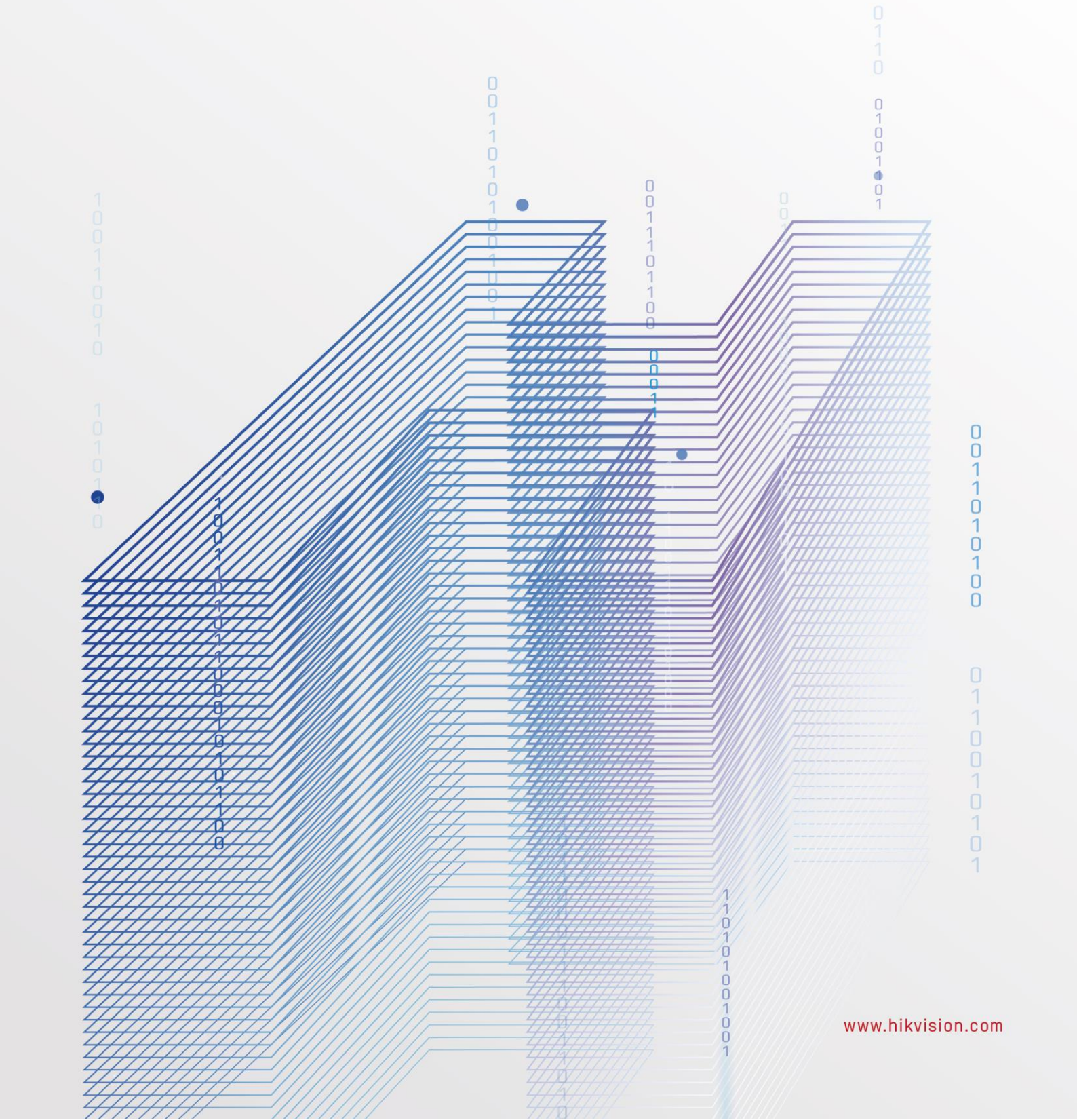
HIKVISION

HIKVISION Cybersecurity White Paper



www.hikvision.com

About this Documentation

Offering an overview of our current practice on product cybersecurity, Hikvision Cybersecurity White Paper provides users with the company's cybersecurity 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 and revised in September 2023.

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. Hikvision is committed to serving various industries through its cutting-edge technologies of machine perception, artificial intelligence, and big data, leading the future of AIoT:

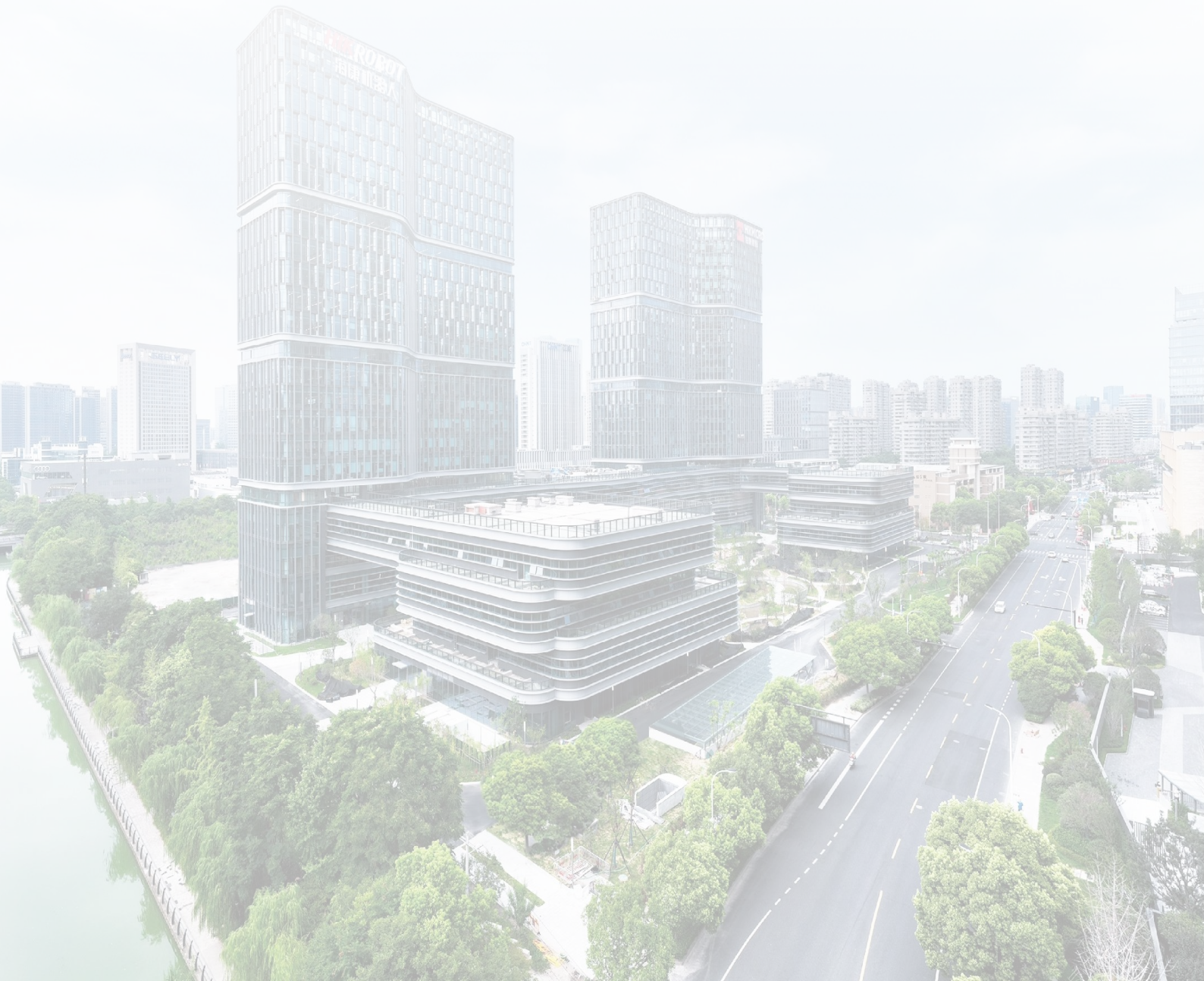
- Through comprehensive machine perception technologies, we aim to help people better connect with the world around them.
- With a wealth of intelligent products, we strive to identify diverse demands by delivering intelligence at your fingertips.
- Through innovative AIoT applications, we are dedicated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

More than 20 years ago, Hikvision began with video technology and has continued to expand and deploy visible light, millimeter wave, infrared, X-ray, sound wave, and other technologies, creating a comprehensive and multi-dimensional IoT perception technology platform. Beyond IoT perception equipment, Hikvision has five categories of software and hardware products including AIoT products that fully integrate with artificial intelligence and big data technologies, basic IT products, platform service products, data service products, and application service products. Hikvision has also expanded into integrated security to smart homes, digital enterprises, smart industries, and smart cities.

