安全+
SECURITY
2024/10 总第 062
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

车联网安全技术现状、突破及趋势

持续威胁暴露管理（CTEM）在国内落地，要避免“水土不服”

技术与威胁交织：大模型在网络安全中的光与影

揭开IEC 62443系列标准的神秘面纱

NSFOCUS

SECURITY

安全+ 技术版
与安全人士分享技术心得
Share technique experience with security professionals

本期看点 HEADLINES

主办：绿盟科技
策划：《安全+》编委会
地址：北京市海淀区北洼路4号院绿盟科技园
邮编：100089
电话：(010)6843 8880-5462
传真：(010)6872 8708
网址：www.nsfocus.com

2024/10 总第 062

安全+ SECURITY

欢迎您来信nsmagazine@nsfocus.com与我们交流，分享您的建议和评论。（《安全+》部分图片来源于网络）

目录 CONTENTS

网络安全领域持续革新，安全新威胁不断涌现，网络安全新形势下，企业需要对抗不断演变的网络威胁的能力。

本期《安全+》将继续立足网络安全发展，从前沿技术发展、安全能力构建、政策分析解读等视角出发，在数智赋能的网安新时代，洞见网络安全背后的技术、生态与实践，探讨数智时代网络安全新思路。

安全产业发展持续向前推进，如何抓住前沿创新技术演进机遇并应对潜在风险，解决传统方法难以解决的问题，是网络安全行业需要共同努力解决的课题。

安全能力的构建需要抓手，面向多变、复杂的网络攻击和数据安全威胁，绿盟科技以创新驱动发展，从构建可信任的安全智能生态出发，积极应对不断变化的网络安全挑战，以更加智能、全面的安全防护能力，护航企业在数字化转型的浪潮中稳健前行，以“技术”的关键词植根绿盟科技的价值追求，持续汇聚高质量发展的新动能。

叶晓虎

车联网安全技术现状、突破及趋势

绿盟科技 创新研究院 张克雷

摘要：当下，车联网数据安全与漏洞挖掘成为技术主流，虚拟汽车系统作为当下最为重要的技术突破点，持续推进车联网安全的发展。未来，随着单车智能化的提升和车路协同的实现，国家交通的智能化将更进一步，但风险也将外置，车联网系统需要更智能、更安全的技术保障。本文从技术现状、技术创新、技术发展趋势这三个方面介绍了车联网安全技术。

关键词：车联网安全 车联网靶场 车路协同 自动驾驶 虚拟化

引言

据公安部 2024 年 1 月 11 日统计，截至 2023 年年底，全国机动车保有量达 4.35 亿辆，其中汽车 3.36 亿辆；机动车驾驶人达 5.23 亿人，其中汽车驾驶人 4.86 亿人。伴随汽车的逐步普及，车联网在十年内经历了巨大的技术变革，汽车智能网联功能已成为当前新车标配，百姓对汽车功能的需求越来越多元化，提供座舱娱乐、自动驾驶等功能的新型汽车部件日趋成熟，多种汽车电子电气架构随之涌现。

然而，汽车网联化也带来了更多的安全风险。云端业务系统漏洞、数据泄露事件被频繁披露，车端复杂的功能带来了更多的攻击面，严重的远程控车漏洞和近场通信漏洞频现，犯罪分子甚至通过黑客发布的开源工具对汽车展开偷窃，拆解汽车后买卖零部件以获利。目前看来，汽车、车主个人信息和轨迹，是未来几年内汽车黑客的重要目标。

为方便读者更清晰地从技术上理解车联网安全态势，本文就车联网技术现状、技术创新、技术趋势三点展开讨论车联网安全新技术态势。

1. 技术现状

漏洞挖掘的成果，即为攻击方法或者工具，也是当前黑客关注的焦点。具备高智能化的中高端汽车，其车主个人信息与资产是黑客和犯罪分子关注的焦点。所以，本节就车联网漏洞挖掘技术和车联网数据安全技术两方面展开阐述。

汽车云端的漏洞挖掘对象与传统的互联网云端服务基本类似，大多数是对 WEB、数据库、认证登录、邮件收发、文件传输、MQTT 等多类服务进行漏洞挖掘，进而获取管理员权限或关键业务系统数据。汽车的业务系统内部，存在车主个人信息、汽车轨迹等敏感信息，这些信息黑客是如何获取的呢？

汽车的轨迹需要汽车上传自身定位信息和车主信息到云端，所以，传输敏感信息的服务是被关注的焦点之一。以 MQTT 服务为例，当手机程序或者汽车启动时，部分汽车云依托 MQTT 服务上传当前汽车的状态信息到云端，此时，黑客可以通过逆向手机程序和汽车内部的固件，来获取登录 MQTT 平台的口令，进而以“合法”的身份加入 MQTT 的推送、订阅的机制中，相当于加入“群聊”进行旁听，群里每个汽车上传回自己的身份 ID 以及位置信息，甚至

回附加车主信息。在车端,犯罪分子可以通过破解汽车的无线钥匙,将钥匙的认证信号复制到无线电设备中进行重放,可以偷走部分没有滚动码认证,或者滚动码算法较弱的汽车。

车联网数据安全是实现车联网数据运营的前提保障,这部分工作需要分两步走。数据分级分类是数据安全保障的重要基础,也是数据治理的第一步。数据分类上,面向自身业务,聚焦对象主体进行划分,包括车辆运行数据、环境数据、个人数据等,或聚焦业务流程进行划分,包括车辆数据、研发数据、运维数据等,在大类划分下,依据业务及应用场景继续向下细分类别;数据分级上,分级明确、就高从严进行数据级别确定;数据安全保障方面,各类型企业均面向自身业务构建形成一套较为完善的数据安全保障体系,具体围绕组织建设、制度流程规范和技术支撑体系等方面展开。

第二步,是使用隐私保护、数据脱敏、数据溯源等技术多方面保障数据安全合规。如何在保证数据安全和个人隐私安全的前提下实现数据流通,激发数据潜能,发挥数据价值,成为当前车联网发展的一个挑战。隐私计算技术可以实现“数据可用不可见”,使数据“不出库”就能实现模型构建、模型预测、身份认证、查询统计等能力,将极大地丰富车联网生态的应用天地。在自动驾驶模型构建过程中,需要用到海量数据参与计算,甚至包括普通车主行驶时的数据,自动驾驶的模型构建过程可基于隐私计算技术,实现各车端原始数据不出域情况下的模型构建。模型构建好以后,在车主的行为预测(如语音指令)过程中,可基于隐私计算技术,实现车端原始数据不出域情况下的模型预测。隐私保护方面,利用同态加密、联邦学习、安全多方计算等技术,探索大模型联合训练,为车联网数据流通过程中隐私保护提供新思路;数据脱敏方面,利用人工智能等技术对车外人脸、车牌数据进行脱敏处理,防止敏感信息泄露;数据溯源方面,基于区块链、数字水印等技术保障数据不可篡改、可溯源。

2. 技术创新

汽车的单价多达数十万元,这本就为车联网安全研究带来巨大的成本压力,然而,疫情的到来,使其雪上加霜。车联网安全研究,如何解决成本问题,显然是各个企业,尤其是信息安全企业要解决的第一个难题。

有没有一种车联网安全的研究环境,可以不依赖任何硬件,或者依赖极少量必要的硬件而建立呢?绿盟科技通过技术创新,研究出虚拟汽车系统,使得汽车的电子电气架构,在零部件的操作系统和 CAN 总线通信两方面得以完全虚拟化,大大降低了汽车研究的环境成本。

对汽车的虚拟化,本质上是对虚拟电子电气架构的虚拟化,涉及四个方面的技术,分别为电子电气架构、汽车总线、虚拟化软件以及车内操作系统。

由于 Linux 和 Android 这两类操作系统基本覆盖全车所有关键零部件的操作系统类别,所以,针对 Linux 和 Android 操作系统的零部件进行虚拟化,是虚拟汽车研究的核心。以往,T-BOX 和车机都会连接在信息域,站在网关的角度看,它们都在同一组 CAN 接口

上相连。而在我们的架构中,为了最简单地描述电子电气架构的可定制性,我们将车机和 T-BOX 分开,放在两个不同的功能域。自动驾驶控制器连接到驾驶域中,这一点保持不变,如图 1 所示。

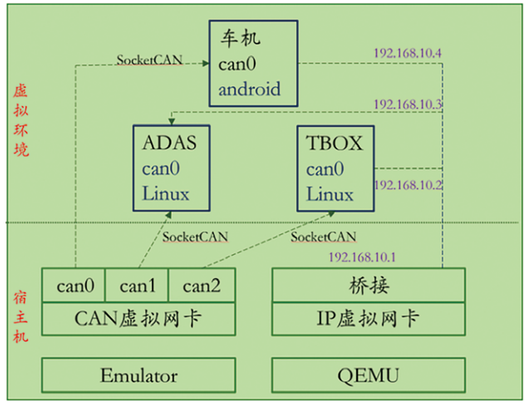


图 1 汽车虚拟电子电气架构

首先,汽车的运行环境需要有 3D 车路的呈现,运行虚拟汽车的主机必须配备性能足够强的显卡,以满足车路效果的稳定呈现。其次,还需要具备方向盘和脚踏板这类外设,可以是实车移植过来的,也可以是购买游戏类的。主机需要读取方向盘的按键编码数据,将控制类信号转发到 CAN 总线后,经由虚拟零部件,转化为前端汽车的控制数据,这一转化,经由“控制引擎”完成汽车的运动控制和车灯、车门等 ECU 的控制。对于信息安全而言,需要向汽车零部件中植入安全探针,如安全 SDK、Agent 等,以满足对汽车信息安全的实时监控。

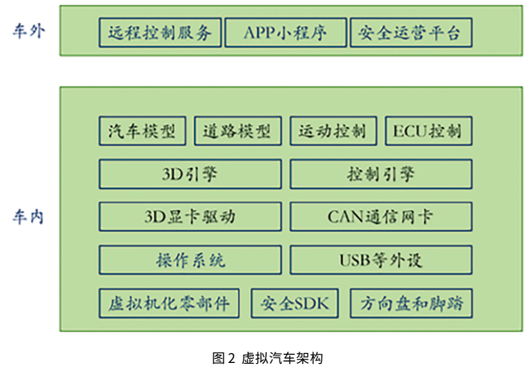


图 2 虚拟汽车架构

这样的虚拟汽车系统,它的实战表现如何呢?下面,我们从电子电气架构的视角,观察虚拟汽车被攻击的过程。首先,构造一个攻击环境;其次,把极光 001 看作真车,使用端口扫描、木马植入等方式进行攻击;最后,核对攻击是否有作用。设计攻击环境时,攻击入口设置为两个,分别是车端入口和云端入口。其中,车端的攻击具体如图 3 所示。左侧所示为驾驶员使用方向盘和脚踏板驾驶汽车,方向盘的控制信号经由宿主机转化为 CAN 信号,发送给 VCU,VCU 将控制方向盘数据转化为前端车辆需要的转向、速度、刹车、倒车等信号,将信号发送给 CAN 转 Unity 的协议转换模块,最后经 Unity 引擎时车辆在车路上驾驶。这其中所有的控制经 CAN 总线。车载以太网方面,宿主机连接外部 Wi-Fi 路由器,QEMU 使用桥接技术将启动的虚拟零部件桥接到 Wi-Fi 路由器下,与宿主机共享一个网段,其中,外部 Wi-Fi 路由器可被当作车辆热点来看待,攻击者接入热点后可对汽车零部件发起攻击。

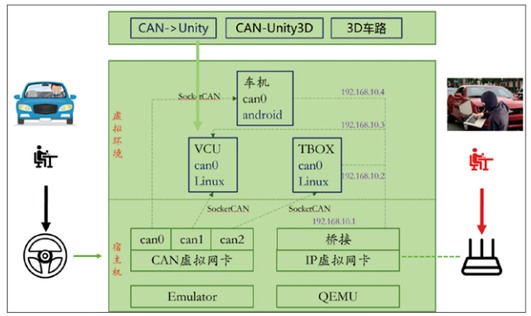


图 3 热点下攻击虚拟汽车的场景

具体的攻击流程为：首先，攻击者接入汽车热点；其次，在热点下对汽车发起主机扫描、端口扫描、弱口令爆破、服务利用等攻击；最后，在获取主机权限后，对零部件发起攻击，如使用 ADB 服务控制车机的空调按钮控制空调，或者发送 CAN 报文实现控车效果。具体如图 4 所示。

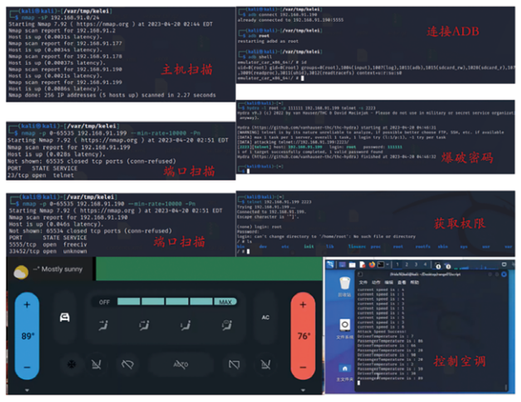


图 4 热点下攻击虚拟汽车的流程

除了可以对其进行攻击以外，虚拟汽车还可以被作为运行汽车应用程序的环境来模拟汽车业务。在零部件的模拟过程中，使用的是 QEMU 启动的 ARM64 架构的 Linux 系统零部件，所以，一些使用该架构的实车中的零部件应用，也可以迁移到虚拟零部件中运行。最为基础的操作为，将实车零部件的根 Linux 文件系统迁移到虚拟零部件中，运行 chroot 命令切换到实车的固件环境下，运行需要被模拟的应用。具体如图 5 所示。应用程序名为“mv_app”的应用经过虚拟零部件启动后，与真实零部件环境下的表现一致，这个“一致”体现在两方面，分别是网络侧监听的端口一致和对 CAN 总线的控制、收发消息的逻辑一致。

图 5 虚拟汽车运行实车业务的效果

对监听的端口和应用，可以进行逆向分析、流量抓取等方式进行漏洞挖掘，对 CAN 总线消息的收发，可以分析车内网总线控车逻辑。利用前者，攻击者可获取零部件权限；利用后者，攻击者可以明确控车报文对部分车辆功能进行控制。

从攻击角度看，虚拟汽车可以支撑汽车靶标的角色，其在虚拟电子电气架构、虚拟汽车零部件、虚拟车内网通信三个方面与发售

的汽车几乎一致。固件模拟执行和业务复现，在虚拟汽车上表现不错，也可达到多零部件联动仿真的效果。虚拟汽车的实现只是第一步，未来，还需要将道路交通的虚拟化纳入其中，使车联网安全研究既更加高效，也更“接地气”。

3. 技术趋势

未来车联网发展有两个大技术方向，其一，是由国家交通战略推动的车路协同技术（V2X），其二，是由用户需求推动的自动驾驶技术（本节自动驾驶指的单车智能）。车路协同的实现，需要智能交通系统作为基建来支撑，是缓解交通拥堵和保证交通安全的重要技术手段。自动驾驶是基于各种感知信息，通过人工智能技术进行决策和车辆控制实现的，在一定程度上本身单车即可实现自主性 [1]。

伴随着车路协同产业链的逐步丰富 [2] 和区域示范区的建立，车路协同和自动驾驶技术也将逐渐落地。针对车路协同，我们讨论两个方面的趋势，其一，是 V2X 网络架构下的一些脆弱点；其二，是 V2X 网络下用户隐私信息保护。

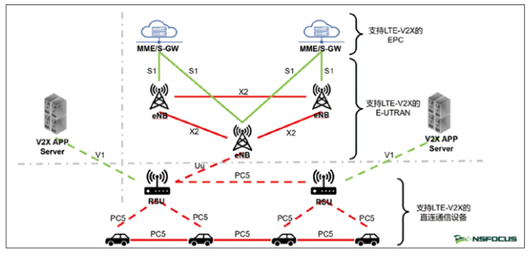


图 6 V2X 通信网络结构

在 V2X 网络中存在车、路侧单元（RSU）、基站（eNB）、应用服务器和其他 LTE 网络设备，其中，应用服务器可作为计算设备采集、分析摄像机、激光雷达、毫米波雷达等多个传感器信息以共享路况。LTE/5G 接入网和核心网的安全性本节不做赘述，处于边缘侧和端侧的 RSU、汽车、服务器、摄像头等会成为攻击者攻击的对象。一方面，这些设备的操作系统为 Linux、Android 等，攻击者攻击类操作系统所使用的手段相对成熟；另一方面，攻击者攻击到这些节点后，可以篡改这些设备生成的各类数据，以欺骗 V2X 网络中的其他节点，使其“谎报军情”，以达到攻击的目的。V2X 网络中各个单元之间的交互可如图 6 所示。

在 V2X 网络下，车辆需要共享位置信息给路侧和其他车辆，用户的隐私信息存在一定的安全隐患，用户隐私信息泄露的担忧可能会为其发展带来一定的阻碍。研究表明，用户选择是否同意将隐私数据共享时考虑的因素中，自身利益，尤其是安全性，是放在第一位的 [3]。所以，在车路协同基础技术建设完成后，第一项进一步的工作，可能是需要加强对用户隐私的保护，使更多的用户“同意”将自己的汽车加入 V2X 的“群聊”而确保不被旁听或泄密。

自动驾驶技术，从结构上看，大体可分三个部分，分别是感知层，计算决策层和执行层。顾名思义，感知层收集摄像头、雷达的数据，供计算决策层分析路况，当路况信息分析完成，需要对汽车下一刻行为做出决策，比如刹车、变道、加速等。计算决策层是自动驾驶的“脑”，所以本节将重点分析计算决策层的安全性。为“脑”提供算力的是自动驾驶控制器，代表芯片厂商为英伟达和 AMD，尤其是英伟达，已在理想、未来、比亚迪等多个厂商高端汽车中装配。从英伟达提供的白皮书 [4] 可知，该控制器使用的是 Linux 或者 QNX 操作系统，系统之上为传感器、神经网络、车辆硬件抽象等库，进而基于各类软件算法，实现路径规划、L2+ 级别自动驾驶、自动泊车等自动驾驶功能。从系统层看，该控制器可以存在 SSH、

TELNET 等具备 Linux 操作系统管理属性的服务，一旦被获取权限，整车“大脑”即被控制。从应用层看，各种应用层输入的传感器数据、产生的分析结果数据、输出的控车执行命令都将影响汽车的驾驶，黑客可以通过这类数据影响、控制汽车的驾驶。

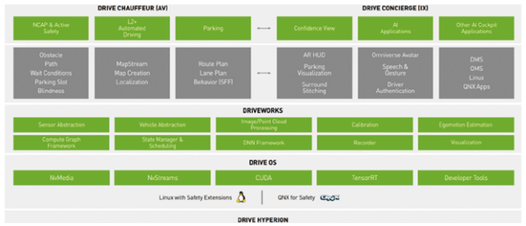


图 7 英伟达自动驾驶控制器软件结构

未来，车路协同单车智能级别的自动驾驶普及后，单车智能与车路协同会形成一体，形成高级别的交通模式，其网络安全风险也将随之聚合，用户隐私也将进一步对外暴露，单车漏洞可造成的威胁也将扩散到整个 V2X 网络范围。构建 V2X 产业链的过程中，建议将基础夯实的网络安全厂商也纳入其中，对 V2X 的网络做整体的信息安全防护设计，以减少自动驾驶和车路协同落地后信息安全漏洞带来的威胁。

4. 总结

本文介绍了车联网安全相关技术的现状、创新以及趋势。当下，车联网安全技术需求聚焦在漏洞挖掘以及数据安全两个方面，其中，使用漏洞挖掘技术可以保证汽车的网络安全或合规，使用数据安全技术把控车联网系统中敏感信息的安全。

绿盟科技独创了虚拟汽车系统（可认为是绿盟造的车），并基于此建立了车联网信息安全靶场，这部分于第三章予以介绍，读者很明显可以感知到，与传统的基于 CAN 总线的虚拟汽车靶场相比，虚拟汽车系统具备所有 ECU 的嵌入式操作系统，包括嵌入式 Android、嵌入式 Linux 两类，兼容 X86 和 ARM 两大类指令集，并具备 CAN 总线及以太网通信的能力。这些特性决定了其具备完整的电子电气架构，其虚拟化的特点大大降低了汽车安全研究的门槛。真实汽车的业务程序可以迁移到异构的虚拟电子电气架构中运行，使绿盟造的车可以具备其他品牌汽车的业务流程。同时，将虚拟汽车并入综合靶场，可满足车联网安全科研、教学、竞技、实训等多方面的需求。

未来，车联网将有两大发展方向，其一，是单车智能；其二，是车路协同。这两大技术相互融合后，道路交通系统将更为智能，但是，也必然将车内的风险外置。在单车智能以及车路协同的系统设计过程中，需要融入安全开发、安全测试等多方面的流程，以确保系统的安全原生化。

2024 Verizon DBIR解读 | 数据泄露转向连接云的第三方软件供应链

绿盟科技 创新研究院 浦明

摘要：本文将对 2024 Verizon DBIR 报告进行全面解读，主要从三个方面进行分析。首先介绍本篇报告的一些核心结论；其次，从 Verizon 定义的 VERIS 框架出发，从威胁参与者、威胁行为、威胁资产和威胁属性四个维度对数据泄露事件进行详细分析；最后，从安全事件的角度，对事件成因的分类、行业分布及区域分布进行再探讨。希望能够通过本文增强大家对数据泄露问题的重视，并为制订更有效的数据安全防护方案提供一些思路。

关键词：数据泄露 Verizon 安全事件 威胁行为

引言

数据泄露已成为当今数字时代企业和个人面临的重大威胁之一，不仅会导致经济损失，还可能损害企业声誉和用户信任。因而了解数据泄露的趋势和成因至关重要。

2024 年 5 月，国际知名咨询机构 Verizon 发布了《2024 年数据泄露调查报告》（*2024 Data Breach Investigations Report*）[1]。该报告综合分析了自 2022 年 11 月 1 日至 2023 年 10 月 31 日间，94 个国家和地区发生的超过 3 万起安全事件以及 1 万多起确认的数据泄露事件。

1. 2024 Verizon DBIR 报告主要结论

2024 Verizon DBIR 全文主要围绕漏洞利用、软件供应链安全、勒索软件、社工以及人的因素几个领域展开描述并输出了许多结论，笔者将部分结论进行了归纳，如下所示：

- 结论1 2023年利用漏洞窃取数据的攻击行为大幅增加，相比去年增加三倍

造成这一结果的部分原因是勒索软件利用未打补丁的软件和设备进行的攻击数量激增，这也表明数据资产的经济价值越来越高，已经成为恶意攻击者的首要目标，及时发现和弥补各类安全漏洞，尤其是应用系统漏洞依然是安全的重中之重。[2]

