内部资料 免费交流

出版物准印证号：内资准印证 京内资准字 2124-L0058 号

SECURITY INSIDER

# 网安26号院

奇安信网络安全通讯

## 夺命寻呼机

### 黎巴嫩系列爆炸事件还原与解析 P13

第46期

2024 年 10 月

奇安信

新一代网络安全领军者

# API安全卫士

曾获首届数据安全大赛金奖（产品能力评比）

检测、分析、防护闭环解决方案

守护API安全 数据安全

扫一扫 了解更多

# 特洛伊木马式突袭
# 打开供应链攻击潘多拉魔盒

对于通信设备爆炸事件，奇安信威胁情报中心的一些观察和思考、感觉可以分享给读者。

1、以色列对真主党接近单向透明的情报优势是本次行动的核心支撑。没有通过情报圈定的设备使用人员情况，大批量的植入于民用设备的爆炸装置的使用，无异于的恐怖袭击，即便情报能力强大，大量的附带损伤导致的人道主义灾难也在所难免。结合前几个月哈马斯领导在伊朗参加完活动以后被暗杀，可以看到以色列对于对手如影随形般的掌控。

2、攻击事件体现了以色列的供应链深度介入能力。目前，爆炸设备在哪个环节被植入致命载荷还没有明确的最终结论，生产阶段还是运输交付阶段，是原产还是重打包，如何批量地生产或改造数以千计的设备，这些细节可能与 Stuxnet 事件一样，多年以后才会全面揭露。从目标开源信息的分析来看，对接真主党的寻呼机转手公司的网站最早在 2020 年 10 月就开始准备，显示多年的精心前置伪装操作。不管怎么样，从最终结果来看，保密操作与毁伤效果似乎都取得了极大的成功。

3、爆炸事件还破坏通信指挥系统，为后续的地面军事战场行动创造了更好的条件，体现出网络与动能效应结合的实操作。从以色列此后开展的针对黎巴嫩境内真主党目标的地面和空袭行动来看，此次通信设备爆炸操作除了直接杀伤真主党人员，还有同时破坏通信指挥系统的目标和效果，为后续的地面战场行动创造更好的条件，体现敌前和敌后活动的紧密配合使整体战果大大增加。与此类似的，俄乌冲突爆发的当天，乌方所使用的卫星通信设备被高端网络攻击致瘫，意图对地面军事行动形成影响。网络作战行动日益被视为常规任务的补充，相信今后的军事冲突必定伴随一定程度的网络行动，发挥收集信息、破坏关基、引导舆论等作用。

民用通信设备被大量植入致命载荷，动摇了基本的供应链信任，其影响恶劣程度远甚于震网行动，将会在更大范围加速脱钩断链和阵营划分。恐怖主义者也很可能纷纷效仿，新的潘多拉魔盒再次被毫无底线的行为打开，将会极大地增加全世界的运行成本。需要永远铭记恐怖主义是全人类的公敌，始作俑者也将被反噬。

总编辑

李建平

2024 年 10 月 1 日

CONTENTS

# 目录

## 安全态势


P4 | 国家发改委《公共数据资源登记管理暂行办法》公开征求意见

P4 | 国家数据局《公共数据资源授权运营实施规范（试行）》公开征求意见

P5 | 《网络安全技术 办公设备安全规范》等 9 项网络安全国家标准获批发布

P5 | 我国工业互联网安全领域首批国家标准发布

《网络安全标准实践指南——学术科技服务平台数据安

P6 | 全要求》公开征求意见

P6 | 《工业和信息化领域数据安全合规指引》公开征求意见

P7 | 法德网络安全机构联合发布 AI 编程助手安全使用指南

P7 | 九国网络安全机构联合发布《运营技术网络安全原则》

P8 | 广东省教育厅短信平台遭入侵，向师生家长群发非法链接短信

P8 | 南昌市某企业 IP 疑被黑客远控并滥用，当地网信办罚款 5 万元

P9 | 科威特卫生部被黑，致使国内多个医疗服务中断

P9 | 以色列黑入贝鲁特机场塔台，阻止伊朗飞机降落

P9 | 英国主要火车站紧急关停公共 Wi-Fi：因被黑后传播恐怖主义信息

P10 | 国家安全部发文披露“台独”网军“匿名者 64”

