HIKVISION Cybersecurity White Paper

About this Documentation

Offering an overview of our current exploration and practice on cybersecurity in the field of AIoT, Hikvision Cybersecurity White Paper provides users with the company's security strategies and capabilities in an open and transparent manner.

Hikvision reserves rights to update this Documentation. Please kindly find the latest version on the company website (http://www.hikvision.com/en/).

Copyright Disclaimer

Trademarks Acknowledgement

Legal Disclaimer

Revision Record

First published in January 2018, revised in September 2023, and revised again in January 2026.

Company Introduction

Founded in 2001, Hikvision is a technology company focusing on technological innovation.

We adhere to the business philosophy of "Professionalism, Reliability, and Integrity," and fulfill the company's core values: dedicated to customers' continual success, adding value to companies and communities, acting with honesty and integrity, pursuing excellence in every endeavor. For over two decades, starting with video technology, Hikvision has progressively built and refined an AIoT technology system centered on IoT perception, AI, and big data, providing security and scenario digitalization products and services to thousands of industries. The company's products and technologies have played important roles in major projects such as the Hangzhou Asian Games, G20 Hangzhou Summit, Beijing Olympics, Shanghai World Expo, APEC meetings, Beijing Daxing Airport, and Hong Kong-Zhuhai-Macao Bridge.

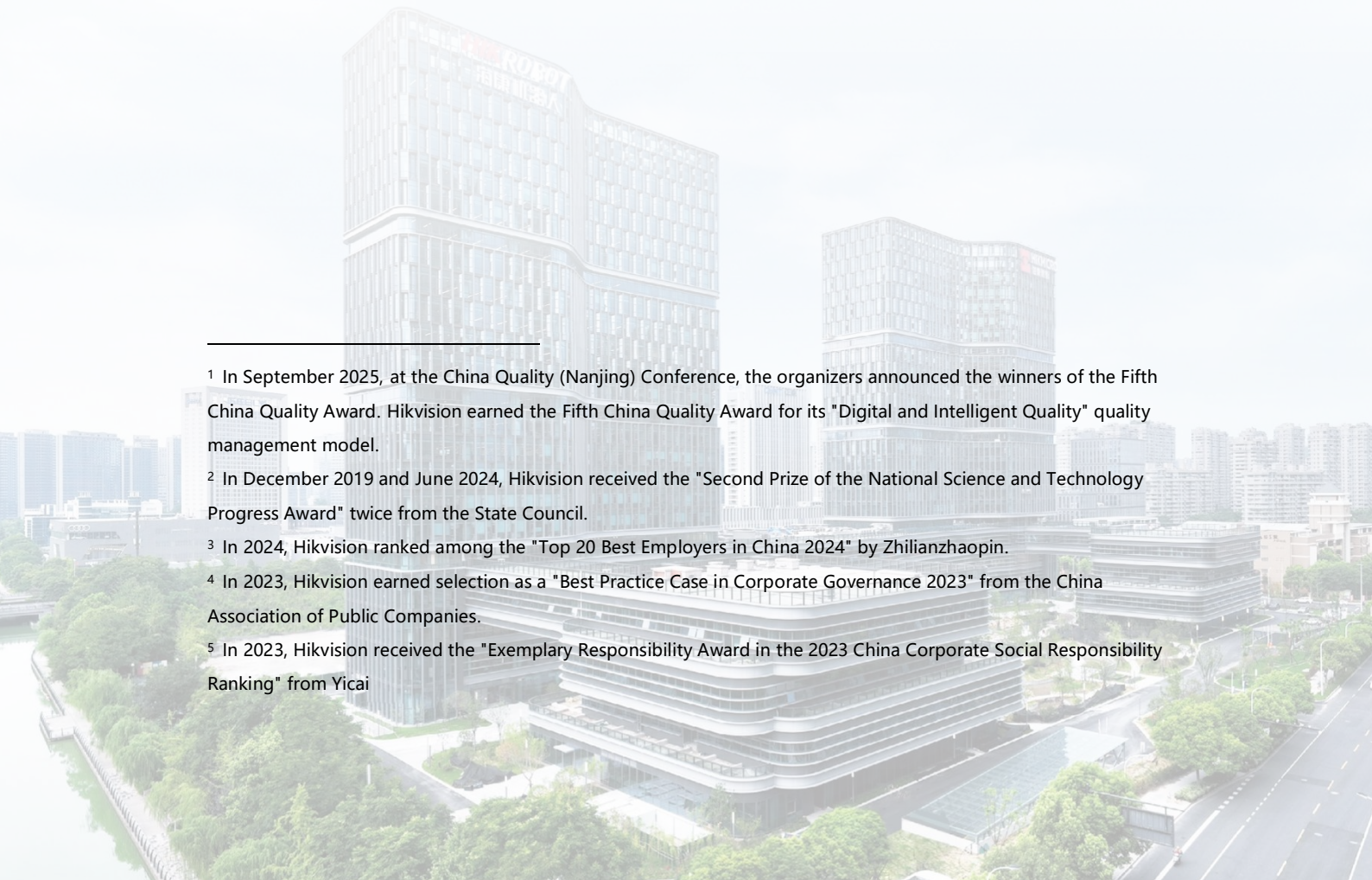
Hikvision is committed to serving thousands of industries. We leverage IoT perception, AI, and big data technologies to lead the future of AIoT. Through comprehensive machine perception technologies, we aim to help people better connect with the world around them. With a wealth of intelligent products, we strive to identify diverse demands by delivering intelligence at your fingertips. Through innovative AIoT applications, we are dedicated to empowering every individual to enjoy a better future by building an intelligent world that is more convenient, efficient, and secure.

Hikvision currently has 57,202 employees (as of the end of 2025), including more than 26,806 R&D personnel and technical service personnel. R&D investment accounts for 12.7% of the annual operating income (2025), making the Company an absolute leader in the industry. The company operates as a postdoctoral research workstation unit. It has established multiple local R&D centers both in China and overseas in addition to its Hangzhou headquarters, forming a multi-level R&D system that radiates from the headquarters to various regions.

Hikvision has established 32 provincial business centers, nearly 300 city branches and offices across mainland China, with technology parks built in cities such as Chengdu, Xi'an, and

Shijiazhuang, and manufacturing bases located in Tonglu (Hangzhou), Chongqing, Wuhan, among others. Overseas, its business covers over 180 major countries and regions worldwide, with branches set up in 60 countries and regions. Through overseas factories in India, Brazil, the UK, and other locations, the company achieves localized manufacturing, providing products and services to global customers.

In May 2010, Hikvision completed its listing on the Shenzhen Stock Exchange under the stock code 002415. The company has won multiple prestigious awards due to its innovative management model and strong operational performance. These include the Fifth China Quality Award[1], and the Second Prize of the National Science and Technology Progress Award[2]. The company also ranked among the Top 20 Best Employers[3] in China for 2024. Additionally, it won the Best Practice Case in Corporate Governance 2023 award.[4] The company also received the Exemplary Award in the 2023[5] China Corporate Social Responsibility List.



[1] In September 2025, at the China Quality (Nanjing) Conference, the organizers announced the winners of the Fifth China Quality Award. Hikvision earned the Fifth China Quality Award for its "Digital and Intelligent Quality" quality management model.

[2] In December 2019 and June 2024, Hikvision received the "Second Prize of the National Science and Technology Progress Award" twice from the State Council.

[3] In 2024, Hikvision ranked among the "Top 20 Best Employers in China 2024" by Zhilianzhaopin.

[4] In 2023, Hikvision earned selection as a "Best Practice Case in Corporate Governance 2023" from the China Association of Public Companies.

[5] In 2023, Hikvision received the "Exemplary Responsibility Award in the 2023 China Corporate Social Responsibility Ranking" from Yicai

CONTENTS

1. A letter from the President

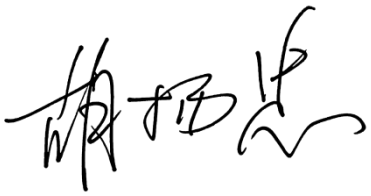
The world is transforming the 'Internet of Everything' from dream into reality. As a precursor to the 'Internet of Everything', video surveillance technology has developed rapidly over the past decade. Evolving from the analog era to the digital era, and then to the network era, it is now entering the intelligent era. Each advancement in technology propels human society forward while also presenting new challenges. The development of internet technology has greatly benefited human society, but it has also brought significant challenges, including those related to cybersecurity. Similarly, Internet of Things (IoT) technology, developed on the foundation of the internet, will enhance human life while introducing new challenges, with cybersecurity being one of them.

Compared to the IT industry, the security industry has not been in the digital era for long, with relatively weaker cybersecurity awareness across the industry. In 2014, following common practice, Hikvision established the Hikvision Security Response Center (HSRC) to create a unified external interface for addressing cybersecurity issues. In 2015, Hikvision founded the Network and Information Security Laboratory, which comprehensively advanced the company's cybersecurity system development. Subsequently, the company established the Network and Information Security Committee and the Cybersecurity Department, which built and refined a cybersecurity framework focused on organization and processes. Particularly, cybersecurity design significantly enhanced the overall cybersecurity integrity of the company's products and systems.

We recognize that cybersecurity is not solely the responsibility of product manufacturers. Every stakeholder involved in a project—including users, integrators, operators, engineering designers, and other service providers, and government entities— shares responsibility for cybersecurity throughout the project's entire lifecycle. All parties face cybersecurity challenges, the successful handling of which relies on 30% technological competence and 70% managerial expertise. Effective cybersecurity depends on consistent, coordinated action across all stakeholders—no single party can address it alone.

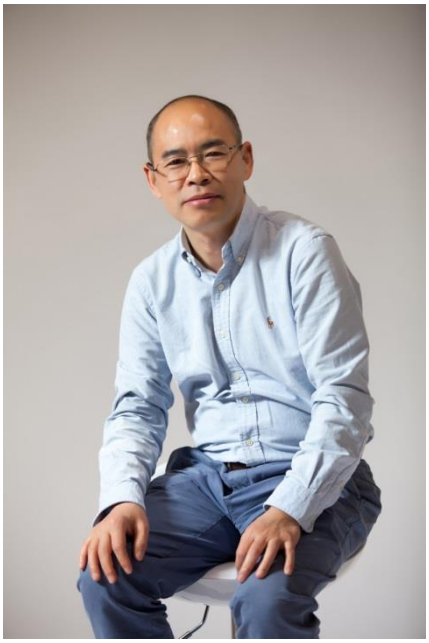
As focus on IoT security continues to increase, we recognize the need to address shared cybersecurity challenges. We are committed to protecting our customers' networks and business operations in alignment with applicable laws, contractual obligations, and

responsible business practices. Cybersecurity challenges are ongoing, and we are committed to continuously improving our security posture and response capabilities.



Hu Yangzhong, President

Hangzhou Hikvision Digital Technology Co., Ltd.



2. Preface

The security industry has evolved rapidly with digital transformation. Advances in artificial intelligence, including large-scale AI models, are enabling new capabilities. Combined with the integration of artificial intelligence and connected devices (AIoT), security systems are shifting from passive monitoring to platforms that support detection, analysis, and decision-making.

The widespread application of AIoT technology has further broken down data barriers between devices, promoting cross-system and cross-platform collaborative operations. However, while networking and intelligence enhance system efficiency, they significantly expand the attack surface. The transition from traditional closed architectures to open network environments has exposed security systems to diversified threats such as cross-domain attacks, data breaches, and supply chain contamination. Although the introduction of large AI models enhances analytical capabilities, it also brings new security risks like model poisoning and adversarial sample attacks; meanwhile, the large-scale deployment of AIoT devices increases the complexity of endpoint vulnerability management.

In the process of transitioning security from analog to digital, from isolated to networked, and from basic data collection to intelligent analysis, the compatibility challenges between legacy architectures and emerging technology stacks, along with the technical debt accumulated from rapid iterations, collectively pose potential security risks.

Hikvision operates in more than 180 countries and regions. To manage risk at this scale, the company maintains a security governance framework that spans the full lifecycle—from R&D and production to delivery and operation. Its approach to AI models and artificial intelligence and connected devices (AIoT) focuses on safe, effective system performance, with emphasis on reliability, data sovereignty, privacy, and critical infrastructure resilience.

Cybersecurity is a shared global challenge that affects all stakeholders—governments, industries, and organizations alike—and requires coordinated international cooperation, risk-based approaches, and the adoption of best practices.

Hikvision is committed to aligning with internationally recognized cybersecurity standards, supporting research that strengthens network defense capabilities, and maintaining transparent practices that enable users to assess our security posture.

We also welcome ongoing collaboration with our customers to strengthen processes, improve technologies, and advance our approach to cybersecurity.

Cybersecurity is a continuously evolving discipline, and the practices described in this document reflect Hikvision's risk-based approach to security at the time of publication.

3. Security Threats in the Internet of Things

The Internet of Things (IoT) connects any object through the network, giving objects intelligence and enabling communication and interaction between people and things, and between things themselves. The interconnection of a massive number of devices has made networks more open and complex, with richer and more diverse services. However, the advent of IoT also brings incredible security challenges.

Figure 3-1 Characteristics of IoT

In addition to traditional cybersecurity risks, IoT environments introduce distinct challenges. These systems rely on large numbers of distributed sensing devices with limited direct oversight and operate at significant scale and density.

Within the IoT architecture, security threats are typically categorized into three layers: perception, transport, and application.

Perception-Layer Threats

- Physical attack

Remotely deployed IoT assets without adequate physical security controls are vulnerable to theft, tampering, and damage. External interfaces may be exposed without proper protection, allowing attackers with physical proximity to gain direct access.

IoT devices installed outdoors or in distributed environments, without proper management and physical safeguards, are particularly vulnerable to physical attacks, tampering, and counterfeiting.

- Data leakage

The lack of encryption or access control during data collection and processing by IoT devices causes sensitive information leakage.

- Unauthorized access

IoT devices lack effective authentication mechanisms, such as relying on factory default credentials and weak passwords, or having design flaws in authentication protocols that can be bypassed. Retained debug interfaces allow attackers to obtain device operation information.

- Unauthorized update

The update verification mechanism of IoT devices is not robust, which allows attackers to install non-official firmware packages containing vulnerabilities or malicious files into the devices.

