工业互联网产业联盟
Alliance of Industrial Internet

工业云安全防护参考方案

工业互联网产业联盟（AII）
2017年2月

工业云安全防护参考方案

声　明

本报告所载的材料和信息，包括但不限于文本、图片、数据、观点、建议，不构成法律建议，也不应替代律师意见。本报告所有材料或内容的知识产权归工业互联网产业联盟所有（注明是引自其他方的内容除外），并受法律保护。如需转载，需联系本联盟并获得授权许可。未经授权许可，任何人不得将报告的全部或部分内容以发布、转载、汇编、转让、出售等方式使用，不得将报告的全部或部分内容通过网络方式传播，不得在任何公开场合使用报告内相关描述及相关数据图表。违反上述声明者，本联盟将追究其相关法律责任。

工业互联网产业联盟

联系电话：010-62305887

邮箱：aii@caict.ac.cn

目录

1 工业云概述

1.1 工业云概念

工业云是在国家工信部“工业云创新行动计划”的背景之下提出的，是充分利用云计算、物联网、大数据等新一代信息技术，结合“资源及能力整合”业务手段，汇集各类加快新型工业化进程的成熟资源，面向工业企业，通过网络将弹性的、可共享的资源和业务能力，以按需自服务方式供应和管理的新型服务模式。工业云为工业转型升级、产业创新发展提供重要支持，通过构建安全、稳定、知识共享及高度适应且可扩展的云端能力资源集，为 “互联网+”和工业实践相结合的“中国制造 2025”提供保障。

本文中说描述的工业云指工业互联网产业联盟发布的《工业互联网体系架构（版本1.0)》中“应用支撑的实施”部分和<<工业互联网平台 通用要求>>中的工业互联网平台架构中所描述的工业云和工厂云平台，从实施部署角度，工业云可以部署在工厂内部，也可以部署在工厂外部，如图1所示。

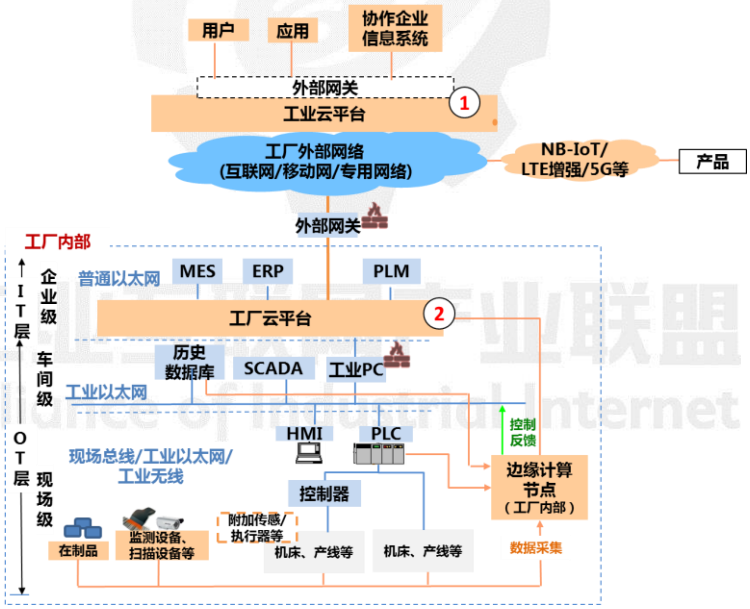

图1　工业互联网平台部署示意

工业云的典型构成如下图 2 所示：

图 2 工业云典型构成图

工业云面向工业产品研发设计、生产、销售以及订单化生产的全生命周期所需制造资源和制造能力实施整合与池化，为工业企业方便、快捷地提供各种制造服务，以实现社会制造资源的共享与制造能力的协同。在工业云，服务提供者与服务客户角色并不固定。作为服务提供者向工业云贡献制造资源、制造能力、制造技术和知识。同时，服务客户角色可以在工业云上获取所需的制造资源、制造能力、制造技术和知识开展活动。工业云能够利用云计算理论开展服务业务，快速叠加多种类型的资源与能力。面对工业用户的需求，工业云通过解决方案契合，合理调度用户所需的服务，推动用户从以订单和产品为中心的传统制造模式向以需求为中心的制造模式转变，实现新一代工业转型升级。

工业云整合了云计算的基础设施和工业制造的基础设施，为工业云平台资源服务和软件应用服务层提供运行最基础的设施支撑，同 IT 云 IaaS 一样，工业云亦可向外提供基础设施服务；工业云亦包括制造资源（智能机器人、3D 打印、智能仪表等）、工业软件（CAX、MES、ERP、PLM

等)、IT 资源（计算资源、存储资源、网络资源等)、大数据资源（设备数据、物料数据、客户数据、知识库等)，不仅可以直接向产业用户提供资源服务，也可通过软件应用将资源服务封装之后，作为应用向最终用户提供。

作为关联产业生态新模式建立，企业智能生产的支撑要素，工业云的在线资源及服务对安全性的依赖程度极高。在工业云提供服务的全过程中，以风险控制，运行、数据安全保障，业务合规核查，冗余副本机制为主要内容的安全保障体系贯穿全局，为工业云的资源能力整合、资源准入、工业云运行以及企业服务交付应用提供全方位的安全保障。

1.2 工业云典型应用

从云计算和工业技术角度来看，典型的应用包括云存储、云应用、云制造、云社区、云设计、云生产、云管理。

1) 云存储

云存储是工业云基于互联网或者分布式存储理论提供的存储解决方案。该服务提供面向工业智能化应用需要实施的查询、实时监管、仿真、渲染、量级归档、流程化或离散化工作逻辑集中的存储服务。

云存储提供给企业分散、分步、分时、分区域的灵活存储方式，并在工业企业生产组织整个生产周期中提供对数据的整体管理、灵活调用。云存储的按需交付、成本低廉，灵活定制、扩展自如等特性使得工业企业或工业智能应用专注生产制造、智能化支撑的核心业务而无需为复杂、逻辑繁琐、权限横向集成要求高的存储业务进行投入。

2) 云应用

工业云应用通过资源整合、能力池化并进一步实施产品化特征封装集群化服务。云应用服务在集成工业资源、工业能力过程中，面向工业企业的宽泛、个性需求，形成产品化落实。

工业云应用包含一系列通用型的信息化管控服务。如：企业管理、企业在线营销、企业信息化协同办公等。还包括一系列面向工业生产制造专项服务。如：生产制造智能化支撑：设备运行优化、虚拟设计（PDM)、CAD、CAM、在线 3D 打印服务、工业管理（WPM)、制造执行（MES)、质量管理（QMS)、供应链（SCM)、产品管理（PLM)、设备远程维护、能源管理、环节管理。

云应用可以把传统软件“本地安装、本地运算”的使用方式变为”即取即用”的服务，通过互联网或局域网连接并操控远程服务器集群，完成业务逻辑或运算任务的一种新型应用，云应用不但可以帮助用户降低 IT 成本，更能大大提高工作效率。

3) 云社区

云社区是工业云集合各个工业产业内外的应用厂商、用户、专家，以灵活多样的形式，实施知识库收集、经验分享、专业化咨询和权威辅导的在线交流平台，同一主题的社区集中了具有共同需求的访问者。

云社区作为工业云平台的服务，一方面可以向企业用户推送消息，使得企业用户随时随地及时地了解最新的行业政策，知晓国内外的行业动向。用户和企业可以在社区中发布相关信息、需求、问题，从不同的拥有直接经验或者权威理论的用户、企业、专家处得到帮助。打造面向新时期工业产业知识汇集的社区化虚拟空间。在知识汇集的基础上，整合专业化服务和资源，向工业企业提供供需对接和资源共享服务，包括：企业资源信息发布、供需对接、企业沟通社交、设计标准、零部件库、设计案例、培训教程等。

4) 云设计

云设计服务于产品研发，为工业企业整体提升研发、创新竞争力提供支持。通过聚合顶端的设计资源和设计人才，打造“工业设计仿真验证快速成型”全流程设计服务，推行网络化协作以及众包的设计模式。从技术角度实现计算机辅助设计（CAD）、计算机辅助工程（CAE）等先进设计工具同生产排产制造的有机融合。以云计算的理论为指导，按需租用将设计软件及周边辅助类应用提供给工业企业，辅以社区专家技术指导，企业能够在极大的成本可控前提下，方便、快捷的完成专业化产品创新研发设计。显著缩短研发周期、提高研发效率。利用协同设计模式，亦能够将企业外部设计能力引入到产品设计之中，使企业更好利用外部智力，提升自体产品竞争力。

5) 云制造

云制造为通过云计算技术为工业企业提供生产管理环节所需的信息技术手段。云制造提供的业务能力服务覆盖计划、排程、制造、质量、能源、设备、库存等各环节。保证生产制造过程的高效、高质、低耗、灵活、准时。

6) 云管理

云管理是指借助云计算和其他相关技术，通过集中式管理系统建立完善的数据体系和信息共享机制。工业云通过资源与能力的整合，将通常意义上的云服务资源管理与企业管理应用进行合并，并封装为云管理应用。是应用互联网、云计算等新兴技术所带来的创新型管理模式，以实现经营管理优化为目的，提升总体管理的信息化与自动化程度。云管理平台服务中，用户可以实现对各种云资源和云服务的运维管理，包括资源管理、服务管理、用户管理、权限管理、费用查询和支付管理等功能。同时，云管理打破传统的组织局限、突破时空局限、突破资源局限，进一步

整合企业资源管理、客户关系管理、制造执行管理、财务管理、进销存管理、成本管理等应用软件，帮助企业构建云端管理新模式。

1.3 工业云典型架构

工业云是在云计算模式下对工业企业提供 TI 服务，使工业企业的社会资源实现共享化。它是传统云与专业的工业软件和定制化管理系统的结合。是通过信息资源整合为工业提供服务支持的一种云计算创新服务模式，通过将云计算、工业软件、物联网、大数据和其他相关技术的有机结合为制造业构建了一种特有的 IT 服务生态链系统，以 PaaS 和 SaaS 模式为主体向工业企业提供云存储服务、云资源服务、云应用服务、云社区服务、云管理服务和云制造服务等。

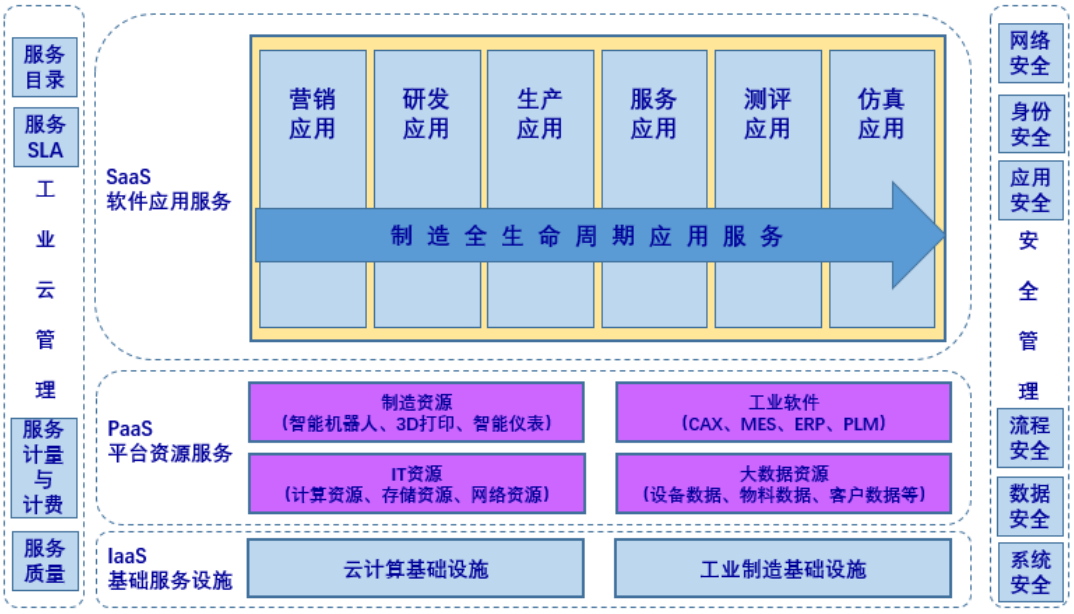

图 3 工业云典型架构

工业云与云计算的架构相同，由基础设施服务层（IaaS）、平台资源服务层（PaaS）、软件应用服务层（SaaS）。

基础设施服务层（IaaS）包含云计算的基础设施和工业制造的基础设施，通过工业云亦可向外提供基础设施服务。基础设施服务层为工业云的平台资源服务和软件应用服务层提供运行最基础的设施支撑。

