GTI
AI-Based Autonomous Security Protection System White Paper

Version:	V1.0.0
Deliverable Type	□ **Procedural Document** ☑ **Working Document**
Confidential Level	□ **Open to GTI Operator Members** □ **Open to GTI Partners** ☑ **Open to Public**
Working Group	**5G Technology and Product**
Task	**Research on AI-Based Autonomous Security Protection System**
Source members	CMCC, ZTE, HUAWEI, BUPT, QIANXIN
Support members	ZTE, HUAWEI, BUPT, QIANXIN
Editor	Jiake Chen (CMCC), Cancan Chen (CMCC), Jianyu Lin (CMCC), Huijuan Zhang (CMCC), Quanchao Liu (CMCC), Li Su (CMCC), Kai Yang (CMCC), Bangling Li (CMCC), Lei Cao (CMCC), Jing Gao (CMCC), Jiachen Zhang (CMCC), Chen Liang (CMCC), Peilin Liu (ZTE), Xiangjun Li (HUAWEI), Guoshun Nan (BUPT), Siyuan Qiao (QIANXIN)
Last Edit Date	（09-29-2024）
Approval Date	

Confidentiality: This document may contain information that is confidential and access to this document is restricted to the persons listed in the Confidential Level. This document may not be used, disclosed or reproduced, in whole or in part, without the prior written authorization of GTI, and those so authorized may only use this document for the purpose consistent with the authorization. GTI disclaims any liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

机密性:本文件可能包含机密信息，而对该文件的访问权限仅限于机密级别的人员。在未经GTI事先书面授权的情况下，本文件不得使用、披露或复制，或全部或部分复制，而授权人仅可将本文件用于与授权一致的目的。GTI对本文件所载资料的准确性、完整性或及时性不承担任何责任。本文件所载资料如有更改，恕不另行通知。

Document History

Date	Meeting #	Version #	Revision Contents

Table of Contents

1	References	4
2	Abbreviations	5
3	Overview	6
4	Challenges in Building an AASP System	8
5	Requirements for an AASP System	9
6	Reference AASP System	11
7	Security Application Scenarios of AASP System	17

1 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

[1] IMT, Research report of 6G Network Security vision technology

[2] IMT, 6G Overall Vision and Potential Key Technologies White Paper

[3] Su L, Zhuang X J, Du H T, et al. Built-in security framework research for 6G network. Sci Sin Inform, 2022, 52: 205–216, doi: 10.1360/SSI-2021-0257

[4] China Mobile Research Institute, 2030+ Technology Trend White Paper, 2020

2 Abbreviations

Abbreviation	**Explanation**
AI	Artificial Intelligence
RBAC	Role-Based Access Control
RCA	Root Cause Analysis
WAF	Web Application Firewall
DDoS	Distributed Denial of Service
AASP	AI-Based Autonomous Security Protection

3 Overview

In the future, the modes of network communication, the types of services carried, the objects served by the network, and the types of devices connected to the network will develop in a more diverse manner. This will make networks highly dynamic and complex, requiring greater flexibility, scalability, and agile responsiveness to demands, transforming them into autonomous networks with self-optimization, self-evolution, and self-growth capabilities. These network characteristics require security capabilities to be finely granulated, deployed elastically on demand, and dynamically adapted to network conditions, terminal environments, and business scenarios. This transformation renders traditional security management models ineffective in addressing the continuously emerging security challenges and network service demands.

In this context, network security also needs to evolve autonomously, constructing an efficient, self-learning, self-evolving, and trustworthy intelligent autonomous security system, which has become an urgent task. Future communication networks will support AI (Artificial Intelligence) applications. In network security governance, AI possesses excellent capabilities in automatic data feature mining and analysis, enabling precise identification of network threats, instant warnings, and rapid response. More importantly, through the self-learning and analyzing capabilities of AI, security capabilities can self-evolve, enhancing the intelligence of the autonomous security system. Therefore, leveraging AI can improve the flexibility, accuracy, and automation of security autonomy. Furthermore, since AI systems often need to process vast amounts of sensitive information and core business logic, any malicious attack on the AI system could trigger chain reactions such as data leaks, service interruptions, or even system crashes. Hence, strengthening the security protection of the AI system is equally indispensable.

To address the security challenges that will emerge in communication networks, this white paper is dedicated to exploring the challenges and opportunities in network security and proposes an AASP (AI-based autonomous security protection) system. This system aims to empower communication network security comprehensively with secure AI. Firstly, we will analyze the unique challenges faced by the AASP system in future communication network environments and extract the core requirements for system construction. Then, we will introduce the reference architecture and key functional modules of this system in detail. Finally, we will describe its detailed operation processes for different application scenarios.

This white paper aims to pave an innovative path in the field of next-generation communication network security protection, providing not only theoretical guidance for building network security but also laying the foundation for the deepening and expansion of AI technology in diversified application scenarios. We expect that, through the AASP system, a robust security barrier can be constructed for global communication networks, leading network security protection into a new era.

4 Challenges in Building an AASP System

The main challenges in designing an AASP system can be summarized as follows：

1.Challenges in Identifying and Confirming Security Risks

Accurate and effective network security protection requires a deep understanding of multiple layers of knowledge and relationships, including the network framework, system dynamics, and security vulnerabilities. The AI systems in network security heavily rely on data analysis and machine learning. Precisely capturing subtle changes in the network and extracting potential patterns and evolution trends of security threats from multi-layer data pose significant challenges to building the security system.