- 结论2 由软件供应链导致的数据泄露事件占安全事件总量的15%，较去年增长68%，供应链安全成为数据安全的一道重要防线

近年敏捷开发模式流行，但开发者安全意识缺失，造成大量供应链组件服务暴露在互联网上，不同程度带有 N Day 漏洞。这些漏洞可能来自组件本身，或来自扩展组件功能的第三方插件，其客观上增加了软件供应链安全的风险，特别是数据泄露的风险。

- 结论3 报告数据表明，勒索软件是所有行业目前面临的最大威胁

勒索软件作为导致数据泄露的一种攻击行为，往往通过钓鱼

邮件、恶意软件或利用零日漏洞的方式进行入侵，在获取到受害者数据时，通常包含以下几种可能的攻击行为：

数据加密：攻击者获取到受害者数据后对其进行加密，并通过支付赎金的方式解锁这些数据；

数据窃取和公开：攻击者对受害者数据进行窃取，再将受害者数据公开或出售，从而增加勒索成功的可能性

据 Verizon DBIR 数据，过去三年中，勒索软件和话术欺诈几乎占据了导致数据泄露的主要攻击的三分之二，比例波动在 59% 到 66% 之间 [1]，如图 1 所示。

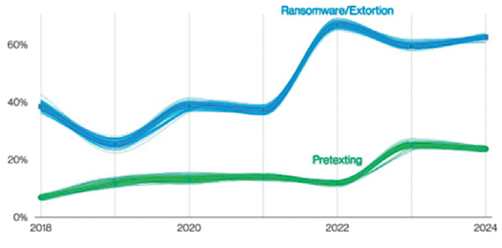


Figure 5. Select action varieties in Financial motive over time

图 1 以金融为动机的威胁行为占比 [1]

- 结论4 人们在钓鱼邮件的整体安全意识上有所提升

由图 2 所示，对比近 7 年来钓鱼邮件的点击率，人们的安全意识在逐步上升 [1]。

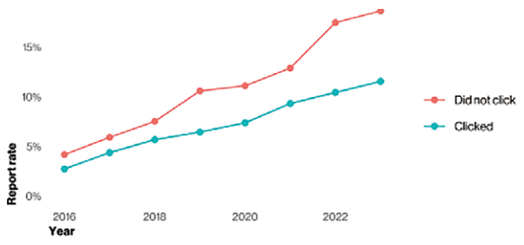


Figure 4. Phishing email report rate by click status

图 2 钓鱼邮件点击率统计 [1]

- 结论5 68%的数据泄露事件涉及人的错误，如配置错误、社工、话术欺诈等，人依然是安全链条上的重要一环

Verizon 在之前的年度分析报告中将人为因素定义为配置错误、社交工程、话术欺诈和内部恶意人员行为等几个部分。然而，近年来，由于内部恶意人员导致的数据泄露事件急剧增加，因此 Verizon 在最新的年度报告中决定将内部恶意人员的行为从人为因素中剔除，并将其归类到权限滥用模式中。这一调整使得人为因素的比例从 76% 降至 68%。这也同时凸显了针对内部人员导致的数据泄露事件防范的重要性。

2. 威胁要点分析

Verizon DBIR 报告提供了一套指标 VERIS（The Vocabulary for Event Recording and Incident Sharing）— 事件记录和事件共享词汇，旨在提供一种结构化和可重复的方式来描述安全事件的通用语言。

在下文开始前，笔者将首先对这些结构化的名词进行解释以方便读者进行后续阅读。

威胁参与者（Threat actor）：泛指安全事件参与者，如发起网络钓鱼活动的参与者

威胁行为（Threat action）：数据泄露事件背后的攻击行为

威胁资产（Threat action）：受数据泄露事件影响的主要资产

威胁属性（Threat Variety）：相对威胁行为更细化的分类，如威胁行为 Web 应用攻击，威胁属性则为 SQL 注入或暴力破解等。

数据泄露事件（Breach）：泛指导致数据泄露的安全事件（Incident）

安全事件（Incident）：泛指会影响信息资产的完整性、机密性或可用性的事件，如 DDoS 攻击通常被视为安全事件而非数据泄露事件（因为 DDoS 攻击不一定导致数据被窃取）

外部参与者 (External)：外部参与者泛指犯罪团伙、黑客等。

内部参与者 (Internal)：内部参与者指来自组织内部的人员，包括公司员工、独立承包商、实习生和其他员工。

合作伙伴 (Partner)：合作伙伴主要包括供应商、托管服务提供商和外包 IT 支持人员等。

有了以上专业名词的解释，笔者首先将重点介绍报告在威胁参与者、威胁行为、威胁资产、威胁属性维度中提到的一些关键数据，之后笔者再进行一些分析与总结，以便读者更全面地理解报告内容。

2.1 威胁参与者维度分析

根据 Verizon 报告的数据，如图 3 所示，2018 年至 2024 年，外部参与者仍然是威胁行为的主要催化剂，所占比例高达 65%。相对而言，内部参与者的比例为 35%，这一数字较去年 Verizon DBIR 报告中提到的 20% 有显著增长 [8]。与此同时，合作伙伴几乎未对威胁事件的发生产生影响。

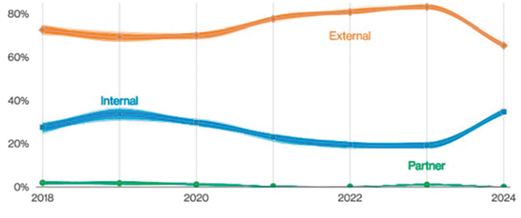


Figure 11. Threat actors in breaches over time

图 3 近年导致数据泄露事件的威胁者类别占比 [1]

2.2 威胁行为维度分析

Verizon 针对威胁行为进行了分类，主要包括以下几种类型：云凭证窃取、勒索软件、错误投递 (Misdelivery)、后门和 C2 攻击、话术欺诈、钓鱼以及漏洞利用等。如图 4 所示，横轴表示各类威胁行为导致的数据泄露事件占比，纵轴则列出了不同的威胁行为类型：

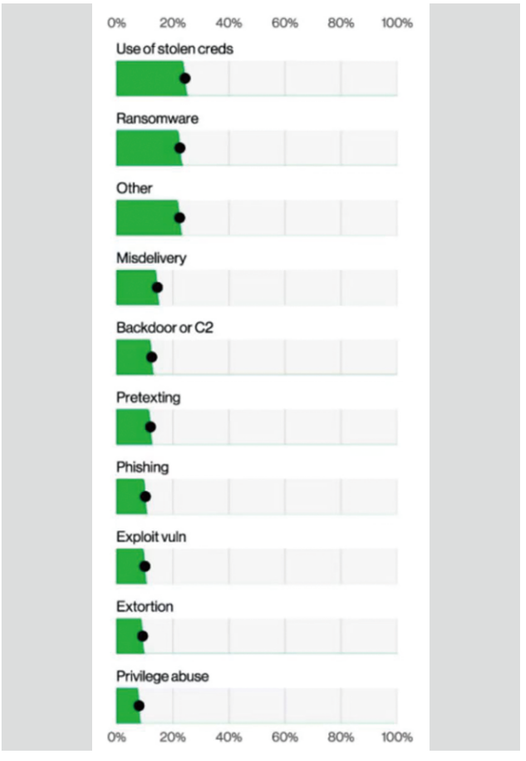


图 4 主要涵盖的威胁行为类别 [1]

2.3 威胁资产维度分析

如图 5 所示，Verizon 从安全事件维度展示了受到数据泄露影响的主要资产类型，图 6 可以看出导致数据泄露事件的主要资产类别为服务器（云端和 on-premise）、人员 (Person)、用户开发环境 (User Dev)，媒体 (Media) 和网络 (Network)，值得注意的是，近年来随着勒索行为的持续增长，人员 (Person) 作为一种威胁资产变得更多 [1]。

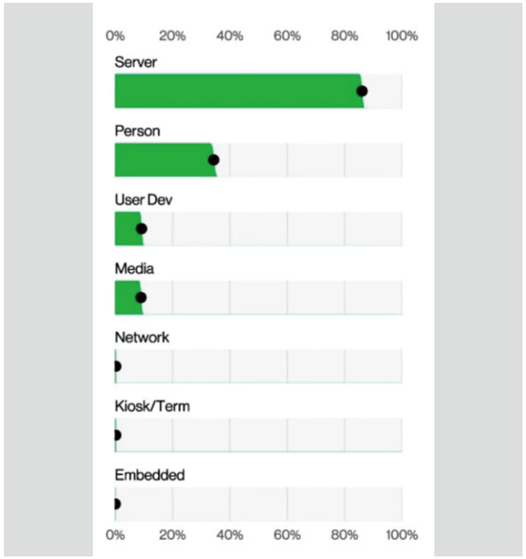


图 5 威胁资产分类 [1]

2.4 威胁属性维度分析

Verizon 从安全三要素的角度，即机密性 (Confidentiality)、完整性 (Integrity) 和可用性 (Availability)，分析了 2022 年至 2024 年间各要素受到威胁的频率变化，如图 6 所示：

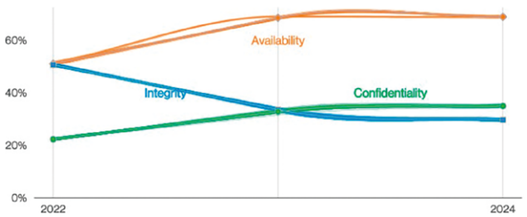


图 6 信息安全三要素角度受到威胁的频率变化 [1]

图 6 中还可以看出，自 2022 年以来，可用性问题导致的威胁频率呈现线性增长；而完整性问题的比例则从 40% 降低至 20%；机密性问题的比例则从 20% 上升至 30%。

其次，从机密性角度来看，泄露事件中最重要的机密数据类别以“个人数据”持续占据榜首，如图 7 所示：

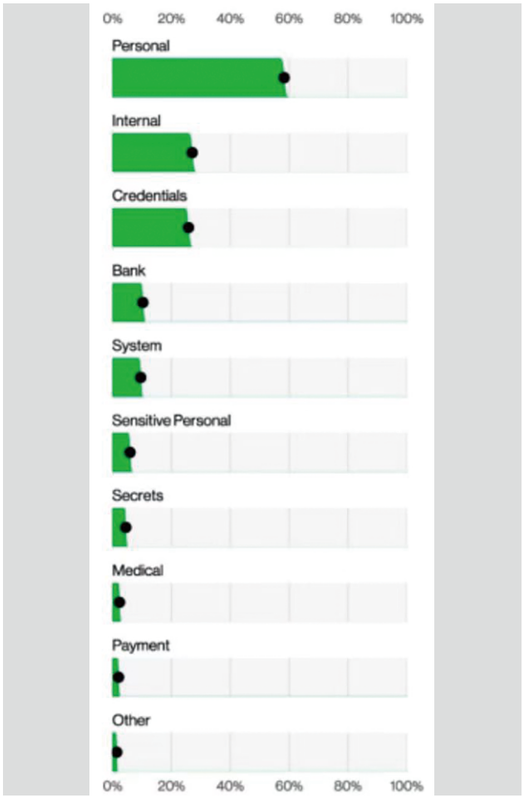


图 7 机密数据类别 [1]

2.5 分析总结

从威胁参与者维度来看，笔者此前阅读了 IBM Security《2023 年数据泄露成本报告》[9]（该报告对 553 家受数据泄露影响的企业进行了深入调研），报告指出，40% 的数据泄露是由安全厂商或外部人员发现的，而 33% 的数据泄露是由内部团队和工具发现的。超过四分之一（27%）的数据泄露是由攻击者在勒索软件攻击中公开的，如图 8 所示。 由于 IBM Security 将外部人员与使用勒索软件的攻击者进行了区分，因此与 Verizon 报告威胁参与者数据的直接对比可能不太明显。然而，如果将这两类参与者合并考虑，可发现 67% 和 33% 的比例与 Verizon 的 65% 和 35% 几乎一致。这表明，外部参与者始终是数据泄露事件的主要原因。究其背后的原因，笔者认为主要有以下几个：

技术手段和工具：外部参与者如黑客通常拥有更先进的技术手段和工具，使他们能够绕过企业的安全防护，获得未授权的访问权限。

商业利益驱动：外部参与者背后通常是商业利益驱动的组织团体。相比于大多数内部人员使用特权获取隐私数据，外部参与者在数据窃取方面更为专业，涉及攻击范围更广，且攻击频率更高。

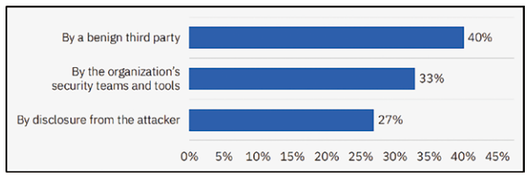


图 8 识别数据泄露方式占比 [9]

从威胁行为维度来看，笔者将部分结论进行了归纳，如下所示：

- 结论1 云凭证窃取仍然是导致数据泄露的主要原因，但2023 年其比例有所下降，占比为24%。与之接近的是勒索软件，其占比为23%。 以上数据表明，尽管云凭证窃取依旧是最常见的攻击方式，勒索软件仍然保持着重要性。

云凭证可能包括数据库连接方式、公有云资源访问凭证（如 AK/SK）以及系统登录密钥等。近年来，由于凭证窃取导致的数据泄露事件频繁发生，笔者认为其主要原因可归结于人为因素。例如，开发者可能将凭证硬编码在代码仓库中，而这些仓库被设置为公开，从而任何人均可访问并获取凭证。此外，公有云为租户提供的临时凭证（STS）需要设置相关资源的访问权限，如果权限配置过于宽松，一旦 STS 泄露，攻击者便能利用这些脆弱的权限访问敏感信息。

勒索软件方面，以 2023 年 5 月 27 日为例，俄罗斯勒索软件组织 CL0P 利用 MOVEit Transfer 和 MOVEit Cloud 中的零日漏洞（CVE-2023-34362）对全球众多企业发起了大规模的软件供应链攻击。此次攻击影响了壳牌公司、德意志银行、普华永道、索尼、西门子、BBC、英国航空公司及美国能源部和农业部等知名企业，涉及超过 900 家私营和公共部门组织，并波及超 2000 万人，其中 80% 的受害者位于美国，金融、医疗和教育行业受到的影响最为严重 [3]。

CVE-2023-34362 是造成此事件的“始作俑者”，该漏洞允许未经身份验证的攻击者通过 SQL 注入（SQLi）访问并操控数据库，进而导致重大数据泄露、敏感信息丢失及服务中断的风险。具体而言，攻击者可以通过构造 Webshell（通常命名为 human2.aspx），并上传至 MOVEit Transfer 的安装路径下（例如 C:\MOVEitTransfer\wwwroot 目录）。该 Webshell 包含一个可连接的 SQL 数据库账号。通过对 human2.aspx 发起 HTTP 请求并结合恶意 Webshell，攻击者能够连接到 SQL 数据库，从而获得 MOVEit

Transfer 中所有文件的列表、文件所有者、文件大小及内容等关键信息。这种方法具有持久性和隐秘性，为提前的信息收集和后续的数据窃取提供了便利条件 [5]。

绿盟科技创新研究院在 2024 年初发布了《2023 年公有云安全风险分析报告》[10]。报告中对云凭证泄露风险进行了详细描述，感兴趣的读者可以参考该报告以获取更多信息。

• 结论2 由话术（Pretexting）欺诈导致的安全事件数量超越网络钓鱼（Phishing），成为更可能的社工手段

据 Verizon 的数据泄露报告显示，2023 年商业邮件欺诈 (BEC) 攻击占社工攻击的一半以上，攻击者在伪造和仿冒邮件上变得更加自动化，这得益于 AI 的发展，攻击者借助 AIGC 可编写极具说服力的钓鱼电子邮件 (话术)，而且还能逃避传统电子邮件安全工具的检测，大规模地提高攻击的覆盖范围和复杂性。

常见的电子邮件安全防御措施包括反欺骗技术（如 DMARC 和 SPF）、行为分析、其他威胁检测、以及多因素身份验证（MFA）和强大的身份与访问管理等。为了建立有效的纵深防御，企业侧需要分层实施威胁情报，并采用以人员为导向的业务和技术政策，以最大限度地降低风险 [6]。

• 结论3 通过对漏洞修复生命周期进行分析，漏洞修复速率在发布补丁可用30天后才开始加快，需要大约55天才能修复50%的关键漏洞，到一年结束时，仍有8%的漏洞处于未修补状态。

据相关数据显示，企业补丁管理周期通常稳定在 30 到 60 天，针对关键漏洞的补丁目标则可能设定为 15 天。但这一进度仍然无法跟上攻击者扫描和利用漏洞的速度（通常为 5 天）。具体如图 9 所示：

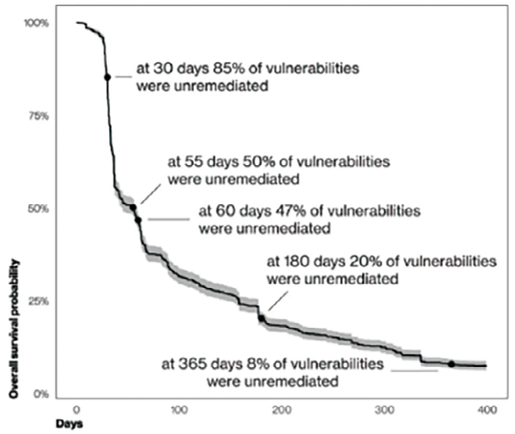


Figure 19. Survival analysis of CISA KEV vulnerabilities

图 9 Cybersecurity and Infrastructure[1]

Security Agency（CISA）机构关于漏洞修复生命周期的调研结果

由于 DevOps 各阶段涉及大量资产（包括设计、开发、测试和运维等），当漏洞在整个网络中大规模爆发时，面向云服务的第三方软件供应链资产将受到重大影响。因此，如何针对性地提升漏洞修复的生命周期成为亟待解决的问题。

从威胁资产维度来看，Verizon 报告指出，“由软件供应链导致的数据泄露事件占安全事件总量的 15%，较去年增长 68%”。这一观点进一步表明，由于软件供应链涉及大量云端资产，而这些资产大多部署在云服务器上，笔者认为，从威胁资产的角度来看，这一趋势在未来将会愈加明显。

值得注意的是，绿盟科技创新研究院在《2023 年公有云安全风险分析报告》中针对连接云的第三方供应链安全风险进行了详

细分析，具体地，我们对在互联网暴露的约 21 万个 DevOps 组件服务的暴露面和攻击面进行了统计分析，如图 10 所示，发现约 45% 的组件存在 N Day 漏洞，如图 11 所示。这些漏洞使互联网暴露的 DevOps 组件服务存在严重安全风险。

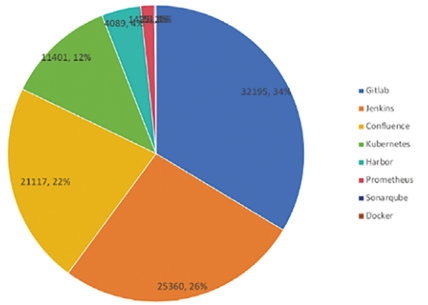


图 10 CVE 漏洞组件分布

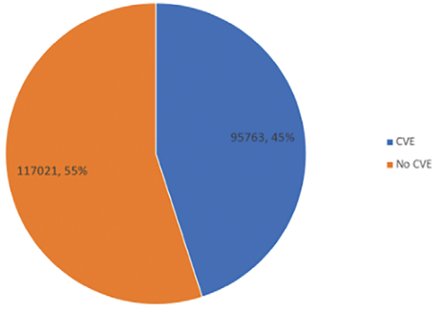


图 11 漏洞数量及占比情况

3. 安全事件分析

我们可根据安全事件和数据泄露事件两种类型进行分析，整体可从事件分类（事件成因），行业分布，区域分布三方面展开。

3.1 事件分类分析

Verizon 将事件分类为八种模式，即基础 Web 应用类攻击 (Basic Web Application Attacks)，拒绝服务攻击 (Denial of Service)，丢失和被窃取的凭证 (Lost and Stolen Assets)，杂项类错误 (Miscellaneous Errors 泛指人的因素，无意行为导致安全事件的发生，但丢失设备并不包含在此类中，而属于盗窃类别)，权限滥用 (Privilege Misuse)，社工 (Social Engineering)，系统入侵 (System Intrusion)，其他 (Everything Else)。图 12，13 从安全事件和数据泄露事件两个维度展示了近年来事件成因随时间推移的变化：

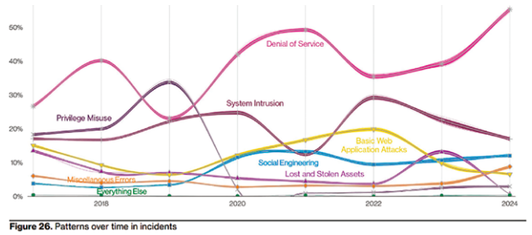


Figure 26. Patterns over time in incidents

图 12 安全事件成因变化 [1]

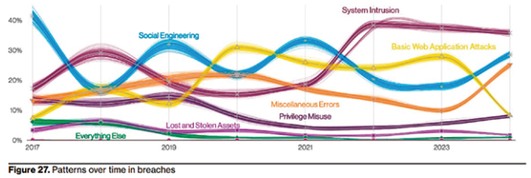


Figure 27. Patterns over time in breaches

图 13 数据泄露事件成因变化 [1]

首先，从安全事件维度来看，自 2018 年以来，拒绝服务攻击持续成为导致事件发生的主要原因。尤其自 2022 年以来，拒绝服

务类攻击的频率显著上升，其次是系统入侵和基础 Web 应用类攻击。

其次，在数据泄露事件维度方面，从 2017 年起，系统入侵、社工攻击和基础 Web 应用类攻击分别成为数据泄露的主要原因。尤其自 2023 年以来，社工攻击和杂项错误模式均显著增加。其中，社工攻击主要以话术欺诈为主，而杂项错误多与配置错误和误投递（Misdelivery）相关。

笔者分析，随着企业业务逐渐向云端迁移，云资产不断增加，不安全的配置，连接云服务的第三方供应链 DevOps 资产数量暴增可能导致数据泄露事件的增多。此外，基础 Web 应用类攻击自 2023 年开始大幅下滑。

3.2 事件行业分布

Verizon 分析了全球发生的 30458 个安全事件，其中有 10626 个被确认为数据泄露事件，按受害者行业和组织规模划分的安全事件和数据泄露数量如图 14 所示：

