GTI Built-in Security for Telecommunication Networks White Paper

GTI Built-in Security for Telecommunication Networks White Paper

Version:	v0.1
Deliverable Type	□ **Procedural Document** ☑ **Working Document**
Confidential Level	☑ **Open to GTI Operator Members** ☑ **Open to GTI Partners** ☑ **Open to Public**
Working Group	5G ENS
Task	
Source members	CMCC
Support members	Huawei
Editor	Xiaojun Zhuang , Li Su
Last Edit Date	01-06-2021
Approval Date	25-08-2021

Document History

Date	Meeting #	Version #	Revision Contents
DD-MM-YYYY		NA	
DD-MM-YYYY			
DD-MM-YYYY			
DD-MM-YYYY			
DD-MM-YYYY			

Table of Contents

1 Executive Summary 5

2 Abbreviations 6

3 References 7

4 5G Security Requirements and Status 8

4.1 5G Security Challenges 8

4.2 5G Security Requirements 9

4.2.1 5G Fundamental Network Security Requirements 9

4.2.2 Security Requirements from 5G Vertical Industries 10

4.3 5G Security Progress 11

5 5G Endogenous Security Goals and Architecture 13

5.1 5G Endogenous Security Goals 13

5.2 5G Endogenous Security Architecture 14

6 Basic 5G endogenous security capabilities 16

6.1 Basic endogenous security capabilities of NFs 16

6.2 Basic endogenous security capabilities of network 18

6.3 Basic security capabilities of service 18

7 Potential requirements on 5G endogenous security 19

7.1 Trust enhancement for NF 19

7.2 Interaction between intelligent detection and disposal 20

7.3 On-demand security services 21

8 Conclusion 22

1 Executive Summary

With the rapid deployment and application in more and more industries, 5G has become a key national infrastructure and has also become one of the major targets of security attacks. Compared with traditional 4G networks, 5G supports new features like network slicing and edge computing; 5G core network adopts new concepts including cloud computing, virtualization and SBA architecture deployment. As a result, 5G networks are being threatened by not only all the existing security challenges from 4G networks but also new security challenges introduced by above mentioned new technologies, architectures, and business solutions. On the other hand, increasing vertical industries using 5G networks also face urgent security requirements. The traditional model of relying on statically deployed security devices to construct a physical security boundary cannot meet the need to defend increasing new attacks such as APT, and it cannot meet the needs of dynamic security protection for cloud-based networks nor the needs of flexible and on-demand security services for customers in vertical industries. Therefore, a novel security concept 5G endogenous security becomes imperative which can provide on-demand security services for the customers in vertical industries while at the same time achieve comprehensive improvements to 5G network's own security protection capabilities.

Based on current 5G network security status and requirements from telecom operators, this white paper provides an overview of the goals and the architecture of 5G endogenous security, its capabilities and key requirements, conclusion are made to telecom operators and equipment vendors on effective collaboration to promote the development and adoption of 5G endogenous security.

2 Abbreviations

Abbreviation	Explanation
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
DDoS	Distributed denial of service
EAP-AKA	Extensible Authentication Protocol-Authentication and Key Agreement
eMBB	Enhanced Mobile Broadband
FW	Firewall
IPS	Intrusion Prevention System
mMTC	Massive Machine Type Communication
MNO	Mobile Network Operator
NF	Network Function
SUPI	Subscription Permanent Identifier
TLS	Transport Layer Security
uRLLC	Ultra reliable and low latency communication
WAF	Web Application Firewall

3 References

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

[1] 3GPP TS 33.501: “Security architecture and procedures for 5G System”

[2] GSMA FS.16-NESAS: **“**Development-and-Lifecycle-Security-Requirements”

4 5G Security Requirements and Status

4.1 5G Security Challenges

In the era of the Internet of Things, 5G serves virtually all industries by supporting the three major business scenarios of eMBB, mMTC, and uRLLC, and has become a key infrastructure for the digitally transformed society. Compared with 4G networks, 5G networks are more open and adopt new concepts including cloud computing, virtualization, and SBA architecture deployment. 5G also supports new service deployment models such as slicing and edge computing. These changes make 5G networks not only face all the existing security challenges from 4G networks, but also being threatened by security challenges introduced by the new architecture, business models and technologies.