Hikvision currently has 58,284 employees (as of the end of 2022), including more than 27,951 R&D personnel and technical service personnel. R&D investment accounts for 11.80% of the annual operating income (2022), making the Company a leader in the industry. The company has R&D centers worldwide, including in Montreal, London, and Dubai, and various Chinese

cities. Hikvision has a global presence with 72 overseas subsidiaries and branch offices, serving clients in more than 150 countries and regions (2022).

Hikvision went public in May 2010, and is listed on the SME Board at Shenzhen Stock Exchange, stock code: 002415.



CONTENTS

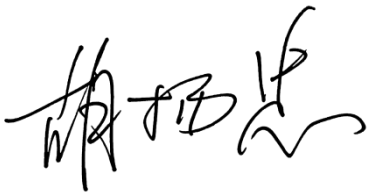
1. A letter from the President

The "Internet of Everything" is being translated from dreams to reality. As a forerunner to the "Internet of Everything", video security technology has developed rapidly over the past 10 years. Evolving from analog, to digital, to the network era, it is now entering the intelligent era. Improvements in technology advance human society, but also present new challenges. The development of Internet technology has greatly benefited human society, but it has also posed significant challenges, including those related to cybersecurity. Similarly, the Internet of Things 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 as long, with relatively less know-how of cybersecurity industrywide. In 2014, following international practice, the company established the "Hikvision Security Response Center" (HSRC), to form a centralized platform for addressing cybersecurity issues. In 2015, Hikvision established the "Network and Information Security Laboratory", greatly enhancing the corporate cybersecurity efforts. The lab, together with the subsequent Network and Information Security Committee and the Cybersecurity Department, facilitated the company's efforts to improve the cybersecurity system centered around organization and processes. Cybersecurity design stood out as a special enabler to the overall cybersecurity integrity of the company's products and systems. We understand that cybersecurity is not solely the responsibility of product manufacturers. Every stakeholder in a project, including users, integrators, operators, engineering designers, other service providers, and government entities, bears the responsibility throughout the project's entire lifecycle. All parties involved are confronted with the challenges of cybersecurity, the successful handling of which could be attributed to 30% of technological competence and 70% of managerial expertise. Collective efforts are needed from all vested parties and never should anyone take cybersecurity for granted.

Confronted with the urgent need for collective efforts to address the common challenges, we are fully aware of the keen public and media attention and concerns over the security of the Internet of Things (IoT), which further underscore the responsibility and mission we carry. Always committed to the corporate values of "being dedicated to customers' continual success, adding value to companies and communities, acting with honesty and integrity, pursuing excellence in every endeavor", we pledge to prioritize the network and business security of our customers over the company's interests.

The challenges of cybersecurity will persist, and we are committed to continuing our efforts for the best solutions.



Hu Yangzhong, President

Hangzhou Hikvision Digital Technology Co., Ltd.

2. Preface

The past several years have witnessed the progression of digitalization and the rapid development in the security industry. In these years, we have seen how the intelligent security industry explores the dream of the Internet of Things and we are happy to see that the industry is at the forefront of developing, exploring and implementing IoT technology.

Without a doubt, the development of the intelligent security industry must follow the trends of digitalization, networking, and intelligence. However, cybersecurity is a completely new field for the security industry and the openness of networks has interconnected security systems which were once independent and completely isolated, promoting data flow and sharing in ways that have drastically benefited society. This has brought about more innovative opportunities, enabled the Internet of Things industry to grow, and pushed the human progress to new heights.

During the industry's transformation from "analog", "isolated", and "data acquisition", to "digital", "networked", and "image intelligence", we have seen the benefits that the digital and networking revolution brings. However, we have also witnessed the spread of various types of malicious cybersecurity attacks from the Internet to the security industry. Furthermore, since the current security systems are based on "seamless" switching from original ones, some of the industry's inherent features may develop into possible security defects when placed in the cyberspace.

As a global company, Hikvision operates in more than 150 countries and regions. As a company of such a scale, Hikvision is actively responding to these challenges. Hikvision deeply understands, from a technological perspective, how intelligent security systems operate safely and effectively, and how technology fundamentally supports and promotes the health, prosperity, and security of the global citizens.

Cybersecurity is not just a problem for certain countries or companies. All stakeholders, governments, and industries must understand that cybersecurity is a problem that everyone in the world faces, and that meeting these challenges requires international cooperation in employing the risk-oriented methods and best practices. To effectively handle security issues, various stakeholders must form mechanisms of trust and cooperation.

Hikvision makes the following commitments: We will support and adhere to internationally recognized cybersecurity standards and the best practices; we will support research efforts

to increase network defense capabilities; we will continue to improve and use open and transparent methods so that users can assess Hikvision's cybersecurity capabilities.

Finally, just as we did in the past, we encourage our clients to help us improve the procedures, technology, and cybersecurity techniques to create even more benefits to them and their customers.

3. Security Threats in the Internet of Things

The Internet of Things (IoT) connects "smart devices" from all over the world through the Internet and allows for the interaction between people and things on a global scale. The interconnection of a massive number of devices has made networks more open, complex and diversified. However, the advent of IoT also brings incredible security challenges.

Figure 3-1 Characteristics of IoT

In addition to the traditional cybersecurity threats, there are still some special security issues in the IoT, because it is composed of a large number of unattended devices or perceptive nodes without effective monitoring, exacerbated by large numbers and huge concentrations. Based on the IoT framework, security threats in the IoT can be categorized as perception-layer threats, transport-layer threats, and application-layer threats.

Perception-layer threats

- Physical attack

IoT assets that are deployed remotely without physical protection are susceptible to theft or damage.

Outdoor devices are sometimes easily accessible, and not well managed, leading to physical attacks, tampering, and counterfeiting.

- Data leakage

Sensitive information leakage is caused by the lack of encryption or access control during data collection and processing by IoT devices.

- Unauthorized access

Lack of authentication requirements, weak passwords, or easily bypassed authentication mechanism leave some IoT devices susceptible to potential attacks and compromises.

Some IoT devices leave a debug interface, which could allow an attacker to obtain device operation information.

- Unauthorized update

Some IoT devices do not use a robust update verification mechanism, which could allow unofficial firmware packages that may contain vulnerabilities or malware to be installed into the devices.

- Expired components

IoT devices come with built-in components with known vulnerabilities or expired components.

- Malicious software

Malicious software may contain malicious code or viruses, which can be used to obtain device information and system files, or affect the normal operation of the device.

Transport-layer threats

- Cyberattack

Exploiting protocol vulnerabilities, such as lack of effective authentication, may lead to leaks on the access side.

- Man-in-the-Middle Attacks

Attackers intercept communication between IoT devices and manipulate data or commands exchanged, leading to unauthorized access or control over these devices.

- Denial-of-Service Attacks

Floods of data requests or commands can overwhelm IoT devices, rendering them unresponsive or causing malfunctions, disrupting regular operations.

- Data leakage

During communication between IoT devices, cloud hosting servers, and mobile devices, attackers can access sensitive data by monitoring the transmission channel.

- Data tampering

When a device communicates over a network, commands and data may be intercepted and altered by attackers if the transmission data is not checked for integrity.

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 and the risk of data leakage.

- Insecure APIs and Interfaces

Weaknesses in application programming interfaces (APIs) and communication interfaces can be exploited to manipulate device functionalities or steal data.

- System vulnerabilities

IoT device application software or operating system software has logical defects or errors in design, which can be exploited by attackers to control the entire device through network implantation of Trojan horses, viruses, and other methods, resulting in abnormal device operation.

- Data leakage

The application layer manages a large volume of data, which is prone to leakage if not encrypted or access control not properly managed.

- Outdated components

The application layer uses components with known vulnerabilities or expired components. If the components are not updated in a timely manner, the inherent vulnerabilities of the components can be easily exploited.

- Configuration vulnerabilities

In the security configuration for applications, frameworks, containers and operating systems, security vulnerabilities caused by unreasonable or improper configuration, such as using versions with security flaws, granting excessive permissions to certain accounts, and failing to control access to sensitive resources may allow attackers to access certain system data or use system functions without authorization.

After investigating the numerous hidden security risks in the IoT environment, as well as the complexities of computational capabilities and the complex hardware and software environment, Hikvision developed the video-centric IoT security solutions that promise to create a brand new security architecture, establish a multi-dimensional security system, and guarantee terminal security, data security, application security, network security, personal data protection, and security compliance.

4. Network and Information Security in the Security Industry

The development of the security industry has gone 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 concern. However, with the rapid adoption of network connectivity, the security industry transitioned directly from analog to IP digital technology. During this transition, security issues didn't get much attention. Consequently, user-friendly designs that were advantageous in the analog era didn't keep up with best practices in information security in the digital era. Security manufacturers often default to enabling all supported protocols to facilitate users in integrating devices from multiple manufacturers with a single click. The server automatically connects using whichever protocol that is supported. Although such a design is very easy to use for customers, it compromises best practices in information security.