平台资源服务层（PaaS）包括制造资源（智能机器人、3D 打印、智能仪表等）、工业软件（CAX、MES、ERP、PLM 等）、IT 资源（计算资源、存储资源、网络资源等）、大数据资源（设备数据、物料数据、客户数据、知识库等），不仅可以直接向客户提供资源服务，也可通过软件应用将资源服务封装之后，作为应用向最终客户提供。

软件应用服务层（SaaS）提供制造全生命周期的软件应用，包括：营销应用、研发应用、生产应用、服务应用、测评应用、仿真应用，可针对客户的需求提供各种不同的软件应用，通过软件应用也可将基础设施服务和平台资源服务进行封装，向外提供软件应用服务。

1.4 工业云的国内外发展现状

1.4.1 国内发展现状

我国高度重视工业云的发展。近年来，国家出台了一系列政策鼓励工业云的发展，把工业云作为推动两化深度融合和“互联网+”的重要抓手，初步形成“政府引导，企业主体，平台共享，联盟推进”的基本方针。工业云政策发展历程见图 1。

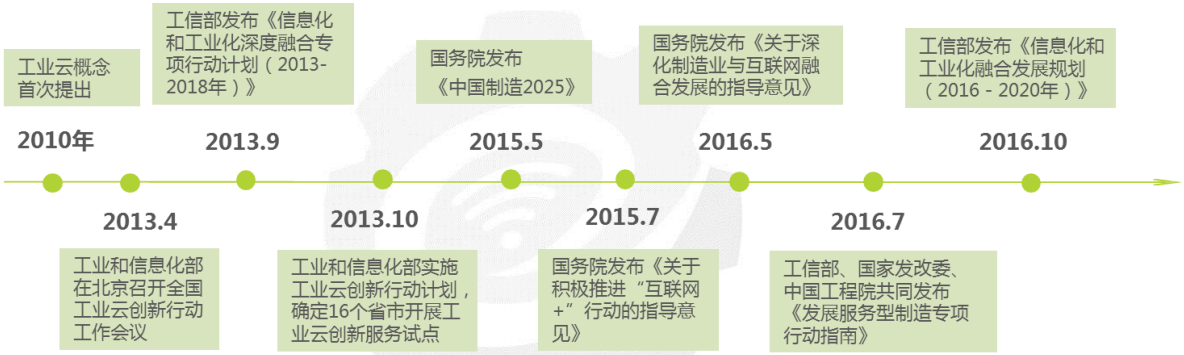

图 4 工业云政策发展历程

除了政府主导搭建以外，各地有条件的企业也在工业云领域加紧布局，对工业云的发展模式进行了全新探索，进一步丰富了工业云的内涵，扩大了工业云产业的规模。

智能云科整合广泛的社会资源，打造社会化协同的云制造服务平台，提供一站式的云制造、个性化定制及工业人才教育服务。

航天云网搭建的工业云平台满足企业以较低的成本获取制造所需的关键资源与服务，高效完成制造业务，支持企业进行产业链条管控与跨企业协同的产业及协作服务，提供协同研发、采购、营销、生产、售后等协作服务，帮助企业打通内外信息流、业务流、物流、资金流。中国电信基于电信云网一体化资源，构建云网合一的工业专网云平台，面向工业企业提供设计协同、制造协同、供应链协同、服务协同、资源共享等服务。

三一重工旗下的树根互联已接入 23 万多台设备，实时采集 5000 多个运行参数，为众多客户提供精准的大数据分析、预测、运营支持及商业模式创新服务。

此外，一些企业也陆续推出了自己的工业云平台，将核心业务向云平台迁移，用云计算模式改造原有生态系统，动态优化配置资源，实现生产制造全过程、全产业链、产品全生命周期的优

化管理，培育企业内部全流程信息共享和业务协同新模式。

沈阳机床基于i5智能数控系统实现了从机床的智能化到车间、工厂智能化的机床加工行业全链条解决方案，诞生了以智能设备互联、基于数据和信息分享的工业云平台，以此为载体连接社会的制造资源，实现社会化生产力协同的“i5新生态”。

经过几年的建设与发展，国内工业云平台已初具规模，并初显成效，为提高企业信息化水平、研发水平和制造能力、促进企业转型升级发挥了积极的作用。据不完全统计，国内公共工业云服务平台累计注册用户已超过1500万，推动了工业云服务的应用落地，合力打造出“化云为雨”的新局面。

1.4.2 国外发展现状

国外主要工业国家，如德国、美国，正在大力推广和应用工业云。德国在产业政策上对工业云相关的技术和应用给予了大力的支持。德国提出的工业 4.0，是以信息物理融合系统(CPS)为基础，基于云计算平台来处理问题，实现生产高度数字化、网络化。德国在中小企业中进行试点示范，为中小型企业在物联网产业和互联网中的项目提供资金，尤其是数字产品，以及适应数字化进程和网络商业模式的开发测试。美国在未来智能制造中，不遗余力地支持工业云。美国提出的工业互联网是要将工业系统与云计算、分析、感应技术以及互联网连接融合，构建制造新模式。美国工业互联网联盟在2015年发布了《工业互联网参考体系架构》，助力软硬件厂商开发与工业互联网兼容的产品，实现企业、云计算系统、网络等不同类型实体互联。

工业云的产业化应用也得到了各个企业的重视，而投身其中的，不仅有工业企业，还有信息技术企业。

2014 年，GE 就发布了首个工业互联网云平台 Predix，该平台将机器、数据、人和其他设备连接起，实现分布式计算、大数据分析、数据资产管理和机器间通信，提高生产效率。到 2014 年底，Predix 平台每天监测和分析来自 1000 万个传感器的 5000 万项元数据，这些数据涉及资产价值高达数万亿美元，2015年底GE宣布Predix营收50亿美元，并宣布开放其云平台，使用户可以开发个性化的应用，这将促使Predix快速增长并形成垄断优势。

2016年西门子推出了开放工业云平台MindSphere，可以提供预防性维护、能源数据管理以及工厂资源优化等数字化服务。菲尼克斯电气为工业定制的云技术“ProfiCloud”，是其在工业物联网领域最创新的产品。日本发那科与思科、罗克韦尔自动化发布了FANUC Intelligent Edge Link and Drive（FIELD）system，FIELD system能实现自动化系统中的机床、机器人、周边设备及传感器

的连接并可提供先进的数据分析。

另外，北欧最大的 IT 业务提供商叠拓（Tieto Information Technology）也推出了工业云服务，并将其称为工业社区云（Industry Community Clouds）。

欧洲另一家 IT 服务提供商 Prevas 公司也推出了工业云服务。由 42Q 公司提供的基于云的 MES(制造企业生产过程执行管理系统)更便于部署和配置，并且更快更便宜。国外的研究机构针对工业云进行了一些列研究工作，欧盟委员会部署的欧洲合作项目 IMC-AESOP （ArchitecturE for Service-Oriented Process—Monitoring and Control）就是典型的代表，该项目从系统架构、技术难点和工程实现等角度对工业云进行了深入的研究。

亚马逊等电商也开始探索工业云服务。亚马逊公司旗下的 Amazon Web Services（AWS）发布了全新平台 AWS IoT，旨在让制造业客户硬件设备能够方便地连接 AWS 服务。SAP、Oracle 等信息技术公司依靠本企业在信息化领域的领先程度，从云计算操作系统（云 OS)、工业软件等方面推进工业云的发展。

2 工业云安全威胁及相关安全标准

2.1 工业云安全威胁

安全问题是阻碍工业云发展的重要因素,近些年国内外很多组织都发布过云安全威胁的报告,在这里我们列举出一些工业云可能需要面对的安全威胁:

1）数据泄露、篡改、丢失

工业云中存储的数据具有较高的敏感性，涉及工业企业知识产权和商业机密，是其核心资产的重要组成部分，有些数据资料甚至关系到国家安全，因此对数据的窃取或者破坏将造成严重经济损失、社会影响甚至国家安全等问题。

2）权限控制出现异常

单一或松散的身份验证、弱口令、不安全的密钥或证书管理都可能导致访问权限出现异常，一旦恶意用户掌握了其不该拥有的权限后，对云计算平台所造成的安全影响是致命的，攻击者就可以伪装成合法用户读取、更改或者删除用户数据，进而影响工业企业的正常运行。

3）API 安全

工业云在提供其服务时会提供一些用户 API 接口。IT 人员利用他们对云服务进行配置、管理、协调和监控，也在这些接口的基础上进行开发，并提供附加服务。而 API 是工业云系统中最暴露的部分，更容易成为攻击目标。

4）系统漏洞利用

工业云服务提供的基础资源属于共享设施，所以其共有的系统安全漏洞可能会存在于所有使用者的云资源当中。这给攻击者提供了便利的攻击途径，并节省了大量的研究成本，一个业务被攻陷后，同一个云中的其它业务很可能会被同一种攻击类型攻击成功。

5）账户劫持

攻击者通过钓鱼攻击和利用软件漏洞可以对用户的账户登录会话进行劫持，在不知道目标账户和口令的前提下，可以仿冒合法用户的登录会话，从而隐蔽的获取访问权。如果攻击者获取了远程管理云计算平台资源的帐户登录信息，就可以对业务运行数据进行窃取与破坏。

6）恶意内部人员

人们在部署各式安全防护设备的同时，往往会忽略来自内部人员的恶意危害，这些人其破坏面广、力度大，可辐射其整个云环境。

7）APT 攻击

高级持续性威胁（APT）通常隐蔽性很强，很难捕获。而一旦 APT 渗透进云平台，建立起桥

头堡，然后在相当长一段时间内，源源不断地、悄悄地偷走大量数据，形同寄生虫，危害极大。APT 攻击已经逐渐成为当前威胁国家安全的重要问题，由于工业云平台涉及到更多国家安全层面的问题，因此工业云可能会遭受到很多的 APT 攻击。

8）拒绝服务攻击

一直以来，分布式拒绝服务(DDoS)一直都是互联网环境下的一大威胁。在工业云中，许多用户会需要一项或多项服务保持 7×24 小时的可用性，业务中断将造成严重的经济损失甚至是危及人员生命财产安全的严重事故，因此应该引起额外的重视。

9）共享技术漏洞

云计算中采用了大量的虚拟化技术和共享技术，而这些技术本身可能存在安全漏洞。因为其处于底层，共享技术的漏洞将对云计算构成了严重威胁。如果一个服务组件被破坏泄露，如某个系统管理程序、一个共享的功能组件、或应用程序被攻击，则极有可能使整个云环境被攻击和破坏。

10）设备接入安全

工业云平台可能涉及到智能设备的接入，针对这些设备的可能存在非法接入，非法控制，连接窃听等问题，一旦这些智能设备被攻击后，如果工业云平台对智能设备的安全接入考虑不周全时，攻击者可以利用智能设备作为跳板对工业云系统进行攻击。

云计算平台与工业系统最近也受到了很大的挑战，越来越多的安全事件在最近几年频繁的爆发。

2014 年，代码空间（Code Spaces）的亚马逊 AWS 账户没有采用多因素认证，攻击者对其成功进行了账户劫持，获得控制权后删除了所有数据，导致其该公司破产。

2015 年，反病毒公司 BitDefender 托管在亚马逊 AWS 公有云应用中的一些客户用户名和密码被黑客窃取，并索要 15000 美元的赎金；

2014 年到 2015 年间，英国电信供应商 TalkTalk 在发生了多起安全事故，导致 400 万客户的个人信息被盗。

2010 年，StuxNet 病毒感染了伊朗 14 个工厂的 PLC，其中包含一个铀浓缩车间，病毒修改了离心机的控制程序导致多台离心机损坏；

2011 年，一个钢铁车间的控制系统遭受黑客的鱼叉攻击，造成高炉的非正常关闭；

2015 年，两名黑客展示了如何通过漏洞，完全实现对一辆汽车的远程控制。

另外，最近越来越多的安全漏洞被发现，根据国家信息安全漏洞共享平台（CNVD）所收录的漏洞数据显示，截至到 2016 年底，收录的云及虚拟化相关的漏洞数以千计，经关键字查询计有 1383 个，并且自 2010 年以来云计算技术及应用服务发展迅速，同时云及虚拟化相关系统的脆弱性问题日益受到安全业内的关注，云及虚拟化相关的漏洞数量也呈快速增长的趋势，如图 5 所示。而这些漏洞也势对工业云安全构成巨大的安全威胁。