- Challenges introduced by the new network architecture: Cloud-based and IT-based network architectures introduce problems such as the exploitation of virtualization software vulnerabilities, virtual machine escape, container escape, virtual machine and container image tampering, etc. In addition, the slices can be accessed illegally or they attack each other due to failure of isolation between network slices. In the SBA architecture, there are issues of illegal access to the API, leakage of sensitive data, etc.

- Challenges introduced by the new models of deployment: Edge computing exposes 5G networks to more attacks. UPF which is deployed in the edge is more vulnerable to physical contact attacks and attackers can further attack the core network through attacking UPF. As slice management is allowed access by third parties, issues such as sensitivity data leakage, illegal access may arise.

- Challenges introduced by new services: Third-party applications hijacked by attackers or malicious third-party applications hosted on edge computing nodes can carry out DDoS attacks or illegally obtain access to edge computing platforms and 5G core networks. Due to the massive amount of terminals with access to 5G networks, attackers may exploit vulnerabilities in some terminals and maliciously hijack them or construct an illegal terminal to access the network repeatedly and illegally. For example, a signaling storm or DDoS attack may be triggered on a data plane and paralyze the network.

- The threat of quantum computing to traditional cryptographic algorithms and other emerging attack mechanisms are also among the new challenges faced by 5G.

5G networks carry not only the voice and data of end users but also high volume traffic for vertical industry services such as unmanned driving, smart cities, and smart factories, resulting in higher value of 5G networks which then are becoming key targets of new attacks such as APT. Once a 5G network is attacked, it will affect all the services carried by the 5G network and even affect the security and stability of the country and society, thus making the security of 5G networks critical.

4.2 5G Security Requirements

To deal with both traditional challenges and new security challenges brought by new technologies, services, and architectures, 5G networks should provide not only the security of their own underlying networks but also the security of the vertical industry applications running on them. On the other hand, it's also important to prevent vertical industry applications from attacking 5G networks. To meet the business needs from different vertical industry customers, 5G networks also need to provide differentiated security capabilities to vertical industries.

4.2.1 5G Fundamental Network Security Requirements

The fundamental security requirements for 5G are to ensure the secure and stable operation of 5G networks. In addition to the traditional communication network security requirements, the security requirements relating to new technologies, architectures, services, and attack types must also be considered. Some 5G fundamental network security requirements include:

- Network security self-protection: includes terminal access authentication, air interface signaling and data protection, user privacy protection, network domain security protection, CU/DU separation interface security, and network link security etc. New requirements from the core network side including SBA architecture authentication and authorization, interconnection security, etc.
- Security requirements for business evolution: New forms of services emerge under 5G such as eMBB, uRLLC, and mIOT, which introduce new requirements for network security such as network slicing, edge computing security, and open security capabilities.

- IT evolution security requirements: New IT technologies such as SDN and NFV put forward new requirements for network security, including DDoS protection for SDN controllers, virtualization software hardening, virtual machines and container escape prevention, etc.

- Security requirements for offensive and defensive confrontation: In addition to the security vulnerabilities related to the new 5G protocols, the open interconnection of 5G networks has added more exposure to core networks and introduced more IT-related security vulnerabilities. In the process of network construction, operation and maintenance, network vulnerabilities should be regularly investigated and patches should be performed after the assessment of service impact.

4.2.2 Security Requirements from 5G Vertical Industries

5G networks provide network services to vertical industries through slicing and edge computing. First of all vertical industries need 5G networks to provide fundamental network security capabilities to ensure a safe and stable operating network environment for applications in vertical industries. In addition, the services of vertical industries also have security requirements by themselves, including security isolation between applications hosted on the edge computing nodes of operators and other applications, prevention of DDoS attacks from terminals or Internet, intrusion detection, etc. The differences between various vertical industries also lead to differences in security requirements. In order to achieve rapid service deployment, vertical industries require 5G networks to provide slicing or edge infrastructure while at the same time provide security protection capabilities that meet their service security requirements and achieve one-stop online deployment. For operators, they can achieve security capability advancement and add value to their network; and on the other hand indirectly mitigate security attacks on 5G networks from vertical industries by providing security services. Therefore, defining the security requirements of 5G vertical industries is of great significance to the security of both vertical industries and 5G networks.

