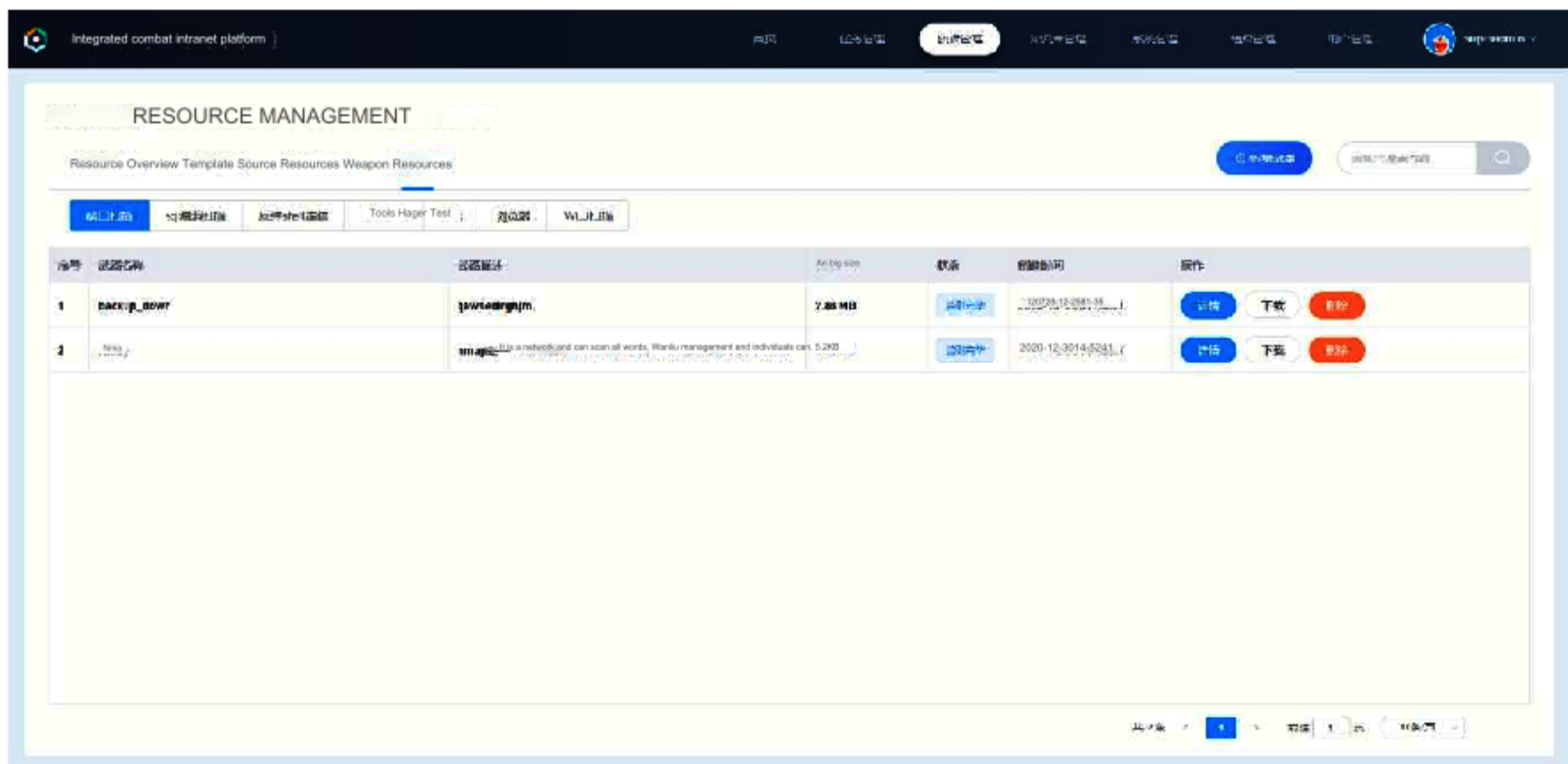


(View by category)



(View details)

- 6) Task statistics function: It is mainly divided into two parts: the first part is to count tasks in different states, tasks at different times, task completion status and distribution of task types from the perspective of tasks; the second part is based on resources. Make statistics and analyze the distribution and usage of overall resources from the perspective of utilization.
- 7) Log management function: The log management function is only visible to administrators. They can view global operation logs, which are divided into two parts: conditional retrieval and content display. In the conditional search section, the operation logs can be filtered by operation time, content keywords, and operation type. In the content display section, the retrieved log content is displayed.
- a) The conditional retrieval part supports date retrieval, time retrieval, log content retrieval, and type retrieval. At the same time, it also supports multiple combinations of search conditions to filter logs more accurately.
 - b) Date retrieval - users can specify a specific start time and end time, and query all operation logs within that time period;
 - c) Time retrieval - users can query all operation logs in the last hour, last six hours, last day, last three days, and last week;
 - d) Log content retrieval - users can enter log content through the search box to perform precise or fuzzy matching on all operations and find all relevant operation records;
 - e) Type search - users can filter a certain type of operation, including new, update, query, delete, download, upload, review/approval, application, transfer, etc.
 - f) The content display part displays the retrieved results in the form of a list. The results include operation time, operator and operation content.
 - g) Without any retrieval operation, the system will display all types of logs in the last hour by default, and sort them in reverse chronological order. When the search conditions change, the corresponding search content is displayed.



(Weapon resources)

4.1.3 Security sandbox module

The security sandbox module mainly performs security detection on any files, data, programs, etc. that enter the intranet. Through the sandbox environment, it simulates the viewing and running functions of various provided data to detect the presence of viruses and malicious programs, and other high-risk data files. It mainly provides six functions: file import analysis, API detection, behavior analysis, process mirror analysis, PACP packet capture analysis, and malicious behavior screenshots.

- 1) File import analysis function: supports analysis of multiple file formats, including windows executable files, DLL files, PDF documents, Office documents, malicious URLs, HTML files, PHP files, CPL files, VBS, ZIP compressed files, jar files, python programs etc.
- 2) API detection function: It can track the win32 API call records of the malware process and all the processes it generates, and provide early warning or record of malicious API behavioral calls.
- 3) Behavior analysis function: After the files to be detected are imported for analysis, the software's file creation, deletion, and download behaviors can be detected and recorded, so as to understand and understand whether the software's behavior complies with regulations and safety regulations.
- 4) Process image analysis function: The imported file program memory can be mirrored 1:1 to obtain a complete version of the memory image of the software process for thorough analysis and comparison.
- 5) PACP packet capture analysis function: After the imported file is executed in the sandbox environment, if network traffic is generated, it can be captured through PACP

Format grab file program's network data for analysis, comparison and security testing.