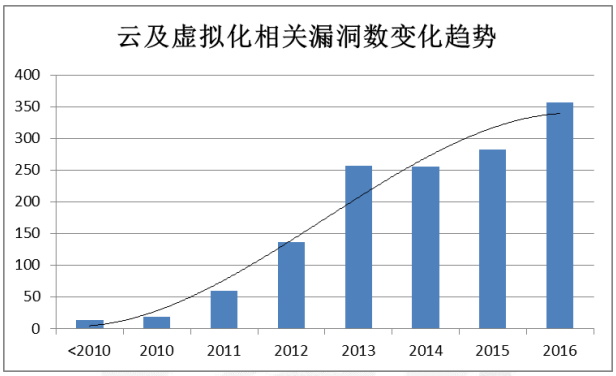

图 5　快速增长的云及虚拟化相关漏洞数

利用云及虚拟化相关漏洞所造成的安全威胁，主要涉及未授权的信息泄露、管理员访问权限获取、拒绝服务攻击、未授权的信息修改以及普通用户的访问权限获取等。根据 CNVD 收录的云及虚拟化漏洞的统计分析可知，未授权的信息泄露、管理员访问权限获取以及拒绝服务相关的漏洞占了大多数，也就是说云计算相关的应用及服务系统的安全防护的重点将是云上的数据安全、系统管理员的账户安全以及提升抗拒绝服务攻击能力以保障云服务的业务连续性（图 6）。对比 2016 年新增的云及虚拟化漏洞的危害性分析情况（图 7），可知涉及数据安全类的漏洞数据增幅明显，可造成信息泄露和信息修改的两类漏洞合计占比高达 2016 年新增漏洞的三分之二。从漏洞危害性的角度来看，在云及虚拟化领域，数据安全类漏洞占有很大的比例。显然，这些漏洞被利用所造成的数据安全威胁将是云及虚拟化安全领域首要解决的问题。

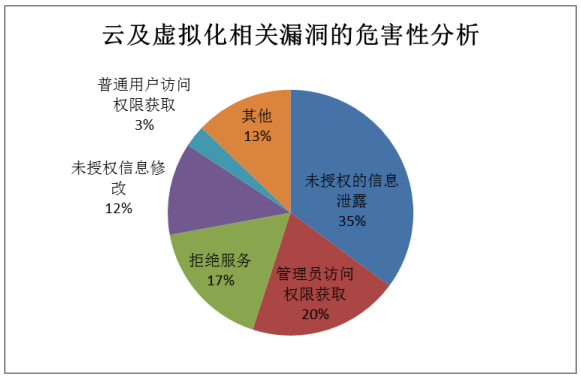

图 6 云及虚拟化相关漏洞的危害性分析

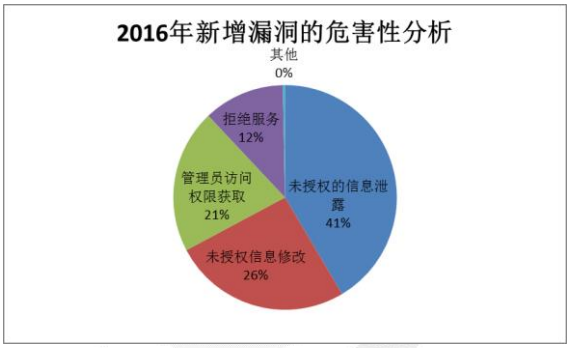

图 7 2016 年新增的云及虚拟化漏洞的危害性分析

从这些安全事件和安全漏洞统计结果可以看出，云计算领域的安全威胁主要是服务异常和信息泄露，这些威胁同样会存在于工业云。工业系统需要稳定的服务保持正常运转，信息系统故障导致停工将造成严重的损失，因此保证云服务的稳定性至关重要，工业云中的企业数据是企业核心资产的一部分，信息泄露也将造成严重损失，而针对工业控制系统的攻击将直接造成严重经济损失或者不可挽回的严重后果，因此工业云的安全性要求将远远高于传统云计算系统。

2.2 工业云安全标准

在工业云安全的标准的研制方面，国外与国内都处于起步阶段，大部分已发布和在研的标准都是针对云计算安全的。

2.2.1 国外云安全标准现状

目前，国际上已经有众多标准化组织开展云安全领域的标准制定，相关的机构主要如下所示：

1、ISO/IEC 第一联合技术委员会（ISO/IEC JTC1）

2、美国国家标准技术研究所（NIST）

3、欧洲网络与信息安全管理局（ENISA）

4、云安全联盟（CSA）

5、国际电信联盟—电信标准化部（ITU-T）

6、区域标准组织（美国）CIO 委员会

7、开放式组织联盟（TheOpenGroup）

8、结构化信息标准促进组织（OASIS）

9、分布式管理任务组（DMTF）

上述标准组织在云安全领域的主要进展如下：

（1）ISO/IEC：在云计算领域的标准化工作主要由 JTC1 下工作组 SC38 来完成。

相关标准研究成果有：《开放虚拟机格式》、《云计算安全与隐私管理系统》、ISO/IEC 27017《基于 ISO/IEC 27002 的云计算服务的信息安全控制措施使用规则》、ISO/IEC 27018《公共云计算服务的数据保护控制措施实用规则》、ISO/IEC 27009《ISO/IEC 27001 在特定行业/服务的认可的第三方认证中的使用和应用》。

目前，ISO/IEC JTC1/SC27 在研的云计算安全标准研究项目有：《云和新数据相关技术的风险管理》、《云安全用例和潜在的标准差距》、ISO/IEC 27036-4《供应商关系的信息安全—第四部分：云服务安全指南》。

（2）NIST:为美国联邦政府提供云架构以及相关的安全和部署策略，包括制定云定义、云安全架构、云风险缓解措施等。

具体标准包括：《云计算参考体系架构》)、《完全虚拟化技术安全指南》、《云计算安全障碍与缓和措施》、《公共云计算中安全与隐私》、《通用云计算环境》、《美国政府云计算安全评估与授权的建议》。

（3）ENISA：自 2009 年，就启动了云计算安全的相关研究工作，云安全标准化方面主要关注云计算中风险评估和风险管理等，由 ENISA 下 WG NRMP 工作小组负责。

与云安全相关标准包括：《云计算—信息安全保障框架》、《云计算—信息安全的好处，风险和建议》、《政府云的安全和弹性》。

（4）CSA：电信安全联盟 CSA（Cloud Security Alliance），2009 年 4 月成立，目标是推广云安全的最佳实践方案，开展云安全培训。组织包括 100 多家来自全球 IT 企业加盟，并与 ITU、ENISA 等二十家标准组织及机构合作，在云安全最佳实践与标准制定方面具有很大的影响力。

在云安全标准化方面工作：以白皮书的形式向全球发布云安全方面的参考与建议，已完成《云

计算面临的严重威胁》、《关键领域的云计算安全指南》、《身份隐私与接入安全》等 3 项标准化建议，发布了《如何保护云数据》、《定义云安全：六种观点》等 2 项云安全相关的建议书。2016 年 10 月，发布了《云计算安全技术要求（草案)》(包括总则及 IaaS 安全技术标准要求、SaaS 安全技术标准要求和 PaaS 安全技术标准要求的草案)。

（5）ITU-T：ITU-T（国际电信联盟通信局）主要关注云安全架构、虚拟化安全等方面，其中 SG13 研究成立了云计算专项工作组，旨在促进电信支持云计算的相关标准开发工作。

ITU-T 下的云计算焦点组（Focus Group on Cloud Computing,PG Cloud）制定了《云安全、威胁与需求》标准、电信云安全研究小组-SG17 制定了《电信领域云计算安全指南》标准。

（6）CIO 委员会：2010 年 2 月，与 MIST、GSA（General Services Administration）以及 ISIMC（Information Security Management Committee）一起合作完成《美国政府云计算风险评估方法》。基于标准化流程的的风险评估：提出将云计算置于联邦监控之下的方法及流程，明确了联邦政府、云提供商以及评估小组在云安全中的作用和职责。

（7）TheOpenGroup：云安全相关的工作组为云工作组（Cloud Work Group），于 2009 年 10 月成立，工作组的标准由组织成员制定，但非成员也可以参与讨论。

云安全标准主要包括《云计算标准》、《云安全和 SOA 参考架构》。

（8）OASIS：结构化信息标准促进组织（OASIS)。与云安全相关活动：云身份（IDCloud）技术委员会，2010 年成立，致力于解决云计算中身份管理带来的严重的安全挑战，包括成员 Red Hat，TBM，Microsoft 等大型 IT 企业。云安全相关标准主要为《身份在云中的使用》。

（9）DMTF：分布式管理任务组（DMTF)。云安全相关的工作组及活动：2009 年 4 月，成立了工作组—开放云标准孵化器（Open Cloud Standard Incubator）;2010 年 7 月成立了云管理工作组；2011 年 4 月成立了云审计数据联邦工作组，它致力于促使云供应商提高安全能力。云安全相关标准主要为《云管理体系结构》。

2.2.2 国内云安全标准现状

在安全问题上，目前国内针对工业云安全的方案与标准还没有制定及发布，近几年国内标准化组织主要是针对云计算发布了一些标准。

国务院发布了《国务院关于促进云计算创新发展培育信息产业新业态的意见》(国发（2015）5 号)。全国信息安全标准化技术委员会(一下简称信安标委)组织研究制定了亟需的云计算安全标准，已发布了 GB/T 31167-2014《信息安全技术 云计算服务安全指南》和 GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》2 项国家标准。

目前正在研制的关于云计算安全的国家标准还有《信息安全技术 云计算安全参考框架》和《信息安全技术 云计算服务安全能力评估方法》，信安标委也正在组织专家研究、制定云计算安全技术路线图，完成云计算安全标准的框架设计，研究和制定我国云计算安全的系列标准。

我国云安全标准处于起步阶段，尚未正式出台，主要由 CCSA 和 TC260 两个组织制定。

（1）中国通信标准化协会（CCSA）

- 正在制定的标准有:
  - 在云计算的总体架构方面，有《云安全标准体系研究》、《公有云安全基线要求》、《云计算安全威胁和需求》等;
  - 在访问控制方面，有《云计算身份识别与访问管理应用场景及技术要求》、《云计算的可信技术研究》等;
  - 在云中隐私和数据保护方面，有《公有云数据安全要求》、《公有云中隐私保护措施》等;
  - 在行业云方面，有《基于云计算的电子政务公共平台安全》、《基于云计算的居民健康服务平台安全框架》等;
  - 在基于云计算的 IDC 方面，有《基于云计算的互联网数据中心信息安全技术要求》和《基于云计算的互联网数据中心信息安全管理要求》;
  - 在云计算应用安全方面，有《云计算应用安全运营技术要求》等。

（2）全国信息安全标准化委员会（TC260）

- 由公安部和全国信息安全标准化技术委员会提出，全国信息安全标准化技术委员会归口的标准《信息系统等级保护安全设计技术要求 云计算安全》于 2016 年 7 月已形成初稿;
- 由全国信息安全标准化技术委员会提出和归口的标准《信息安全等级保护基本要求 第 2 部分：云计算安全扩展要求》于 2016 年 7 月已形成征求意见稿;
- 在信安标委内部设立了专门对云计算及安全进行研究的课题，正在制定的标准有:《云计算安全及标准研究报告 V1.0》、《政府部门云计算安全》、《基于云计算的因特网数据中心安全指南》等。

2016 年 6 月 21 日在南京举办了一场专业会议—全国信息技术标准化技术委员会云计算标准工作组工业云标准编制会，为中国制造 2025 起到了添砖加瓦的作用。本次会议期间，来自全国的共计十余家单位的二十余位专家将对《工业云服务模型》（解决工业云的定义与范围）、《工业云服务能力总体要求》（解决通过工业云服务为智能制造提供业务支撑的问题）的标准内容进行讨论，并形成标准草案。除此之外，《工业云服务服务水平协议（SLA）规范》（解决工业云服务质量的

基本要素及其考核基本要求的问题)、《工业云服务计量规范》(解决工业云服务使用量的计量问题)标准也正在同步编制中，标准草案预计年内形成。

2016 年 8 月 23 日，全国信息技术标准化技术委员会云计算标准工作组工业云标准编制会在拉萨召开，工业云实际上是利用网络和云计算将资源和能力进行扁平化配置的一种工业化的载体工具，进而可实现经济安全高效和可持续性发展。

云安全技术在工业领域的应用将成为未来几年国家标准化组织关注的热点。我国有着与国际同步的标准研究基础和机遇，通过对国内外云安全标准研究现状的分析，我们可以发现无论国内还是国际，云安全标准的研制还有好多工作要做，对此给出了一些思考和建议。