- Outdated components

IoT devices come with built-in components that have known vulnerabilities or are outdated; since outdated components are no longer maintained, they pose significant security risks.

- Malicious software

Due to performance limitations, IoT devices lack security software protection and are easily infected by malicious software, which affects their normal operation.

Transport-Layer Threats

- Cyberattack

Defects in network protocols themselves, such as the lack of effective authentication, may lead to leaks on the access side.

Unencrypted communication processes are susceptible to Man-in-the-Middle attacks such as hijacking, replay, tampering, and eavesdropping.

- Data leakage

During communication between devices, cloud platforms, and mobile applications, if encryption is not properly implemented, control commands and collected data may be exposed, allowing attackers to intercept sensitive information.

- Data tampering

When devices communicate over the network, if integrity verification mechanisms are absent or insufficient, attackers may alter control commands and collected data in transit.

Application-Layer Threats

- Device management

There are challenges in managing the update process and the security of the numerous devices managed by the application-layer.

- Unauthorized access

Imperfect authorization (rights) management at the application layer may lead to unauthorized access, resulting in the risk of data leakage.

- System vulnerabilities

IoT device application software or operating systems may contain design or implementation flaws that can be exploited by attackers. If successfully exploited, these vulnerabilities may allow unauthorized access, execution of malicious code, or disruption of normal device operation.

- Data leakage

The application layer manages a large volume of data, which is prone to leakage if not encrypted or if access controls are inadequate.

- Outdated components

The application layer uses components with known vulnerabilities or outdated components. If not updated in a timely manner, these components may be exploited by attackers.

- AI model adversarial attacks

Attackers may manipulate AI model inputs by introducing small, targeted changes that cause incorrect decisions. For example, subtle modifications to image data can result in misclassification in image recognition models.

- AI model hallucination

During the content generation process, AI models may generate false information that appears logically consistent but is completely inconsistent with objective facts.

- Abuse of AI-generated false information

AI technology may be used to generate false audio and video content, with typical methods including face replacement and voice mimicry. Such technologies have triggered security issues such as telecommunications fraud and spoofing face authentication systems.

- Configuration vulnerabilities

Improper configuration of applications, frameworks, containers, and operating systems can introduce security vulnerabilities. Practices such as employing versions with security flaws, assigning excessive permissions to specific accounts, and neglecting access control over sensitive resources, may allow attackers to illegally obtain critical data.

To address these threats, Hikvision has established and continues to evolve a video-centric IoT security architecture. This multi-layered framework is designed to strengthen terminal, data, application, and network security, along with personal information protection and compliance.

4. Network and Information Security in the Security Industry

The development of the security industry has progressed through an initial analog phase followed by a digital phase. During the analog era, security systems operated within private networks, so the industry focused more on product cost, performance, and ease of use. Due to the characteristics of systems at that time, security was not a primary design focus. However, with the rapid advancement of networking in the security industry, the sector transitioned directly from the original analog mode to IP digitalization. During this transition, security was not consistently prioritized across the industry, and design approaches from the analog era did not always align with modern information security practices. To facilitate users in integrating devices from multiple manufacturers with a single click, the security industry generally defaults to enabling all supported protocols, allowing the server to automatically match and connect using whichever protocol is supported. While this design improves ease of use, it does not align with cybersecurity best practices.

These challenges reflect the industry's evolution in recent years, but do not indicate broad vulnerability. The industry has recognized these risks and continues to address them.

Cybersecurity is not unique to the security industry—it is a shared challenge across all sectors. These risks are widespread across today's IT landscape, and several fundamental principles have emerged.

- The Common Occurrence of Security Vulnerabilities

There is no such thing as an IT system or product with no security vulnerabilities. In fact, security vulnerabilities are very common. In products composed of millions of lines of code, a single incorrect parameter setting or the reversed order of two lines of code can lead to a system vulnerability. Currently, it is impossible to detect all potential security issues through automated or manual techniques. Therefore, security issues may arise across all manufacturers.

- Security for the Entire System

The security of any system cannot be guaranteed by securing a single point; the entire system must be secured. To ensure the security of a video security system, collaboration and supplementation among various components are necessary. This includes front-end and

back-end devices, platform systems, network equipment, security devices, and more. By establishing a multi-layered defense system, or "defense in depth," the overall system's security can be ensured. A failure in any single link can lead to the system being compromised. But if implemented correctly, it's very hard for attackers to achieve their goal.

- Security of Third-Party Open Source Software

Currently, various third-party open-source software is widely utilized in different systems. These software solutions come with attributes like openness, sharing, and freedom, and they play an increasingly crucial role in software development. They are also a significant part of the software supply chain. While businesses benefit from the convenience provided by open-source software, they also assume substantial security risks. In recent years, open-source software has frequently revealed high-risk vulnerabilities, such as Struts2, OpenSSL, Fastjson, and so on. Since many of these components are deeply integrated into the underlying infrastructure of information systems and are used extensively, the security risks posed by these vulnerabilities are far-reaching. They often evolve into "generic" vulnerabilities that can potentially affect entire industry sectors or a company's product lines.

- Security in Dynamic Balance

There is no such thing as "absolute" security; all security is relative. The perpetual game of offense and defense is a dynamic balance, where advancements on one side can counter gains made on the other. Mechanisms and methods deemed secure today might be vulnerable tomorrow. Likewise, attackers might compromise products considered "secure" today by tomorrow. As a result, security is an ongoing process with no definitive endpoint. Throughout its lifecycle, any product will consistently face information security challenges and risks. The uncertainty lies in whether these risks will materialize and when they might arise, making it difficult to predict in advance.

- Product Security Management

Effective system security depends on proper security management. Even technically secure systems may be exposed to risk if they are not configured, operated, and maintained appropriately.

Some security issues arise from misconfiguration, weak credential practices, or the absence of appropriate network protections. For example, the use of weak passwords or the lack of firewalls and boundary protections can increase exposure to risk.

Users play an important role in maintaining system security by following established best practices, including monitoring security advisories, applying firmware updates, and installing patches in a timely manner.

5. Hikvision Security Development Maturity Model

With our extensive research and development efforts, and drawing on industry best security practices—such as OpenSAMM, BSIMM, CSDL, MSDL—as well as customer feedback, we have established the Hikvision Security Development Maturity Model (HSDMM). By quantifying the security activities in product security development, this model integrates a comprehensive organizational structure, well-defined security development management processes, and robust technical measures to ensure the effective implementation of security activities. This, in turn, enhances product confidentiality, integrity, and availability, while strengthening personal data protection, ultimately providing customers with safer products and solutions. In subsequent section of the paper, we will walk you through the HSDMM across three dimensions: security governance, security processes, and security technologies.

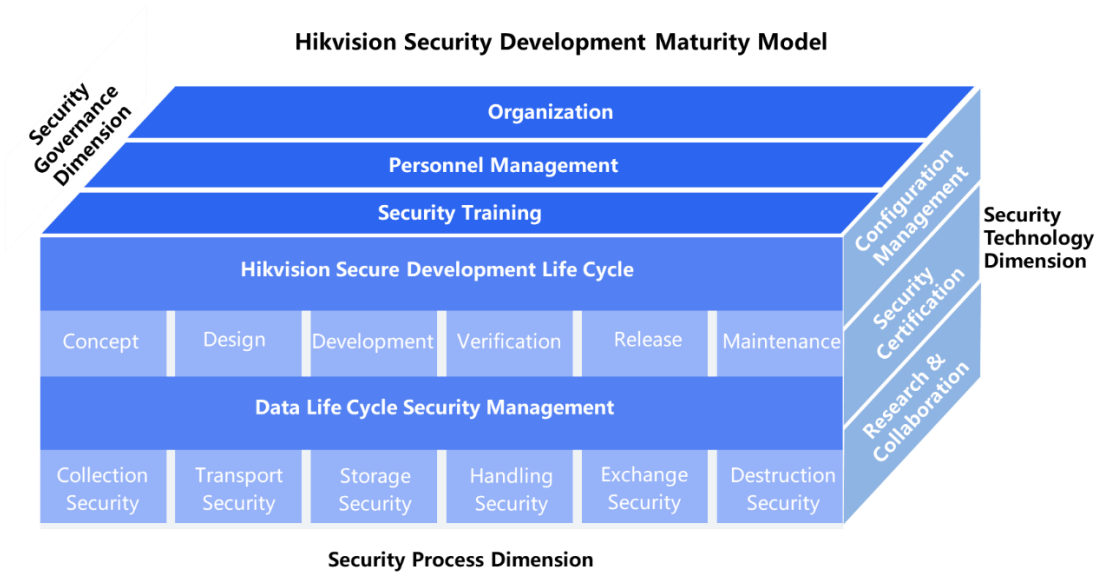


Figure 5-1 Hikvision Security Development Maturity Model

6. Security Governance

6.1 Organization

To ensure that Hikvision product development incorporates security into every phase—including R&D, supply chain, marketing and sales, project delivery and technical service—we first need to establish an organizational structure that can guarantee its implementation and assign clear responsibilities to each group.

The security organizational structure of Hikvision is as follows:

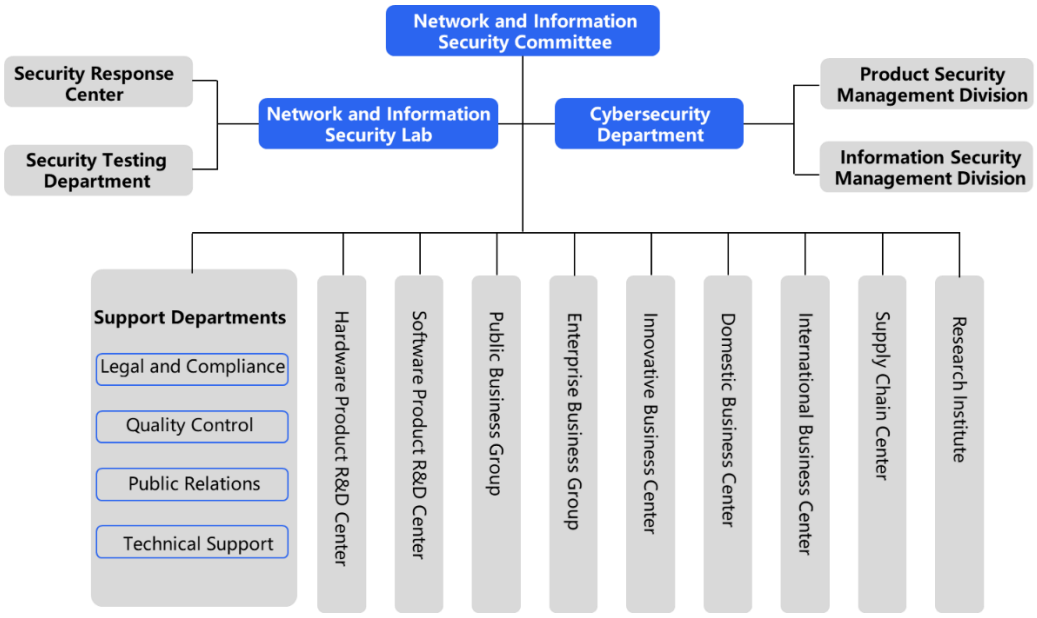


Figure 6-1 Hikvision Security Organization Structure

Network and Information Security Committee

Hikvision's Network and Information Security Committee is responsible for strategic planning and policy making for network and information security. If any conflict or serious issue arises, the committee has the authority to make decisions and make necessary adjustments to services. The General Manager of Hikvision acts as the head of the committee. The daily management of formulating network and information security strategies, policies, procedures, and standards, as well as resource allocation on a daily basis, is handled by the Cybersecurity Department, a permanent specialized body under the committee.

Cybersecurity Department

As a standing body of the Network and Information Security Committee, the Cybersecurity Department is responsible for implementing the product security strategies, establishing the product security baselines, and conducting product security assessments. The department also promotes external collaborations related to product security, conducts research into product security technical standards of the industry, advances product security research and development, participates in major project reviews of product security, and provides recommendations for leadership decisions. It is also responsible for aligning the company's product security strategy with industry requirements, establishing research and development specifications, embedding security elements into the product research and development process, and promoting its implementation in product lines.

Network and Information Security Laboratory

The Network and Information Security Laboratory is dedicated to the research and practice of IoT-related security technologies. It mainly covers areas such as IoT perception, product security components, video security products, penetration testing and IoT security protection. The laboratory aims to research the cutting-edge of IoT security technology and promote its improvement. All laboratory staff have extensive experience in information security, and many of them have obtained industry-recognized certifications, including Certified Information Security Professional (CISP) or Certified Information Systems Security Professional (CISSP) certification.

Security Response Center

The Hikvision Security Response Center (HSRC) is a platform responsible for receiving, addressing, and publicly disclosing security vulnerabilities related to Hikvision products and solutions. It is also responsible for sharing best practices and incident response experiences with other security organizations worldwide, enhancing trusted communication and cooperation, and improving the effectiveness and timeliness of the company's response to security incidents.

Product Security Management Division

Each Hikvision product line has a product security division, which works with the Cybersecurity Department to establish product security baselines and related product technical standards.

It is responsible for implementing the relevant security requirements during product planning, R&D, and testing phases within the product line, and is responsible for the security of the product line.

Information Security Management Division

The Information Security Management division is responsible for assisting the Cybersecurity Department in implementing information security policies, procedures, standards, and processes within the company. It also assists in conducting information security monitoring, auditing, training, and awareness activities, as well as handling internal security incidents.

Security Testing Department

The Security Testing Department is a third-party body independent of the product lines, responsible for conducting product security testing for all of Hikvision's product lines. This department verifies whether the company's product security policies and baselines are effectively implemented in the products, preventing potential security issues that may arise during the research and development process, ensuring the security of the released products.

Support Departments

The Support Departments are responsible for providing support related to product security in areas such as internal control, legal compliance, quality operations, brand promotion, auditing, and public relations.