- 6) Malicious behavior screenshot function: If the imported file is found to have malicious behavior in the file, such as file copying, file name modification and other malicious behaviors, screenshots will be recorded.

4.1.4 Weapon resource management module

The weapons and equipment module is deployed on the external network platform, but the module is independent from other modules and provides a multi-login authentication mechanism to download and use weapons and equipment. The entire module provides weapon sandbox security detection functions, weapons library management functions, and weapons library update functions.

4.1.4.1 Weapon sandbox security detection function

It mainly provides various types of weapons that need to be built into the external network platform, provides a sandbox environment for security testing and inspection, and detects that all types of weapons and equipment imported to the platform meet safety requirements and usage requirements. The weapon sandbox security detection function also mainly provides program import analysis and API analysis. It has six major functions: detection, behavior analysis, process image analysis, PACP packet capture analysis, and malicious behavior screenshots.

- 1) Program import analysis function: supports analysis of multiple file formats, including windows executable files, DLL files, PDF documents, Office documents, malicious URLs, HTML files, PHP files, CPL files, VBS, ZIP compressed files, jar files, python programs, etc.
- 2) API detection function: It can track the win32 API call records of the malware process and all the processes it generates, and provide early warning or record of malicious API behavioral calls.
- 3) Behavior analysis function: After the files to be detected are imported for analysis, the software's file creation, deletion, and download behaviors can be detected and recorded, so as to understand and understand whether the software's behavior complies with regulations and safety regulations.
- 4) Process image analysis function: The imported file program memory can be mirrored 1:1 to obtain a complete version of the memory image of the software process for thorough analysis and comparison.
- 5) PACP packet capture analysis function: After the imported file is executed in the sandbox environment, if network traffic is generated, the network data of the file program can be captured through PACP format for analysis, comparison and security detection.
- 6) Malicious behavior screenshot function: If the imported file is found to have malicious behavior, such as file copying, the file

Take screenshots and record various malicious behaviors such as name modification:

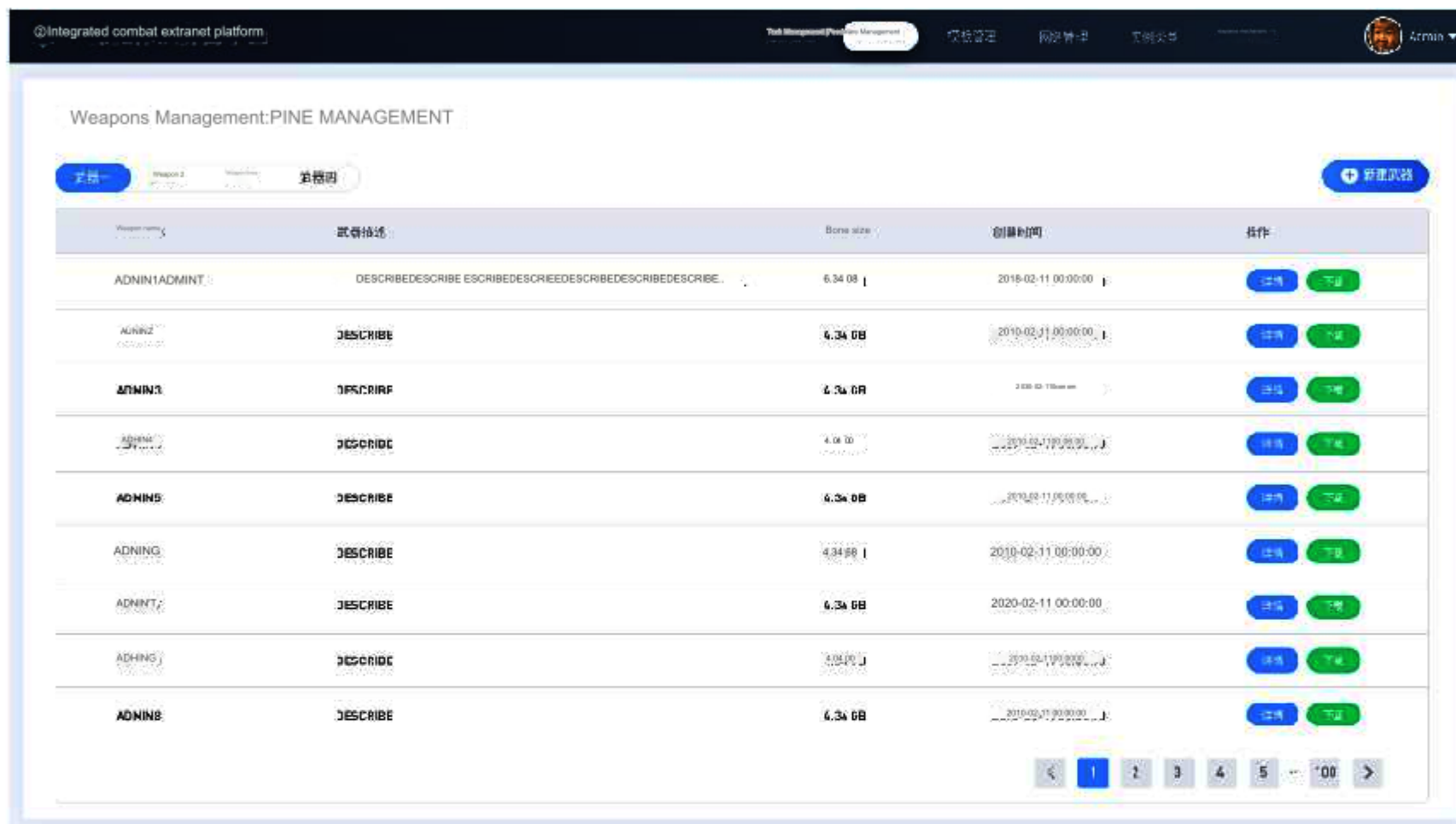
4.1.4.2 Weapon management function

The weapons library management function mainly includes comprehensive management and maintenance applications of various weapons resources on the external network, and mainly provides

five major functions: weapon storage management, weapon storage management, weapon information annotation, weapon classification encrypted storage, and weapon download log recording. Through standardized

management of weapons depots, we ensure the legal and compliant use of weapons.

1) Weapons storage management function: The weapons storage management platform provides basic functions such as weapons storage, retrieval, and display.



