HIKVISION

海康威视网络安全白皮书

www.hikvision.com

关于本文档

海康威视网络安全白皮书，旨在概览海康威视针对网络产品安全问题所进行的探索与实践，以开放透明的视角让广大用户了解海康威视的安全能力。

海康威视可能对本文档进行更新，最新版将发布于公司官网（https://www.hikvision.com/cn/）。

版权声明

商标声明

责任声明

在法律允许的最大范围内，本文档所述内容均“按照现状”提供，海康威视不提供任何明示或默示保证，包括但不限于适合特定目的、商用性等保证。

海康威视不保证本文档内容的精确性，并保留对其进行纠正或修改的权利，不另行通知。

任何使用或信赖本文档的内容而做出的决定及因此造成的后果由行为人自行承担。

如本文档中所述内容与适用的法律相冲突，则以法律规定为准。

修订记录

首次发布于 2018 年 1 月，2019 年 5 月第一次修订

关于海康威视

海康威视是以视频为核心的物联网解决方案提供商，面向全球提供综合安防、智慧业务与大数据服务。

海康威视全球员工超 34000 人（截止 2018 年底），其中研发人员和技术服务人员超 16000 人，研发投入占企业销售额的 7-8%，绝对数额占据业内前茅。海康威视是博士后科研工作站单位，以杭州为中心，建立辐射北京、上海、武汉以及加拿大蒙特利尔和英国伦敦的研发中心体系。海康威视拥有视音频编解码、视频图像处理、视音频数据存储等核心技术，及云计算、大数据、深度学习等前瞻技术，针对公安、交通、司法、文教卫、金融、能源和智能楼宇等众多行业提供专业的细分产品、IVM 智能可视化管理解决方案和大数据服务。在视频监控行业之外，海康威视基于视频技术，将业务延伸到智能家居、工业自动化和汽车电子等行业，为持续发展打开新的空间。

海康威视在中国大陆拥有 32 家省级业务中心/一级分公司，在境外建立了 44 个分支机构（截止 2018 年底），产品和解决方案应用在 150 多个国家和地区，在 G20 杭州峰会、北京奥运会、上海世博会、APEC 会议、德国纽伦堡高铁站、韩国首尔平安城市等重大项目中发挥了极其重要的作用。

海康威视是全球视频监控数字化、网络化、高清智能化的见证者、践行者和重要推动者。2011-2017 年蝉联 IHS Markit 全球视频监控市场占有率第 1 位[1]；连年入选“国家重点软件企业”[2]、“中国软件收入前百家企业”[3]、a&s《安全自动化》“中国安防十大民族品牌”、

[1] IHS Markit 是世界著名的三大咨询调查公司之一，官方网站 https://www.ihs.com/。

[2] “国家重点软件企业”名单由国家发展改革委、工业和信息化部、商务部、国家税务总局等联合公布。

[3] “中国软件收入前百家企业”由工业和信息化部发布。

CPS《中国公共安全》“中国安防百强”（位列榜首）；2016-2018 年， a&s《安全自动化》公布的“全球安防 50 强”榜单中，蝉联全球第 1 位。

2010 年 5 月，海康威视在深圳证券交易所中小企业板上市，股票代码：002415。基于创新的管理模式，良好的经营业绩，公司先后荣获“2016&2017 CCTV 中国十佳上市公司”[4]、“中国中小板上市公司价值十强”[5]、“2016 年 A 股上市公司未来价值排行以及 A 股最佳上市公司”榜首[6]、“第六届中国上市公司口碑榜最佳公司治理实践奖”[7]、“中国中小板上市公司投资者关系最佳董事会”[8]、“上市公司金牛投资价值奖”和“最佳投资者关系管理奖”[9]等重要荣誉。

海康威视秉承“专业、厚实、诚信”的经营理念，坚持将“成就客户、价值为本、诚信务实、追求卓越”核心价值观内化为行动准则，不断发展视频技术，服务人类。

---

[4] 2016 年 12 月 12 日，2016 央视财经论坛暨中国上市公司峰会上正式发布了“2016CCTV 中国十佳上市公司”榜单，海康威视位列其中。

[5] 2016 年 9 月，第十届中国上市公司价值评选，海康威视荣获“中国中小板上市公司价值五十强前十强”。

[6] 2016 年 11 月，第三届“2016 A 股上市公司未来成长价值排行榜暨行业先进性排序”，海康威视荣登 2016 年 A 股上市公司未来价值排行以及 A 股最佳上市公司榜首。

[7] 2016 年 11 月，由每日经济新闻主办“第六届中国上市公司领袖峰会”上颁发“中国上市公司口碑榜”九大奖项，海康威视获颁 2016“最佳公司治理实践奖”。

[8] 2016 年 4 月，海康威视荣获证券时报、中国基金报颁发的“中国上市公司投资者关系天马奖——中国中小板上市公司投资者关系最佳董事会”。

[9] 2017 年 8 月 15 日，由中国证券报主办的“第十九届中国上市公司金牛奖颁奖典礼暨高端论坛”在贵阳举行，海康威视荣获“2016 年度上市公司金牛投资价值奖”和“2016 年度最佳投资者关系管理奖”。

目 录

1 总裁寄语

“万物互联”，正在从梦想变成现实。作为“万物互联”的先行者，在过去十多年，视频监控技术发展很快，从模拟时代进入数字化时代、网络化时代，正在进入智能化时代。技术的每一次进步，在推动人类社会进步的同时，也会给人类社会带来新的挑战。互联网技术的发展，让人类社会大受其益，也给人类带来了巨大的挑战，包括网络安全的挑战。基于互联网基础上发展起来的物联网技术，同互联网一样，会让人类生活更加美好，也会让人类社会面临一些新的挑战，网络安全就是挑战之一。

相对 IT 产业，安防产业进入数字时代时间不长，安防产业界对网络安全的意识相对也弱一些。2014 年，按照惯例，海康威视成立“安全应急响应中心”，就网络安全问题建立公司统一的对外接口。2015 年，海康威视成立“网络与信息安全实验室”，网络安全实验室全面推进海康威视的网络安全体系建设，先后成立产品安全委员会、网络安全部，建立和完善以组织和流程为重心的网络安全体系，特别是网络安全设计，全面提升公司产品和系统的网络安全水平。

我们知道，网络安全不只是产品厂商的责任。项目的任何参与方，在项目的全生命周期，用户、集成商、运营商、工程设计方、或其它服务提供商、政府，都是网络安全的责任人，都面临网络安全的挑战。三分技术，七分管理，需要所有的利益关联方共同努力迎接挑战，任何一方都不能抱有侥幸的心理。

在面临行业亟需同心协力去解决这些行业所面临的共同问题的时候，我们看到公众与媒体对物联网安全表现出的极大关注与担忧，这些更让我们感受到了身上肩负的责任与使命，海康

威视将一直秉承“成就客户、价值为本、诚信务实、追求卓越”的企业价值观，我们承诺将客户的网络和业务安全性保障的责任置于公司的利益之上。

网络安全的挑战，会一直存在下去，我们会继续努力！

杭州海康威视数字技术股份有限公司

2 前言

过去的五年，我们见证了安防产业的数字化进程，也见证了安防产业高速发展，这五年我们见证了智能安防产业如何探索人们“万物互联”的梦想，我们也欣喜地看到智能安防走在了物联网发展的前列，为实现真正的“万物互联”做了积极地探索和实践。

毫无疑问，智能安防产业的发展必须顺应数字化、网络化和智能化潮流发展的趋势，但是网络空间对于安防产业是一个全新的领域，网络的开放性将此前独立的、完全隔离的各个安防系统进行了互联，促进了数据的流动和共享，推动了社会的进步与发展，带来更多创新机会，促进了物联网产业的发展，也使得人类的文明发展到了一个新的高度。

然而，在我们把安防从“模拟”、“孤立”、“数据采集”引领到“数字”、“网络”、“图像智能”的过程中，我们看到了数字和网络革命对安防产业带来的里程碑式的意义；同时，我们也看到了针对互联网所发起的各类恶意攻击开始蔓延到了安防领域。另外，由于当前的安防系统是基于原有系统“无缝”做的切换，所以产业本身固有的一些特征，在网络化的环境下可能成为安全缺陷。

海康威视是一个全球性的公司，业务延伸到 150 多个国家和地区，连续多年蝉联全球视频监控市场占有率第一。作为这样一家公司，海康威视积极正面地应对这些挑战。作为全球领先的安防行业解决方案提供商之一，海康威视从技术方面能深刻地理解智能安防系统如何安全、有效地运行，以及技术如何从根本上支撑和促进全球公民的健康、富裕和安全。

网络安全并不是某个国家或公司的问题。所有的利益相关方、政府和行业都必须意识到网络安全是全球共同面临的问题，需要我们采取基于风险的方法以及最佳实践，并进行国际合作

去应对这个挑战。近年来爆发的“美国断网”事件、“永恒之蓝”勒索软件等，让我们看到了新的形势下，安全问题的有效应对策略是各相关利益方建立信任协助机制协同处理。

在此，海康威视做出了如下承诺：我们将支持和采用广义的国际认可的网络安全标准和最佳实践；我们将支持增强网络防御能力的研究工作；我们将继续改善和采用开放透明的方法，让用户能够评估海康威视的安全能力。