	Incidents				Breaches			
Industry	Total	Small (1–1,000)	Large (1,000+)	Unknown	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	30,458	919	1,298	28,241	10,626	617	986	9,023
Accommodation (72)	220	16	9	195	106	16	9	81
Administrative (56)	28	7	7	14	21	6	4	11
Agriculture (11)	79	5	0	74	56	4	0	52
Construction (23)	249	17	6	226	220	12	5	203
Education (61)	1,780	82	630	1,068	1,537	56	618	863
Entertainment (71)	447	16	2	429	306	10	1	295
Finance (52)	3,348	75	122	3,151	1,115	54	87	974
Healthcare (62)	1,378	54	21	1,303	1,220	41	18	1,161
Information (51)	1,367	79	62	1,226	602	49	19	534
Management (55)	22	4	1	17	19	4	1	14
Manufacturing (31–33)	2,305	102	81	2,122	849	62	49	738
Mining (21)	30	1	2	27	20	1	1	18
Other Services (81)	462	13	5	444	417	8	5	404
Professional (54)	2,599	205	102	2,292	1,314	124	73	1,117
Public Administration (92)	12,217	56	115	12,046	1,085	39	27	1,019
Real Estate (53)	432	35	5	392	399	29	2	368
Retail (44–45)	725	90	47	588	369	55	32	282
Transportation (48–49)	260	21	38	201	138	17	12	109
Utilities (22)	191	17	11	163	130	12	6	112
Wholesale Trade (42)	76	22	21	33	54	17	14	23
Unknown	2,243	2	11	2,230	649	1	3	645
Total	30,458	919	1,298	28,241	10,626	617	986	9,023

Table 2. Number of security incidents and breaches by victim industry and organization size

图 14 按受害者行业和组织规模划分的安全事件和数据泄露数量汇总 [1]

从数据泄露事件数量来看，主要受到影响较大的行业为：

医疗：事件模式分类上以杂项类错误，权限滥用和系统入侵为主，约占比医疗行业数据泄露事件的 83%

教育：事件模式分类上以系统入侵，社工，杂项类错误为主，约占比教育行业数据泄露事件的 90%

金融：事件模式分类上以系统入侵，社工，杂项类错误为主，约占比金融行业数据泄露事件的 78%

制造业：事件模式分类上以系统入侵，社工，杂项类错误为主，约占比制造行业数据泄露事件的 83%

信息行业：事件模式分类上以系统入侵，基础 Web 应用类攻击，社工为主，约占比信息行业数据泄露事件的 79%

行政单位：事件模式分类上以系统入侵，社工，杂项类错误为主，约占比行政单位数据泄露事件的 78%

服务或专业知识（会计、广告和营销以及法律服务）：事件模式分类上以系统入侵，社工，杂项类错误为主，约占比服务业数据泄露事件的 85%

从事件分类模式上来看，绝大多数事件成因以系统入侵、社工、杂项类错误为主。

与此相比，国内发布的数据泄露报告，如《全球数据泄露态势报告》[11]（由数事咨询与零零信安联合发布）和《2024 上半年数据泄露风险态势报告》[12]（由威胁猎人发布）描述了数据泄露事件在不同行业的分布情况。其中《全球数据泄露态势报告》指出，信息和互联网行业、金融行业、党政军与社会、文体娱乐业和批发零售业等行业的泄露事件较为频繁。《2024 上半年数据泄露风险态势报告》指出数据泄露事件数量 Top5 行业分别为银行、电商、消费金融、保险、快递。可以看出与国外相比，国内医疗和教育行业的安全事件相对较少，这也进一步反映出一些问题，笔者认为主要归结为以下两方面：

攻击者兴趣：国内相较于互联网、金融等行业，医疗和教育行业由于金钱驱动力较弱，攻击者的兴趣可能较低，因此这些行业成为攻击目标的概率也较低。

报告数据差异化：不同国家和地区在数据泄露事件的发生频率和行业分布上存在差异，这可能反映了各地行业安全状况、数据安全法和防护水平的不同。

3.3 事件区域分布

根据联合国 M4997 标准，Verizon 对全球各个地区进行了详细的划分和考察，主要包括以下三个区域：

亚太地区：涵盖南亚、东南亚、中亚、东亚和大洋洲；

欧洲、中东和非洲：包含北非、欧洲、东欧以及西亚；

北美：包括美国和加拿大

Region	Frequency	Top patterns	Threat actors	Actor motives	Data compromised
APAC	2,130 incidents, 523 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 95% of breaches	External (98%), Internal (2%) (breaches)	Financial (75%), Espionage (25%) (breaches)	Credentials (69%), Internal (37%), Secrets (24%), Other (17%) (breaches)
EMEA	8,302 incidents, 6,005 with confirmed data disclosure	Miscellaneous Errors, System Intrusion and Social Engineering represent 87% of breaches	External (51%), Internal (49%) (breaches)	Financial (94%), Espionage (6%) (breaches)	Personal (64%), Other (36%), Internal (33%), Credentials (20%) (breaches)
NA	16,619 incidents, 1,877 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 91% of breaches	External (93%), Internal (8%) (breaches)	Financial (97%), Espionage (4%) (breaches)	Personal (50%), Credentials (26%), Internal (19%), Other (16%) (breaches)

图 15 时间区域分布 [1]

图 15 展示了亚太地区、欧洲、中东和非洲和北美三个地区的事件数量分布情况。数据显示，北美地区的事件数量最多，共计 16619 起，而亚太地区地区的事件数量最少，仅为 2130 起。

从事件成因方面来看，系统入侵和社工攻击为主要因素，其中 70% 的系统入侵事件是由勒索软件攻击引发的。

从威胁者的角度来看，外部攻击者成为主要威胁，这一点并不令人意外，因为绝大多数的攻击都是由外部因素造成的。在行为动机方面，金融驱动一直是攻击者的主要动机之一。

从威胁资产的类型来看，各地区表现出不同的特征：亚太地区主要以凭证丢失为主；EMEA(欧洲、中东和非洲) 地区则以个人数据丢失为主，其余情况涉及内部数据和凭证的丢失；而北美地区同样以个人数据丢失为主，其次是凭证和内部数据的丢失。

4. 总结

本文对 2024 年 Verizon DBIR 报告进行解读，提炼出报告的主要结论。可以看出，数据泄露事件的严重性在近几年持续上升。安全同行应对事件背后的成因进行全面分析，梳理出当前数据泄露攻击路径的整体情况。唯此才能有针对性地预防数据泄露的发生。

绿盟科技创新研究院在云上风险发现和数据泄露领域已经开展了多年的研究。借助 Fusion 数据泄露侦察平台，我们已监测到数万个云端暴露资产存在未授权访问的情况，包括但不限于自建仓库、公有云对象存储、云盘、OLAP/OLTP 数据库，以及各类存储中间件等，具体可参考《2023 公有云安全风险分析报告》[7]。

Fusion 是由绿盟科技创新研究院研发的一款面向数据泄露测绘的创新产品。如图 16 所示，Fusion 集探测、识别、泄露数据侦察于一体，针对互联网中暴露的泛云组件进行测绘，识别组件关联的

组织机构和组件风险的影响面，实现自动化的资产探测、风险发现、泄露数据分析、责任主体识别、数据泄露侦察全生命周期流程。

图 16 Fusion 能力全景图

Fusion 的云上风险事件发现组件具有如下主要特色能力：

资产扫描探测：通过多个分布式节点对目标网段 / 资产进行分布式扫描探测，同时获取外部平台相关资产进行融合，利用本地指纹知识库标记，实现目标区域云上资产探测与指纹标记。

资产风险发现：通过分布式任务管理机制对目标资产进行静态版本匹配和动态 PoC 验证的方式，实现快速获取目标资产的脆弱性暴露情况。

风险资产组织定位：利用网络资产信息定位其所属地区、行业以及责任主体，进而挖掘主体间存在的隐藏供应链关系及相关风险。

资产泄露数据分析：针对不同组件资产的泄露文件，结合大模型相关技术对泄露数据进行分析与挖掘，实现目标资产的敏感信息获取。

公众号后台回复“数据泄露”获取更多信息。

参考文献

[1] https://www.verizon.com/business/resources/reports/dbir/ .

[2] https://www.leadsec.com.cn/News_detail/66.html .

[3] https://www.secrss.com/articles/56932 .

[4] https://gist.github.com/JohnHammond/44ce8556f798b7f6a7574148b679c643 .

[5] https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response .

[6] https://www.secrss.com/articles/63573 .

[7] https://www.nsfocus.com.cn/html/2024/92_0313/212.html .

[8] https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/ .

[9] https://www.ibm.com/cn-zh/reports/data-breach .

[10] https://mp.weixin.qq.com/s/VQmh_jU5mF-iV1hWFDiBzw .

[11] https://www.dwcon.cn/post/3587 .

[12] https://www.threathunter.cn/blog/2024 .

电力交易数据安全分类分级管理初探

绿盟科技 服务交付能力部 尹亮 郭涛 湖北代表处 廖方兴 潘丽媛

摘要：随着智能电网的发展和电力市场化改革的深入，电力交易数据量急剧增加，数据类型日趋复杂。有效的数据分类分级对于提升电力系统运行效率、保障电力市场稳定运行具有重要意义。本文旨在深入探讨电力交易数据的分类与分级方法，并分析其在电力交易、市场监管和数据分析等领域的应用。首先，本文分析了电力交易数据的特性，并基于这些特性提出了一个综合的数据分类框架；其次，根据不同级别的数据敏感性和重要性进行了分级研究。在分类与分级的基础上，本文进一步分析了电力交易数据在各个领域的应用。本文通过深入探讨电力交易数据的分类分级管理，为电力市场的规范化、透明化和高效化提供了新的理论和方法指导。

关键词：电力交易 数据分类 数据分级 智能电网 电力市场

引言

随着全球能源市场的快速发展和数字化转型的推进，电力交易数据作为能源行业的重要信息资产，其分类分级管理显得越发重要。在能源互联网的背景下，电力交易数据不仅涉及电力市场的运营和监管，还关联到国家能源安全、经济发展乃至社会民生。因此，对电力交易数据进行科学、合理的分类分级管理，既是提升电力市场运行效率的需要，也是保障能源安全、促进可持续发展的必然要求。

当前，电力交易数据呈现爆炸性增长的态势。据统计，目前全球电力交易数据规模已达到数十亿条，且呈现持续快速增长的趋势[1]。这些数据不仅来源广泛，包括发电企业、电网公司、售电企业等多个主体，而且数据内容种类繁多，涵盖电力交易价格、交易量、交易时间等多个维度。然而，在数据量快速增长的同时，也暴露出电力交易主体数据管理和利用上的诸多问题。例如，数据质量参差不齐、数据标准不统一、数据安全性难以保障等，这些问题严重制约了电力交易数据的有效利用和电力市场的健康发展。

通过对数据分类分级，可以更加清晰地了解电力市场的运行状况，为政策制定者提供决策支持。例如，通过分析历史交易数据，可以发现市场价格的波动规律，预测未来的价格走势，为电力企业的生产和经营提供指导。同时，对数据分类分级还有助于提高数据的安全性和隐私保护。电力交易数据涉及企业商业秘密和用户个人信息，如果不进行适宜的保护，可能会引发数据泄露和滥用等风险。通过分类分级，可以对不同级别的数据采取不同的保护措施，确保数据的安全性和隐私性。

因此，对电力交易数据进行分类分级管理显得尤为重要。数据分类，可以将不同来源、不同类型的数据进行有序整合，形成统一的数据资源池，为数据分析和利用提供基础。数据分级，可以根据数据的重要性和敏感性，对不同级别的数据制定相应的访问权限和保密措施，确保数据的安全性和可控性。同时，分类分级管理还有助于提升数据的质量和价值，为电力市场在风险管理、业务创新等方面提供有力支撑。

1. 电力交易数据概述

电力交易数据作为能源经济学的核心数据资源，其重要性不

言而喻。正如著名经济学家阿尔弗雷德·马歇尔所言，“数据是经济学的原材料”[2]。随着数据科学和分析技术的不断进步，电力交易数据将在未来的能源市场中发挥更加重要的作用，为能源行业的可持续发展提供有力支撑。

1.1 电力交易数据的概念

电力交易数据，作为能源市场的重要组成部分，涵盖了从发电、输电、配电到最终用户消费的全过程信息。这些数据不仅记录了电力市场的实时交易情况，还反映了能源市场的供需关系、价格波动以及市场主体的行为特征。随着智能电网和大数据技术的深入发展，电力交易数据的规模和复杂性不断增加，其潜在价值也日益凸显。

以某地区的电力交易数据为例，电力交易中心通过对其进行深度挖掘和分析，可以发现该地区在哪些高峰时段的电力需求旺盛，而低谷时段则相对宽松。这一发现为电力调度部门提供了宝贵的参考信息，有助于他们更加精准地预测电力需求，优化调度策略，确保电力系统的稳定运行。同时，这些数据还可以为能源企业提供市场趋势分析，指导企业制定合理的生产和销售策略，提高市场竞争力。

此外，电力交易数据在能源政策制定和监管方面也发挥着重要作用[3]。通过对历史数据分析，政策制定者可以了解能源市场的演变规律和发展趋势，从而制定更加科学合理的能源政策。同时，监管机构可以利用实时交易数据对市场主体的行为进行监控和评估，确保市场的公平、公正和透明。

1.2 电力交易数据的来源

电力交易数据的来源广泛且多样，主要包括发电企业、输电企业、配电企业、售电企业以及电力交易市场等各个环节[4]。这些企业在日常运营中产生的数据，如发电量、电价、交易电量、负荷预测等，构成了电力交易数据的基础。

以发电企业为例，其产生的数据包括各类机组的运行数据、燃料消耗数据、设备维护数据等。这些数据不仅反映了发电企业的运营状况，也为电力交易提供了重要的参考。例如，当某地区的负荷预测显示需求增加时，发电企业可以根据自身机组的运行状况调整发电计划，以满足市场需求。

输电企业则主要负责电力的输送和分配，其产生的数据包括输电线路的负载情况、电压波动、功率因数等。这些数据对于保障电力系统的稳定运行至关重要。同时，输电企业还需要与发电企业和配电企业紧密合作，确保电力交易的顺利进行。

配电企业和售电企业则更侧重于电力市场的营销和服务。他们通过收集和分析用户用电数据，为用户提供更加精准的电力产品和服务。例如，通过对用户用电行为的分析，配电企业和售电企业可以推出更加符合用户需求的电力套餐，提高用户满意度。

此外，电力交易市场作为电力交易的核心环节，其产生的数据更是丰富多样。包括电力交易的成交量、成交价格、交易双方的信息等，这些数据不仅反映了电力市场的供求关系，也为政策制定和市场分析提供了重要依据。

综上所述，电力交易数据的来源广泛且多样，各个环节的数据相互关联、相互影响。通过对这些数据的收集和分析，我们可以更加深入地了解电力市场的运行状况和发展趋势，为电力行业的可持续发展提供有力支持。

1.3 电力交易数据的特点

电力交易数据具有大规模性、实时性、多维性的特点。

首先，电力交易数据具有大规模性，随着电力市场的不断扩大，交易数据量呈现出爆炸性增长。全球电力交易数据规模已达到数十亿条，这些数据涵盖了发电、输电、配电和售电等各个环节。因此，对如此庞大的数据进行有效分类和分级，有助于提升数据处理效率。

其次，电力交易数据具有实时性。电力市场的运行需要实时数据的支持，以便及时调整交易策略和优化资源配置。例如，在电力负荷高峰时段，电力交易数据能够实时反映供需关系。因此，对电力交易数据进行实时分类和分级，有助于把握市场动态，提高电力市场的运行效率。

此外，电力交易数据还具有多维性。电力交易涉及多个维度，如时间、空间、价格、电量等，这些维度相互交织，构成了复杂的数据结构。例如，在电力交易中，需要考虑不同地区的电价差异、不同时段的负荷变化等因素。因此，对电力交易数据进行多维度的分类和分级，有助于揭示数据间的内在联系，为电力市场的分析和预测提供有力支持。

2. 电力交易数据分类

数据分类是数据挖掘的第一步,也是最重要的一步。通过科学、合理的分类方法，我们能够更好地理解和利用电力交易数据，为电力市场的健康发展和监管提供有力支持。

2.1 分类原则

在数据分类过程中宜遵循以下原则：

系统性原则：数据分类宜基于对机构所有数据的考量，建立一个层层划分、层层隶属、从总到分的分类体系，每一次划分应有单一、明确的依据。数据类目的排列宜依据数据类目主题之间的内在联系，遵循概念逻辑，遵循最大效用原则，将全部类目系统地组织起来，形成具有隶属和并列关系的分类体系，以揭示出机构数据不同类别之间的联系和区别。

规范性原则：所使用的词语或短语能确切表达数据类目的实际内容范围，内涵、外延清楚；在表达相同的概念时，保证用语一致性；在不影响数据类目含义表达的情况下，保证用语简洁性。在行业内已有统一数据用语的情况下，使用统一数据用语。

稳定性原则：宜选择分类对象最稳定最本质的特性作为数据分类的基础和依据。

明确性原则：同一层级的数据类目间宜界限分明。当数据类目名称不能明确各自界限时，可以用注释来加以明确。

扩展性原则：在数据类目的设置或层级的划分上，宜保留适当余地，利于后续数据的分类需要增加时的类目扩展。

2.2 分类方法

在电力交易数据的分类方法中，主要依据数据的性质、用途、敏感性以及处理难度等多个维度进行划分[5]。

首先，从数据性质来看，电力交易数据可以分为基础数据和衍生数据。基础数据，如电量、电价、交易时间等，是电力交易活动的直接记录，具有原始性和直接性；而衍生数据，如电力市场的供需关系、价格波动趋势等，则是基于基础数据通过一定的分析模型得出的，具有间接性和预测性。这种分类有助于我们更好地理

解数据的本质和用途。

其次，从数据用途来看，电力交易数据可以分为交易数据、监管数据和分析数据。交易数据主要用于电力交易的直接执行和结算，具有高度的实时性和准确性要求；监管数据则用于政府对电力市场的监管和调控，需要保证数据的完整性和透明度；分析数据则主要用于电力市场的分析和预测，要求数据具有足够的广度和深度。这种分类有助于我们明确数据的使用方向和需求。

此外，从数据敏感性来看，电力交易数据可以分为公开数据和敏感数据。公开数据是指那些不涉及商业机密和个人隐私的数据，可以对外公开和共享；而敏感数据则涉及商业机密和个人隐私，需要严格保密。这种分类有助于我们更好地保护数据的安全和隐私。

最后，从数据处理难度来看，电力交易数据可以分为结构化数据和非结构化数据[6]。结构化数据是指那些具有固定格式和结构的数据，如数据库中的表格数据；而非结构化数据则是指那些格式不固定、结构复杂的数据，如文本、图像、音频等。这种分类有助于我们更好地选择和处理数据。

2.3 分类实践

在电力交易数据的分类实践中，电力交易数据可根据性质分为直接交易数据、间接交易数据和第三方数据。直接交易数据主要来源于电力交易市场的买卖双方，反映了市场的实时交易情况；间接交易数据则通过电力调度中心、能源监管机构等渠道获取，提供了市场的宏观运行状况；第三方数据则包括研究机构、媒体等发布的相关数据，为市场参与者提供了丰富的市场信息和趋势分析。分类示例如表 1 所示。

表 1 数据分类示例

数据大类	子类	内容
直接交易数据	交易管理类	指存放的交易规则数据，包括规则名称、规则编码、规则类型、规则应用方、交易规则注册、规则注册人、规则场景等。
	合同管理类	指存放合同管理的基础数据，包括合同类型、合同范本、合同属性、签章、日志、模板等。
	计划管理类	指计划编制中用到的数据，包括计划单元状态、版本、参数值、购入电力、售出电力、最大需求负荷、用电需求、计划曲线、计划调整等。
间接交易数据	业务管控数据	指交易业务在合规监视产生的数据，包括流程标识、流程名称、预警、监控类型等。
	风险管控数据	指交易全过程中可能出现的风险并进行管控的数据，包括三公报表名称、上报时间、状态以及风险分类、标识、指标、级别等。
	信用评价数据	指评价市场主体信用数据，包括信用等级、判定规则、奖惩指标、佐证材料、欠费金额、违约金额、评价得分、信用状态、评价结果等。
	电网运行数据	指电力系统在发电、输电、配电过程中产生的各类数据，如：电力系统测量数据、监控数据等。
第三方数据	市场运营数据发布	指电力市场发布的市场运营数据，包括业务场景、最大负荷、更新时间等。

电力交易数据分类的结果对于电力市场的运营和管理至关重要[7]。通过对电力交易数据进行科学分类，我们可以更加清晰地了解数据的性质、来源和用途，从而更有效地进行数据管理和利用。

3. 电力交易数据分级

在信息时代，数据是最宝贵的资源，但同时也是最脆弱的资产。因此，在电力交易数据的分级原则下，我们需要精心设计和实施数据保护和利用的平衡策略，以确保电力市场的稳定、公平和高效。

3.1 分级原则

在数据分级过程中宜遵循以下原则：

可执行性原则：宜避免对数据进行过于复杂的分级规划，保证数据分级使用和执行的可行性。

自主性原则:机构可根据自身的数据管理需要，例如战略需要、业务需要、对风险的接受程度等，按照数据分类原则进行分类之后，按照数据分级方法自主确定更多的数据层级，并为数据定级。

合理性原则：数据级别宜具有合理性，不能将所有数据集中划分至某一两个级别中，而其他级别中没有数据。级别划定过低可能导致数据不能得到有效保护；级别划定过高可能导致不必要的业务开支，应注意不宜将高敏感度数据定为低敏感度级别。

客观性原则：数据的分级规则是客观并可以被校验的，即通过数据自身的属性和分级规则就可以判定其分级，已经分级的数据可被复核和检查。

3.2 分级方法

在电力交易数据分级的过程中，分级方法的选择至关重要。一种常见的分级方法是基于数据的重要性和敏感性进行划分。例如，可以将电力交易数据分为公开数据、内部数据和机密数据三个级别。公开数据包括电力市场的交易价格、交易量等基本信息，这些数据对公众透明，有助于市场参与者做出电量出让或受让的决策。内部数据则涉及电力公司的运营情况、供需状况等，这些数据对于电力公司的内部管理至关重要。而机密数据则包括电力公司的商业秘密、客户隐私等高度敏感的信息，需要严格的保密措施。数据分级参照表如表 2 所示。

表 2 数据分级参照表

数据级别标识	数据特征
第三级：机密数据	1. 一般特征：数据主要用于行业内大型或特大型机构中的重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。
	2. 数据的安全属性（完整性、保密性、可用性）遭到破坏后数据损失后，影响范围大（跨行业或跨机构），影响程度一般是“严重”。
第二级：内部数据	1. 一般特征：数据用于一般业务使用，一般针对受限对象公开；一般指市场内部管理且不宜广泛公开的数据。
	2. 数据的安全属性（完整性、保密性、可用性）遭到破坏后数据损失后，影响范围中等（一般局限在本市场主体），影响程度一般是“中等”。
第一级：公开数据	1. 一般特征：数据可被公开或可被公众获知、使用。例如官方网站上公布的数据、向社会公众披露的信息。
	2. 数据的安全属性（完整性、保密性、可用性）遭到破坏后数据损失后，影响范围较小（一般局限在本机构），影响程度一般是“轻微”或“无”。