6.2 Personnel Management

Hikvision maintains a company-wide cybersecurity awareness program and promotes a strong security culture across the organization. All new employees receive cybersecurity training, supported by ongoing awareness initiatives and education campaigns. The company conduct training on cybersecurity knowledge and skills tailored to specific business needs, as well as other awareness-building activities. These include studying cybersecurity case studies relevant to the characteristics of different business domains. The company regularly promotes cybersecurity periodicals on the internal platform for all employees; at the same time, it also promotes cybersecurity education to all employees through information security promotional posters, videos/micro movies, startup reminders, etc.

Hikvision has identified cybersecurity-critical roles across its business functions, including product security. For employees in these roles, the following requirements apply:

- Employees must pass background checks prior to employment to ensure suitability for their roles. Employees in safety-critical positions are required to sign confidentiality agreements outlining their obligations.
- While on duty, job qualification standards are applied to support security awareness, maintain relevant skills, and require regular reviews.
- When an employee leaves the company, offboarding procedures require timely revocation or modification of system access, as well as the return of company assets. When an employee leaves the company, offboarding procedures require timely revocation or modification of system access, as well as the return of company assets. Offboarding procedures apply to both internal transfers and employee resignations.

Employees are accountable for their actions and the outcomes of their work, including both technical and legal responsibilities.

Employees are expected to understand that cybersecurity issues may have significant impacts on customers, organizations, and individuals. Accordingly, Hikvision takes appropriate action to maintain accountability and protect the security of its systems and products.

6.3 Security Training

Drawing on industry best practices, Hikvision established a comprehensive cybersecurity training system. The stages incorporate various forms of training such as employee onboarding, job placement, and promotions, enhancing employees' security capabilities. Coupled with the company's well-developed security research and development management processes, this ensures the delivery of secure and compliant products and services to customers.

Cybersecurity capability certification for product R&D positions: To enhance employees' awareness of cybersecurity, improve their cybersecurity capabilities, and elevate the security quality of our products, a cybersecurity competency certification is required for employees at software research and development (R&D) positions such as technical planning demand design, solution development, code implementation, and verification testing. Employees must pass the competency certification before being eligible for job placement or applying for promotions.

Cybersecurity capability training camp: The Cybersecurity Department regularly organizes cybersecurity capability training camps to provide concentrated training for the core security personnel. The training encompasses areas such as cybersecurity standards, certification, product security design, practical threat modeling, and product security management. This continuous effort enhances the security capabilities of core personnel and empowers them to better support their respective teams, ultimately elevating the security competence of all employees.

Special cybersecurity activities: Hikvision conducts targeted, practice-oriented programs to strengthen the knowledge and skills of employees in key cybersecurity roles. Examples include Cybersecurity Promotion Week, expert lectures, cybersecurity forums, and a case library.

7. Security Process

7.1 Hikvision Security Development Life Cycle

Product security and personal data protection rely on processes and systems for protection. Hikvision has developed the Hikvision Security Development Life Cycle (HSDLC), which deeply integrates product security requirements with the company's research and development process, and has formulated clear security requirements from concept, design, development, verification, release, and maintenance stages to ensure the safety and quality of our products.

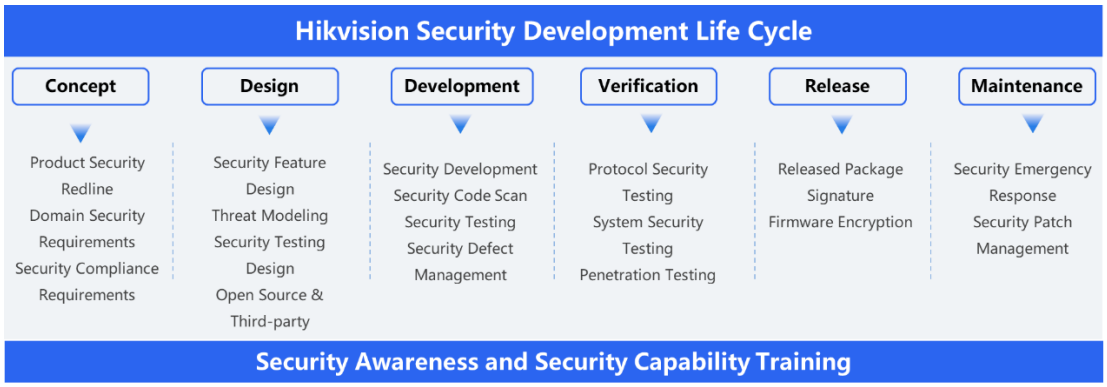


Figure 7-1 Hikvision Security Development Life Cycle

Concept Stage

During the concept stage, there are three key considerations when analyzing product security requirements:

1. The product security redlines are mandated in the requirement list. Redlines represent the fundamental requirements that ensure the security objectives or minimize risks to acceptable levels. These requirements stem from laws, regulations, government mandates, client admissions, industry standards, and more. They aim to ensure product security compliance, safeguard sensitive user data, enhance system access control, and bolster the system's resistance to attacks.

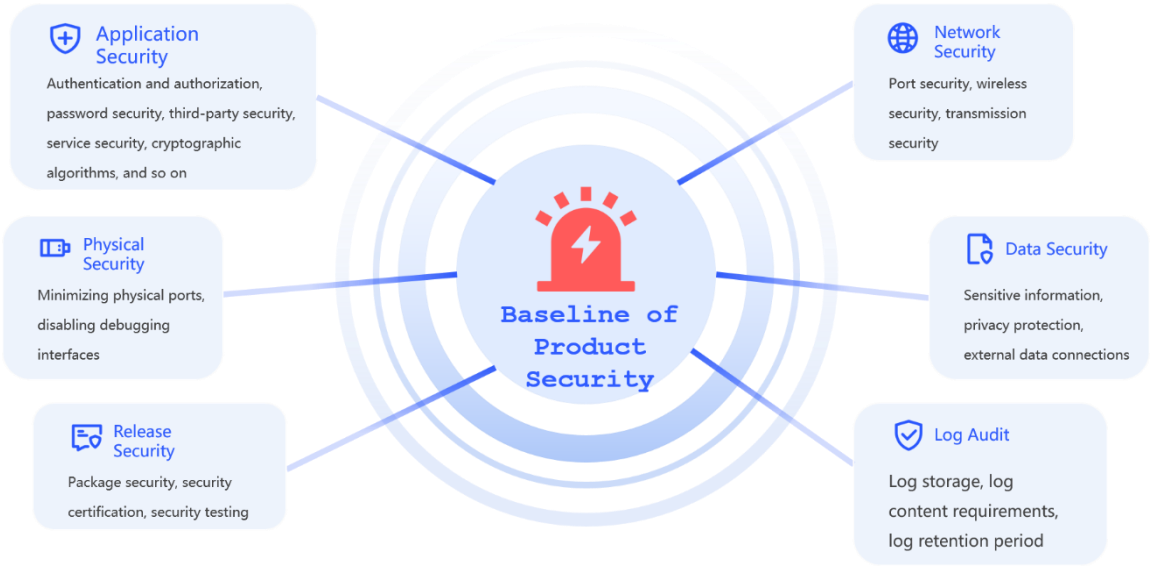


Figure 7-2 Baseline of Product Security

2. If a product involves personal data, the team will identify and assess the types of data required during the conceptual stage, in alignment with applicable data protection and privacy regulations.

3. A threat analysis of the product's future usage scenarios is conducted to identify targeted security requirements. The analysis involves identifying all potential threat sources, types, and attack vectors specific to the product's usage scenarios. This helps us assess risks and ensures that the product requirement list incorporates relevant response and preventive measures.

Design Stage

Threat modeling is a crucial structured approach utilized in the product design phase. Using abstract methods, it helps to identify, quantify, and address security risks associated with the product. The purpose of threat modeling is to identify potential system threats early on, and establish appropriate response measures. By identifying security issues and clarifying security requirements during the design phase, we can avoid risks during coding, effectively control product security risks and reduce the cost of remediation.

Hikvision requires that all baseline versions of new projects undergo threat modeling, and the Cybersecurity Department will review the threat modeling files through auditing:

1. Based on the logical architecture of the product, threat-modeling methods are used to identify potential security threats at the architecture level and develop corresponding mitigation measures.

2. Security design and functional design are integrated together. When conducting functional design, we also establish threat modeling at a functional level to recognize security threats in the design in a timely manner and implement mitigation measures accordingly.

3. We conduct detailed analysis and design of collected or identified security requirements, with dedicated cybersecurity engineers providing professional technical support throughout the product security design process.

4. For residual high risks in threat modeling, attack path analysis will be provided.

5. In the design stage, analysis on attack surface minimization will be conducted for all products to reduce overall product security risk.

Hikvision follows the HSDLC process to ensure that product functional design and safety design are synchronized, which can better balance safety and functional efficiency. Based on industry-wide design principles and the specific scenarios of our main products, Hikvision has summarized six key principles: attack surface minimization, minimal privilege, default distrust, open design, default security and defense in depth.

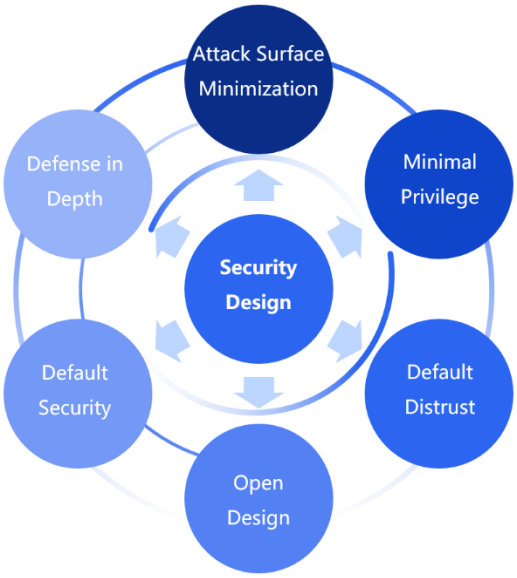


Figure 7-3 Security Design Principles

Large models technology provides revolutionary solutions for threat modeling. By leveraging natural language processing and image recognition technologies, large models can automatically parse text and flowchart information from design documents to accurately identify system assets, data flow paths, and potential attack surfaces. Compared to traditional manual modeling approaches, these models can complete semantic analysis of hundred-page documents within minutes. By integrating industry vulnerability knowledge bases such as CWE and CAPEC, they automatically generate threat model reports containing attack trees, mitigation strategies, and risk ratings, which are reviewed and validated by qualified security engineers prior to adoption.

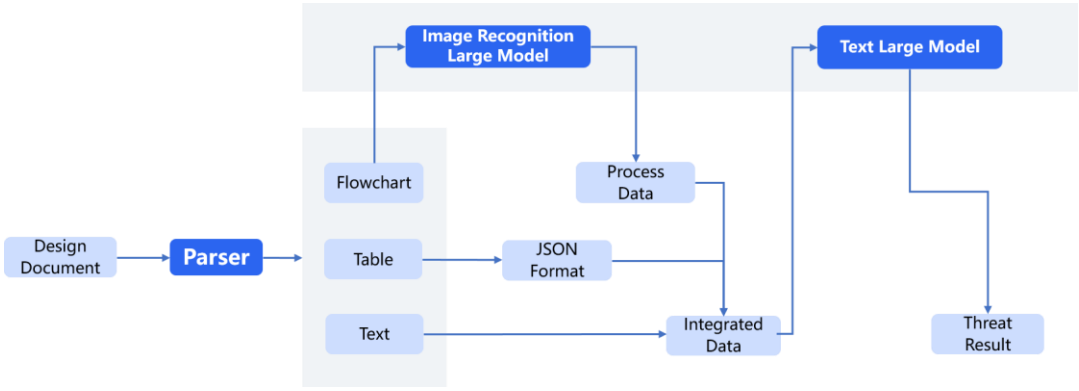


Figure 7-4 Threat Modeling Based on Multimodal Large Language Models

Development Stage

Hikvision requires R&D personnel to follow secure coding standards and conduct peer reviews during the development process. Through self-developed source code-scanning platforms, code defects can be checked to quickly and accurately identify dangerous functions and defect issues in high complexity codes, reduce code security defect rates, and identify areas that require further inspection. Through self-developed code defect, analysis and scanning tools, known defects can be identified through code features, and R&D personnel can be informed of defects in various branches. The synchronization of defects is evaluated to ensure they are in place, and defects are intercepted during continuous construction activities to control known code problems in the source code stage, greatly reducing repair costs.

Large models break through the detection boundaries of traditional tools. With semantic understanding capabilities trained on massive open-source code, they can deeply comprehend code logic. Their context-aware features intelligently identify complex defects that are difficult for conventional tools to detect, such as weak implementations of encryption

algorithms and logic bypasses in permission controls, significantly enhancing the security coding quality of development teams.

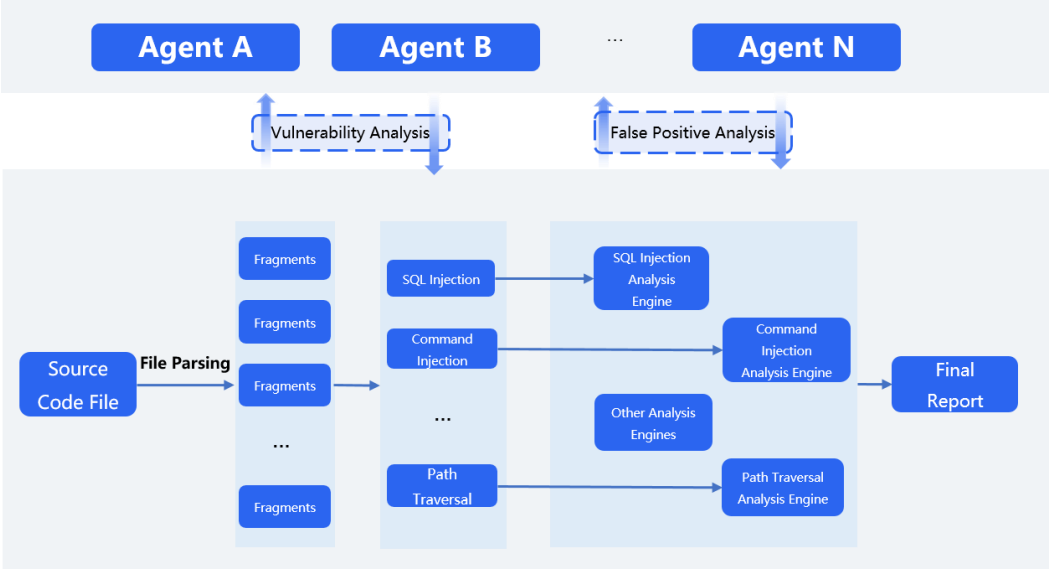


Figure 7-5 Code Audit Based on Large Language Models

Verification Stage

In order to ensure the security of Hikvision products and prevent various security issues that may occur during the development process, we conduct comprehensive security tests at every stage of product development:

- Strengthen protocol security testing by conducting network protocol security, robustness and reliability analysis on all products.
- Introduce vulnerability-scanning tools in system security testing, and timely track vulnerability database updates to comprehensively identify various issues in the product, including general vulnerabilities, configuration issues, and flaws within application systems.
- Introduce dynamic application security testing tools in application security testing to discover Web application vulnerabilities.
- Conduct App security compliance testing to meet various security, personal data, and compliance requirements.
- Use multiple mainstream antivirus software to detect known viruses, Trojan horses, and

other malicious code before product release.

