Hikvision Cybersecurity White Paper

www.hikvision.com

About this Documentation

Hikvision Cybersecurity White Paper is proposed to make an overview of Hikvision's current practice on product cybersecurity issues and to provide an open and transparent angle to the public to access Hikvision's cybersecurity capabilities.

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

Copyright Disclaimer

This Documentation shall not be reproduced, translated, modified, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision.

Trademarks Acknowledgement

海康威视 , HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

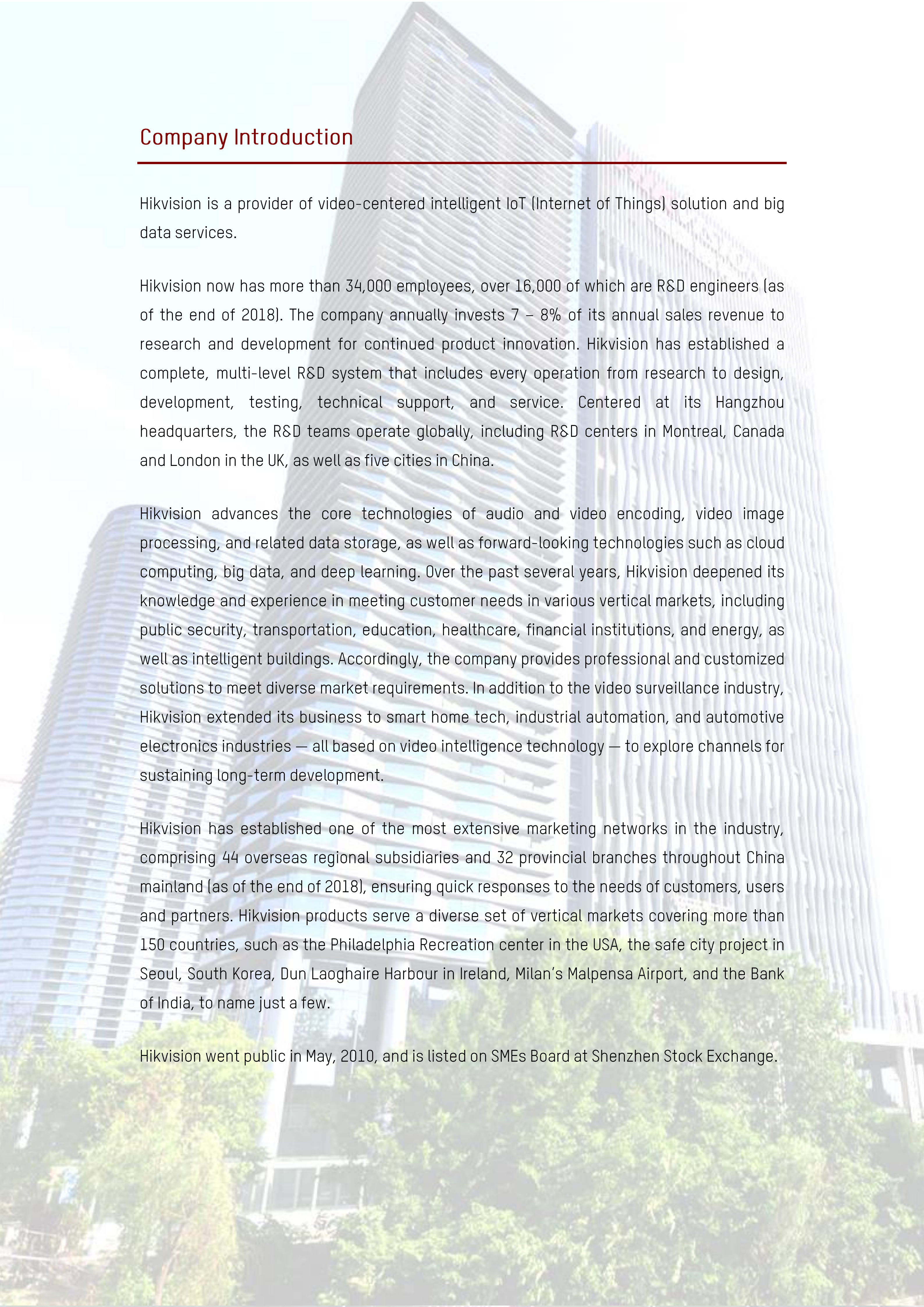
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE CONTENT DESCRIBED IN THIS DOCUMENTATION IS PROVIDED "AS IS", AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, FITNESS FOR COMMERICAL USE OR A PARTICULAR PURPOSE.

HIKVISION PROVIDES NO WARRANTY ON THE ACCURACY OF THIS DOCUMENTATION CONTENT, AND RESERVES RIGHTS TO CORRECT OR MODIFY THE CONTENT WITHOUT FURTHER NOTICE. ANY DECISIONS RELIED ON OR BY THE USE OF THIS DOCUMENTATION TOGETHER WITH ANY CONSEQUENCES THAT IT MAY CAUSE SHALL BE UNDER YOUR OWN RESPONSILIBITY.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Revision Record

New release – January, 2018；First revision – May, 2019



Company Introduction

Hikvision is a provider of video-centered intelligent IoT (Internet of Things) solution and big data services.

Hikvision now has more than 34,000 employees, over 16,000 of which are R&D engineers (as of the end of 2018). The company annually invests 7 – 8% of its annual sales revenue to research and development for continued product innovation. Hikvision has established a complete, multi-level R&D system that includes every operation from research to design, development, testing, technical support, and service. Centered at its Hangzhou headquarters, the R&D teams operate globally, including R&D centers in Montreal, Canada and London in the UK, as well as five cities in China.

Hikvision advances the core technologies of audio and video encoding, video image processing, and related data storage, as well as forward-looking technologies such as cloud computing, big data, and deep learning. Over the past several years, Hikvision deepened its knowledge and experience in meeting customer needs in various vertical markets, including public security, transportation, education, healthcare, financial institutions, and energy, as well as intelligent buildings. Accordingly, the company provides professional and customized solutions to meet diverse market requirements. In addition to the video surveillance industry, Hikvision extended its business to smart home tech, industrial automation, and automotive electronics industries — all based on video intelligence technology — to explore channels for sustaining long-term development.

Hikvision has established one of the most extensive marketing networks in the industry, comprising 44 overseas regional subsidiaries and 32 provincial branches throughout China mainland (as of the end of 2018), ensuring quick responses to the needs of customers, users and partners. Hikvision products serve a diverse set of vertical markets covering more than 150 countries, such as the Philadelphia Recreation center in the USA, the safe city project in Seoul, South Korea, Dun Laoghaire Harbour in Ireland, Milan's Malpensa Airport, and the Bank of India, to name just a few.

Hikvision went public in May, 2010, and is listed on SMEs Board at Shenzhen Stock Exchange.

CONTENTS

1. A letter from CEO

The “Internet of Everything” is turning from dream to reality. As a forerunner to the “Internet of Everything”, video surveillance technology has developed rapidly over the past 10 years. It moved from the analog era to the digital era, then to the network era, and is now entering the smart era. Improvements in technology can advance human society, but they may also present new challenges. The development of Internet technology, for example, has largely benefited human society, but it has also brought about cybersecurity challenges. The same is true for Internet of Things (IoT) technology, which was developed based on the Internet, is similar to the Internet in that it vastly improves human life. However, it has also created new challenges for society. Cybersecurity is one such challenge.

The surveillance industry entered the digital era later than the IT industry, and cybersecurity awareness remains relatively weak within the surveillance industry. In 2014, Hikvision founded the “Security Emergency Response Center” to form a centralized external interface to deal with cybersecurity issues. In 2015, Hikvision established the “Network and Information Security Laboratory” which was fully incorporated into Hikvision’s cybersecurity system. A product security committee was formed, as well as a Network and Information Security Laboratory and Network Security Department. The company also established a security testing laboratory and a network security system which focused on organization, procedures, and especially network security design. It was created to improve the overall cybersecurity standards of the company’s products and systems.

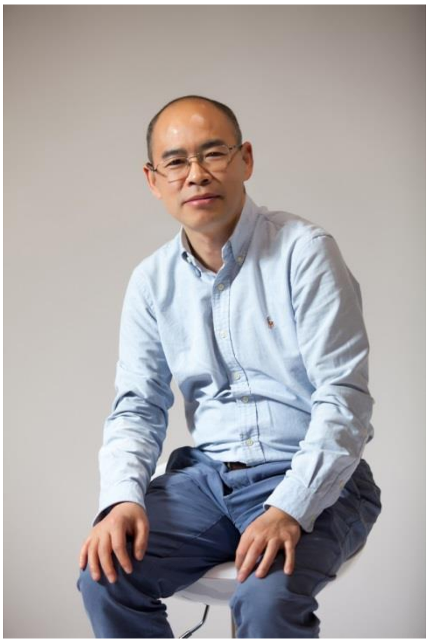
Cybersecurity is not only the responsibility of product manufacturers. Everyone who participates throughout a project's lifecycle, including users, system integrators, operators, system designers, other service providers, are all responsible for using cybersecurity best practices and face the same challenges of cybersecurity. The solution to this problem is 30 percent technology and 70 percent management; all stakeholders need to work together to contend with cybersecurity obstacles.