2.Dynamic Optimization of Security Policies and Stable Operation

In the face of ever-changing network security threats, AI systems need to have continuous learning and self-optimization capabilities to adapt to new threat landscapes promptly. Implementing online learning and updates of AI models without affecting the normal operation of the system is a major challenge. This requires the system to dynamically adjust model parameters while ensuring system stability and reliability.

3.Complexity of Resource Allocation and Management

With the rapid development of communication networks, the large number of devices and massive data volume make it challenging to efficiently and rationally allocate computing, storage, and network resources required for data analysis. Ensuring stable system operation and performance optimization, as well as invoking distributed security tools to quickly and fully respond to security needs, are important challenges.

5 Requirements for an AASP System

Building an AASP system aims to utilize advanced communication technologies and artificial intelligence to achieve self-detection, self-repair, and self-optimization capabilities for network systems to address increasingly complex network security threats. The design of this system needs to fully consider deep integration with the characteristics of communication networks and the security of the AI system. The main requirements for constructing a autonomous security protection system under this framework are as follows:

1.Integration and Complementation of Multi-Source Knowledge: Develop efficient data collection processes to gather massive heterogeneous business data from different scenarios. Integrate structured knowledge from knowledge graphs and existing open-domain knowledge of AI with expert knowledge to build advanced AI models for data analysis and correlation. This enables knowledge integration and complementation, discovering potential security threats within the network, thus creating more intelligent and precise security solutions.

2.Flexible Self-Evolution Mechanism: First, it needs to have automatic handling capabilities. When security risks are confirmed, it should automatically invoke security tools to promptly take response measures for remediation to restore the network's normal functionality. It also needs a channel to issue optimized configurations for security tool rules and policies, allowing administrators to customize the trigger conditions for optimization, such as optimization time and prerequisites. Through self-optimization and iteration, it continuously enhances its intelligence level, improving stability and reliability when facing complex and variable threats in communication networks.

3.Resource Orchestration: Through orchestrated scheduling, intelligently adjust resource allocation strategies based on business needs, operational status, and other factors. Allow customization of differentiated needs for different scenarios, achieving dynamic balancing of

computing resources, intelligent expansion of storage space, efficient allocation of network bandwidth, flexible scheduling of security tools, and efficient cross-layer and cross-domain resource scheduling and unified service. This intelligent resource management mechanism not only greatly improves resource utilization efficiency but also significantly enhances system stability and performance optimization capabilities.

4.Dynamic Configurability of AI Security Protection Solutions: First, introduce AI security tools and management mechanisms to provide basic guarantee for secure AI. Then, through monitoring and evaluation tools, promptly detect AI component update dynamics and execution status, automatically updating security configurations or administrator custom settings to ensure that security policies remain consistent with the latest state of the AI system and find the best combination of protection accuracy and business balance.

In summary, the design of an AI-based autonomous security system needs to consider the security issues of AI system as well as the need to fully reflect the various requirements of the AASP system under communication networks. Such a system architecture helps improve the overall level of network security, reduce security risks, and ensure the safe operation of critical infrastructure and important information systems.

6 Reference AASP System

6.1 Overview of AASP System

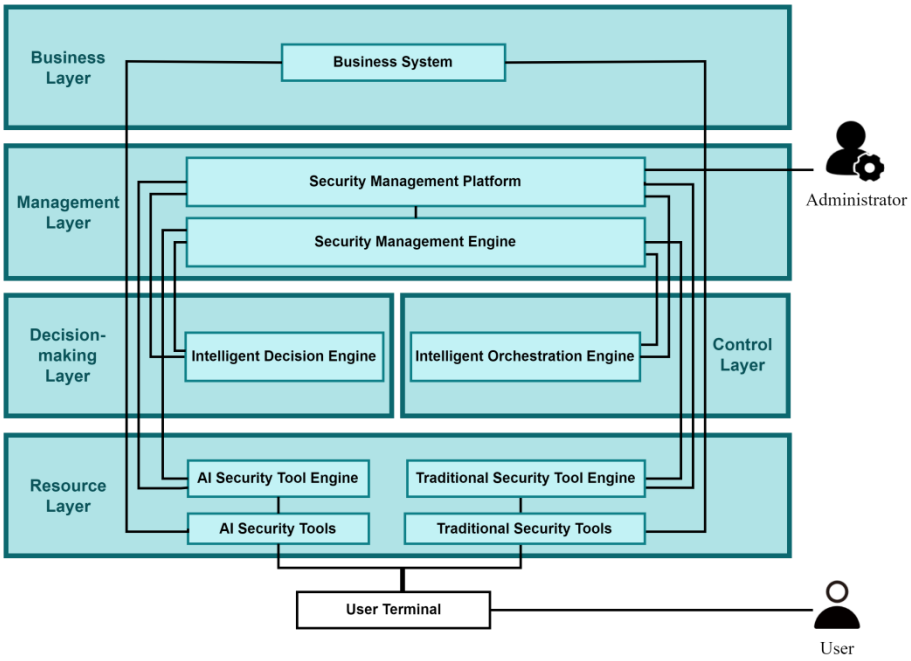

Figure 6-1 Overview of AASP System

1.Management Layer: Responsible for managing the modules, global data, and tasks within the system, including the security management engine and security management platform.

2.Decision Layer: Utilizes AI to perform comprehensive analysis of multi-source and cross-domain data to identify security events or protection deficiencies and make response decisions. This layer enables knowledge integration and application, as well as self-learning and evolution of the system. The decision layer includes intelligent decision engine.