最后，正如我们迄今为止所做的一样，我们热烈欢迎我们的客户来帮助我们改善流程、提高技术、改进网络安全的方法，让我们可以为他们以及他们的客户带来更多的利益。

3 物联网安全威胁

物联网（Internet of Things）将任何物体通过网络相连接，给物体赋予智能，实现人与物、物与物之间的沟通和对话。海量设备的互联，使得网络更开放、也更复杂，业务更丰富多样。然而，物联网也面临着巨大的安全挑战。

物联网除了传统网络安全威胁之外，还存在着一些特殊安全问题。这是由于物联网是由大量的设备或感知节点构成，缺少人对设备的有效监控，并且数量庞大、设备集群度高等，物联网的安全威胁可以根据物联网的架构分为感知层威胁、传输层威胁和应用层威胁。

感知层威胁

- 物理攻击

  部署在远端的缺乏物理安全控制的物联网资产有可能被盗窃或破坏。物理接口直接暴露在设备外部，没有做安全保护，易被非法访问。

  终端在户外分散安装、易被接触又没有纳入管理，导致物理攻击、篡改和仿冒。

- 数据泄露

  敏感信息预置在设备中，易被读取或篡改。

  基于数据的隐私威胁，物联网中数据采集和处理等过程中的隐私信息泄露。

- 非法接入

  物联网环境中的部分访问无认证或认证采用弱密码，认证机制易被绕过。

  固件中保留了调试接口，由于没有进行正确的保护，导致攻击者可以远程访问。

  调试接口没有限制代码执行的权限，导致攻击者访问该接口服务后就可以完全控制设备。

- 非法更新

物联网设备的更新验证机制不健全，非官方固件包易被直接更新进设备。

非官方固件包未经验证，可能存在漏洞，或其本身就是恶意软件。

- 过期组件

OS 或软件过时，漏洞无法及时修复。设备的数量巨大使得常规的更新和维护操作面临挑战。

物联网设备，出厂时，其上装载的组件就已经“过期”或即将过期。即使有些设备出厂的时候装载的是最新版本软件，但由于未及时更新，也可能在未来出现漏洞。因此，除非拥有持续的软件更新机制，否则物联网终端设备存在较高的软件漏洞风险。

- 恶意软件

恶意软件可能会影响物联网设备的操作，获取未授权的访问或者实施攻击。

传输层威胁

- 网络攻击

通过无线接入渗透到网络，协议本身缺陷如缺乏有效认证可能导致接入侧泄密。

未加密的通信过程容易发生劫持、重放、篡改和窃听等中间人攻击。

IP 化后面临 IP 体系的安全问题。如来自互联网的攻击和入侵。

病毒攻击物联网设备，引起僵尸网络，对互联网目标发起 DDOS 攻击。。

- 数据泄漏

设备和云端以及移动应用端通信传输时，控制命令和采集的数据没有加密，攻击者可通过监听获取敏感数据。

- 数据篡改

设备在网络通信时，网络传输数据没有校验机制，控制命令和采集的数据可能会被攻击者篡改。

应用层威胁

- 设备管理

平台层面所管理的设备分散、繁多，设备的升级过程和安全状态等难以管理。

- 越权操作

权限管理不完善，越权访问导致隐私和安全凭证等重要数据有被泄露的风险。

- 系统漏洞

应用层的操作系统，大多为通用系统，通常大规模网络攻击和漏洞利用均是系统漏洞问题。

- 数据泄漏

应用层管理大量的数据，不做加密处理，很容易产生数据泄漏。

- 过期组件

如组件更新不及时，组件本身存在的漏洞易被利用。

- 配置漏洞

安全配置长期不更新、不核查。较多的网络攻击也是利用配置不合理的问题而产生的。

- 非法更新

非官方软件未经验证直接更新，可能存在漏洞，或其本身就是恶意软件。

在深入思考物联网环境中的诸多安全性隐患后，结合物联网设备在软硬件环境、计算能力等方面的复杂性，海康威视设计的以视频为核心的物联网解决方案，力求打造出全新的安全架构，建立多维度的安全体系，充分保障终端安全、数据安全、应用安全、网络安全、隐私保护以及安全合规。

4 关于安防产业的网络安全

安防产业的发展历程是先模拟后数字，在模拟时代安防系统都是在专网内工作，所以产业注重的是产品的成本、性能和易用性。由于当时系统的特点，安全性一直不在考虑之中，但是随着安防产业网络化的快速推进，安防产业直接从原来的模拟进入 IP 数字化，在这个切换的过程中整个行业并未过多地考虑安全问题，这就导致了原来在模拟时代是优势、强项的易用性设计，到了数字时代可能就会与信息安全的最佳实践存在偏差。安防厂商一般为了方便用户实现一键集成多个厂商设备，把所有支持的协议都默认开启，服务器端支持哪种协议就自动匹配连接，但是这样的设计虽然极大方便了客户，却与信息安全的最佳实践相违背。

也正是由于安防产业的这种发展历程，导致了安防产业近年来出现了一些信息安全问题，但是出现这些问题并不代表整个产业如外界所说的那么不堪一击。另外值得庆幸的是我们已经看到了这些既成与潜在的安全风险，并且已经为此开展了大量卓有成效的工作。

客观的来说，网络安全问题并不是安防产业专有的问题，网络安全是当前人类社会共同面对的一个挑战。纵观当前的整个 IT 领域，网络安全问题在所有的领域都存在，并且存在以下几个基本共识：

- **安全漏洞存在的普遍性**

不存在没有安全漏洞的 IT 系统和产品，安全漏洞的存在是普遍的。由几百万行代码组成的产品，其中一个参数的设置错误，或者两行代码位置的顺序弄错都会导致系统出现高危漏洞，目前人类的智慧还不能做到通过自动化或手动方式把所有可能的安全问题都检测出来，所以产品出现安全问题是一个正常的现象。

- **安全是整个系统的安全**

任何系统安全不是靠单点安全能够保证的，必须要做到整个系统的安全。要保证视频监控系统的安全，需要系统中前端设备、后端设备、平台系统、网络设备、安全设备等相互配合、相互补充，形成纵深防御体系，才能保证整个系统的安全，任何一个环节出现问题都会导致系统被攻击。

- **第三方开源软件的安全**

当前在各种系统中会使用各种第三方开源软件，其具有开放、共享、自由等特性，在软件开发中扮演越来越重要的角色，也是软件供应链的重要组成部分，但是企业在享受开源软件带来的便利的同时，也在承担着巨大的安全风险。近年来，开源软件频繁爆出高危漏洞，例如 Struts2、OpenSSL 等。这些组件很多都应用于信息系统的底层，并且应用范围非常广泛，因此漏洞带来的安全危害非同一般，往往成为行业或企业产品线的“通杀”漏洞。

- **安全处于动态的平衡之中**

没有“绝对”的安全，所谓安全都是相对的，攻守的博弈永远是此消彼长，今天被认为安全的机制、方法，可能明天就是不安全的；今天被认为是“安全”的产品，可能明天就会被“攻破”。所以对于安全永远没有终点，任何一个产品在其生命周期内始终都会存在信息安全挑战和风险，只是这些风险是否会爆发以及何时爆发难以事先被预估。

- **安全的管理和使用产品**

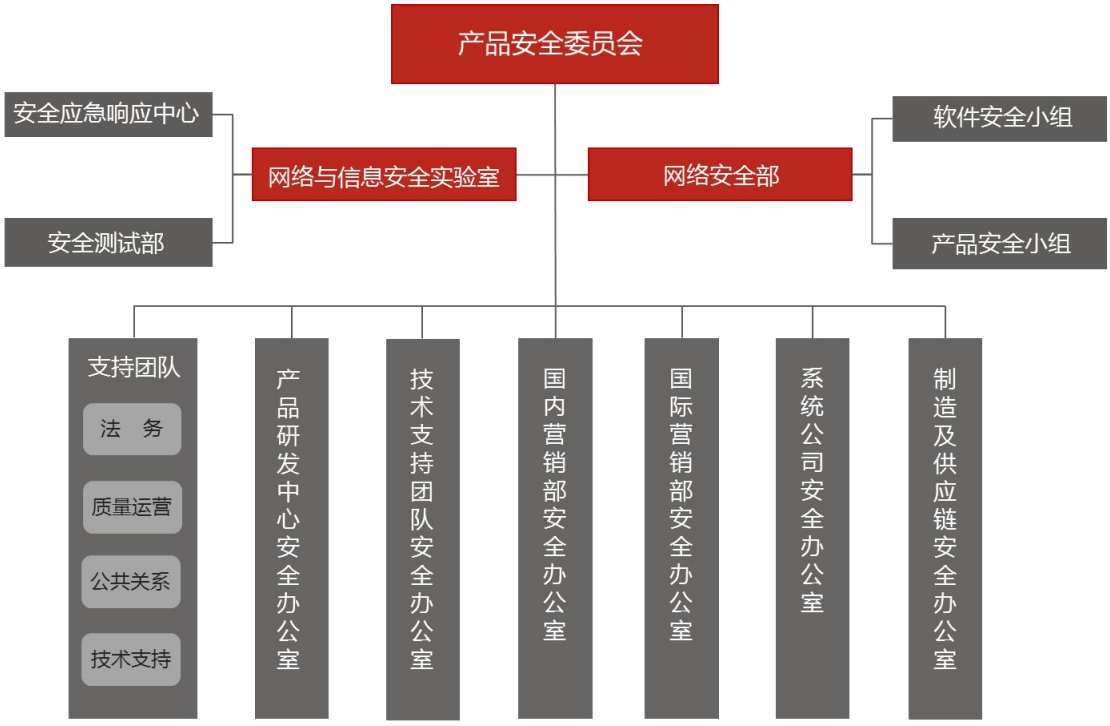
系统安全中最重要的安全元素：管理安全。技术上再安全的系统，如果用户不能很好的管理和操作，系统的安全仍然是无法保证的，当前安防业内出现的有些安全事件的主要原因就是用户的使用“不当”，并且缺乏有效的安全管理，如目前仍然有部分安防设备在使用“弱口令”；部分安防系统在网络的出口无防火墙等安全设备。另外用户要养成良好的安全习惯，应该经常关注厂商的安全公告，有升级版本应尽快升级到最新版本。