3 工业云安全防护方案

3.1 工业云安全总体方案

当前的信息安全处于持续攻击的时代，需要完成对安全思维的根本性切换，即应该充分意识到安全防护是一项持续的处理过程。从“应急响应”到“持续响应”，前者认为攻击是偶发的，一次性的事故；而后者则认为攻击是不间断的，不可能完全拦截的，系统应承认自己时刻处于被攻击中。由于工业系统的重要性，工业云可能会面临更多的威胁，与通常 IT 环境下的云相比，必须更加重视安全性和恢复能力。

工业互联网平台应在云基础设施、平台基础能力、基础应用能力的安全可信方面应制定五个基本计划活动：

（1）识别（Identify）：识别的管理系统，资产，数据和功能的安全风险。

（2）保护（Protect）：对平台实施安全保障措施，确保工业互联网平台能够提供服务。

（3）检测（Detect）：对平台使用、维护、管理过程实施适当的持续性监视和检测活动，以识别安全事件的发生。

（4）响应（Respond）：对平台使用、维护、管理过程制定和实施适当的应对计划，对检测到的安全事件采取行动。

（5）恢复（Recover）：对平台使用、维护、管理过程制定和实施适当的活动及维护恢复计划，以恢复由于安全事件而受损的任何能力或服务。

工业云安全总体设计如下图 8 所示：

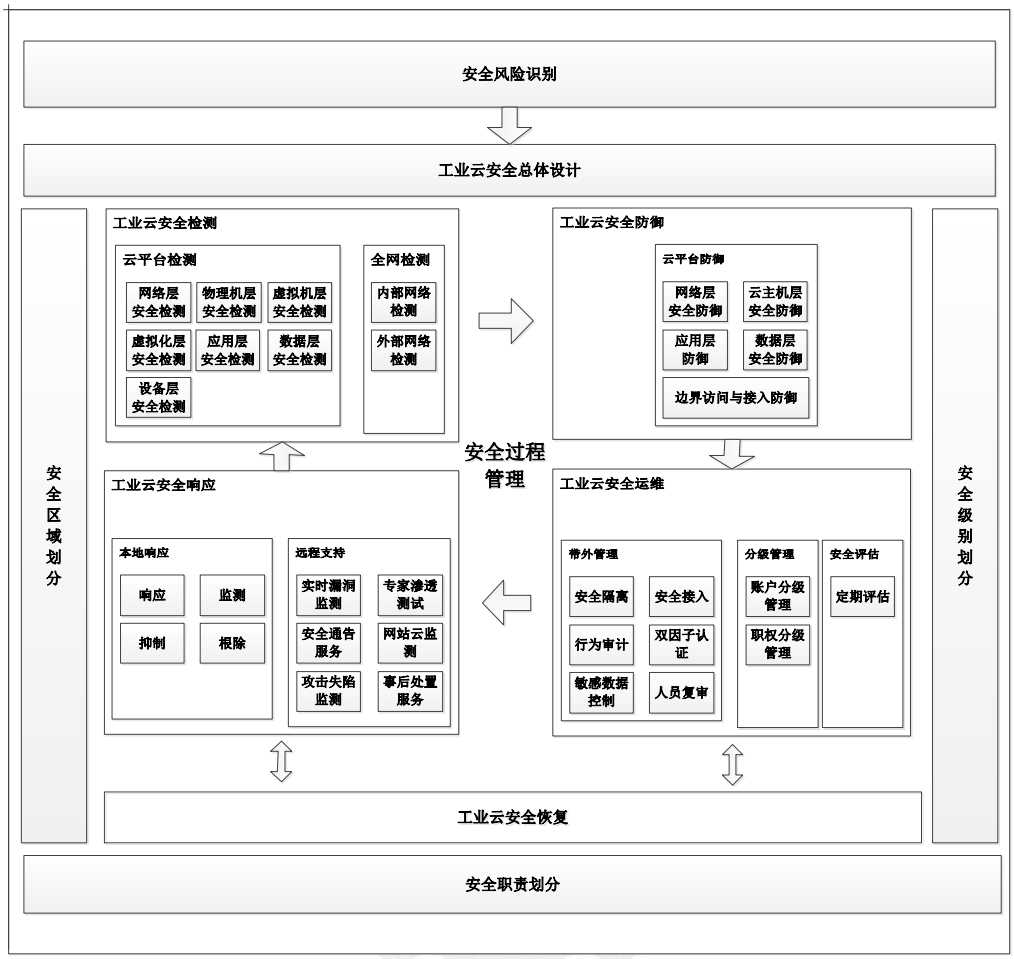

图 8 工业云安全防护方案

1）安全风险识别：安全风险识别是总体设计的基础，通过对整个系统进行详细分析，识别出各个部分的安全隐患，之后根据实际情况制定明确的设计方案。

2）安全职责划分：安全职责划分是整体方案的基础，需理清工业云各方安全责任边界对整个活动中的安全事件进行详细的责任划分设计。

3）分区分域设计：工业云平台环境相对复杂，涉及多类业务，多类系统，因此在安全防护上需要进一步细化安全域的划分以及不同安全域、不同安全级别的访问控制设计。

4）云安全防御：防御能力指一系列策略、产品和服务，可以用于防御攻击。这个方面的关键目标是通过减少被攻击面来提升攻击门槛，并在受影响前拦截攻击动作。

5）云安全检测：检测能力用于发现那些逃过防御网络的攻击，该方面的关键目标是降低威胁造成的“停摆时间”以及其他潜在的损失。检测能力非常关键，因为安全管理人员应该假设自己已处在被攻击状态中。

6）云安全运维与安全管理：实现安全运维操作的分级管理，对不同级别的用户予符合其安全

职责划分的操作或审计权限，实现安全运维。坚持日常安全运营与应急响应相结合，以数据为驱动力，以安全分析为工作重点。

7）云安全响应：响应能力用于高效调查和补救被检测分析所发现的安全问题，提供入侵取证分析和根本原因分析，并产生新的防护措施以避免未来出现安全事件。

8）云安全恢复：工业互联网云平台与通常 IT 环境下的云相比，更加重视恢复能力，一旦监测到系统遭受攻击，云安全响应中心应立即开启系统恢复功能，防止数据丢失，应用错误，减少对工业系统带来的损失。

3.2 工业云安全职责划分

3.2.1 工业云关键角色与职责划分

工业云运营中的关键角色包括如下：

云服务商：管理、运营、支撑云计算的计算基础设施、软件、与工业云链接的设备，通过网络将云计算的资源，工业设备的生产能力交付给客户的运营商。

云安全服务商：为工业云提供安全服务的供应商。

云用户：使用工业云平台资源的工业企业或者个人。

云监管方：工业云的监管单位。

关键角色的主要的职责如下：

云安全服务商应按照国家信息系统对云平台的信息安全要求进行安全防护，云服务商应积极配合安全服务商的安全工作。

为确保用户的数据和业务系统安全，云服务商和安全服务商应先通过安全审查，才能向用户提供云服务和安全服务。云服务商和安全服务商应积极配合监管方进行监管工作，对云服务商所提供的云计算服务进行安全监视，确保持续满足安全需求。

用户首先应当配合云服务商， 落实工业云安全规范。另外用户需承担部署或迁移到云计算平台上的数据和业务的最终安全责任；用户对云计算服务的运行进行监督和管理，根据相关规定开展信息安全检查。

监管方作为工业云的监管单位，负责安全建设项目和安全运营制度的审批，负责安全工作实施过程中的监督、协调与沟通。

3.2.2 工业云安全组织架构与职责

信息安全管理组织是确保落实工业云的信息安全决策、支撑信息安全工作开展的基础。在工

业云的信息安全建设过程中，信息安全制度规范的建立、日常安全管理、具体控制措施的贯彻执行、以及对信息安全管理方针贯彻落实情况的监督等工作的开展都需要一个完善有效的信息安全组织架构来支撑。信息安全管理组织建设的目的主要是通过构建和完善信息安全管理组织架构，明确不同安全角色的定位、职责以及相互关系，强化信息安全的专业化管理，实现对安全风险的有效控制。

初步建议工业云的信息安全管理组织架构如下图所示：

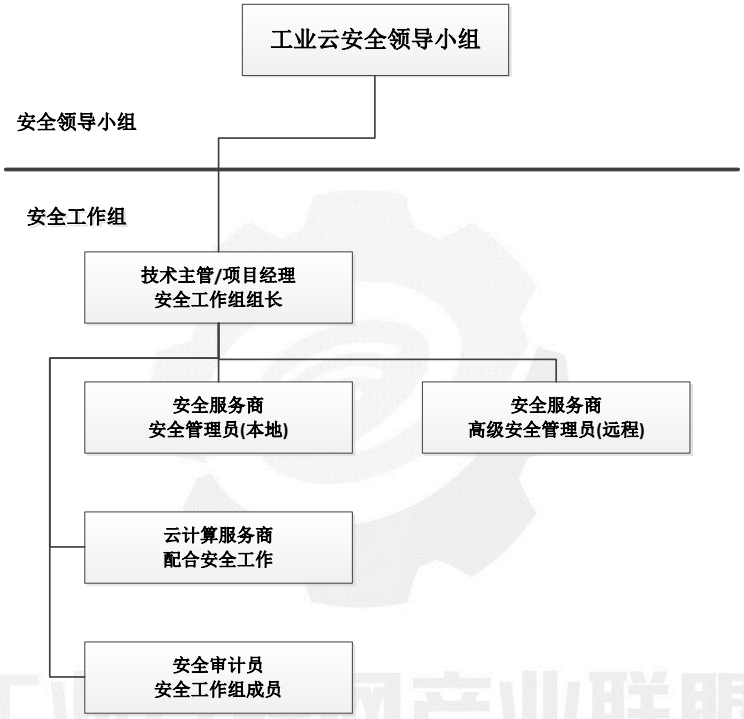

图 9 工业云的信息安全管理组织架构

其中：

安全领导小组：负责对工业云中信息安全工作进行监管。

安全工作组：由安全服务商本地驻场的安全工程师及负责远程联合响应的高级安全工程师、工业企业的用户的信息安全主管和运维人员、工业云计算中心工程师联合组成，负责日常具体安全工作的落实。同时，云计算服务商应指派运维工程师配合安全工作组的工作。

安全领导小组的主要职责如下：

a)确定工业云的信息安全建设与安全运营目标、原则和工作方法；

b)主管工业云的信息安全项目建设；

c)分配工业云的信息安全管理职责；

d)审批工业云的信息安全管理制度；

e)监管安全管理制度和安全工作的落实；

f)负责指挥、协调、督促、审查重大安全事件的处理，并监督整改措施的落实；

g)作为主管部门，负责安全服务参与方之间的沟通与协调；

h)负责检查和考核工业云的信息安全运营服务质量。

安全工作组负责日常具体安全工作的落实，主要职责包括：

a)制定工业云的信息安全管理制度和安全策略；

b)贯彻执行和解释安全领导小组批准的信息安全管理制度和安全策略；

c)指导租户落实安全策略和相关安全工作；

d)落实事前、事中、事后全流程中的信息安全各项工作，并对具体落实情况进行总结和汇报；

e)制定应急处置预案，并定期开展应急演练；

f)定期安排安全培训；

g)配合工业云租用单位的安全自查和安全等级测评工作。

安全工作组组长岗位

a)负责组织安全小组成员进行工业云的信息安全管理制度和安全策略的制定和维护，包括但不限于安全管理制度、安全策略实施规范、安全审计方案、应急处置预案，各系统安全加固基线手册等。

b)管理工业云日常信息安全运营工作；

c)检查和监督组员的日常工作情况，并及时指导改进；

d)定期组织开展应急演练、安全培训等项工作；

e)协助安全管理员处理日常的信息安全问题；

f)听取安全管理员的安全工作汇报，了解信息系统与网络的安全现状；

g)听取安全审计员的安全审计报告，督促各项信息安全制度和策略的落实和考核；

f)定期向安全领导小组汇报安全工作情况，在安全领导小组的指导下组织协调各方做好信息安全工作。

安全管理员(本地)