It is precisely due to this evolution of the security industry that certain information security issues have arisen in recent years. However, the emergence of these issues does not necessarily mean that the entire industry is as vulnerable as some portray it to be. Hikvision has recognized both existing and potential security risks. Substantial and effective efforts have already been undertaken to address these challenges.

Objectively speaking, cybersecurity issues are not exclusive to the security industry. They represent a challenge faced collectively by human society today. Given the entire IT landscape, cybersecurity challenges are present in all domains, and several fundamental consensuses exist:

- 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. There are millions of lines of code in each product, and if only one parameter is incorrectly set, or if the positioning of two lines of code is incorrect, this may lead to a high-risk vulnerability in a system. Currently, automated or manual techniques cannot be used to detect all potential cybersecurity issues. Therefore, product security issues are common across all manufacturers.

- Security for the Entire System

The security of any system cannot be guaranteed solely by a single point; it must encompass the entire system. 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. Any problems in any part of the system can potentially lead to a system breach but if implemented correctly, attackers must get past the many layers of security 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 and OpenSSL. Many of these components are deeply integrated into the underlying infrastructure of information systems and are used extensively. As a result, the security risks posed by these vulnerabilities are far-reaching, often evolving into "generic" vulnerabilities that can potentially impact entire industry sectors or a company's product lines.

- Security in Dynamic Balance

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

- Product Security Management

The most important element in system security is security management. Even with systems that are more secure, if the user cannot manage or operate them properly then system security cannot be maintained. Currently, some security issues within the security industry are caused by "inappropriate" usage of users and ineffective security management. Some cybersecurity devices still have "weak" passwords and some security systems do not have firewalls or other security equipment installed. Users also need to develop good security habits, take regular note of security announcements from manufacturers, update firmware to the latest version and install patches as soon as possible.

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, and customer feedback, we have established the Hikvision Security Development Maturity Model (HSDMM). 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 security governance, security processes, and security technologies.

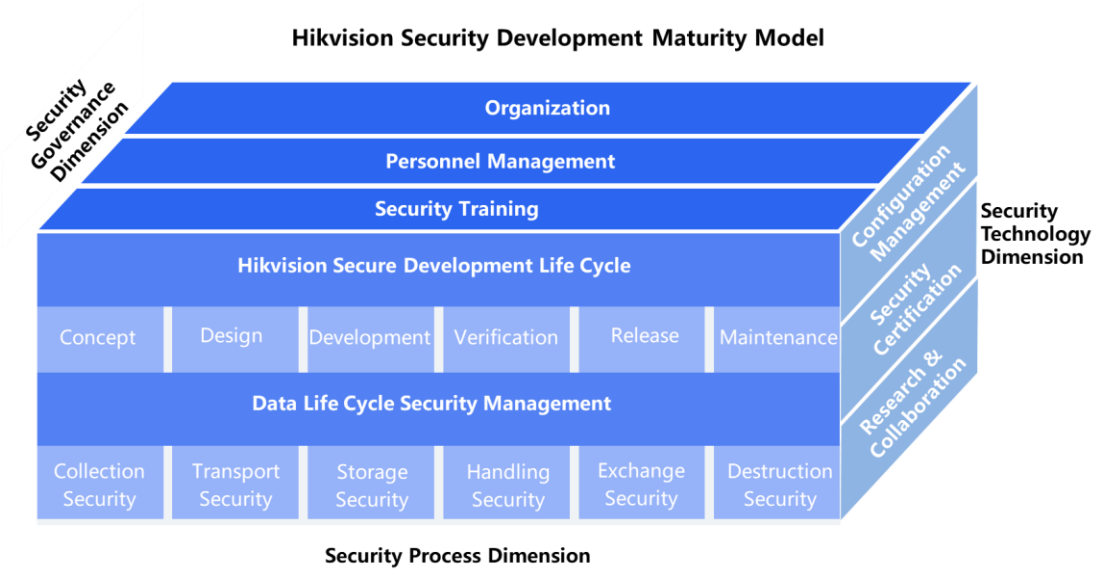


Figure 5-1 Hikvision Security Development Maturity Model

6. Security Governance

6.1 Organization

To ensure that product security is incorporated into every aspect of Hikvision product the development, supply chain, marketing and sales, delivery, technical service and other processes, we first need to establish an organizational structure that can guarantee its implementation and assign clear responsibilities to each group. The security administrative structure of Hikvision is as follows:

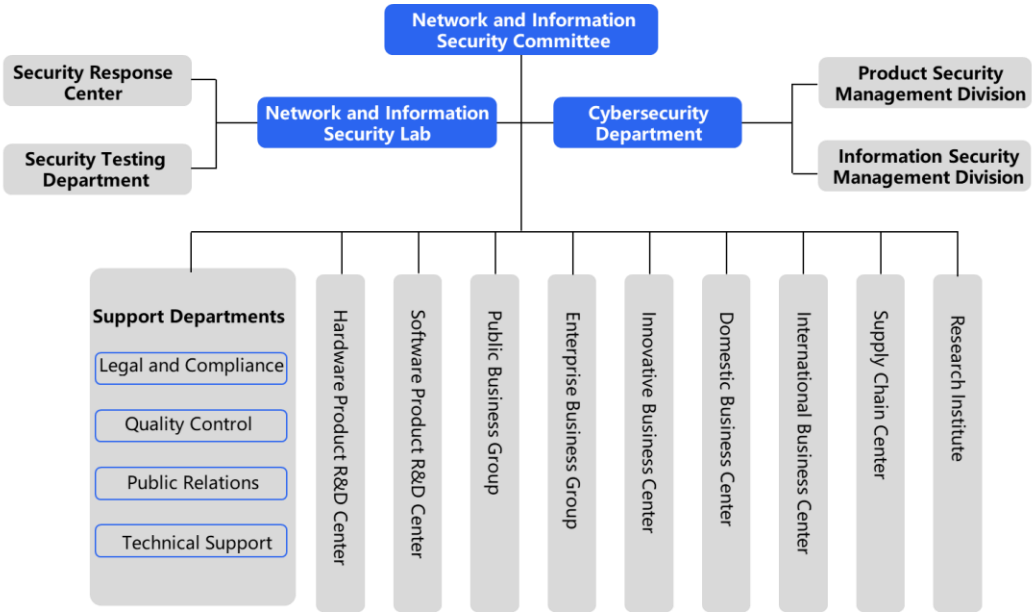


Figure 6-1 Hikvision Security Organization Structure

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. Hikvision President, Mr. Hu Yangzhong, acts as the head of the committee, which has set up a specialized Cybersecurity Department to formulate network and information security strategies, policies, procedures, and standards, and to manage resource allocation on a daily basis.

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 researches and implements technologies related to Internet of Things security. It mainly covers IoT perception, product security components, video security products, penetration testing, IoT security and other areas. The laboratory aims to research the cutting-edge of IoT security technology and promote its improvement. All laboratory staff boasts many years of experience in information security, and many of them have obtained Certified Information Security Professional (CISP) or Certified Information Systems Security Professional (CISSP) certification.

Security Response Center

The Hikvision Security Response Center is responsible for receiving, addressing, and disclosing Hikvision product and solution security vulnerabilities. Hikvision is a member of the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) and the Security Emergency Service Support Organization of the Industrial Information Security Industry Development Alliance. It shares best practices and experience in security emergencies with other excellent members worldwide, enhances reliable communication and cooperation, and enhances 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

and is responsible for the implementation of processes such as product planning, R&D, and testing on 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. They also assist in conducting information security monitoring, auditing, training, and awareness activities. Additionally, they are responsible for handling internal security incidents.

Security Testing Department

The Security Testing Department is a third-party body independent of the product lines and is responsible for the product security testing for all of Hikvision's product lines. This department inspects the company's product security policies, and assesses the implementation of security baselines in products. It is also responsible for ensuring that the released products are secure, and for preventing various types of security issues that may arise during the research and development process.

Support Departments

The Support Departments are responsible for providing related internal control, laws and regulations, brand promotion, auditing, and PR support for matters related to product security.

6.2 Personnel Management

In terms of cybersecurity awareness education for all employees, Hikvision intends to build a company-wide security awareness education and cultural atmosphere. In order to achieve this, Hikvision provides cybersecurity training for all new employees, organizes continuous cybersecurity awareness popularization and education activities, and carries out training and learning of cybersecurity knowledge and skills based on their respective business needs and other awareness. Educational activities will also feature education and learning of cybersecurity cases based on the characteristics of their own business fields. The company regularly promotes cybersecurity periodicals on the internal platform for all employees; at the same time, it also promotes cybersecurity awareness to all employees through posters, information security promotional posters, videos/micro movies, startup reminders, etc.