During this time when the surveillance industry desperately needs cooperation to solve the issues we all face, we have noticed public and media attention and concern about IoT security. This makes us keenly aware of our responsibility and mission. Hikvision upholds the company values of “corporate value dedication to client’s success, value oriented, integrity and down-to-earth, pursuit of excellence” Hikvision prioritizes responsibility to our clients' network and information security over company profits.

Cybersecurity challenges will always be around, so we must remain vigilant and keep working on improving product security.

Hu Yangzhong, President

Hangzhou Hikvision Digital Technology Co., Ltd.



2. Preface

Over the past five years, we have witnessed the progression of digitalization in the surveillance industry and also seen the industry's rapid development. In these five years, we have seen how the smart surveillance industry has explored 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 smart surveillance industry must conform to digitalization, networking, and smart technology trends. However, cybersecurity is a completely new field for the surveillance industry and the openness of networks have interconnected security systems which were formerly independent and completely isolated, promoting data flow and sharing in ways that have drastically improved society. This has brought about even more innovative opportunities, enabled the Internet of Things industry to grow, and has pushed the development of civilization to new heights.

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

Hikvision is a global company, and services more than 150 countries and regions. As a company of such scale, Hikvision takes these challenges very seriously. As one of the world's leading security solutions providers, Hikvision deeply understands, from a technological perspective, how to support and promote the health, prosperity, and safety of the world's citizens.

Cybersecurity is not just a problem for certain countries or companies. All stakeholders, governments, and companies must understand that cybersecurity is a problem that everyone in the world faces, and that meeting these challenges requires international cooperation, risk aversion methods, and use of cybersecurity best practices. With the sharp rise in "cyber-attacks in America"[1], ransomware like "EternalBlue" and similar incidents, it is

[1] https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

apparent that we have entered a new era in the fight against cybercrime. 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 have done in the past, we encourage our clients to help us improve our procedures, technology, and cybersecurity techniques to enable us to bring even more benefits to them and their customers.

3. Security Threats in the Internet of Things

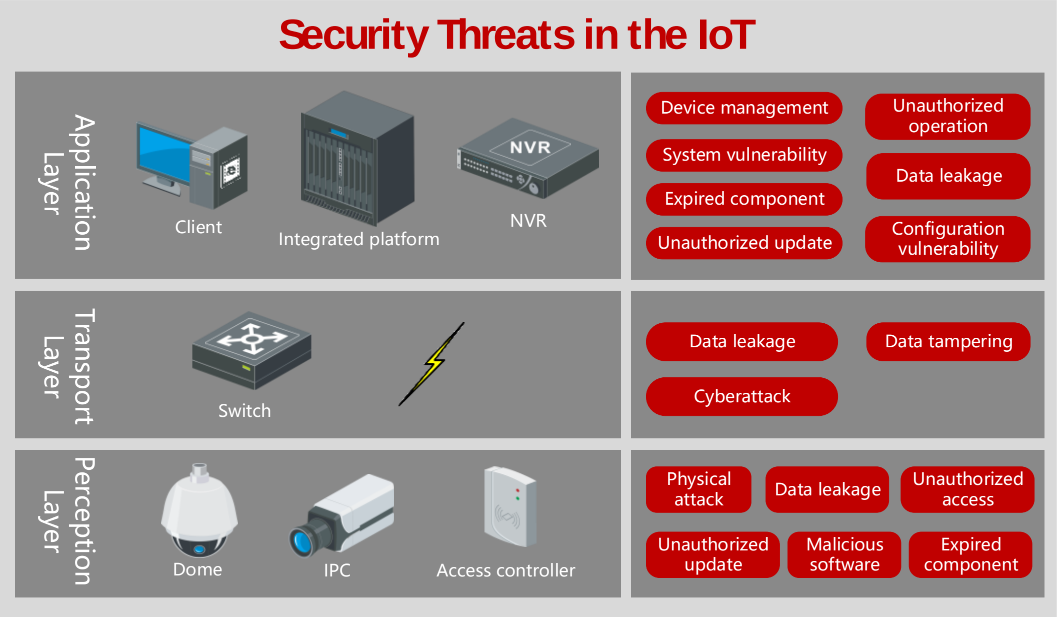
The Internet of Things (IoT) connects "smart devices" from all over the world through the Internet and allows for the interaction between people and things on a global scale. The interconnection of massive devices has made networks more open, complex and diversified. However, the advent of IoT also brings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

In addition to the traditional network security threats, there are still some special security issues in the IoT. This is due to the fact that the IoT is composed of a large number of unattended devices or perceptive nodes, which are not consistently maintained. Based on the IoT framework, security threats in the IoT can be categorized as perception-layer threats, transport-layer threats, and application-layer threats：

The Perception Layer is the physical layer.

The Network Layer is responsible for connecting and facilitating communications between other IoT devices, network devices and servers.

The Application Layer is responsible for interfacing with users by accepting and providing data to those users.



Perception-layer threats

- Physical attack:

IoT assets that lack physical protection are susceptible to theft or damage and can easily be accessed without authorization.

Outdoor devices and distributed installations must have the appropriate physical controls to prevent physical attack, tampering, and counterfeiting.

- Data leakage:

Sensitive information that is not properly encrypted and secured could be read and possibly altered. This includes data at rest (stored on the device) and data in transit (moving across a network)

- Unauthorized access:

In many IoT devices, default usernames and passwords are used for ease of installation, however if end users do not change from those defaults, it gives attackers an easy way to gain access to the device. A similar attack can be successful if the end user creates weak, easily guessed passwords.

Some IoT devices use test and debug ports in the firmware, prior to releasing to the public. If these ports are not closed, it can give an attacker a means for executing code, and potentially taking complete control of the device.

- Unauthorized update:

All computers, including all IoT devices, will require security updates and sometimes feature updates from time to time. These updates are an attractive target for attackers by either pretending to be an official update or tricking a user into installing a malicious update, or trying to embed malicious code into a valid update. To prevent this, computer and IoT vendors need to have a code verification process to ensure that only valid code from the vendor can run on that hardware. Without this verification, malware installation is possible.

- Expired components:

When an IoT device is manufactured, it is installed with the latest code. However, by the time an end user installs the device, the code may be outdated and require software updates and patches. Unless there is a process for automated patching, many IoT devices are left vulnerable to attacks that have already been patched by the vendor because the end user did not know, or remember, to manually patch the device regularly

- Malicious software:

If an attacker is successful in gaining access to an IoT device, it is likely that they will install malicious software, or malware, on that system. The type of malware that is typically installed on IoT devices is called Trojan Horse malware and it gives the attacker a remote control of the IoT device's computing resources. Once the attacker has access to enough devices (thousands, or tens of thousands, or more) they create something called a botnet. The attacker is usually not interested in the data on the IoT device, rather, they want to use the computer in the IoT device as part of their botnet Internet weapon. When the attacker wants to attack a website or anything connected to the Internet, they can tell all of the botnet-infected devices to attack at the same time

Some famous examples of botnets include Mirai, Bashlite, Lizkebab, Torlus and Gafgyt, to name just a few, which can cause large-scale Distributed Denial of Service, or DDoS attacks. The Mirai botnet was used to take down and slow down parts of the Internet by infecting IoT devices, including home routers, video surveillance cameras and video recorders.

Transport-layer threats

- Cyberattack:

Attackers can gain unauthorized access to a network that uses wireless networks by exploiting Wireless protocol vulnerabilities. For example, weak authentication may allow an attacker to connect to the network and watch and record all network traffic.

If an attacker can gain unauthorized access to a network, he or she can monitor that network traffic and if it is not encrypted, they can see all of the data as it traverses the network. Unencrypted communication is prone to hijacking, repeating, tampering, and eavesdropping by an attacker.

- Data leakage:

During communication between IoT devices, cloud hosting servers, and mobile devices, attackers can access sensitive data if the network traffic is not encrypted.

- Data tampering:

When a device communicates through a network, the data collected by an attacker may be altered by attackers if there is no verification mechanism. This is called a man-in-the-middle attack

Application-layer threats

- Device management:

There are difficulties in managing the update process and security of the various and scattered devices managed by the platform layer.

- Unauthorized access:

User accounts need to be unique for each person and account credentials must not be shared. If account credentials are shared, there is no individual accountability and may result in leakage of sensitive data, and cause a privacy and security breach.