a)对工业云计算中心进行日常安全维护，进行日常监控、定期巡检、配置变更、故障处理等运维服务工作；

b)对各个租户在云主机上自主安装并运行的系统软件、数据库、中间件、应用系统软件等，安全管理员应负责进行安全扫描，并提交安全检查报告提交给租户和监管方；

c)实施相关的信息安全工作，承担日常安全巡检和日志分析、漏洞扫描和修复、安全加固等；

d)负责安全巡检，具体包括：对安全监测的结果进行审核确认，通过工具或人工方式检查各系统安全性，对各类设备的运行情况进行检查；

e)负责编写安全检测报告、信息系统安全优化方案等；

f)与云计算服务商共同实施云平台的安全加固工作，例如宿主机安全加固和云主机镜像安全加固；

g)辅助租户实施云主机的安全加固工作；

h)负责对云计算资源的操作行为进行安全审计；

i)负责工业云的安全预警分析，具体工作包括：综合分析安全监控和安全巡检的结果，结合告警策略，提出预警报告；搜集设备厂商、安全组织、安全服务商的安全预警信息。

j)负责保障工业云的业务连续性工作，具体工作包括：参与制定应急预案、定期进行应急演练、培训，以及根据应急预案对发生的安全事件及时处置。

安全管理员(远程)

a)重大安全事件的联合应急响应；

b)重要时期的信息安全实时监控；

c)定制并下发威胁情报和安全通告；

d)对本地安全管理员的技术支持。

安全管理员(工业企业租户)

a)负责本单位业务系统接入工业云的过程中与信息安全相关的配置、联调、测试等工作；

b)负责按照工业云安全策略，对本单位租用的云计算资源进行安全策略配置、安全检测与加固，例如云主机漏洞扫描及安全加固、云主机病毒防护等；

c)负责云主机上自主安装并运行的系统软件、数据库、应用系统软件、业务数据等的安全监控与防护；

d)遵照工业云安全管理制度和安全策略，规范本单位网络内对云主机的访问和配置操作；

e)负责本单位内部网络与信息安全、应用与业务数据安全的运维工作，包括日常监控、定期巡检、配置变更、安全事件处置等；

f)配合安全服务商及云计算服务商安全管理员的工作；

g)及时向监管方上报本单位系统内发生的安全事件及处理情况；

h)依据本单位和上级部门的规定，定期进行安全自检与安全等级测评，其间与安全服务商和

云计算服务商积极沟通；

i)积极参加应急响应演练、安全培训等。

安全审计员

a)负责安全管理员的操作行为进行审计、跟踪分析和监督检查。

b)负责网络安全审计系统的日常维护，对审计日志进行定期分析和事件记录。

c)发现安全管理员违规行为或是审计日志中的可疑问题，要及时将审计事件上报主管领导。

d)负责相关审计资料的记录、整理、归档等管理工作，配合安全管理部门和技术支持单位进行资料调阅。

e)负责定期向主管领导和系统安全保密管理机构进行审计报告。

f)负责与网络安全审计有关的其他工作。

3.3 工业云分区分域设计

3.3.1 总体安全域划分

安全域的划分需要考虑如下几个原则：

业务保障原则：安全域方法的根本目标是能够更好的保障网络上承载的业务。在保证安全的同时，还要保障业务的正常运行和运行效率。

结构简化原则：安全域划分的直接目的和效果是要将整个网络变的更简单，简单的网络结构便于设计防护体系。

等级保护原则：安全域划分和边界整合遵循业务系统等级保护要求，使具有相同等级保护要求的数据业务系统共享防护手段。

生命周期原则：对于安全域的划分和布防不仅仅要考虑静态设计，还要考虑云平台扩容及因业务运营而带来的变化，以及开发、测试及后期运维管理要求。

立体协防原则：安全域的主要对象是网络，但是围绕安全域的防护需要考虑在各个层次上立体防守，包括在物理链路、网络、主机系统、应用等层次。同时，在部署安全域防护体系的时候，要综合运用身份鉴别、访问控制、检测审计、链路冗余等各种安全功能实现协防。

结合以上原则及工业云安全实际情况，具体划分以下几个安全域。同一个安全域内可以根据实际需求进一步划分不同的子域：

图 10 工业云安全域划分

数据服务域：基于安全云平台集中工业云所有计算资源和数据资源，为整个工业云平台所有租户提供数据支撑服务和计算服务，具体包括计算应用资源和存储应用数据，是整个工业云平台的核心区域以及重点保护区域。

安全接入域：主要为数据服务域与制造资源域、终端用户域与数据服务域的数据交互提供可靠的安全接入。

运营管理域：主要为工业云网络提供运维管理服务和安全管理服务。

终端用户域：主要为整个工业云所有的租户。

设备资源域：主要为工业企业具备先进制造能力的设备

3.3.2 安全域边界防护

工业云安全在安全域边界防护上需要考虑如下因素：

1) 应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；
2) 应在网络边界部署访问控制设备，启用访问控制功能；
3) 应对进出网络的信息内容进行过滤，实现对应用层协议，工业协议命令级的控制；
4) 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；
5) 应在网络边界处对恶意代码进行检测和清除；
6) 应对通信过程中的整个报文或会话过程进行加密；

7) 应采用密码技术保证通信过程中数据的完整性；

8) 应确保与外部网络或信息系统的连接只能通过严格管理的接口进行，根据云服务商的安全架构，该接口上应部署有边界保护设备；

9) 应采取有关措施对所传输的信息流进行必要的保密性和完整性保护；

10) 应对所有的通信会话提供真实性保护，如防止中间人攻击、会话劫持。

11) 应对工业设备接入层设计专门的安全防护层，增加审计功能，防止工业设备被作为入侵工业云的跳板。

12) 应考虑使用 VPN 链接工业云，在工业云边界部署堡垒机。

13) 工业企业与工业云相连接，安全威胁较低，因此在边界主要通过防火墙进行边界防御，同时结合虚拟化安全平台的防病毒、入侵防御等功能进行立体防御。

14) 个人用户因业务需要与工业云进行互联，对安全级别要求较高，因此边界采用专有的安全隔离边界进行隔离和数据交换。

3.4 工业云安全检测

3.4.1 网络层安全检测

运维管理员可通过云安全管理平台虚拟网络可视化界面，实现对网络层进行安全检测。

云安全管理平台通过与云平台结合，生成虚拟机交换机流量镜像，利用这些数据可以提供云平台环境中虚拟网络的结构和变化，还可以通过这些数据制定态势感知系统，对攻击进行预警。

日常网络层安全检测包括:

网络拓扑的可视化

针对每个租户的网络形成一个图形结构，清晰的展示虚拟网络之间的关系，图中包括关键要素，如:虚拟机，虚拟网络，虚拟路由，虚拟防火墙等。

网络分析的可视化

能够针对特定的网络展示最新的网络流信息，能够及时反应网络节点，设备的被攻击情况，方便安全管理员第一时间处理。包括对网络层 SDN（Software Defined Network, SDN）设备的重要程序和配置信息进行完整性检测，能够发现变更并按照用户策略设置进行告警或其他处置

3.4.2 物理机层安全检测

运维管理员针对日常系统文件，可通过云安全管理平台核心文件完整性检测，及时的发现核心系统文件的变化，帮助管理员发现攻击者的入侵。

云安全管理平台使用预设的完整性检查规则可对文件和目录针对多方面的更改进行监控,包括：内容、属性（如所有者、权限和大小）以及日期与时间戳。完整性检查检测 Config 目录，保存的是需要监控的文件和目录。在运行完整性检测时，会生成新的签名信息，通过和基线数据库比较，找出被篡改的文件。

对物理机层设备或组件（包括软件、硬件和固件）进行完整性检测，对物理机层系统加载过程中的重要程序、文件和配置状态等进行完整性检测，能够发现变更并按照用户策略设置进行告警或其他处置。

核心文件签名扫描通过收集核心文件的版本，创建时间，文件大小，md5 等信息。帮助及时分辨出哪些文件被修改。同时还需要对主机的进程，内存，网络进行监控，时刻了解当前主机的运行状态。

3.4.3 虚拟化层安全检测

云安全运维管理员负责监控工业云平台中虚拟化层安全威胁，针对虚拟化层出现新的攻击层面，通过安全漏洞扫描工具，定时扫描发现虚拟化层漏洞并处理，避免因黑客攻击造成的虚拟机逃逸现象，针对突发漏洞情况，通过安全厂商提供工具进行防护。云安全管理平台虚拟化层漏洞扫描引擎通过虚拟化系统的符号特征、版本信息等条件匹配相应的平台漏洞，检测虚拟化漏洞信息。扫描完成后对所有的漏洞进行汇总分析，提供漏洞排名、漏洞分布情况、漏洞发生趋势等信息展示，并通过报表形式向管理员展示主机存在的系统脆弱性风险。

其中云安全管理平台针对宿主机层分析虚拟机的底层 I/O 操作，形成独有的安全基线行为准则，运维管理员无需配置，可直接通过云安全管理平台下发匹配任务，从而发现和拦截各种已知和未知的虚拟机逃逸攻击，并能对未知攻击进行溯源。对服务器进行免疫保护，免招病毒传染。

对于云平台中特殊文件与进程（包括误报、误删在内），统一通过云安全管理平台白名单进行控制。 云安全管理员在虚拟化层中安装驱动组件，在控制中心显示可被管理的主机数量。在宿主机列表中，选择被检测的物理主机，下发扫描任务。当扫描完成后，云安全管理中心显示发现漏洞，针对漏洞信息，安全管理员可以查看对应主机的漏洞信息详情。

对虚拟化层运行过程中重要程序(包括虚拟机监视器等)、文件和配置状态等进行完整性检测，能够发现变更并按照用户策略设置进行告警或其他处置。

3.4.4 虚拟机层安全检测

1）文件防病毒检测

对于日常云主机运行中病毒安全防护，由运维管理员配置实时防御策略。虚拟机开启实时防护后，进行主动防御，系统中进行每一个动作时（修改文件，启动进程，变更服务），主动防御模块都进行安全检查。可以有效避免常驻内存型病毒和服务型木马的攻击，还可以避免恶意黑客所利用 0day 漏洞进行的网络渗透和攻击。

2）云平台操作检测

云安全管理平台负责对日常操作进行行为监控，记录用户日常操作内容，提供操作记录查询。利用虚拟机操作审计可以帮安全管理员实现精细化的安全分析、降低人为安全风险，满足合规要求。

云平台安全监测包括：记录云平台中创建、迁移、删除云主机操作记录，云平台中添加、删除网络端口及存储配置。记录用户登录服务器的时间，登录的 IP,执行的程序，命令。通过对数据的裁剪，过滤，聚合，统计。云安全管理平台将直观展现，并给管理员建议判断用户的操作是否合规。

3）云平台 API 检测

运维管理员通过 API 监测获得关于云平台 API 调用的历史记录。包括通过云 web 管理平台、命令行工具进行的 API 调用。API 审计可以做资源变更追踪以及合规性检查。主要功能如下:

资源变更跟踪:

操作(创建、修改、删除)云主机 API 资源跟踪

操作(创建、修改、删除)浮动 IP 资源跟踪

操作(创建、修改、删除)镜像 API 资源跟踪

操作(创建、修改、删除)安全组 API 资源跟踪

操作(创建、修改、删除)块存储 API 资源跟踪

操作(创建、修改、删除)负载均衡 API 资源跟踪

操作(创建、修改、删除)工业应用软件 API 资源跟踪

通过备份链的形式，告诉管理员，资源在什么时候做了操作，资源变更一目了然。

资源合规性监测:

操作(创建、修改、删除)云主机 API 合规监测

操作(创建、修改、删除)浮动 IP 合规监测

操作(创建、修改、删除)镜像 API 合规监测

操作(创建、修改、删除)安全组 API 合规监测

操作(创建、修改、删除)块存储 API 合规监测

操作(创建、修改、删除)负载均衡 API 合规监测

操作(创建、修改、删除)工业应用软件 API 资源跟踪

4）虚拟机资源检测

云安全管理平台需要对虚拟机的资源使用情况进行监控，防止云资源被滥用，如 DDos 攻击等。对虚拟机的配置信息、镜像文件等数据进行完整性检测，能够发现变更并予以提示。

3.4.5 应用层安全检测

1）应用漏洞扫描

运维管理员需要对云主机的应用，进行定期安全扫描，并保存记录扫描报告。对于扫描所暴露漏洞，需要通过云平台管理软件或原厂商补丁进行修复，修复完成后，再次扫描并记录完成结果。

2）应用系统日志监测

运维管理员需实时针对应用系统日志进行观察，对于云安全管理平台提供的应用系统报警进行快速处理。应用程序的重要文件和配置参数等进行完整性检测，能够发现变更并予以提示。

3.4.6 数据层安全检测

对于云平台中敏感工业信息防泄漏，运维管理员需通过云安全管理平台进行实时监测。

云安全管理平台通过设备过滤驱动技术和文件级智能动态加解密技术进行数据安全监测。运维管理员首先在数据安全等级高的云主机中安装代理程序，代理程序中设备过滤驱动负责实现对终端设备的安全保护及控制。自动识别硬件信息、用户标识、存储设备与非存储设备、授权设备与非授权设备等信息。另外文件级过滤驱动可以实时拦截文件系统的读/写请求，对文件进行动态跟踪和透明加/解密处理。代理程序性能影响小，系统运行效率高；不改变原始文件的格式和状态。