The security requirements of 5G vertical industries mainly include:

- Provide flexible network security functions and configuration capabilities, including access authentication, data confidentiality and integrity protection, user privacy protection, infrastructure security level and security isolation, etc.

- Provide on-demand security service capabilities: terminal DDoS attack detection, Internet DDoS attack detection and mitigation, intrusion detection and defense, security isolation, access control, malicious code detection, web security protection, data security protection, etc.

With the deep integration of 5G networks and vertical industries, the security requirements for 5G vertical industries will be further explored and the security service capabilities of 5G networks will also be more completed.

4.3 5G Security Progress

To ensure 5G network security, standardization organization 3GPP has defined 5G security technical requirements. Based on terminal access authentication, air interface signaling/data protection, handover security, and network domain security provided by 4G networks, 5G security offers additional supports of integrity protection of air interface user data, 5G-AKA, EAP-AKA authentication methods, user identification SUPI protection, and TLS encryption protection of inter-network information. 5G also achieves more comprehensive data security protection, richer authentication mechanism, tighter user privacy protection, and more flexible network information protection. The GSMA NESAS adopts 3GPP's security technical requirements and provides security assurance evaluations for 5G equipment and evaluation reports, which can be used as a security reference for operators' equipment to access the network. Based on the 3GPP standards and combining all the requirements of equipment access, deployment, operation and maintenance, operators can further strengthen network security capabilities in terms of security domain division, network boundary protection, security operation and maintenance through enterprise standards and specifications.

Since standardization focuses only on the security of device interconnection and security configuration, operators have added network boundary protection, operation and maintenance and other requirements to meet the need of their network construction. However, the boundary protection provided by security device statically deployed and the

security reinforcement of a single device still cannot fully meet the 5G security requirements. There are some issues and requirements being identified as follows:

- The abnormal process and abnormal files on the NF cannot be identified quickly. The code on the NF, the operating system, database and middleware being used inevitably have backdoors and loopholes, which can only be checked manually through the log on the network management platform of the NF after the service is affected due to the lack of link between the NF and the border security device; as a result, the border security device cannot receive the abnormality of the NF. On the other hand, centralized deployment and the use of common operating systems increase the risk of NFs being infected by worms, which can spread quickly or even affect all NFs in the resource pool.
- Detection methods based on known signatures cannot defend new types of attacks such as APT. Currently security devices detect abnormal codes and traffic based on known security knowledge(e.g. malicious code fingerprint). The advancement of attacking techniques allows attackers to avoid using known knowledge when carrying out attacks, instead by using new features that can't be detected by security devices. Moreover, in the event of a security attack, traditional methods of manual log screening and response strategy configuration on security device not only take a long time to locate the problem but also increase the workload and are very prone to configuration errors.
- Poor support for the differentiated security requirements of vertical industries: 5G networks can provide customized network services for vertical industries through technologies such as slicing and edge computing. The differences in various vertical industries also lead to differences in security requirements. For example, customers in the smart factory industry require confidentiality of production data, while customers in the IoT industry with massive terminal access require anti-DDoS attacks. Only relying on physical statically deployed security devices at the boundary cannot achieve differentiated security services and security levels.

In summary, 5G security should be based on existing security capabilities and further elevate the security and credibility of the 5G NF, the reliability of the network and the differentiated security service capabilities to fence off attacks. This requires 5G networks to build endogenous security capabilities across NFs, networks and security services, and to achieve NF credibility, network reliability, and service availability.

5 5G Endogenous Security Goals and Architecture

5.1 5G Endogenous Security Goals

In order to solve the security problems faced by 5G networks and comprehensively improve the security of 5G networks, some domestic security vendors, equipment vendors and operators come up with the concept of endogenous security but focus on different aspects. Security vendors emphasize on the formation of self-adaptive, independent and self-growth endogenous security by integrating security device into the businesses of its organization, which include security systems and information systems, security data and service data, security talents and IT talents. Telecom equipment vendors emphasize that security capabilities are built into sNFs, and NFs have credibility and monitoring capabilities, thus forming a closed loop of NF detection, monitoring, and action. Telecom operators propose to build an adaptive, autonomous, and self-growing endogenous security system of "defense, detection, response, and prediction" for cloud-network convergence scenarios.