Hikvision has identified the key positions of cybersecurity in various business fields, and the key positions of product security. For employees in key product safety positions, we have put forward the following requirements:

- Employees must pass background checks before taking up their jobs to ensure that people with backgrounds and experience that meet customer requirements are assigned to the correct positions. The "Safety-Critical Positions Confidentiality Agreement" will be signed to clarify the confidentiality obligations of employees.
- Employees should follow the qualification standards to enhance their awareness and improve their related skills. We conduct regular security reviews. Personnel in key positions will be subject to on-the-job investigations for possible violations.
- We instruct human resources and security specialists to regulate or modify the authority account for resigned employees, and their assets when necessary. Resignation review includes internal transfer and resignation.

We require every employee to be responsible for what they do and the results they produce, not only for technology, but also for legal responsibilities. Our employees know that once a cybersecurity issue occurs, it may have a great impact on customers, companies and individuals. Therefore, regardless of whether it is intentional or unintentional, Hikvision will continue to take action to ensure accountability and cybersecurity of its systems and products.

6.3 Security Training

Drawing on the best practices of the industry, Hikvision established a comprehensive cybersecurity training system. Various forms of training are incorporated into stages 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, the training system ensures our provision of secure and compliant products and services to customers.

Cybersecurity capability certification for product R&D positions: 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, in order to enhance employees' awareness of cybersecurity, improve their cybersecurity capabilities, and elevate the security quality of our products. Employees must complete the competency certification before being eligible for job placement or applying for promotions.

Cybersecurity capability training camp: The Cybersecurity Department regularly organizes cybersecurity competency 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 has carried out various practice-oriented special capacity-enhancing activities to enhance the knowledge and skills of employees in key positions in cybersecurity, such as: 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 relies on processes and systems for protection. Hikvision Security Development Life Cycle (HSDLC) is developed by Hikvision, 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.

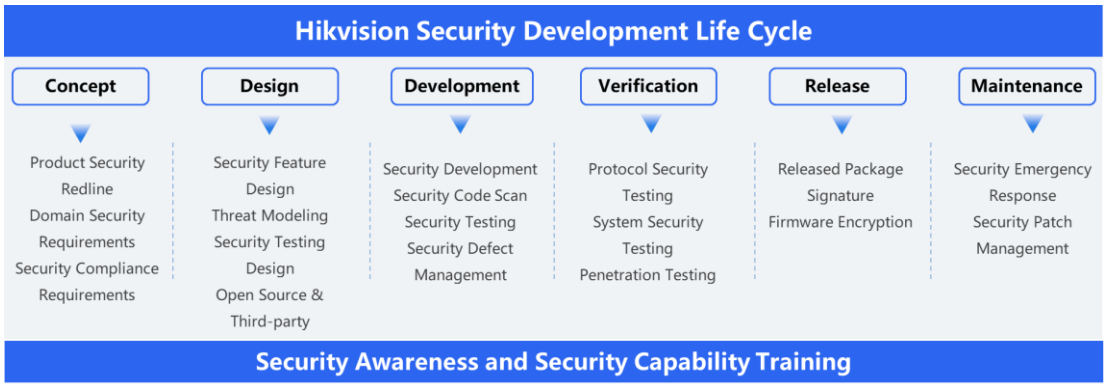


Figure 7-1 Hikvision Security Development Life Cycle

Concept Stage

During the concept stage, there are three important points in product security requirement analysis:

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.

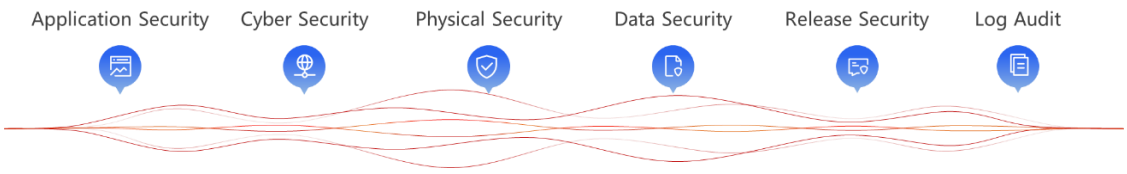


Figure 7-2 Product Security Redline

2. If the product involves personal data, a list of personal data involved in the product will be identified during the conceptual stage.

3. A threat analysis for the future usage scenarios of the product is conducted, aimed at identifying 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 relevant response and preventive measures are incorporated into the product requirement list.

Design Stage

Threat modeling is crucial in the product design phase. It's a structured approach that uses abstract methods to aid in risk assessment, aiming to identify, quantify, and address security risks associated with the product. The purpose of threat modeling is to identify potential threats to the system during the design phase, identify risks, and establish appropriate response measures. Threat modeling can identify security issues during the design phase, sort out security requirements, and avoid security risks during the coding phase, which helps to effectively control product security risks and reduce the cost of fixing security issues.

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 model the architecture level threats to the product, identify potential security threats to the product from 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 on a functional level to timely recognize security threats in the design and make mitigation measures accordingly.

3. Collected and identified security requirements are analyzed and designed in detail, and there are special security architects in the company to provide technical support for the security design of various products.

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 the overall product security risk.

Hikvision follows the HSDLC safety research and development 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 combined with the company's main products, Hikvision has summarized six key principles: attack surface minimization, minimal privilege, default distrust, open design, default security and defense in depth.

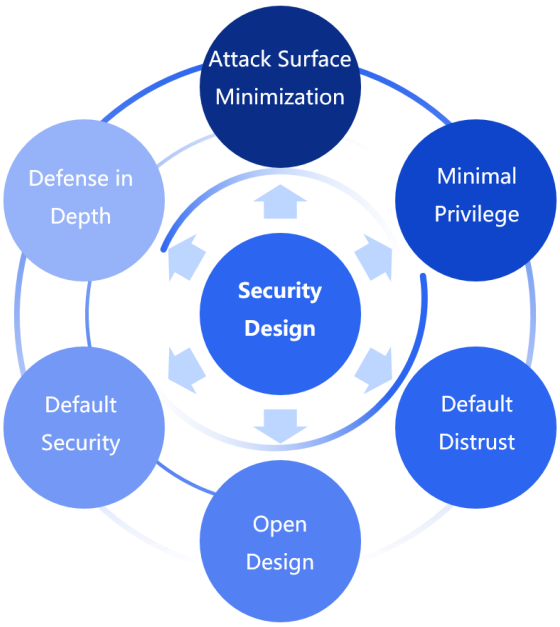


Figure 7-3 Security Design Principles

Development Stage

Hikvision requires R&D personnel to follow secure coding standards and conduct cross 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 for company business scenarios, known defects can be identified through code features, and R&D personnel can be informed of the existence of defects in various branches. The synchronization of defects is evaluated to ensure they are in place, and interception is carried out during continuous construction activities to control known code problems in the source code stage, greatly reducing repair costs.

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 relevant security tests at stage of product development to ensure product security:

- Strengthen protocol security testing in product security testing, conduct network protocol security, robustness and reliability analysis on all products.
- Introducing vulnerability scanning tools in system security testing and timely tracking of CVE vulnerability library information can comprehensively identify various vulnerability issues in the product, including security vulnerabilities, security configuration issues, and application system security vulnerabilities.
- 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.
- Hikvision's Interactive Application Security Testing (IAST) utilizes a proxy server to capture and simulate the request traffic that can monitor all instructions executed on the server

side in real-time by loading the monitoring program's jar package through configuring JVM parameters. It can transparently track the flow of the testing script in memory, and has 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 will conduct penetration tests on products regularly to minimize business risks and keep security risks within controllable range.

- The company's product security management team analyzes security issues discovered during product testing on a quarterly basis, compiles a list of typical common security issues, and then delivers them to each product line for self-inspection to prevent similar problems from happening again.

Release Stage

Before the product release, Hikvision needs to develop a security test plan and strategy according to the product demand stage to complete the test. 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.

The product release packages of Hikvision are digitally signed by the product development management to ensure the source and integrity of the software release packages are verified, effectively avoiding illegal software packages.

Maintenance Stage

1. Technical Support

The technical support team provides services to customers. With customer authorization, they may need access to some sensitive customer information. Therefore, providing them with essential training in network and information security is of utmost importance, which empowers them to assist in safeguarding customer interests and preventing errors in access control, communication security, and personal data protection. For employee management, the company has established the “Hikvision Technical Support On-Site Service Standards”,

encompassing guidelines for behavior, personal safety, information security, and other aspects.