P10 | 供应商泄露用户数据，美国电信巨头 AT&T 被罚超 9000 万元

P10 | 黎巴嫩寻呼机遭远程攻击大规模爆炸，致使 9 人死亡数千人受伤

P11 | Oracle 10 月补丁日多个产品高危漏洞安全风险通告

P11 | Mozilla Firefox 释放后重用漏洞安全风险通告

P12 | 微软 10 月补丁日多个产品安全漏洞风险通告

P12 | GitLab SAML 认证绕过漏洞安全风险通告

P12 | Ivanti Cloud Service Appliance 命令注入漏洞在野利用风险通告

## 月度专题


# 夺命寻呼机

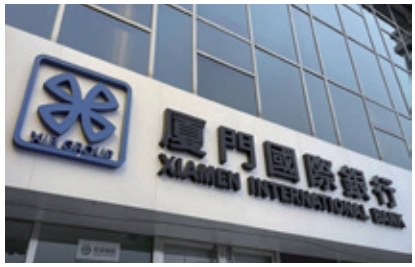
## 黎巴嫩系列爆炸事件还原与解析

P13


黎巴嫩寻呼机爆炸，是一场精心策划、利用各种技术实施的攻击行动，它是首个硬件篡改攻击，凸显供应链武器化的灾难后果，预示着“一切武器化”正成为现实。同时，这一事件使网络战和物理战争在冲突中深度融合，开启了网络战的新篇章，其影响可能将会极其深远。

## 安全之道


P29
厦门国际银行安全编排
与自动化响应系统的创新实践


## 专　栏


P40
SOAR 的未来

P44
加拿大建立武装部队网络司令部
以整合军事网络能力

P46
“定期更换密码”是
最愚蠢的密码规则?


## 奇安资讯


P34 | 2024 补天白帽黑客大会举行：多方共话白帽黑客实网攻防能力培养
P34 | 白帽驱动安全，实战化白帽人才能力图谱 160 项能力发布
P34 | 上海市杨浦区与奇安信集团签署战略合作协议
P35 | 国家信息中心主任徐强莅临奇安信集团调研
P35 | 齐向东与李克强院士共议智能网联汽车信息安全发展之路
P35 | 吴云坤：立足加速攻防 OODA 闭环 探索 AI 驱动安全
P36 | 奇安信集团副总裁韩永刚：新思维构建车路云一体化网络安全体系
P36 | 南京市数据安全创新实验室正式揭牌
P36 | 齐向东：用一体化安全体系护航一体化算力体系
P36 | 中国电子外部董事莅临奇安信安全中心调研
P37 | 信创新标杆！奇安信中标中国移动 2024 年至 2026 年终端安全集采项目
P37 | 奇安信防火墙中标中国电信安全大脑 2024 年集采项目
P37 | 云数据安全资源池发布：一键升级实现云上数据安全快速落地
P37 | All in 国产 | 奇安信集团渠道发布 15 款防火墙产品与标杆案例
P38 | 数千万！奇安信中标“东数西算”某数据中心集群一体化安全项目
P38 | 奇安信天擎 V10 全项满分通过 AV-TEST 测评
P38 | 入选领域最多！奇安信七项技术获全球权威机构推荐
P38 | 奇安信集团连续六年入选“民营企业百强”“科技创新”及“社会责任”三大榜单
P39 | 奇安信入选攻击面管理报告推荐供应商
P39 | “眼明心安”公益项目线上培训开讲
P39 | 重庆移通学院举办“奇安信奖助学金”颁发仪式



《网安 26 号院》编辑部
**主办**　奇安信集团

**总　编　辑**：李建平
**安全态势主编**：王　彪
**月度专题主编**：李建平
**安全之道主编**：张少波
**奇安资讯主编**：陈　冲
**报告速递主编**：刘川琦
**专　栏主编**：任润波


奇安信集团　虎符智库　安全内参


索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557
出版物准印证号：内资准印证 京内资准 2124-L0058 号
编印单位：奇安信科技集团股份有限公司
发送对象：奇安信集团内部人员
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2024 年 10 月 26 日



**版权所有 ©2023 奇安信集团，保留一切权利。**
非经奇安信集团书面同意，任何单位和个人不得擅自摘抄、复制本资料内容的部分或全部，并不得以任何形式传播。

**无担保声明**
本资料内容仅供参考，均“如是”提供，除非适用法要求，奇安信集团对本资料所有内容不提供任何明示或暗示的保证，包括但不限于适销性或者适用于某一特定目的的保证。在法律允许的范围内，奇安信在任何情况下都不对因使用本资料任何内容而产生的任何特殊的、附带的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉或预期节约的损失进行赔偿。