- System vulnerabilities:

Operating systems allow humans and applications to run on hardware. Most IoT devices run Linux, Windows, Android, and iOS as their operating system. The majority of large-scale network attacks focus on exploiting known vulnerabilities in operating systems that have not been patched.

- Data leakage:

The application layer manages a large volume of data, which is prone to leakage if not encrypted.

- Expired components:

The application layer has significantly more components than IoT devices do. If those components are not updated properly in time, unpatched vulnerabilities may exist and be easily exploited.

- Configuration vulnerabilities:

Security configurations that haven't been updated or examined for a long time may have configuration issues that can be exploited by network attackers.

- Unauthorized update:

Unofficial software that is updated without verification may have vulnerabilities, or the software itself may be malicious.

After considering the many hidden security risks in the IoT environment, as well as the complexities of computational capabilities and the complex hardware and software environment, Hikvision created its video-centric IoT solution with an all new security framework. The goal is to establish a multidimensional security system that can ensure device, data, application, privacy, and network security, as well as security compliance. Below, six aspects of product security technology are described to explain how security technologies and functions are implemented in Hikvision's IoT solution.

4. Network and Information Security in the Surveillance Industry

The surveillance industry began as analog before moving to digital. During the analog era, surveillance systems operated in private networks, so the industry was focused on product cost, performance, and ease of use. The cybersecurity features of the systems at that time were not the main focus, but as the surveillance industry developed rapidly toward network connectivity, it moved directly from analog to digital, the industry's initial failure to contemplate cybersecurity issues led to the advantages of the original analog equipment, such as its strong usability, to deviate from the best information security practices for the digital era. In the past, surveillance industry vendors generally enabled default support for all protocols to make it more convenient for users to use devices from all manufacturers. They also enabled automatic protocol selection in the server. Although these settings make it much more convenient for the client, they do not follow information security best practices.

The surveillance industry has encountered cybersecurity issues in recent years because of the way the products and the industry developed. However, the existence of these issues does not mean the entire industry is as vulnerable as some might claim. Furthermore, the industry is now making a concerted effort to deal with potential security risks, and is implementing effective counter-measures.

Objectively speaking, cybersecurity issues are not issues specific to the surveillance industry, but are issues that society as a whole face. Looking at the overall field of IT, cybersecurity issues exist in all fields, and the following basic consensus exists:

➢ The Prevalence 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.

➢ Security is for the Entire System

The security of a system cannot be guaranteed by the security of a single point. The entire system must be secured. To ensure the security of video surveillance systems, the front-end, back-end, network, security devices and the platform system must work together and complement each other to form a system that provides defense in depth. A cybersecurity issue with any device in the link will be a vulnerability that could expose the entire system.

➢ Third-Party Open Source Software Security

A variety of third-party open source software is currently used in various types of systems. Such software is open, shared, and free, and is playing a growing role for software developers. Open source software is also a very important component in the software supply chain. But as companies enjoy the benefits of open source software, such products also carry huge security risks. In recent years, open source software has suffered frequent high risk vulnerabilities, for example Struts2, OpenSSL, etc. Many of these components are used in the lower layers of information systems and have a very broad scope of application. Vulnerabilities therefore exhibit critical security risks and have been detrimental to entire industries, not just specific products.

➢ Security is in Dynamic Balance

There is no such thing as “absolute” security. Security can only be relative. Offensive and defensive games are always zero-sum. Mechanisms and techniques that are considered secure today may be insecure tomorrow. Products that are considered “secure” today may be hacked tomorrow. This means that there is no final destination in security. Every product will possibly have information security risks and challenges during its life cycle. The question is if and when these risks would be exploited, while it is hard to predict.

➢ Products Security Management

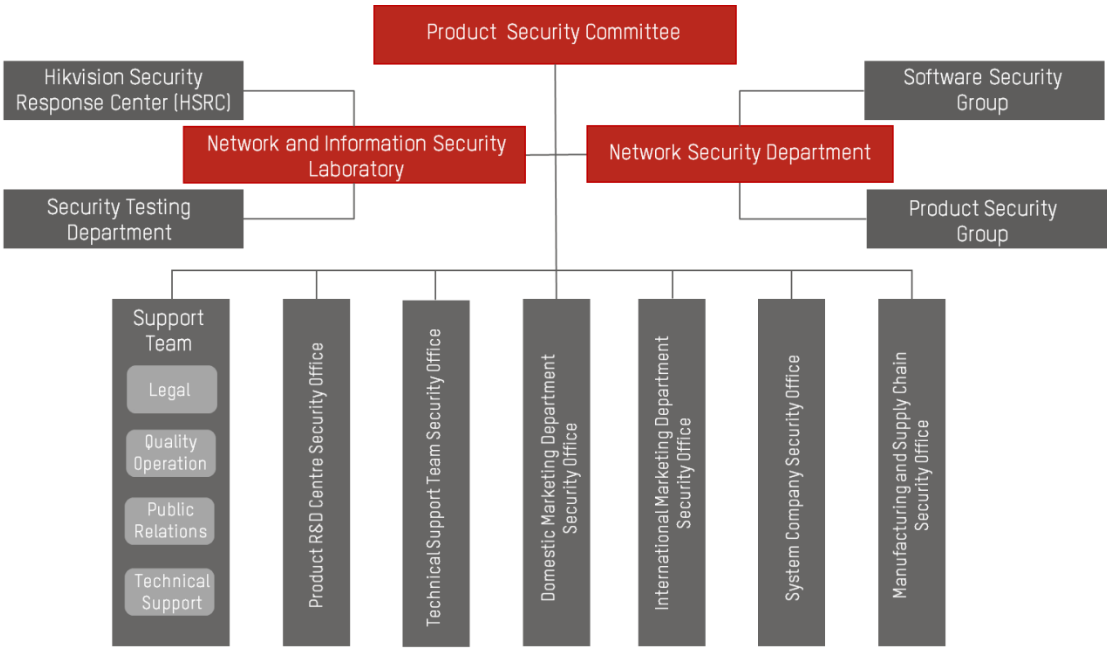
The most important element in system security is security management. Even with systems that are more secure, if the user cannot manage or operate them properly then system security cannot be maintained. Currently, some security issues within the surveillance industry are mainly due to “inappropriate” usage by users and by 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 to the latest firmware and install patches as soon as possible. Eventually, all Internet-connected devices need to support a patching process that informs users when a patch needs to be installed.

5. Product Security Life Cycle

This section is structured as seven aspects that introduce Hikvision's work to create the product security life cycle.

5.1 Organization

To ensure that product security assurance activities are incorporated into 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:


Product Security Committee
Hikvision Security Response Center (HSRC)
Network and Information Security Laboratory
Security Testing Department
Network Security Department
Software Security Group
Product Security Group
Support Team
Legal
Quality Operation
Public Relations
Technical Support
Product R&D Centre Security Office
Technical Support Team Security Office
Domestic Marketing Department Security Office
International Marketing Department Security Office
System Company Security Office
Manufacturing and Supply Chain Security Office

Product Security Committee

The Product Security Committee is responsible for strategic planning and policy making for company network and information security. In terms of network information security, if any conflict or serious issue arises, the committee has the authority to make decisions and make necessary adjustments to services. Hu Yangzhong, the President of Hikvision acts as the head of the product security committee. The Product Security Committee has set up a specialized Network Security Department which formulates network and information security strategies, policies, procedures, and standards, and manages resource allocation on a daily basis.

Network Security Department

As a standing body of the Product Security Committee, the Network Security Department is responsible for the implementation of product security strategies, the establishment of product security baselines, the implementation of product security assessments, external cooperation regarding product security, industry product security technical standards research, promotion of product security research and development, participation in reviewing major events in product security, and for providing suggestions to company leaders. It is also responsible for combining 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 various 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 awareness, product security components, security video surveillance products, penetration testing, IoT security defense and other areas. The laboratory aims to research the cutting-edge of IoT security technology and promote its improvement. All laboratory staffs boast many years of experience in information security, and over 50% of them have obtained CISP (Certified Information Security Professional) or CISSP (Certified Information Systems Security Professional) certification.

HSRC: Hikvision Security Response Center

The Hikvision Security Response Center is responsible for receiving, processing, and revealing Hikvision security vulnerabilities related to products and solutions. Hikvision values its own security and has always strived to safeguard user security. We also hope to use the center as a platform to enhance cooperation and exchange within the industry.

Product Line Security Offices

Each Hikvision product line has a product security office, which works with the Network Security 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 security requirement testing on the product line.