分级方法的实施需要综合考虑数据的多个维度。除了数据的重要性和敏感性外，还应考虑数据的来源、使用目的、传播范围等因素。例如,对于来自不同来源的数据,其分级标准可能有所不同。同时,数据的使用目的也会影响其分级。如果数据仅用于内部决策，

那么其分级可能会相对较低；但如果数据需要对外公开或共享，那么其分级就需要更加严格。

在分级方法的实际应用中，电力交易主体还可以借鉴信息安全领域的风险评估模型。电力交易主体通过对数据的保密性、完整性和可用性进行评估，可以确定数据的风险等级，从而制定相应的分级策略。同时，电力交易主体也可以参考国内外相关法律法规和标准，确保数据的分级符合法律要求和行业规范。

3.3 分级结果

在电力交易数据的分级实践中，根据数据的重要性和敏感性将电力交易数据分为三级，分级示例如表 3 所示。

表 3 数据分级示例

数据大类	子类	参考级别
直接交易数据	交易管理类	3
	合同管理类	3
	计划管理类	2
间接交易数据	业务管控数据	1
	风险管控数据	2
	信用评价数据	2
	电网运行数据	2
第三方数据	市场运营数据发布	1

电力交易数据的分级结果对于实际应用具有重要意义。根据分级原则和方法，我们可以将电力交易数据划分为不同的级别，每个级别对应着不同的数据敏感性和重要性。高级别的数据通常包含更为核心和敏感的信息，如电力交易价格、交易量等，这些数据对于电力市场的监管至关重要。而低级别的数据则可能是一些基础数据，如电力设备的运行状态、电力负荷等，这些数据虽然对于电力交易也有一定影响，但敏感性相对较低。

总之，电力交易数据的分级结果对于实际应用具有重要意义。通过对不同级别的数据进行不同的处理和应用，可以更好地满足不同用户的需求，同时也能够更好地保护数据的安全性。随着电力市场的不断发展和数据技术的不断进步，相信未来电力交易数据的分级处理和应用也将更加精细化和智能化。

4. 电力交易数据分类分级的应用

电力交易数据的分类分级在电力交易、市场监管、数据分析中具有广泛的应用前景和重要的实践价值 [8]。通过科学分类和合理分级，我们可以更加深入地了解电力市场的运行规律和风险状况，为电力交易主体的发用电决策和监管部门的监管提供更加精准、高效的数据支持。

4.1 在电力交易中的应用

数据是经济分析的原材料。在电力交易中，数据的分类分级就是对这些原材料进行精细加工的过程，旨在提取出有价值的信息。电力交易数据不仅涉及庞大的信息量，还包含多种敏感信息，如电价、供需关系、能源类型等。因此，对电力交易数据进行科学分类和合理分级，对于提高交易效率、保障市场公平性和促进能源可持续发展具有重要意义。

以电价数据为例，通过精细分类，我们可以将电价数据划分为不同类型，如批发电价、零售电价、峰谷电价等。这样的分类有助于研究者和决策者更深入地了解电价的形成机制和市场动态。同时，根据数据的敏感性和重要性，可以通过对电价数据进行分级，确保不同级别的数据得到适当的保护和应用。

在实际应用中，我们可以借助数据分析模型，如聚类分析、回归分析等，对电力交易数据进行深入挖掘和分析。这些模型可以帮助我们识别数据中的规律和趋势。例如，通过对历史电价数据的分析，可以对未来电价走势进行预测，为电力交易主体出让或受让电量提供决策参考。

4.2 在电力市场监管中的应用

在电力市场监管中，电力交易数据的分类分级的应用尤为重要。通过对电力交易数据进行科学分类和合理分级，监管机构能够更准确地掌握市场动态，及时发现和应对潜在风险。例如，通过对电力交易数据的分类分析，监管机构可以识别出不同类型电力交易的特点和趋势，从而判断市场供需状况。同时，通过对电力交易数据分级管理，监管机构可以针对不同级别的数据采取不同的监管措施，确保市场运行的公平、公正和高效。

在具体实践中，监管机构通过对电力交易数据进行分类分级，发现某些时段内某些区域的电力交易价格异常波动。经过深入分析，监管机构发现这是由于部分发电企业利用市场供需矛盾，通过操纵交易价格来获取不当利益。针对这一问题，监管机构及时采取了相应的监管措施，包括加大市场监管力度、完善交易规则等，有效维护了电力市场的稳定运行。

此外，电力交易数据的分类分级还有助于提高监管机构的准确性。通过对电力交易数据的综合分析，监管机构可以建立科学的数据分析模型，预测市场走势，为政策制定提供科学依据。

4.3 在电力数据分析中的应用

在电力数据分析中，电力交易数据的分类分级具有至关重要的作用。通过对电力交易数据进行科学分类和合理分级，我们可以更加精准地掌握电力市场的运行状况，为电力交易者主体出让或受让电量的决策提供更加有力的数据支持 [9]。例如，通过对电力交易数据的分类分析，我们可以发现不同电力品种的交易特点和规律，为电力企业的交易策略制定提供参考。同时，通过对电力交易数据的分级分析，我们可以评估电力市场的风险水平，为电力企业的风险管理提供重要依据。

在实际应用中，我们可以借助先进的数据分析工具和模型，对电力交易数据进行深入挖掘和分析 [10]。例如，通过运用聚类分析、时间序列分析等统计方法，我们可以对电力交易数据进行分类和趋势预测，为电力企业的市场预测提供支持。此外，我们还可以结合机器学习、深度学习等人工智能技术，对电力交易数据进行智能分析和预测，提高分析的准确性和效率。

5. 总结

在深入探讨电力交易数据分类分级的过程中，我们发现这一领域具有巨大的潜力和挑战。电力交易数据作为能源行业的重要信息资产，其分类分级有助于提升数据的管理效率 [11]。

通过对电力交易数据的深入研究，我们提出了一套科学、实用

的分类分级体系。在分类方面，我们根据数据的来源、特点和用途，将其划分为多个类别，如直接交易数据、间接交易数据、第三方数据等。每个类别都有其独特的管理和应用价值，为电力市场的各方参与者提供了清晰的数据视图。

在分级方面，我们采用了多层次的评价指标和模型，综合考虑数据的敏感性、重要性等因素，将数据划分为不同的安全等级，如机密数据、内部数据、公开数据等。这不仅有助于保护数据的安全性和隐私性，还能为数据的使用和共享提供明确的指导。

电力交易数据分类分级的应用前景广阔。在电力交易中，电力交易主体通过精细化的数据分类和分级，可以提高交易的透明度和公平性，促进市场的健康发展。在电力市场监管方面，分类分级体系可以为监管机构提供有力的数据支持，帮助其更好地履行监管职责。在电力数据分析方面，分类分级体系可以为分析师提供清晰的数据视图和分析框架，提高分析的准确性和效率。

展望未来，电力交易数据分类分级机制将在能源行业发挥越来越重要的作用。随着技术的不断进步和市场的不断发展，我们相信分类分级体系将不断完善和优化，为电力市场的健康发展提供有力支持。同时，我们也期待更多的行业专家和学者加入这一领域的研究工作中来，共同推动电力交易数据分类分级的发展和创新。

参考文献

[1] 张根周 . 大数据在智能电网领域的应用 [J]. 电网与清洁能源 ,2016,32(6):114-117。

[2] 段云琦 . 基于数据挖掘的电网规划多场景建模研究 [D]. 北京：华北电力大学 ,2018，7-16。

[3] 向德军，周睿，黄志生，等 . 基于混合云计算平台的电力市场交易平台关键技术的研究 [J]. 山东农业大学学报（自然科学版），2021,4:15-20。

[4] 朱海明 . 电力市场分析在电力交易运营中的应用 [J]. 电力设备管理 ,2024(1):269-271。

[5] 梁社潮 , 詹一佳 , 黄昭 . 基于多源数据融合的电力用户多维度信息化分类系统设计 [J]. 电气技术与经济 ,2024(5):288-291。

[6] 周亮 , 张晓娟 , 邱意民 , 等 . 电力数据分类分级方法研究 [J]. 电力信息与通信技术 ,2023,21(4):25-30。

[7] 丁天池 . 电力市场的运营模式探讨 [J]. 电力系统装备 ,2020,4:138-139。

[8] 李莉华，徐志宇，尤鸣宇 . 面向未来智能电网的电力大数据交易 [J], 经营与管理，2018,2:10-16。

[9] 余文辉，吴争荣，钟华赞，等 . 基于电力大数据的用户用电行为分析 [J]. 机电信息，2019,20:18-25。

[10] 鄂宇航，陈飞云 . 基于大数据技术的电力交易平台的研究 [J]. 电力设备管理，2021,3:23-30。

[11] 刘杰 . 智能电网中的电力大数据应用 [J]. 电子技术与软件工程，2018,23:66-70。

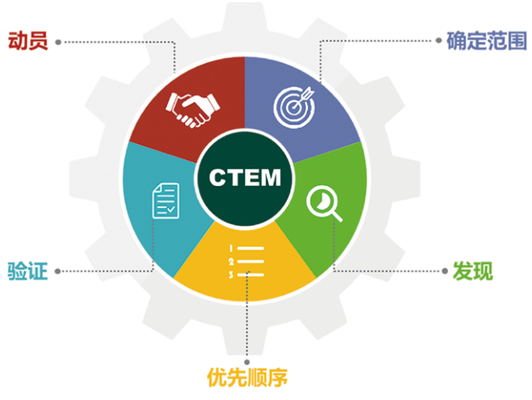
持续威胁暴露管理（CTEM）在国内落地，要避免“水土不服”

绿盟科技 通用领域销售部 尹航

摘要：CTEM 方法指向了更高成熟度的路径，甲方很容易想要一步到位，从乙方购买多种产品、服务来补充自身还不具备的能力，这很容易造成技术能力的堆砌，不但不能解决具体问题，还会带来运营上额外的负担，CTEM 并不是一些单一的技术组合，而是一个经过设计、动态、迭代的过程。

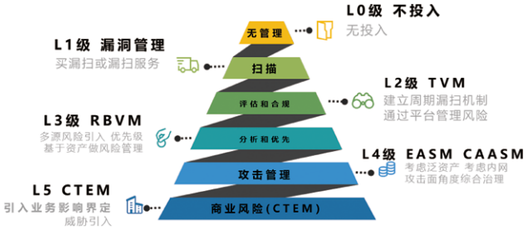
关键词：CTEM 攻击面 攻击路径 漏洞修复

某国际咨询机构 2024 年十大战略技术趋势报告几乎是 AI 的天下，在其中持续威胁暴露管理（Continuous Threat Exposure Management，CTEM）却独树一帜。AI 被认为是颠覆式的创新，能和 AI 技术并列，说明 Gartner 认为 CTEM 极具潜力，但就目前看，也许人们并没有认识到 CTEM 的价值。



CTEM 计划的五个阶段

CTEM 可以看成一个指导安全风险管理者实现更成熟管理目标的方法。近些年，Gartner 提出了多项网络安全风险管理相关技术，比如 TVM（威胁和漏洞管理）、VPT（漏洞优先级技术）、RBVM（基于风险的漏洞管理）、ASM（攻击面管理）。如果给这些技术应用在不同风险管理成熟度做个分级，CTEM 站在最高级别的风险管理成熟度角度，给安全管理者提供攻击和防守完整视角下实施更成熟风险管理方法的路径，管理者可以审视企事业单位自身技术、流程上缺少什么能力、哪些运营环节需要打通。



但是，正因为 CTEM 方法指向了更高成熟度的路径，甲方很容易想要一步到位，从乙方购买多种产品、服务来补充自身还不具备的能力，这很容易造成技术能力的堆砌，不但不能解决具体问题，还会带来运营上额外的负担。在没有了解清楚之前就采取行动，这也是通常企事业单位引入一个先进理念却达不到效果而水土不服的主要原因。

绿盟科技认为，CTEM 方法对甲方的流程管理能力、乙方的技术支撑能力、综合运营能力提出了非常高的要求，落实 CTEM 的过程，并不是一些单一的技术组合，而是一个经过设计、动态、迭代的过程，落实后是否能够达到理想效果，需要根据国内外政策、行业、企事业单位自身情况的不同做出适应性调整。接下来我们就三个最能体现 CTEM 价值的场景，探讨不同场景下如何更好地落实 CTEM 方法。

1. 提升攻击面可见性

网络资产攻击面的可见性，可以理解为：企事业单位现有能力对网络资产风险的管理范围，能够覆盖全部网络资产攻击面的覆盖率。在数字化开始发展的今天，IT 系统供应链条长、开发运营参与角色多、数字资产爆发式增长，多数企事业单位对网络资产攻击面的可见性能力是不足的，这经常会导致被监管单位通报，严重时会造成数据泄露，甚至被实施勒索攻击。

Gartner 提出了一系列攻击面相关的技术，包括三项主流技术：

外部攻击面管理，External attack surface management, EASM

网络空间资产攻击面管理，Cyber asset attack surface management, CAASM

数字风险防护，Digital risk protection, DRP

但是在国内，部分技术适用度不高，需要综合性手段来补充，如 CAASM 需要通过 API 接口全面对接企业云平台、DevOps 工具、安全平台等保存资产信息的系统，以获得资产数据，即便在欧美公有云应用极广的场景下，做得好的乙方厂商也需要达到对接几百种系统的数量级别，在国内软件通用性和数据规范性程度较低的情况下，需要对接的系统数量级是不能接受的，国内厂商更侧重通过融合主动资产测绘技术，形成整体攻击面识别方案。

那么，在国内要怎么提升攻击面可见性能力呢？近些年，国内绿盟科技等领先的漏洞管理厂商已经发生了转变，在漏洞管理平台已经具备很好的内网资产发现和管理能力的情况下，开始融入其他风险评估产品数据，如 EASM、部分 CAASM 能力、供应链管理等，形成了完整的网络空间资产测绘能力。

国内大多数企事业单位已经搭建了自己的漏洞管理平台，在这个基础上逐步向 CTEM 方向演化，提升网络资产攻击面可见性能力，是最低成本取得最大效果的安全建设路线。

当然，多源数据的汇聚，对技术平台提出了更高数据分析要求，包括建立资产范围基线、建立内外网资产对应关系、建立资产关系图谱、资产管理血缘图谱等。

必须指出，网络空间资产梳理是一个持续的过程。CTEM 五个步骤，能够为实现攻击面可见性方面提供很好的指导。在范围阶段，确定企事业单位需要管理的资产基线；在识别阶段，通过技术平台提供的能力分析违规资产带来的风险；在优先级阶段，给出修复清单；在验证阶段，指出关键风险并给出证据；在动员阶段，根据证据指导业务部门的整改。

2. 真正达到验证的目的

CTEM 方法引入了攻击者视角，验证环节是体现攻击视角的核心环节。关于验证，在 CTEM 方法中要达到三个方面的目的：

安全控制能力验证：对于发现的风险，防护体系是否奏效

发现潜在攻击路径：发现关键攻击路径，评估关键业务会受怎样的影响

风险修复有效性验证：评估修复成功率、响应效率

安全控制能力验证，是以验证防护体系在攻击者利用已知风险攻击时是否能够做出有效响应为目的，发现潜在的脆弱点，这需要随着攻击面风险的发现而及时进行验证。国内很多企事业单位都采购过第三方渗透测试服务来进行此类验证，但实际工作中，第三方渗透测试由人工执行，间隔时间长，执行周期长，不能随着风险的发现及时进行验证，不适合应用在 CTEM 五步流程中。这就需要 BAS 这样自动化的验证工具，或者 PTaaS 这样 SaaS 化的轻量级渗透测试服务，能随时调用以完成验证测试工作。

发现潜在攻击路径验证，主要是为了验证新出现的风险可能以哪种方式对关键资产产生影响，便于更好地指导修复动员。这个更多的是基于资产网络分析，勾画出所有到达关键资产的可能路径，这不一定要存在漏洞。国内部分厂商提供了一些工具，能够做到部分能力，但是想要达到攻击路径验证的核心目标，需要完善的资产画像能力，对多种来源的资产数据标签化，以便做到充分的攻击路径分析。

风险修复有效性验证，更偏重管理环节，能力支持方面引入 BAS 工具以及闭环管理流程，国内领先的漏洞管理厂商在漏洞风险闭环管理方面已经具备了这样的能力，随着融合更多的风险数据来源，能够纳入更多风险类型的管理能力。

验证环节会引入多种技术手段，如轻量化的渗透测试即服务 PTaaS、BAS、自动化渗透和红队技术（攻击队，国内更多称为蓝队）。对验证环节真正的挑战，在于如何整合分析和更好地利用这些数据，给修复动员环节带来有价值的参考。

3. 为修复动员提供更多支撑

传统上漏洞修复一直存在两个方面难题，一个是跨部门协调，另一个是工作量持续增长。就国内的实际情况来看，跨部门难题的本质在于安全部门因为“误报”给非安全部门带来更多不切实际的困扰；另外，企事业单位在传统合规驱动下建立的漏洞管理流程，随着漏洞库因时间推移不断积累，以及业务系统数量增长，已经开始让安全相关工作达到极限。

解决漏洞修复问题，不在修复动员环节本身，绿盟科技认为在 CTEM 中更多的是为“修复和态势改善”提供足够的支撑和准备。验证技术能够减少误报，并给安全部门提供足够的依据，以进行跨部门的协调。优先级技术，充分考虑攻击视角下系统面对外部威胁时的真实风险，提供一份安全人员需要处置的短清单，聚焦问题，从而降低工作量。

但是在国内，在面对合规监管场景的时候，优先级技术没有办法打消安全人员可能被通报的顾虑，放心地采用短清单，这需要乙方厂商有足够的行业安全运营经验积累，能够关注监管单位的政策导向，并转化为实际的操作方法，为优先级技术提供可靠的输入，才能有依据地减少合规场景下风险清单的数量。

4. 总结

CTEM 是一个逐步扩展范围而实现安全风险管理成熟度自我提升的方法，可以根据需要扩展技术组件。由于国内缺少安全产品的数据规范，厂商产品之间数据互通能力弱，在考虑乙方厂商时建议选择产品线足够长的厂商，不仅考察厂商是否能够支撑现在需求，也要考虑能否支撑未来的计划。

达到 CTEM 方法的效果不是“买”来的，需要具体到每一个企事业单位的实际情况，评估已经具备了哪些能力，优先补充能够得到快速提升的能力，然后通过持续的安全运营推动五步流程的开展。

最后，CTEM 方法为我们带来的是面向数字化时代繁复多样的资产风险、游刃有余的弹性能力和从海量离散的修复任务中抽丝剥茧厘清脉络的工作方法，从根本上减轻风险管理工作量。CTEM 也从威胁的视角看风险，引领风险管理工作实现从管理 IT 资产到管理泛资产，从漏洞为核心到攻击面风险为核心，从闭环修复到安全控制有效性，从被动响应到主动防御的四大转变。

全视角攻击面管理 常态化构筑安全“第零道”防线

绿盟科技 解决方案销售中心 张铮

摘要：持续开展攻击面管理，有效应对“两高一弱”等专项行动。通过多维度风险主动探测、流量分析被动风险识别、高危漏洞无效化防护、多源风险统一闭环管理等关键技术能力，构建自查自检、高效治理及常态化风险运营结合的管理和技术体系，建立资产、风险、威胁一体化管理的长效机制。

关键词：持续威胁 暴露管理 攻击面管理 两高一弱

随着我国网络和数据安全法律法规颁布实施，各行业单位网络安全建设持续投入，关键信息基础设施和重要业务系统安全防护能力长足发展。但伴随传统安全架构逐步完善、攻防技术逐步升级，安全防护已进入实战化对抗、常态化防御的新阶段，对安全运营能力提出更高要求。违规资产、高危漏洞、高危端口服务和弱口令等低投入、高收益的攻击触点，已成为安全防护“木桶短板”，在引起攻击者关注的同时，更应引起监管单位、系统运营单位的重点关注。

近年来，各行业开展各类风险治理专项行动，“三无七边、两高一弱、一面四方”等抽象术语时常出现在安全工作者案头。其中，2023 年以来，公安部门持续开展专项行动，针对高危端口、高危漏洞和弱口令进行专项治理，制定风险隐患清单，针对各行业单位关键信息基础设施、重要网络系统、门户网站、联网式电子屏等暴露在互联网的“两高一弱”问题清零。同时，各个行业主管部门也在加强“两高一弱”治理行业化要求，针对互联网和内网风险问题形成常态化排查和整改机制。因此，有效收敛攻击面、持续开展风险运营成为考验安全治理基本功的重要科目。

1. 主要思路

全视角、体系化开展攻击面管理，有效管控泛资产泄露，高效治理高危端口、高危漏洞及弱口令，常态化构筑网络安全“第零道”防线。依托多维度风险主动探测、流量分析被动风险识别、高危漏洞无效化防护、多源风险统一闭环管理等关键技术能力，构建自查自检、高效治理及常态化风险运营相结合的管理和技术体系，建立资产、风险、威胁一体化管理的长效机制。

在此，还需赘述攻击面管理定义。Gartner 将攻击面管理定义为：持续地发现、分类和评估组织所有资产的安全性，是人员、流程、技术和服务的有机结合。赛迪顾问在 2022 年发布的《中国攻击面管理市场白皮书》指出，攻击面管理的最大特性就是以外部攻击者视角来审视系统运营单位所有资产可被利用的攻击可能性，而这里的所有资产包含已知资产、未知资产、数字品牌、泄露数据等一系列可存在被利用的风险的资产内容。

此外，按照“目标侦察、武器构建、武器投递、武器激活、木马安装、连续控制、攻击执行”的网络杀伤链来看，作为系统运营者，应首先针对各环节威胁建立合理、对等的防御手段。在“目标侦察环节”，系统运营者更应采取基于攻击视角的攻击面收敛等技术手段，构建网络安全防御第零道防线。

基于全局视角攻击面管理思路，开展“两高一弱”专项治理，通过 SaaS 服务外加本地专业检测能力，完成泛资产排查及攻击触点识别，基于攻击视角、主被动数据融合，动态形成违规资产、两高一弱等风险清单；实战阶段重点开展风险治理，依托平台化工具进行多维度风险关联及闭环管理，针对无法修复的漏洞，通过漏洞无效化等技术手段降低漏洞风险，并引入入侵防御能力评估技术，动态识别攻击路径，确保攻击面有效收敛；常态化阶段通过实施持续威胁暴露管理，系统性构建常态化防御、实战化运营能力。下文将按照各阶段开展技术路径介绍。