The screenshot shows a web interface titled "Weapons Management: PINE MANAGEMENT". It features a table with columns for "Weapon name", "Weapon description", "Bore size", "Creation time", and "Action". The table contains 10 rows of data, each representing a different weapon model (e.g., ADMIN1, ADMIN2, etc.). Each row has a "Creation time" and a "Bore size". The "Action" column contains two buttons: "Edit" (in blue) and "Delete" (in green). The interface also includes a search bar at the top and a pagination control at the bottom.

Weapon name	Weapon description	Bore size	Creation time	Action
ADMIN1	ADMIN1	6.34 08	2018-02-11 00:00:00	[Edit] [Delete]
ADMIN2	ADMIN2	6.34 08	2018-02-11 00:00:00	[Edit] [Delete]
ADMIN3	ADMIN3	6.34 08	2018-02-11 00:00:00	[Edit] [Delete]
ADMIN4	ADMIN4	6.34 08	2018-02-11 00:00:00	[Edit] [Delete]
ADMIN5	ADMIN5	6.34 08	2018-02-11 00:00:00	[Edit] [Delete]
ADMIN6	ADMIN6	6.34 08	2018-02-11 00:00:00	[Edit] [Delete]
ADMIN7	ADMIN7	6.34 08	2018-02-11 00:00:00	[Edit] [Delete]
ADMIN8	ADMIN8	6.34 08	2018-02-11 00:00:00	[Edit] [Delete]
ADMIN9	ADMIN9	6.34 08	2018-02-11 00:00:00	[Edit] [Delete]
ADMIN10	ADMIN10	6.34 08	2018-02-11 00:00:00	[Edit] [Delete]

(Weapon management list)

2) Weapon storage management function: Weapons from each manufacturer and related documents such as instructions for use are stored in the weapons depot, and corresponding

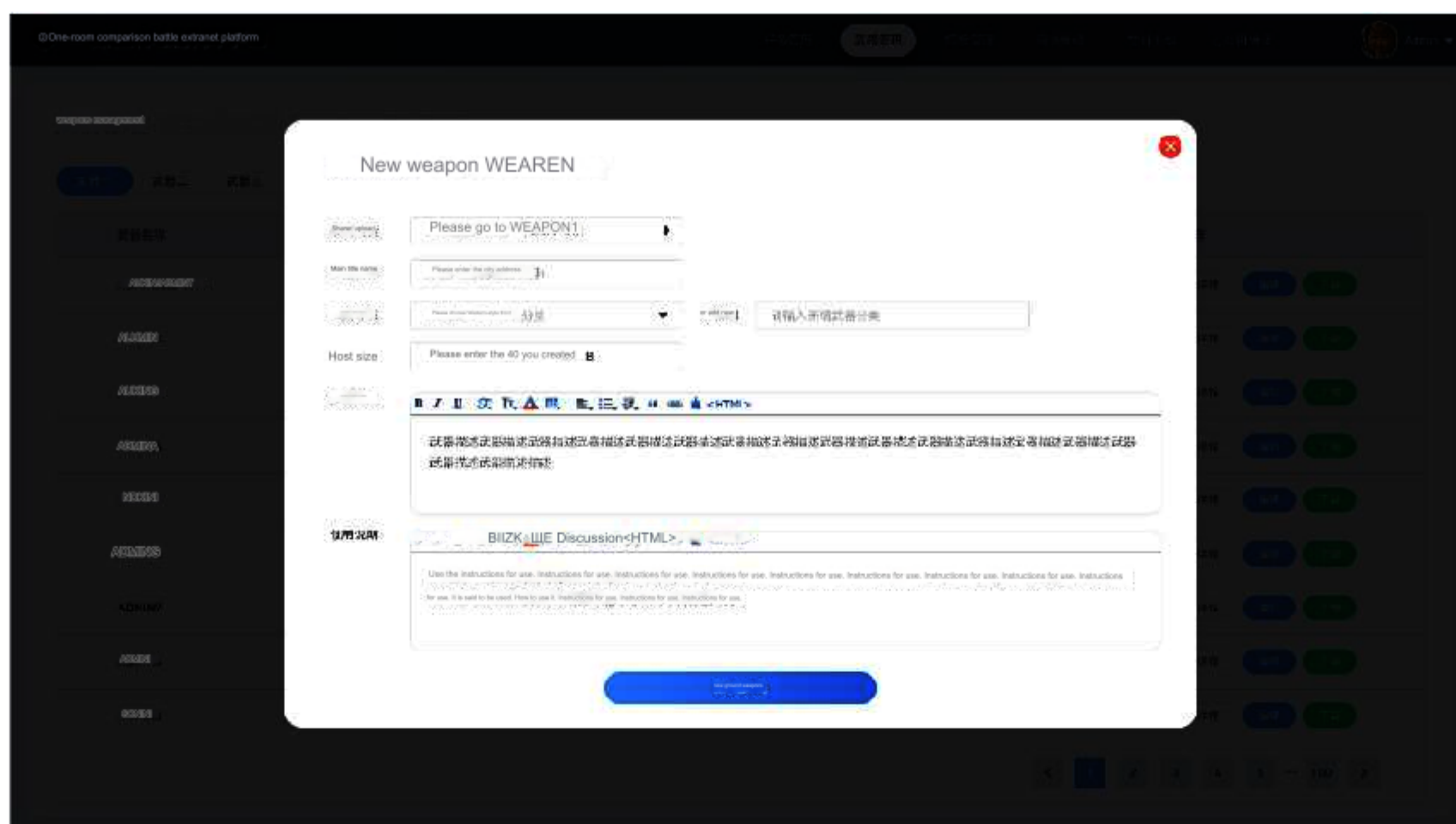
records are generated on the weapons depot management platform.

3) Weapon information annotation function: Weapon maintainers can search according to manufacturer, weapon category, name, etc. on the weapons library management

platform. The weapon library list displays information such as the category, manufacturer, version, rating, authorization expiration time, USB Key port, and whether

the weapons in the current weapons library have expired.

The latest version number, update time and other information of the server update.