5 产品安全生命周期

本章主要分为七个主题来介绍海康威视在建设产品安全全生命周期的工作。

5.1 组织架构

为确保产品安全保障活动融入研发、供应链、市场与销售、工程交付及技术服务等各环节中，我们首先需要建立一个能保证其实现的组织架构，并且赋予每个组织清晰的责任。海康威视的安全组织架构如下：



产品安全委员会

负责公司网络信息安全战略规划、政策的制定。在网络信息安全方面，如果出现了任何冲突或严重问题，该委员会有权做出决策，并对业务做出必要的调整。海康威视胡扬忠总裁担任产品安全委员会主任。网络信息安全战略、政策、流程、标准的制定和资源的配置由产品安全委员会常设的专门机构网络安全部负责日常管理。

网络安全部

网络安全部作为产品安全委员会的常设机构，负责落实公司产品安全战略、建立公司产品安全基线、实施产品安全测评，产品安全对外合作、行业产品安全技术标准的研究和产品安全研发推进，参与产品安全的重大项目评审并为公司领导决策提供建议。结合公司产品安全战略和业界要求，建立研发安全规范，嵌入安全要素到产品研发流程，并推进在各产品线落地。

网络与信息安全实验室

网络与信息安全实验室致力于物联网相关的安全技术的研究与实践，主要覆盖物联网感知、产品安全组件、安全视频监控产品、渗透测试、物联网安全防护等多个领域，旨在研究前沿的物联网安全技术，推动物联网安全技术的进步。实验室全体人员均具备多年信息安全从业背景，其中超过 50%人员拥有国家注册信息安全专业人员 CISP 或国际注册信息系统安全师 CISSP 资质证书。

安全应急响应中心 HSRC

海康威视安全应急响应中心 HSRC（Hikvision Security Response Center）是一个负责接收、处理和公开披露海康威视产品和解决方案相关的安全漏洞的平台。海康威视既重视自身安全，也一直致力于保障用户安全，我们也希望通过此平台加强与业界的合作和交流。

产品线安全办公室

海康威视各产品线均设立产品安全办公室，该办公室协同网络安全部一起建立产品安全基线及相关产品技术标准，并负责相关安全要求在产品线中的产品规划、研发、测试等过程的落地实施，对产品线的安全负责。

安全测试部

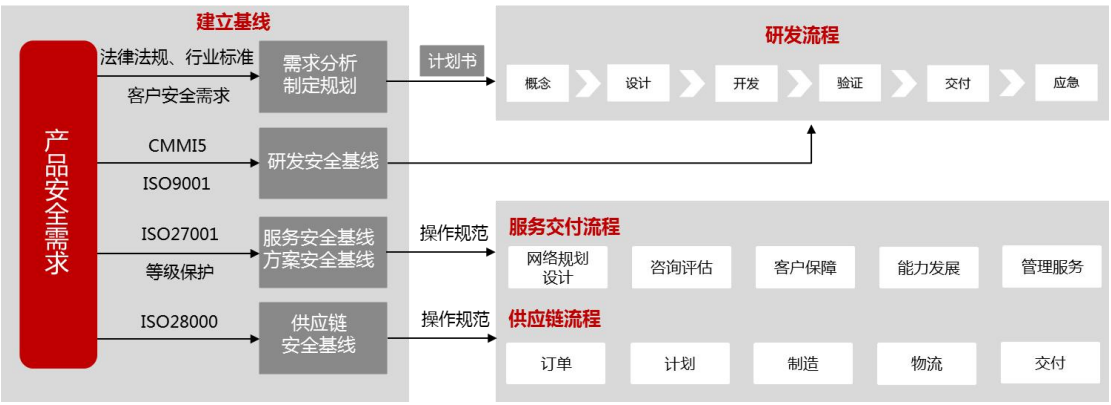
安全测试部是独立于产品线的第三方部门，负责海康威视所有产品线的产品安全测试，检验公司产品安全策略、安全基线是否在产品中得到有效地执行，发现在研发过程中引入的潜在的各种安全问题，确保发布产品的安全性。

支持部门

负责提供与产品安全相关的内控、法务、质量运营、品牌宣传、审计及公共关系支持。

5.2 流程与标准

海康威视基于现行的国内外法律法规、行业标准、客户安全需求、第三方分析、行业活动、同行经验和具体业务安全要求，制定了一整套涉及产品安全的通用安全基线、安全编码、安全密码应用、安全密钥管理、安全会话管理、产品安全认证、安全渗透测试、安全事件管理等规范和标准，这些规范和标准涵盖了产品安全的方方面面。



产品安全总则

产品安全总则是公司的产品安全大纲，主要包括产品安全的方针、目标、组织、管理、流程和活动。产品安全总则是公司产品安全的总纲、蓝图，所有下层文件以此为基础。

产品安全流程文件

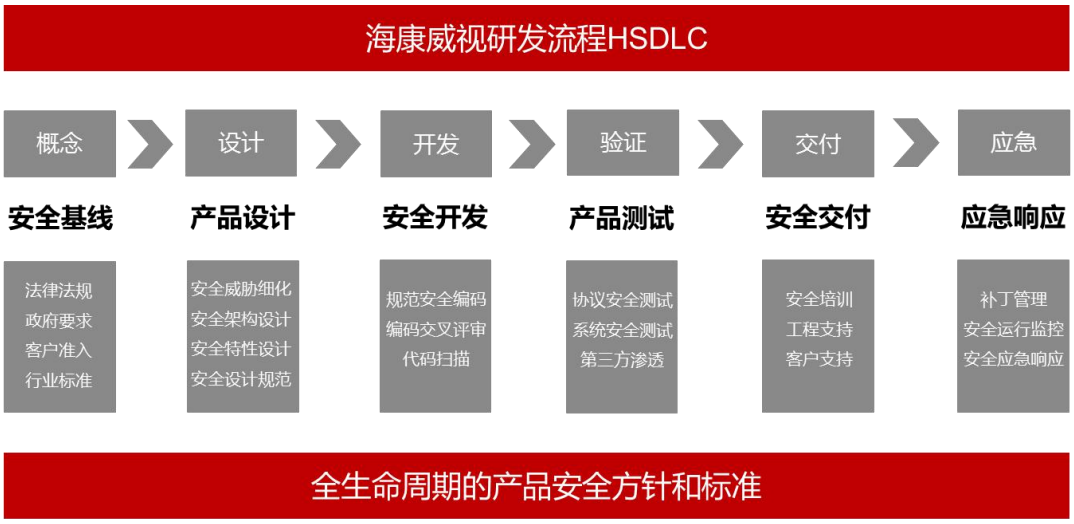
产品安全融入到公司的核心流程中 ,根据需求制定安全管理流程 ,如产品安全事件响应流程，产品安全考核细则和基线要求。在产品安全要求总则的指导下，制定产品安全基线技术要求和模板，对各产品系列制定产品安全基线、供应链安全基线、服务安全基线；建立安全基线的最佳实践；制定产品安全测试要求和测试模板。

安全基线

公司产品不仅包括自研产品，也包括第三方产品。由于各个产品、系统的安全水平不一致，为了保障产品安全水平，公司需要对交付产品的安全进行检查和加固，使之达到安全基线的要求，以杜绝安全隐患。安全基线是产品研发、第三方产品采购、系统运维配置、安全加固、安全测评、安全管理的依据。新产品批量生产前必须完成安全基线检查，确认符合要求后才能批量生产。