Security Testing Department

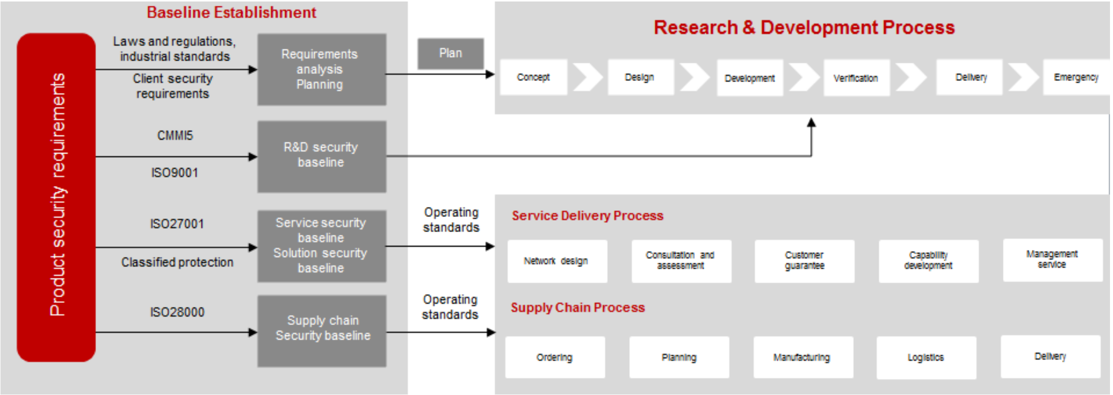
The Security Testing Department is a third-party department independent of the product lines and is responsible for the product security testing for all of Hikvision's product lines. It is responsible for inspecting the company's product security policies, and whether or not the security baselines are implemented effectively in the 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.

5.2 Procedures and Standards

Hikvision has formulated a set of general security baselines for product security based on current domestic and international laws and regulations, industry standards, customer security requirements, third-party analysis, industry activities, peer experience, and specific service security requirements. It also includes specifications and standards for security baselines for various product lines, secure coding, safe password usage, security key management, secure session management, security certification, security testing, security incident management and so on. These specifications and standards cover all aspects of product security.



General Provisions for Product Security

The General Provisions for Product Security is an outline for the company's product security matters and mainly includes product security policies, goals, organization, management, procedures, and activities. The General Provisions for Product Security is the general outline and blueprint for the company's product security and will form the basis for all lower-level documents.

Product Security Procedure Documents

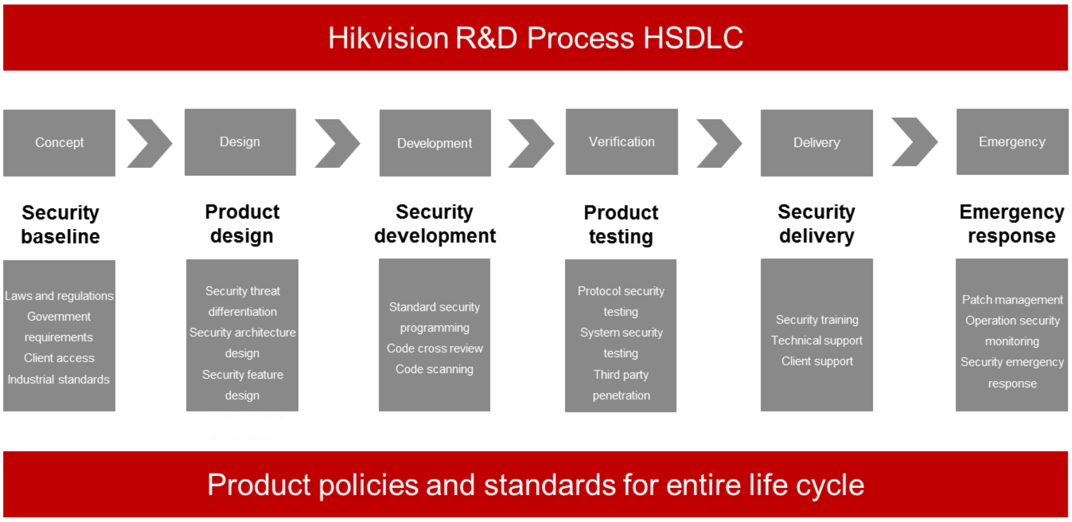
Product security has been incorporated into core company procedures, and security management procedures are formulated according to requirements. For example, the product security incident response procedures are formulated according to product security assessment details and red line requirements. Technical requirements and templates for product security baselines are formulated in accordance with the guidelines for product security requirement outlines. Product security baselines, supply chain security baselines, and service security baselines are formulated for each product line. Best practices for the security baselines are also established, and product security testing requirements and testing templates are also formulated.

Security Baseline

Company products do not only include self-developed products, but also third-party products. Since the security standards for various products and systems are different, in order to ensure company product security standards, inspection and reinforcement is required for the security of the delivered product so that it reaches the security baseline and so that known security threats are eliminated. Security baselines are formulated in accordance with product R&D, third-party product procurement, system operation and maintenance, security reinforcement, security testing, and security management. Before mass production of new products, security baseline checks must be performed. Only after ensuring that the requirements are met can mass production begin.

5.3 Security Research and Development Process HSDLC

We have incorporated a broad range of security activities into the R&D process, including security design, security development, security testing, combining Hikvision's wide ranging research and development activities and referencing the industry's best security practices, such as OpenSAMM, BSIMM, CSDL, MSDL and customer feedback. We ensure that the security activities are effectively implemented, and improve product health, enhance privacy protection, and provide more secure products and solutions for our clients. Besides, Security training will be organized regularly to raise staff's security awareness and capability.



Hikvision R&D Process HSDLC

Concept → Design → Development → Verification → Delivery → Emergency

Security baseline
Laws and regulations
Government requirements
Client access
Industrial standards

Product design
Security threat differentiation
Security architecture design
Security feature design

Security development
Standard security programming
Code cross review
Code scanning

Product testing
Protocol security testing
System security testing
Third party penetration

Security delivery
Security training
Technical support
Client support

Emergency response
Patch management
Operation security monitoring
Security emergency response

Product policies and standards for entire life cycle

Concept Stage

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

First, the product security baseline should be in the mandatory requirement list. The product security baseline is used to guarantee the basic requirements of implementing security goals or risk control at an acceptable level. The security goals come from international or domestic laws and regulations, customer input, industrial standards, etc., and their objective is to ensure security standards are met, to protect user communications and privacy, enhance system access control/sensitive data protection, and to increase system defensive capabilities.

Second, threat analysis will need to be performed on these products in the future at the application scenario to identify other targeted security requirements. Threat analysis is used to find the source, type, and point of attack of threats in situations where the products are used. This is performed to make it easier for us to evaluate risks and ensure that the related measures are incorporated into the product requirements list.

Design Stage

The threat modeling and attack surface verification are the most complex and also the most important parts of SDL process. The purpose of threat modeling is to understand the potential threats to the system, identify risks, and establish appropriate countermeasures. Threat modeling enables problems to be resolved in the early stage of the software development lifecycle and helps to effectively control product security risks.

1. Based on the logical architecture, the threat modeling for the product is established on architectural level with the method of STRIDE, aiming to recognize potential security threat on architectural level and make mitigation measures accordingly.

2. Security design and function design are integrated together. When conducting function design, we also establish threat modeling on function level to timely recognize security threats in the design and make mitigation measures accordingly.

3. Collected and recognized security requirements will be analyzed and designed in detail, and there will be special security working group in the company to provide technical supports for 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.

Development Stage

During the development stage, product developers perform cross-reviews in accordance with secure coding specifications. The automatic code scanning tool, Coverity Static Analysis, is used for quick and accurate scanning for high-risk functions and defects in highly complicated code. This reduces the chances of code security issues. By applying the self-developed code defect analysis and scanning tool designed for business scenarios of the company, we can identify the known defects by code features, after which, we inform the R&D staff of the existence of defects in each branch, evaluate whether the defect synchronization is in place, and then we conduct interception in the continuous build activity, so as to realize the control of known code problems in the source code stage and greatly reduce the repair cost.

Verification Stage

In order to guarantee the security of Hikvision products and to prevent the occurrence of various types of security issues during the research and development stage, we perform security tests at every stage in this process:

- During product security testing, Hikvision enhances protocol security testing, using protocol security testing tools, Defensics from Codenomicon and Peach Fuzzer to perform network protocol security, robustness, and reliability analyses for all products, and to find unknown vulnerabilities;

- The vulnerability scanning tools, Nessus Professional and NSFOCUS Remote Security Assessment System (RSAS), are used during the system security testing stage to keep track of CVE[2] vulnerability information. This enables the discovery of various types of weaknesses in the system, including security vulnerabilities, security configuration issues, and application system security vulnerabilities;

- Dynamic application security testing tools, such as IBM AppScan, Burp Suite and Acunetix WVS, will be adopted in the application security testing, helping to discover vulnerabilities in Web applications

- Mainstream antivirus software such as Symantec or Avira are used before a product is released to find known viruses, Trojans, backdoors and other malicious software;

- The company also regularly invites well-known security companies and public testing platforms to conduct penetration testing. To minimize business risks and keep security risks under control, as many penetration tests as possible are performed.