3.4.7 设备层安全检测

1）防盗防毁

可以采用增加设备标识，锁定装置，监控报警三种方式

设备标识：通过硬件级部件（安全芯片或安全固件）方式对设备进行唯一身份标识，硬件安全部件颁发的证书可代表该设备身份，在其接入工业云平台时对其身份合法性进行检测，能够发现变更并予以提示。

锁定装置：通过使用粘性物质，锁头或者光纤电缆。

监控报警：监控报警时安全报警与设备监控的有效融合，监控报警系统包括安全报警和设备监控两个部分，一方面对设备进行实时监控，另一方面，当设备出现问题时，监控报警系统可以迅速发现问题，并及时通知负责人进行故障处理。

2）电源保护

电源是设备运行的基础，在电源保护上需要考虑使用 UPS，在选择 UPS 时，需要考虑这种 UPS 能否满足设备运行需求，同时还要考虑切换备用电源所需要的时间，是否有内装的电源调整器，是否有过高及过低电压保护等几个方面。

3）设备维护

对于设备要定期进行防护与保养，对于报废的设备也要正确处理和利用，如将设备进行地点转移也应该按照规定进行执行，以免由于疏忽造成数据的泄露和丢失。

3.4.8 全网检测

信息安全形势已经变得越发严峻，单独靠对自身环境的安全管控已经无法满足整体安全的需要。因此，需要建立专门的威胁情报系统，感知外部安全形势，感知来自国内外的最新安全威胁与隐患，这些外部的信息主要包括：

IP 黑名单

DNS 黑名单

恶意文件

恶意 URL

严重的漏洞通告

安全事故信息

恶意 APT 组织

网站安全事件

3.5 工业云安全防御

3.5.1 网络层安全防御

对于总体安全域划分中云平台部分,云安全管理端采用虚拟防火墙方式对安全边界进行划分。云安全管理平台虚拟防火墙与工业云平台 VPN 网络组划分功能互为补充。

对网络层 SDN（Software Defined Network, SDN）设备的安全启动、运行状态的完整性保护并支持远程验证的能力。同时，还应支持 SDN 控制流量的机密性保护和 SDN 业务流量的机密性保护。

从工业云服务器到应用单位实现端到端物理隔离，云平台中对云主机无需划分单独安全域；工业互联网中，汇集所有业务系统，需要进行访问策略限制。安全管理员与工业云运维人员首先根据实际环境建立不同安全组，并在安全组中定义各种访问规则，当云主机加入该安全组后，即受到这些访问规则的保护。

安全组规则支持入方向和出方向。对于入方向规则，限制源地址为安全组或者网段；对于出方向规则，限制目的地址为安全组或网段需要绑定弹性 IP 并设定相应规则方可通信。

另外网站层安全防御中考虑如下几种攻击:

1） 暴力破解

2） Ddos 攻击

3） ARP 攻击

4） CC 攻击

5） 远程登入非法探测

3.5.2 物理机层安全防御

应支持硬件级部件（安全芯片或安全固件）作为系统信任根，建立从系统到应用的信任链，实现从设备加电到应用加载过程的安全启动，以及基于硬件级的重要程序或文件的完整性保护。

3.5.3 云主机层安全防御

1）防病毒安全

运维管理员登录云安全管理平台配置本单位云主机的病毒扫描策略，并通过定期扫描和实时防护两种方式进行病毒安全扫描，根据结果，进行病毒杀除和文件修复。

2）账户安全

账号作为主机的入口，需要保证身份唯一标识、密码的安全性（口令复杂性、定期更换等）及账号的生命周期管理，防止暴力破解、未知账号等风险。

云安全管理平台通过控制用户密码输入重试次数，当达到限制则自动锁定用户一段时间，防止对主机账号密码的暴力破解。建立用户密码增强策略，控制密码最小长度、密码复杂度（要求必须由大写字母、小写字母、数字、特殊字符等字符进行组合）要求。当账号长期未使用，则锁定用户，可由云平台管理员进行解锁，Linux 默认无密码使用时长限制，为降低密码暴力破解的可能性，应保持定期更换口令，在账号密码长期未修改，则锁定用户，可由管理员进行解锁。

运维管理员按时对云平台中云主机账号，进行日常审计维护，主要是帮助管理员检测用户账号策略是否合规，可配置检查策略如下：

用户登录审计：记录所有的登陆事件，包括登陆 IP,用户名,登陆是否成功等信息。系统审计所有的异地登陆，暴力破解等行为。

用户账号创建、权限变更审计：记录所有账号创建，权限变更的事件。包括新账号的用户名，权限等信息。系统审计所有的 webshell 提权行为

活跃的 Root 账号：系统创建后，就不应该再用 root 用户登陆。

长期没人使用的账号：对于这种账号要定期删除

长期没有修改的密码：对于这种密码要提示进行修改

3）漏洞修复

运维管理员负责定期通过云安全管理平台对所管理平台内的云主机进行漏洞扫描及修复。扫描完成后，由云安全管理平台生成安全管理报告，进行漏洞修复后，需再次扫描并留存扫描结果。

针对特定时期或重大活动期间，由云安全运维管理员对全网云主机进行统一检查，并提前下发扫描通知。

4）漏洞防御

云安全运维管理员负责对全部工业云环境中的底层虚拟化安全进行安全监测，通过云安全管理平台对虚拟化层漏洞扫描完成后，云安全管理中心显示发现漏洞，云安全服务运维管理员首先查看对应主机的漏洞信息详情。

在发现漏洞后，由控制中心进行开启安全保护。采用虚拟补丁方式提供宿主机层系统修复，即在不重启云平台的情况下完成漏洞的防护。云安全管理端通过互联网更新云平台层漏洞信息，并向云平台推送官方的漏洞修复程序，对漏洞进行彻底修复。

对于 Hypervisor 层运行的可疑文件放到沙箱中评估其行为，阻断虚拟化漏洞利用程序，对脆弱点进行有效的防护。运维管理员进行安全扫描后，统一由云安全管理平台生成安全管理报告。

5）进程行为监控

通过对进程进行监控，可以更加主动的对恶意程序进行防护，防止一些恶意程序在运行期间做一些非法的行为。另外通过进程监控，可以更多的了解用户的进程状态，并保证一些关键的进程在运行期间不受攻击。

6）敏感文件操作

在工业系统中一些关键文件恶意修改可能直接影响工业生产，导致工业事故，通过对敏感文件进行监控和权限的设置，可以防止关键的文件或者数据被修改或者恶意利用。

7）远程异地登录

对于异地的远程登录进行监控和权限控制，防止攻击者登录后对系统一步攻击。

8）虚拟化层安全防御

虚拟化层应支持基于硬件级的安全启动，应支持对涉及到重要程序、重要文件和配置信息等进行基于硬件级的完整性保护，并支持远程验证能力。

9）虚拟机层安全防御

应对虚拟机的配置信息、镜像文件等信息，以及启动过程、运行过程和迁移过程进行基于硬件级的完整性保护。

3.5.4 应用层安全防御

运维管理员负责确保工业云平台在保护下不被入侵。云安全平台以图形化的方式展示,运维管理员可对历史攻击数据进行自定义查询和提取报告，通过互联网更新全球安全情报，第一时间做出与云平台相关的情报提醒，深度挖掘云平台安全漏洞。对云安全管控平台的专家级监控、巡检及应急响应服务,对新上线业务系统的安全评估、渗透测试及安全加固服务，并且在网站遇到问题时提供专家级的网站应急响应服务。

对当前的网站和服务器进行监控，实时监控当前网站的状况，并输出网站的探测时间、结果内容、发现问题监测点、持续时间等信息 ，在出现异常时做出及时的反应。

1） 本地防御虚拟集群

本地防御虚拟集群是指需在云平台中划分部分虚拟机资源,并将这些虚拟机资源集群化处理,部署防护软件。安全防护中心提供 DDoS 防护、CC 防护、漏洞攻击防护、SQL 注入防护、流量负载均衡等功能。当本地防御不足以应对大规模 DDoS 攻击时，可自动切换至云端防护。

2） 云端防御

云端防护与本地防护相同，区别在于可以提供更高的带宽进行流量攻击防御。

3.5.5 数据层安全防御

工业云数据安全主要考虑云上数据安全问题，工业云上数据可以分为结构化数据、非结构化数据形态、以及工业大数据平台内的混合型数据。

结构化数据主要是指工业云上各类门户网站数据、ERP 平台、OA 系统以及其他业务平台的关系型数据库中的结构化数据，主要威胁为攻击者针对业务平台或暴露在外的数据管理接口上的攻击，直接导致数据失窃；另外就是运维过程中运维人员直接对数据库的操作风险。

非结构化数据存在两种数据泄露途径，一是内部人员直接数据外发，二是攻击者直接获取系统控制权限后的数据窃取。

1）数据隔离与权限管理问题

针对大数据平台，主要面临的风险在数据平台上各组件的认证过程中存在越权、非授权访问的问题，导致直接获取大数据平台中的相关数据。

针对非结构化数据，如工业云平台上存在的文件、图表等非结构化数据，可以使用 DLP（数据防泄漏）方案来应对。在工业云平台上，需要特别针对网络流量及邮件数据进行数据防泄密监控。

针对结构化数据的防护主要从应用防护角度展开,主要是指针对云上业务平台的应用界面攻击例如注入、针对数据库的接口的攻击，防护能力由上述云安全保障部分防御能力来完成，主要涉及入侵防御系统或 WEB 应用安全网关。

面对认证、授权、审计三个数据安全核心问题，数据安全管理系统面向大数据基础平台，兼容各主流大数据平台的版本。为不同角色用户提供快捷服务的门户系统，其核心的基础就是用户身份的管控，包括用户管理、机构管理、角色管理、权限管理、操作行为管控、统一用户信息管理这几个部分，即通常所说的三个统一：统一认证管理、统一授权管理和统一安全审计。

工业云平台建设过程中通常会涉及不同级别的网络间的数据交换,如互联网区域和企业外网

区域，采用数据交换平台，可以实现异构数据间的安全可信交换。

各业务平台的非授权或是越权使用，也是数据泄露的重要途径，可以通过系统日志、网络日志、业务日志、运维审计（堡垒机）等方式采集各类业务操作数据，基于业务操作数据的分析，可以发现工业云上违规操作、恶意操作行为，从业务审计自身的角度解决数据安全的问题。

云数据安全还需要采用安全评估的方法，针对云上业务的互访关系、数据的分类分级等进行评估，找出各类数据传递过程中的可能存在的安全威胁，再使用前面提到的各类安全技术措施，采用适当的安全策略，才能达到有效的针对数据安全的防护能力的落地。

工业云上主要承载各类生产业务应用，以上针对数据、管理、保障的防护方案主要针对云上的业务安全需求展开。工业云的使用除了互联网区域的对公业务外，还有很多应用是针对于生产活动，使用各类终端的接入来进行生产业务的操作、数据的传递，在这个过程中，如果对于接入的终端控制不严格，会导致恶意代码对生产应用的影响、敏感数据非受控传输等。

2）数据加密

在工业云上对数据进行加密尤其重要，特别是对于一些机密的数据一定要考虑使用加密手段，另外就是对密钥进行管理。

加密主要三种实现方法是：硬件加密；软件加密合网络加密

硬件加密指通过专用加密芯片或独立的处理芯片等实现加密运算；软件加密指使用相应的加解密软件实现加解密操作；网络加密指不使用本机的软硬件进行加密，而由基于网络的其他计算机或设备来完成加解密或验证工作。

3）数据备份

在数据安全问题上另外一个问题就是数据的丢失，通常导致数据丢失的原因包含如下几个方面：

数据处理和访问软件平台故障

操作系统的设计漏洞或设计者出于不可告人的目的而人为预置的黑洞

系统的硬件故障

人为的操作失误

网络内非法访问者的恶意破坏

网络供电系统故障

解决数据丢失的一个出来办法就是对数据进行备份，尤其是一些重要的数据。

3.5.6 边界访问与接入防御

重点关注对云平台接入边界的网络流量中攻击数据的控制、检测；在工业云出口，关注恶意代码、入侵攻击、信息窃取、拒绝服务等攻击行为的发生，需要针对于工业云上的业务系统提供相应的防护能力。