5.3 安全研发流程 HSDLC

结合海康威视广泛的研发活动，并参考业界最佳安全实践 如 OpenSAMM、BSIMM、CSDL、MSDL 以及客户的反馈，我们在研发流程中融入了安全活动，比如安全设计、安全开发、安全测试等，制定了符合海康威视的产品研发安全管理流程（HSDLC：Hikvision Security Development Life-cycle），保证安全活动的有效落地，提升产品机密性、完整性和可用性，增强隐私保护，为客户提供更安全的产品和解决方案。另外，公司定期举行安全赋能培训，提升员工的安全意识和安全能力。



概念阶段

在概念阶段，产品安全需求分析关注两点：

第一，把产品安全基线强制纳入需求列表。产品安全基线是保障安全目标实现或将风险控制在可接受水平的最基本要求，来源于法律法规、政府要求、客户准入、行业标准等，其目标是确保产品安全合规、保护用户隐私和敏感数据、加强系统访问控制、增强系统防攻击能力。

第二，要对该产品未来在客户现场的使用场景进行威胁分析，识别出有针对性的安全需求。威胁分析是针对产品的具体使用场景找到所有可能的威胁来源、类型以及攻击点，以便我们评估风险，确保相关的应对和防范措施纳入到了产品需求列表中。

设计阶段

威胁建模和攻击面验证是 SDL 流程中最复杂，但同时也是最重要的部分。威胁建模的目的是理解系统的潜在威胁，确定风险，建立适当的应对措施。威胁建模使问题在软件开发生命周期的早期就得到了解决，有助于有效控制产品的安全风险。

1、 根据产品逻辑架构，通过 STRIDE 威胁建模方法，对产品进行架构级的威胁建模，从架构层面识别产品可能受到的安全威胁，制定对应的缓解措施。
2、 安全设计与功能设计融合，在对产品进行功能设计的同时进行功能级别的威胁建模，及时识别功能设计中的安全威胁，并制定对应的缓解措施。
3、 对收集或识别的安全需求进行详细的分析与设计，并且公司有专门的安全架构师为各个产品在安全设计中提供专业的技术支撑。
4、 对于威胁建模中遗留的高风险，提供攻击路径的分析。

5、 所有产品在设计过程中都会做攻击面最小化分析，降低产品总体的安全风险。

开发阶段

在开发阶段，产品开发人员遵循安全编码规范进行编码并进行交叉评审，通过自动代码扫描工具 Coverity Static Analysis 快速、准确地查找高复杂度代码中的危险函数和缺陷问题，降低代码安全缺陷率，识别需要进一步检查的范围。通过自研的针对公司业务场景的代码缺陷分析和扫描工具，能够通过代码特征识别到已知缺陷，告知研发人员各个分支的缺陷存在情况，评估缺陷同步工作是否到位，并在持续构建活动中进行拦截，实现已知代码问题在源码阶段得到控制，大大降低修复成本。

验证阶段

为了保证海康威视产品的安全性 ,防止由于研发过程中可能会导致产品出现的各种安全问题，我们在产品研发的每个阶段都进行相关安全测试，确保产品的安全：

- 在产品安全测试中加强协议安全测试力度，引入协议安全测试工具 Codenomicon Defensics、Peach Fuzzer，对所有产品进行网络协议安全性、健壮性、可靠性分析以及未知漏洞挖掘；
- 在系统安全测试中引入漏洞扫描工具 Nessus Professional、绿盟远程安全评估系统(NSFOCUS RSAS)及时跟踪 CVE 漏洞库信息 ,能够全面发现系统存在的各种脆弱性问题，包括安全漏洞、安全配置问题、应用系统安全漏洞；
- 在应用安全测试中引入动态应用安全测试工具 IBM AppScan、Burp Suite、Acunetix WVS 发现 Web 应用程序漏洞；

- 在产品发布前使用主流防病毒软件，如 Symantec、Avira 等检测已知病毒、木马、后门等恶意代码；
- 公司还会定期邀请知名安全公司以及众测平台做渗透测试，通过尽可能多地进行渗透测试，最大限度地减小业务风险以保持安全风险在可控制的范围内；
- 公司网络安全小组会按季度对产品测试过程中发现的问题进行分析，整理出典型的 TOP N 问题列表，再推送到各产品线进行自检，杜绝同类问题再次发生。

配置管理

配置管理是保障产品完整性、一致性、可追溯性的重要活动。配置管理包含多个流程，分别是配置管理战略和规划、配置项识别、配置项变更管理、配置状态跟踪、配置活动报告、配置审计、构建管理、发布管理、第三方软件和开源部件管理、版本库管理等。配置管理保障海康威视交付的产品的完整性，包括产品中涉及的第三方软件和开源部件。海康威视的配置管理流程是 IPD 流程不可分割的一部分。在 IPD 流程的不同阶段都开展上述配置管理活动，实现了产品的可追溯性。

1.构建管理规范

构建管理规范包括构建资源管理、构建过程管理、构建过程优化三个部分。配置管理中很重要的一部分就是职责分离，在构建流程规范中对构建过程中的活动、角色、职责有明确的定义。结合产品开发的不同阶段，明确构建流程在 IPD 流程中的生命周期。

2.编译构建中心

为了保证构建流程的可重复性，海康威视建立了一个编译构建中心，构建中心除了满足编译管理规范的管理要求外，还对所有的硬件、编译工具、第三方软件、数据源和操作系统做了严格的准入标准控制。编译构建中心是产品编译构建的整体解决方案 ,提供编译构建云服务，支撑 IPD 流程中的软件构建活动。

构建过程标准化：通过工具的统一管理、构建脚本标准化、一键式构建、构建环境自动安装等，实现对产品从环境搭建、代码下载、一键式编译、打包、静态检查、自动的单元测试，到系统测试整个构建过程的自动化，确保产品构建过程的可复制/还原、可追溯。

构建中心还有两个额外的功能：病毒扫描中心和数字签名中心。病毒扫描中心同时运行数十款杀毒软件进行扫描，并融入到测试流程中；为了安全起见，数字签名中心使用存储在密钥数据库的密钥对编译的代码进行数字签名，海康威视会对签名活动进行授权和记录，确保整个工作的可溯性。

3.组件管理

海康威视使用组件化开发的模式开发产品，组件在开发完成后，会进入组件验证，验证完成后，推送到 SWMS 软件管理平台（海康威视自研的软件管理平台）的组件库中。组件库会标识每个组件的名称、群组、版本、运行平台、源代码、静态分析结果、是否包含第三方软件、是否安全等信息，并具备生命周期管理功能。海康威视使用类似于 Maven 的方式管理 C/C++等嵌入式的组件，通过跟 POM（Project Object Model 项目对象模型）逻辑一致的组件配置器集成各个组件，直至组合成一个成品软件。并依据集成的信息建立统一的版本信息结构和软件 BOM（Bill of Material 物料清单）库，用于跟踪组件的应用情况，一旦某个组件出现安全问题，能快速反查使用了组件的软件，以便维护和升级。

4.工具和第三方部件管理

海康威视从全球采购很多第三方和开源软件部件，并将它们使用到产品中。因此，海康威视会非常重视以下方面的问题：

- 使用的源代码或部件来源是否可靠
- 是否满足公司的安全风险评估要求
- 是否遗留已知漏洞
- 许可证的合规性管理
- 如何应对新的漏洞爆发
- 第三方部件的生命周期
- 将第三方部件融入海康的产品生命周期中

海康威视不仅仅需要考虑第三方部件 ,我们还需要确保所有编译源代码或第三方部件所需的相关组件及其选择都有管控。海康威视对第三方部件的引入制定了《第三方组件及源码管理规范》、第三方部件引入流程，确保所有引入的第三方部件符合我们的预期要求并能被有效管理。

海康威视非常重视第三方软件的合规合理安全使用 ,在整个管理中 ,引入了 ProteCode SC、BlackDuck Hub、BlackDuck Protex 等多个二进制和源码分析软件，并将这些工具与软件管理平台融合，实现自动检测，确保能精准快速地洞察软件中第三方软件的成分。

5.创新型的版本和源代码管理

海康威视管理源代码、文档、库、组件、产品软件等各个维度的配置项，并针对每个不同的对象建立不同的管理工具，并打通这些管理工具，形成一体化的软件开发平台 SWMS。所有库、组件、软件之间的关系得到有序的结构化管理，方便跟踪，回溯。

安全交付

技术支持是公司服务客户的一线人员，在获客户授权的情况下可能接触到客户的敏感信息。正因为如此，对他们进行必要的网络和信息安全培训非常重要，让他们可以帮助保护客户利益，防止出现访问控制问题、通信安全问题和隐私数据保护问题等。在员工管理方面，海康威视根据 ISO27001 和其他标准，制定了《海康威视技术支持现场服务规范》，包括行为准则，人身安全，信息安全等方面。

海康威视对可以接入客户网络的员工进行严格管理，与这些员工签订承诺书，承诺书详细说明了他们的角色、职责和潜在的法律责任，并要求他们学习网络安全知识，参加相关考试。

应急响应

海康威视成立了 HSRC（Hikvision Security Response Center），负责接收、处理和披露海康威视产品和解决方案与安全相关漏洞的应急响应，其职责还包括：