2. 风险暴露自查自检

攻击面的有效管理需要以外部视角来审视单位数字资产可能存在的攻击面及脆弱性，重点关注边界处存在被利用的攻击可能性，强调整个系统运营单位资产可能存在的脆弱性，而不仅仅是已知资产和漏洞。此时，首要关心的是资产的外延。数字资产的对象既包括网站域名、数字证书、敏感数据、业务 API、云资产、SaaS 应用、第三方组件等，也包括物联网设备如传感器、摄像头等非传统 IT 资产。其次，不能仅对已知资产进行管理，还要发现并管理未知资产、老化资产、僵尸资产、被遗忘的资产等影子资产；采用包括被动情报、主动探测、人工渗透等多种方式，获取暴露在外的影子资产。最后，要针对新入库的数据进行自动化比对，自动识别并标记老化资产、僵尸资产等各种影子资产。

此外，攻击触点发现与识别是实施攻击面管理的重要能力之一。通过多维度、主被动的自动化安全测试，以攻击者视角绘制完整的资产攻击面。将漏洞、弱口令、不安全配置、敏感信息泄露、暗网监测等多个方面风险整合，并打通弱点与资产、情报、响应间的关系，分析弱点可能产生的风险情况，识别弱点优先级，自动化进行标记和生命周期跟踪。

依托互联网攻击面管理 SaaS 服务，实现未知资产排查、互联网两高一弱发现：通过单位名称、主域名等关键信息，深入排查互联网暴露面，精确识别未纳管资产、影子资产及仿冒资产，并对代码信息、系统设计文档、关键业务信息等泛资产泄露风险实施重点监控。采用高频次、全天候的巡检策略，对高危端口服务、高危漏洞及弱口令进行严密监测，结合高精度人工研判，确保高风险、高敏感异常信息得到及时响应与处理，同时协同业务部门与资产管理部门，形成整改合力，保障两高一弱、泛资产暴露等风险问题源头治理。

工具化落实监管及行业高风险管控技术指标，实现两高一弱内外网风险巡检：按照监管单位、行业主管部门下发的高危端口服务、高危漏洞和弱口令排查整改技术指标，实现扫描工具模板化，针对互联网、内网有关风险“一键排查”；紧跟实战演练步伐，实时关注并应对新型漏洞威胁，如 0day、1day 漏洞，结合资产情况进行超危漏洞专扫，实现攻击面全方位动态收敛。

依托被动流量分析，高精度交叉验证两高一弱风险问题：为了提升风险识别的准确性，依托被动流量分析技术，通过镜像网络出口核心交换流量数据，进行深度剖析，基于网络访问行为信息精确识别高危端口服务、高危漏洞及存活弱口令信息，并与主动扫描结果进行交叉验证，以形成双重保障，有效提高两高一弱风险发现精确度。

3. 攻击触点高效治理

攻击面管理需要专注于对抗本质进行分析和研判，并不是所有的漏洞和风险都需要修复，也不是所有漏洞都具备修复条件，更重要的是，不是所有的漏洞经过一次评估后其危害就一成不变，此外，除了要考虑漏洞自身危害性，扩散范围、可利用性、资产价值等内容外，还要考虑漏洞对于业务的实际影响、利用成本，以及该漏洞是否能构成实现攻击的环节等。

进入实战阶段后，迅速响应自主检查阶段发现的风险或上级监管机构下发的整改要求，有效落实网络安全协防联控要求，开展风险自主治理，并完成闭环管理。在资产关联、风险排查基础上，针对能够整改的风险进行整改加固；针对无法整改的漏洞，漏洞无效化等技术手段降低或消除漏洞被利用的可能性，消除漏洞影响。并通过入侵防御能力评估技术,验证漏洞风险等是否整改到位，确保攻击面有效收敛。

漏洞管理平台完成资产全面梳理、风险快速关联，多源风险统一闭环管理：资产全面梳理，漏洞与资产信息快速匹配，迅速锁定漏洞修复责任人。实施全流程闭环管理策略，将互联网攻击面排查、内网风险巡检、流量被动分析风险识别等多源风险数据统一纳入管理平台进行集中管理，实现从风险发现到整改完成的全过程可视化监控与保障。通过平台化工具调用与快速检验修复成果机制，确保风险治理工作的高效与准确。

漏洞无效化技术，助力消除高危漏洞风险短期无法修复风险：结合资产、业务情况，部分中高危漏洞无法修复，则需要通过漏洞无效化技术，有效屏蔽攻击行为，将漏洞风险进行“模糊隐藏”。依托专业技术工具，基于扫描工具的指纹特征进行识别，自动进行会话阻断，并同时生成自动阻断规则，最终实现基于扫描 IP 的持续生效的阻断指令；基于漏洞维度的精准防护能力，自动匹配资产漏洞及攻击信息，形成针对高危漏洞的自动化防护。

入侵防御能力评估，验证漏洞风险等是否整改到位，确保攻击面有效收敛。通过模拟攻击，将人员、流程、配置、弱点、业务融合,发现攻击点并绘制完整攻击链路。在此基础上,引入流量分析,进一步发现影子资产、僵尸资产，并识别其中可能的 0day 漏洞攻击与未知威胁，绘制更完善的攻击面。

4. 常态化风险运营体系

常态化风险运营体系，穿针引线助力走完产品无法到达的安全最后一公里：围绕“两高一弱”资产与漏洞管理关键要素，开展全类型资产测绘与关联管理、持续风险监测与发现、风险排序与验证、风险修复动员。建设以资产和风险为核心，持续暴露面收敛、持续风险排查、持续攻击视角评估的风险运营体系，系统性构建常态化防御、实战化运营能力。通过常态化风险运营体系建立与持续完善，有效弥补网络安全产品无法触及的安全短板，为网络安全治理提供持续保障。

参考文献

[1] 李庆华 ; 郭晓黎 ; 张锋军 等 攻防对抗视角下的网络安全主动防御体系研究 [J]. 信息安全与通信保密 ,2024(1):77-85。

[2] 梁群 网络空间资产测绘与攻击面管理的技术研究 湖南邮电职业技术学院学报 2022(12):26-29。

[3] Austin Zhao. IDC Innovators: 中国攻击面管理 (ASM) 技术 , IDC#CHC50359923[R]. 北京 : IDC,2023:7。

[4] 赛迪 中国攻击面管理市场白皮书。

CTEM违规资产治理场景技术分析

绿盟科技 企业安全运营产品部 李昀磊

摘要：近年来，随着“三无七边”资产在攻防演习中频繁成为突破口，以及违规搭建系统引发的数据泄露事件屡见不鲜，各行业对违规资产治理的重视程度逐步提升。本文以电网和金融行业为例，总结了三种典型的违规资产治理场景：违规发布业务、互联网违规自建系统以及内网私搭乱建与暗资产。针对每个场景分析了治理中的难点与挑战，并提出了相应的技术解决方案，特别是将流量分析作为资产管理的辅助手段，希望为相关人员提供切实可行的技术思路。

关键词：CTEM 违规资产治理 攻击面管理 流量分析

引言

近年攻防演习中许多突破口出现在“三无七边”资产，因员工或供应商违规搭建系统而导致的数据泄露事件也时有发生，逐渐引起各行业对违规资产治理的重视，并加强相关监管措施。

电网行业中，南方电网明确规定了各类因私自搭设互联网应用导致安全事件的处罚细则，国家电网也明确禁止在第三方云网络或平台部署网站、APP，并鼓励各省公司互相监督。金融行业中，中国证券投资基金业协会发文要求防范不法分子实施仿冒网站、APP 等违法活动，并要求基金公司提升处理能力和效率。当前各主管单位发力整治的“两高一弱”，其高危端口场景也属于一种违规的资产暴露。在合规 / 通报和实战对抗的双重压力下，客户的关注度也明显提高。

本文总结在违规资产治理方面的典型场景、难点和技术思路，尤其是流量分析在资产管理中的应用，供探讨。

1. 典型场景技术分析

1.1 违规发布业务

1.1.1场景说明

互联网暴露面的控制收敛通常是网络安全的第一道防线，规范上线发布流程、评估暴露面风险是安全运营最基础的一项工作。

许多企业经常出现绕过常规上线流程，擅自将业务映射到互联网的情况，这些业务并未经过安全评估，导致暴露面风险失控。

1.1.2治理难点

流程缺少强制性：业务发布需要开发、运维、安全等多部门合作，传统 IT 管理中开发 - 运维的衔接通常以运维分配 IT 资源为卡点实现流程管控，但安全团队往往缺少有效的流程管控手段，工作仅限于事后发现。

感知速度慢：资产稽查一直是安全运营工作的一部分，以期及时发现资产尤其是暴露面的变化，进而控制风险。最主流的方式是主动探测，优点是技术成熟、部署快速、侵入性小、操作简单，缺点是只能以一定频率探测，存在滞后性。而当客户资产量较大或业务健壮性不足时，往往会进一步降低探测频率，难以达到稽查的预期效果。事实上，大部分单位甚至无法每月对互联网暴露面做一次全面检查。

源头定位难：互联网发布可能涉及多次地址、端口映射或反向代理，安全团队在缺少完整网络映射信息时，无法直接定位到最终发布的某个端口 /URL 属于哪个业务，无法第一时间确认并完成遏制，甚至会出现开发团队用反向代理复用已经完成资源申请和发布的 IP、端口的情况，由于不涉及新资源申请，连运维团队也无法掌握其发布情况。

1.1.3技术思路

流量分析辅助识别对外发布：在主动探测发现的基础上，增加流量监控作为暴露面稽查补充手段。借助互联网出口部署的流量探针，我们可以从 HTTP、SSL 等元数据日志中筛选来自互联网的访问日志，将 HTTP 日志的 Host 字段和 SSL 日志的 SNI 字段与合规资产库对比，发现合规范围外的外对内访问行为，其目的资产即为潜在的违规发布业务。

大致逻辑：

UTS: (sip not in 内网 IP 段) and ((http.host not in 合规库) or (ssl.sni not in 合规库))

由于流量相关日志是实时产生和处理的，可以提高发现的及时性。

配置解析关联内外部资产信息：目前客户侧常见的资产映射包括 NAT（如各类防火墙）、负载均衡（如 F5）、反向代理（如 Nginx），以及衍生出的 SSL 网关、反向代理 WAF 等。各类主流产品大多具有 API 或开放配置文件规范，可以查询、分析配置信息进而识别出从互联网边界到内部最终业务主机的多级转发路径。同时搭配扫描探测，从互联网向内发送带有特殊标记的探测请求，通过内网流量探针进一步追踪和验证转发路径。

F5-WAF 多级映射示例

在云环境中，以上各类映射功能几乎都由云平台自身提供，标准化程度更高，未来全面云化甚至基础设施即代码（IaC）大范围应用后，还将进一步提高识别能力。

1.2 互联网违规自建系统

1.2.1场景说明

电网、银行等单位严格要求业务系统仅部署在专用网络中，如自有 IDC、私有云，严格禁止未经允许在公有云、外部 IDC 部署系统，结合互联网收口降低暴露风险。但有的员工、下级单位、合作单位为图方便，擅自将业务部署在外部，导致客户被上级单位通报。

1.2.2治理难点

超出客户网络范围：虽然从上级监管的角度来看，管理责任在客户单位，但从客户单位的角度来看，这些系统并不属于自身资产，客户“被动违规”。技术上，这些系统不在客户网络中、不使用客户 IT 资源、分布范围不定（可能涉及多个公有云、外部 IDC）、关联特征较弱，导致客户安全部门难以发现，也难以判定其违规责任人。

违规人员刻意隐藏：部分违建人员会刻意降低自身系统特征试图隐藏，导致客户安全人员发现的难度进一步提高。但上级单位使用跨单位的排名、考核等手段，让客户各个兄弟单位“卷起来”，相互检举，导致仍有违规行为被挖出通报。

1.2.3技术思路

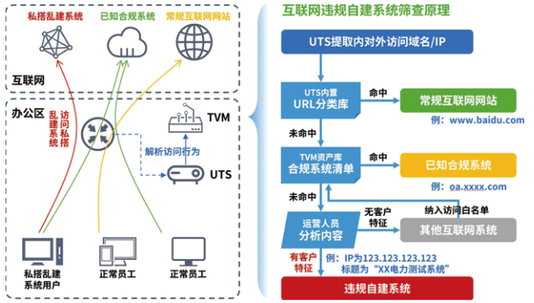
员工或下级单位违规建设系统也是为了自身使用，客户网络中会存在相关对外访问流量。可在客户网络中部署探针监测流量，提取内对外访问日志，过滤掉常规互联网访问和合规行为，剩余访问会话交由运营人员分析判断，识别潜在的违规自建系统。

目前的治理实践中，网站类和客户端类的违规自建系统都存在。

对于网站类系统，其 Web 流量混杂在大量互联网流量中不易分辨，可在 HTTP 日志 host 字段、SSL 日志 sni 字段中提取对外访问的域名，对比知名网站（URL 分类库 / 上网行为管理）、合规库（资产管理平台 / CMDB）、白名单（逐渐积累）等信息逐层过滤掉合理的访问行为，剩余可疑访问活动。

对于客户端类系统，对外访问通常是数据库操作，可用会话日志的目的端口、数据库连接日志识别对外的数据库操作，识别可疑的访问活动。

依此识别的可疑访问活动目标，可利用 HTTP 日志识别网站 Title 和 URL、SSL 日志识别证书主体结合测绘类工具（如扫描器、EASM、第三方测绘平台）提取网站快照，辅助运营人员快速、准确判定违规属性，并利用各类访问日志快速关联到近期访问的内部主机和人员，定位违规责任人。



违规自建系统筛查逻辑

大致逻辑：

UTS: ((dip in 互联网 IP 段) and (dip not in (客户业务互联网 IP 段 or 白名单 or 合规库 or 知名网站 IP)) and (host not in (客户域名 or 白名单 or 合规库 or 知名网站域名)) and (sip in (内网 IP 段 or 客户互联网出口 IP))) or ((dip in 互联网 IP 段) and (dport in (3306,1521,1433,5432,27017)))

同时，网站安全监测中钓鱼网站监测从原理上是发现与客户网站相似的网站，也可作为发现违规自建系统的辅助手段。

1.3 内网私搭乱建与暗资产

1.3.1场景说明

员工在办公网中私自搭建服务，脱离组织的运维和安全管理，引入额外风险。同时，许多单位仅对互联网暴露资产做跟踪管理，内网资产长期未形成有效的管控流程和措施，台账老旧失效，导致许多内网正常系统成为运维和安全团队都不知道的“暗资产”，缺少有效的安全保障，在面对演习等强对抗场景时容易成为内网驻点和跳板。

1.3.2治理难点

办公终端与系统难以区分：常规的主动探测主要针对 IP 地址固定、有开放端口的业务系统。办公网中私搭乱建系统可能与大量办公主机混在相同网段，加之动态 IP 等因素，主动探测效率极低，无法有效识别。而在部分有大量专用系统（如医院的医疗设备）的单位中，出于业务稳定性考虑甚至无法发起探测。

资产量大无台账：许多安全团队资源和精力有限，只能优先管理相对更重要、范围也更小的互联网暴露资产。内网资产量通常远大于互联网资产，在早期 IT 管理不完备的情况下经年累月，运维和安全团队几乎无法建立一份有效的资产台账。

1.3.3技术思路

考虑到大部分系统是 C/S 架构，使用时传输层方向是客户端到服务端，而资产管理主要关注的就是服务端。基于流量探针抓取的元数据日志，可提取源目 IP、目的端口、协议、应用（部分）等信息，关注内对内访问行为的目的 IP 目的端口，默认源为客户端、目的为服务端，并根据协议、应用信息筛除部分不关注的服务（如 NetBIOS），即得到服务端 IP 地址和开放端口服务，可视为内网业务系统做进一步确认和管理。

相对于主动探测，被动流量识别避免了 ACL 干扰、系统稳定性弱、系统数量大等问题，可作为内网资产识别的主要手段。

2. 总结

除上文提到的三种场景外，退网未离网、无主 / 无人运维、终端 Agent 未覆盖等也是违规资产治理的重要场景。要解决这些问题除了用前文讨论的各种方法提高事后发现能力之外，更重要也更基础的是提高资产管理的流程规范性和技术强制力。安全运营中的资产管理本质在解决业务与安全的衔接问题，包含目标、流程、责任、信息的衔接。完善业务开发、测试、上线、运维、下线全过程的资产管理工具链，用技术手段打通 Dev/Sec/Ops 三个团队，避免违规行为的发生，才有可能真正做好资产管理。

安全工作的效果通常依赖于客户上层的管理力度和决心，但客观地说，对于大部分单位这既不现实也不合理。客户更需要的是“七分技术、三分管理”，靠技术创新解决原本只能依赖高成本的管理动作解决的安全问题，才是做好安全运营的唯一路径。

技术与威胁交织：大模型在网络安全中的光与影

绿盟科技 创新研究院 杨博杰

摘要：大型语言模型（LLM）在网络安全领域具有双重作用。一方面，LLM 为安全防御带来了革命性提升，可在代码安全、恶意软件检测和个人信息防护等方面发挥重要作用。另一方面，LLM 也被不法分子利用，成为新的安全威胁。因此，在利用 LLM 加强防御的同时，必须警惕其潜在的恶意应用，采取有效的防御措施，才能构建更安全的数字世界。

关键词：大语言模型 大模型安全 大模型攻击

1. 光与影：LLM 的两面性

在技术的浪潮中，大模型（LLM, Large Language Model）如同双刃剑，在网络安全领域展现出惊人的潜力与挑战。它不仅可以助力安全专家解决代码审计、漏洞挖掘等烦琐任务，也成为黑客实施攻击的有力工具。随着大模型的普及，网络安全的边界正被重新定义：一方面，它为防御提供了前所未有的力量；另一方面，恶意应用却潜伏在阴影中，威胁着数字世界的安全。

2. 光芒闪耀：大模型塑造安全未来

2.1 代码安全

LLM 通过学习大量的代码和示例，能够在软件生命周期的各个阶段提供帮助，包括安全编码，测试用例生成，漏洞检测及修复等。

由于学习了大量的样本代码以及安全最佳实践，基于 LLM 的编程助手能够生成更规范的代码，避免常见的安全漏洞，减少新安全漏洞引入的概率。很多漏洞本质上都是编码不规范引起的（比如内存使用不合理，序列化反序列化不一致等），LLM 对于安全编码规范的遵循可以有效避免这种情况。

将 LLM 用于生成测试用例，是目前安全界探索的一个重要方向。研究表明，相比传统方法，LLM 生成的测试用例有更高的覆盖率，可以更有效的测试软件供应链攻击。模糊测试（fuzzing）是业界广泛使用的生成测试用例以及挖掘漏洞的技术，引入 LLM 辅助后，利用其自然语言理解能力，可以更加高效地生成以及针对性地修改测试用例，提升测试效率和测试覆盖率。

现有的静态代码扫描工具基本都依赖人工维护的规则集，LLM 可以帮助生成和修改相关的规则，减少人工编写和维护的成本。传统工具对代码的语义理解有限，仅能根据规则或者模式匹配来寻找漏洞，而 LLM 可以理解代码，因此，将 LLM 应用在扫描中，可以检测一些更复杂的攻击场景。

Work	Life Cycle							LLM(s)	Domain	When compared to SOTA ways?
	Coding (C)	Test Case Generating (TCG)	Running and Executing (RE)							
			Bug Detecting	Malicious Code Detecting	Vulnerability Detecting	Fixing				
Sandoval et al. [31]	●	○	○	○	○	○		Codex	-	◎ Negligible risks
SVEN [13]	●	○	○	○	○	○		CodeGen	-	◎ More faster/secure
SALLM [73]	●	○	○	○	○	○		ChatGPT etc.	-	-
Madhav et al. [30]	●	○	○	○	○	○		ChatGPT	Hardware	-
Zhang et al. [35]	○	●	○	○	●	○		ChatGPT	Supply chain	◎ More valid cases
Libro [38]	○	●	○	○	●	○		LLaMA	-	◎ Higher FP/FN
TitanFuzz [37]	○	●	●	○	●	○		Codex	DL libs	◎ Higher coverage
FuzzGPT [36]	○	●	●	○	●	○		ChatGPT	DL libs	◎ Higher coverage
FuzzMutRL [73]	○	●	●	○	●	○		ChatGPT	Languages	◎ Higher coverage
WhiteFox [39]	○	●	●	○	●	○		GPT4	Compiler	◎ High-quality tests
Zhang et al. [40]	○	●	●	○	●	○		ChatGPT	API	-
OSATark [41]	○	●	●	○	●	○		ChatGPT	Protocol	◎ Higher coverage
Henrik [12]	○	●	○	●	○	○		ChatGPT	-	◎ Hgier FP/FN
Apostol [14]	○	○	○	○	○	●		NA	-	-
Ajmani [18]	○	○	○	○	●	●		ChatGPT	-	◎ 4X faster
Bakhshandeh et al. [45]	○	○	○	○	●	○		ChatGPT	-	◎ Low FP/FN
Mounika et al. [46]	○	○	○	○	●	○		ChatGPT	-	◎ Higher FP/FN
Cherkhire et al. [47]	○	○	○	○	●	○		ChatGPT	-	◎ No better
LATTE [48]	○	○	○	○	●	○		GPT	-	◎ Cost effective
Sobania[49]	○	○	○	○	●	○		Codex	-	-
Chen et al. [50]	○	○	○	○	●	○		ChatGPT	Blockchain	-
Hu et al. [51]	○	○	○	○	●	○		ChatGPT	Blockchain	-
KARTAL [52]	○	○	○	○	●	○		ChatGPT	Web apps	◎ Less manual
YuhiGhor [53]	○	○	○	○	●	○		LLaMa	Libs	◎ Higher accuracy/speed
Ahmad et al. [54]	○	○	○	○	●	●		Codex	Hardware	◎ Fix more bugs
InferFix [55]	○	○	○	○	●	●		Codex	-	◎ CI Pipeline
Pearce et al. [16]	○	○	●	○	●	○		Codex etc.	-	◎ Zero-shot
Fu et al. [56]	○	○	●	○	●	●		ChatGPT	APR	◎ Higher accuracy
Sobania et al. [57]	○	○	○	○	●	●		ChatGPT etc.	APR	◎ Higher accuracy
Jiang et al. [58]	○	○	○	○	○	●		ChatGPT	APR	◎ Higher accuracy

● The model can enhance the specific facets of data protection.
○ The model can not enhance the specific facets of data protection.