3.Control Layer: Provides unified control over the resource layer based on resource orchestration and scheduling capabilities, enabling capability scheduling. It includes intelligent orchestration engine, which enables the orchestration of security resources.

4.Resource Layer: Provides security capabilities, as well as network traffic, logs, endpoint

status and other data to and under the control of the management layer. This layer includes AI security tools, traditional security tools and their respective tool engines. It realizes security protection for AI systems by integrating AI security tools.

5.Business Layer: Contains the customer's business platforms in the communication network that interface with and are protected by the security tools in the resource layer.

6.2 Components of the AASP System

6.2.1 Security Management Platform

The security management platform serves as the command center of the architecture, providing management interfaces for security personnel to unify the management of the engines and the security tools within the system. It covers every critical aspect from engine configuration to the response of security tools to security events, aiming to build an efficient, flexible, and adaptable security ecosystem. The security management platform needs to support at least the following functionalities:

1.Engine Configuration and Management: Provides integrated engine configuration management functions, such as setting protection rules, personalized security requirements, model operation status, data processing rules, and configuring the time constraints and order of security tool updates. This realizes in-depth customization of the security management engine, intelligent decision-making engine, intelligent orchestration engine, and security tool engine, ensuring that the security autonomy protection system can accurately respond to the specific needs of different scenarios and industry standards, which greatly improves the adaptability and flexibility of the system.

2.Security Service Management: Provides flexible methods to invoke security tools to meet different management needs, such as invoking security tools by configuring security policies,

sending invocation commands to security tools, and invoking security tools by entering natural language descriptions of requirements.

3.Dynamic Monitoring and Health Assessment System: Provides a dynamic monitoring and health assessment mechanism to collect real-time information on the operational status of each engine and security tool. This includes providing administrators with a centralized dashboard for quickly identifying, analyzing, sequencing, responding to, and recovering from security events, and alerting administrators of performance degradation, potential security vulnerabilities, or intrusion attempts to help them respond and deal with them quickly. These features ensure that incidents are handled in a timely and effective manner, minimizing potential losses and safeguarding the stability and security of the engine and tools.

6.2.2 Security Management Engine

The security management engine is responsible for data management, orchestration task management, and security tool management.

1.Data Management: Uses intelligent classification model to categorize the logs, reports, performance and other data of security tools, and generate knowledge graphs of security risks, threat events, etc. in order to get information such as event correlation data, whether risks have been repaired, and whether threat events have been disposed of, etc., so as to provide data support for subsequent security analysis.

2.Orchestration Task Management: Responsible for the decomposition and execution planning of orchestration tasks. It parses optimization plans generated by the security decision engine, translates them into specific, executable service scheduling task sequences, and then assigns these tasks to the intelligent orchestration engine for execution. This function ensures that security response strategies are implemented efficiently and accurately..

3.Security Tool Management: Manages the configuration and scheduling of security tools,

such as specifying the tool engine to which the security tool belongs, and forwarding the scheduling or configuration commands for the security tool to the tool engine to which it is deployed, and verifying and authorizing the application for the security tool's usage privileges by means of RBAC (role-based access control) capabilities.

6.2.3 Intelligent Decision Engine

The intelligent decision engine plays a crucial role in security protection capabilities by utilizing AI technology to convert natural language into machine instructions, identify potential security risks, perceive the overall network situation, recognize weak points in protection, and generate improvement plans.

1.Data Preprocessing: Automatically complete complex semantic mapping and data standardization, data combination and data vectorization of multi-source cross-domain data based on AI models and rule templates to ensure the high quality and consistency of the input data of the intelligent decision-making model, which is an important component to improve the performance and accuracy of the overall system.

2.Intelligent Decision Model Management: Responsible for the centralized management of intelligent decision models, including storage, optimization, and monitoring of the operation status of algorithms and models. These models are used to analyze multi-source and cross-domain data to provide accurate insight into security posture and potential threats, which is the key to achieving security autonomy.

3.AI Model Interface Protocol Adaptation: Converts AI model protocols based on an abstract and scalable protocol conversion mechanism to smoothly invoke the interfaces of various AI models. This not only improves the compatibility of the system with various AI models, but also reserves sufficient expansion space for the introduction and upgrade of future AI models.

4.Threat Event Intelligent Analysis: fuses and analyzes multi-source and cross-domain data

collected from security tools through intelligent decision-making models to provide accurate insights into security posture and potential threats, and to provide a basis for rapid response to security incidents. This is the key to realizing security autonomy.

6.2.4 Intelligent Orchestration Engine

The intelligent orchestration module serves as the commander for task execution. It designs and generates scheduling tasks based on AI and guides security tools to perform policy updates to ensure continuous optimization and dynamic adjustment of security defense measures, which meets the stringent requirements of security protection policies in terms of rapid response, precise execution and flexible configuration to cope with evolving security threats.

1.Security tool scheduling orchestration: Using data correlation and rule analysis capabilities of AI, it automatically generates a precise security tool task scheduling plan for each orchestration task based on the functionality match and performance applicability of the security tool, which includes but is not limited to the sequential arrangement of task execution and the setting of trigger conditions.

2. Rule and Configuration Generation: With the text generation technology of AI, customize security rules and configuration parameters for various security tools. This process enables self-optimization of security tools and enriches the functions of security autonomy.

6.2.5 AI Security Tool Engine

The AI security tool engine is focused on the scheduling of AI security tools, data transformation and interface adaptation, information merging, and redundancy handling, ensuring the efficient execution of AI security tools.

6.2.6 Traditional Security Tool Engine

The traditional security tool engine focuses on the scheduling of traditional security tools, data transformation and interface adaptation, information merging, and redundancy handling, ensuring the agility of responses and a high success rate in task execution for traditional security tools.