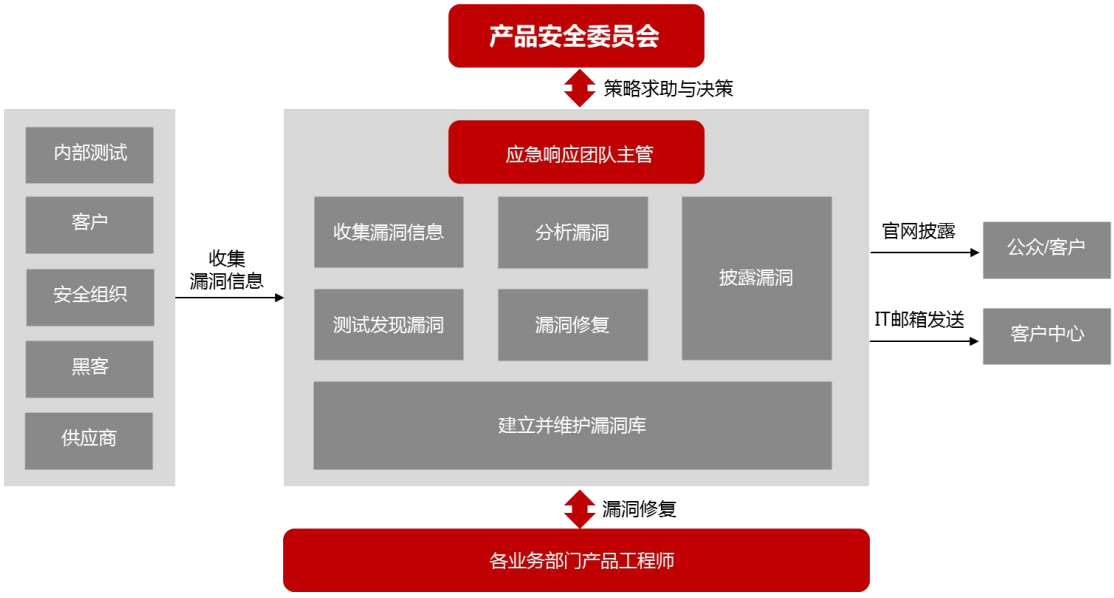
- 响应和处理客户提交的安全事件
- 响应和处理行业协会公布的安全事件
- 制定公司信息安全事件管理策略和安全事件处理方案

- 分析系统软件提供商和专业安全厂商发布的漏洞及补丁

另外，公司还规定产品安全事件管理的流程和各部门职责，保证产品安全事件管理的质量和效率。管理规范覆盖公司产品安全工作的售前、售中、售后全部过程，包括客户安全专题交流、安全组织合作、应急响应管理、安全信息发布、信息安全合规、法律合规的流程和实施细则。

对于安全事件的执行效率，管理规范有明确的规定，如安全事件初步确认时间不超过 24 小时，高危以上级别的安全漏洞修复期限为 30 天。

海康威视是国际安全响应联盟组织 Forum of Incident Response and Security Teams(FIRST)的重要成员，与全球范围内的其他优秀会员单位共享安全应急的最佳实践和处置经验，增进可信沟通和合作，提升公司对安全事件应对的有效性和及时性。



漏洞处理

海康威视参照 ISO/IEC 30111 、ISO/IEC 29147 等，建立产品安全漏洞处理及预警披露流程，包括 3 个阶段：

- 漏洞研究与收集：我们通过客户、外部 CERT、安全研究人员或相关安全网站发布的资讯获取漏洞信息。同时我们通过内部团队不断发现潜在安全威胁。我们鼓励负责任的披露，即外部漏洞发现者应该在公开披露之前，给厂商一段合理的时间去处理和解决问题。
- 安全漏洞评估、分析和验证：不论是疑似漏洞还是已经确认的漏洞，HSRC 团队都会与产品责任人一起合作，快速完成漏洞的真实性及相关风险的评估。
- 跟踪与解决：一旦漏洞确认，HSRC 会立即把信息传递给漏洞提交者，然后积极跟踪反馈解决进展。还会对漏洞进行排查，从而确保该问题在所有产品版本和产品模型中都得到解决。HSRC 流程与研发核心流程紧密结合，确保对漏洞的及时响应。

在这个流程的各个阶段，保护客户和漏洞信息的机密性对海康威视来说至关重要。漏洞信息如果提早落入怀有恶意的人手中，会产生极为恶劣的影响。各方都必须要保护其机密性。

海康威视安全应急响应团队积极参与业界与公众的活动，与 CERT、漏洞披露平台、客户 SRC、其他供应商、研究人员和第三方协调机构建立长期的联系。海康威视是国际知名漏洞信息库 Common Vulnerability & Exposures (CVE) 编号机构组织成员，可以第一时间获取外部组织发现的安全漏洞，提升安全应急响应速度，为客户提供更安全的产品和解决方案。

5.4 供应链安全

供应链系统具有参与主体复杂多样、过程环节步骤众多、产品传递跨地域等特征，这使供应链系统容易受到来自内部的不利因素的影响和来自外部的威胁。供应链系统面临的安全威胁主要包括未经授权的生产、篡改、盗窃、植入恶意软件及硬件，以及供应链中不良的制造和开发实践。供应链系统的漏洞可能潜伏数年才被发现，而且在很多情况下，难以确定安全事件是否是供应链漏洞的直接结果。供应链的安全问题有可能对组织造成持续的负面影响。

为了解决制造安全风险，确保硬件和软件的完整性，海康威视在产品生产关键环节，包括软件提供、芯片烧录/校验、软件加载、生产测试等，采取防篡改、防植入、防调包等安全管控措施，以防范未授权的硬件替换、软件植入或篡改、病毒感染等风险。产品数据管理系统把设备需要烧录的软件下载到一个安全的制造分发系统，软件在烧录之前会经过多次完整性验证。

供应链用于生产的软件烧录、软件加载、组装和测试网络隔离于公司的办公 IT 系统和公共互联网之外。

海康威视的产品都实现了自动化测试。通过自动测试，海康威视降低了人为错误带来的风险和安全威胁。

海康威视不仅通过技术手段来提高供应链的安全性，还通过管理体系建设来保障供应链的安全。ISO 28000 供应链安全管理体系的目标是全面改进供应链的安全，它能帮助组织各部门审核安全风险并实施控制和减轻风险的措施来应对供应链潜在的安全威胁。ISO 28000

与 ISO 9001 质量管理体系及 ISO14001 环境管理体系是兼容的，可以在一个组织内把质量系统、环境系统和供应链安全管理系统整合起来。

海康威视在明确供应链运作环境、识别各个环节威胁并进行风险评估和应对的基础上，建立了一个全面符合 ISO 28000 的供应链安全管理体系，并且通过 PDCA 管理循环，实现供应链安全管理体系的不断更新和完善。

海康威视实施了一个安全、严格的维护流程，确保流程中产品的完整性。海康威视在制造和条码系统中记录整个流程中的信息，为研发、采购、生产制造（芯片烧录、软件加载、组装、测试等）、仓储、物流环节建立详细的执行记录及日志，以确保可追溯性。

5.5 安全合规

全球法律环境错综复杂且持续变化，以及行业监管要求的日趋复杂，特别是网络安全法律领域，不少国家或地区在近些年陆续出台相关的法律、法规，如中国《网络安全法》、欧盟《一般数据保护规定（General Data Protection Regulation）》等，安全合规性已然成为物联网服务提供商面临的一大挑战。海康威视致力于建立高效的安全内控体系，紧随不同行业、领域、国家的合规要求，从制度流程及控制活动等方面完善自身的合规基础。为适应全球业务拓展的需要，帮助公司在全球范围内更好的符合合规要求，推动各个国家和地区的规范经营，2018 年公司优化了内部合规组织架构，成立了合规部，负责全球合规体系的建设工作。

海康威视拥有一支内部专业律师团队对公司运营所适用的法律法规进行调查、识别和跟踪。同时，海康威视也积极与业内经验丰富的国内外知名律师事务所建立长期合作。我们建立专项工作小组，将适用的法律法规与海康威视业务实际相融合，对产品研发、制造、交付和服

务各环节的法律风险进行识别和管控，提出合规建议和支持。我们持续为新入职员工、中高层管理者、网络安全关键岗位就新颁布的法律法规、热点法规进行合规专项培训，不断提高合规意识。

正如我们在《关于构筑视频监控产品网络安全保障体系的声明》中所述，海康威视致力于提升和完善视频监控产品的安全性能，在遵从所有适用的国家和地区安全法规、参考业内最佳实践的基础上，从公司政策、组织、流程、技术和规范等方面建立和完善可持续、可信赖的安全保障体系。

海康威视支持主流国际标准，并为这些标准的制定积极做出贡献。截至 2016 年底，海康威视已经加入了数十个国内外行业标准组织，TC260[10]、TC100[11]、CSA[12]、ONVIF[13]等。并参与行业安全标准的制定及推广，从而进一步开放核心安全技术，与不同的行业专家和国家标准机构合作，共同完善物联网相关的安全标准体系。