- Interactive Application Security Testing (IAST) utilizes a proxy server to capture and simulate the request traffic. By configuring JVM parameters to load the monitoring program's JAR package, it monitors all server-side instructions in real time. It transparently tracks the flow of the testing script in memory and offers the advantages of high efficiency, low false positives, and clear alerts (including call stacks, final executed commands, and other information) compared to traditional black-box testing tools, greatly facilitating developers to locate and fix security issues.

- The company conducts penetration tests on products regularly to minimize business risks and keep security risks within a controllable range.

- The company's product security specialists analyze newly found vulnerabilities during product testing on a quarterly basis, compile a list of typical common security issues, and then deliver it to each product line for self-inspection to prevent similar problems from recurring.

Release Stage

Before the product release, Hikvision develops a security test plan and strategy according to the product design stage. The test methods include functional security test, adversarial security test, fuzzing, penetration test, static source code review, and virus scanning through the company's self-developed security testing platform. The Cybersecurity Department and the Testing Department conduct a comprehensive security assessment.

Hikvision's product R&D management platform digitally signs the product release packages to ensure their source and integrity are verified, effectively preventing unauthorized software packages.

Maintenance Stage

The technical support team provides services to customers and may require access to certain customer information with proper authorization. Personnel are required to complete relevant network and information security training to support the secure handling of customer data and reduce risks related to access control, communication security, and personal data protection.

Hikvision has established Technical Support On-Site Service Standards, which define requirements for employee conduct, personal safety, and information security.

Hikvision strictly manages employees who can access customer networks and signs commitment letters with these employees, detailing their roles, responsibilities, and potential legal liabilities. They are required to learn cybersecurity knowledge, as well as take and pass relevant exams.

7.2 Vulnerability Management

Hikvision has systematically built a sustainable and trustworthy vulnerability management system across multiple dimensions, including policies, organization, processes, technologies, and standards. Embracing an open and collaborative philosophy, Hikvision works closely with stakeholders such as supply chain partners, security researchers, and regulatory bodies to address security challenges collectively.

Guided by this approach, Hikvision has established five fundamental principles for vulnerability management, defining five key stages of the vulnerability lifecycle and corresponding behavioral guidelines. These principles comprehensively direct various business departments in conducting orderly vulnerability management activities, continuously enhancing the security and trustworthiness of products and services.

Emergency Response

Hikvision has established the Hikvision Security Response Center (HSRC), which is responsible for receiving, handling, disclosing, and resolving security vulnerability related to Hikvision's products and solutions. Responsibilities include:

- Responding to and handling security incidents submitted by customers.
- Responding to and handling security incidents reported by external organizations.
- Formulating the company's security incident management strategies and handling procedures.
- Analyzing the vulnerability advisories and security patches released by system software providers and security organizations.

The company also specifies each department's responsibilities and the procedures for managing product security incidents to ensure the quality and efficiency of security incident management. The Security Response Center's management guidelines covers the entire pre-sales, sales, and after-sales processes of product security, including security-related communication with customers, cooperation with security organizations, emergency response management, security advisory releases, and the implementation of legal compliance.

Hikvision is a member of CNCERT Cybersecurity Emergency Response Technical Support Units. The company actively collaborates with global security organizations to share best practices and incident response experience, foster trusted communication and cooperation while improving the effectiveness and timeliness of its cybersecurity incident response.

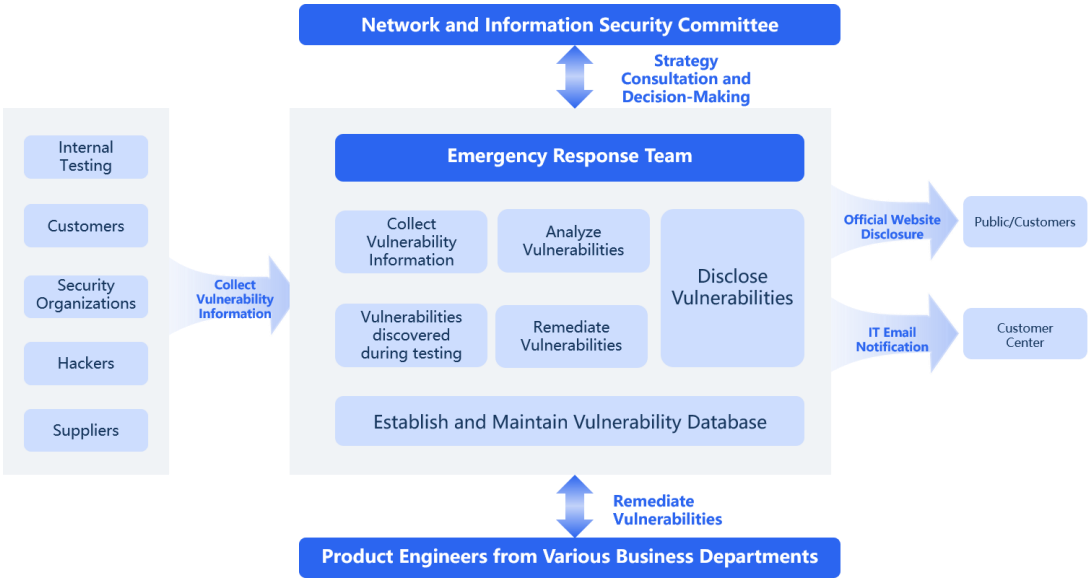


Figure 7-6 Security Emergency Response

Core Principles of Vulnerability Management

The five core principles of vulnerability management are as follows:

- **Prevent Risks, Safeguard Security**

  Commit to reducing or eliminating actual harm caused by product and service vulnerabilities to customers, while mitigating potential security threats.

- **Strengthen Defenses, Minimize Hidden Risks**

  Enhance the protective capabilities of products and services to effectively reduce the exploitability of vulnerabilities.

- **Proactive Accountability, Clear Boundaries**

  Identify responsibilities within vulnerability management, clarify compliance requirements (such as regulations, contracts, and industry standards), and establish systematic management mechanisms for proactive control.

- **Iterative Optimization, Pursue Excellence**

  Continuously improve vulnerability management processes and standards, incorporate industry best practices, and drive the maturity of management capabilities.

- **Open Collaboration, Build an Ecosystem**

  Foster open collaboration with supply chain partners, security researchers, institutions, and other stakeholders to deepen cooperative efforts in vulnerability governance and build a trusted security community.

Key Stages of Vulnerability Handling

Hikvision has established a product security vulnerability handling and warning disclosure process based on the Regulations on the Management of Network Product Security Vulnerabilities, ISO/IEC 30111, ISO/IEC 29147, etc., which includes five stages:

Figure 7-7 Vulnerability Handling Process

- Vulnerability research and collection: We obtain vulnerability information through customers, external CERTs, security researchers or related security websites. At the same time, we continue to discover potential security threats through our internal team. Hikvision supports a responsible vulnerability disclosure and handling process, and respects the research results of every security researcher. External vulnerability discoverers should allow manufacturers a reasonable and coordinated period to process and solve problems before public disclosure.

- Vulnerability assessment, analysis and verification: Whether it is a suspected vulnerability or a confirmed one, the HSRC team will work with the product teams to complete the assessment of the vulnerability's authenticity and related risks quickly.

- Tracking and resolution: Once the vulnerability is confirmed, HSRC team will immediately notify the vulnerability submitter, actively track and provide feedback on the remediation progress, and investigate the vulnerability to ensure that the problem is resolved in all product versions and product models. The HSRC process is deeply integrated with the R&D core process to ensure a timely response to vulnerabilities.

At all stages of the process, protecting the confidentiality of customer and vulnerability information is critical to Hikvision. If vulnerability information falls into the hands of malicious actors before patches or mitigation information are publicly released, it could allow threat

actors to exploit vulnerabilities on unpatched systems. Therefore, all parties must maintain strict confidentiality throughout the vulnerability disclosure process.

HSRC team actively participates in industry and public activities, and establishes long-term relationships with CERTs, vulnerability disclosure platforms, customer SRCs, suppliers, researchers, and third-party coordinating agencies. Hikvision is a recognized CVE Numbering Authority (CNA) participant of the Common Vulnerabilities and Exposures (CVE) program, and maintains partnerships with vulnerability databases and information-sharing platforms such as CNNVD, CNVD, NVDB and CICSVD. Through these collaborations, Hikvision can obtain information on newly discovered vulnerabilities in a timely manner, significantly improving its security incident response capabilities and delivering more secure products and solutions to customers.

7.3 Data Life Cycle Security Management

Data Classification and Grading

Hikvision has established the Information Asset Security Management Procedure, pursuant to which data is classified and graded. Classification involves categorizing data based on its source, content, and purpose; grading entails defining sensitivity levels based on the data's importance and sensitivity, as well as the varying degrees of harm that may result from data security incidents. Data is categorized into five grades. For different grades of data, distinct management and usage strategies are formulated in accordance with the requirements of the Data Classification and Grading Management Specification. Differentiated technical controls are adopted to ensure that technical means and management measures satisfy the security requirements of data processing activities, thereby preventing insufficient protection of sensitive data. Hikvision prioritizes the protection of important data such as personal information and implements strict protection for core data.

Hikvision has developed a company-level data governance platform and an information asset management system to implement unified and standardized data management across the entire company, including R&D data. The system provides explicit definitions, classifications, and grading for various types of data involved in products. This facilitates product R&D teams in querying the grade of data associated with their products, thereby aligning data grading standards and protection levels across all product R&D teams company-wide.

Data Lifecycle Security Management

The company's product and service teams must consider personal information protection during the requirements analysis and design phases. Based on specific business usage scenarios, appropriate technical and managerial measures must be adopted to ensure the security of personal data. For instance, when Hikvision handles personal information, corresponding product interfaces provide a Product Personal Information Statement detailing all types of personal data involved, their purposes, processing methods, retention periods, risks, and recommendations. In particular, Hikvision's cloud services provide users with a Personal Privacy Statement that outlines security management measures for personal information throughout the entire data lifecycle.

Personal data subjects possess rights including the right to be informed, the right of access, the right to rectification, the right to erasure (the right to be forgotten), the right to restrict processing, the right to data portability, the right to object, and the right not to be subject to automated decision-making. To ensure compliance and better protect users' personal information security, product and service design and implementation must incorporate functionalities that support the exercise of these rights by personal data subjects.

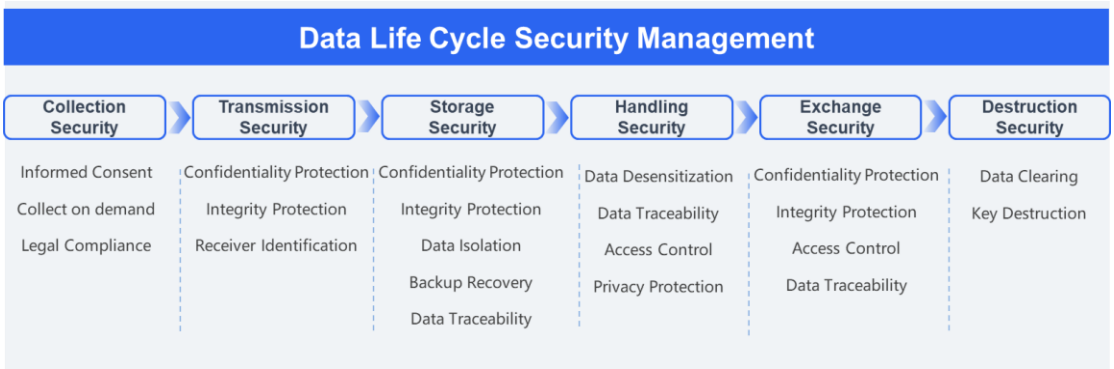


Figure 7-8 Data Lifecycle Security Management

1. Data Collection Security

Compliance with the applicable laws and regulations is mandatory for data collection. Users must be informed, and principles such as user consent and data minimization should be followed. The personal privacy policy should specify that data collection is limited to what is necessary and clearly define the scope and purposes for its use. When users engage with services or products that involve personal data, such as using Hikvision cloud services or IoT devices, Hikvision will inform users of the scope and purposes of data collection in accordance with applicable laws and regulations. Personal data will be collected only upon obtaining user consent.

2. Data Transmission Security

When transmitting collected data, it is crucial to authenticate the identities of both communication parties to ensure that the entity receiving or sending data is a legitimate user. This process primarily relies on cryptographic techniques like message digests and digital signatures. During transmission, it is essential to prevent data leakage and promptly detect any tampering, which primarily relies on traditional cryptographic algorithms such as encryption, hashing, and digital signatures. For Hikvision products, transmission security is ensured by utilizing the SSL/TLS protocol to guarantee the confidentiality and integrity of the data.

3. Data Storage Security

The data storage process involves segregating data based on different levels of sensitivity. This can be achieved through techniques such as physical isolation, logical isolation, or virtualization to create separation between areas containing data of different security levels.

To mitigate potential hardware malfunctions or data loss and ensure data availability, redundancy mechanisms are employed to back up the data. When the data storage media becomes available again, data recovery and restoration are carried out to bring the data back to its original state.