内部资料　免费交流

## 政策篇

国内，数据产业发展与安全政策层出不穷，近一个月已发布近十项。国务院公布《网络数据安全管理条例》，两办发布《关于加快公共数据资源开发利用的意见》，国家数据局就促进数据产业高质量发展征求意见，发改委等部门就数据资源开发发布多份文件；

国际上，人工智能安全受关注。美国加州《前沿人工智能模型安全创新法案》未通过签署而流产，法德网络安全机构联合发布人工智能编程助手安全使用指南。

## 国内

### 国家发改委《公共数据资源登记管理暂行办法》公开征求意见

10 月 12 日，国家发展改革委会同有关部门起草了《公共数据资源登记管理暂行办法》，现向社会公开征求意见。该文件共 5 章 27 条，包括总则、登记要求、登记程序、登记管理、监督管理。该文件提出，公共数据资源登记应当维护国家安全和公共利益，保护国家秘密、商业秘密、个人隐私和个人信息权益，遵循依法合规、公开透明、标准规范、安全高效的原则。该文件要求，登记机构应建立健全数据资源登记管理责任机制，履行数据安全保护义务，妥善保管登记信息，登记主体在申请登记前应当自行或委托第三方专业服务机构，通过技术手段在保障安全的前提下，对公共数据资源进行存证，确保来源可查、加工可控。

### 国家数据局《公共数据资源授权运营实施规范（试行）》公开征求意见

10 月 12 日，国家数据局会同有关部门研究起草了《公共数据资源授权运营实施规范（试行）》（公开征求意见稿），现向社会公开征求意见。该文件共 7 章 26 条，包括总则、基本要求、方案编制、协议签订、运营实施、运营管理、附则。该文件提出，公共数据资源授权运营应遵循依法合规、公平透明、公益优先、合理收益、安全可控的原则。该文件要求，实施机构应建立健全管理制度，明确数据分类分级安全保护要求，加强技术支撑保障和数据安全管理；运营机构应履行数据安全主体责任，加强内控管理、技术管理和人员管理，不得超授权范围使用公共数据资源，严防数据加工、处理、运营、服务等环节数据安全风险。实施机构、运营机构应通过管理和技术措施，加强数据关联汇聚风险识别和管控，保障数据安全。

### 住建部公布《“数字住建”建设整体布局规划》

10 月 12 日，住房和城乡建设部公布《“数字住建”建设整体布局规划》。该文件提出，到 2027 年底，“数字住建”建设取得显著成效，一体化数字基础设施和数据资源体系建成运行，数字化政策标准和安全防护支撑能力明显提升。该文件要求坚持安全可控原则，落实网络和数据安全主体责任，构建制度、管理和技术衔接配套的安全防护体系，强化基础设施、数据资源和应用平台等安全保障能力，守牢网络和数据安全底线。

### 中共中央办公厅、国务院办公厅发布《关于加快公共数据资源开发利用的意见》

10 月 9 日，中共中央办公厅、国务院办公厅联合发布《关于加快公共数据资源开发利用的意见》。该文件共 6 章 17 条，其中第 12 条要求加强安全管理。具体包括强化数据安全和个人信息保护，加强对数据资源生产、加工使用、产品经营等

开发利用全过程的监督和管理。建立健全分类分级、风险评估、监测预警、应急处置等工作体系，开展公共数据利用的安全风险评估和应用业务规范性审查。运营机构应依据有关法律法规和政策要求，履行数据安全主体责任，采取必要安全措施，保护公共数据安全。加强技术能力建设，提升数据汇聚关联风险识别和管控水平。依法依规予以保密的公共数据不予开放，严格管控未依法依规公开的原始公共数据直接进入市场。

## 《网络安全技术 办公设备安全规范》等 9 项网络安全国家标准获批发布

10 月 9 日，根据 2024 年 9 月 29 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2024 年第 22 号），全国网络安全标准化技术委员会归口的 9 项国家标准正式发布。具体包括《网络安全技术 信息安全控制》《网络安全技术 网络和终端隔离产品技术规范》《网络安全技术 办公设备安全规范》《网络安全技术 智能门锁网络安全技术规范》《网络安全技术 实体鉴别 第 2 部分：采用鉴别式加密的机制》《网络安全技术 消息鉴别码 第 2 部分：采用专门设计的杂凑函数的机制》《网络安全技术 杂凑函数 第 1 部分：总则》《网络安全技术 杂凑函数 第 2 部分：采用分组密码的杂凑函数》《网络安全技术 杂凑函数 第 3 部分：专门设计的杂凑函数》。