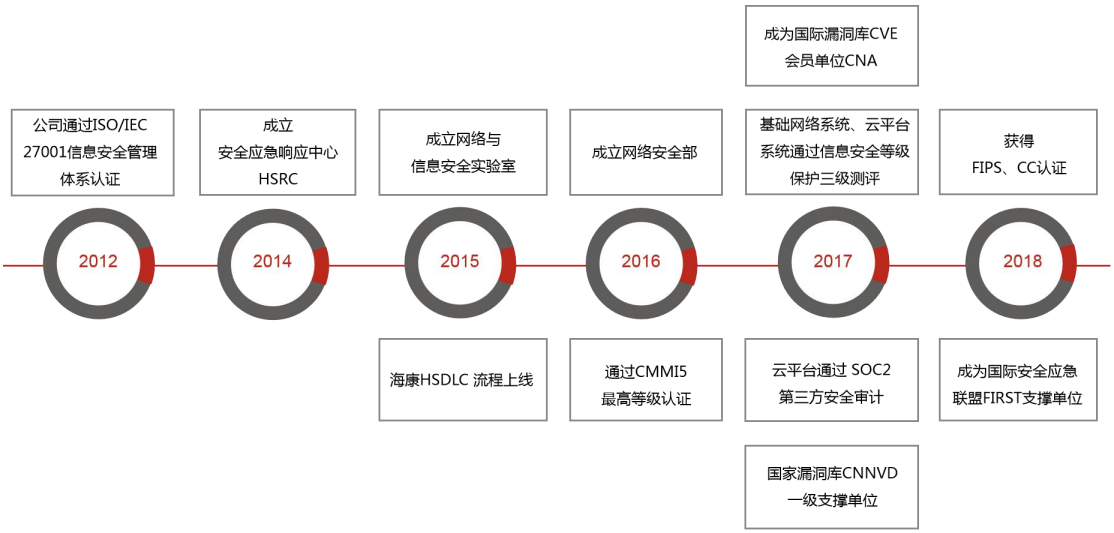
海康威视还与独立的第三方评估机构和人员合作，对我们的产品进行公正的安全评估和认证。

[10] 全国信息安全标准化技术委员会：http://www.tc260.org.cn/

[11] 全国安全防范报警系统标准化技术委员会：http://www.tc100.org.cn/

[12] 云安全联盟(Cloud Security Alliance): https://cloudsecurityalliance.org/

[13] 开放型网络视频接口论坛（Open Network Video Interface Forum）:https://www.onvif.org/



商用密码产品许可

海康威视在商用密码（SM1、SM2、SM3、SM4、SM7、SM9）使用上，严格遵守国家相关法律法规、标准规范，确保合法合规安全的使用商用密码。至今已取得多种不同类型产品的商用密码产品型号证书[14]：

- SRM1701 安全门禁读卡器；
- SYT1703 密钥管理系统；
- SHT1810 视频监控安全管理系统；
- SJT1809 视频采集加解密系统。

同时，海康威视是密码行业标准化委员会会员，积极参与商用密码标准的评审、制定工作。

[14] 商用密码产品型号证书查询： http://www.oscca.gov.cn/app-zxfw/xzspsx/symmcp.jsp

加密验证（FIPS 140-2)

美国商务部下属机构美国国家标准与技术研究院（NIST），联合加拿大通信安全机构（CSE），建立了旨在评测、验证和认证密码模块安全性的 FIPS 140-2 标准，该标准“被广泛认可为密码模块的实操标准”（NIST 官网)。作为一个相对综合和全面的认证标准，FIPS 140-2 的认证要求不仅仅是密码模块算法及技术，还涵盖了正确的环境与密钥管理、物理安全、设计保障、安全实现等诸多方面，指定了密码模块需要被满足的安全需求。该标准不仅在美国和加拿大的政府中被普遍采纳，在金融、医疗、法律、公用事业等其他领域也被广泛采用。

海康威视于 2018 年 7 月获得了 FIPS 140-2 安全认证，证书编号为 3228[15]。

通用标准认证(Common Criteria / ISO 15408)

CC(Common Criteria)认证是信息技术安全领域认可度最高的国际性认证之一，得到美国国家信息安全保障合作计划的认可（该计划受美国国家技术与标准研究院监督），同时也被英国、加拿大及其他西方国家所认可。目前全球已有来自 28 个国家的安全认证机构加入了 CC 互认协定（CCRA）。由于 CCRA 成员均为其所在国的政府主管部门或第三方权威机构，因此 CC 认证在全球范围内具有很高的接受度与可信度，成为安全性评估的重要依据。

CC 认证主要用于评估信息技术产品或解决方案的安全性、可靠性，以及对信息隐私的保护。按评估保证级别，该认证分为七个级别，从 EAL1 到 EAL7，对应的验证要求依次增高。

[15] FIPS 140-2 证书查询 https://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

海康威视相关产品于 2018 年 9 月成功通过 EAL2+级别认证[16] ,在安防行业内树立了良好示范。海康威视将积极参与开发当前还未实施的保护描述文件（PPs)。并且海康威视将继续针对当前已实施的 PPs 新版本和更新版本来评估和开展认证。

ISO/IEC 27001

ISO/IEC 27001: 2013 信息安全管理体系是国际上针对信息安全领域最权威、严格，也是最被广泛接受及应用的体系认证标准。通过该认证，就意味着企业已经建立了一套科学有效的信息安全管理体系，以统一企业发展战略与信息安全管理的步伐，确保相应的信息安全风险受到适当的控制与正确的应对。萤石云是国内首家获得 ISO/IEC 27001:2013 认证的家用安防云服务提供商，通过这套“量体裁衣”的信息安全管理控制措施和保护信息资产的制度框架，遵循 PDCA 持续的改进路线，对您的信息安全做出承诺，提供可靠的信息服务与相关安全保障。

CMMI5 软件成熟度认证

CMMI 即能力成熟度模型集成，是企业级过程管理的框架，是世界最优秀企业的最佳实践，是业界公认的衡量企业产品及服务能力的权威标准，同时也是过程改进的方法，可以帮助企业实现商业目标、确保质量、保证交付、提高客户满意度。软件 CMMI 规范中针对企业改进过程能力设定了 5 个阶梯式上升的成熟等级，其中 5 级为最高级别。

[16] CC 证书查询： https://www.commoncriteriaportal.org/products/

信息安全等级保护认证

信息安全等级保护是我国信息安全保障的一项基本制度，是保护信息化发展，维护国家信息安全的根本保障。信息系统的安全保护等级是根据信息系统在国家安全、经济建设、社会生活中的重要程度，以及遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素将其划分为五个等级，五级为最高系统等级。

依据《信息安全等级保护管理办法》的有关规定，萤石云，海康威视内部信息系统已通过信息安全等级保护三级测评，严格遵循国家在信息系统安全建设方面的技术保障和安全管理要求，建立了自身的长效机制，进一步保证安全保护工作的持续进行。

SOC 审计

SOC 报告 （System and Organization Controls Reports）是由专业的第三方会计师事务所依据美国注册会计师协会（AICPA）的相关准则出具的服务机构内部控制相关的系列报告。SOC 2 报告是参照 AICPA 审计准则 SSAE No. 18 中的 AT-C section 105、205 以及 TSP section 100 2017 版，针对云服务体系的安全性、可用性和保密性相关的控制设计适当性出具的报告。SOC 2 报告：云用户机构、独立审计师、监管机构、公司股东及其他相关利益方可以根据 SOC 2 报告评估云服务商相关的内部控制（覆盖安全性、可用性、过程完整性、保密性和隐私性）。

海康威视萤石云于 2017 年 2 月成功通过 SOC2 安全审计。

CSA-STAR 认证

CSA-STAR 认证是一项全新而有针对性的国际专业认证项目，由全球标准奠基者——英国标准协会（BSI）和国际云安全权威组织云安全联盟（CSA）联合推出，旨在应对与云安全相关的特定问题。

云安全国际认证(CSA-STAR)以 ISO/IEC 27001 认证为基础 ,结合云端安全控制矩阵 CCM 的要求，运用 BSI 提供的成熟度模型和评估方法，为提供和使用云计算的任何组织，从沟通和利益相关者的参与、策略、计划、流程和系统性方法、技术和能力、所有权、领导力和管理、监督和测量等 5 个维度，综合评估组织云端安全管理和技术能力，最终给出独立第三方外审结论。

海康威视萤石云于 2019 年 1 月成功通过 CSA-STAR 认证。

GDPR

海康威视致力于保护个人数据并全力支持 GDPR 要求的实施。海康威视一直采取多项举措来保护个人数据，包括通过数据收集授权，最小化数据收集，数据匿名化，通信和存储加密，数据安全审计等。 为了确保海康威视产品和服务的安全性，公司提出了一系列保护数据的政策，并建立了数据保护组，将 GDPR 要求融入到海康威视业务运营中。