After data is stored, it is important to establish data traceability mechanisms. This ensures that if data is illicitly leaked, it can still be traced, allowing identification of the leak source

and enabling relevant audits. Digital watermarking technologies are utilized to achieve data traceability in such cases.

When storing data, it is also essential to ensure data confidentiality and integrity. This means that even if attackers manage to access the data, they should not be able to retrieve meaningful information, and any unauthorized modifications should be detectable. Traditional cryptographic techniques such as encryption, hashing, and digital signatures can be used to safeguard data from unauthorized access and tampering.

Hikvision products ensure data confidentiality and integrity by employing standard cryptographic algorithms. The cryptographic algorithm calculation module provided by the vendor utilizes cryptographic cards that comply with commercial cryptography specifications. Algorithms and implementations are selected in accordance with applicable local standards and regional regulatory requirements.

4. Data Processing Security

When processing and computing data, it is essential to ensure that users have the corresponding permissions. When data is used, sensitive information should be masked based on business relevance and the principle of least privilege. In data calculations, it is crucial to prevent the extraction of additional personal information from intermediate results. Privacy-preserving technologies such as secure multi-party computation, homomorphic encryption, and differential privacy computing can be employed to protect personal information during data usage. Hikvision employs techniques such as data masking, encryption, and privacy-preserving computing to safeguard personal information during data processing.

5. Data Exchange Security

Security controls on data exchange channels are necessary for data transmission and sharing, with measures such as mandatory identity authentication and strict access control. Data watermarking and other methods are used for traceability in the process of data exchange. Hikvision adopts cryptographic technologies to ensure data confidentiality, integrity and access control, and employs digital watermarking technology for data traceability when interacting with data.

6. Data Destruction Security

Logical deletion and physical destruction are employed for data destruction to prevent the

data, especially sensitive data such as passwords and keys, from being recovered or retrieved after erasure.

Personal Information Security Management Requirements for Cloud Products

Hikvision's internet business data is stored in the cloud. The security of Hikvision's cloud data adheres to the following data protection requirements at each stage of the data security lifecycle:

1. Cloud Data Collection

We clarify the purpose, scope, and legal basis for data collection. For all business data, identification, classification, grading, and privacy impact assessments are conducted. We also follow the principles of data minimization, obtain user consent, standardize data collection practices, and explicitly declare data collection details in the privacy policy. Additionally, the cloud performs legality checks on collected data, verifies their sources, and maintains collection records.

2. Cloud Data Transmission

To ensure channel and content security during data transmission, the transport layer employs SSL/TLS protocols to secure data transmission channels. Additionally, data in transit is encrypted using a Key Management Service (KMS).

3. Cloud Data Storage

Hikvision enforces comprehensive requirements for data encryption, digital watermarking, audit logs, and disaster recovery. For cloud storage, we the company implement multi-layered encryption strategies, including field-level encryption, by integrating Key Management Service (KMS) and Hardware Security Modules (HSM). Depending on business needs, we may also anonymize or de-identify data. We ensure the confidentiality, integrity, and availability of stored data through regular key rotation, audit log recording, and disaster recovery mechanisms (such as data backup and restoration).

4. Cloud Data Usage

Strict requirements govern data access control, data masking, digital watermarking, permission management, and audit logs. Access to data is securely managed through identity authentication, permission assignment, and the principle of least privilege. Data is subjected to dynamic or static masking, and digital watermarking is applied for traceability. Additionally, the system records operation logs for sensitive personal information to ensure compliance and facilitate anomaly detection.

5. Cloud Data Destruction

Clear data retention periods and destruction mechanisms are established. The minimum retention periods are determined based on privacy impact assessments and legal requirements. Once this period expires, the cloud platform securely destroys the data via physical deletion, anonymization, or masking. Furthermore, upon user account cancellation, all associated user data is securely destroyed in compliance with relevant regulatory standards.

7.4 Open Source Software Security Governance

Hikvision has established a comprehensive management system of open source compliance. By integrating resources from the Cybersecurity Department, Legal and Compliance Department, Quality Management Department, and R&D teams through standardized processes, technical tools, and organizational support, Hikvision has formed an Open Source Compliance Team and developed corresponding management specifications. This system is deeply integrated into the secure development lifecycle, creating a closed-loop management mechanism covering the entire process: pre-admission prevention, ongoing management, and post-incident response. This ensures the security and compliance of all open source software used by the company. Through this governance system, three core objectives are achieved:

- Security and Controllability: Mitigate risks to devices and data arising from firmware vulnerabilities, supply chain attacks, and malicious components;

- Compliance and Adaptability: Address legal risks such as open source license reciprocity and intellectual property infringement, ensuring component usage is compatible with business models and license types;
- Efficiency and Collaboration: Standardize the processes for component selection, introduction, and maintenance, reducing redundant development and version conflicts, thereby supporting the stable operation of IoT devices throughout their entire lifecycle from R&D to end-of-life.

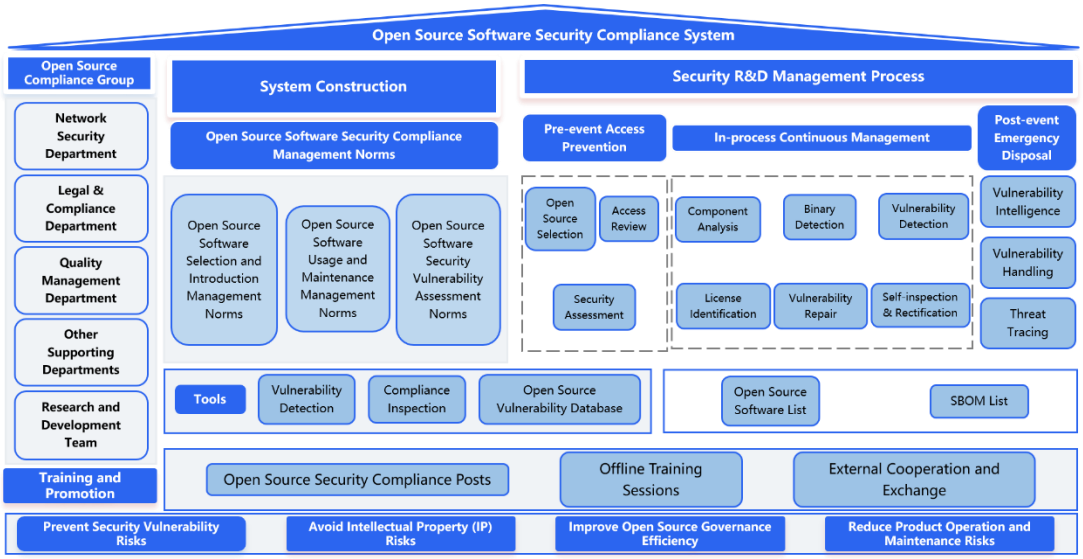


Figure 7-9 Open Source Software Security Compliance System

Hikvision's governance system of open source software is deeply integrated into the secure development lifecycle. In accordance with the company's management specifications and leveraging its self-developed software management platform, Hikvision exercises comprehensive control over the usage and release of open source software throughout the project development process:

- Requirements Phase: Define the project's open source compliance plan and identify the requirements for introducing open source software;
- Design Phase: Create an open source configuration table and complete the application process for any open source software not yet introduced;
- Development Phase: Finalize the open source configuration table, replace prohibited software, and fix open source components with security vulnerabilities;

- Verification Phase: Conduct compliance and security testing on the open source software used to ensure it meets specifications;

- Release Phase: Generate and publish the Software Bill of Materials (SBOM) and declaration documents for open source licenses.

8 Security Technology

8.1 Configuration Management

Configuration management is a critical activity to ensure product integrity, consistency, and traceability. Through processes such as configuration management strategy and planning, baseline management, configuration item management, configuration activity reporting, configuration auditing, build management, release management, version management, component management, and repository management, Hikvision ensures the integrity of delivered products while managing the open-source and third party components involved in the process. The configuration management process is an integral part of the Integrated Product Development (IPD) process. The aforementioned configuration management activities take place across different stages of the IPD process, achieving product traceability.

Build Management Specifications

Build management specifications include three parts: build resource management, build process management, and build process optimization. The segregation of duties is an important part of configuration management. The specifications must clearly define the activities, roles, and responsibilities during the build process. In alignment with different stages of product development, the life cycle of the build process should be clearly incorporated into the IPD process.

Compiling and Build Center

To ensure the repeatability and consistency of the construction process, Hikvision has established a Compiling and Build Center. In addition to meeting the management requirements of compilation, the center enforces strict admission standards control for all hardware, compilation tools, third-party software, data sources, and operating systems. As a

comprehensive solution for product compilation and build, the center supports software build activities throughout the IPD process.

Standardization of the Build Process: Through unified tool management, standardized build scripts, one-click building, and automated installation of the build environment, the center enables full automation of the product building process, including environment setup, code downloading, one-click compilation, packaging, static checks, automated unit testing, and system testing. These capabilities ensure replicability, reproducibility, and traceability of the product building process.

The center also features two additional functionalities: a Virus Scanning Center and a Digital Signature Center. The Virus Scanning Center operates multiple antivirus software tools simultaneously for scanning, which is integrated into the testing process. The Digital Signature Center employs key pairs stored in a key database to sign the compiled code digitally. All signing activities are strictly authorized and logged to ensure traceability throughout the entire process.

Software and Component Version Management

With its self-developed SWMS software management platform, Hikvision establishes a structured and standardized software version organizational structure. Focusing on the entire software development process, the platform aligns with software lifecycle management principles—spanning requirements, design, development, integration, testing, and release—to facilitate the intuitive display of software development processes and process data.

Furthermore, Hikvision utilizes a component-based development approach for its products, focusing on managing the lifecycle of these components. This entails component version, build, delivery, and data management. Once a component's development is complete, it undergoes component version validation. Once validation succeeds, the system submits the component to the component repository within Hikvision's proprietary SWMS software management platform. The component repository identifies information about each component package, including its name, group, version, target platform, source code, static analysis results, third-party software inclusion, and security status. Hikvision employs a methodology similar to Java's Apache Maven to manage embedded components such as C/C++ components. A component configurator, which aligns logically with the Project Object Model (POM), integrates each component, gradually assembling them into a finalized software

product. Based on the integrated information, a unified version information structure and Software Bill of Materials (SBOM) repositories are established to track component version applications. Should a security issue arises with a specific component version, developers can quickly trace back to the software versions utilizing that component, aiding in maintenance and updates. Additionally, this approach offers the ability to disable problematic component versions and provide replacements to prevent issues from spreading unnoticed.

Code Static Analysis

In the quality and security management of source code, Hikvision not only purchases industry-leading commercial static detection tools, but also develops a variety of known defect analysis and scanning tools for the company's specific business scenarios.

One of the key self-developed tools for code feature analysis is the Tailuge Intelligent Defect Analysis Platform, which can intelligently analyze the distribution of defects in the company's code warehouse, software version warehouse, order system and other systems based on the characteristics of defect codes. The system will inform R&D personnel of defects in each branch, the risk situation of each version, and even the potential impact on orders, to ensure that R&D can systematically evaluate defects and work synchronously. We have implemented a comprehensive closed-loop mechanism to ensure all defects identified by Tailuge are properly resolved. Before a new code branch is created, the source code is scanned for known defects using Tailuge. If defects are identified, relevant personnel are notified to address them promptly, including through remote remediation where applicable. For specified high-risk defects, the branch may be automatically disabled. During the code development process, if there are known defects in the code, warnings and pending remediation tasks are pushed directly to the developer's IDE (Integrated Development Environment). When the code development is completed to trigger the CI (Continuous Integration) build, Tailuge's defect scanning function will be triggered first to detect any known defects in the current branch. The scan results will inform the builders immediately. If there are specified types of high-risk defects, we will directly stop the build and require that the defects be repaired first. In addition, we have also integrated problematic version status management with PLM (Product Lifecycle Management) to realize software disabling, and link it with the production order system to

facilitate the immediate interception of high-risk defect orders.

Another self-developed static code-scanning platform supports the detection of critical vulnerabilities such as null pointer references, resource leaks, and buffer overflows, as well as capabilities like industry coding standard checks and rule orchestration. This platform integrates both analysis and management functions. It identifies various issues by analyzing source code while providing efficient issue management and remediation suggestions. Integrated with the software management platform, it performs static code analysis through continuous integration pipelines during the software development phase. This enables developers to promptly address security and quality concerns during development, efficiently manage and resolve issues within the HSDLC process, and helps R&D teams comprehensively monitor and improve code quality.

8.2 Security Certification

The global legal environment is intricate and constantly evolving, and industry regulatory requirements are becoming increasingly stringent. Particularly in the field of cybersecurity, many countries and regions have successively issued relevant laws and regulations in recent years. Notable examples include China's Cybersecurity Law, Data Security Law, and Personal Information Protection Law, as well as the EU's GDPR, NIS2 Directive, AI Act and Cyber Resilience Act. Security compliance has become a major challenge for IoT service providers. Hikvision is committed to establishing efficient internal control security systems that follow the compliance requirements of different industries, fields, and countries, while perfecting its own compliance foundation through improved policies, processes, and control activities. To support global business expansion, ensure global compliance , and promote standardized operations across various countries and regions, the company optimized its internal compliance organizational structure in 2018 and established the Compliance Department, which is responsible for building the global compliance system.

Hikvision has a team of legal professionals for the research, identification, and tracking of laws and regulations that are applicable to the company's global operations. Hikvision has also established a long-term cooperation with experienced and prestigious law firms domestically and internationally. We have a dedicated group to align the applicable laws and regulations with Hikvision's operations, identifying and mitigating legal risks across product development, manufacturing, delivery, and service, while providing compliance advice and support. We

continue to provide targeted compliance training on newly enacted regulations for new employees, mid and high-level managers, and employees in key cybersecurity roles to improve compliance awareness.

Hikvision strives to improve the overall security of its products. In addition to abiding by the applicable security regulations in the countries and regions where we operate, and referencing the best practices within the industry, the company has also established a comprehensive, sustainable, and reliable security system that involves company policy, organization, process, technology, and specifications.

Hikvision supports mainstream international standards, and contributes actively to their development. Hikvision has participated in the formulation of industrial security standards, which further open key security technologies to work with other industry experts and national standards organizations to perfect security standards related to IoT. Hikvision also cooperates with independent third-party assessment organizations and staff for fair security assessments and certification.