6.2.7 Business System

The business system encompasses the client's production business platform and the AI service platform oriented towards business operations. It is the direct manifestation of the security architecture serving actual business needs, aiming to ensure business continuity and data security.

7 Security Application Scenarios of AASP System

7.1 Autonomous Security Scenarios for Anomalous Access Detection

As communication networks progressively evolve towards service-oriented paradigm, they inevitably expose more surface areas while providing diverse services, thereby increasing higher security risks. The stability and security of the network are not only crucial for the normal operation of network communication services but also directly impact the overall reliability and safety of the entire communication system. Therefore, to effectively address the increasingly complex security threats, it is especially important to enhance the detection and protection capabilities against anomalous network access. The workflow of AASP system for anomalous access is as follows:

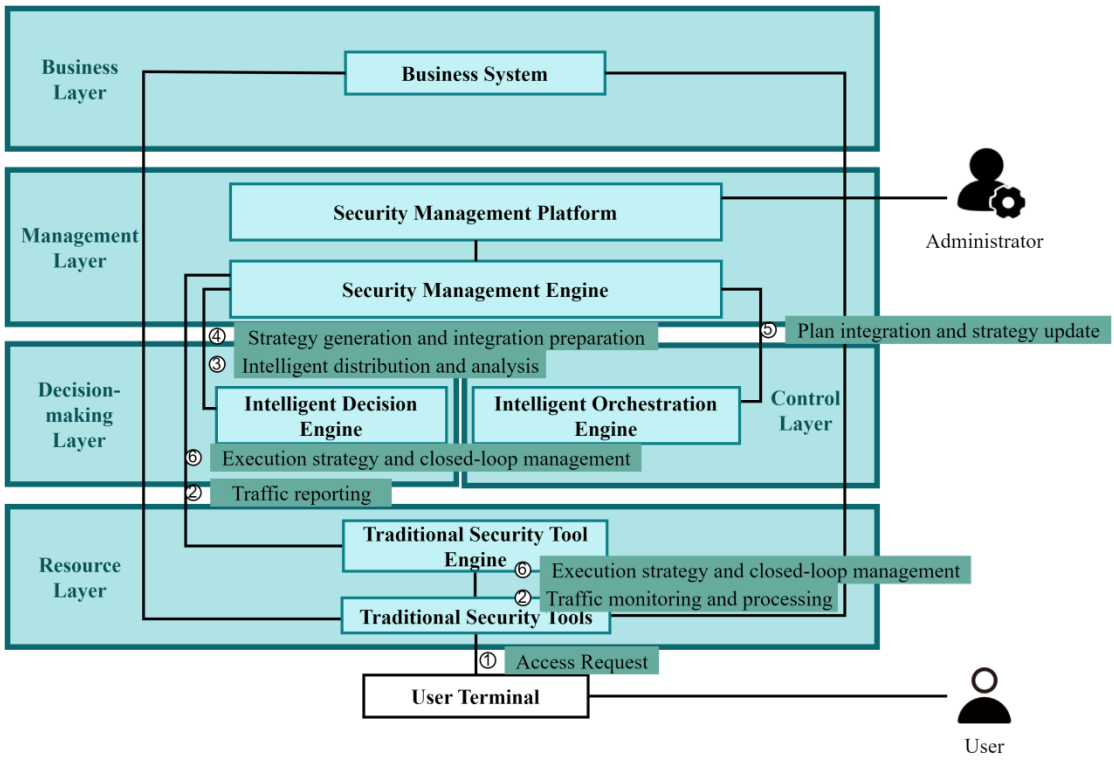

Figure 7-1 Autonomous Security Scenarios for Anomalous Access Detection

1. User Access and Traffic Filtering: Terminal users initiate malicious access requests to the

business system through the client. All incoming and outgoing network traffic of the business system must pass through an integrated security protection gateway, including WAF (web application firewalls), traditional firewalls, and DDoS (distributed denial of service) protection devices. These devices are responsible for real-time interception and filtering of malicious or suspicious traffic, ensuring the availability and security of the business system.

2. Traffic Monitoring and Intelligence Reporting: Security protection devices continuously monitor all traffic passing through, recording detailed access logs, anomaly alerts, and attack attempts. These raw data is reported in real-time to the traditional security tool engine, where it undergoes preliminary data cleansing and aggregation to eliminate redundancy, errors, or irrelevant information, ensuring the accuracy and efficiency of subsequent analysis. The processed data is then reported to the security management engine for further analysis and decision-making.

3. Intelligent Distribution and Analysis: After receiving the security data processed by the traditional security tool engine, the security management engine invokes the AI classification model of the intelligent decision engine to identify the data. The security data is intelligently categorized based on its characteristics. Categorized data is further correlated and mined for potential connections through a knowledge graph generated from threat intelligence databases, extending and supplementing threat intelligence and security information. Subsequently, the intelligent decision engine uses its AI language models to perform in-depth attack behavior analysis on the extended and categorized data, identifying complex attack patterns and hidden threat sources that conventional rules might miss.

4. Strategy Generation and Integration: Based on the results of the large model analysis and the required actions, the intelligent decision engine uses its AI language models to generate targeted protection strategy plans, including but not limited to rule updates, access control policy adjustments, and emergency response process optimizations. These strategy plans are

reported to the security management engine, providing guidance for subsequent strategy execution and optimization.