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

2. Emergency Response

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

- Responding to and handling customer-submitted security incidents.
- Responding to and handling security matters reported by industrial associations.
- Formulating the company's information security incident management strategy and procedures for handling security incidents.
- Analyzing the vulnerabilities and patches announced and released by system software providers and professional security companies.

The company also specifies each department's responsibilities and the procedures for product security incident management to ensure the quality and efficiency of security incident management. The scope of the Security Response Center's management responsibility covers product security during the pre-sales, sales, and after-sales processes, and includes customers' security related interactions, cooperation with security organizations, emergency response management, security information announcement, information security compliance, and the process and implementation of legal compliance.

Hikvision is a member of the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) and the Security Emergency Service Support Organization of the Industrial Information Security Industry Development Alliance. It shares best practices and experience in security emergencies with other excellent members worldwide, enhances reliable communication and cooperation, and enhances the effectiveness and timeliness of the company's response to security incidents.

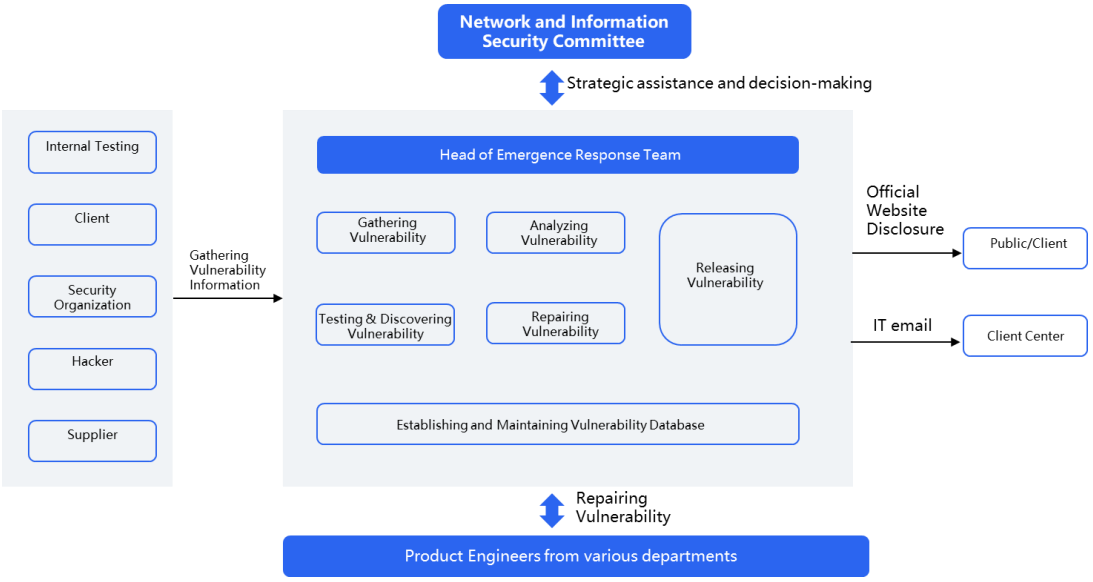


Figure 7-4 Security Emergency Response

3. Vulnerability Management

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 7-5 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 responsible vulnerability disclosure and handling process, and respects the research results of every security researcher. External vulnerability discoverers should give manufacturers a reasonable period of time 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 personnel responsible for the product to quickly complete the assessment of the authenticity of the vulnerability and related risks.

- **Tracking and resolution**: Once the vulnerability is confirmed, HSRC team will immediately pass the information to the vulnerability submitter, and then actively track and feedback about the progress of the solution, and will also investigate the vulnerability to ensure that the problem is resolved in all product versions and product models. The HSRC process is closely 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 people before patches or mitigation information is publicly released, it could allow threat actors to exploit vulnerabilities on unpatched systems. All parties must protect their confidentiality throughout the vulnerability disclosure process.

The Hikvision security response team actively participates in industry and public activities, and establishes long-term relationships with CERTs, vulnerability disclosure platforms, customer SRCs, other suppliers, researchers, and third-party coordinating agencies. Hikvision is a member of the internationally renowned vulnerability information database Common Vulnerability & Exposures (CVE) as a CVE Partner. The company is also a member of the China National Vulnerability Database of Information Security (CNNVD), China National Vulnerability Database (CNVD), China National Cyber Security Vulnerability Database (CICSVD). With these memberships, Hikvision can obtain security vulnerabilities discovered by external organizations without delay, improve security emergency response speed, and provide customers with more secure products and solutions.

7.2 Data Life Cycle Security Management

The company's product or service team consider the protection of personal data during the requirements analysis and design phase, and use appropriate technical and management measures to ensure the security of personal data according to specific business use scenarios. A Product Personal Data Statement is included in the product interface, if the company is involved in the processing of personal information. The Statement describes the type, purpose, processing method, retention period, risks or recommendations of all personal data generated in the product.

Data subjects have the right to be informed, the right of access, the right to rectification, the right to erasure (right to be forgotten), the right to restrict processing, the right to data portability, the right to object, and the right to not be subject to automated decisions. To comply with regulations and better protect the data security, functions that support data subjects in exercising the above rights are included in the design and implementation of products and services.

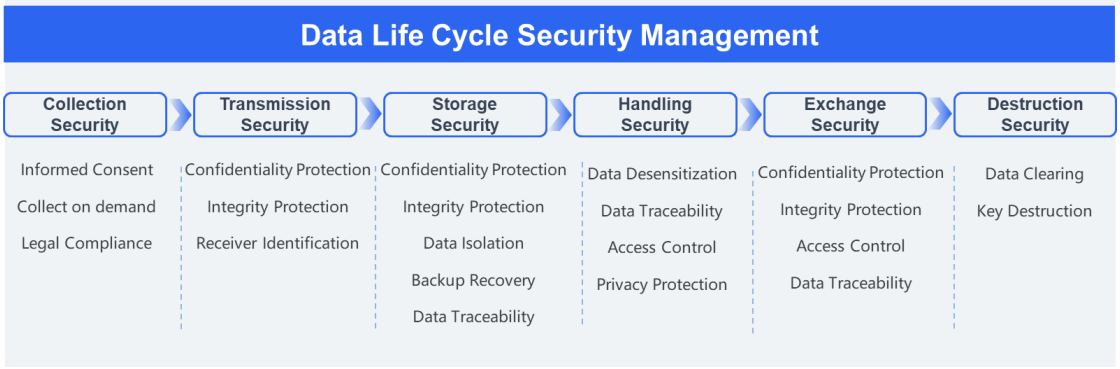


Figure 7-6 Data Life Cycle Security Management

1. Data Collection Security

Compliance with the applicable laws and regulations is a must for data collection. Users must be informed, and principles such as user consent and data minimization should be followed. Data should only be collected as needed, and the scope of collection and purposes of use should be clearly outlined in the personal data policy. 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's crucial to authenticate the identities of both communication parties to ensure that the entity receiving or sending data is a legitimate user. This is primarily achieved through cryptographic techniques like message digests and digital signatures. During transmission, it's essential to prevent data leakage and to detect any tampering with the data. This involves ensuring the confidentiality and integrity of the transmitted data, which can be achieved using encryption, hashing, and digital signatures, among other traditional cryptographic algorithms. Hikvision product transmission security is ensured by utilizing the SSL/TLS protocol to guarantee the confidentiality and integrity of the data.

3. Data Storage Security

When storing data, data can be segregated and stored based on different levels of sensitivity. This can be achieved through various techniques such as physical isolation, logical isolation, or virtualization to create separation between areas containing data of different security levels.

Data storage media can potentially experience malfunctions or data loss. To ensure the availability of stored data, 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's important to establish data traceability mechanisms. This ensures that if data is illicitly leaked, it can still be traced, allowing identification of the source of the leak and enabling relevant audits. Digital watermarking technologies can be employed to achieve data traceability in such cases.

When storing data, it's 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. To achieve this, traditional cryptographic techniques such as encryption, hashing, and digital signatures can be used. These techniques play a vital role in safeguarding data from unauthorized access and tampering.

Data storage security is ensured by employing standard cryptographic algorithms to ensure data confidentiality and integrity. The cryptographic algorithm calculation module provided by

the vendor utilizes cryptographic cards that comply with commercial cryptography specifications.

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 anonymized 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 the data usage process. Hikvision employs techniques such as data anonymization, encryption, and privacy-preserving computing to safeguard personal information during the data processing.

5. Data Exchange Security

Security control on data exchange channels is 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 password technology to ensure data confidentiality, integrity and access control in interacting with data, and employs digital watermarking technology for data traceability.

6. Data Destruction Security

Logical deletion and physical destruction are to be employed for data destruction to prevent the data from being recovered or retrieved after erasure, especially sensitive data such as passwords and keys.