## 我国工业互联网安全领域首批国家标准发布

10 月 8 日，根据 2024 年 9 月 29 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2024 年第 22 号），全国通信标准化技术委员会归口的《工业互联网企业网络安全 第 1 部分：应用工业互联网的工业企业防护要求》《工业互联网企业网络安全 第 2 部分：平台企业防护要求》《工业互联网企业网络安全 第 3 部分：标识解析企业防护要求》三项工业互联网企业网络安全国家标准发布。这三项标准聚焦三类工业互联网企业网络安全防护需求，提出不同级别企业的网络安全防护要求，为企业实施工业互联网安全分类分级管理工作提供指导，是我国实施工业互联网企业网络安全分类分级管理与防护工作的创新成果与经验总结。

## 国家发改委等六部门联合印发《国家数据标准体系建设指南》

10 月 8 日，国家发展改革委、国家数据局、中央网信办、工业和信息化部、财政部、国家标准委联合印发《国家数据标准体系建设指南》。该文件提出，到 2026 年年底，基本建成国家数据标准体系。该文件以数据“供得出、流得动、用得好、保安全”为指引，从基础通用、数据基础设施、数据资源、数据技术、数据流通、融合应用、安全保障等 7 个部分，加快构建数据标准体系，全面指导数据标准化工作开展。其中，安全保障部分包括数据基础设施安全、数据要素市场安全、数据流通安全三方面。

## 国务院公布《网络数据安全管理条例》

9 月 30 日，国务院总理李强签署国务院令，公布《网络数据安全管理条例》，自 2025 年 1 月 1 日起施行。该文件共 9 章 64 条，包括总则、一般规定、个人信息保护、重要数据安全、网络数据跨境安全管理、网络平台服务提供者义务、监督管理、法律责任、附则。该文件主要规定了五方面内容，一是提出网络数据安全管理总体要求和一般规定；二是细化个人信息保护规定；三是完善重要数据安全制度；四是优化网络数据跨境安全管理规定；五是明确网络平台服务提供者义务。

## 《网络安全技术 统一威胁管理产品（UTM）技术规范》等 15 项国家标准公开征求意见

9 月 30 日，全国网络安全标准化技术委员会归口的 15 项国家标准已形成标准征求意见稿，现公开征求意见。这批标准包括《网络安全技术 公钥密码应用技术体系框架》和 14 项网安产品技术规范标准，分别为《网络安全技术 统一威胁管理产品（UTM）技术规范》《网络安全技术 身份鉴别产品技术规范》《网络安全技术 数据泄露防护产品技术规范》《网络安全技术 终端接入控制产品技术规范》《网络安全技术 负载均衡产品技术规范》《网络安全技术 网络型流量控制产品技术规范》《网络安全技术 USB 移动存储介质管理系统技术规范》《网络安全技术 信息过滤产品技术规范》《网络安

全技术 电子文档安全管理产品技术规范》《网络安全技术 终端安全监测产品技术规范》《网络安全技术 日志分析产品技术规范》《网络安全技术 安全配置检查产品技术规范》《网络安全技术 数据销毁软件产品技术规范》《网络安全技术 抗拒绝服务攻击产品技术规范》。

## 《网络安全标准实践指南——学术科技服务平台数据安全要求》公开征求意见

9 月 30 日，全国网络安全标准化技术委员会秘书处组织编制了《网络安全标准实践指南——学术科技服务平台数据安全要求（征求意见稿）》，现公开征求意见。该文件规定了学术科技服务平台数据安全保护要求，提出了学术科技服务平台运营者应履行的安全责任和义务，适用于规范学术科技服务平台运营者数据处理活动，也可为有关主管监管部门组织开展相关检查评估提供参考。该文件不适用于涉及国家秘密的数据。