International Standard Certifications

By systematically securing authoritative international certifications, Hikvision has established a comprehensive assurance framework covering information security management, privacy protection, cloud computing security, vulnerability governance, data governance, and industrial cybersecurity. Anchored by the ISO/IEC 27001 Information Security Management System, the company extends its scope to privacy-focused standards (such as ISO/IEC 27701 and 29151) and cloud security-specific standards (such as CSA STAR, ISO/IEC 27017 and 27018), while reinforcing vulnerability management (ISO/IEC 29147 and 30111). Additionally, through ISO 38505 data governance certification, Hikvision has achieved closed-loop management spanning from strategic governance to technical implementation. This series of certifications demonstrates that Hikvision has deeply integrated security and privacy requirements into its business processes, continuously benchmarking against international best practices to provide trustworthy products and services to global customers.

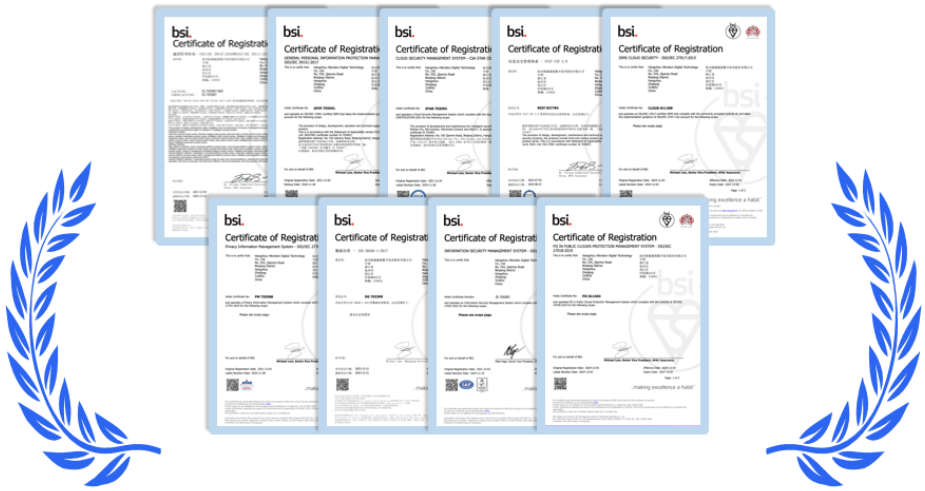


Figure 8-1 Overview of International Standard Certifications

ISO/IEC 27001

ISO/IEC 27001 Information Security Management System (ISMS) is the most authoritative, rigorous, widely accepted, and widely applied certification standard in the field of information security internationally. Acquiring this certification suggests that a company has established a scientifically effective ISMS to align its business development strategy with information security management. This ensures appropriate control and responses to information security risks. Hikvision first established its ISMS in 2012 and, after a decade of innovation and improvement, officially launched Hikvision Information Security Management System 3.0 (HISMS3.0) in 2021. Covering management requirements for cybersecurity, information security, and privacy protection, this system follows the PDCA (Plan-Do-Check-Act) continuous improvement approach, providing reliable support and assurance for Hikvision's operations.

In January 2023, Hikvision successfully obtained certification from the British Standards Institution (BSI), an internationally renowned audit organization. It marked Hikvision as one of the first companies worldwide to receive the ISO/IEC 27001:2022 certification, displaying Hikvision's management capabilities of information security as a global leader on the international stage.

ISO/IEC 27701

As the privacy extension of ISO/IEC 27001 of the Information Security Management System (ISMS), ISO/IEC 27701 is designed to assist organizations in effectively protecting and compliantly handling personal information. As the most authoritative privacy protection standard globally, it serves as an internationally recognized guide for best practices in privacy protection. The standard also offers guidance for the appropriate technical and organizational measures stipulated in the GDPR, making it an important reference and major support for privacy-related legal compliance.

Hikvision obtained the ISO/IEC 27701:2019 certification awarded by BSI in December 2021.

ISO/IEC 29151

The ISO/IEC 29151 standard addresses security concerns related to personal information in the rapidly advancing IT sector. With the protection of personal information at its core, it regulates various data operations throughout the stages of personal information collection, storage, processing, usage, and disclosure. The standard aims to strengthen the identification of risks associated with personally identifiable information, conduct accurate assessments, and implement effective control measures. ISO/IEC 29151 further enhances the security and reliability of business processes, reduces the risks associated with personally identifiable information in IT operations, and maximizes the protection of users' legal rights and societal interests.

Hikvision obtained the ISO/IEC 29151:2017 certification awarded by BSI in December 2021.

ISO/IEC 27017

ISO/IEC 27017 is a code of practice for information security controls based on ISO/IEC 27002, specifically tailored for cloud computing scenarios. It provides additional controls and implementation guidelines for both cloud service providers and cloud service customers, clarifying shared responsibility boundaries and focusing on cloud-specific risks such as virtualized resource management, cloud administrator privileges, security logging, and cross-tenant isolation. This standard assists organizations in extending their information security management systems from traditional IDCs to cloud environments when building or using cloud services.

Hikvision obtained the ISO/IEC 27017:2015 certification awarded by BSI in December 2024.

ISO/IEC 27018

ISO/IEC 27018 is a privacy extension standard specifically designed for the protection of Personally Identifiable Information (PII) in public cloud environments. Based on the ISO/IEC 29100 privacy framework and incorporating the control principles of ISO/IEC 27002, it establishes common control objectives and implementation measures for public cloud service providers acting as PII processors. It covers requirements regarding data collection, use, storage, deletion, as well as audit, transparency, and contractual terms, helping cloud services meet privacy regulations such as GDPR.

Hikvision obtained the ISO/IEC 27018:2019 certification awarded by the British Standards Institution (BSI) in December 2024.

ISO/IEC 29147

ISO/IEC 29147 is the core international standard for security vulnerability management. Focusing on vulnerability disclosure, it guides vendors on how to establish standardized mechanisms for receiving, communicating, and publishing information regarding vulnerabilities. Complementing the ISO/IEC 30111 standard, it forms a comprehensive vulnerability management system covering the entire chain of "discovery—disclosure—remediation—reporting." This helps enhance the transparency, timeliness, and traceability of an organization's response to security vulnerabilities, thereby strengthening trust with customers, partners, and the broader security community.

ISO/IEC 30111

ISO/IEC 30111 is the core international standard for security vulnerability management: focusing on vulnerability handling, it stipulates management requirements for the entire process, from vulnerability intake and validation to remediation release and risk notification.

In December 2025, Hikvision obtained the ISO/IEC 29147 and ISO/IEC 30111 certifications awarded by BSI, demonstrating alignment with international best practices in vulnerability management for product security and coordinated disclosure.

ISO 38505

ISO 38505 is a significant international standard in the field of data governance, used to guide organizations in making effective, compliant, and auditable governance decisions throughout the data lifecycle. This standard integrates data governance into the overall framework of corporate governance and IT governance, emphasizing a balance between data quality, data security, and the value realization of data assets. By clarifying governance bodies, decision-making principles, and responsibility boundaries, it helps organizations mitigate data-related compliance and operational risks while supporting business innovation.

Hikvision obtained the ISO 38505-1:2017 certification awarded by BSI in December 2023. The company has continuously maintained and expanded the scope of this certification, fully integrating data governance requirements into its data management and security management practices.

ISO 28000

Supply chain systems are characterized by a diverse range of participants, numerous procedural steps, and cross-regional product transfer, making them susceptible to internal influences and external threats. The primary security threats facing supply chain systems include unauthorized production, tampering, theft, malware and hardware implantation, as well as substandard manufacturing and development practices. Vulnerabilities within supply chain systems may not be immediately identified and can be complex to trace. As a result, supply chain–related security issues may have operational and organizational impacts if not appropriately managed.

To address manufacturing security risks and ensure the integrity of hardware and software, Hikvision implements security control measures—such as anti-tampering, anti-implantation, and anti-substitution—at critical stages of product production, including software provisioning, chip programming/verification, software loading, and production testing. These measures are designed to mitigate risks such as unauthorized hardware replacement, software implantation or tampering, and virus infection. The Product Data Management System downloads the software required for device flashing to a secure manufacturing distribution system, and the software undergoes multiple integrity verifications before being deployed.

The networks used for software flashing, loading, assembly, and testing in the supply chain are isolated from the company's office IT systems and the public internet.

Hikvision not only enhances supply chain security through technical means but also safeguards it through the establishment of management systems. The ISO 28000 Supply Chain Security Management System aims to improve supply chain security comprehensively. It assists various departments within an organization in auditing security risks and implementing controls and mitigation measures to address potential security threats in the supply chain. ISO 28000 is compatible with the ISO 9001 Quality Management System and ISO 14001 Environmental Management System, allowing an organization to integrate quality, environmental, and management systems of supply chain security.

Based on defining the supply chain operational environment, identifying threats at various stages, and conducting risk assessments and responses, Hikvision has established a Supply Chain Security Management System that fully complies with ISO 28000. Through the PDCA management cycle, the company achieves continuous improvement and refinement of the system.

Hikvision implements a secure and rigorous maintenance process to ensure product integrity throughout the process. The company records information from the entire process within its manufacturing and barcode systems, establishing detailed execution records and logs for R&D, procurement, manufacturing (i.e. chip programming, software loading, assembly, testing, etc.), warehousing, and logistics to ensure traceability.

Internationally Recognized Standard Certification

Hikvision has established a system of international standards and practices covering information security, software development, and data compliance. This system not only includes internationally authoritative certifications such as CMMI Level 5 for software maturity and IEC 62443-4-1 for industrial cybersecurity development lifecycles, but also incorporates systematic practices such as deeply integrating Privacy by Design principles into the R&D process and establishing a comprehensive vulnerability management mechanism. These efforts ensure continuous compliance with GDPR and the EU Cyber Resilience Act (CRA), supporting continuous security and compliance throughout the product lifecycle.

IEC 62443-4-1

IEC 62443-4-1 is the Secure Development Lifecycle (SDLC) requirement for product vendors within the ISA/IEC 62443 series of industrial cybersecurity standards. It covers eight practice areas: security management, security requirements specification, architectural design, secure implementation (including secure coding), verification and validation, defect management, security update management, and security guidelines. The standard emphasizes embedding security throughout the entire lifecycle of industrial and embedded products—from project inception to end-of-life (EOL)—thereby enhancing their attack resistance and maintainability within Industrial Automation and Control Systems (IACS) environments.

Hikvision obtained the IEC 62443-4-1 Secure Development Lifecycle certification in January 2025.

CMMI5 Software Maturity Certification

Capability Maturity Model Integration (CMMI) is an enterprise-level process management framework and a set of best practices used by the world's top companies. The industry recognizes it as the authoritative standard for measuring an enterprise's product and service capabilities. This process improvement method helps companies meet commercial goals, ensure quality and delivery, and boost customer satisfaction. The CMMI framework defines five maturity levels, with Level 5 being the highest.

Hikvision successfully passed CMMI5 certification in April 2016.

CSA STAR Certification

The CSA STAR Certification is a rigorous third party independent assessment of the security of a cloud service provider. It is an international certification program established by the founders of global standards, including the British Standards Institution (BSI) and the international Cloud Security Alliance (CSA), which are the world's leading organizations dedicated to defining best practices that help ensure secure cloud computing environments.

Based on ISO/IEC 27001 certification, combined with the requirements of cloud security control matrix CCM, and using the maturity model and evaluation method provided by BSI, CSA STAR conducts a comprehensive assessment of the cloud security management and technical

capabilities of the organization who provides and uses cloud computing, and finally produces an independent third-party audit result.

Hikvision achieved CSA-STAR certification in December 2021.

ETSI EN 303 645 Consumer IoT Security Standard

ETSI EN 303 645 Cybersecurity for Consumer IoT: Baseline Requirements is the first globally applicable cybersecurity standard for consumer IoT devices, released by the European Telecommunications Standards Institute (ETSI). The standard outlines over 30 mandatory requirements and several recommendations across 13 security categories, including "prohibition of universal default passwords, provision of vulnerability disclosure channels, ensuring continuous software updates, protection of sensitive security parameters, reinforcement of communication and attack surfaces, and safeguarding personal data security." It covers various connected devices such as smart cameras, home routers, smart locks, and smart appliances, providing a unified technical basis for regulations and certification schemes in multiple countries, including the UK's PSTI, Singapore's CLS, and the IECEE CB scheme.

With the inclusion of EN 303 645 into the CYBR category of the IECEE CB scheme, multiple internationally recognized testing bodies can now issue CB Type Test Reports and CB Certificates based on this standard, serving as a universal credential for market access and local certification in numerous countries worldwide.

Hikvision has proactively aligned with the security requirements of EN 303 645, implementing systematic security enhancements and testing across its front-end cameras, back-end NVRs, and cloud platform management software. As of 2025, multiple series of Hikvision's front-end network cameras, back-end NVR product lines, and the HikCentral Pro (HCP) software platform have passed cybersecurity tests conducted by international testing laboratories in accordance with EN 303 645, obtaining corresponding CB (Certification Body) Certificates. This demonstrates that the relevant products comply with internationally recognized baseline security requirements for consumer IoT in areas such as identity authentication, security configuration, firmware updates, vulnerability management, data transmission, and privacy protection, providing global users with a higher level of security and trust assurance.

General Data Protection Regulation (GDPR)

Hikvision is committed to protecting personal data and fully supports the implementation of GDPR requirements. The company has been taking multiple initiatives to safeguard personal data, including authorized data collection, minimization of data collection, data anonymization, communication and storage encryption, and data security audits.

To ensure that privacy protection is integrated into the design of products and services from the outset, Hikvision promotes the Privacy by Design (PbD) principle internally. Privacy assessment requirements are embedded at every stage, including demand analysis, architecture design, testing, and release. For business operations involving large-scale or high-risk data processing, the company conducts Data Protection Impact Assessments (DPIA) to identify and mitigate potential privacy risks.

Hikvision has formulated and implemented a series of data protection policies, established a data protection working group, and integrated GDPR requirements into its business operations, contract management, and supply chain management, continuously strengthening its capability to protect users' personal data.