(Weapons added and updated)

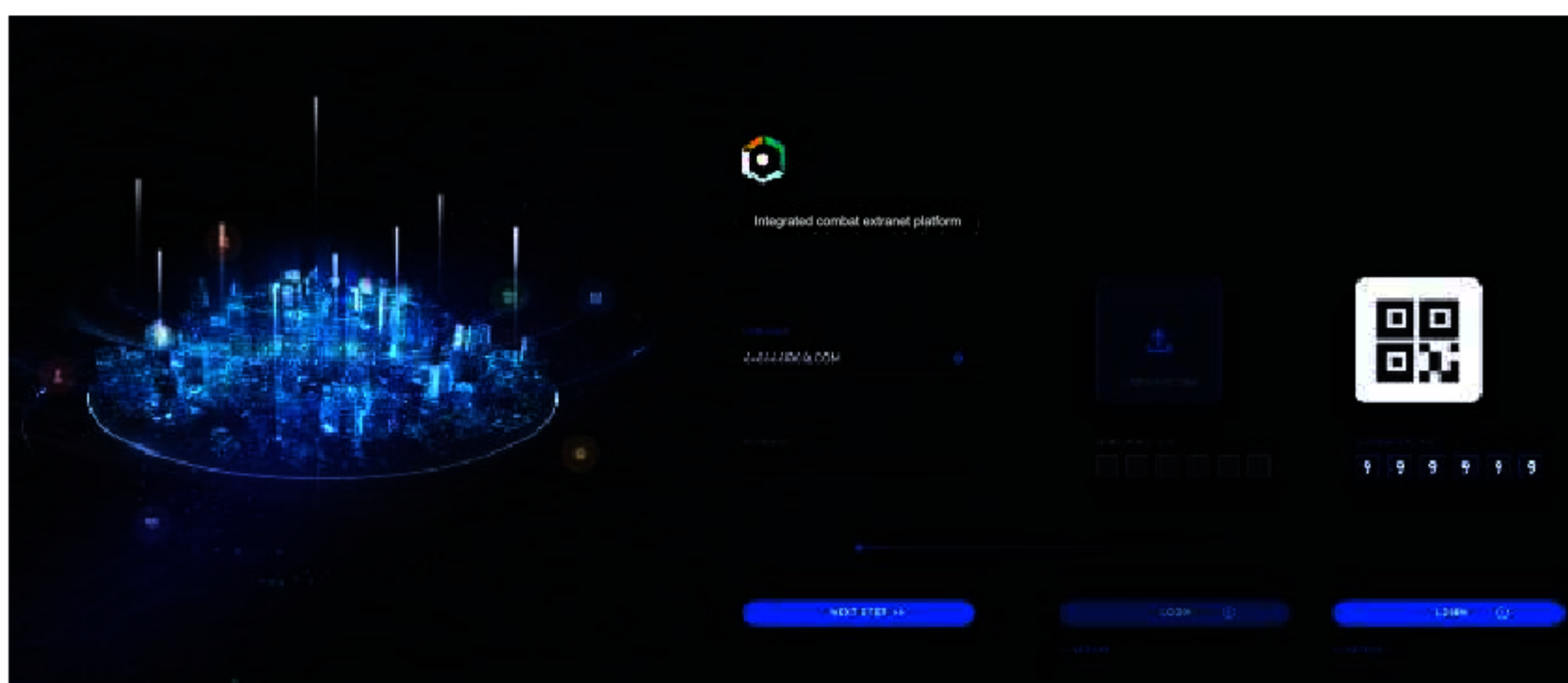
Weapon updates are generally performed during non-working hours or system idle time. Weapons already loaded in the mission cloud host will not be

replaced and updated.

4.2 External network platform functions

The function of the external network platform mainly consists of four parts: the external network task management module, the weapon resource management module, the link resource application module

and the combat environment management module.



(External platform login)

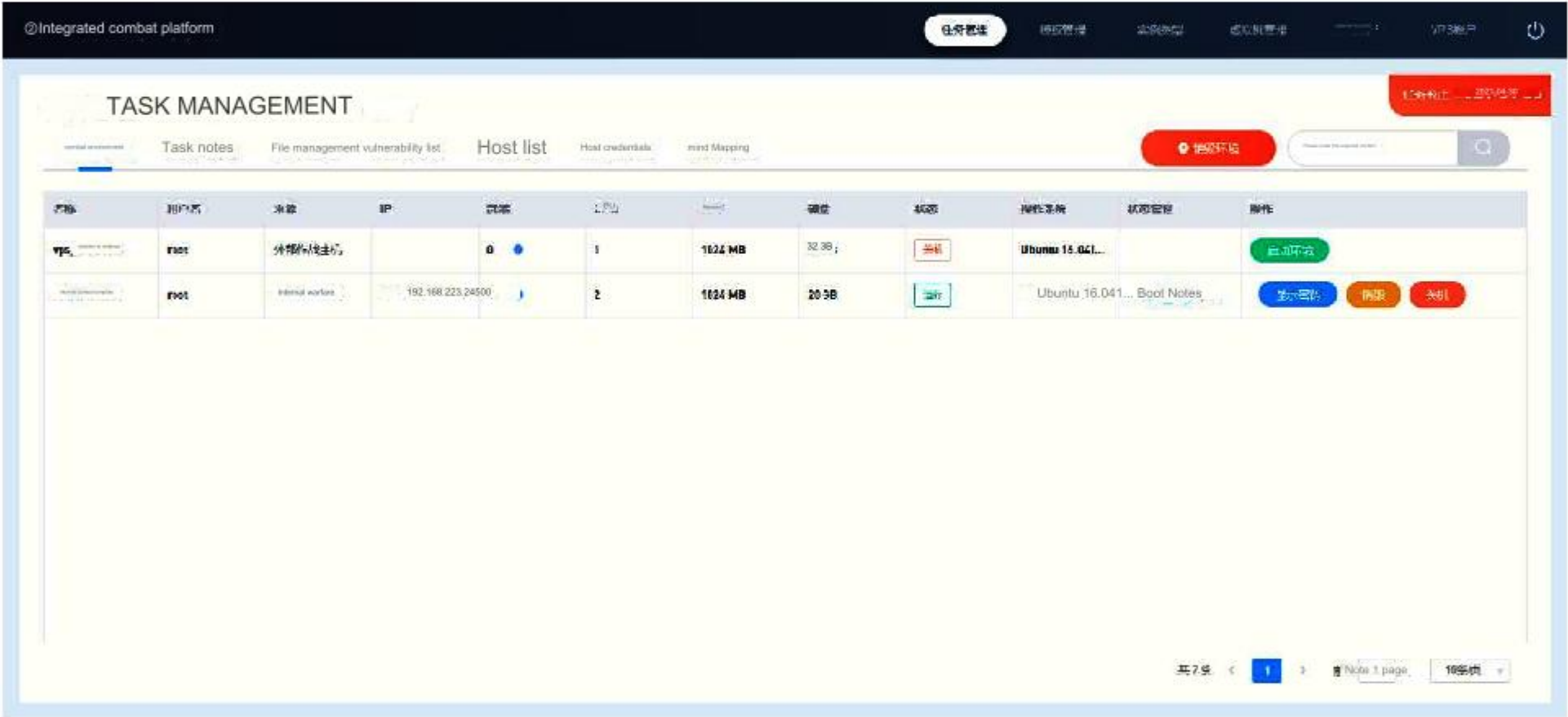
4.2.1 External network task management module

The external network task management component displays the task list that the current user has created, supports the decryption of task QR codes generated by the private network, and can generate task cloud hosts based on the decrypted task information. The task list includes the task name, the status of the enabled task cloud host, and the task time limit. Each task generates up to three task cloud hosts.