8. Security Technology

8.1 Configuration Management

Configuration Management plays a vital role to guarantee a product's integrity, consistency, and traceability. It contains many processes, including strategy and planning, configuration item identification, configuration item change management, configuration status tracking, configuration activity reporting, configuration auditing, build management, release management, third-party software and open-source component management, and repository management, etc. Configuration management underlines the integrity of Hikvision's product delivery, including third-party software and open-source components within the product. Hikvision's configuration management process constitutes an inseparable part of the IPD process. The aforementioned configuration management steps are conducted at each stage in the Integrated Product Development (IPD) process to promote the implementation of product traceability. They are a key part of security.

Build Management Specifications

Build management specifications include build resource management, build process management, and build process optimization. The segregation of duties is an important part of configuration management. The activities, roles, and responsibilities must be clearly defined in the specifications during the build process. The various stages of product development should be integrated, and the life cycle be clearly incorporated into the IPD process.

Compiling and Build Center

To ensure the repeatability and consistency of the construction process, Hikvision established a compiling and build center. In addition to meeting the management requirements of compilation, the center also 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 offers compilation and build cloud services, supporting software building within the IPD process.

Standardization of the Build Process: unified tool management, standardized build scripts, one-click building, and automated installation of the build environment realize automation throughout the entire product building process, including environment setup, code downloading, one-click compilation, packaging, static checks, and automated unit testing,

up to system testing. This ensures 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 former operates multiple antivirus software tools simultaneously for scanning, integrated into the testing process. For security purposes, the Digital Signature Center employs key pairs stored in a key database to digitally sign the compiled code. Hikvision authorizes and records signature activities to ensure traceability throughout the entire process.

Software and Component Version Management

With its self-developed SWMS software management platform, Hikvision enjoys a structured and standardized software version organizational structure. Focusing on the entire software development process, the platform aligns with the software lifecycle management approach spanning requirements, design, development, integration, testing, and release. It facilitates the intuitive display of software development processes and process data, ultimately achieving artifact management and realizing the goal of effective software management.

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. After completing the version development of a component, it undergoes component version validation. Once validation is successful, the component is submitted 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, whether it includes third-party software, and security status. Hikvision employs a methodology similar to Maven to manage embedded components such as C/C++ components. Each component is integrated using a component configurator that aligns logically with the Project Object Model (POM), gradually assembling them into a finalized software product. Based on the integrated information, a unified version information structure and Software Bill of Material (SBOM) repository are established to track component version application. In case a security issue arises with a specific component version, it allows for quick identification of software versions utilizing that component version, aiding in maintenance and updates. Additionally, the ability to disable problematic component versions and provide replacement versions is offered to prevent issues from spreading unnoticed.

Third-party Component Management

Hikvision procures many third-party and open-source components from around the world and uses them in our products. That is why Hikvision takes the following issues seriously:

- Reliability of the source code or component source
- Compliance with the company's security risk assessment requirements
- Elimination of any known vulnerabilities
- Management of license compliance
- Strategies to address newly discovered vulnerabilities
- Life cycles of third-party components
- Incorporation of third-party components into Hikvision's product life cycle

Hikvision not only needs to assure the security of third-party components, we also need to ensure that the related components required by all compiled source code or third-party components are managed properly. Hikvision has formulated the "Third-party Component and Source Code Management Specifications" to ensure that third-party components comply with our requirements and can be effectively managed.

Hikvision places great emphasis on the compliant, reasonable and secure use of the third-party software. Various binary and source code analysis software, such as FOSSID, Cybellum, etc., are introduced into the management process and integrated with the software management platform to realize automatic detection and ensure an accurate and fast insight into the components of third-party software.

Code Static Analysis

In the quality and security management of source code, Hikvision not only purchases mainstream commercial static detection tools on the market, but also develops a variety of known defect analysis and scanning tools for Hikvision business scenarios.

One of the key self-developed code feature analysis tools is the Tailuge defect intelligent 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 the existence of defects in each branch, the risk situation of each version, and even the impact of orders, so as to ensure that R&D can systematically evaluate defects and work synchronously. We have a complete set of mechanisms to ensure that the defects identified by Tailuge analysis form closed-loops: Before new code branches are generated, we will scan the source code for Tailuge defects. When there are known defects, we will remind relevant personnel to repair in time and support online one-click repair. If there is a specified type of high-risk defect, we will automatically disable the branch, requiring that the defect be repaired first. During the code development process, if there are known defects in the code, we will give an early warning in the IDE used by the developer and push related pending repairs. When the code development is completed to trigger the CI build, Tailuge's defect scanning function will be triggered first to detect whether the current branch version contains Tailuge's known defects. The scan results will inform the builders immediately. If there are specified types of high-risk and high-risk defects, we will directly stop the build and require that the defects be repaired first. In addition, we have also added problem version status management, aligned with PLM to realize software disabling, and also aligned with the production order system, and realized immediate interception of high-risk defect orders.

Another key code feature is the iScan code static scanning platform developed by Hikvision, which supports the detection of serious vulnerabilities such as null pointer references, resource leaks and buffer overflows, and supports industry coding standard detection and rule arrangement capabilities. iScan has both analysis and management functions, it identifies various problems by analyzing the source code, and provides efficient problem management and repairing suggestions. It is integrated with the SWMS software management platform and performs static analysis of the iScan code through the continuous integration pipeline during the software development stage. Developers can pay attention to safety and quality in a timely manner during the development process, and efficiently manage and solve problems in the HSDLC process, covering from task assignment to tracking to problem closure, helping the R&D team to fully understand and improve code quality.

8.2 Security Certification

The global legal environment is complicated and is constantly evolving, and industry supervision requirements are becoming increasingly complex. Particularly in the field of cybersecurity laws, many countries and regions have issued laws and regulations in recent years, such as the Cybersecurity Law of China, and the General Data Protection Regulation (GDPR) of the EU. Security compliance has become a major challenge for Internet of Things service providers. Hikvision strives to establish effective internal control security systems that follow and comply with the requirements of different industries, fields, and countries, while also completing its own compliance foundation in its system processes and control activities. To meet the needs of global business expansion, help the company better comply with global regulations and laws, and promote the normalization of operations in countries and regions, Hikvision established the Compliance Department in December 2018 to improve its global compliance system.

Hikvision has a professional team of lawyers for the investigation, identification, and tracking of laws and regulations that are applicable to the company around the world. Hikvision has also established a long-term cooperation with experienced and prestigious law firms domestically and internationally. We have a dedicated group to integrate the applicable laws and regulations into Hikvision's operations, and to identify and control the legal risks involved in the product development, manufacturing, delivery, and service processes and also to provide compliance advice and support. We continue to conduct special compliance training for new employees, mid and high-level managers, and employees in key cybersecurity posts as new laws and regulations are issued to improve compliance awareness.

Hikvision strives to improve the security integrity of our video 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 complete, sustainable, and reliable security system that involves company policy, organization, process, technology, and specifications.

Hikvision supports mainstream international standards, and contributes actively to the formulation of these standards. 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 Internet of Things.

Hikvision also cooperates with independent third-party assessment organizations and staff for fair security assessments and certification.

Supply Chain Security

Diverse participating entities, numerous process steps, and cross-regional product transfers of supply chain systems render it susceptible to both internal adversities and external threats, such as unauthorized production, tampering, theft, malicious software and hardware implantation, as well as poor manufacturing and development practices within the supply chain. Vulnerabilities in supply chain systems may remain latent for years before being discovered, and in many instances, it's difficult to ascertain whether security events are a direct result of supply chain vulnerabilities. Security issues within the supply chain could exert sustained negative impacts on organizations.

In order to reduce security risks and ensure hardware and software integrity, Hikvision uses anti-tampering, anti-implantation, anti-replacement and other security management measures during key stages of product manufacturing, such as software provision, chip burning/calibration, software loading, and production testing. This helps prevent unauthorized hardware replacement, software implantation and tampering, virus infection and other risks. The product data management system takes the software required by the devices and downloads them onto a secure distribution system. Before software is embedded into devices, multiple integrity checks are conducted.

The network used in the supply chain for software burning, software loading, assembly, and testing should be isolated from the company's office IT system and from the Internet.

Automated testing is implemented for Hikvision products. Hikvision uses automated testing to reduce the risk and security threat brought about by human errors.

Besides by technical means, Hikvision also guarantees its supply chain security by management system. ISO 28000 supply chain security management system is aimed at comprehensively improving supply chain security, and helping organizations and departments deal with potential security risks in supply chain by auditing security risks and implementing control and mitigation measures. ISO 28000 is compatible with ISO 9001 quality management system and ISO 14001 environmental management system, and can be integrated with them in the organization.

After specifying the operating environment of supply chain, identifying threats from various links and conducting risk assessment and response, Hikvision established a supply chain security management system that fully complies with ISO 28000, and has realized continuous update and improvement of the system with the management method of PDCA (plan–do–check–act).