Due to differences in the standpoints and scenarios among above three major players, the understanding of endogenous security concepts among them is also slightly different. Considering the current pain points of 5G network security, we believe that 5G endogenous security is the integrated security capability of the network through building some security functions into the NFs and providing intelligent network analysis and flexible security orchestration capabilities. As the result, 5G networks can achieve automatic immunity, active defense, and on-demand security services, and so achieve the following endogenous security goals of trusted NF, network reliability, and service availability:

- Trusted NF means that the device is designed to follow the security design principles to ensure code security and no backdoors, to ensure secure configuration of operating systems, middleware, and databases, and to support security functions interconnection and intrusion detection capabilities. Trusted NF should have an integrated root of trust and ensure that it behaves as expected during deployment, operation and upgrade.

- Network reliability refers to the ability of the network to detect, monitor, and process abnormal events and information. It can combine the security events reported by the NFs, network traffic, and security logs from security devices, and use AI technology to perform intelligent analysis to detect security threats in advance. Furthermore, automatic response and action can be achieved through dynamic reallocation of the security resource pool and dynamic update of the security configuration. And network security should have resilience, support high-level protection of important business systems, improve the ability to defend security attacks, and ensure uninterrupted operation of important business systems.

- Service availability refers to providing customers with fundamental network security capabilities and customized security services. Fundamental network security capabilities are intrinsically available when 5G networks are built, including access authentication, data protection, and privacy protection. On-demand security services are the capabilities that 5G networks provide to customers with on-demand security detection, authentication, protection, operation and maintenance auditing, attack source tracing, and host security through the establishment of a secure resource pool and security capability exposure.

5.2 5G Endogenous Security Architecture

The 5G endogenous security architecture consists of the security management center, NFs, virtualized security devices, and dedicated security devices (as shown in Figure 1). In this architecture NFs have built-in security capabilities such as trusted integrity protection, security reinforcement, kernel vulnerability prevention, and intrusion detection, and NFs can report abnormal state to the security management center.