5.6 人员管理

在全员网络安全意识教育上，海康威视意在构建全公司范围的产品安全意识教育氛围和文化氛围。为了做到这点，海康威视对于新入职的所有员工进行网络安全培训，并组织了持续的网络安全意识普及教育活动，开展基于各自业务需求的网络安全知识和技能的培训学习及其他意识教育活动，也会针对自己业务领域的特性进行网络安全案例的教育学习。公司会定期在内部宣传平台针对全员进行网络安全期刊宣传推动；同时还会通过宣传海报、信息安全视频/微电影、屏保等形式向全员宣传网络安全教育内容。

海康威视对各业务领域的网络安全关键岗位进行了识别，并明确定义了产品安全关键岗位。对产品安全关键岗位上的员工，我们提出了以下要求：

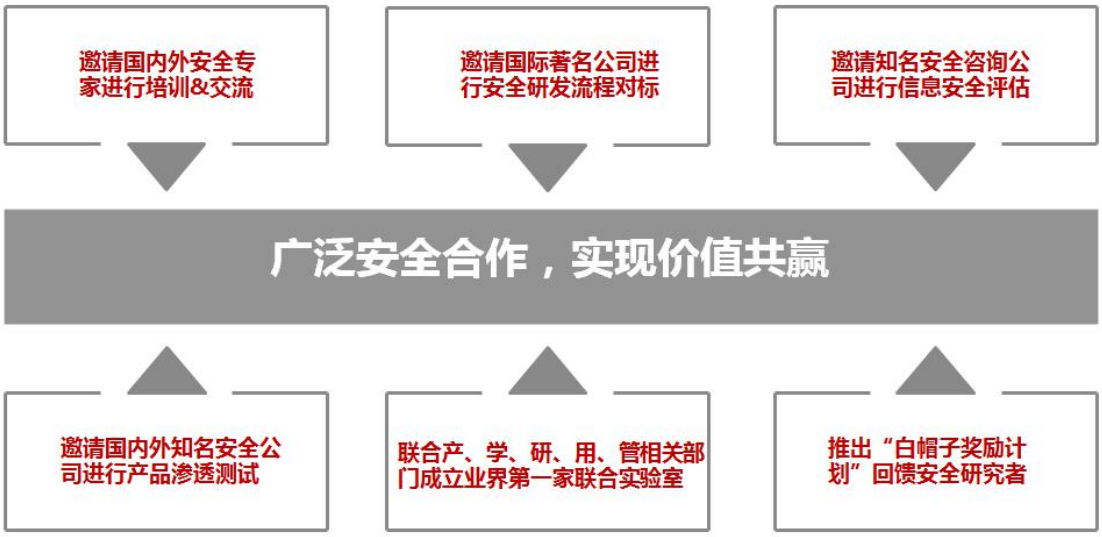
- 员工上岗前，要通过背景调查，确保安排背景和经历符合客户要求的人到岗位上，并签署《安全关键岗位保密协议》，明确员工的保密义务。
- 员工在岗时，要通过任职资格标准进行牵引，引导他们增强意识，提高相关技能。我们会定期进行安全审查。针对网络安全关键岗位人员在岗期间的行为，通过对员工在岗期间的网络安全行为进行调查，确定是否存在违规行为。
- 员工离岗时，通过实施离岗审查要点指导 HR 与安全专员进行离岗权限账号的清理或修改，必要时，清理离岗员工的资产。离岗审查含内部调动离岗和离职。

提高员工的技能和知识，让他们能够充分有效地履行职责。海康威视制定了针对性的安全能力提升计划和基线课程，通过系统的学习方案来提升员工的网络安全能力。

公司意在提升关键岗位员工网络安全方面的知识和技能，牵引员工主动学习。海康威视还通过开展各种实践导向的专项能力提升活动，提升网络安全关键岗位员工的知识和技能。 比如：网络安全专家大讲堂、网络安全论坛、网络安全案例库。

我们要求每个员工都要对自己所做的事情和产生的结果负责，不仅要对技术负责，也要承担法律的责任。我们的员工知道，网络安全问题一旦发生，可能会对客户、公司和个人带来极大影响。因此不管有意还是无意，海康威视都会以行为和结果为主要依据进行问责。

5.7 交流合作



- 邀请英国 EY 对公司的整个集团公司的信息安全评估工作，完善公司的整体的网络安全体制建设；
- 邀请 Cisco 安全部门对公司的研发安全管理体系进行对标建设 ,保证海康研发安全体系与国际一流公司看齐；
- 加强与国内外安全厂商的交流与合作，与 Synopsys、IBM 等进行广泛的交流与合作，提升公司产品的安全性；

- 邀请国内外知名的安全测试团队对公司产品进行渗透测试，最大限度地减小业务风险以保持安全风险在可控制的范围内；
- 邀请英国 EY 来对公司云产品进行 SOC2 审计，保证云产品的安全性和保密性；
- 邀请国内外知名安全专家来公司对研发进行授课，提高研发人员的安全业务水平；
- 产品安全实验室每年均与客户进行多次有关产品安全专题、应急响应工作机制和安全需求的交流，并及时向客户推送安全进展，了解客户需求；
- 公司面向社会推出的“安全白帽子奖励计划”对关注海康威视信息安全的国内外白帽子进行奖励，回馈推进海康威视产品安全不断进步的优秀安全技术研究者。

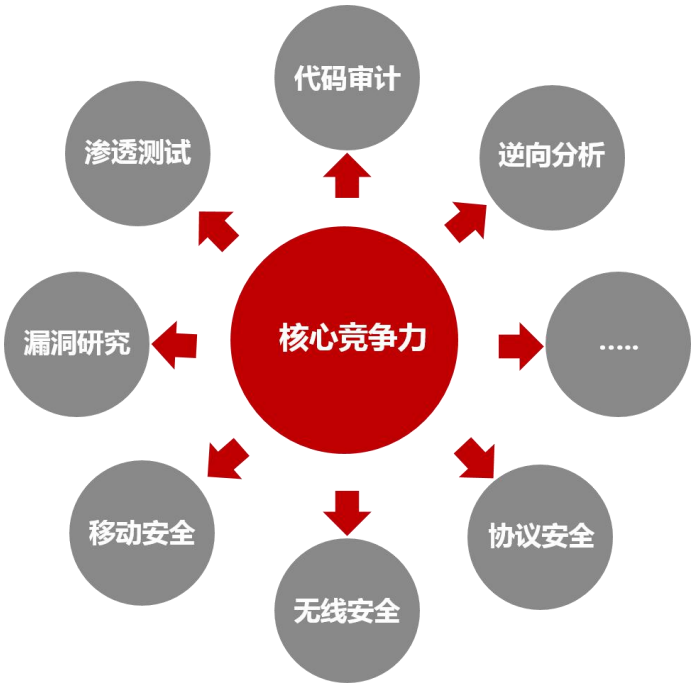
海康威视通过对外交流与合作，接纳利益相关方的反馈，吸收安全领域先进技术和管理经验，系统地转换为未来改进的目标，不断提升公司的信息安全能力。

6 产品安全研究

6.1 技术研究

网络与信息安全实验室致力于物联网相关的安全研究与实践，工作内容包括渗透测试、模糊测试、源码审计、逆向分析、漏洞跟踪、工具开发、物联网安全方案分析与研究；团队主要研究方向覆盖 WEB 安全、移动安全、协议安全、无线安全、固件安全、威胁情报、机器学习等多个领域，旨在先于黑客发现并及时解决安全问题。

目前团队已获得国家信息安全漏洞库 CNNVD 技术支撑单位，中国互联网网络安全威胁治理联盟成员，工业信息安全产业发展联盟安全应急服务支撑单位等荣誉。



核心竞争力：

- 嵌入式设备漏洞挖掘

结合海康威视在嵌入式设备安全领域的经验，使用固件逆向、串口调试、静态分析、符号执行等手段进行漏洞挖掘。

- 协议漏洞挖掘

集成商业工具和自研模糊测试工具，利用 Fuzzing 技术对主流物联网设备协议进行自动化漏洞挖掘，目前已发现数十个协议高危漏洞。

- 无线安全研究

团队拥有 RFID、无线射频、蓝牙模块等多种安全硬件测试环境，可实现无线数据报文窃听、无线信号重放攻击、无线信号欺骗攻击、无线信号劫持攻击、RFID 破解攻击、NFC 克隆攻击。

- 白盒审计

集成商业工具对所有内部使用的开源组件已知漏洞进行跟踪检测、威胁预警；内部团队在渗透测试过程中将针对目标源码进行白盒审计，全面提升漏洞挖掘效率。

- Web 安全

集成商业工具和自研 Web 测试工具，利用爬虫探测技术和被动代理技术对 Web 平台进行渗透测试，支持对 SQL 注入，XSS 跨站脚本，敏感信息泄露，命令注入等各类 Web 安全问题的检测 ,核心安全测试团队将对目标系统进行深入的渗透测试以发现更多潜在安全漏洞。

- 移动安全

团队结合内部移动安全检测分析工具，对移动 APP 进行全方位的安全检测，支持实时捕获交互协议报文、敏感信息自动识别；支持对 Android 内核已知漏洞进行检测；支持对移动 APP 进行安全加固，防止恶意攻击。