Hikvision has implemented a secure and strict maintenance process to ensure the integrity of products during the process. Information from the entire process is recorded in Hikvision's manufacturing and barcode systems. A detailed executive record and log is kept for the research and development, procurement, manufacturing (chip burning, software loading, assembly, testing, etc.), warehousing, and logistics processes to ensure traceability.

Common Criteria / ISO 15408

CC (Common Criteria) certification is one of the most widely recognized international certifications in the field of information technology security. It is endorsed by the United States National Information Assurance Partnership (NIAP), which operates under the oversight of the National Institute of Standards and Technology (NIST). It is also recognized by countries such as the United Kingdom, Canada, and other Western nations. Currently, security certification organizations from 31 countries around the world have joined the CC Recognition Arrangement (CCRA). Since CCRA members are either government agencies or third-party authoritative organizations in their respective countries, CC certification has high acceptance and credibility on a global scale. It has become an important foundation for security assessments.

CC certification is primarily used to evaluate the security, reliability, and privacy protection of information technology products or solutions. The certification is divided into seven levels based on the Evaluation Assurance Levels (EAL), ranging from EAL1 to EAL7, with increasing levels of verification requirements.

In September 2018, two series of Hikvision cameras were certified with EAL2+[1], and another three series of cameras with EAL3+ in June 2022. Hikvision is committed to making all products up to the EAL3+ standards, thus improving the company's security practices to new heights and setting a great example within the industry.

[1] CC certificate query: https://www.commoncriteriaportal.org/

ISO/IEC 27001

ISO/IEC 27001 Information Security Management System (ISMS) is the most authoritative, rigorous, widely accepted, and 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, showcasing Hikvision's information security management capabilities 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 General Data Protection Regulation (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 British Standards Institution (BSI) 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.

CMMI5 Software Maturity Certification

Capability Maturity Model Integration (CMMI) is an enterprise-level process management framework and a best practice used by the world's top companies. It is recognized by the industry as the authoritative standard for measuring an enterprise's product and service capabilities. It is also a method for improving processes that can help companies achieve commercial goals, ensure quality, guarantee deliveries and improve customer satisfaction levels. There are five maturity levels which companies are assigned in the Software CMMI specifications. Level 5 is the highest level.

Hikvision successfully passed CMMI5 certification in April 2016.

Information Security Level Protection Certification

The Information Security Level Protection 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 levels based on factors such as the importance of the information system in national security, economic development, and social life, as well as the degree of harm to national security, social order, public interests, and the legitimate rights and interests of citizens, legal persons, and other organizations after being destroyed. The fifth level is the highest system level.

According to the relevant provisions of the "Management Measures for Information Security Level Protection", both EZVIZ Cloud and Hikvision's internal information systems have passed the third-level evaluation of information security level protection. 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.

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.

In December 2021, Hikvision achieved CSA-STAR certification.

GDPR

Hikvision is always committed to protecting personal data and will fully support the implementation of the GDPR. Hikvision has been taking a number of initiatives to protect personal data, including data collection through authorization, minimization of data collection, data anonymization, communication and storage encryption, data security audit, etc.

To ensure the security of products and services, Hikvision has put forward a series of data protection policies and established a data protection working group, integrating GDPR requirements into the business operation.

8.3 Product Security Research and Collaboration

The Network and Information Security Laboratory is dedicated to research and practical applications of security in the Internet of Things. Our work includes penetration testing, fuzz testing, source code auditing, reverse analysis, vulnerability research, tool development, and analysis of IoT security solutions. Our team's main research areas cover web security, mobile security, protocol security, wireless security, firmware security, threat intelligence, machine learning, and many other fields. Our goal is to discover and solve security issues before hackers can exploit them.

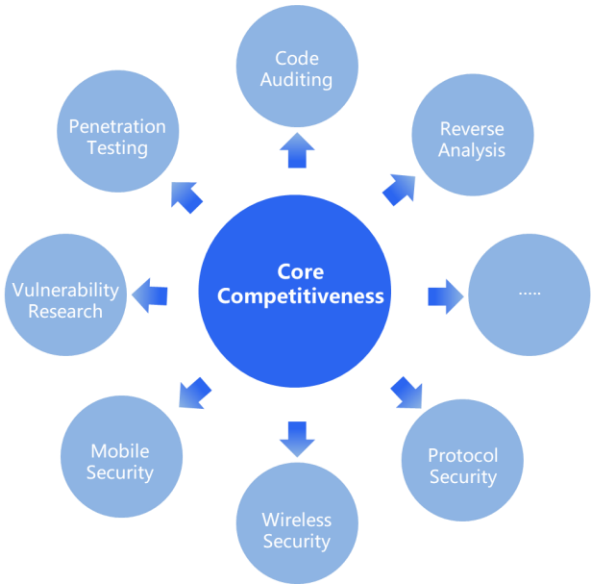


Figure 8-1 Research on core competitiveness of product security

Core Competitiveness:

- **Embedded Device Vulnerability Mining:** Benefiting from experience in embedded device security, Hikvision employs firmware reverse, firmware emulation, serial debugging, static analysis, symbolic execution, and other means for vulnerability mining.

- **Protocol Vulnerability Mining:** Integrating commercial tools and self-developed fuzzing testing tools to automatically mine high-risk vulnerabilities in mainstream IoT device protocols, hundreds of which have been discovered to date.

- **Wireless Security Research:** The team has a variety of security hardware testing environments, including RFID, wireless radio frequency, and Bluetooth modules, which can achieve wireless data packet eavesdropping, wireless signal replay attacks, wireless signal deception attacks, wireless signal hijacking attacks, RFID cracking attacks, and NFC cloning attacks.

- **White-box Audit:** Integrating commercial tools to track and detect known vulnerabilities of all open-source components used internally and provide threat warnings; the internal team will conduct white-box auditing of target source code during penetration testing to comprehensively improve vulnerability mining efficiency.

- **Web Security:** Commercial tools and proprietary web testing utilities are integrated with crawler-based reconnaissance techniques and passive proxy technology to conduct

penetration testing on web platforms. This approach supports the detection of various web security issues such as SQL injection, cross-site scripting (XSS), sensitive information leakage, and command injection. The core security testing team will perform in-depth penetration testing on the target system to uncover more potential security vulnerabilities.

- **Mobile Security:** The team integrates internal mobile security detection and analysis tools to conduct comprehensive security testing on mobile apps, supporting real-time capture of interaction protocol messages and automatic identification of sensitive information; supporting detection of known vulnerabilities in the Android kernel; supporting personal data compliance testing of apps; supporting security reinforcement of mobile apps to prevent malicious attacks.

- **Threat Intelligence:** The team builds various types of distributed high/low interaction honeypots, which can sense all kinds of malicious IoT attacks and capture attack samples in real-time and conduct real-time correlation analysis and warning.

- **Machine Learning:** The team uses machine learning algorithms to conduct security analysis of IoT device logs, providing various security attack detection models, which can quickly detect potential or known malicious attack behaviors from massive logs and conduct real-time threat warnings.

Security Engine

1. IoT Security Protection Engine

In order to continuously improve the detection and defense capabilities of IoT devices against cyber threats, the Network and Information Security Laboratory team has independently developed intrusion defense and protocol firewalls for security detection and protection engines that can be applied to IoT devices. This achieves a comprehensive monitoring of the status of IoT devices, full perception of risks, and real-time blocking of attacks for security protection capabilities. The engine supports non-destructive upgrades through hot updates to cope with new types of network attacks, providing reliable and stable operation of IoT devices.

2. Intrusion Prevention Engine

The intrusion prevention engine is specifically designed and developed for the IoT devices of a company. The IoT devices are equipped with built-in intrusion defense engine modules at

the factory. After booting up, the engine monitors and analyzes the real-time status and operational behavior of the device's files, networks, processes, and other aspects. It blocks the startup and operation of malicious processes through a process whitelist. It also monitors and detects malicious file creation, deletion, modification, and other operations, and intercepts them. Moreover, the engine monitors and blocks abnormal device external network behavior in real-time, preventing the possibility of IoT devices being controlled as zombie network bots.

3. 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 for use. In order to effectively defend against common cyber-attacks on device security and stability, 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 content from the business module and conducts cyber-attack behavior detection before the message enters the business 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 attack target based on the interception strategy. By deeply integrating with the business module, this solution overcomes the pain point of traditional security protection products' inability to detect encrypted messages and can comprehensively detect and analyze various IoT protocols, effectively resisting various common cyber-attacks and enhancing the security and stability of IoT devices.

Security Situational Awareness

The enormous Internet of Things system, formed by devices, network, platforms and applications, requires multi-layer protection and End-Cloud Collaboration with smart, big data security analysis capabilities. The implementation of smart security situational awareness, visualization, and security for entire networks will be an emerging trend for the Internet of Things.