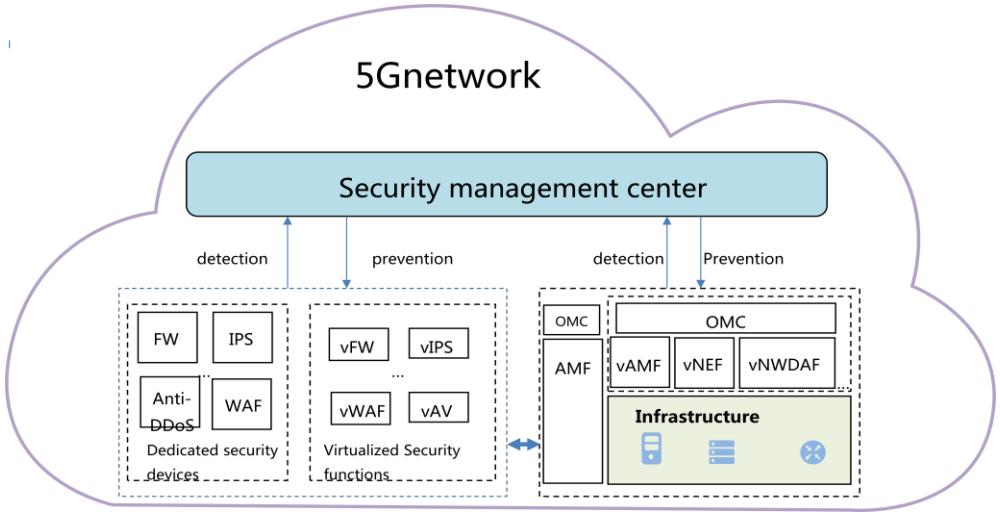

Figure 1 5G Endogenous Security Framework

The security management center intelligently analyzes the abnormal state from the NFs and the security logs reported by the NFs and security devices, and provides a response strategy which will be distributed to the security devices for execution, thereby forming a security closed loop of intelligent detection and processing. In addition to providing fundamental security capabilities such as security domain division/isolation and data security protection, the security management center supports security intelligent analysis and can link NFs/network management of the NF, security device/security controllers, and security devices to take coordinated actions. With the help from the security management center, security device is no longer isolated but becomes part of the 5G endogenous security capabilities that can be coordinated and orchestrated to offer comprehensive security protection. To support vertical industries, the security management center can provide differentiated security configurations and the security capabilities of 5G networks and security resource pools can be invoked to provide security services to vertical industries through NEF or other equipment. Therefore, 5G endogenous security enables 5G networks to be a unified, intelligent, active, and flexible security defense system with the ability of self-immune, proactively preventing epidemics, and providing security services on demand.

6 Fundamental 5G endogenous security capabilities

6.1 Fundamental endogenous security capabilities of NFs

In the design phase of 5G, some security functions have been considered to be built into the network functions. NF Various domestic and foreign standardization bodies such as 3GPP, GSMA, and CCSA have promoted 5G security functions standardization, to standardize the devices produced by manufacturers. Operators also define the security capabilities of 5G NF in enterprise standards and device centralized procurement specifications. The basic endogenous capabilities of 5G NFs are summarized in Table 1.

Table 1 Existing endogenous security capabilities of 5G NFs

Endogenous security of NF	capability categories	Description
General safety	Software integrity	Support software version package (mirror, software package, VNFD, NSD, etc.) integrity verification, and eliminate software security vulnerabilities through patches or software upgrades
	Account and password security	Support assigning accounts and passwords for users; Supportadding, changing, deleting, lockingaccount etc.; Support set ting password complexity only according to the requirements of the operator. Support modification and expiration reminders. Support secure storage of password.
	Authentication and authorization	Support static passwords, dynamic passwords, biometric authentication technologies such as fingerprints for identity authentication. After successful authentication, users are allowed to log in to the NF; support authorization methods such as RBAC, Oauth, etc., and only authorized users are allowed to access NF.

	Log security	Support logging in/out of users, providing logs to record the operations on device for review; Logs should be stored safely, and the storage time should be set according to requirements
	Protocol security	Support secure protocols, prohibit insecure protocols; only open necessary and used ports/protocols
	Digital certificate security	Support digital certificates in X509v3 format, and secure digital signature algorithms; supports SAN (Subject Alternative Names) extensions and restrictions on certificate validity period
Specific security of NF	AMF security	Support encryption and integrity protection for signaling message. Support anti-degradation protection for UE security capability, and verifying the security capability sent by the UE, etc.
	UDM/AUSF security	Support encrypted storage of root key which cannot be read in plain text. Support decryption from SUCI to obtain SUPI and storing UE authentication status, etc.
	UPF security	Support confidentiality and integration protection of user data transmitted by N3. Support the restriction on terminal mutual access, etc.
	NRF security	Support access control and authorization for NF service.
	gNB security	Support confidentiality and integrity protection for access layer signaling, and support activating the corresponding user plane security capability according to security policy sent by the core network, etc.

GSMA and domestic accreditation laboratories currently have launched the security assurance certification for 5G NFs. If a device passes the GSMA NESAS or the domestic

equivalent department accreditation, it can meet the basic credibility requirement of NFs.

6.2 Fundamental endogenous security capabilities of network

The fundamental endogenous security capabilities of 5G networks include:

- Security domain division and isolation: 5G network can be divided into non-trusted domains, semi-trusted domains (DMZ), and trusted domains. Set up DMZ zone at the border with the Internet, deploy DDoS detection and cleaning device, IPS, WAF, and double-layer heterogeneous firewalls to resist attacks from the Internet and protect 5G outbound traffic. Inside the 5G network, the access between different security domains is controlled through firewalls or port whitelists.