## 《工业和信息化领域数据安全合规指引》公开征求意见

9 月 29 日，中国钢铁工业协会、中国有色金属工业协会、中国石油和化学工业联合会、中国电子信息行业联合会、中国通信标准化协会、中国通信企业协会等十七家行业组织共同编制《工业和信息化领域数据安全合规指引（征求意见稿）》，现面向成员单位公开征求意见。该文件共 9 章，包括概述、数据分类分级、数据安全管理体系、数据全生命周期保护、数据安全风险监测预警 & 报告 & 处置、数据安全事件应急处置、数据安全风险评估、数据出境、数据交易。该文件聚焦数据处理者在履行数据安全保护义务过程中的难点问题，明确数据安全合规依据，提供实务指引，指导数据处理者开展数据安全合规管理，以提升数据安全保护能力。

## 国家数据局《关于促进数据产业高质量发展的指导意见》公开征求意见

9 月 27 日，国家数据局会同有关部门研究起草了《关于促进数据产业高质量发展的指导意见》，现向社会公开征求意见。该文件共 9 章，包括总体要求、加强数据产业规划布局、培育多元经营主体、加快数据技术创新、提高数据资源开发利用水平、繁荣数据流通交易市场、强化基础设施支撑、提高数据领域动态安全保障能力、优化产业发展环境。该文件在安全保障部分共两方面。一是创新数据安全产品服务。推动基础设施安全、数据安全、应用安全协同发展，加强身份认证、数据加密、安全传输、合规检测等技术创新，培育壮大适应数据流通特征和人工智能应用的安全服务业态。支持企业创新数据分类分级、隐私保护、安全监测、应急处置等数据安全产品和服务。二是加强动态数据安全保障。扩大数据空间、区块链、隐私计算等可信流通技术及模式应用范围，增强数据可信、可控、可计量开发利用能力。建立健全数据安全风险识别、监测预警、应急处置等相关规范，落实数据流通利用全过程相关主体的安全责任。健全数据分类分级标准，加强对涉及国家安全、商业秘密、个人隐私等数据的保护。

## 国家数据局《关于促进企业数据资源开发利用的意见》公开征求意见

9 月 27 日，国家数据局会同有关部门研究起草了《关于促进企业数据资源开发利用的意见》，现向社会公开征求意见。该文件共 7 章 16 条，包括总体要求、健全企业数据权益实现机制、培育企业数字化竞争力、赋能产业转型升级、服务经济社会高质量发展、营造开放透明可预期的发展环境、保障措施。该文件要求，落实国家数据分类分级保护制度要求，在防范实质性风险前提下，鼓励企业针对不同敏感级别的数据和数据处理场景，采取差异化的数据安全与合规管理措施，优化对同类型数据处理行为的内部合规审批流程。鼓励企业采用数据空间、区块链、隐私计算、匿名化等技术模式，促进数据安全流动和开发利用。

## 《网络安全标准实践指南——敏感个人信息识别指南》发布

9 月 18 日，全国网络安全标准化技术委员会秘书处组织编制了《网络安全标准实践指南——敏感个人信息识别指南》。该文件给出了敏感个人信息识别规则及常见敏感个人信息类

别和示例，可用于指导各组织识别敏感个人信息，也可为敏感个人信息处理和保护工作提供参考。

## 国际

### 法德网络安全机构联合发布 AI 编程助手安全使用指南

10 月 4 日，法国网络安全局（ANSSI）和德国联邦信息安全办公室（BSI）共同编制发布了《AI 编程助手》，为开发人员安全使用 AI 编码助手提供了风险和安全建议。该文件提出，在软件开发中使用 AI 编程助手可能面临敏感信息通过用户输入泄露、输出低质量或不安全的代码、供应链攻击、被攻击者滥用等风险。该文件指出，AI 编程助手无法替代经验丰富的开发人员，无节制使用此类工具，将带来严重安全隐患。该文件建议，引入 AI 工具应进行系统的风险分析，并加强质量管理。

### 九国网络安全机构联合发布《运营技术网络安全原则》

10 月 2 日，澳大利亚信号局网络安全中心与五眼联盟、德国、荷兰、日本、韩国的网络安全机构联合发布《运营技术（OT）网络安全原则》，阐述了指导创建和维护安全、可靠的关键基础设施 OT 环境的六项原则，包括安全至上（确保系统安全）；了解业务至关重要（了解并保护关键系统）；OT 数据极其宝贵且需要保护（保护 OT 数据）；将 OT 与其他所有网络进行隔离和分段（守好边界关紧后门）；供应链必须安全（确保网络安全供应链）；人员在 OT 网络安全中至关重要（人员是第一道防线）。