- The network security team will regularly analyze issues found in the testing, producing a general "TOP N" issues list, and then push it to each product line for self-inspection, so as to prevent similar problems from happening again.

Configuration Management

Configuration Management is an important activity to guarantee product's integrity, consistency, and traceability. Configuration management contains many processes,

[2] CVE：The world's most authoritative vulnerability database: Common Vulnerabilities and Exposures, http://cve.mitre.org

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 is an inseparable part of the IPD process. The aforementioned configuration management activities are conducted at each stage in the 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 should be clearly incorporated into the IPD process.

Compiling and Build Center

To ensure the build process is repeatable, Hikvision has established a build center where all hardware, compilation tools, third-party software, data sources and operating systems meet a rigorous set of standards and support requirements. The build center is the integrated solution for product building and compilation and it provides a cloud service to support software-building activities during the IPD process.

Standardization of the build process: Using centralized management of tools, standardization of building scripts, one-click building, and automated installation of build environments, the entire building process is automated, including environment building, source code downloading, one-click compiling, packaging, static code review, automated unit testing, and system testing. This ensures that the product build process is repeatable, traceable, and can be restored.

The build center also has two additional functions: virus scanning and digital signatures. The virus scanning center runs dozens of antivirus programs simultaneously and is integrated into the testing process. For security reasons, the digital signature center uses a source code compiled with a key from a key database for digital signatures. Hikvision authorizes and records signature activities to ensure that the entire process is traceable.

Component Management

Hikvision applies component-based development model to develop products. After the development, the component will enter the verification stage, and then it will be pushed to the component library of the software management system (SWMS) that is developed by Hikvision, which will identify the information of each component, e.g. name, group, version, running platform, source code, static analysis results, the usage of third-party software, security information, etc., and is also equipped with the lifecycle management function. Hikvision manages embedded components, such as C/C++, in a Maven-like manner, and integrate components into a finished software through component configurators that are consistent with the POM (Project Object Model) logic. Based on the integrated information, a unified version information structure and software Bill of Material (BOM) library are established to track the application of components. Once any security problem occurs in certain component, the software using the component will be positioned quickly for maintenance and upgrade.

Tool and Third-party Component Management

Hikvision procures many third-party and open source components from around the world, and applies them into its products. That is why Hikvision takes the following issues seriously:

- Reliability of the source code or component source
- Security risk assessment requirements of the company
- Known vulnerabilities that still exist
- Authorized compliance management
- How new vulnerabilities are handled
- Life cycles of third-party components
- Incorporation of third-party components into Hikvision's product life cycle

Not only does Hikvision need to consider 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 complies 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 ProteCode SC, BlackDuck Hub, BlackDuck Protex, etc., are introduced into the whole 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.

Innovative Management of the Version and Source Code

Hikvision manages various configuration items of source code, documents, libraries, components, product software, etc., then establishes different management tools for each different object, and incorporates these management tools to form an integrated software development platform SWMS. The relationships among all libraries, components and software are managed in an orderly and structured way to facilitate tracking and backtracking.

Security Delivery

Technical support staffs are front-line employees of the company for serving customers, and may have access to potentially sensitive information (with the customer's consent). Mandatory network and information security training are therefore essential so that they can help protect customer interests and prevent access control issues, communication security issues, and privacy data protection issues. In terms of employee management, Hikvision formulated the "Hikvision Technology On-site Support Service Standards" according to ISO27001 and other standards. These specifications include codes of conduct, personal safety, information security, etc.

Hikvision strictly manages employees' network access. Employees are required to sign letters of commitment which stipulate their roles, duties, and potential legal liabilities in detail. They are also required to take cybersecurity training and participate in relevant tests.

Emergency Response

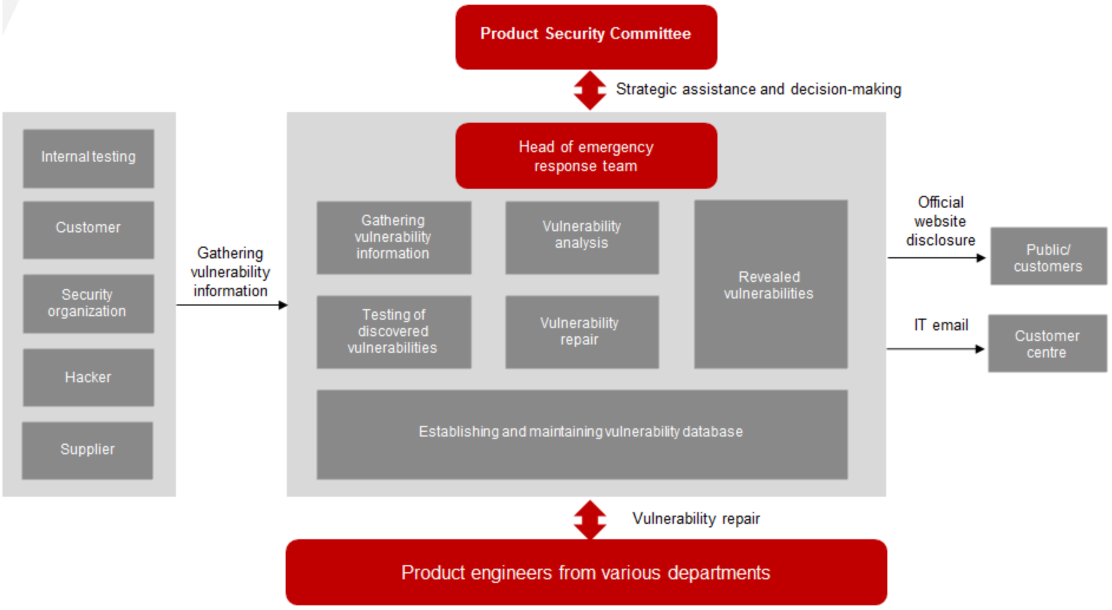
Hikvision established the Hikvision Security Response Center (HSRC), which is responsible for accepting, processing, disclosing, and resolving security-related vulnerability issues with Hikvision's products and solutions. Responsibilities include:

- Responding to and handling customer-submitted security incidents
- Responding and handling security matters announced 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.

There are clear provisions for the effectiveness of security matters. For example, initial confirmation of security incidents must be completed in less than 24 hours, and high-risk vulnerabilities must be corrected within 30 days.

As an important member of Forum of Incident Response and Security Teams (FIRST), Hikvision is committed to sharing the best practice and disposal experience with other member teams globally, enhancing trusted communication and cooperation and improving its own efficiency and performance in incident response.


Product Security Committee
Strategic assistance and decision-making
Internal testing
Customer
Security organization
Hacker
Supplier
Gathering vulnerability information
Head of emergency response team
Gathering vulnerability information
Vulnerability analysis
Revealed vulnerabilities
Testing of discovered vulnerabilities
Vulnerability repair
Establishing and maintaining vulnerability database
Official website disclosure
Public/ customers
IT email
Customer centre
Vulnerability repair
Product engineers from various departments

Vulnerability Management

Hikvision follows ISO/IEC 30111, ISO/IEC 29147, and other specifications to establish procedures for processing and warning about product security vulnerabilities. These include four stages:

- Vulnerability research and data collection: We obtain vulnerability information via customers, external CERT, security researchers, and related security websites. At the same time, our internal teams are constantly looking for potential security threats. We encourage responsible disclosures, that is, if an external agent discovers a vulnerability, they should give the manufacturer a suitable amount of time to process and solve the issue before disclosing it to the public.

- Security vulnerability assessments, analysis, and verifications: For suspected or confirmed vulnerabilities, the HSRC team will work with the person responsible for the product to quickly complete practical and related risk assessments.

- Tracking and solution: Once a vulnerability is confirmed, the HSRC will immediately forward information to the person who submitted the vulnerability and actively track the process and feedback. They will also investigate the vulnerability to ensure that the issues will be resolved for all affected versions and models of the product. The HSRC process and the core research and development process are tied closely together to ensure timely response to vulnerabilities.

Hikvision strives to protect customer confidentiality and information about vulnerabilities during every stage of the process. If vulnerability information falls into the hands of those with malicious intent, it may lead to adverse consequences. All parties must protect the confidentiality of this information.

Hikvision's Security Response Team actively participates in industry and public activities and has established long-term relationships with CERT, vulnerability disclosure platforms, client SRCs, other suppliers, researchers, and third-party coordinating agencies. Hikvision has been designated as a Common Vulnerability and Exposures (CVE) Numbering Authority (CNA). This appointment enables Hikvision to get access to security vulnerabilities in time after they discovered by outside organizations, improve security response, and provide customers with securer products and solutions.