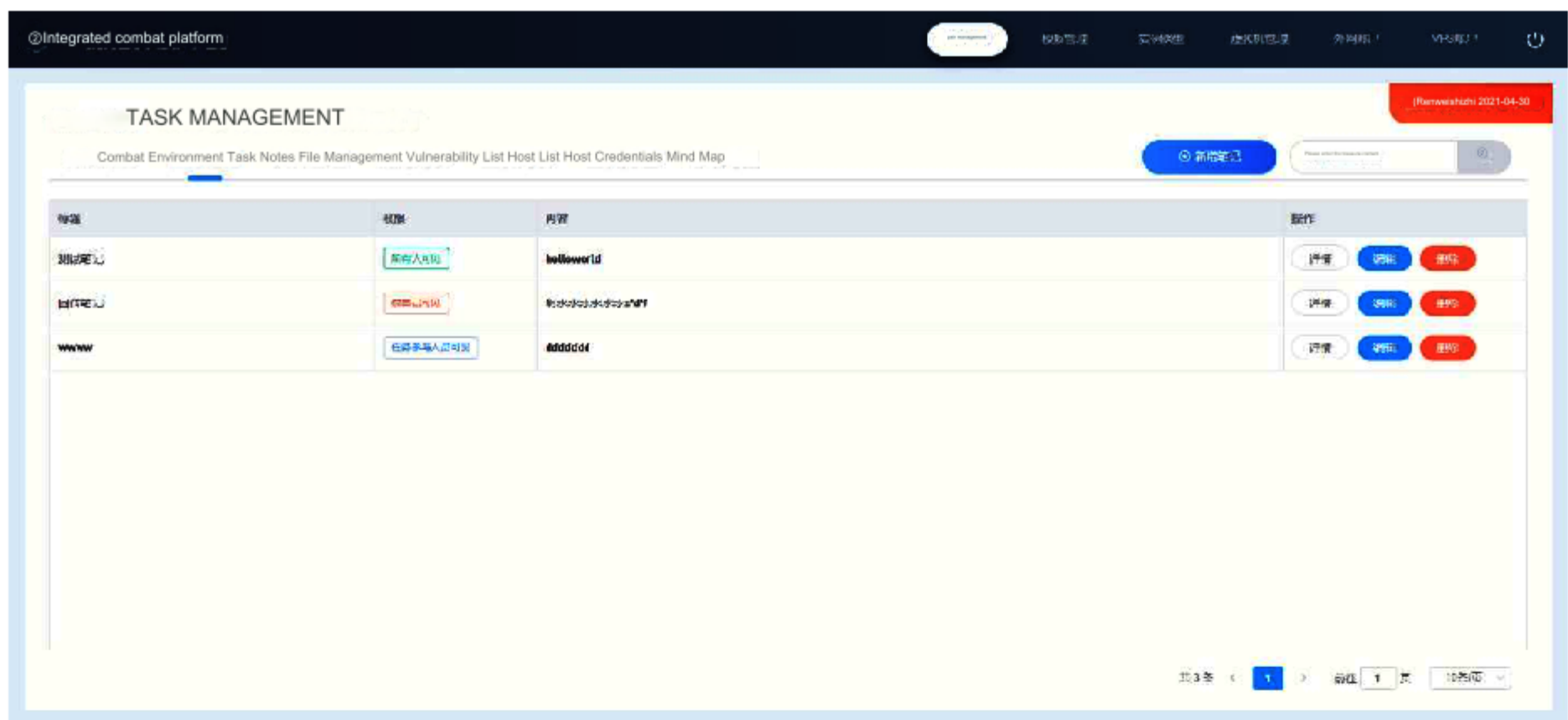
After selecting the corresponding task, you can create a task cloud host or view the details of the generated cloud host. In the cloud host details, you can view the resource configuration of each cloud host (including CPU, memory, hard disk, operating system, IP, language, time zone , installed software, installed weapons, etc.).

Users can perform the following operations on the task cloud host: power on, soft shutdown, power off, forced restart, release the cloud host, change password, modify configuration, remote access, etc. Changing the password and modifying the configuration requires the use of the personnel login QR code for secondary identity