### 欧盟发布《数据治理法案》指导文件，进一步明确非个人数据跨境流动规则

9 月 24 日，在《数据治理法案》推出一周年后，欧盟委员会发布了一份关于实施《数据治理法案》的指导文件。该文件明确指出，《数据治理法案》的适用范围包括个人数据和非个人数据。对于个人数据，《通用数据保护条例》和《电子隐私条例》将同时适用。该文件重申，《数据治理法案》不会修改《通用数据保护条例》，也不涉及《通用数据保护条例》中监管机构的作用。该文件还指出，在非个人数据跨境流动规则方面，《数据治理法案》仅为非个人数据的跨境转移设定规则，个人数据的跨境转移仍受《通用数据保护条例》第五章规定的约束。

### 美国拟禁用中国、俄罗斯智能网联汽车软硬件

9 月 23 日，美国商务部工业与安全局发布《保障信息和通信技术及服务供应链：网联汽车》的拟议规则通知，并于 9 月 26 日正式公布了文本，面向公众征求意见。该文件提出了一项规则，旨在解决由于某些外国对手（如中国和俄罗斯）设计、开发、制造或供应的信息和通信技术及服务用于网联汽车而带来的国家安全风险。该文件重点关注集成到车辆连接系统（VCS）中的硬件和软件（如蓝牙、卫星、蜂窝和 Wi-Fi 模块）及集成到自动驾驶系统（ADS）中的软件。这些关键系统通过特定的硬件和软件，可以在网联汽车中实现外部连接和自动驾驶功能。该文件将禁止 2027 年款的车辆进口 VCS、ADS 软件，以及 2030 年款的车辆进口硬件。小规模生产者可能会获得豁免，以防止行业混乱。

### 美国 CISA 发布《联邦民事行政部门运营网络安全协调计划》

9 月 16 日，美国网络安全与基础设施安全局（CISA）发布《联邦民事行政部门（FCEB）运营网络安全协调计划》，以指导对各 FCEB 的协调支持和服务，推动优先事项有效开展，协调集体运营防御能力。该计划包括五个优先事项，资产管理、漏洞管理、可防御架构、网络供应链风险管理、事件检测与响应。该计划并非一份全面清单，而是旨在将资源集中在可实质推动运营网络安全改进和协调目标的行动上。CISA 表示，通过与各 FCEB 合作共同推进计划，将实现美国联邦机构网络安全现代化。

## 事件篇

网络物理战迈向新范式，颠覆了传统的网络战认知。黎巴嫩寻呼机遭远程攻击大规模爆炸，致使 9 人死亡数千人受伤；以色列黑入贝鲁特机场塔台，阻止伊朗飞机降落；多个政府机密系统遭 APT 组织攻破，物理隔离不等于绝对安全。

### 广东省教育厅短信平台遭入侵，向师生家长群发非法链接短信

10 月 12 日综合消息，广东省教育厅发布声明称，发现有不法分子入侵该部门短信平台，以“广东省教育厅”的名义向师生和家长发送包含非法链接的短信。该部门已第一时间向公安机关报案，并配合开展调查。请广大师生和家长提高警惕，切勿点击短信中的非法链接，避免个人信息泄露或遭受财产损失。此前，社交媒体上有多位用户表示，收到一条来自“广东省教育厅”的短信，写着“深夜必备成人电影戳链接”与非法内容链接。

### 南昌市某企业 IP 疑被黑客远控并滥用，当地网信办罚款 5 万元

9 月 30 日网信南昌公众号消息，南昌市网信办在日常的网络安全监测中发现，属地企业所属 IP 疑似被黑客远控，频繁对外发起网络爆破攻击。经过立案调查、现场勘验、远程勘验（采样技术分析）、笔录问询等工作，查明：1. 该企业未履行网络安全保护义务，未对运营的网络及信息系统开展网络安全等级保护测评等相关工作，并采取防范计算机病毒和网络攻击等危害网络安全行为的技术措施；2. 该企业未及时处置计算机病毒、网络攻击等安全风险，所属终端感染木马病毒，持续对外发起网络攻击，导致产生危害网络安全的后果。相关行为违反了《中华人民共和国网络安全法》第二十一条、第二十五条的规定。9 月 29 日，南昌市网信办依据《中华人民共和国网络安全法》第五十九条的规定，对该企业作出罚款 5 万元、对直接负责的主管人员罚款 1 万元的行政处罚。