Cyber Resilience Act (CRA)

In response to the European Union's Cyber Resilience Act (CRA) requirements for products with digital elements—including security by design, vulnerability management, and mandatory reporting—Hikvision has implemented lifecycle-based measures across its products. Hikvision integrates security into its development processes by incorporating requirements analysis, threat modeling, secure coding standards, SBOM management, and security testing into standard R&D workflows, gradually aligning with secure development standards such as IEC 62443-4-1. On the other hand, focusing on vulnerability management and incident response, Hikvision relies on internal vulnerability management mechanisms to standardize the processes for vulnerability intake, classification assessment, patch release, and customer notification.

Compliance with Global Standards

Hikvision continuously improves its global information security and compliance system, achieving significant results in domestic and international standards and regulations. Domestically, it has passed the Level 3 assessment of Classified Protection of Cybersecurity, ensuring that the security construction of critical information systems complies with national standards. Internationally, Hikvision systematically enhances its cybersecurity governance and risk management capabilities based on the NIST CSF 2.0 framework. The company also actively addresses regional regulations such as the UK PSTI Act and Brazil's Anatel cybersecurity requirements. Through measures such as eliminating default passwords, strengthening vulnerability management, and implementing firmware update mechanisms, Hikvision has achieved compliant market access for its products in multiple markets, establishing global security and privacy protection capabilities.

Cybersecurity Multi-Level Protection Scheme (MLPS) Certification

The Cybersecurity Multi-Level Protection Scheme is a fundamental system in China's information security guarantee, which aims to protect the development of information technology and maintain the fundamental guarantee of national information security. The security protection level of information systems is divided into five tiers. This classification depends on two main factors. First, it considers the system's importance to economic development, and social life. Second, it assesses the potential harm caused by system damage, which could affect social order, public interests, and the legitimate rights of citizens and organizations. Level 5 is the highest system level.

According to the relevant provisions of the Management Measures for Information Security Level Protection, Hikvision's internal information systems have passed the Level 3 evaluation. The system strictly adheres to the technical guarantees and security management requirements of China in information system security construction, establishes long-term mechanisms, and further ensures the continuous implementation of security protection work.

NIST CSF 2.0

The NIST Cybersecurity Framework (CSF), published by the National Institute of Standards and Technology (NIST), is a cybersecurity risk management framework designed for organizations

of all types. Version 2.0 was officially released in 2024. Building upon the original five functions of "Identify, Protect, Detect, Respond, and Recover," it adds a new "Govern" function. This update further strengthens senior-level governance, supply chain security, as well as measurement and improvement, while helping organizations assess, plan, and continuously enhance their cybersecurity capabilities through implementation examples and reference mappings.

Hikvision passed a third-party assessment and certification based on NIST CSF 2.0 in July 2025, systematically verifying the company's cybersecurity governance and risk management capabilities.

8.3 Security Technology

The Network and Information Security Laboratory is dedicated to security research and practices related to the IoT. Its work encompasses penetration testing, fuzzing, code auditing, reverse engineering, vulnerability research, tool development, and the analysis and research of IoT security solutions. The team's primary research areas cover web security, mobile security, protocol security, wireless security, firmware security, threat intelligence, and machine learning, with the aim of discovering and resolving security issues before they can be exploited by malicious actors.

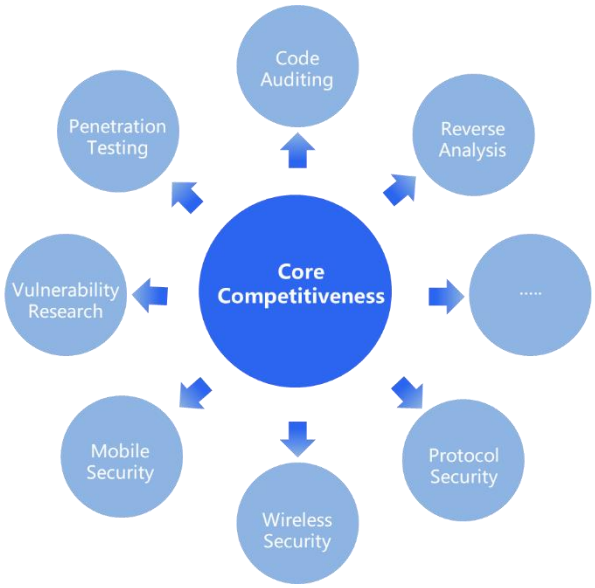


Figure 8-2 Research on core competitiveness of product security

Core Competencies:

- Embedded Device Vulnerability Mining: Leveraging Hikvision's experience in the field of embedded device security, we utilize methods such as firmware reverse engineering, firmware emulation, serial debugging, static analysis, and symbolic execution to discover vulnerabilities.

- Protocol Vulnerability Mining: By integrating commercial tools with self-developed fuzzing tools, we utilize fuzzing technology to conduct automated vulnerability mining on mainstream IoT device protocols. To date, our researchers have discovered hundreds of high-risk protocol vulnerabilities.

- Wireless Security Research: Our team possesses various security hardware testing environments for RFID, radio frequency, and Bluetooth modules. This allows us to perform wireless packet sniffing, wireless signal replay attacks, spoofing, hijacking, RFID cracking, and NFC cloning.

- White-box Auditing: We integrate commercial tools to track and detect known vulnerabilities in internally used open-source components, issuing timely threat alerts. During penetration testing, our internal team conducts white-box audits on target source code to improve vulnerability discovery efficiency comprehensively.

- Web Security: Combining commercial tools with self-developed web testing tools, we utilize crawler detection and passive proxy technologies to perform penetration testing on web platforms. This enables the detection of various web security issues, including SQL injection, Cross-Site Scripting (XSS), sensitive information leakage, and command injection. The core security testing team conducts in-depth penetration testing on target systems to uncover more hidden security vulnerabilities.

- Mobile Security: Utilizing internal mobile security analysis tools, the team performs comprehensive security testing on mobile apps. These tools enable the real-time capture of interactive protocol packets and automatic identification of sensitive information. They also facilitate privacy compliance checks for personal information and support security hardening to prevent malicious attacks.

- Threat Intelligence: The team has deployed various types of distributed high- and low-interaction honeypots. These enable the real-time detection of IoT-targeted malicious

attacks and the capture of attack samples across the network, facilitating real-time correlation analysis and early warnings.

- Machine Learning: The team utilizes machine-learning algorithms to conduct security analysis on IoT device logs. By deploying various attack detection models, we can rapidly identify potential or known malicious attack behaviors from massive logs and issue real-time threat warnings.

Security Engine

IoT Security Protection Engine

To continuously improve the threat detection and defense capabilities of IoT devices, the Network and Information Security Laboratory has independently developed security detection and protection engines, —including intrusion prevention systems and protocol firewalls that can be applied to IoT devices. This achieves a comprehensive monitoring of device status, full risk perception, and real-time attack blocking. The engine supports non-destructive upgrades through hot updates to counter emerging network attacks, ensuring the reliable and stable operation of IoT devices.

Intrusion Prevention Engine

The company has specifically designed and developed the intrusion prevention engine for its IoT devices. With this built-in module, the devices can perform comprehensive, real-time monitoring and analysis of files, networks, processes, and other operational behaviors after booting up. It blocks the startup and execution of malicious processes through a process whitelist. It also monitors, detects, and intercepts malicious file creation, deletion and modification. Moreover, the engine monitors and blocks abnormal outbound network traffic in real-time.

Protocol Firewall Engine

Due to resource constraints, IoT devices are unable to cope with large-scale malicious scans and cyber-attacks, and conventional security software cannot be deployed on them. In order to effectively defend against common cyber-attacks, the company's security team, through accumulated knowledge of security attack and defense techniques and a deep understanding of embedded devices, collaborated with the R&D team to customize and develop a lightweight IoT protocol firewall engine module. The engine directly obtains the raw request message from the business module and conducts attack detection before the message enters the core

processing logic. When an attack is detected, the engine notifies the business module to promptly discard the message and decides whether to automatically block the attacker based on the interception strategy. By deeply integrating with the business module, this solution overcomes the limitations of traditional security protection products. It can comprehensively detect and analyze various IoT protocols, effectively resisting common cyber-attacks and enhancing the security and stability of IoT devices.

Security Situational Awareness

The enormous IoT system, comprising devices, networks, platforms and applications, requires multi-layer protection and End-Cloud Collaboration powered by intelligent big data security analysis. The implementation of intelligent security situational awareness, visualization, and protection for entire networks will be an emerging trend for the IoT.

Security situational awareness refers to the acquisition, understanding, display, and prediction of important security elements that can cause changes in the system state within large-scale system environments.

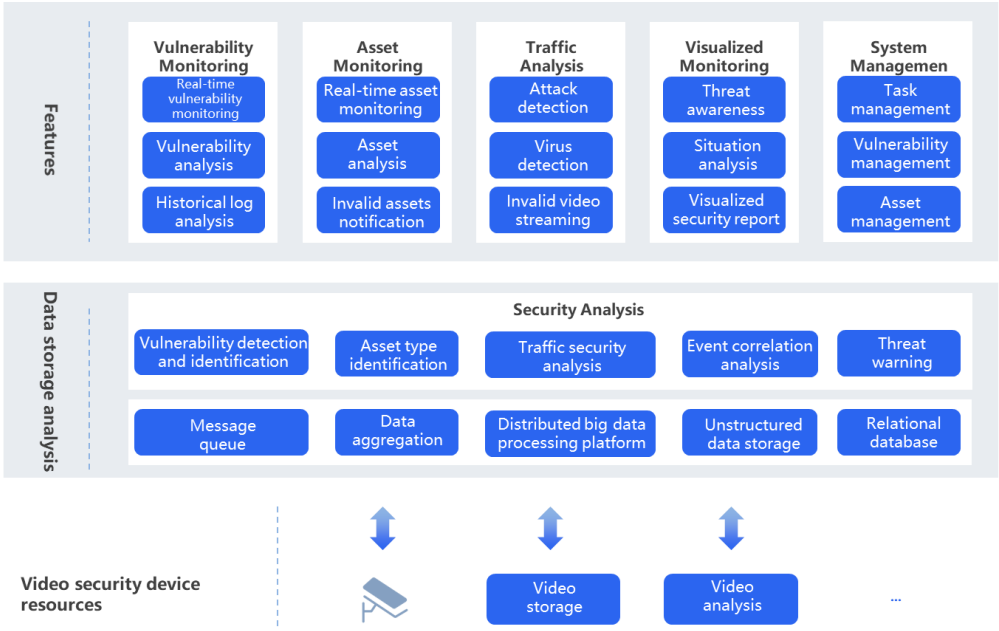


Figure 8-3 Security Situation Awareness

Vulnerability Assessment

Vulnerability assessment supports the effectiveness of security monitoring systems in identifying potential risks. The Hikvision security situational awareness system integrates mainstream vulnerability databases to detect known vulnerabilities.

Hikvision also maintains a dedicated vulnerability research team that continually tracks security advisories released by other well-known security organizations and vendors. The team also continuously analyzes, explores, and verifies new vulnerabilities. Through continuous investment by Hikvision's vulnerability research team and the ongoing upgrading of the vulnerability database, the system promptly helps users identify potential security risks, allowing them to take preventive measures before incidents occur.

Furthermore, the system can perform correlation analysis on discovered security threats and asset information. By leveraging established big data analysis model, it performs dynamic analysis on both real-time and historical data, enabling accurate and efficient perception of the overall network security status and development trends. This, in turn, supports the hardening of AIoT systems and ensure their security.

Security Visualization

Security visualization presents data characteristics intuitively, making them easy for users to understand. Therefore, the results of big data analysis (such as deep packet inspection and full traffic analysis) must be visualized.

When a system is under attack, it is necessary to quickly identify the source and path of the attack and respond in a timely manner. Effective measures should be implemented before the attack causes further damage in order to reduce losses. After the attack, steps must be taken promptly to prevent similar incidents from occurring again.

Security Center

As a core component of the system's security protection, the Security Center helps users build a robust security defense line through intelligent detection and visualized monitoring. It mainly comprises the following three modules: Account Security, Basic Security, and Configuration Security.

Account Security: Covers risk alerts for insecure configurations and abnormal operation regarding user management, password reset reserved information, and login management.

Basic Security: Includes sub-items such as trusted protection, firmware encryption, configuration file security, secure backup, storage encryption, security defense, and security auditing to ensure a solid system foundation.

Configuration Security: Detects common service configurations and provides risk alerts for insecure protocols enabled by users to ensure usage security.

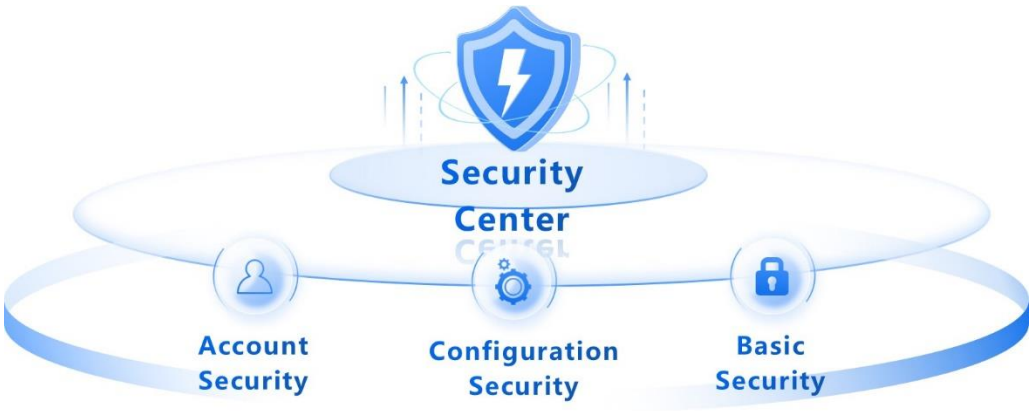


Figure 8-4 Security Center Schematic

Honeypot

Honeypot technology is essentially a deception technique used against attackers. By deploying decoy hosts, network services, or information, it lures attackers into compromising themselves. This allows defenders to capture and analyze attack behaviors, understand the tools and methods used, and infer the attacker's intent and motivation.