图 1 不同大模型对于代码安全的能力分布

图 1 展示了各个不同的模型拥有的代码安全相关的能力强化，可以看出，目前的 LLM 还是各有侧重，还没有出现涵盖整个软件生命周期的全能型大模型。

2.2 恶意软件检测与分析

恶意软件是现代网络安全中一个重大的威胁，快速且准确地识别恶意软件可以帮助保护系统、数据的隐私和安全。

传统的检测工具常常依赖于静态签名或者特定的规则，LLM 通过学习大量的恶意软件样本，提取常见的恶意代码模式和行为特征，在面对新的变种时，可以帮助安全人员实现更快速和高效的分析。

代码混淆是恶意软件规避检测的主要方法之一，让 LLM 学习大量的反混淆方法后，可以将其用于分析混淆后的代码，判断软件真实意图，并帮助恢复恶意软件的原始逻辑。

LLM 可以整合多个维度的数据进行综合分析，常规的检测手段比如 NIDS（Network-based Intrusion Detection System，网络入侵检测系统）和 HIDS（Host-based Intrusion Detection System，主机入侵检测系统）是相互独立的，LLM 可以处理两边的数据，同时对系统事件和网络流量做分析，更加全面地识别恶意软件运行时的行为，提取特征。

2.3 个人信息防护

网络钓鱼是恶意攻击者常用的手段之一，通过伪造高相似度的网站和电子邮件，欺骗受害者输入敏感信息，从而实现账户盗用等恶意行为。LLM 可以有效识别带有钓鱼内容的网站和钓鱼邮件，保护用户隐私。

PII（Personally Identifiable Information，个人身份信息）检测是隐私泄露检测的一个重要组成部分。常规的检测手段大部分是基于正则匹配或者规则，这些都需要人工维护，容易有遗漏和误报。LLM 拥有强大的上下文理解能力，能结合上下文更好地判断信息是否是 PII。同时，LLM 可以实现跨语言的检测，而不需要为不同的语言配置不同的规则。

3. 暗影侵袭：大模型引发的隐匿威胁

虽然 LLM 带来了许多安全性的提升，但其强大的能力也被用于恶意行为，引发了新的安全威胁。图 2 中紫色框展示了 LLM 可以参与攻击的部分，可以看到在各个维度 LLM 都有可使用的场景。

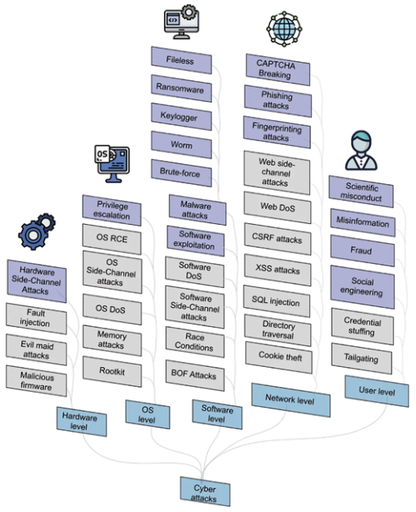


图 2 网络攻击的分类

3.1 帮助实施攻击

虽然 LLM 无法直接访问操作系统或硬件，但它们可以通过分析操作系统信息来协助攻击者实施攻击。研究显示，LLM 能够协助自动化提权攻击，帮助攻击者发现系统漏洞并执行恶意操作。攻击者输入系统信息后，LLM 能够分析系统上存在的漏洞并给出可行的攻击方案。LLM 还可能被用于攻击网络基础设施，模拟和部署复杂的网络钓鱼和中间人攻击。

3.2 编写恶意软件

LLM 拥有强大的编程能力，可以帮助生成恶意软件。直接让 LLM 生成恶意软件通常会被底层的安全措施拦截，但是可以通过拆解软件功能，利用简单的提示生成不同部分的代码，最终生成完整的恶意软件，如勒索软件或网络蠕虫。为了逃避检测，还可以利用 LLM 重写恶意软件代码，经过 LLM 修改的代码可能会改变原有的二进制特征，使其更难以被传统的防病毒软件检测。随着 LLM 生成代码能力的提升，这种恶意应用的风险可能会进一步扩大。

3.3 针对用户的攻击

LLM 生成逼真文本和推理的能力，可以被恶意利用。最常见的应用是社会工程攻击，如钓鱼攻击和信息误导。攻击者可以利用 LLM 分析已知信息，推断受害者的隐私信息；可以生成高度真实的虚假邮件或消息，诱使受害者泄露个人信息或点击恶意链接。此外，LLM 还能被用于生成虚假新闻或不实信息，进一步扩大信息操控的范围。

LLM 在安全领域具有巨大的潜力，但同时也带来了新的挑战。我们需要在利用 LLM 的积极应用的同时，警惕其潜在的恶意应用，并采取有效的防御措施。通过不断地研究和创新，我们可以更好地利用 LLM，为构建更安全的数字世界做出贡献。

参考文献

Yifan Yao, Jinhao Duan, Kaidi Xu, Yuanfang Cai, Zhibo Sun, Yue Zhang, A survey on large language model (LLM) security and privacy: The Good, The Bad, and The Ugly, High-Confidence Computing, Volume 4, Issue 2, 2024, 100211, ISSN 2667-2952.

技术解读 | 软件敏感信息检测工具对比分析

绿盟科技 创新研究院 杨双镇

摘要：本文分析了五种开源和四种专有敏感信息检测工具的精度和召回率，重点讨论了各工具在误报和漏报方面的表现。通过对比实验，发现目前没有一种工具能够同时达到高精度和高召回率，显示出敏感信息检测工具在实际应用中的不足。因此建议开发人员应根据项目需求选择合适的工具，以更好地保护代码库中的敏感信息。

关键词：敏感信息检测工具 代码安全 云上风险

引言

随着软件开发的日益复杂，敏感信息（如 API 密钥和访问令牌）的安全性变得尤为重要。如图 1，根据 GitGuardian 的监测数据，2023 年 GitHub 存储库中的密钥暴露数量较 2022 年增长了 28%，累计泄露超过 1280 万个身份验证和敏感密钥。这一问题不仅威胁到软件的安全性，还可能导致严重的安全漏洞和经济损失。例如，2022 年 9 月，一名攻击者通过利用 Uber 公司 PowerShell 脚本中硬编码的管理员凭证，成功接管了该公司的内部工具和应用程序。

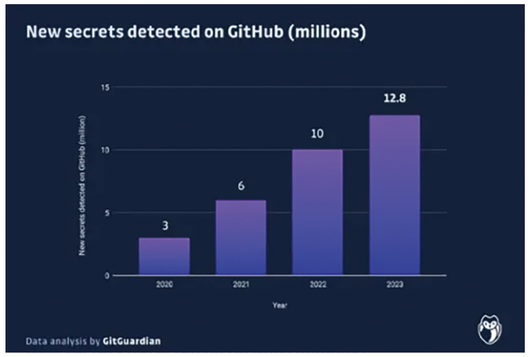


图 1 2020 年至 2023 年 Github 密钥泄露数量

为了应对这一问题，市场上出现了许多开源和专有的敏感信息检测工具，如 Gitleaks 和 SpectralOps 等。然而，这些工具在实际使用中存在许多问题，其中最为突出的是高误报率。误报率过高不仅增加了开发人员的工作负担，还可能导致警报疲劳，使得开发人员忽视真正的安全威胁。

本文介绍《软件敏感信息检测工具比较研究》的相关工作，作者通过对 5 个开源和 4 个专有密钥检测工具进行的实证研究，详细分析了这些工具在精度和召回率方面的表现，揭示了误报和漏报的主要原因。

1. 敏感信息识别的工具比较

1.1 基准数据集

评估软件敏感信息检测工具选择 SecretBench 作为基准数据集。SecretBench 是一个公开可用的软件敏感信息基准数据集，通过 Google Cloud Storage 和 Google BigQuery 访问。该数据集包含从 Google BigQuery 公共 GitHub 数据集中提取的 818 个公共 GitHub 存储库，使用 761 种正则表达式模式来识别不同类型的敏感信息，总计 97479 个被标记为真或假，其中 15084 个是真实的密钥。如图 2，密钥被手动分为八个类别，前三个类

别分别是私钥、API 密钥和认证密钥。

Category	True Secrets	Total Secrets
Private Key	5,789	8,584
API Key and Secret	4,529	5,162
Authentication Key and Token	3,569	5,833
Other	524	66,690
Generic Secret	334	439
Database and Server URL	162	9,970
Password	150	705
Username	27	96

图 2 SecretBench 中的 8 种密钥类型

此外，数据集覆盖了 49 种编程语言和 311 种文件类型，并提供了详细的敏感元数据，如存储库名称、文件路径和提交 ID。如图 3，不同文件类型中敏感数据最多的是 txt 文件、toml 配置文件、js 文件、html 文件与 pem 文件。

File Type	Description	True Secrets
txt	Text File	2,935
toml	Configuration File	1,985
js	Javascript file	1,583
html	Hypertext Markup Language File	1,337
pem	Privacy Enhanced Mail Format File	813

图 3 Top 5 的敏感文件类型

1.2 测试的敏感信息识别工具

根据可访问性、扫描能力、活跃度、标记精度和报告格式五个标准选择了 9 个工具（5 个开源工具和 4 个专有工具）进行敏感信息识别比较。

- 5个开源识别工具

git-secrets 是由 AWS-Labs 开发的开源工具，旨在防止将敏感信息提交到 Git 存储库中。该工具通过扫描整个 Git 历史，检测并输出存储库中的敏感信息。

Gitleaks 是一个用 Go 编写的开源工具，主要用于检测 Git 存储库中的敏感信息。通过使用详细模式扫描存储库，以检索匹配敏感信息的元数据，最后将检测到的结果输出为 JSON 文件，便于后续分析。

Repo-supervisor 是一个用 JavaScript 编写的开源工具，支持通过 webhooks 扫描 GitHub 拉取请求，以及从命令行扫描本地存储库目录。该工具在命令行模式下运行，扫描本地存储库并将结果输出为 JSON 文件。

TruffleHog 是由 Truffle Security 开发的开源工具，用于检测 Git 存储库中的高熵字符串和正则表达式匹配的敏感信息信息。通过启用正则表达式和熵计算标志来扫描存储库，最后将检测结果输出为 JSON 文件，以便进一步分析。

Whispers 是一个用 Python 编写的开源工具，支持 YAML 和 XML 等结构化文本解析格式。该工具将源代码解析为键值对，并检测硬编码的敏感信息，通过使用 whispers 命令扫描存储库，将结果输出为 JSON 文件。

- 4个专有识别工具

Commercial X 是一个专有识别工具，既能够扫描 GitHub 存储库中的敏感信息，还可以检测图像和不可搜索的 PDF 中的敏感信息。该工具支持与 Slack、JIRA 和 Google Drive 集成。作者联系了供应商团队，提供了基准存储库的快照，并接收了扫描报告，最后将报告中的敏感信息和元数据被解析并输出为 CSV 文件。

ggshield 由 GitGuardian 开发，是一个依赖 GitGuardian 公共 API 的开源工具。通过使用详细模式扫描每个存储库，并将检测到的敏感信息输出为 JSON 文件。

GitHub Secret Scanner 是 GitHub 集成的扫描工具。通过在每个存储库中启用“Secret Scanner”设置，工具自动扫描并在“Security/Secret scanning alerts”选项卡下显示检测到的结果，利用 Python 脚本通过 GitHub Rest API 提取每个存储库的敏感信息，并输出为 CSV 文件。

SpectralOps 是一个专有识别工具，提供了开发者、安全和审计三种扫描模式。工具使用“安全”模式扫描存储库，以获得更好的精度和召回率。同样地，将敏感信息的详细元数据与对应扫描结果输出为 JSON 文件。

1.3 工具对比实验与结果

实验中敏感元数据包括 Commit ID、文件路径、行号和纯文本，这些信息能够识别出工具检测到的具体敏感信息的位置及其上下文。标准化文件路径和纯文本敏感信息有助于提高不同工具报告之间的比较精度。

如图 4，不同工具的检测结果不同，为了准确评估敏感信息检测工具的性能，通过 Jaro-Winkler 相似度和 Gestalt 模式匹配算法，计算工具报告的敏感信息与基准数据集敏感信息的相似度，设定相应的相似度阈值，确保高效准确地匹配。

图 4 种不同工具对于相同敏感信息的测试结果

通过对 9 种工具的实验比较，评估其在检测敏感信息方面的精度、召回率和 F1 得分。如图 5 所示，GitHub Secret Scanner 在精度方面表现最佳（75%），但其召回率较低（6%），表明它漏掉了许多敏感信息。Gitleaks 在两种召回率情况下均表现出色（情况 1：86%，情况 2：88%），并且在精度方面也表现良好（46%）。

此外，TruffleHog 在召回率方面表现良好，但精度较低 (6%)。总的来说，没有一个工具同时具有高精度和高召回率，这表明目前的工具在检测敏感信息方面仍存在不足。使用机器学习技术的工具(如 Commercial X 和 SpectralOps)在减少误报方面的表现并不理想，分别只有 25% 和 1% 的精度。

Tool	Precision (Total Alerts, TP)	Recall - Case 1 (TP, FN)	Recall - Case 2 (TP, FN)	F1 Score	ST (min.)	PS
git-secrets	0.05 (94491,4907)	0.04 (671,14413)	0.21 (956,3501)	0.08	6.71	0.92
Gitleaks	0.46 (45932,21047)	0.86 (12954,2130)	0.88 (3901,556)	0.60	46.29	0.85
Repo-supervisor	0.02 (181310,3652)	X	0.17 (751,3706)	0.04	0.32	0.04
TruffleHog	0.06 (90982,5426)	0.31 (4736,10348)	0.52 (2323,2134)	0.11	8.52	0.87
Whispers	0.01 (416516,2448)	0.01 (122,14962)	0.38 (1707,2750)	0.02	0.91	0.00
Commercial X	0.25 (86607,21674)	0.22 (3255,11829)	0.48 (2151,2306)	0.32	X	X
ggshield	0.19 (167046,32277)	0.23 (3536,11548)	0.46 (2068,2389)	0.26	228.94	0.06
GitHub-scanner	0.75 (1721,1292)	0.03 (408,14676)	0.36 (1606,2851)	0.48	54.48	X
Spectralops	0.01 (1547994,4777)	X	0.67 (2979,1478)	0.02	50.03	X
	Highest	Second Highest	Third Highest			

图 5 种工具的准确率、召回率、F1 得分、扫描时间结果

作者对敏感信息检测工具的误报和漏报进行了详细分析，发现工具使用通用正则表达式、无效的熵计算是误报的主要原因。另外，错误的正则表达式、跳过特定文件类型和规则集不足是漏报的主要原因。

2. 总结

本文评估了 9 种敏感信息检测工具在检测代码库中的敏感信息方面的性能。通过对 5 个开源工具和 4 个专有识别工具的比较得出，GitHub Secret Scanner 在精度方面表现最佳，而 Gitleaks 在召回率方面表现突出。当然，不同工具在检测敏感信息方面各有优劣，开发人员应根据具体需求选择合适的工具。例如，GitHub Secret Scanner 尽管精度高，但召回率较低，表明其可能漏掉许多敏感信息。相反，Gitleaks 在召回率和精度之间表现较为平衡，是一个值得推荐的工具。开发人员在选择和使用检测工具时，应根据项目中的具体需求和敏感信息类型综合考虑工具的精度、召回率和功能，通过合理选择和配置这些工具，可以有效地保护代码库中的敏感信息，增强软件开发过程中的安全性和可靠性。

参考文献

https://www.gitguardian.com/files/the-state-of-secrets-sprawl-report-2024.

集散控制系统工控安全研究

绿盟科技 四川代表处 向国勇 重庆代表处 孙德福 解决方案销售中心 马跃强

摘要：随着工业互联网的发展，工业控制系统不再是封闭的信息孤岛，面临的网络安全威胁逐渐增多。集散控制系统 DCS 作为工业控制系统中最重要的控制系统之一，其安全性决定了整个工业控制系统的安全水平。为此，本文以艾默 DeltaV DCS 为研究对象，对其存在的安全问题进行分析，分别从操作系统漏洞、DeltaV 安全漏洞、网络通信脆弱性、安全基线配置、供应链隐患等方面进行研究，研究出艾默生 DeltaV DCS 存在的安全隐患，并给出安全防护建议，对今后提升国家工业安全防护能力、促进工业信息安全产业发展具有重要意义。

关键词：集散控制系统 DCS 漏洞 脆弱性 网络安全

引言

集散控制系统 DCS (Distributed Control System)，其基本思想是分散控制、集中操作、分级管理、配置灵活以及组态方便。作为自动化应用水平重要体现的 DCS 系统，已经在我国电力、化工、石化等行业中得到了广泛应用 [1]。

随着工业互联网的发展，OT 和 IT 的边界不断融合，DCS 的通信系统不再孤立，系统漏洞不断增多，网络安全风险逐渐增大 [2]。DCS 作为工业控制系统中最重要的组成部分，其安全性程度决定了整个工业控制系统的安全水平。研究 DCS 中潜在安全风险及问题对提升国家工业安全防护能力、促进工业信息安全产业发展具有重要意义 [3-4]。

艾默生 DeltaV 系统是全球第四代 DCS 典型代表，具备一体化、智能化等特点；且 DeltaV 系统在我国化工、石化等 DCS 市场长期占据第二名的位置 [5]。因此，本文选择具备技术和市场代表性的艾默生 DeltaV 系统进行研究。

1 . 研究对象介绍

DeltaV 系统是依据基金会现场总线 FF 标准设计的全新控制系统，于 1996 年正式上市，主要应用于流程行业，如化工、医药等。现在我国主流版本为 2014 年推出的 V13 版本、2018 年推出的 V14 版本和 2022 年上市的 V15 版本。

DeltaV 主要由工作站、通信网络、控制器和 I/O 卡件 4 个部分组成 [6]。

（1）工作站

DeltaV 工作站分为 4 种：主工程师站、工程师站、操作员站和应用工作站。其中，主工程师站在 DeltaV 系统中有且只有一个，系统的所有控制策略都通过主工作站传输到 DeltaV 系统的各个节点。

应用工作站可作为历史数据库服务器、OPC 服务器或 WEB 服务器，通常通过第三块网卡实现系统对外通信。

（2）通信网络

工业控制网络，工作站及控制器间由冗余的高速以太网连接。

现场仪表通信，包括 HART、FF、Profibus-DP 等总线。

系统对外通信：以 OPC 为主，数据库通信为辅。

（3）控制器

DeltaV 控制器用于管理 I/O 卡件、控制策略等。

（4）I/O 卡件

卡件分为两类：一类是传统 IO 卡件，可连接常规数字量、模拟量信号；另一类是现场总线卡件，可连接基于 FF、Profibus DP、AS-i、DeviceNet 及 RS485 串口通信的仪表。

2. DCS 脆弱性分析

本文依据《GB/T 33009.4-2016 工业自动化和控制系统网络安全 集散控制系统（DCS）第 4 部分：风险与脆弱性检测要求》作为整体研究框架，结合重点问题进行分析 [7-10]。

2.1 操作系统安全漏洞

根据研究发现，DeltaV 工作站和服务器操作系统，先后支持 Windows XP /Server 2003 组合，Windows 7 /Server 2008 组合，从 DeltaV v13.3.1 之后，支持 Windows 10 IoT Enterprise LTSB 2016 或 LTSC 2021、Windows Server 2016 64-bit 或 Server 2022。

由于 DeltaV 系统的使用寿命可长达几十年，导致众多在运老版本操作系统，都无法得到微软官方的安全支持，如 Windows XP 和 Windows7，微软分别于 2014 年 4 月 8 日和 2023 年 1 月 10 日结束对其支持。然而，Windows7 等老旧操作系统在 DeltaV 在运系统中的保有量依然巨大，Windows7 再现“永恒之蓝”级漏洞的风险依旧高企，DeltaV 将持续面临威胁和挑战。

2.2 DelatV 安全漏洞

通过梳理 CNNVD（国家信息安全漏洞库）、CVE（通用漏洞披露）及相关行业研究报告，对艾默生 DeltaV DCS 漏洞进行统计和分析，有如下信息：

漏洞数量：DeltaV 共暴露出 25 个漏洞（见表 1），其中 2022 年，DeltaV 新增漏洞 6 个。

表 1 DeltaV 漏洞统计

序号	CNNVD编号	CVE编号	漏洞类型	漏洞级别
1	CNNVD-202206-2914	CVE-2022-30260	数据伪造	高危
2	CNNVD-202206-2913	CVE-2022-29965	加密问题	中危
3	CNNVD-202206-2915	CVE-2022-29964	信任管理问题	中危
4	CNNVD-202206-2916	CVE-2022-29963	信任管理问题	中危
5	CNNVD-202206-2918	CVE-2022-29962	信任管理问题	中危
6	CNNVD-202206-2922	CVE-2022-29957	访问控制错误	高危
7	CNNVD-202112-2093	CVE-2021-44463	代码问题	高危
8	CNNVD-202112-2097	CVE-2021-26264	访问控制错误	中危
9	CNNVD-201901-433	CVE-2018-19021	权限许可和访问控制	中危
10	CNNVD-201808-562	CVE-2018-14797	代码问题	高危
11	CNNVD-201808-563	CVE-2018-14795	路径遍历	高危
12	CNNVD-201808-565	CVE-2018-14793	缓存区错误	高危
13	CNNVD-201808-564	CVE-2018-14791	权限许可和访问控制	高危
14	CNNVD-201905-587	CVE-2018-11691	信任管理问题	超危
15	CNNVD-201611-704	CVE-2016-9345	提权问题	中危
16	CNNVD-201611-705	CVE-2016-9347	其他	中危
17	CNNVD-201405-453	CVE-2014-2350	信任管理问题	低危
18	CNNVD-201405-452	CVE-2014-2349	权限许可和访问控制	中危
19	CNNVD-201303-143	CVE-2012-4703	资源管理错误	中危
20	CNNVD-201209-727	CVE-2012-3035	缓冲区错误	中危
21	CNNVD-201205-322	CVE-2012-1818	权限许可和访问控制	高危
22	CNNVD-201205-321	CVE-2012-1817	输入验证	中危
23	CNNVD-201205-320	CVE-2012-1816	缓冲区溢出	中危
24	CNNVD-201205-319	CVE-2012-1815	SQL注入	高危
25	CNNVD-201205-318	CVE-2012-1814	跨站脚本	中危

（2）漏洞级别：参考 CNND 的漏洞级别划分方式，漏洞从高到低可分为四个危害等级，即超危、高危、中危和低危级别。按照漏洞级别统计，DeltaV 包括超危漏洞 1 个、高危漏洞 9 个、中危漏洞 14 个和低危漏洞 1 个，如图 1 所示：

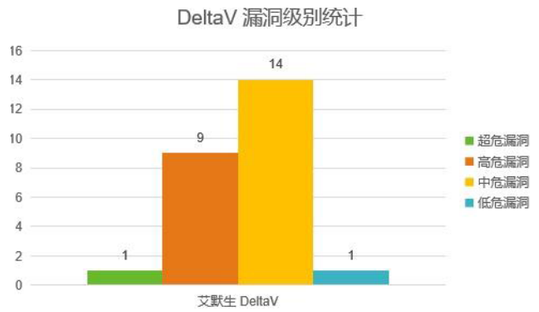


图 1 DeltaV 漏洞级别统计

（3）漏洞分类：参考 CNNVD 的漏洞分类方式，按照漏洞类型统计分析，主要存在信任管理问题、访问控制错误、缓冲区错误、权限许可和访问控制等类型漏洞，如图 2 所示：