- Network security management: 5G network cloud infrastructure, virtual resource orchestration and management system (MANO) should support security reinforcement to reduce exposure to attackers and the possibility of being attacked, including hardening of host operating system, virtualization software, etc., which can ensure the security isolation between virtual machines and containers. Key open source components (such as OpenStack , K8s , etc.) should support security configuration according to the requirements from industry best practices.

- Backup and recovery: various backup mechanisms such as 1+1 or N+1 are supported in 5G networks for different important levels of systems, which can ensure the service operate normally in the event of a failure.

6.3 Fundamental security capabilities of service

5G network supports the configuration of security capabilities and opening network security capabilities and services.

5G network supports the construction of dedicated slices with proprietary physical device and the construction of slices with shared physical device to provide vertical industries with slices of different security levels and security isolation levels. 5G network supports providing application-layer access authentication, privacy protection, data confidentiality and integrity

protection according to customer requirements.

In addition, the fundamental network security capabilities opening to vertical industry is supported in 5G network through the open API of NEF, and only authenticated and authorized users can access the API. Based on the capabilities of security resource pool and security management center, the security device and capabilities can be uniformly managed to provide security services for vertical industry.

7 Key technologies on 5G endogenous security

7.1 Trust enhancement for NF

The reliability of 5G network is based on the trusted NFs. With the fundamental NFs being trusted, the hardware and software functions of 5G network can continuously operate as expected, which then contributes to the complete and comprehensive trustiness of network devices. The trust enhancement of 5G devices includes:

- Support hardware-based trusted boot: Verifies the trustworthiness of the system hardware, firmware, system boot program, operating system, and system security components through the built-in hardware based trusted root. Build a complete trust chain in device through verification and trust in every layer. It can realize the integrity check of the device hardware, firmware, and operating system during startup to ensure the trusted initial state of the system.
- Support trust measurement for NF: static and dynamic integrity measurement can be performed on key NF applications and processes of the system during operation. Through periodic or event-triggered measurement mechanisms, a trusted operating environment (not subject to unintentional or malicious interference) for NF is established to ensure system operating as expected.
- Support remote trust management: Generate a trust status report through trust measurement during the startup and operation of the device. It will be reported to the remote management center by the trusted client of the NF. The trusted management center verifies the trusted identity and status of device, provides

remote verification for establishing trusted connections between different networks. The trusted management center monitors and analyzes the status of the trusted NFs to provide trust report of overall network. It can dynamically configure the security policies of the trusted NFs according to the changes of security situation and management requirements.

7.2 Interaction between intelligent detection and response

Intrusion detection capabilities should be supported in operating system, NFs, network management, orchestration and management systems of the 5G cloud infrastructure:

- Malware detection, including rootkit, reverse shell, webshell
- Abnormal account detection, including brute force cracking, illegal account, illegal login
- Privilege escalation detection, including account, file and process privilege escalation detection
- Information destruction detection, including key file tampering and deletion, shell file tampering, illegal file downloading, etc.
- Abnormal behavior detection, including abnormal account changes and unauthorized new accounts.
- Security baseline verification, including OS security configuration, DB security configuration, web component security configuration check, and network security configuration.

The cloud infrastructure and NFs of the 5G network should support the escalation of the detected security status to the management system, and the security device supports the reporting of security events to the security device controller. The virtual infrastructure management system and OMC should support the unified perception and configuration capabilities of 5G network cloud infrastructure, NF configuration files, component versions, and key parameter configuration, etc., and support operation and maintenance personnel to be aware of whether the device currently has security vulnerabilities, whether the configuration is non-compliant or abnormally tampered in real time, so that the risk is visible and perceivable.

Centralized configuration of security device is supported in security device controller. 5G network management system (including the virtual infrastructure management system, OMC, and security device controller) reports security events, logs, etc. to the security management center, which can achieve intelligent threat analysis and display on the 5G network. Then 5G network management system delivers security configurations to the cloud infrastructure, NFs, and security device based on the analysis results of the security management center, so as to realize the closed loop of threat detection and disposal.