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 8-2 Security Situation Awareness

Vulnerability Assessment

Vulnerability assessment is key to determining the effectiveness of a security situational awareness system in detecting security vulnerabilities. The Hikvision security situational awareness system integrates mainstream vulnerability databases to conduct checks on existing vulnerabilities. In addition, Hikvision has a professional vulnerability research team that continually tracks security announcements released by other well-known security organizations and vendors. The team also continuously analyzes, explores, and verifies various new vulnerabilities. With the continuous investment of Hikvision's professional vulnerability research team and the continuous upgrading of the vulnerability database, users can be promptly alerted to potential security risks and take preventive measures.

Furthermore, the Hikvision video security situational awareness system can perform correlation analysis on discovered security threats and asset information. By establishing a big data analysis model and dynamically analyzing real-time and historical data, the system can accurately and efficiently perceive the security status and development trends of the entire network. This enables users to make reasonable security reinforcements for video security networks and ensure the security of video security systems.

Security Visualization

Security visualization can present data characteristics intuitively and be easily accepted and understood by readers. Therefore, big data analysis (such as deep packet inspection and full

traffic analysis) results require visualization.

When a system is under attack, it is necessary to quickly identify the source of the attack, the attack path, and respond to the attack quickly. Effective measures should be implemented before the attack causes greater damage in order to reduce losses. After the attack, it is necessary to quickly prevent such attacks from happening again.

Honeypot

Honeypot technology is essentially a deceptive technique used against attackers. By deploying some hosts, network services, or information as bait, attackers are lured into attacking them, allowing for the capture and analysis of the attack behavior, understanding the tools and methods used by the attacker, and inferring the attack intent and motivation.

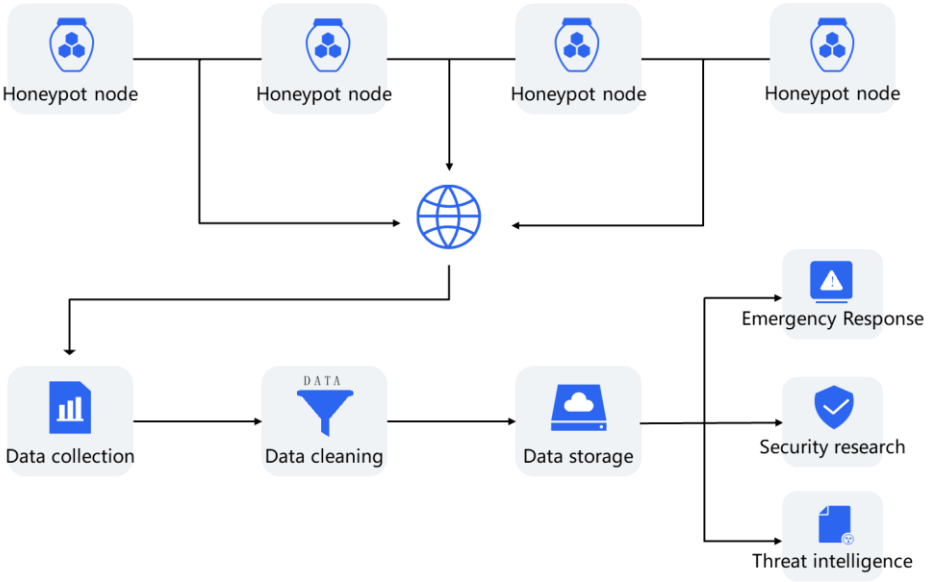


Figure 8-3 Honeypot system

Benefiting from the rise and development of technologies such as data storage, retrieval, mining, and threat intelligence, the value of honeypot technology can be more fully realized. Hikvision has deployed honeypot nodes worldwide based on self-developed and modified honeypots as data collectors, and has established a honeypot data pipeline for collecting, processing, storing, and retrieving honeypot data, providing data support for security research, emergency response, attack tracing, and situational awareness.

Hikvision's honeypot system is based on a rule engine that monitors attacks on IoT devices in real time and issues alerts for unknown threats. The analysis engine of the honeypot system can focus on monitoring and correlating analysis of malicious attackers based on historical data from the honeypot system, and predict threat trends.

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

Digital Watermark

Data watermarking refers to the embedding or implicit marking of display in data files (such as videos, audios, images, documents, databases, models, etc.) based on information security, information hiding, data encryption and other technologies, in order to cope with traceability and copyright declaration after data leakage.

The digital watermarking system mainly includes two stages: embedding and extraction. In the embedding stage, the main goal of the embedding algorithm is to find a better compromise between the invisibility and robustness of the digital watermark. The extraction stage includes an extraction algorithm corresponding to the embedding process. At present, in order to prevent attackers from removing the watermark, most watermarking schemes use keys in embedding and extraction, and only those who have the key can read out the watermark. Data watermarking is the last line of defense against data leakage. Therefore, from the perspective of watermarking technology itself, it has broad application prospects and huge economic value.

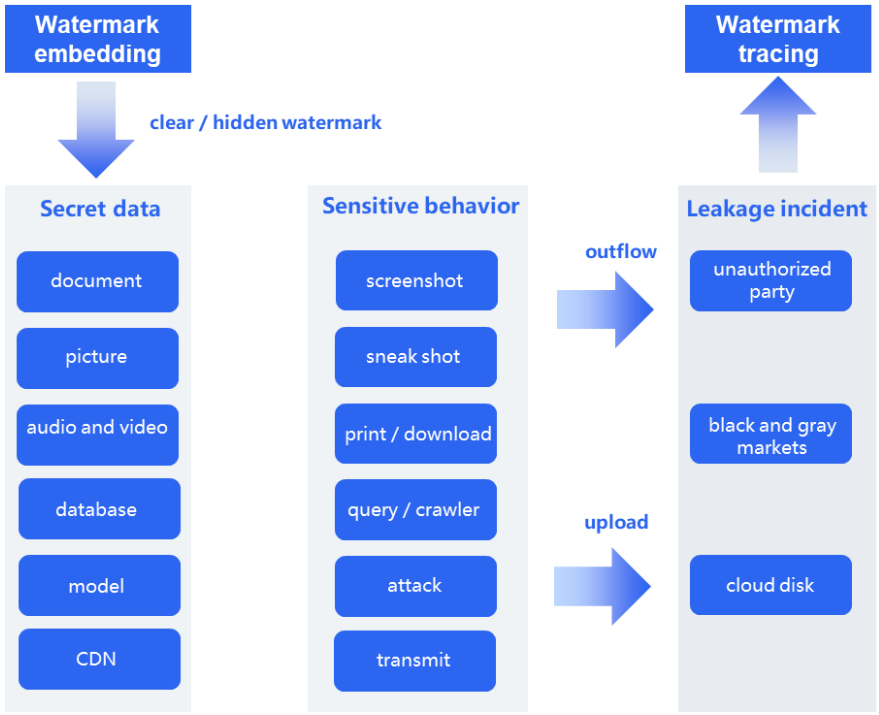


Figure 8-4 Digital watermark

Exchange and Collaborations

- Invite well-known domestic and foreign security assessment institutions to benchmark and construct the company's R&D security management system, ensuring that Hikvision's R&D security system is in line with international first-class companies.

- Strengthen communication and cooperation with domestic and foreign security vendors to enhance the security of the company's products.

- Invite well-known domestic and foreign security testing teams to conduct penetration testing on the company's products, minimizing business risks to maintain security risks within a controllable range.

- Invite well-known domestic and foreign security experts to the company to teach R&D personnel, improving their competencies of security.

- The company communicates with customers several times a year on product security topics, emergency response mechanisms, and security requirements, and timely pushes security progress to customers to understand their needs.

- The "Security White Hat Rewards Program" launched by the company to reward domestic and foreign white hats who pay attention to Hikvision's information security, and to collaborate with excellent security technology researchers who promote the continuous improvement of Hikvision's product security.

Figure 8-5 Exchange and Collaborations

Hikvision through external exchange and collaboration, accepts feedback from stakeholders, absorbs advanced security technology and management experience in the field, systematically transforms them into future improvement goals, and continuously improves the company's information security capabilities.

9. Security Commitment

Hikvision is committed to using leading security and personal data protection technologies to help customers protect their personal information and to adopting a comprehensive approach to protect user data.

Hikvision uses a unified integrated security infrastructure throughout the entire video IoT application ecosystem. Hikvision has a professional security team responsible for supporting all Hikvision products. This team provides security audits and testing for products released or under development. The security team also provides security training and actively monitors reports of newly discovered security issues and threats. To learn more about how to report issues to Hikvision, please contact us here:

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

Hikvision
Cybersecurity White Paper

See Far, Go Further

HIKVISION®

Hangzhou Hikvision Digital Technology Co., Ltd.
No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China