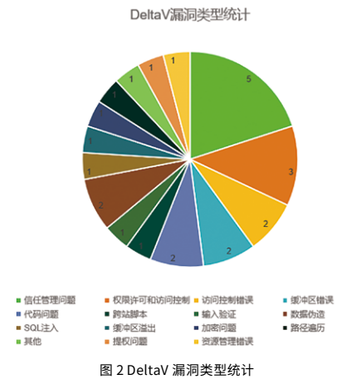


图 2 DeltaV 漏洞类型统计

攻击者可以利用这些漏洞进行拒绝服务攻击、重放攻击、中间人攻击等。2018 年 ICS-CERT 报告称 [11]，攻击人员可利用栈缓冲溢出漏洞 CVE-2018-14793，在目标网络中横向移动并可任意控制其他 DeltaV 工作站。2022 年 6 月 Forescout 发布的“冰瀑漏洞”工控安全报告 [11] 披露了 DeltaV 新增 6 个重大工控漏洞，这些漏洞表明：DeltaV 持续存在不安全设计问题。

本文只对已知 DeltaV 漏洞进行了相关分析，由于 DCS 系统的相对封闭性，潜在的漏洞问题并未得到披露，因此被忽视并继续使用。

2.3 网络通信脆弱性

DeltaV 系统对外通信，主要通过 DeltaV 应用工作站的 OPC 软件，如 OPC Event Sever、OPC History Sever、OPC Data Access Server 等，使用 OPC 协议，包括 OPC Classical 和 OPC UA 协议。目前只有 DeltaV V14 版本及以上支持 OPC UA 协议，其余 DeltaV 版本只支持 OPC Classical。

研究发现，OPC Classic 协议基于 COM/DCOM 技术开发，实质上是基于 TCP 的 DCERPC 通信，所以，如果利用 Wireshark 软件查看 OPC Classic 报文，Wireshark 会显示通信协议为 DCERPC，并非显示为 OPC Classic。

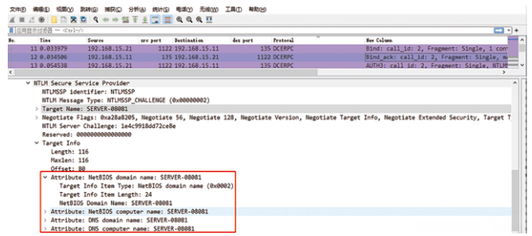


图 3 读取 OPC server 地址

由于 OPC Classic 设计时只考虑到通信的实时性、稳定性，导致 OPC Classic 安全性极差：采用明文传输、缺乏足够强度的认证或授权措施等。在分析 OPC Classic 报文时，可任意读取 OPC Classic 通信信息。如图 3 所示，读取 OPC server 地址。

2.4 安全基线配置弱

由于编程工程师缺乏网络安全防护意识，在 DCS 系统配置及编程过程中，对安全配置往往不予考虑，这样直接导致 DCS 安全配置基线薄弱，给攻击者带来了便利。例如：工程实施人员为了快速完成工程上线，在对 DeltaV 移动端的测试和调试时，不使用证书颁发机构的签名证书，转而使用 DeltaV 生成的自签名证书，由于自签名证书可由任何人生成，WEB 浏览器等客户端无法验证此类证书的真实性，增加了 DeltaV 的暴露面。如图 4 所示：

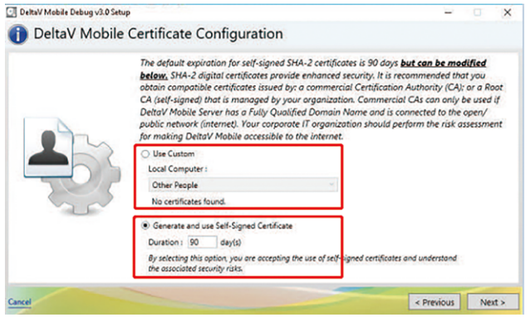


图 4 DeltaV 使用自签名证书

2.5 供应链隐患

俄乌冲突以来，以美国为首的西方国家，将基础软硬件及关键行业应用的供应武器化，对俄罗斯实行全面断供，俄乌冲突再次证明，大国必须建立独立自主的供应链体系。

据 2019 数据 [5] 统计，艾默生占据国内 16% 的 DCS 市场，市场排名第二，是我国主要的 DCS 供应商之一。DeltaV 母公司艾默生作为一家美国公司，在当下贸易全球化趋冷和中美摩擦加剧的背景下，供应链正受到冲击，系统性风险陡升。

DCS 作为工业自动化核心系统，一旦出现供应链问题就会造成严重的工业损失，甚至危害国家安全。

3.DCS 安全问题验证

3.1 验证环境搭建

本次基于工业和信息化部电子第五研究所工控实验室的 DeltaV 系统进行安全问题验证，网络拓扑如图 5。

具体配置详情如下：

DeltaV 应用工作站 1：操作系统为 Windows 7 专业版 SP1。

DeltaV 应用工作站 2：操作系统为 Windows 7 专业版 SP1、安装 OPC Data Access Server。

数据采集 PC1：安装 kepserver。

数据采集 PC2：安装 kepserver。

攻击 PC1：操作系统 CentOS 6.10、安装 python3.7.0、MS17-010 攻击脚本。

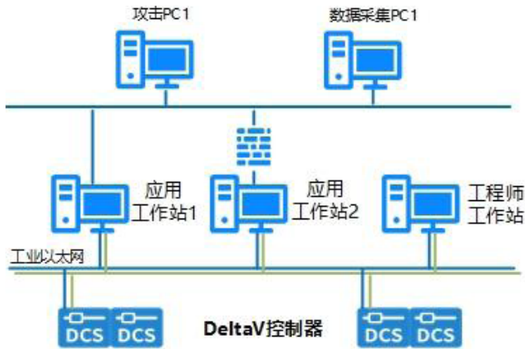


图 5 验证环境拓扑

3.1 操作系统脆弱性验证

验证原理：利用永恒之蓝 Windows SMB 远程代码执行漏洞（CVE-2017-0144）（MS17-010）对无防护的 Windows7 进行攻击，致使业务中断。

验证过程：

第一步：在攻击 PC1 上执行 MS17-010 攻击脚本，向应用工作站 1 的 IP 进行攻击，导致应用工作站 1 蓝屏及死机。永恒之蓝是 2017 年席卷全球的勒索软件的罪魁祸首，是微软近些年来最为严重的远程代码执行漏洞，可以直接获得系统权限，并以此开展破坏行为。

第二步：在应用工作站 2 与攻击 PC1 间部署工业防火墙并引用入侵防护模板，如开展应用工作站 2 的 MS17-010 补丁升级工作，也可完成相关验证工作。

修改攻击地址为应用工作站 2 的 IP，执行攻击脚本进行攻击，PC2 无蓝屏现象，见图 6，在工业防火墙日志审计 - 入侵防护日志中可以查看到阻断日志信息，见图 7。

图 6 DeltaV 应用工作站 2 无蓝屏

图 7 工业防火墙拦截记录

验证结论：系统未及时升级或边界无防护，极易造成 DCS 遭受操作系统漏洞攻击。

3.2 通信协议脆弱性验证

验证原理：DeltaV 13.3.1 中 OPC Data Access Server 基于 OPC Classic 开发，该协议缺乏强度足够的认证、加密或授权措施等，易被劫持和修改指令、业务数据泄露。

验证过程：

第一步：完成 DeltaV OPC Data Access Server 基础配置，将应用工作站 2 选定为“OPC Data Access Server and OPC Mirrior”，如图 8 所示，与数据采集 PC1、数据采集 PC2 建立通信。

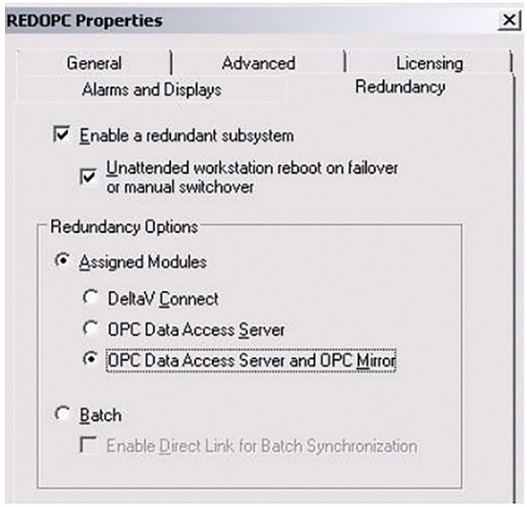


图 8 OPC 功能配置

第二步：通过 wireshark 工具对 DeltaV 应用工作站 2 通信报文抓包，获取到通信中的明文数据，如读取用户名密码、动态端口信息等。

（1）允许匿名登录：因为较低的身份认证、授权安全机制，允许允许匿名登录，攻击者只要满足 OPC Classical 协议报文规则，即可与 DeltaV 应用工作站建立通信，同时攻击者拥有最大操作权限，如图 9。

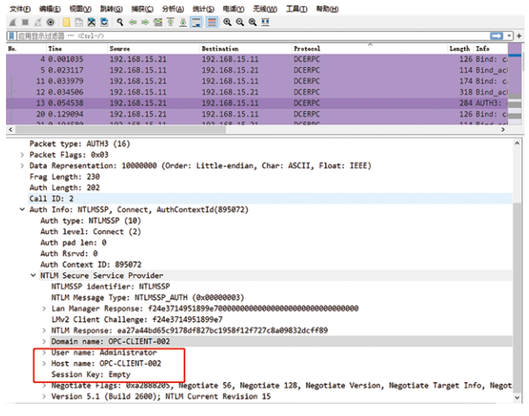


图 9 允许匿名登录

（2）动态端口信息读取：OPC Classic 需进行动态端口通信，如图 10，完整通信内容如下：

OPC 客户端使用 1122 作为源端口首先向 OPC 服务器的 135 端口发起连接，连接成功后再经过 OPC 服务器分配新端口 1034，并通过接口 ISystemActivator 的方法 RemoteCreateInstance 的应答报文返回给客户端，之后客户端使用 1123 作为源端口向服务器的 1034 端口发起新的连接用来后面的真正数据的传输。

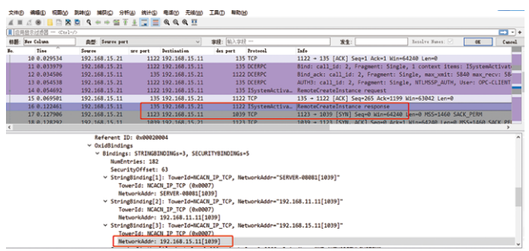


图 10 动态端口显示明文传输

（3）同用户名的多 Client 同时连接：使用 OPC Classical 时，所有的 Client 端会使用相同的用户名和密码进行通信，这样虽然提高了信讯的便捷性，但也增加了信息泄露的风险。图 11 为数据采集 PC2 与应用工作站 2 的通信信息，结合图 10 分析，证明了多 Client 端可以使用相同的账号和匿名登录方式，与同一 Server 端通信。

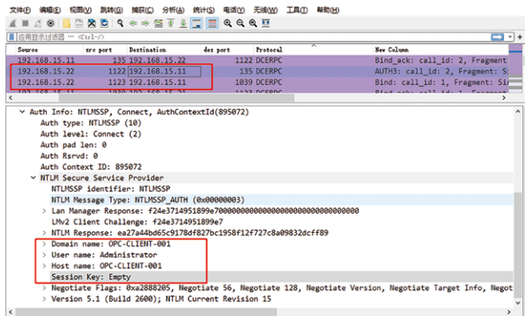


图 11 同用户名的多 Client 连接

验证结论：DeltaV V14 版本之前所有 OPC 类产品，缺乏强度足够的认证、加密或授权措施等，易被劫持和修改指令、业务数据泄露，需要及时升级或采取防护措施。

4. 安全建议

单一的安全产品或技术并不能有效地保护 DCS，需要结合技术和管理两个维度，建立纵深防御体系。为了高效实施纵深防御策略，需要重点关注以下五点。

4.1 供应链管理

运营者在采购 DCS 时，应当遵循《中华人民共和国网络安全法》《网络安全审查办法》等法律法规，开展网络安全审查工作，落实关键信息基础设施的供应链安全工作。我国政府对网络安全审查也极为重视，如：2023 年 3 月 31 日，网络安全审查办公室开启了对美国最大的电脑存储芯片生产商美光公司（Micron）在华销售的产品实施网络安全审查工作 [17]。

突破国外技术封锁，实现自主可控，不仅源于技术和商业需求，而且在中美两国科技博弈背景下，自主可控的需求越发强烈。建议运营者在选购时，关注国产自主可控 DCS，降低供应链风险。

4.2 漏洞及补丁管理

漏洞管理包括 Windows 漏洞和 DCS 系统漏洞，实际上，由于 DCS 系统稳定、配置固定、升级验证烦琐，现场很少进行系统升级，须转变这种工作思路，提升员工工控安全意识，加强工控安全管理制度的落实，对漏洞补丁进行安全评估和测试验证后，应及时完成系统的升级。

4.3 DCS 配置基线管理

基线配置管理，可以说是 DCS 防护的第一道防线，须充分利用好 DCS 自身的安全防护能力，完善安全配置管理，才能有效减少风险暴露面，涉及操作系统、网络设备、安全设备、控制器等。

常见策略包括：（1）应遵循最小安装及配置的原则，仅安装必需的组件、仅开放必要的端口；（2）及时完成相关配置的备份管理工作；（3）账户配置管理：账户强度、更换周期等；（4）移动介质管理；（5）关闭不安全配置。

4.4 部署工控安全产品

工控安全防护产品，是为了满足工业控制系统特殊环境的专属网络安全产品，可以有效降低工业控制系统安全风险。在部署工

控安全产品之前，须开展兼容性测试等措施，确保其不会对 DCS 运行的可用性、实时性、可靠性造成任何负面影响。

DCS 系统常用工控安全产品如下：

（1）恶意代码防护软件：加装恶意代码防护软件，如基于“可执行程序白名单”的理念主机白名单软件，相对于杀毒软件，更适应 DCS 这种封闭工业环境，不用频繁升级。

（2）工业防火墙：具备访问控制、动态端口防护、工业协议深度解析等防护功能；且具备导轨式、无风扇、工作温度 -40° C 至 70° C、抗电磁辐射、抗震动等物理特性。

（3）工业审计：旁路部署，建立工业网络通信行为基线，识别安全风险。

4.5 建立安全管理体系

应从组织机构、管理制度、人员管理、系统建设、运维管理多个维度落实安全管理要求。定期开展工控安全检查评估、考核评价、培训等工作。

5. 总结

本文通过对艾默生 DeltaV 的安全问题研究，总结出艾默生 DCS 主要存在操作系统漏洞、DeltaV 安全漏洞、网络通信脆弱性、安全基线配置弱、供应链隐患五个方面的问题，针对安全问题，进行了安全研究，并给出安全建议，对今后 DCS 安全防护提供了理论指导。

参考文献

[1] 冯伟 . 我国工业控制系统面临的信息安全挑战及措施建议 [J]. 信息安全与技术 ,2013,3（02）:120-124。

[2] 陶耀 , 东李强 , 李宁 . 工业互联网的安全挑战及应对策略 [J]. 中兴通讯技术 , 2016,22（05）:36-41。

[3] 邱金龙 . 工业控制系统信息安全的未来趋势 [J]. 信息与电脑 ,2016（04）。

[4] 夏春明 , 刘涛 , 王华忠 , 吴清 . 工业控制系统信息安全现状及发展趋势 [J]. 信息安全与技术 ,2013,26（14）:28-31。

[5] 华经情报网 .2019—2025 年中国 DCS 控制系统市场运行态势及行业发展前景预测报告 [R].2019。

[6] 王畅 . 艾默生 Deltav 系统作用下自动化升级研究 [J]. 中国石油和化工标准与质量 ,2022,10:26-28。

[7] 马跃强 , 杨盛明 , 韩儒剑 , 杨涛 , 曹旭 . 可编程控制器(PLC）的安全问题研究 [J]. 工业信息安全 ,2022,6（3）:126-128。

[8] 赵峰 , 马跃强 . 基于等保 2.0 工业控制系统网络安全技术防护方案的设计 [J]. 网络安全技术与应用 ,2020,13（5）:117-120。

[9] 王旭 .DCS 安全可靠运行问题的探讨 [J]. 中国仪器仪表 ,2020,9:56-59。

[10] 张雄杰 , 曹旭 , 周金鹏 . 智慧城轨车载网络安全防护解决方案 [J]. 工业信息安全 ,2022,6（3）;86-88。

[11] 安全内参 . 艾默生工作站爆严重漏洞 [EB/OL].https://www.secrss.com/articles/4817。

揭开IEC 62443系列标准的神秘面纱

绿盟科技 服务交付能力部 尹亮 郭涛

摘要：IEC 62443 是一套针对工业自动化和控制系统网络安全的国际标准，旨在降低工控网络安全风险的发生及其影响。该系列标准的制定始于 2005 年，得到了广泛的认可和应用，成为国际上通行的工控网络安全标准。涵盖了组织政策、程序、风险评估以及硬件和软件组件的安全性，为构建更安全的工业基础设施提供了全面的指导。总的来说，IEC 62443 系列标准为工业自动化和控制系统的网络安全提供了一套全面而灵活的框架。

关键词：IEC 62443 IACS 工控安全 程序 组件

1. 制定背景

1.1 工控系统的现状和发展

工业自动化和控制系统（Industrial Automation and Control Systems，简称 IACS）是指由计算机技术与工业过程控制部件（控制器、传感器、执行器和外围电路等）组成的系统（简称工控系统）。这些组成部分通过工业通信网络，按照一定的通信协议进行连接，形成一个具有自动控制能力的工业生产制造或加工系统。通常包括监控和数据采集（SCADA）系统、分布式控制系统（DCS）和可编程逻辑控制器（PLC）以及其他控制系统。

工控系统是工业生产的核心组成部分，超过 80% 涉及国计民生的关键基础设施依靠工控系统来实现自动化作业。工控系统初期并未考虑大规模联网通信，不同厂商之间的工控协议不同，且协议并不完全公开，未形成标准化。随着工业 4.0、工业互联网、智能制造等战略的提出，原来封闭的工控系统逐渐走向互联互通，网络边界逐渐模糊。自伊朗“震网”事件打开“潘多拉”魔盒以来，工控安全事件频发，可以说二进制数据也有核弹一样的威力。

1.2 IEC 62443 的起源和演进

IEC 62443 是工控系统网络安全的基石。

2005 年，国际自动化学会 ISA 成立了 ISA99- 工业自动化和控制系统安全委员会，负责制定工控系统的网络安全标准。

2007 年，ISA99 与 IEC/TC65/WG10 成立联合工作组，共同制定并陆续发布 ISA/IEC 62443 系列标准。

2018 年年底，联合国欧洲经济委员会（UNECE）在其年会上确认，将把广泛使用的 ISA/IEC 62443 系列标准纳入其即将推出的网络安全共同监管框架（CRF）。CRF 将作为联合国在欧洲的官方政策立场声明，为欧盟贸易市场内的网络安全实践建立一个共同的立法基础。

随后，IEC 62443 系列标准逐渐成为国际通行的工控网络安全标准，并在不同工业行业和领域实现了应用。

1.3 IEC 62443 的范围和目的

IEC 62443 是在国际上被广泛采纳和认可的标准，旨在降低部署和操作工业自动化和控制系统的风险。

IEC 62443 的适用范围包括那些使用自动化的或远程被控制监控的资产，读者包括所有的 IACS 用户、生产者、供应商、政府组织、工控系统实践者和安全实践者。

IEC 62443 系列标准提供了一个清晰、灵活且全面的框架，提出了对 IACS 的软硬件的技术要求，同时为确保 IACS 的安全性、完整性、可用性和保密性，对其所需的人员和流程也做出了规定，以实现网络安全和功能安全的融合。

2. 内容解读

2.1 标准框架

图 1 IEC 62443 系列标准框架

随着 IEC 62443 的持续发展，该系列标准有多种标准框架，图 1 是最常见的标准框架。IEC 62443 的名称是工业通信网络 网络和系统安全，IEC 62443 共分为 4 个部分 12 个标准。第一部分是通用标准，是其他标准的基础；第二部分是策略和规程，针对用户网络安全能力的要求；第三部分是系统级的措施，针对服务提供商保护系统所需的技术性网络安全要求；第四部分是组件级的措施，针对制造商提供的单个部件的技术性网络安全要求。IEC 62443 系列标准通过四个部分涵盖了所有的利益相关方，即资产所有者、系统集成商、组件供应商，以尽可能地实现全方位的安全防护 [1]。

IEC 62443-1 是第一部分，包括三个文件，描述了 IACS 网络安全通用方面的内容，如术语、概念、模型、缩略语、系统符合性度量及工控设备的安全生命周期。

IEC 62443-2 是第二部分，包括四个文件，详细规定了 IACS 安全管理体系的要求、安全管理体系实施指南、IACS 环境中补丁更新管理以及对资产所有者和服务提供商的安全程序要求。

IEC 62443-3 是第三部分，包括三个文件，提供了系统安全要求、安全等级和安全风险评估以及系统设计的基本指导和原则。包括将整体 IACS 设计分配到各个区域和管道的方法，以及安全等级的定义和要求。

IEC 62443-4 是第四部分，包括两个文件，提出了针对制造商提供的单个部件的技术性网络安全要求。它包括系统的硬件、软件和网络部分，以及当开发或获取这些类型的部件时需要考虑的特定技术性网络安全要求。

2.2 等同采用

IEC 62443 是在国际上被广泛采纳和认可的工控系统标准，我国已将表 1 所示标准等同采用并转化为国家标准，归口部门为全国工业过程测量控制和自动化标准化技术委员会 SAC/TC124。这些标准涵盖了工业通信网络 网络和系统安全的术语、概念和模型，

程序过程，补丁管理，服务提供商的安全程序要求，系统安全技术，设计评估以及组件的安全技术要求等方面。我国等同采用 IEC 62443 系列标准，标志着国内工控安全领域的标准化工作与国际先进水平保持同步。这不仅有助于提升国内工控系统的安全性能，也为我国工控安全产品的国际交流与合作奠定了坚实的基础。

表 1 IEC 62443 系列标准国标等同采用情况

序号	IEC 62443 标准名称	国标等同采用名称	备注
1	IEC/TS 62443-1-1:2009	GB/T 40211-2021《工业通信网络 网络和系统安全 术语、概念和模型》	
2	IEC 62443-2-1:2010	GB/T 33007-2016《工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序》	
3	IEC TR 62443-2-3:2015	GB/T 42445-2023 《工业自动化和控制系统安全 IACS 环境下的补丁管理》	
4	IEC 62443-2-4：2015	GB/T 40682-2021 《工业自动化和控制系统安全 IACS 服务提供商的安全程序要求》	
5	IEC/TR 62443- 3 -1：2009	GB/T 40218-2021《工业通信网络 网络和系统安全 工业自动化和控制系统信息安全技术》	
6	IEC 62443-3-2：2020	GB/T XXXXX-XXXX《工业自动化和控制系统信息安全 系统设计的安全风险评估》	征求意见稿
7	IEC 62443-3-3:2013	GB/T 35673-2017《工业通信网络 网络和系统安全 系统安全要求和安全等级》	
8	IEC 62443-4-2:2019	GB/T 42456-2023 工业自动化和控制系统信息安全 IACS 组件的安全技术要求	