5. Plan Integration and Strategy Update: After receiving the rectification plans, the security management engine integrates this information with the current configuration status of the monitoring devices into unified security rectification instructions and sends them to the intelligent orchestration engine. This engine uses AI for logical reorganization to automatically generate security tool task scheduling plans. Based on the established security policies and business needs, the plans are orchestrated and optimized, and the security tool configuration strategies are sent back to the security management engine.

6. Strategy Execution and Closed-Loop Management: The security management engine sends the optimized plans along with updated configuration strategies back to the traditional security tool engine. The engine adapts the data formats and further communicates the information to the security tools for configuration upgrades and policy adjustments. Once all remediation actions are completed, the system automatically enters the next cycle of self-monitoring and optimization, achieving continuous security management and improvement.

Through this closed-loop autonomous process, the entire security protection system can self-learn, self-optimize, and self-repair, effectively addressing the evolving network security threats and ensuring the stable operation and data security of the business system. After completing one cycle, the system automatically enters the next cycle, continuously improving the security protection level.

7.2 Autonomous Security Scenarios for Self-Security Detection of Business Systems

With the rapid increase in connected devices, business systems within networks have become

more diverse and complex, leading to a significant rise in security risks. Traditional manual security detection methods are no longer sufficient to address these increasingly complex security threats. Therefore, it has become crucial to introduce AI technology to build a more intelligent and automated autonomous security protection system. The workflow for AASP system under the self-security detection of business systems is as follows:

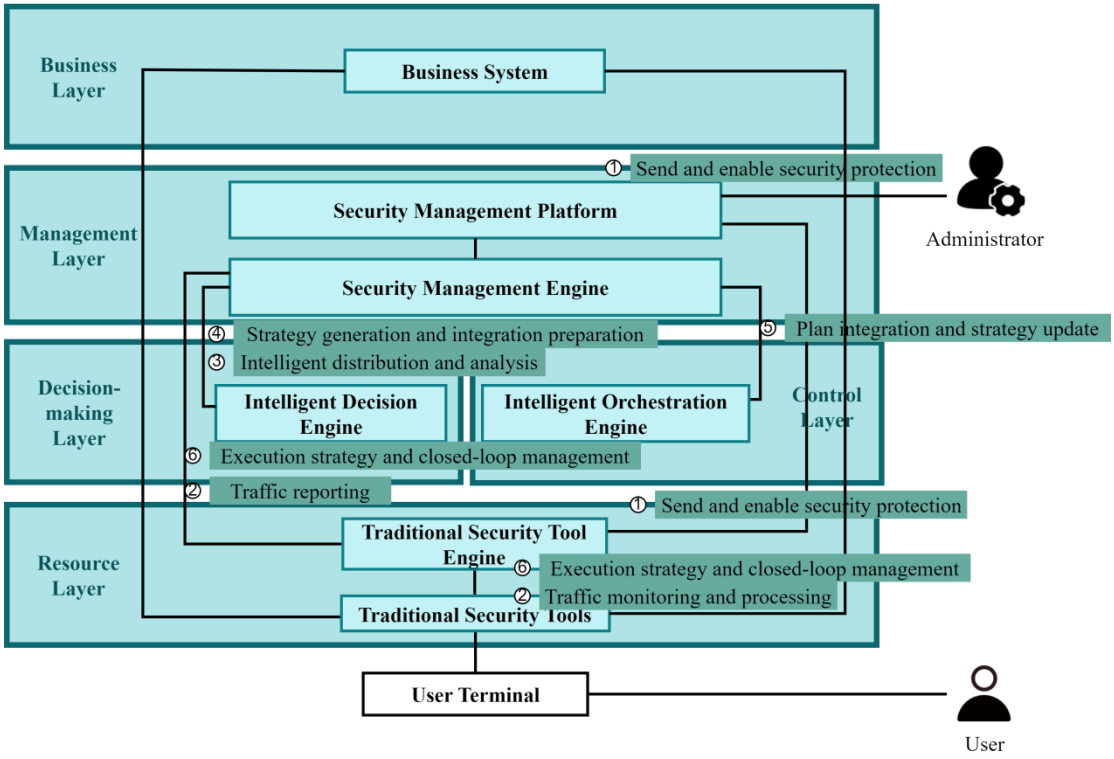

Figure 7-2 Autonomous Security Scenarios for Self-Security Detection of Business Systems

1.Activating Traditional Security Protection: Administrators perform a comprehensive health check of the business system's network, applications, and infrastructure. They configure the startup status and invocation settings for traditional security tools such as database audit tools and vulnerability scanners on the security management platform. Instructions are forwarded through the security management engine to manage the startup status of these traditional

security tools. Additionally, the configuration data are converted into a format suitable for traditional security tools before being deployed for configuration, thereby initiating security protection for the business system, internal security threats, vulnerabilities, and abnormal behaviors.

2.Initial Data Reporting and Preprocessing: Once the instructions are received, the security tools begin security detection on the business system, and the captured alerts and risk data are uploaded in real time to the traditional security tool engine, serving as the first checkpoint in the security event response chain. Meanwhile, the raw data undergoes preliminary cleaning and aggregation to eliminate redundancy, errors, or irrelevant information, ensuring the accuracy and efficiency of subsequent analysis. The processed data is then reported to the security management engine, preparing for the core analysis phase.

3.Centralized Analysis and Intelligent Distribution: The security management engine calls the intelligent decision engine in the decision layer to process the data using automated recognition and generation algorithms. The security monitoring data is intelligently classified based on its characteristics. Initial rule matching and anomaly detection algorithms are applied to perform preliminary screening and tagging of potential threats to determine their urgency and type. Subsequently, this data is accurately forwarded to the intelligent decision engine, which utilizes its AI language model to conduct in-depth analysis of system vulnerabilities, security weaknesses, and other complex issues, extracting valuable information from large data sets and identifying hidden threat patterns.