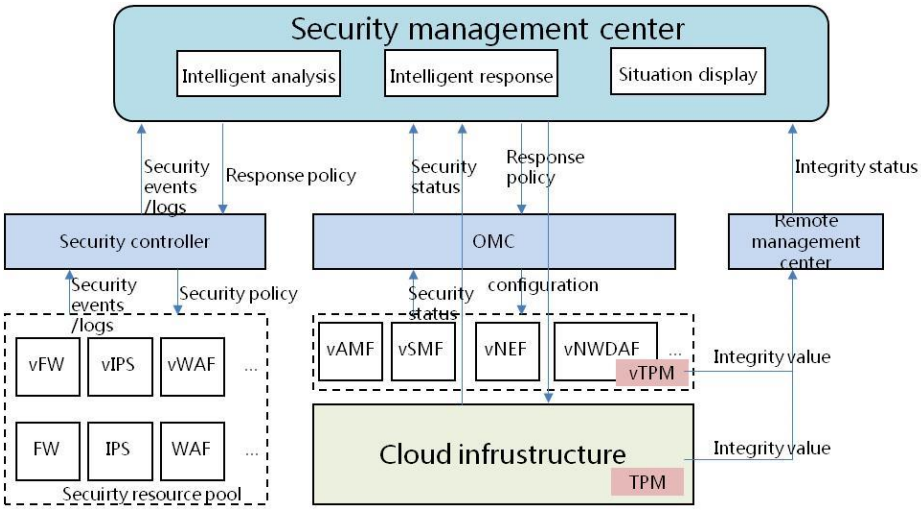

Figure 2 Interaction between intelligent detection and response

7.3 On-demand security services

5G networks should support construction of security resource pools in order to provide on-demand security services for vertical industry. It provides customers with security services such as protection, detection, scanning, operation and maintenance audit, host security and so on, which can protect customer business security while meeting requirements of relevant national laws and regulations.

The security resource pool should support the decoupling between the control function and execution function of the security device. Centralized security management and orchestration of the virtualized security device and the physical boundary security device is supported through the security device controller. The physical/virtualized security device or the network management should support standard northbound interface to interact with the security device

controller, including alarms, reporting operating status, and issuance of security policies. The northbound API provided by the security device controller should support interaction with the security management platform and 5G capability open platform to provide security capabilities to vertical industry on demand.

8 Conclusion

In order to achieve 5G endogenous security and improve 5G network security capabilities comprehensively, it is urgent for MNO, traditional CT equipment manufacturers, IT equipment manufacturers, software manufacturers, research institutions and other joint efforts to engage in 5G endogenous security research and key security capacity building, to ensure the security of 5G network and vertical industry. We recommend advancing 5G endogenous security from the following aspects:

- Promote 5G endogenous security standards: Telecom operators work with partners to promote 5G endogenous security standardization in security architecture, trusted computing solutions, northbound interfaces of security devices, security management platform functions, and intelligent analysis function and so on.
- Promote pilot verification project of trusted computing in 5G: there are challenges in the application of trusted computing technology because of the dynamics of 5G networks and the diversity of business. It is necessary for the industry to discuss feasible technical solutions of trusted computing based on the 5G network characteristics, and promote the gradual application based on pilot verification projects.
- Research and promote the built-in security capabilities of NFs: Research on security capabilities which should be built-in according to the functions of NFs, and promote the gradual application of built-in security capabilities of NFs. The security capabilities of NFs and border device should be complementary to avoid duplication of construction and save safety costs.
- Advance security device virtualization and decoupling: Achieve on-demand security capabilities. Security devices should be able to rapidly deployed and dynamically

scaled on demand. Similar to 5G NFs, security devices should also support virtualization, decoupling of control and execution layers, centralized control layers, and the virtualization of firewalls, IPS and WAF, etc., and be able to open northbound interfaces which are unifiedly managed and orchestrated by security device controllers.

- Construct comprehensive capability of detection and response closed-loop: It is a complex set of technologies and management system to construct intelligent detection and response closed-loop capabilities as it involves not only the capability of NFs, security devices, and security management centers, but also AI technologies related to 5G network attack and protection, the capabilities of operations and maintenance personnel. Operators should work together with the industry to explore and promote the capabilities of detection and response closed-loop, to achieve 5G network self-immunization and self-defense, and comprehensively enhance the security capabilities of 5G network.