5.4 Supply Chain Security

Supply chain system has the characteristics of complex and diverse participants, numerous process links and steps, and cross-regional product delivery, which make it vulnerable to internal adverse factors and external threats. Security threats to the supply chain system includes unauthorized production, tampering, theft, malicious software and hardware implantation, as well as non-compliant manufacturing and development practices in supply chain. Vulnerabilities in supply chain systems may remain latent for years before discovered, and in many cases it is difficult to determine whether a security incident is a direct result of a supply chain vulnerability. Therefore, supply chain security issues have the potential to have a lasting negative impact on the organization.

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 error.

Besides by technical means, Hikvision also guarantees its supply chain security by management system, such as ISO 28000 supply chain security management system, which is aimed to comprehensively improve supply chain security, and to help 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.

5.5 Security Compliance

The global legal environment is complicated and is constantly evolving, and industry supervision requirements are becoming increasingly complex. Particularly in the field of cybersecurity law, many countries and regions have issued laws and regulations in recent years, for example the EU (General Data Protection Regulation). 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 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 be responsible for the construction of the global compliance system.

Hikvision has a team of lawyers for the investigation, identification, and tracking of laws and regulations that are applicable to the company. At the same time, Hikvision also actively establishes long-term cooperation with experienced and prestigious law firms domestically and internationally. We have established 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.

As stated in the "Statement on the Establishment of the Cybersecurity Guarantee System for Video Surveillance Products," Hikvision strives to improve and complete the integrity of our video surveillance security. In addition to abiding by the applicable national and local security regulations, 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. By late 2016, Hikvision had already joined dozens of domestic and international industrial standards organizations such as TC260[3], TC100[4], CSA[5], and ONVIF[6]. 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.

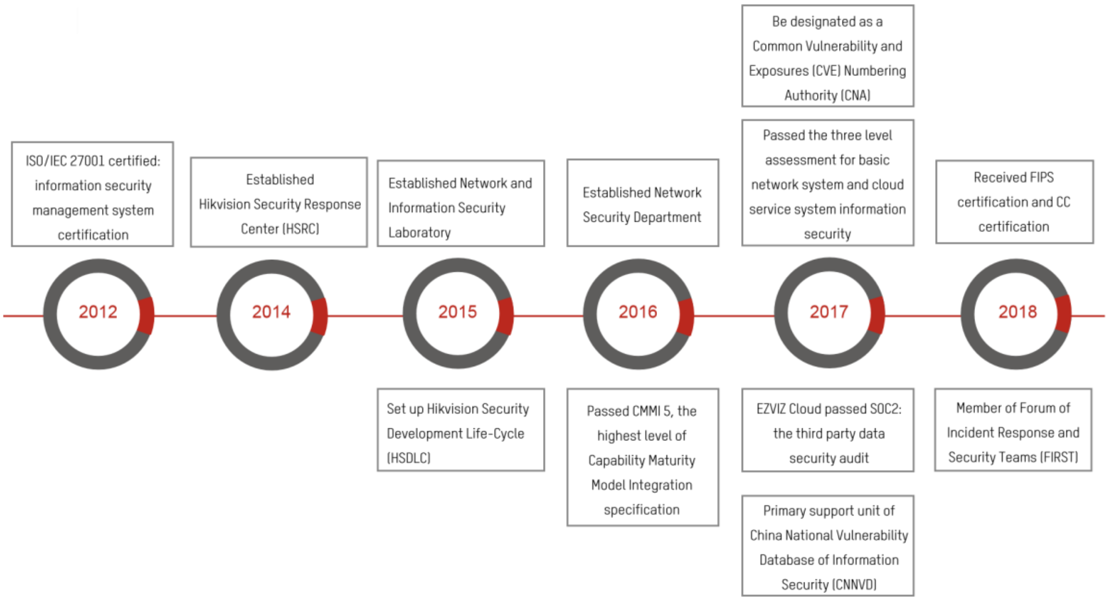
Hikvision also cooperates with independent third-party assessment organizations and staff for fair security assessments and certification.

[3] http://www.tc260.org.cn/

[4] http://www.tc100.org.cn/

[5] Cloud Security Alliance: https://cloudsecurityalliance.org/

[6] Open Network Video Interface Forum: https://www.onvif.org/



2012
ISO/IEC 27001 certified: information security management system certification
2014
Established Hikvision Security Response Center (HSRC)
2015
Established Network and Information Security Laboratory
Set up Hikvision Security Development Life-Cycle (HSDLC)
2016
Established Network Security Department
Passed CMMI 5, the highest level of Capability Maturity Model Integration specification
2017
Be designated as a Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)
Passed the three level assessment for basic network system and cloud service system information security
EZVIZ Cloud passed SOC2: the third party data security audit
Primary support unit of China National Vulnerability Database of Information Security (CNNVD)
2018
Received FIPS certification and CC certification
Member of Forum of Incident Response and Security Teams (FIRST)

FIPS 140-2

FIPS 140-2 establishes the Cryptographic Module Validation Program (CMVP) as a joint effort by the National Institute of Standards and Technology (NIST), a division of the U.S. Department of Commerce, and the Communications Security Establishment (CSE) for the Government of Canada. FIPS 140-2 is used by U.S. and Canadian government agencies, and regulated industries such as finance, healthcare, legal, and utilities, as well as commercial businesses. It is used and referenced by numerous standards bodies and international testing organizations, including the ISO standard.

Hikvision has achieved FIPS 140-2 certification with certificate number 3228[7] in July, 2018. Cryptographic modules in all similar products of Hikvision are exactly the same and comply with FIPS requirements. For future new products, Hikvision will continue to submit modules for corresponding verification.

Common Criteria / ISO 15408

As one of the most widely recognized international standards (ISO/IEC 15408) in information technology security, the Common Criteria certification is mainly applicable to evaluating security and reliability of information technology products or solutions, and is also focused

[7] For FIPS 140-2 Certification, please refer to: https://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.

on the protection of private information. Government organizations or government agencies from 28 countries have participated in the Common Criteria Recognition Arrangement (CCRA), including National Information Assurance Partnership, Department of Defense of U.S. Many enterprise organizations also use CC as a requisite in relevant procurements.

Hikvision's relevant products have achieved the CC certification with assurance type EAL2 augmented with ALC_FLR.2 (EAL2+)[8]. It demonstrates Hikvision's commitment to global customers on reliability and cybersecurity.

Hikvision will actively participate in the development of currently unimplemented protection profiles (PPs), and will continue to conduct evaluation and certification based on the new and updated versions of PPs that are already implemented.

ISO/IEC 9001

ISO/IEC 9001 is currently the world's most well-established quality management system. This system revolves around company products or services, and provides guiding principles and specifications. Making sure company products and services pass the entire quality management structure is fundamental for the company's growth and development.

ISO/IEC 27001

ISO/IEC 27001: The 2013 Information Security Management System is the most authoritative, strict, and widely accepted system certification standard for information security in the world. Passing this certification will mean that a company has already established a scientifically valid information security management system. Together with a unified company development strategy and information security management, it is guaranteed that information security risks will be controlled to an appropriate degree and that appropriate responses will be given. EZVIZ Cloud is the first home-use security cloud service provider in China to receive the ISO/IEC 27001:2013 certification. Using these information security management control measures and the framework for information asset protection, and continuing to follow the PDCA improvement guidelines, we are committed to information security and will provide reliable information services and related security guarantees.

[8] For CC certification, please refer to: https://www.commoncriteriaportal.org/products/

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.

Graded Protection of Information Security

The Graded Protection of Information Security Certification is a basic system used for information security protection in China. It serves as a basis for the protection of developments in informing and maintaining national information security. The security protection levels for information systems utilize a five-level grading scale with a maximum system rating of five. This scale is based on the system's importance in terms of national security, national economy, and society in general; it also considers the potential harm to national security, social order, public welfare, and the potential degree of damage to the legal rights and interests of citizens, legal entities, or other organizations. Level 5 is the highest system rating.

In accordance to the relevant stipulations in the "Administrative Measures for the Graded Protection of Information Security", EZVIZ Cloud and Hikvision's internal information systems have passed the Level 3 grading for information security protection and strictly adhere to the technical guarantees and security management requirements of the national information security standards. They have also established their own long-term mechanisms to guarantee the continuation of security related work in the future.

SOC Audit

System and Organization Controls (SOC) Reports are given by professional third-party accounting firms according to related standards issued by the internal control department of the American Institute of Certified Public Accountants (AICPA).