4.Solution Generation and Feedback: Based on the results of the deep analysis, the AI language model, in collaboration with its subordinate models, designs targeted security remediation plans. These plans include specific remediation measures as well as preventive strategies and optimization recommendations. Once the plans are developed, the results are reported back to the model and simultaneously forwarded to the security management engine

to facilitate the execution plan.

5.Solution Integration and Policy Deployment: After receiving the remediation plans, the security management engine consolidates this information into a unified security remediation directive, which is sent to the intelligent orchestration engine. This module, considering existing resources and environmental constraints, develops new system vulnerability remediation plans and security monitoring strategies, arranges and optimizes these plans to align with the organization's overall security objectives. The strategies are then reported to the security management engine to provide directives and guidance for subsequent execution and optimization.

6.Policy Execution and Closed-Loop Management: The security management engine sends the optimized plans and updated configuration strategies back to the traditional security tool engine, which communicates these to the security protection devices to execute configuration upgrades and policy adjustments. Once all remediation actions are completed, the system automatically transitions to the next cycle of self-monitoring and optimization, ensuring continuous security management and improvement.

Through this closed-loop mechanism, the entire security governance system maintains high adaptability and effectiveness in an ever-changing threat environment, ensuring the continuous and stable operation of business systems.

7.3 Self-Healing and Upgrading in AI Systems

As AI continues to advance in intelligence, its applications are becoming more widespread, necessitating enhanced security measures for AI systems in networks. The increasing complexity and autonomy of AI systems make their decision-making processes difficult to fully predict and control. Therefore, by incorporating AI technology, it is crucial to implement a autonomous security protection system that features self-detection, self-healing, and

self-optimization. The workflow of AI-based security autonomy in AI systems is as follows:

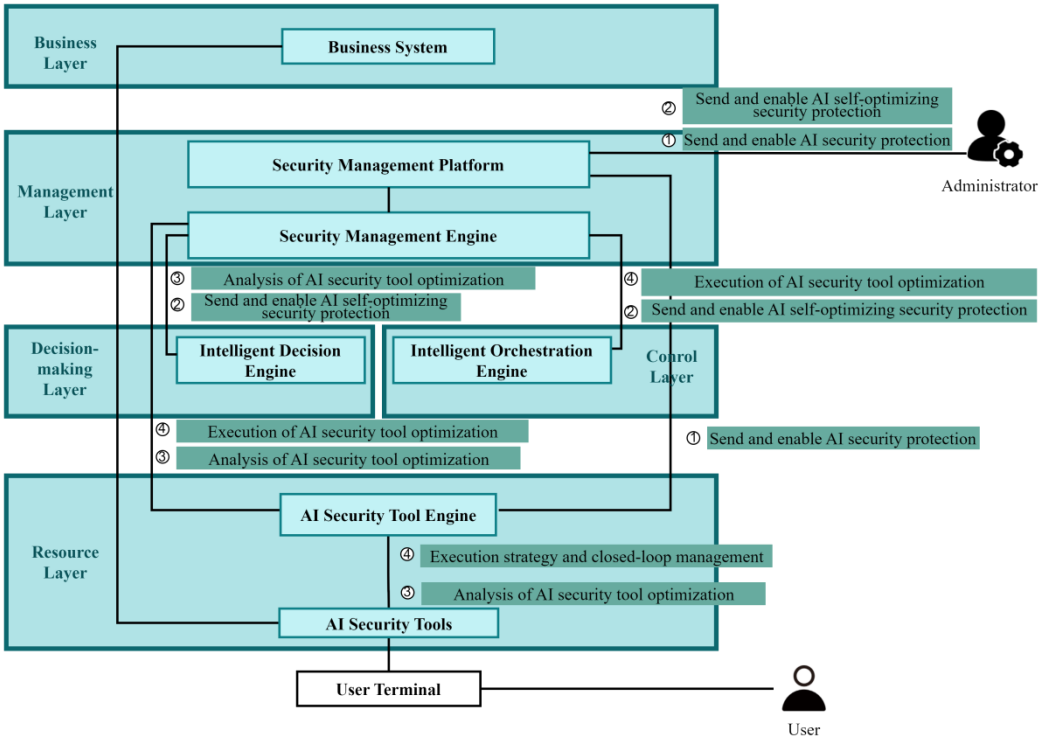

Figure 7-3 Self-Healing and Upgrading in AI Systems

1.AI Security Protection Activation: Administrators configure security protection plans for potential AI security risks. On the security management platform, they set up the activation status and invocation configurations for AI security tools such as AI model auditing tools and data leakage detection tools. Instructions are forwarded via the security management engine to the AI security tool engine for managing the activation status of AI security tools, and data format conversion is performed to match the requirements of AI security tools. This configuration activates the security protection for business systems and AI within the system.

2.AI Self-Optimization Protection Activation: Administrators set the AI vulnerability protection large model in the intelligent decision engine to an active state on the security management platform. This model identifies highly credible security threats from the AI

security tool's alert logs, and generates optimization plans for relevant rules based on the AI security tool's rules. Additionally, administrators set the AI security tool policy generation large model in the intelligent orchestration engine to an active state on the security management platform, generating specified policies for the AI security tools.