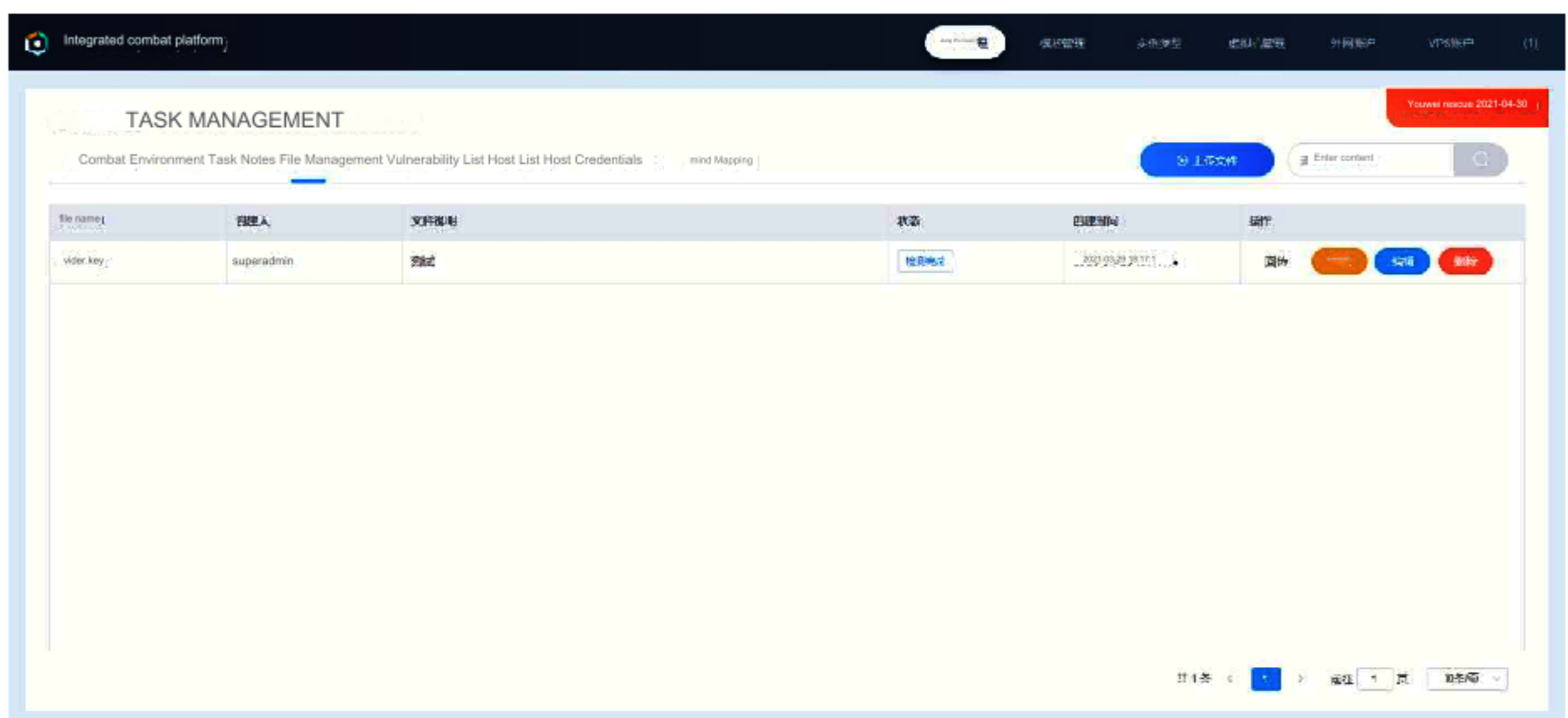
verification.



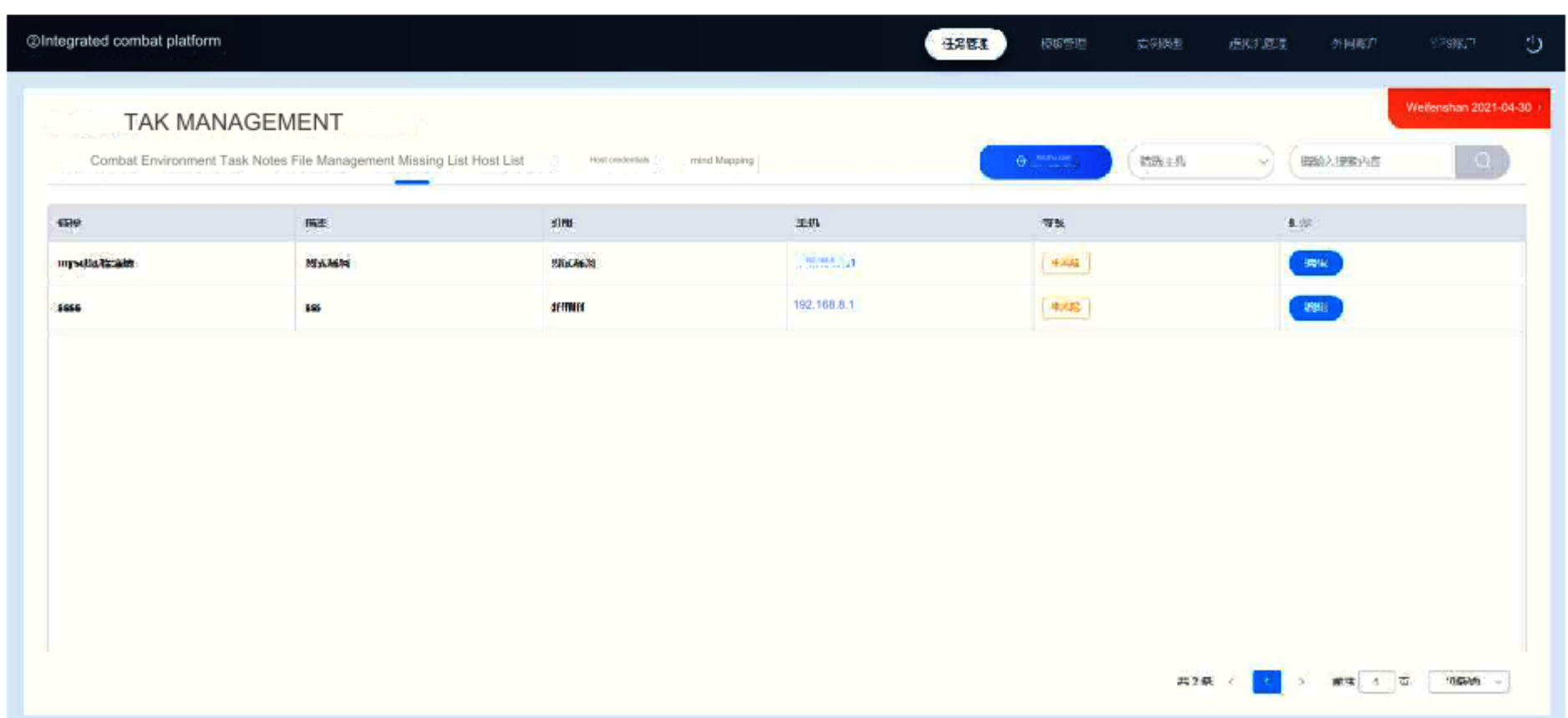
(combat environment)