针对云上的业务防护，采用软件定义安全框架来实现云环境下基础安全能力的部署并借助虚拟化的优势实现自适应的安全体系架构，可以实现云上的安全能力根据业务安全需求进行动态调整，实现更加智能化的安全。

通过云安全管理平台完成各类云上安全信息如日志、攻击数据、漏洞数据、情报数据、流量数据等内容的集中采集，然后采用大数据分析技术，对各类数据进行如关联分析、聚类挖掘，依据前期设定的场景规则，匹配驱动流平台和安全资源池的调度，以实现根据不同安全场景进行安全能力的调整，实现自适应的安全体系架构。

工业云安全接入主要包含三个方向的内容:

1）针对于移动端的安全，主要涉及生产应用移动终端的管控，如移动执法、移动办公的手机、平板电脑等，需要对移动端进行统一的设备管理、应用管理，以及文件的数据落地管理，保障移动端的应用、数据的安全可控。

2）桌面操作终端，主要实现对终端层面的恶意代码防护、终端 DLP、终端行为管理等能力，保证接入工业云的桌面终端的安全可控。

3）工业云设备接入，主要涉及工业云设备身份的鉴定，权限的控制，和数据的可靠性，保证接入工业云的设备是合法的。

4）无论是移动端，桌面端，还是工业云设备的接入，需要采用统一的认证、可靠的方式，限定非认证的终端不允许接入云端。同时，对于终端到工业云的数据连接，采用有效的加密通讯过程。

接入工业云平台的终端或设备，应支持以硬件级部件（安全芯片或安全固件）作为系统信任根，为工业云平台的机密性和完整性保护提供支持；支持基于硬件级部件的唯一标识符，硬件安全部件颁发的证书可代表该设备身份，为工业云平台及上层应用提供拥有硬件标识的身份证书的能力；支持安全启动的能力。

3.6 工业云安全运维

3.6.1 带外管理模式

工业企业用户远程访问堡垒机，通过堡垒机及配套的短信认证网关进行身份认证，堡垒机对于用户的 RDP、SSH 等管理协议进行实时录屏，同时由边界防火墙进行基础的访问控制，防止各工业企业用户安全管理员跳过堡垒机直接对服务器进行管理。当用户需要通过工业云平台对虚拟机进行深层次管理时，则通过安全网关访问工业云平台，通过分配的账号进行管理。

工业企业用户共用一个带外管理域，其中包含工业云平台管理系统、带外管理的堡垒机、APT 威胁感知分析平台、下一代安全管理平台等，将带外管理平台与业务网分割，提高数据通信效率和安全性。

带外管理平台采用了安全隔离技术、数据摆渡技术、网络行为审计技术等技术。可以全程记录现场运维人员对运维设备的操作行为，用于事前警示与事后定责。通过带外管理管理平台，避免运维设备自身感染的恶意代码扩散到脆弱的业务系统。通过这种带外的远程管理让用户可以随时操作这台服务器，只要被控制的服务器无硬件故障，管理员就不必亲临现场，通过远程控制就能实现对服务器的管理和使用，就如果直接面对服务器一样。

3.6.2 分级管理模式

为加强工业云平台信息及网络安全与保密管理，避免操作权限失控,并防止一些用户利用非法取得的权限进行不正确的活动，云安全管理平台针对日常云安全相关操作制定操作权限分级管理设计。

云安全管理平台通过权限设置模块，支持建立五级管理管理账户，可以为操作人员按照功能点配置是否有进入功能点的权限。现有阶段使用三级账户管理对相关人员的角色来划分权限的，整体分级对应表如下:

管理员（分级）	管理对象	管理权限
安全管理员（云平台）	管理整个工业云平台，包括所有用户云主机，应用，云平台边界安全等。	最高管理员权限：添加、编辑、删除云安全平台策略
安全管理员（工业企业用户）	管理本租户单位内的所有云主机	普通管理员权限：添加、编辑、删除租户平台内的安全策略

个人租户	管理的个人云主机	普通用户权限：支持对本台云主机的安全策略操作

3.7 工业云安全响应

3.7.1 重点工作内容

工业云响应方案的重点工作内容主要是处理下列的突发信息安全事件：

(1)用户业务系统的服务异常事件

(2)网页信息篡改事件

(3)云平台内宿主机/云主机/终端后门发现事件

(4)病毒爆发事件

(5)网络攻击事件

(6)zero-day 漏洞安全事件

(7)工业设备使用异常

应急响应处理流程主要分为响应、检测、抑制、根除和恢复五个阶段。

1) 响应阶段

在实施应急响应工作前，当安全管理员收到用户的申请应急响应支持，由安全管理员第一时间与其取得联系，了解事件发生情况，判断事件类型，并与其确认是否需要启用应急响应服务。当安全管理员自己收到云安全监测中心的安全告警或人工发现系统异常时，则做相关记录后直接进入下一工作阶段。

2) 检测阶段

启用应急响应服务后，安全管理员在现场进行信息收集，使用检测搜集流量信息、检测搜集系统信息及主机检测等多种技术手段对事件进行详细分析，并查找入侵痕迹。最后确定安全事件类型，评估安全事件的影响。必要情况下，安全服务商的本地安全管理员应及时与远程的高级安全管理员取得联系，取得远程联动响应的支持；并及时联系用户和云计算服务商的工业云运维人员，以便协同处理安全事件。

3) 抑制阶段

安全管理员及时采取行动限制事件扩散和影响的范围，限制潜在的损失与破坏，同时由用户与相关系统负责人沟通，确保抑制方法对涉及相关业务影响最小。

抑制阶段通常采用的技术手段如下：

- 确定受害系统的范围后，将被害系统和正常的系统进行隔离，断开或暂时关闭被攻击的系统，使攻击停止；
- 持续监视系统和网络活动，记录异常流量的远程 IP、域名、端口；
- 停止或删除系统非正常账号，隐藏账号，更改口令，加强口令的安全级别；
- 挂起或结束未被授权的、可疑的应用程序和进程；
- 关闭存在的非法服务和不必要的服务；
- 使用反病毒软件或其他安全工具检查文件，扫描硬盘上所有的文件，隔离或清除病毒、木马、蠕虫、后门等可疑文件。

4) 根除阶段

在安全服务商安全管理员的辅助下，用户应检查所有受影响的系统。在准确判断安全事件原因的基础上，安全工作小组讨论并提出基于安全事件整体安全解决方案，排除系统安全风险。

5) 恢复阶段

安全工作小组（安全服务商、租户、云平台服务商协同）恢复安全事件所涉及到的系统，并还原到正常状态，使业务能够正常进行。恢复工作时应避免出现误操作导致数据的丢失。

针对每次安全事件输出《应急响应报告》。

3.7.2 安全应急流程

1）内网渗透事件

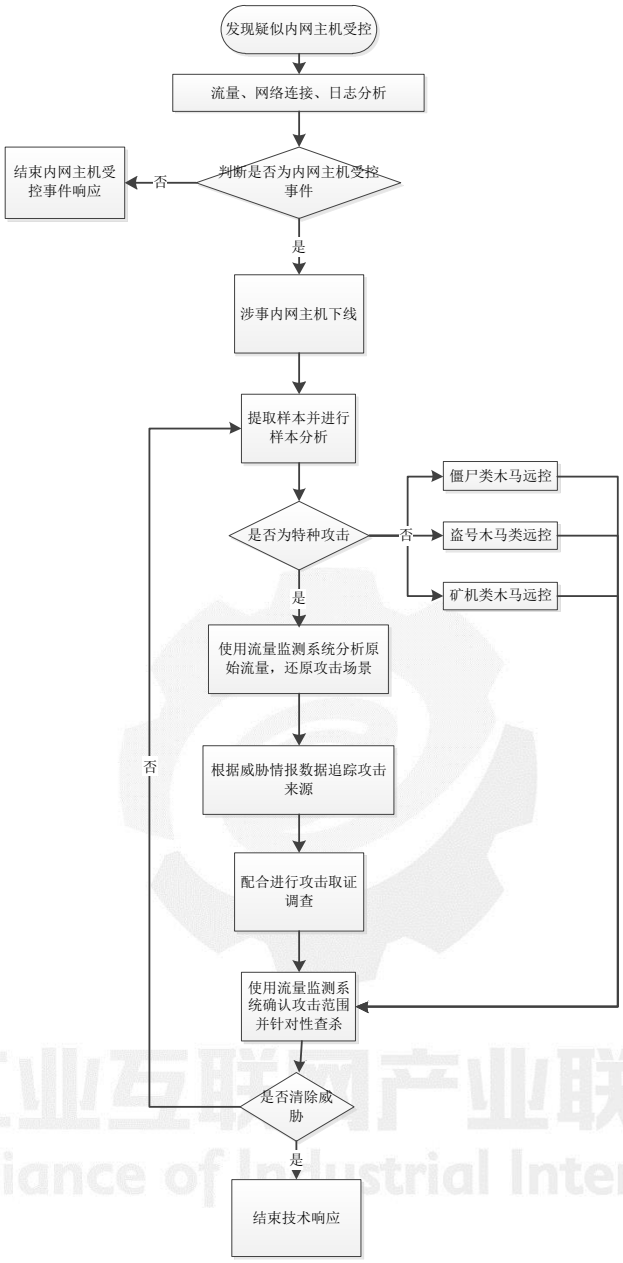

图 11 内网渗透事件处理流程

1. 通过日常的日志监测告警、流量监测告警或威胁情报发现内网主机受控事件；
2. 对涉事内网主机进行下线操作，防止持续遭受到攻击者控制造成敏感的信息外泄；
3. 提取涉事内网主机中的恶意代码病毒并进行分析，针对非特种攻击可通过防恶意代码软件进行分析鉴定，并通过流量监测系统确定其攻击影响范围并进行查杀，最终输出响应报告；
4. 针对特种攻击的样本需进行深入分析，判断其是否有针对性及目的性的攻击行为，通过流量监测系统对原始流量进行分析还原攻击场景，对木马的敏感操作行为进行识别，最后确定影响范围并查杀；

5. 参考威胁情报数据跟踪攻击来源，并对涉事内部主机进行取证调查；最后输出响应报告。

2）应用入侵事件

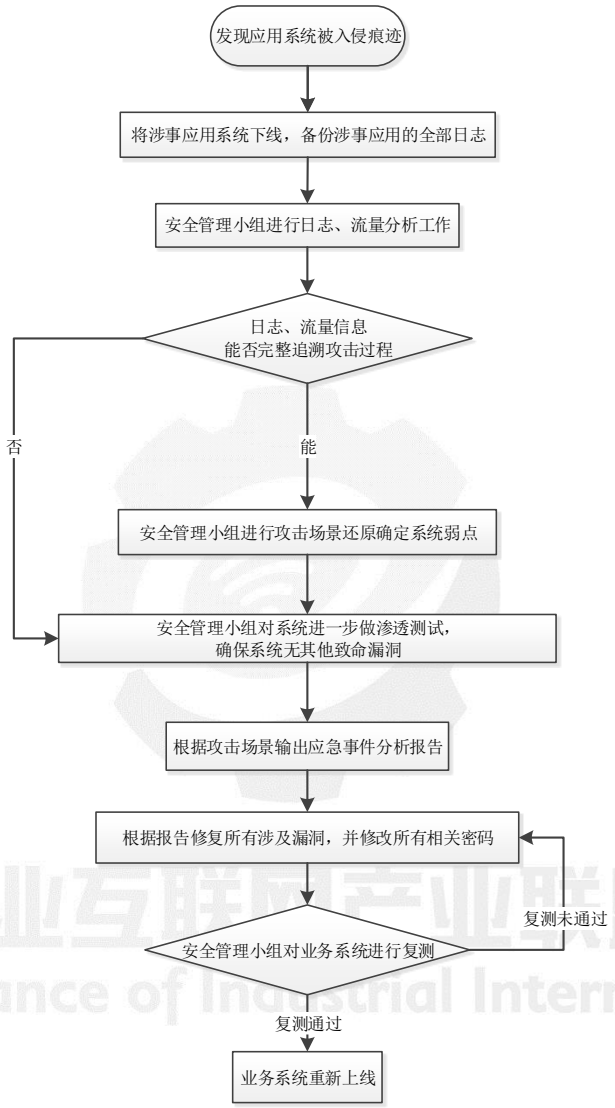

图 12 应用入侵事件处理流程

1. 通过日常的日志监测告警、流量监测告警或威胁情报发现应用系统入侵事件；
2. 针对涉事应用系统应及时进行下线处理并保护当前应用系统自身文件、内存、网络连接等信息，防止应用系统遭受到未预期破坏；
3. 响应小组提取涉事系统相关日志（如有日志服务器应从日志服务器中进行提取）及流量信息，通过对日志记录及流量信息的综合分析，确定可疑的攻击行为，并尝试还原攻击现场以确定系统当前所存在的弱点；当无法确定攻击路径时，应采取渗透测试方式主动发现涉事应用系统当前所存在的安全漏洞；
4. 根据分析结果总结本次应急响应的结果，并记录关键的证据信息，形成应急事件的分析