- 威胁情报

团队搭建多种类型分布式高交互蜜罐 ,可全网实时感知各种物联网恶意攻击行为并进行实时关联分析预警。

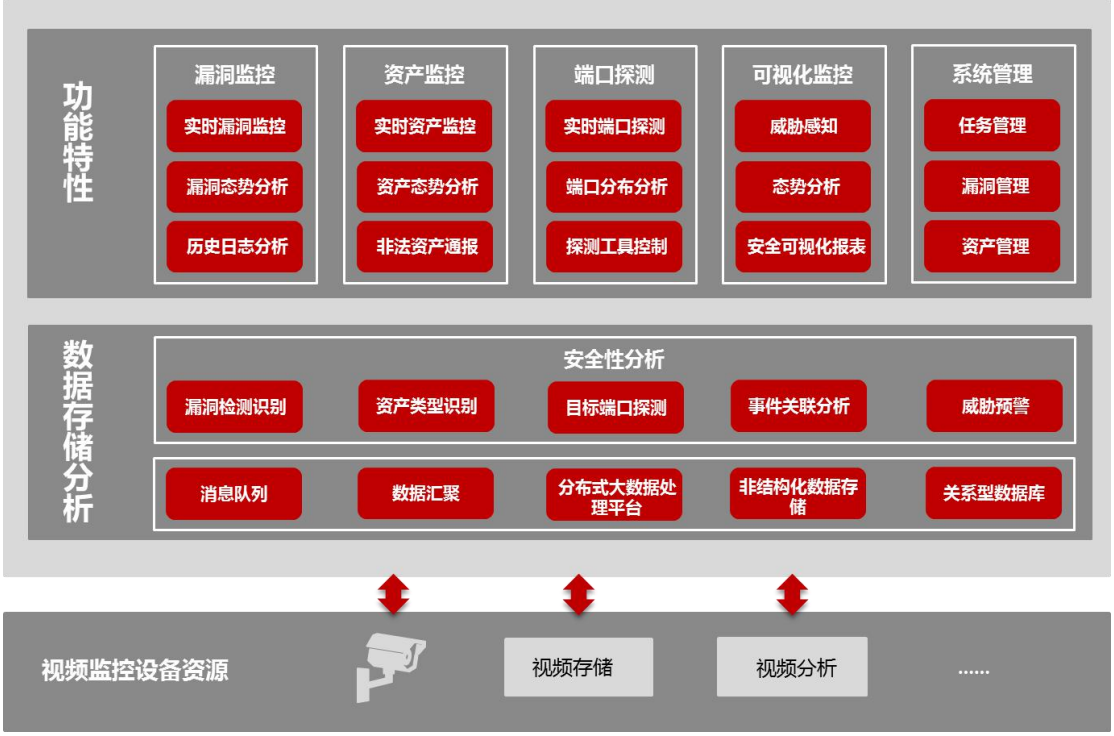
- 机器学习

团队利用机器学习算法对物联网设备日志进行安全分析，提供多种安全攻击检测模型，可以快速从海量日志中发现潜在或已知的恶意攻击行为并进行实时威胁预警。

6.2 安全态势感知

由终端与设备、通信与网络、平台与应用构成的庞大的物联网系统，不但需要每个层面的多重安全防护，还需要有端云协同的智能大数据安全分析能力。实现整网的智能安全态势感知、可视化和安全防护，必将是物联网安全的发展方向。

态势感知是在大规模系统环境中，对能够引起系统状态发生变化的安全要素进行获取、理解、显示以及预测未来的发展趋势。



脆弱性评估

脆弱性评估是决定安全态势感知系统能否有效检查安全隐患的关键。海康威视安全态势感知系统集成业内主流的漏洞库，可针对目前已出现的漏洞进行检查。另外，海康威视拥有专业的漏洞研究团队，不断跟踪其它知名安全组织和厂商发布的安全公告，并持续分析、挖掘、

验证各种新型漏洞。借助海康威视专业漏洞研究团队的持续投入和漏洞库的持续升级，可及时帮助用户发现安全隐患，防患于未然。

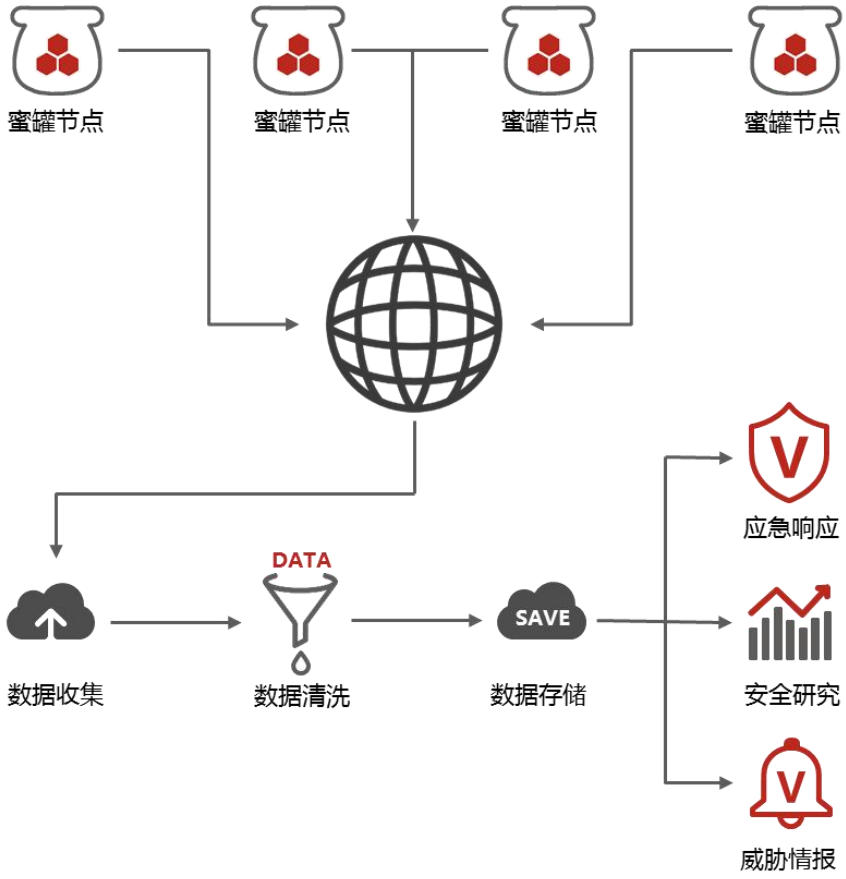
除此之外，海康威视视频安全态势感知系统还可对发现的安全威胁和资产信息进行关联分析，通过建立的大数据分析模型对实时数据和历史数据进行动态分析，可准确、高效地感知整个网络的安全状态以及发展趋势，从而对视频监控网络的资源作出合理的安全加固，保障视频监控系统安全。

安全可视化

可视化展示能够直观地呈现数据特点，同时容易被读者接受和理解，所以大数据分析（深度包检测、全流量分析）结果需要可视化展示。

当系统遭到攻击时，需要快速地识别攻击来源，攻击路径，对攻击做出快速的响应，在攻击造成更大的破坏之前，实施有效的措施，减少损失。在攻击之后，需要快速地防止此类攻击的再次发生。

6.3 蜜罐



蜜罐技术本质上是一种对攻击方进行欺骗的技术，通过布置一些作为诱饵的主机、网络服务或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机。

得益于数据存储、数据检索、数据挖掘和威胁情报等技术的兴起和发展，蜜罐技术的价值可以被更充分的发挥。海康威视基于自研和改造的蜜罐作为数据采集器，在全球范围内部署蜜罐节点，并建立了对蜜罐数据进行收集、处理、存储和检索的蜜罐数据管道，为安全研究、应急响应、攻击溯源和态势感知提供数据支撑。

海康威视蜜罐系统基于规则引擎，实时监测针对物联网设备的攻击行为，并对未知威胁进行

预警。蜜罐系统的分析引擎，基于蜜罐系统的历史数据，可以对恶意攻击者进行重点监控和关联分析，并预测威胁趋势。

海康威视的蜜罐系统作为海康威胁情报平台的重要组成，将持续监控来自全球的安全威胁，保障用户设备的安全稳定运行。

7 安全性承诺

海康威视致力于使用领先的安全及隐私保护技术来帮助客户保护其个人信息 ,以及采用全面的方法来保护用户的数据。

海康威视在整个视频物联网应用生态系统中使用统一的集成安全基础架构。海康威视拥有一支专业的安全团队，负责为所有海康威视产品提供支持。该团队为开发中和已发布的产品提供安全审核和测试。安全团队还提供安全培训，并积极监控新增安全问题和威胁的报告。要进一步了解如何向海康威视报告问题以及如何订阅安全通知，请参阅 https://www.hikvision.com/cn/about_593.html。

海康威视

网络安全白皮书

见远 行更远

See Far, Go Further

HIKVISION

杭州海康威视数字技术股份有限公司
地址:杭州市滨江区阡陌路555号
电话:0571-88075998