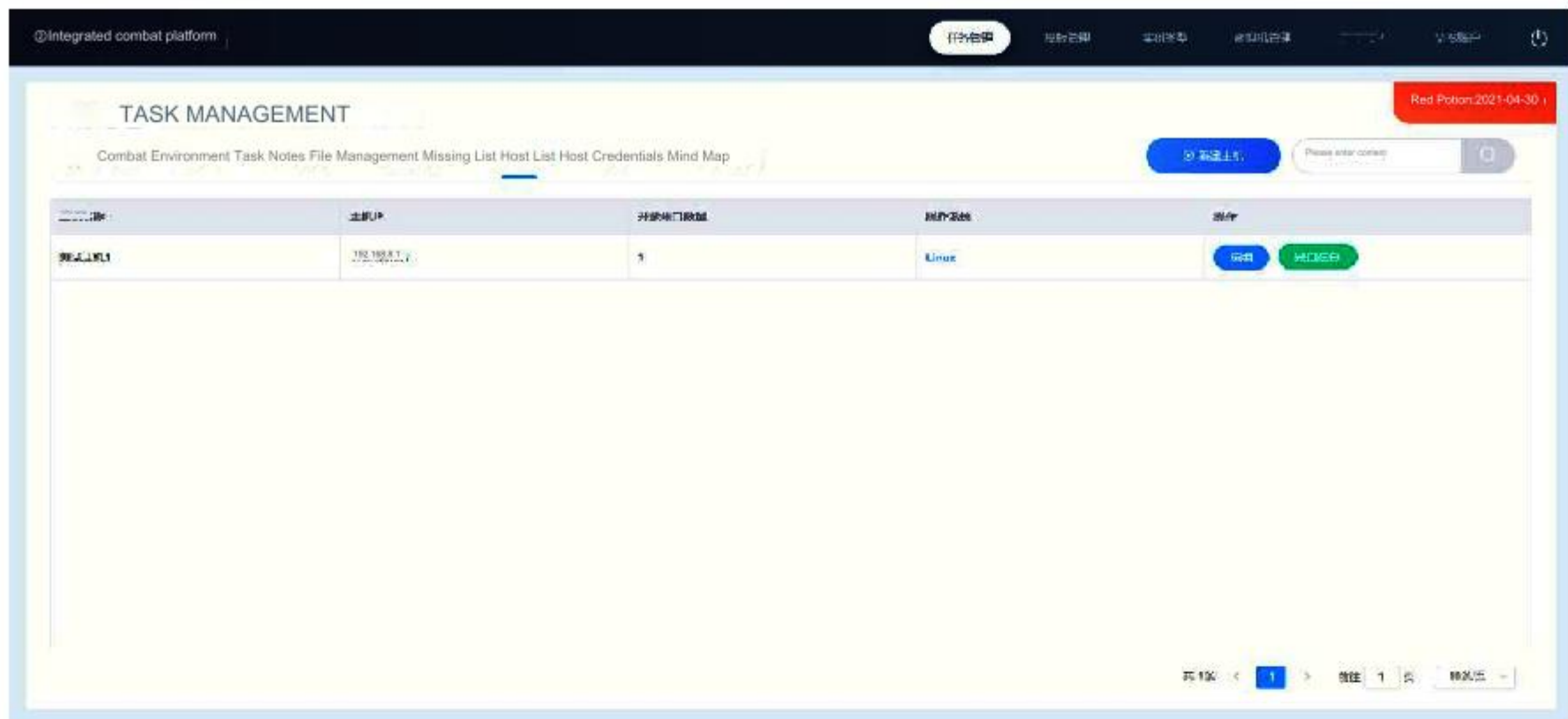
(Task notes)



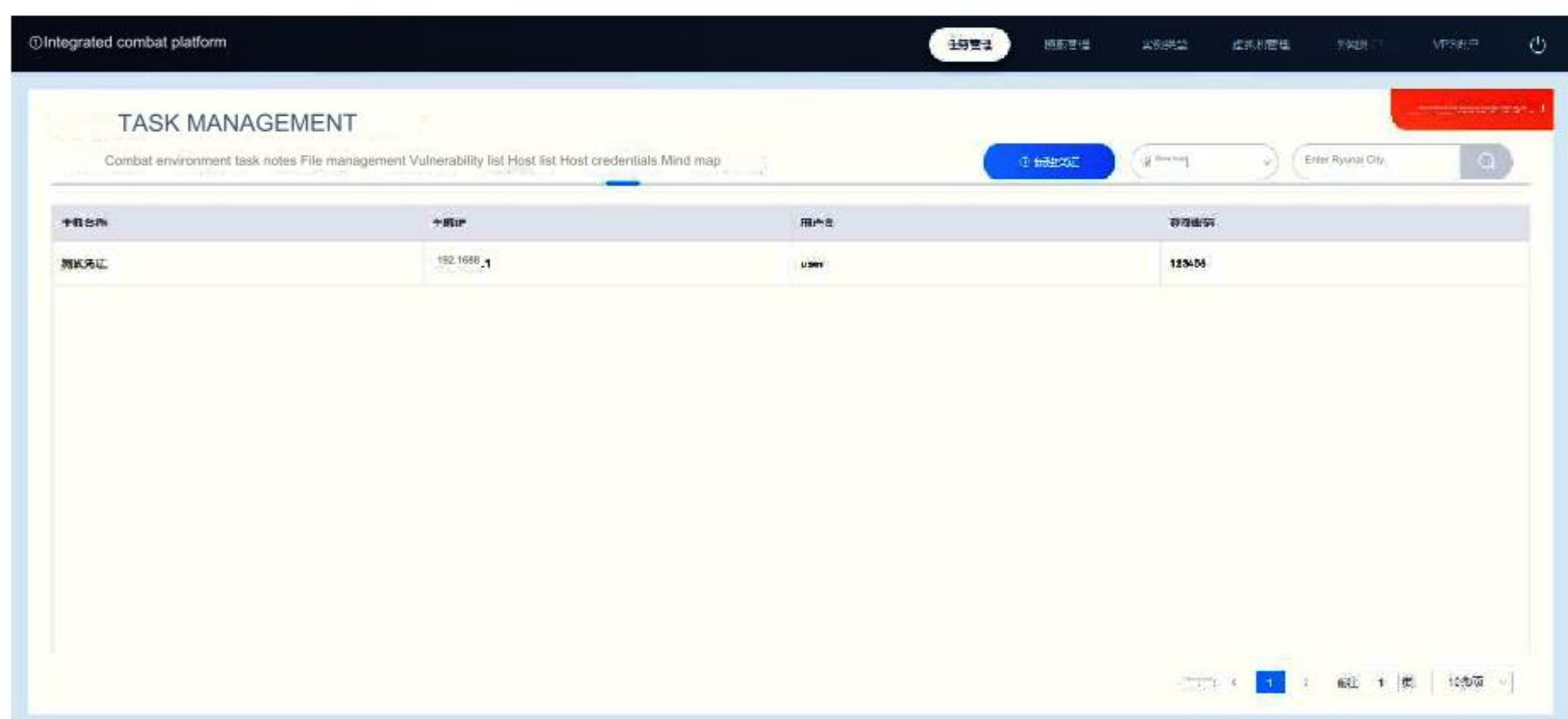
(File management)