### 打破物理隔离！多个政府机密系统遭 APT 组织攻破

10 月 8 日 BleepingComputer 消息，欧洲网络安全厂商 ESET 发布报告称，名为 GoldenJackal 的 APT 组织成功攻破了欧洲政府机构的气隙隔离系统。该组织至少成功实施了两起攻击行动，第一起发生在 2019 年 9 月和 2021 年 7 月，目标是某南亚国家驻白俄罗斯大使馆。第二起针对的是一个欧洲政府机构，发生在 2022 年 5 月至 2024 年 3 月之间。黑客使用了两套自定义工具集窃取了大量敏感数据，包括电子邮件、加密密钥、图像、档案及文件。此前 2023 年 5 月，卡巴斯基发布关于 GoldenJackal 组织攻击活动的报告，指出该组织专注于政府和外交机构，主要目的是进行间谍活动。

### 美国水务巨头遭网络攻击：水计费系统瘫痪，上千万人无法处理账单

10 月 8 日 The Record 消息，美国水务公司（American Water Works）7 日发布 SEC 文件称，其供水和废水设施未受到上周发生的网络攻击影响。该公司管理层在网站上警告，为遏制此次攻击采取了停用和隔离措施，客户目前无法访问用于管理个人账户和支付水费的门户网站。目前公司的 MyWater 账户系统已瘫痪，所有客户预约的服务将被重新安排。所有账单处理已暂停，直至另行通知。但是，系统恢复上线之前，不会产生逾期费用或停止服务。该公司的呼叫中心也无法正常运作。美国水务公司是美国最大的受监管水务公共事业公司。

## 科威特卫生部被黑，致使国内多个医疗服务中断

9 月 27 日 The Record 消息，中东国家科威特的卫生部日前遭遇网络攻击，导致该国多家医院的系统瘫痪，国家医疗应用 Sahel 也因此下线。截至 9 月 26 日下午，卫生部官网仍处于瘫痪状态。该部门通过科威特通讯社发布声明称，政府通过备份数据，已经成功恢复了科威特癌症控制中心的系统，以及国家健康保险和外籍人员体检管理办公室的相关系统。声明还称，黑客未能攻入“核心数据库”，但为进行必要的安全更新，卫生部不得不暂时关闭部分系统。卫生部没有提供系统全面恢复的确切时间表，仅表示恢复工作将很快完成。目前尚无任何勒索软件组织对这次攻击事件宣称负责。

## 以色列黑入贝鲁特机场塔台，阻止伊朗飞机降落

9 月 28 日 Middle East Monitor 消息，黎巴嫩贝鲁特国际机场的控制塔台疑似遭以色列网络攻击，导致一架伊朗民航班机未能降落，被迫返回德黑兰。黎巴嫩交通部长阿里 · 哈米向黎巴嫩媒体《An-Nahar》透露，以色列国防军拦截了贝鲁特机场控制塔的无线电通信，并威胁称，如果这架伊朗飞机降落，将攻击机场基础设施。以色列媒体《耶路撒冷邮报》也报道称，以色列军方入侵了贝鲁特控制塔的通信系统，警告一架来自“卡西姆航空”的货运飞机，航班号为 QFZ9964，在其准备降落时发出警告。以色列军方声称，贝鲁特国际机场被用作向真主党输送武器的入口，但黎巴嫩当局对此予以否认，强调机场是完全用于民用的基础设施。

## 英国主要火车站紧急关停公共 Wi-Fi：因被黑后传播恐怖主义信息

9 月 26 日英国卫报消息，由于发生“网络安全事件”，英国境内 19 个主要火车站宣布暂停提供 Wi-Fi 服务，其中伦敦有 10 个车站受到影响。有乘客在皮卡迪利站连接 Wi-Fi 时，被引导到一个标题为“我们爱你，欧洲”的网页。该网页包含了反伊斯兰的信息，以及关于英国和欧洲几起恐怖袭击的详细内容。英国铁路网公司（Network Rail）的发言人表示，“我们正在应对影响铁路网公司管理的车站公共 Wi-Fi 的网络安全事件。由于 Wi-Fi 服务由第三方提供，调查期间该服务已被暂停。”为该公司提供 Wi-Fi 服务的 Telent 公司表示，Wi-Fi 登录页面遭遇“未经授权的更改”，该更改是通过该网页供应商 Global Reach 公司的“合法管理员账号”进行的。稍晚时候，英国交通警察局表示，一名受雇于 Global Reach 的男子已因涉嫌违反《1990 年计算机滥用法》被捕。