3.AI Security Tool Optimization Analysis: Security vulnerabilities captured by AI security tools during protection, such as AI model vulnerabilities, data leakage incidents, and potential attack indicators, are reported in real-time to the AI security tool engine. This platform manages data format conversion and redundancy processing, and the processed data is then reported to the security management engine for further data filtering, correlation, and the creation of an AI security risk knowledge graph. Once the AI vulnerability protection large model is active, the intelligent decision engine periodically requests data from the security management engine, combining related data in a specified manner for analysis by the large model, and sends the optimization plans generated by the large model back to the security management engine.

4.AI Security Tool Optimization Execution: The security management engine breaks down the optimization plan into multiple tasks based on criteria such as security tool categories and rule library fields. These tasks are sent individually to the security arrangement engine, where they are orchestrated if needed. The AI security tool policy generation large model creates optimization strategies based on the tasks and sends them back to the security management engine. The security management engine forwards the optimized strategies to the AI tool engine for data format processing, based on policies in the AI tool engine such as AI security tool optimization constraints, sends them to the AI security tools for execution.

Through this closed-loop autonomous process, the entire AI security protection system achieves self-learning, self-optimization, and self-healing, effectively addressing the evolving security threats in the AI domain and ensuring the stable operation and data security of AI

application systems.

7.4 Adaptive Network Device Maintenance Scenario

Network device maintenance is not only fundamental for ensuring the normal operation of the network but also crucial for enhancing network service quality and maintaining business competitiveness. With the support of AI technologies, communication networks will become increasingly autonomous, necessitating adaptive maintenance of network devices to ensure their proper functioning. Whether it is for ensuring network stability, improving security, optimizing performance, or reducing operational costs, increasing user satisfaction, adapting to technological advancements, and supporting business expansion, adaptive maintenance of network devices are essential. The AASP workflow for the adaptive network device maintenance scenario is as follows:

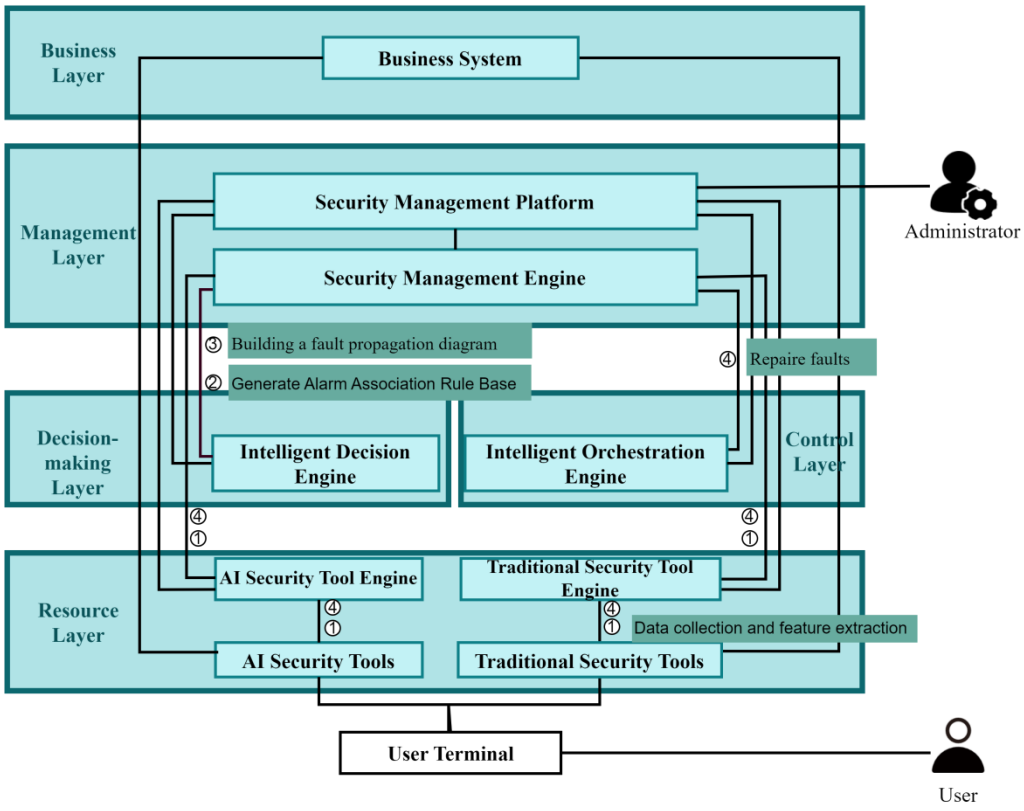

Figure 7-4 Adaptive Network Device Maintenance Scenario

1.Data Collection and Feature Extraction: The Security Management Engine collects alarm data from the Traditional Security Tools engine. Then, using built-in rules or AI models, it performs feature engineering on historical alarm data to extract key alarm features and the topological relationships between network elements.

2.Generate Alarm Correlation Rule Library: Based on the key alarm features and topological relationships, the Intelligent Decision Engine's AI model generates RCA (root cause analysis) rules for alarms. It performs statistical analysis on the support and confidence levels of all alarm rules to create an alarm correlation rule library.

3.Construct Fault Propagation Map to Locate Faults: Combining the alarm correlation rule library with the network topology, the Intelligent Decision Engine's AI model constructs a fault propagation map and calculates the maximum spanning tree to identify the root cause of

the fault.

4.Fault Repair: After identifying the root cause of the fault, the Security Management Engine issues repair tasks to the Intelligent Orchestration Engine for security tool orchestration. Upon receiving the preliminary repair plan, the Security Management Engine, considering the performance status of security tools, uses AI models to select appropriate tools for executing the repair, then forming a complete repair plan. The Security Management Engine then sends the repair plan to the Traditional Security Tool Engine, which dispatches the necessary security policies to the Traditional Security Tools and schedules the relevant security tools to perform the fault repair.