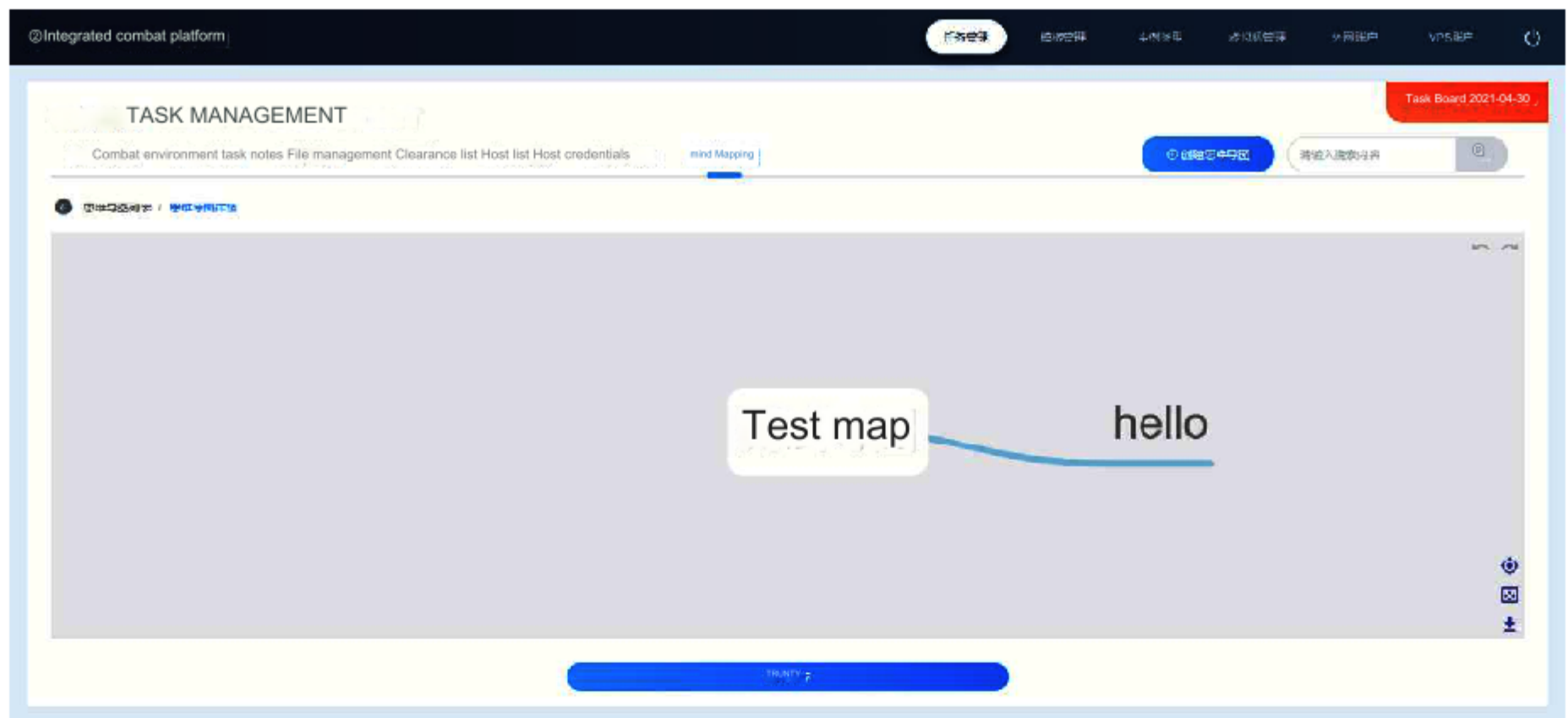
(vulnerability list)



(host list)



(host credentials)



(mind Mapping)

4.2.2 Combat environment management module

The combat environment management module mainly provides cloud host management functions, template management functions, data return functions, task note functions,

and terminal access functions.

4.2.2.1 Cloud host management function

1) Task cloud host function: Task cloud host needs to be created in an established task. New tasks require a valid task QR code and scan for authentication.

The way to verify the task QR code here is the same as logging in to the external application cloud platform, and multiple verification methods are supported:

a) Manual input: Obtain the login verification code through the mobile APP (the verification code is valid within 60S and can only be used once), implement verification

code authentication, and then log in to the platform through auxiliary authentication with an additional security code.

b) Matching login: Scan the QR code for personnel login through the PC or mobile terminal camera, and then log in after identification and verification in

the background.

c) Key login: The key here refers to the picture file of the QR code for personnel login. The background will identify and verify the

key before logging in.

After the task is created, the user can set the parameters of the task cloud host according to actual needs. The configuration limit of the task cloud host

(number of CPU cores, memory size, hard disk size) and the weapons that can be installed are determined by the task information carried by the task QR code.

Users cannot use weapons beyond the scope set by the mission. Weapons that need to be installed in the mission cloud host can be installed directly from the weapons library platform, and the weapon installation source files are not landed on the mission cloud host. The operating system language and time zone settings are to protect the operator's true identity information. The IP selection system provides two options: public IP and private IP, which can be selected according to actual needs.

After the task cloud host is generated, the network where the task cloud host is located is automatically disconnected from the management network of the external application cloud platform to ensure the security and concealment of the management network. The external application cloud platform will not store any task-related information or task cloud host information, nor will any services be embedded in the task cloud host, ensuring the purity of the task cloud host and the security of the task.

Since the task is time-sensitive, the generated corresponding task cloud host is also time-sensitive, and its existence time is shorter than the task timeliness.

After the task timeliness is reached, the task cloud host is automatically destroyed; or after the task is completed, the task cloud host is actively released. After the task cloud host is destroyed, data cannot be recovered through hard disk recovery technology to ensure that task information, target information, and result data are

It is safe.

2) Temporary cloud host: Each user is allowed to create a temporary cloud host. The temporary cloud host will be automatically destroyed after 24 hours. The temporary cloud host does not support automatic installation of software.

Allowing the creation of temporary cloud hosts is a security precaution to prevent unrelated persons from logging into the external application cloud platform through some means and performing unwarranted operations. At the same time, it is also convenient for users to search for relevant information overseas. Users can set the parameters of the cloud host according to actual needs.

4.2.2.2 Template management function

Supports generating templates from configured cloud hosts so that you can directly use the templates to create cloud hosts when necessary. The generated template is not only visible to you, but can also be set to be open to other people in the organization.