报告；

5. 根据分析报告，对应用系统当前所发现的弱点进行修复，应用系统重新上线运行并对该应用系统后续运行情况进行重点关注。

3.8 工业云安全恢复

云平台恢复是指：制定和实施适当的活动，去维护恢复计划以及恢复由于安全事件而受损的任何能力或服务。

3.8.1 恢复能力

弹性是一个云系统的新出现的特性，它在完成所分配的任务时，应避免，吸收和管理这些动态不利的条件，并重建其操作能力在收到干扰之后。通常，通过设计系统来实现恢复能力，使得故障被划分。 如果单个函数失败，它不应该导致其他函数失败，并且应该有可选择的方式去执行失败的函数在设计中，设计可以自动，立即和可靠地调用。对于元素及其之间的相互连接，保持恢复能力增加了物理或逻辑冗余，并在需要时提供可选择的元素和连接进行调用。 应该对正常和异常情况进行测试，并检查攻击者是否可以故意中断组件的联系。

软件还必须能够转移到可能具有不同弱点的替代功能，实施，配置，位置或网段，因此相同的威胁和危害不会对替换能力也造成破坏。

工业互联网云平台在各个阶段，各个位置都是有可能被攻破的，因此需要定制各个位置，各个阶段在出现破坏后的所具备的恢复能力。

3.8.2 云平台智能恢复

通过云平台智能恢复程序，可以尽快的完成恢复工作，减少在恢复过程中出现的错误，避免了二次异常。同时也能够使系统尽快的恢复到正常状态，减少了工业云异常所造成的影响和损失。

3.9 工业云安全过程管理

安全运营管理主要是对工业云提供日常的运行保障，其主要工作是通过安全事件管理、环境和资产管理、可移动介质管理、网络和系统管理、恶意代码及移动代码防护管理、变更管理、密码密钥管理、补丁管理、安全监控管理、日志安全管理加强日常各个环节的管理和控制，其目的是通过这些环节的日常安全工作，提高整体安全运营水平。

3.9.1 安全事件管理

信息安全事件管理分为四个组成部分，包括事件的定义与分类、报告和处理、分析与总结、定性及责任认定部分。信息安全事件定级应参照事件的定级表对事件经行分类和定级；事件定级后应对事件进行报告与处理，对于重大级别的安全事件处理程序需依据应急管理规定进行；事故处理完成后应急时组织和调查，分析事故的原因，启动事故责任界定流程，确定事故的责任，事故责任单位负责落实整改。

3.9.2 环境和资产管理

信息资产的管理工作包括信息资产分类、定级与标识、信息资产的使用和管理、信息资产的保密等工作。信息资产分类应根据信息资产分类表进行分类；信息资产应根据敏感性划分级别，敏感性各级别应按照安全保障级别划分；划分各类信息资产时应严格遵守相关规定，保证资产安全；应对不同信息资产的保密要求设置不同的保密期限。

3.9.3 网络和系统管理

网络和系统管理包括配置管理、性能管理、故障管理、日志管理、安全管理等工作；配置管理包括规划、建设、变更、发布、配置管理数据库更新等；性能管理主要包括容量、服务级别、服务可用性服务连续性等；故障管理主要包括监控、预警、问题管理、应急响应、故障报告制度等；日志管理包括日志记录、日志查看、日志保存、日志销毁管理等；安全管理包括控制和服务管理等。

3.9.4 可移动介质管理

可移动介质管理包括介质的配发、日常使用、保管、介质数据清除、介质数据销毁等工作；介质配发包括领取、登记、配发的管理工作；日常使用应指明介质的使用范围，复制数据时应准守的规定；介质保管应遵照保密性保管要求；介质数据清除应明确数据的清除条件，指明不同类型的介质采用的清除手段；介质销毁应规定介质的销毁条件、销毁流程、销毁方式等。

3.9.5 恶意代码防护管理

恶意代码防护管理包括病毒分类、防病毒软件的部署、终端防病毒管理、服务器防病毒管理、病毒应急处理、病毒事件报告等部分；应干根据病毒危险类型形成分类，根据分类制定病毒通告级别；防病毒软件的部署应根据防病毒设计体系进行；终端和服务器防病毒应设置相应的防病毒

策略；当发生病毒感染事件是应按照相关的流程规范进行处置；应对病毒入侵进行报告，报告包括问题时间、受感染范围、具体处理细则、问题解决时间、改进建议等。

3.9.6 变更管理

变更管理包括变更申请、变更测试与风险评估、变更上线的审批与执行、变更后续工作等；变更申请应说明变更原因；应根据变更申请制定测试方案和技术方案，技术方案包括变更目的、变更参与人员、涉及系统、实施详细方案、测试方案及前期测试报告、回退和应急方案、风险评估和通知文档等；变更上线的审批与执行包括提交变更上线会签材料的提交与审批，对变更操作进行现在审核并记录，变更实施失败后要实行回退方案；应对变更完成后各项异常情况准备好应急方案，同时归档整理变更材料。

3.9.7 补丁管理

补丁管理包括补丁的跟踪与分析、测试与分发、补丁的疑难解决和检查；补丁的跟踪与分析应对最新安全补丁进行跟踪，同时对补丁对应的漏洞严重程度进行分类；补丁分发前应遵照进行严格的测试流程进行测试，分发时应制定分发方案；对于补丁测试过程中出现的问题，应该尽快进行总结并制定 FAQ 并发布。

3.9.8 安全监控管理

安全监控管理包括监控分类、监控原则、监控策略、监控策略的实施等；应根据监控对象、监控内容对监控进行分类；应遵循监控的有效性、可靠性、可行性开放性等原则进行监控；应制定机房环境、设备硬件、程序及进程、网络及安全设备的监控策略；监控策略实施时应制定监控方案，方案包括监控内容、监控对象、监控工具、监控方法、监控阀值、监控周期、验证方法等内容。

3.9.9 日志管理

日志管理工作包括日志记录、日志的管理、日志的保护等工作；日志记录是指应建立适当的日志审核策略；日志管理应对日志记录的内容进行分析，编写日志分析报告等；日志保护是应对日志的完整性和可用性进行保护，制定适当的保护策略。

4 工业云安全发展与展望

工业云不仅能够解决或缓解工业领域过去面临的痛点，也能够在未来为大家在工业领域带来更多展望。在国家政策大力支持下，工业云应用成为工业发展的大势所趋，工业云平台将在以下领域持续发挥更大的作用：

1）资源的利用

工业云使各种资源和业务能力得到集中并池化，为优化分配、充分利用提供了基础。工业云的建设和完善，实现对存储资源、计算资源、数据资源、生产资源等各类资源的集中管理。同时将资金流、信息流、物流、服务流统一构成制造资源和制造能力池。

2）能力的开放

未来研发设计、数据管理、工程服务等制造企业资源将在工业云平台上充分共享，特别是随着行业标准化的完善。中小企业能够以较低成本，获取以往需要大量投入才能获取的各种资源和能力。根据统计，我国中小企业总数已达 7000 万，占企业总数的 99%以上，同时贡献着 50%的税收，60%的国内生产总值(GDP)、70% 的发明专利、80%的就业岗位，是国民经济的重要组成部分。但是，中小企业普遍存在着研发能力弱、市场拓展能力不足、资金和人才短缺、管理不规范等普遍问题，这在很大程度上阻碍了企业发展。工业云旨在解决中小型工业企业的困难，提升其创新能力的功能，在工业软件及平台搭建、计算机建模和仿真、研发人员培养等诸多方面向中小型工业企业倾斜，降低中小型工业企业的设计与制造成本、缩短企业产品升级换代周期、提高产品性能，为中小型工业企业的信息化能力、自主创新效率、核心竞争优势的提升提供帮助。

3）互连与集成

工业云不是各自孤立的平台，而是工业与各行业、技术领域的充分连接的渠道。工业云将资源、能力、服务汇集并有机结合，打破了传统工业企业间的基础技术能力与信息壁垒。提升工业企业整体的产品与服务能力。各工业云平台间也将通过互连实现充分的信息共享，宏观上构筑工业领域整体的信息化格局，结合信息安全方面的协同防护，面向用户在业务上提供专业、广泛、协同、安全的服务。

4）新技术融合

工业云将与人工智能、数字孪生、虚拟现实、增强现实、区块链、物联网、软件定义等方面充分结合，使工业整体上实现快速更新升级。工业云平台作为大数据处理的基础设施，能够使人工智能在工业领域得到快速发展。提高资源分配效率、优化生产过程并提升决策能力。工业，极大地改善了体力劳动的生产效率。工业云，与人工智能的结合也将使人类从大量重复的简单脑力

劳动中解放出来。工业云在未来的发展中，将进一步与云计算、物联网、工业大数据挖掘等新一代信息技术融合，深化在工业研发设计、生产制造、市场营销、售后服务等产品全生命周期、产业链全流程各环节的应用。使新技术在工业领域得到普遍应用，迎来工业领域的全面升级。

工业云改善工业，工业服务一切。工业云将依托工业体系在各个领域的影响，为社会发展、人民生活提供有力的支持。

可以看出工业云在未来将会越来越发挥重要的作用，更多的工业企业将依赖工业云，但随着工业云的发展，越来越多新的安全问题将会出现，在工业云的安全防护上也应该采用更多新的思路：

1） 纵深防御

纵深防御是经典信息安全防御体系在新 IT 架构变革下的必然发展趋势。原有的可信边界日益削弱、攻击平面也在增多，过去的单层防御已经难以维系，而纵深防御体系能大大增强信息安全的防护能力。纵深防御两个主要特性是多点联动防御和入侵容忍技术：

多点联动防御：在过去的安全体系，每个安全节点各自为战，没有实质性的联动。而如果这些安全环节能协同作战、互补不足，则会带来更好的防御效果。例如 FireWall、IDS/IPS、WAF、UTM、SIEM 等之间的有机联动，可以更加准确的锁定入侵者。

入侵容忍技术：我们假设虚拟逃逸是存在的。因此我们的设计原则是：即使攻击者控制了某些点，我们会通过安全设计手段避免攻击者进一步攻击其他点。

2） 软件定义安全

软件定义安全是一种应用信息安全的设计理念，是一种架构思想，这种思想可以落地为具体的架构设计。基于软件定义安全的设计理念，用户的意志最重要，传统安全设备厂商按照约定的软件定义安全规范提供细分领域的专业安全设备，用户通过 API 级的互动，深度整合这些安全设备形成一个有机的整体，提升了整体安全性。

3） 安全设备虚拟化

安全设备虚拟化是安全硬件的软化(例如 Hypervisor 化、或 container 化、或进程化)，也即利用各种不同的虚拟化技术，借助云平台上标准的计算单元创造一个安全设备。安全设备虚拟化带来的好处是大大降低了成本、同时提高了敏捷度、降低了成本、甚至提高了并发性能。但我们也要认识到，和硬件安全设备相比，安全设备虚拟化增加了攻击平面、降低了可信边界，需要我们小心翼翼的设计安全设备虚拟化的整个技术架构、在全生命周期中谨慎管理虚拟化安全设备，以避免带来新的威胁。

3) 用户与实体行为分析

用户与实体行为分析(User and Entity Behavior Analytics,以下简称 UEBA)会从网络设备、系统、应用、数据库和用户处收集数据。利用这些数据，可以创建一条基线以确定各种不同情况下的正常状态是什么。

一旦基准线建立，UEBA 解决方案会跟进聚合数据，寻找被认为是非正常的模式。这一确定过程仅评估新事件在上下文环境中是否不正常，以及不正常的程度有多深，并排序事件的重要性及可能的业务影响。用户行为分析管理员也可以创建自定义规则来定制解决方案，以便更贴合公司及其特定服务、数据和过程的需求。

UEBA 平台非常有前景。在不远的将来，可以预期用户行为分析平台会更直接地集成到基础设施中，并进行自动化响应。我们已经在见证防火墙和其他网络设备被配置为纳入用户行为分析驱动的情报并立即创建新的流量规则，在安全人才注意到之前就将入侵威胁挡在门外。

联系我们

工业互联网产业联盟 秘书处

地址：北京市海淀区花园北路52号，100191

电话：010-62305887

邮箱：aii@caict.ac.cn

网址：http://www.aii-alliance.org