Through this autonomous process, the entire AI-driven security protection system can automatically mine, analyze, locate, and repair faults, effectively handling a large volume of alarm information.

7.5 Customized Configuration of Security Tools

As communication networks evolve, society's management, economic production, and human life increasingly rely on efficiently and reliably operating networks. Even a single user might represent an entire ecosystem, requiring a network architecture that provides business and user-centered experiences. This necessitates a mechanism for differentiated network services and customized network operations to meet the diverse and personalized needs of business system owners. The AASP workflow in the customized configuration of security tools scenario is as follows:

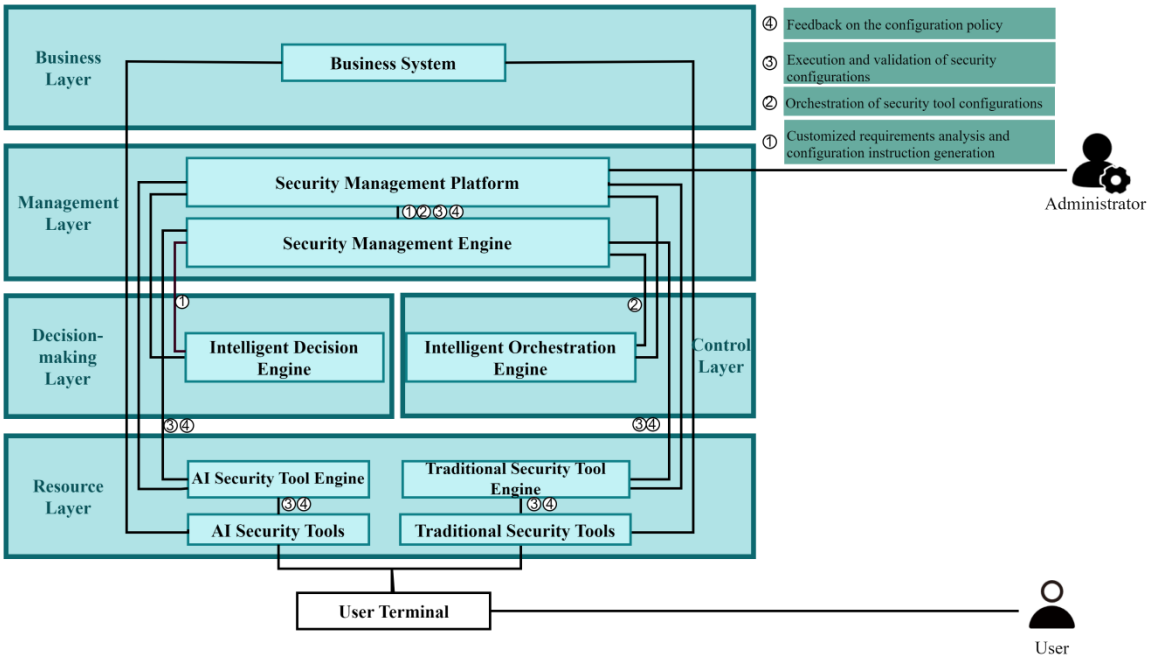

Figure 7-5 Customized Configuration of Security Tools

1.Customized Demand Analysis and Configuration Instruction Generation: When the owner of a business system has customized security protection needs, they can send a description of their requirements to the administrator via email. The administrator inputs the customized demand and optimization requirements for the business system's security strategy into the Security Management Platform. This description is then transmitted to the Intelligent Decision Engine through the Security Management Engine, where an AI large model analyzes the demand. Based on the analysis and breakdown from the Intelligent Decision Engine, corresponding configuration strategies are developed, and configuration instructions are generated. These instructions are then verified for legality and completeness by an AI validation model. Once validated, the configuration instructions are returned to the Security Management Platform via the Security Management Engine.

2.Security Tool Configuration and Orchestration: After the administrator confirms the configuration instructions on the Security Management Platform, the Security Management

Engine drives the Intelligent Orchestration Engine. The Intelligent Orchestration Engine creates a configuration plan based on the instructions, extracting the security tools to be configured, configuration parameters, and requirements. It orchestrates the configuration sequence and then feeds this information back to the Security Management Engine.

3.Security Tool Configuration Execution and Validation: Upon receiving the configuration plan from the Security Management Engine, the AI Security Tool Engine or Traditional Security Tool Engines initialize the selected security tools with relevant parameters, such as threshold values and policy configurations. After the configuration is completed, the administrator can review the configuration of the security tools via the Security Management Platform to ensure it meets the expected setup.

4.Feedback on Configuration Strategy: The Security Management Engine continuously collects performance data from the security tools. Administrators can monitor the performance of the configured security tools on the Security Management Platform, including metrics such as response time, resource usage, and error rates. This allows administrators to understand the operational status of the security tools following the implementation of the configuration strategy.

As communication networks evolve, society's management, economic production, and human life increasingly depend on efficiently and reliably operating networks. Even a single user can represent an entire ecosystem, necessitating a user-centered business experience from the network architecture. Users should participate in defining network services and customized network operations to meet their diverse and personalized needs. The described AI-based fully autonomous protection system continuously receives security demands from users and business systems, allowing for ongoing adjustments and feedback on security configurations. This enhances the performance and security of the overall security architecture, improving adaptability and protection effectiveness.