Benefiting from advancements in data storage, retrieval, mining, and threat intelligence, the value of honeypot technology has been further enhanced. Hikvision utilizes self-developed and modified honeypots as data collectors, deploying honeypot nodes globally and establishing a data pipeline for collecting, processing, storing, and retrieving honeypot data. This provides data support for security research, incident response, attack tracing, and situational awareness.

Hikvision's honeypot system utilizes a rule engine to monitor attacks on IoT devices in real time and issue alerts for unknown threats. Its analysis engine leverages historical data to

focus on monitoring and correlating malicious attackers, predicting threat trends.

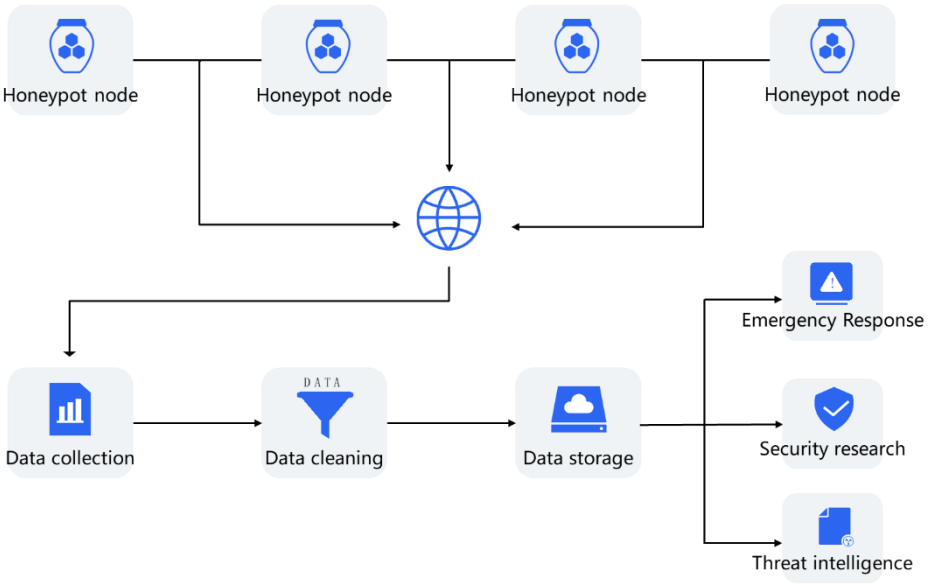


Figure 8-5 Honeypot system

As an important component of Hikvision's threat intelligence platform, the honeypot system continuously monitors security threats from around the world to ensure the secure and stable operation of user devices.

Digital Watermark

Digital watermarking refers to the technology of embedding identification information into digital carriers (such as images, audios, videos, documents, etc.) to achieve copyright confirmation, content authentication, or covert communication, without affecting the normal use of the carriers. Its core principles are based on signal processing and cryptography, where watermarks are hidden by modifying data bits or introducing imperceptible redundancy, while ensuring the detectability and security.

Furthermore, model watermarking is a watermarking technology oriented towards AI models (especially generative models). By embedding identification information into model parameters, the training process, or generated outputs, it achieves model ownership verification, content traceability, and intellectual property protection.

Data watermarking serves as the "last line of defense" against data leakage. Therefore, the technology itself possesses broad application prospects and immense economic value.

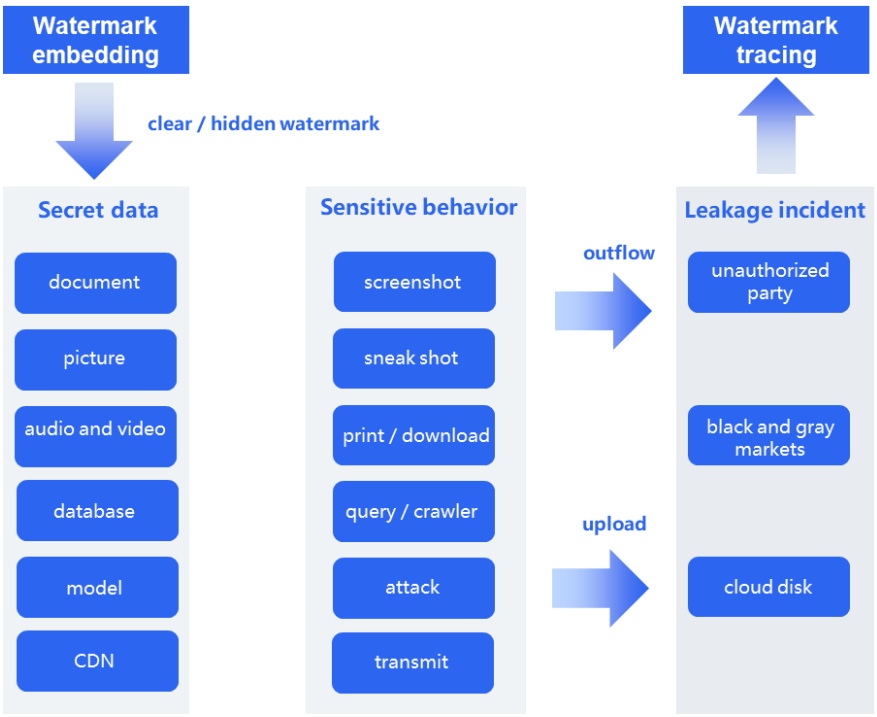


Figure 8-6 Digital Watermark

With the release of the Measures for the Labeling of AI-Generated Synthetic Content and its supporting national standard, Cybersecurity Technology—Methods for Labeling AI-Generated Synthetic Content, the application of digital and model watermarking technologies is expected to become more widespread. Hikvision is one of the core contributors to the national standard "GB/T 45909-2025 Cybersecurity Technology—Implementation Guidelines for Digital Watermarking Technologies," possessing extensive technical expertise in secure and robust multimodal implicit/explicit watermarking and model watermarking.

9 Artificial Intelligence Security

With the widespread application of Artificial Intelligence (AI) technology, it has integrated into various aspects of daily life (such as smart homes and intelligent access control) and public services (such as smart transportation systems and urban public security governance). AI security is the core prerequisite for ensuring the compliant and reliable operation of such intelligent applications, directly affecting personal privacy rights, corporate property security, and social public interests.

AI security is an interdisciplinary field at the intersection of AI technology and information security, focusing on two core objectives: first, ensuring the secure, stable, and reliable operation of AI systems, enabling them to resist various attacks; second, preventing the malicious misuse of AI technology to avoid potential harm to individuals, enterprises, and society.

In recent years, rapid advancements in technologies such as generative AI (including intelligent conversational assistants and image generation tools) and large models have significantly enhanced AI applications but have also intensified the complexity and proliferation of security risks. While large models empower production and daily life with their cross-domain understanding and generation capabilities, their complex model structures, massive training data, and open interaction modes have given rise to new security risks such as prompt injection, model jailbreaking, and the misuse of generated content. For instance, malicious actors leverage large model technology to mass-produce disinformation or optimize fraudulent methods, thereby improving the precision and efficiency of attacks while significantly increasing the difficulty of defense.

To regulate AI development and mitigate security risks, numerous countries and regions worldwide have enacted targeted policies and regulations.

In China, a multi-layered and systematic AI security governance framework has been established. Recent regulatory developments have introduced provisions relevant to AI governance, strengthening requirements related to security, risk monitoring, and ethical oversight of AI applications. These provisions explicitly support fundamental AI research and infrastructure development, while mandating the improvement of ethical guidelines and mechanisms for risk monitoring and assessment. The "Interim Measures for the Management

of Generative AI Services," effective August 15, 2023, adopts an inclusive yet prudent regulatory approach, clearly outlining general requirements for providing and using such services. The "Measures for Labeling of AI-Generated Synthetic Content," effective September 1, 2025, and accompanied by a mandatory national standard, focus on the critical aspect of labeling AI-generated synthetic content. These measures and standards aim to help users identify disinformation through labeling, clarify the labeling responsibilities and obligations of relevant service entities, and regulate labeling behaviors throughout the content creation and dissemination processes.

Internationally, the European Union's AI Act, the world's first comprehensive AI regulation, officially entered into force in 2024. Based on the potential impact of AI systems on users and society, the act classifies AI risks into four levels—Unacceptable risk, high-risk, limited risk, and minimal risk—and establishes corresponding regulatory requirements and compliance standards accordingly.

9.1 AI Model Security Evaluation

With the improvement of computing resources on edge devices, a massive number of these devices have achieved functions such as speech recognition, image processing, natural language understanding, and predictive analysis through built-in AI algorithms and hardware support, thereby enhancing user experience and device performance. However, the increasingly widespread application, massive scale, and increasingly complex structure of intelligent algorithms on edge devices have led to security threats at multiple levels, including data, models, and algorithms. Examples include adversarial sample attacks, training data poisoning attacks, and model backdoor implantation attacks. Such issues not only directly threaten the secure operation and performance of models but may also infringe upon data privacy and lead to overall system failure.

In response to these issues, Hikvision has conducted in-depth research on technologies such as efficient security evaluation for intelligent models and real-time monitoring of security risks. It has constructed an AI algorithm model security evaluation platform that covers mainstream AI algorithm models and supports multi-dimensional evaluations including robustness, fairness, and interpretability. This meets the needs for vulnerability detection and proactive risk prevention and control for trillion-parameter-scale intelligent models.

Specifically, IoT intelligent models are characterized by their wide variety, rapid iteration, large scale, and diverse application scenarios, which lead to problems such as scarce abnormal samples, high difficulty in black-box testing, and insufficient test coverage. To address these problems, the platform has built a dynamically orchestrated large-scale vulnerability scanning framework. Relying on key technologies such as automatic test sample generation, adversarial sample testing, privacy leakage detection, and model backdoor scanning, it accurately identifies typical security risks like adversarial attacks, data poisoning, and model theft. Oriented toward real-world AIoT scenarios, the platform provides one-click, multi-type black-box intelligent testing capabilities. It supports customizable test configurations and automated test report generation, enabling visualized, verifiable, efficient, and systematic security evaluation for intelligent algorithm models.

Furthermore, for large language models and multimodal models, Hikvision has constructed a security evaluation containing over one million entries. It is complemented by specialized security capability evaluations covering more than a dozen categories, such as compliance of generated content, refusal capability, hallucination output, and information security, it achieves the effective screening of security risks in large models.

9.2 AI Security Protection Enhancement

Model Protection Enhancement

Model security is a core component of AI security. Key protection technologies include adversarial training, model encryption, and data preprocessing.

Adversarial training enhances the model's resilience against malicious perturbations by actively introducing adversarial samples (input data with minute perturbations applied) during the training process, thereby reducing the impact of adversarial attacks.

Model encryption protects trained model parameters and structures through encryption techniques. During deployment, secure hardware (such as TPM/TEE Trusted Execution Environments) decrypts and executes the model, preventing unauthorized parameter extraction and protecting core enterprise AI assets.

Data preprocessing technology filters, normalizes, and removes noise from input data to eliminate the impact of adversarial perturbations, thereby effectively defending against attacks.

Permissions and Deployment Environment Protection Technologies include:

1. Strictly partitioning user permissions during model training, deployment, and inference phases; for example, only administrators can modify model parameters, while ordinary users are restricted to calling inference interfaces to prevent privilege abuse.

2. Adopting sandbox or containerized deployment to isolate models from the host system resources, preventing attacks or tampering by malicious programs;

3. Regularly performing vulnerability scanning and patch updates on the deployment environment, including security hardening for operating systems, deep learning frameworks, and dependent libraries;

4. Maintaining full-link operation audit logs, including user identity, operation time, request content and model output, enabling traceability and analysis of security events.

Data Security Protection

Data is the core foundation for AI model training and inference, making data security a prerequisite for AI security. Hikvision provides full lifecycle AI data security protection across dimensions such as data encryption, data privacy protection, and data leakage detection.

Data encryption technology primarily addresses security issues during processes such as static storage and dynamic transmission. This includes: 1) using encryption algorithms to encrypt raw training datasets and model weights; and 2) employing secure transmission protocols and data integrity protection measures to safeguard data in transit.

Data desensitization, as a key privacy-enhancing technology, ensures that sensitive personal information is not exposed during training and usage. This is achieved through methods such as generalization, suppression, perturbation, or encryption.

Data leakage detection focuses on identifying unauthorized data exfiltration or anomalous model behavior. It is essential not only to detect the direct leakage of raw data but also to identify risks of indirect leakage through model outputs, parameters, and gradients.

10 Exchange and Collaborations

Through external exchanges and cooperation, Hikvision gathers feedback from stakeholders and advanced technologies and management practices in the security field, and systematically transforms them into future improvement targets, continuously enhancing the company's information security capabilities.

Figure 10-1 Exchange and Collaborations

- We engage well-known global security assessment institutions to benchmark and optimize the company's R&D security management system, ensuring it aligns with top-tier international standards.
- We strengthen communication and cooperation with global security vendors to enhance product security.
- We invite well-known global security testing teams to conduct penetration testing on our products, minimizing business risks to maintain security risks within a controllable range.
- We invite prominent industry security experts to the company to train R&D personnel, improving their security competencies.
- We communicate with customers regularly on topics such as product security topics, emergency response mechanisms, and security requirements, while sharing security progress in a timely manner and address customer needs.
- We launched the Security White Hat Rewards Program to reward global white hats who

contribute to Hikvision's information security, fostering collaborations with these excellent security researchers.

11 Security Commitment

Hikvision is committed to leveraging leading technologies to help customers safeguard their personal information, and to adopt a comprehensive approach to protect user data.

Hikvision employs a unified, integrated security infrastructure throughout the entire video IoT application ecosystem. Hikvision maintains a professional security team responsible for supporting all Hikvision products. This team conducts security audits and testing for both in-development and released products. It also provides security training and actively monitors reports of newly discovered security issues and threats.

To learn more about how to report security issues to Hikvision and how to subscribe to security notifications, please visit this webpage:

https://www.hikvision.com/en/support/cybersecurity/

见远 行更远

See Far, Go Further

微信扫一扫
关注海康威视网络安全

海康威视

www.hikvision.com

客服热线：400-800-5998

股票代码：002415

微博：@海康威视hikvision