The SOC 2 report references the AICPA auditing standards of AT-C section 105, 205, and TSP section 100 2017 in SSAE No. 18, and is a report that focuses on security, availability and confidentiality related control designs for cloud service systems.

SOC 2 report: cloud user organizations, independent auditors, supervising organizations, company shareholders, and other stakeholders can use the SOC 2 report to assess the cloud provider's internal control mechanisms (including security, availability, process integrity, confidentiality and privacy).

In February 2017, EZVIZ Cloud passed SOC2 third party data security audit.

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 - the British Standards Institution (BSI) and the international Cloud Security Alliance (CSA), which is the world's leading organization 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 computation, and finally produces an independent third-party audit result.

In January 2019, EZVIZ Cloud 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.

5.6 Personnel Management

Hikvision aims to create a company-wide culture of security knowledge and awareness. In order to do this, Hikvision has conduct network security training for all new employees, organized general cybersecurity awareness and educational activities and has launched educational activities and training based on various types of cybersecurity knowledge and the skills required by various services. Hikvision will also hold cybersecurity case study classes targeted at the characteristics of surveillance industry. Hikvision will publish cybersecurity periodicals on its internal notification platform and will also use posters, pamphlets and other methods to spread information about cybersecurity.

Hikvision has identified key posts in regard to cybersecurity for each area of service and has clearly defined key posts for product security.

The following requirements apply to employees in key posts related to product security:

- Before an employee assumes the post, they must pass a background check to ensure that they possess a background and history that matches the clients' needs. The *Confidentiality Agreement for Key Security Positions* will be signed to clarify the confidentiality obligation of employees.

- An employee must pass qualification standards when they assume a post which encourages them to increase their awareness and improve related skills. We will also conduct regular security reviews. The behavior of employees in key cybersecurity positions is investigated to decide whether any violations have occurred.

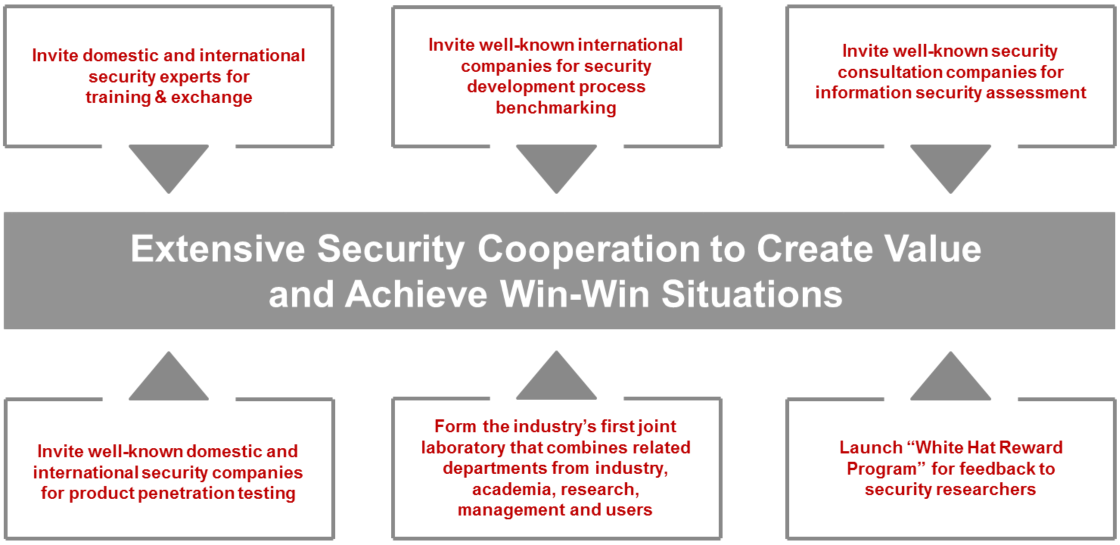
- When an employee leaves their post, the HR and security staff delete or modify the permissions and accounts of the departing employee according to a post-departure review. If necessary, the employee’s assets will also be cleared. The post-departure review also applies to transfers and terminations.

In order to improve our staff's technical knowledge so that they can perform their duties effectively, Hikvision has formulated a targeted security improvement plan and baseline course which improves employee cybersecurity capabilities via a learning plan.

The company aims to improve the cybersecurity knowledge and skills of employees in key posts and encourage employees to proactively learn on their own. By launching a broad range of specialized training activities that follow practical guidelines, Hikvision hopes to improve cybersecurity knowledge and the skills of employees in key posts. For example, Hikvision hosts cybersecurity expert seminars, cybersecurity forums and cybersecurity case studies.

We require all of our employees to take technical and legal responsibility for the outcomes of their individual actions. Our employees know that cybersecurity incidents can significantly impact clients, the company and other personnel. Hikvision therefore holds employees accountable for their actions and the outcome of their actions, whether intentional or not.

5.7 Exchange and Cooperation



Invite domestic and international security experts for training & exchange

Invite well-known international companies for security development process benchmarking

Invite well-known security consultation companies for information security assessment

Extensive Security Cooperation to Create Value and Achieve Win-Win Situations

Invite well-known domestic and international security companies for product penetration testing

Form the industry's first joint laboratory that combines related departments from industry, academia, research, management and users

Launch "White Hat Reward Program" for feedback to security researchers

- EY from the United Kingdom was invited to evaluate Hikvision's overall information security practices and to help improve the company's cybersecurity system;

- Cisco's security department was invited to benchmark the company's research and development security management system to ensure Hikvision's R&D security system matches that of world-class companies;

- Hikvision increased exchange and cooperation with domestic and international security companies, such as Synopsys and IBM, to improve the security of the company's products.

- Hikvision invited well-known domestic and international security testing teams for penetration testing on the company's products. Minimizing risks to ensure that they remain within a controllable range;

- Hikvision invited EY from the United Kingdom for SOC2 audit for the company's products, to ensure the security and confidentiality of cloud products;

- Hikvision invited well-known domestic and international security experts to offer classes for Hikvision's R&D personnel and to improve their security standards;

- Every year, the Network and Information Security Laboratory holds multiple product security workshops with clients to exchange knowledge regarding emergency response and security requirements, inform clients of new tactics in security, and to better grasp client requirements;

- The company has also launched the "White Hat Rewards Program" to encourage domestic and international white hat hackers to review Hikvision's information security and give feedback so that Hikvision can continue to improve product security.

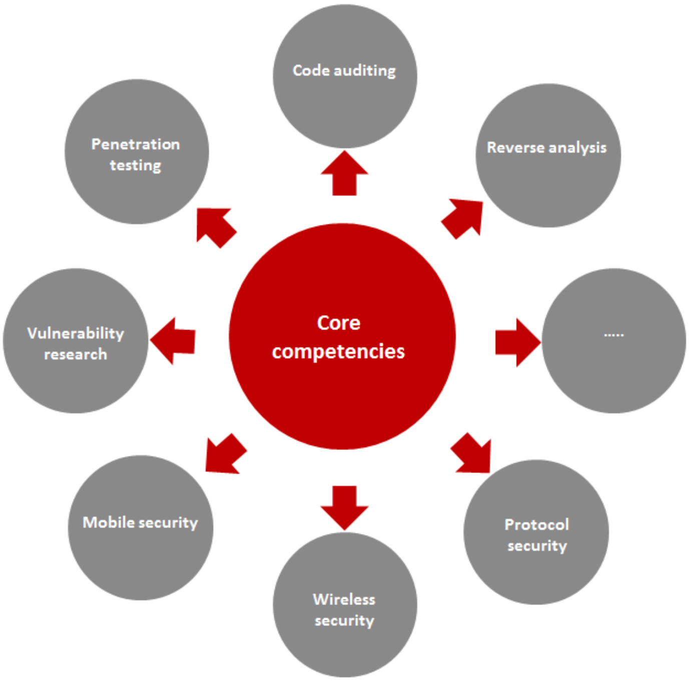
Hikvision also engages in external exchange and cooperation and accepts feedback from stakeholders. Hikvision absorbs advanced techniques and management experience from other surveillance industry leaders and constantly strives to improve the company's information security capabilities.

6. Product Security Research

6.1 Technology research

The Network and Information Security Laboratory is dedicated to the security research and practice of IoT, including penetration testing, fuzzy testing, source code audit, reverse analysis, vulnerability tracking, tool development, analysis and research of IoT security scheme. The main research direction of the team covers WEB security, mobile security, protocol security, wireless security, firmware security, threat intelligence, machine learning, etc., aiming to discover and solve security problems before hackers do.

As a technical support unit of China National Vulnerability Database of Information Security (CNNVD) and a security response support unit of National Industry Security Industry Alliance (NISIA), the team has also become a member of China Cyber Threat Governance Alliance (CCTGA).



Core competencies:

Embedded device vulnerability discovery: combining Hikvision’s experience with embedded device security and using firmware reverse engineering, serial port debugging, static analysis, symbolic execution, and other methods to discover vulnerabilities.