IEC 62443-1-1 工业通信网络 网络和系统安全 术语、概念和模型

IEC 62443-1-1 的主要内容是定义工控系统的基础概念，以确保在讨论和实施与工控系统网络安全相关的措施时，所有利益相关方都有共同的理解基础 [2]。本标准对工控安全相关的一百多个名词进行了解释，介绍了整个 IEC 62443 系列标准所使用的基础概念和模型，给出了 IACS 的概念模型、资产模型和安全域模型。特别是五层防护模型的提出，为安全防护体系的建立打下了坚实的基础。

IEC 62443-2-1 工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序

IEC 62443-2-1 的主要内容是建立网络安全管理体系，并且持续监测和改进体系。本标准规定了如何在 IACS 中建立网络安全管理体系，并且提供了如何开发这些元素的指南 [3]。本标准中描述的 CSMS 中的元素主要是政策、过程、规程以及与人员相关的内容，描述了在组织范围内最终的 CSMS 将要包括或应当包括哪些内容。

IEC 62443-2-3 工业自动化和控制系统安全 IACS 环境下的补丁管理

IEC 62443-2-3 的主要内容是建立 IACS 环境中的补丁更新管理程序。本标准定义了补丁的生命周期状态和状态模型，包括可用、测试中、未认可、不适用、已认可、发布等阶段以及状态之间的转换，明确了资产所有者和产品供应商在补丁更新中的工作分工，推荐了一种定义好的交换补丁信息（VPC）格式用于补丁的部署和安装等活动 [4]。

IEC 62443-2-4 工业自动化和控制系统安全 IACS 服务提供商的安全程序要求

IEC 62443-2-4 的主要内容是 IACS 服务提供商可以向资产所有者提供的一系列安全能力要求。资产所有者可以使用本标准向服务提供商要求特定的安全能力，服务提供商必须确保在自动化解决方案中（包含在控制系统产品中或单独添加到自动化解决方案中）支持这些措施 [5]。本标准明确了 IACS 集成服务提供商和

维护服务商提供安全能力时的工作分工，定义了四级安全能力、十二个功能域以及它们之间的映射关系，为 IACS 服务商提供了全面的安全能力要求。

IEC 62443-3-1 工业通信网络 网络和系统安全 工业自动化和控制系统信息安全技术

IEC 62443-3-1 的主要内容是确定了若干类可用于保护 IACS 网络的工具、对抗措施和技术。这些建议的措施和技术旨在增强网络的安全性，以防止或减缓网络攻击和其他安全威胁的影响 [6]。本标准包括六类条款，分别是鉴别与授权技术、过滤 / 阻塞 / 访问控制技术、加密技术和数据确认、管理 / 审计 / 测量 / 监视和检测工具、工业自动化和控制系统计算机软件、物理安全控制。每类条款中提供了每种技术、工具和对抗措施类别的概述，在 IACS 环境中使用这些产品的典型部署和利弊，以及该如何应用才能更好地满足 IACS 的需求的论述。

IEC 62443-3-2 工业自动化和控制系统信息安全 系统设计的安全风险评估

IEC 62443-3-2 的主要内容是评估 IACS 面临的风险，确定目标安全等级（SL-T）并记录安全性要求 [7]。本标准为 IACS 的风险评估提供了全面的框架和方法，给出了风险评估的基本流程和详细流程，将被评估系统（SuC）划分为区域（Zone）和管道（Conduit），评估每个区域和管道的风险，并建立各自的目标安全等级（SL-T），并记录和实施相应的安全性要求。

IEC 62443-3-3 工业通信网络 网络和系统安全 系统安全要求和安全等级

IEC 62443-3-3 的主要内容是确定系统级的网络安全要求和网络安全保障等级 [8]。本标准定义了七项基本要求（FR）、四级安全能力以及它们之间的映射关系。每个基本要求（FR）扩展成一系列系统要求（SR），每个系统要求（SR）包含一个基线要求或 N 个增强要求（RE）。每个基线要求随后会被映射到可提供的安全等级（SL-C）的 1 级至 4 级。通过遵循这一标准，为 IACS 提供了一种量化评价系统安全能力的方法。

IEC 62443-4-2 工业自动化和控制系统信息安全 IACS 组件的安全技术要求

IEC 62443-4-2 的主要内容是确定组件级的网络安全要求和网络安全保障等级 [9]。本标准在系统级的七项基本要求（FR）的基础上扩展了对嵌入式设备（EDR）、主机设备（HDR）、网络设备（NDR）和软件应用要求（SAR）等产品的安全要求，四级安全能力与系统级的安全等级保持一致并给出了它们之间的映射关系。本文件将指导产品供应商可以分配哪些要求以及哪些要求需要在组件中内置，通过实施组件要求（CR）、增强要求（RE）、CR 和 RE 的组合将决定组件可提供的安全等级（SL-C）。这些要求和等级用于指导工控系统的组件设计和实施，确保各个组件在信息安全方面的性能符合系统整体的安全目标。

3. 标准实践

3.1 标准认证总体介绍

IEC 62443 认证提供了符合工业网络安全要求的保证，并证明了组织对其产品的安全性和完整性的承诺。

认证并非 IEC 62443 标准最初的一部分，随着标准的不断推广，认证需求也在不断增长。为了确保产品、系统和软件都能够满足 IEC 62443 标准，选择通过第三方认证能够较大程度上保证网络的安全性。

全球多个机构均可提供相关认证，包括 TÜV SÜD、TÜV Rheinland、TÜV Nord、TÜV Saar、SGS 等。每一家认证机构会不仅限于标准来进行测试，其主旨是最终保证系统和设备的安全。认证业务如表 2 所示：

表 2 IEC 62443 系列标准认证业务情况

认证客户类别	针对部门	认证类型	认证对象	参考标准
产品供应商	研发部门、产品部门	流程	**通用研发流程**	IEC 62443-4-1
		产品或系统	**产品** 工业通信模块、工业主机、控制器、工控软件、嵌入式工控设备等	IEC 62443-4-1 IEC 62443-4-2
		产品或系统	**产品级系统** 空调控制系统、工业机器人等	IEC 62443-4-1 IEC 62443-3-3
集成服务商	工程部门	流程	**集成流程**	IEC 62443-2-4
		产品或系统	**典型的集成系统** 变电站自动化系统、核电 DCS 系统、汽车工业生产系统等	IEC 62443-2-4 IEC 62443-3-3

3.2 全生命周期的应用

根据 IEC 62443 系列标准，将 IACS 生命周期划分为需求阶段、设计阶段、实施阶段、运行阶段、维护阶段以及退役阶段。在应用 IEC 62443 系列标准时，企业可以结合 IACS 所处的生命周期的阶段进行应用。IEC 62443 系列标准为 IACS 的网络安全提供了全面的指导，通过遵循这些标准，企业可以确保其系统在各个生命周期的安全性和可靠性。

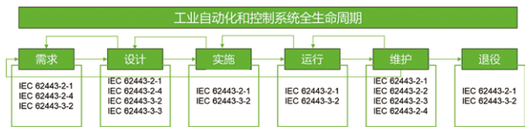


图 2 IEC 62443 系列标准全生命周期的应用

3.3 多视角标准的应用

根据 IEC 62443 系列标准，将 IACS 的角色分为资产所有者、服务提供商和产品供应商。

资产所有者是指对 IACS 负责的组织。资产所有者也是 IACS 和受控设备的使用、操作、运营方。资产所有者根据 IEC 62443-2-1 的要求定义 IACS 的安全管理要求，根据 IEC 62443-2-4 提出对供应商的安全能力要求。

服务提供商可以分为集成服务商和运维服务商。服务提供商根据 IEC 62443-2-4 的要求证明自身具备的安全能力，根据 IEC 62443-3-2 的要求开展风险评估，根据 IEC 62443-3-3 确定系统级的安全要求和保障等级。

产品供应商是生产 IACS 硬件或软件的组织。产品供应商根据 IEC 62443-4-1的要求证明产品开发生命周期的安全性。以此为基础，产品供应商就可以根据 IEC 62443-4-2 的要求证明其 IACS 组件的安全性以及根据 IEC 62443-3-3 的要求证明 IACS 系统级的安全性。

IEC 62443 系列标准多视角的应用如图 3 所示：

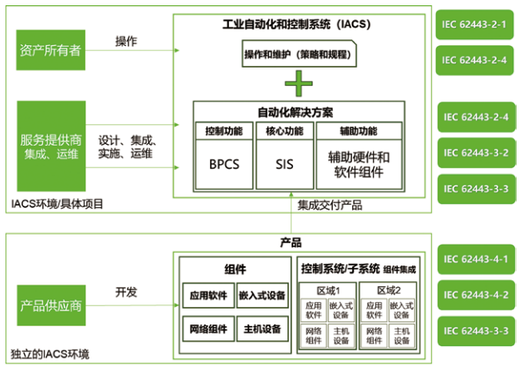


图 3 IEC 62443 系列标准多视角的应用 [10]

4. 总结

IEC 62443 标准体系在不断的发展过程中，其**发展起源、范围目的、安全框架、应用实践以及最新动态**都是了解这一国际标准的关键方面。IEC 62443 向着更广泛的行业应用、更全面的安全要求、更灵活的安全策略以及更细化的风险管理方向发展。各国和各行业在制定相关工控安全标准政策时，都会参考和吸收 IEC 62443 提供的概念和方法。

随着工业互联网和数字经济时代的到来，IEC 62443 标准越来越受到重视，其更新和扩展也越发频繁。IEC 62443 与其他国际标准和国家政策的协同发展，保证了全球范围内工业网络安全的统一性和有效性。IEC 62443 标准体系的发展是一个持续的、多方参与的过程。它不仅涵盖了技术层面的更新，还包括了对新兴威胁的应对和对创新技术的融合。随着工业互联网的兴起，该标准在未来的工业信息安全领域中将发挥越来越重要的作用。对于从事相关工作的专业人员来说，持续关注和学习 IEC 62443 的最新动态，是确保 IACS 安全的关键。

参考文献

[1] 欧阳劲松 , 丁露 . IEC 62443 工控网络与系统信息安全标准综述 [J]. 信息技术与标准化 ,2012 (3) :24-27. DOI:10.3969/j.issn.1671-539X.2012.03.007。

[2] GB/T 40211-2021《工业通信网络 网络和系统安全 术语、概念和模型》。

[3] GB/T 33007-2016《工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序》。

[4] GB/T 42445-2023《工业自动化和控制系统安全 IACS 环境下的补丁管理》。

[5] GB/T 40682-2021《工业自动化和控制系统安全 IACS 服务提供商的安全程序要求》。

[6] GB/T 40218-2021《工业通信网络 网络和系统安全 工业自动化和控制系统信息安全技术》。

[7] GB/T XXXXX-XXXX《工业自动化和控制系统信息安全 系统设计的安全风险评估》征求意见稿。

[8] GB/T 35673-2017《工业通信网络 网络和系统安全 系统安全要求和安全等级》。

[9] GB/T 42456-2023 工业自动化和控制系统信息安全 IACS 组件的安全技术要求。

[10] ISAGCA Quick Start Guide FINAL.

网络安全政策导读（2024年6—9月）

绿盟科技 总体技术部 林涛

栏目说明：

本专栏基于绿盟科技团队在网络安全政策法规方面的日常跟踪，筛选国内外当期热点政策法规文件，并重点结合网络安全产业的发展，对其内容和影响等进行简要分析。本期研究的国内外政策法规的发布时间范围为 2024 年 6 月—9 月。

更多内容敬请关注“网络安全罗盘”和“绿盟科技”微信公众号。

1. 国内篇

1.1《关于向社会公开征求 < 电力监控系统安全防护规定 > （公开征求意见稿）意见的公告》

【内容概述】7 月 25 日国家发改委发布。《规定》主要在以下几方面进行了修订：一是明确电力监控系统的对象和业务范畴，将电力监控系统的范围由罗列典型系统名称改为按系统功能描述的形式进行列举，同时明确电力监控系统运营者等相关适用对象。二是优化安全分区要求，调整安全区名称，细化分区保护粒度，强化安全接入区设置及防护要求。三是深化技术防护原则与策略，补充了业务横纵向交互、设备选型、安全加固、态势感知等技术要求，以及应急备用等管理措施。四是强化供应链管理，明确电力监控系统专用安全产品的管理机制。五是进一步优化技术监督管理，明确电力监控系统运营者和电力调度机构的技术监督要求，增加技术监督风险管控措施。六是细化了罚则。

【绿盟观点】《规定》是对 2014 年版本的修订，内容完善方面主要反映了上位法依据更新、行业发展新情况和风险等方面的考量。

本次修订涉及电力监控系统范畴、细化防护策略和要求、细化罚则等诸多方面。而有三个方面需要强化学习理解。一是关于安全分区，将电力控制系统分为生产控制、运行管理、接入三大区域，对不同区域明确了保护级别要求。其中“接入区”及其安全要求属于新增内容。二是供应链安全，较为系统地明确了电力监控系统专用安全产品管理机制。三是技术监督机制，明确了电力监控系统运营者和电力调度机构的技术监督要求，增加了技术监督风险管控措施等。

对于网络安全行业而言，有两个方面需要格外关注。一是《规定》所提出的事关未来电力安全行业市场准入机会的一个“目录”、两个“黑名单”。一个“目录”即《电力监控系统专用安全产品目录》，该目录将由新建的“电力监控系统专用安全产品管理工作机制”负责维护；两个“黑名单”即“工作机制通报存在供应链安全

风险的产品”（第二十七条）、“经国家相关管理部门检测认定并经国家能源局通报存在漏洞或风险的产品和服务”（第十七条）。二是关于电力控制系统网络安全产品和服务方向，《规定》在”通用技术要求“一章中新增了“态势感知”的规定（第十八条），不仅反映了态势感知在应对电力控制系统新安全问题上的重要性，也对电力控制网络安全新需求做出了明确提示。

1.2《电子政务电子认证服务管理办法》

【内容概述】9 月 10 日国家密码管理局发布。《办法》分为总则、资质认定、行为规范、监督管理、法律责任和附则共 6 章 42 条。《办法》明确要求，在我国从事电子政务电子认证服务的机构，应当经国家密码管理局认定，依法取得电子政务电子认证服务机构资质。国家密码管理局对全国电子政务电子认证服务活动实施监督管理。县级以上地方各级密码管理部门对本行政区域的电子政务电子认证服务活动实施监督管理。

【绿盟观点】《办法》是在 2023 年 10 月征求意见稿基础上修改完善而来。二者相比，基本框架不变，主要监管制度和机制如：资质认定、年度合规评估报告、年度工作报告等也都未做大的修改。

变化主要有四个方面。一是资质申请受理主体进一步明确，即省级密码管理部门;二是强化数据保护，在认证服务机构行为规范中，尤其强调对于数据和信息保护要有专门技术和措施；三是明确了年度合规评估机制，对评估方式、评估依据做出了细化；四是进一步强化对认证依赖方的保护，尤其是增加了认证机构的过错责任。

对网络安全行业而言，《办法》所强调的加强数据和信息保护要求，无疑将为包括数据防泄露、数据审计、监测溯源等技术产品细分领域带来新的市场机会。另一方面，电子政务电子认证年度合规评估等监管工作，也无疑将带动网络和数据安全咨询、运营等服务业务的增长。

1.3《关于加强银行业保险业移动互联网应用程序管理的通知》

【内容概述】9 月 14 日国家金融监督管理总局发布。《通知》从四方面提出 18 条工作要求。一是加强统筹管理，要求金融机构明确移动应用管理牵头部门、建立移动应用台账、完善准入退出机制、控制移动应用数量；二是加强全生命周期管理，要求金融机构规范移动应用的需求分析、设计开发、测试验证、上架发布、监控运行等环节，强化移动应用与运行环境的兼容性、适配性管理；三是落实风险管理责任，要求金融机构落实移动应用备案、网络安全、数据安全、外包管理、业务连续性及个人信息保护等监管要求；四是加强监督管理，要求金融监管总局各级派出机构加强移动应用监管工作。

【绿盟观点】《通知》是国家金融监督管理总局成立以来发布的又一项网络安全相关重要制度，本次规范的领域是移动互联网应用程序。此前，国家金管局曾发布过加强数据监管的《银行保险机构数据安全管理办法（征求意见稿）》。

《通知》主要明确了银行业、保险业移动互联网应用程管理中的合规要求。涉及建设运维、安全保障、监督管理等方面。

这些合规要求中涉及的安全要点可概括为以下六点。一是网络安全，包括落实等保制度，加强测试分发、升级适配管理，强化 APP 备案和重要系统报告制度要求等；二是数据安全，包括明确数据安全责任主体，强化数据防泄露、防篡改和防勒索等；三是个人信息保护，包括信息明确收集原则、告知义务、及时处置等；四是供应链安全，主要包括源代码或组件安全管理、服务外包安全管理；五是业务连续性，包括建立应急处置机制，制定应急预案，定期开展演练，及时报告重大突发事件；六是监管机制，包括针对科技风险和业务风险开展年度风险评估、三年审计和专项审计等。

对网络安全行业而言，需全面看待《通知》的关联和影响。一是关注重点行业，目前已经发布移动互联网应用程序监管制度的行业，除了银行保险，还有教育（教育部 2019 发布《教育移动互联网应用程序备案管理办法》）等部门。二是加强对移动互联网应用程序监管法规的跟进，目前我国出台的一般性监管法规包括《移动互联网应用程序信息服务管理规定》（网信办 2016）、《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》（工信部 2020）、《工业和信息化部关于开展移动互联网应用程序备案工作的通知》（工信部 2023）等。三是持续关注潜在市场机会，如涉及移动互联网应用程序安全合规的咨询服务、监管技术支撑、网络和数据安全产品方案等。

2. 国外篇

2.1 美国发布《新兴技术优先顺序框架》（Emerging Technology Prioritization Framework），划定 FedRAMP 授权优先级

【内容概述】6 月 27 日美国总务管理局发布。“新兴技术优先顺序框架”（简称框架）概述了 FedRAMP 在其授权过程中优先考虑提供特定新兴技术的云服务产品的清单，且规定每年公布两次。框架的初始清单包含生成式人工智能功能的三项新兴技术：聊天界面、代码生成和调试工具以及基于提示的图像生成器。

【绿盟观点】美国注重政府对技术发展的引导，于 2020 年发布了《美国政府关键和新兴技术国家战略》，并每两年更新一次《关键和新兴技术清单》。框架所述“新兴技术”即从属于科技政策办公室列出的关键和新兴技术。同时，框架还是对《关于安全、可靠和值得信赖的人工智能开发和使用的行政令》中“开发和发布一个框架，用于优先考虑联邦风险和授权管理计划授权过程中的关键和新兴技术产品”规定的贯彻落实，并突出承载了“首先是生成式人工智能产品”的相关要求。

“新兴技术优先顺序框架”概述了在 FedRAMP 授权过程中的优先级排序，旨在加快将国家倡导的新兴技术纳入 FedRAMP 市场。其内容要点涵盖以下三方面。

从程序来看。框架提供了一个集成（Integrate）优先授权的操作流程，包括两部分：一是治理（Governance）流程，确定适当的新兴技术功能，进行优先级排序和加速授权；二是评估流程，

审查云服务产品（CSO）是否符合新兴技术（ETs）的定义和标准。

从审查标准来看。优先级审查标准不仅包括新兴技术优先级能力，还要考察市场需求，合格的云服务产品要求符合列出的优先级标准、且需满足至少有 1 个当前代理客户及 3 分（需求评分 Demand Scoring，根据市场需求评分指南评定）的最低需求门槛。

从新兴技术列表内容来看。FedRAMP 基于对生成式人工智能的优先考虑，框架首版清单包括聊天界面、代码生成和调试工具、基于提示的图像生成器、提供这些功能的相关应用程序编程接口（API）三类产品。

“新兴技术优先顺序框架”确定了 FedRAMP 优先级授权的工作依据和审查流程，有利于确保符合国家倡导方向的新兴技术在 FedRAMP 授权审查期间得到优先考虑。

2.2 美国发布“网络事件报告平台”（Cyber Incident Reporting Portal），拓展网络风险事件报告渠道

【内容概述】8 月 29 日美国网络安全和基础设施安全局发布。平台包括网络事件报告、与 login.gov 凭证的集成、保存和更新报告、与同事或客户共享提交的报告以进行第三方报告、搜索和筛选报告等功能。同时发布《自愿网络事件报告资源》，内容包括实体报告事件主体、报告内容（时间、措施等）、降低网络风险的资源等。

【绿盟观点】拜登总统 2022 年签署《关键基础设施网络事件报告法案（CIRCIA）》，授权 CISA 制定和实施法规，要求所涵盖的实体向 CISA 报告相关网络事件。此后，美国的网络事件报告机制得到进一步完善和健全。

本次新平台发布即是其系列完善举措之一，将此前的“网络事件报告表”正式迁移到 CISA 网站服务平台，可实现在线自主或匿名填报网络事件。新平台丰富和完善了网络事件报告功能，包括：与 login.gov（联邦身份平台）衔接，可保存和更新报告、与同事或客户共享提交的报告、检索报告等，用户还可与 CISA 就报告进行非正式讨论等。

在此之前，美国 CISA 已在其网站专门就网络事件报告的意义、范围、“网络事件报告表”主要内容等进行了较为全面的阐述和展示。针对各方自愿报告的网络事件，联邦政府还提供一系列资源和工具，帮助进行事件响应和恢复，降低网络事件影响。这些资源和工具主要包括：网络安全绩效目标框架、已知被利用的漏洞目录、免费的网络安全服务和工具、网络安全警报和建议等等。

网络事件报告对于快速发现和识别网络安全风险、迅速响应、减少损害等都具有重要意义。近年来，我国也十分重视网络事件报告机制的完善，并发布了《网络安全事件报告管理办法（征求意见稿）》等政策法规。美国关于推进相关主体自愿报告网络事件的模式、及保障其实施的具体举措，或对我国加快建设完善网络事件报告工作机制具有一定参考意义。

NSFOCUS

API NSFOCUS

绿盟API安全监测与审计系统

点亮API风险监测盲区 提升敏感数据防护

【智能识别】数据资产全透视，识别接口敏感数据

【联动融合】扫描监管齐联动，API接口安全全闭环

【实时监控】API调用实时监控，点亮风险监控盲区

【国产可控】硬件部署国产化，海光一体机是首选

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，
为政府、金融、运营商、能源、交通、科教文卫等行业用户和各类型企业用户，
提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。
在这些巨人的后面，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS绿盟科技