Protocol vulnerability discovery: integrating both commercial and self-developed fuzzy testing tools for vulnerability discovery in mainstream security protocols.

Wireless security research: the team has various hardware security testing environments for RFID, radio frequency, Bluetooth, etc., and can achieve wireless data message eavesdropping, wireless signal replay attack, wireless signal spoofing attack, wireless signal hijacking attack, and RFID attack defense.

White-box audit: integrated commercial tools will track and detect known vulnerabilities in internal open-source components and provide threat alerts. The internal team will conduct white-box audit on the target source code in the penetration testing process to comprehensively improve the efficiency of vulnerability exploitation.

Web security: system integrator tools, self-developed web testing tools, crawler detection and passive proxy technologies are used for penetration testing of the web platform. These tools support the detection of SQL injection, XSS cross-site scripting, sensitive information leakage, command injection and various other types of web security issues. The core security testing team will conduct in-depth penetration testing on the target system to find more potential security vulnerabilities.

Mobile security: with the internal mobile security detection and analysis tool, the team carries out an all-round security detection on the mobile APP, supporting real-time capture of interactive protocol messages, automatic identification of sensitive information, detection on known vulnerabilities in the Android kernel, security reinforcement and prevention against malicious attack.

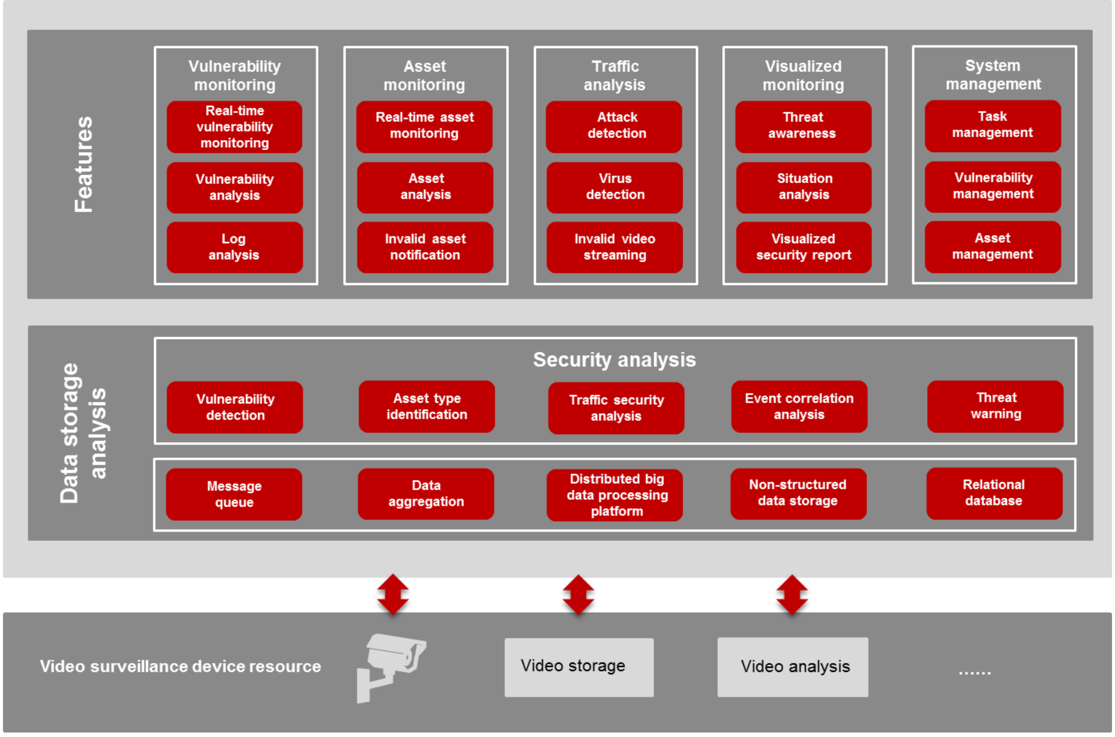
Threat intelligence: the team builds a variety of distributed high interactive honeypots, which can perceive all kinds of IoT malicious attacks in real time and carry out real-time correlation analysis and early warning.

Machine learning: the team makes use of machine learning algorithm to conduct security analysis on logs of IoT devices, and provides a variety of security attack detection models, which can quickly detect potential or known malicious attacks from massive logs and provide real-time threat alert.

6.2 Security Situational Awareness

The enormous Internet of Things network system, formed by devices, network, platforms and applications, requires multi-layer protection and cloud-based, 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, and display of important security elements that can cause changes in the system state within large-scale system environments.



Vulnerability Assessment

Vulnerability assessment is key to deciding whether or not the security situational awareness system can effectively detect security threats. Hikvision's security situational awareness system incorporates the mainstream industrial vulnerability database and can detect known vulnerabilities. Furthermore, Hikvision has a team of vulnerability researchers who are constantly keeping track of the security announcements by other well-known security organizations and manufacturers, and are constantly analyzing, discovering, and verifying various types of new vulnerabilities. Thanks to the continuing work of Hikvision's professional vulnerability research team, security threats are discovered in a timely manner and remediation measures are taken.

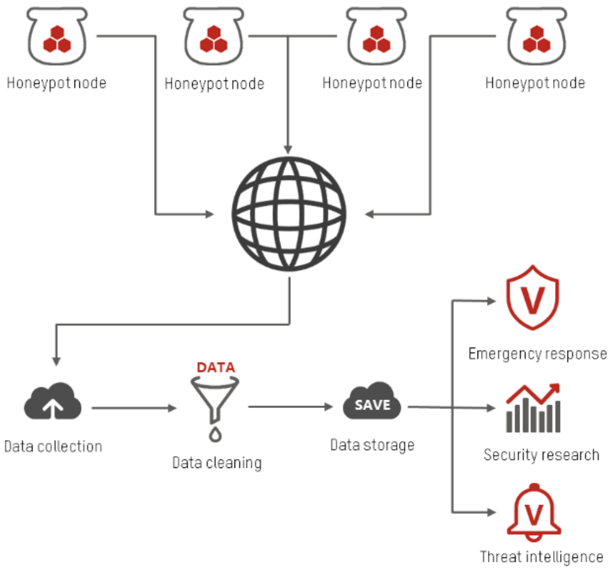
Furthermore, Hikvision's video security situational awareness system can also discover security threats and perform correlation analysis on asset information. By establishing a big data analysis model for dynamic analysis of real-time and historical data, the security status and development trend of the entire network can be accurately and effectively perceived. Reasonable security reinforcements on video surveillance network resources can then be made to ensure the security of the surveillance system.

Visualization of Security

Visualization can directly help in the display of data characteristics and make it easier for the reader to interpret data. Therefore, big data analysis (deep packet inspection, traffic analysis) results require a visualized display.

When a system is under attack, quick identification of the attack source, attack path, and a quick response is required. Effective measures must be taken before the attack causes additional damage. After an attack, measures must be quickly taken to prevent similar attacks from happening again.

6.3 Honeypot



A honeypot is essentially a mechanism for deceiving attackers. Decoy hosts or network services are deployed to lure attackers to access them. The attacker's behavior is then captured and analyzed so the attacker's tools, methods and intentions can be identified.

Thanks to the rise and development of data storage, data retrieval, data mining, threat intelligence and other technologies, there is great value in honeypot technology. Hikvision takes the self-developed and modified honeypots as data collectors, deploys honeypot nodes worldwide, and establishes a data pipeline for collection, processing, storage and retrieval of honeypot data, providing data support for security research, emergency response, attack tracing and situational awareness.

Based on a Hikvision rule engine, Hikvision's honeypot system can monitor the attack behavior against IoT devices in real time and provide an early alert of unknown threats. The analysis engine of a honeypot system, based on its historical data, can perform intensive monitoring and correlation analysis on malicious attackers, and predict the threat trend.

As an important part of its threat intelligence platform, Hikvision's honeypot system will continuously monitor security threats from around the world to ensure that Hikvision's HSRC is aware of, and able to rapidly respond to new threats and quickly create product updates when necessary.

7. Commitment to Security

Hikvision strives to use leading privacy and security technologies to protect customers' personal information and to protect user data in comprehensive ways.

Hikvision uses an integrated security infrastructure for its entire Internet of Things video surveillance ecosystem. Hikvision also has a professional security team responsible for providing support on all Hikvision products. This team provides security reviews and testing of released products and products in development. The security team also provides security training and actively monitors new security issues and threat reports. To find out how to report issues to Hikvision and how to subscribe to security notifications, please visit: https://www.hikvision.com/en/Support/Cybersecurity-Center.

Hikvision

Cybersecurity White Paper

See Far, Go Further

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