## 美国汇款巨头速汇金遭网络攻击，支付服务中断约 5 天

9 月 24 日 BleepingComputer 消息，全球第二大汇款公司速汇金（MoneyGram）23 日发布公告称，自 9 月 20 日以来，该公司由于遭受网络攻击，导致系统故障和支付服务中断。公告中指出：“速汇金近期发现了一个影响我们部分系统的网络安全问题。我们在发现问题后，立即展开调查，并采取了保护措施应对此次事件，其中包括主动下线部分系统，这对网络连接产生了影响。”该公司此前一直声称这是一次“网络故障”，直到 23 日才披露是一次“网络安全事件”，但并未披露攻击细节，媒体认为该事件的特征与勒索软件攻击极为类似。25 日下午，速汇金在 X 平台上称，许多代理合作伙伴的汇款和收款服务已经恢复，待处理的交易正在陆续完成，公司将继续恢复剩余的其他服务，包括官方网站。

## 背调公司发生超大规模数据泄漏，一亿美国人隐私信息暴露

9 月 23 日 Cybernews 消息，网络安全研究机构 Cybernews 发现，美国背景调查和公共记录服务公司 MC2 Data 发生了大规模数据泄露事件，由于数据库没有设置密码保护，暴露了该公司 2.2TB 的敏感数据。这些数据中包含超过 1 亿美国公民的个人信息，涉及姓名、电

子邮箱、电话号码、家庭住址、加密的密码、部分支付信息、房产记录、法律记录、就业经历、家庭亲戚及邻居信息等，严重威胁了个人隐私与信息安全。这是 Facebook（2019 年 5 亿）和 Linkedin（2021 年 7 亿）之后，近年来美国发生的最严重的数据泄漏事件。MC2 Data 旗下运营的网站包括 PrivateRecords.net、PrivateReports、PeopleSearcher、ThePeopleSearchers 及 PeopleSearchUSA。这些网站通过汇集公开数据，如犯罪记录、就业历史、家庭信息和联系方式，提供背景调查服务，广泛应用于雇主、房东等作出决策时的参考。

## 国家安全部发文披露“台独”网军“匿名者 64”

9 月 23 日国家安全部消息，国家安全部公众号发布文章《起底“台独”网军“匿名者 64”》称，今年以来，一个名为“匿名者 64”的黑客组织，针对中国大陆和港澳地区，频繁开展网络攻击，试图获取有关门户网站、户外电子屏幕、网络电视等控制权限，进而非法上传、插播诋毁大陆政治制度和大政方针的内容，颠倒黑白，散布谣言。对此，国家安全机关立即行动，采取有效措施，处置危害隐患，消除不良影响。深入调查确认，“匿名者 64”组织并非普通黑客，而是由“台独”势力豢养的一支网军。目前，国家安全机关锁定了实施相关网络攻击活动的台湾人员身份信息，其中包括台湾资通电军现役人员罗俊铭、洪莉棋、廖韦纶。国家安全机关已依法对三人立案侦查。

## 供应商泄露用户数据，美国电信巨头 AT&T 被罚超 9000 万元

9 月 17 日 CyberScoop 消息，美国联邦通信委员会（FCC）与 AT&T 就 2023 年 1 月发生的重大数据泄露事件达成了一项 1300 万美元（约合人民币 9181 万元）的和解协议，该事件导致 AT&T 超过 890 万名移动客户的信息被窃取。根据和解协议，AT&T 向一家提供用于营销、账单处理和生成个性化视频内容服务的供应商共享了大量客户数据，双方签署合同明确了数据保护和删除要求，此前多年评估均显示该供应商遵循了数据删除政策，但本该被删除的数据却在 2023 年 1 月被泄露。FCC 最终认定，AT&T 对这一失误负有不可推卸的最终责任，并要求其实施安全改进计划。FCC 执法局局长 Loyaan Egal 指出，这份和解协议提醒企业，FCC 正对企业在供应链中如何确保客户数据安全进行更为严格的审查。

## 黎巴嫩寻呼机遭远程攻击大规模爆炸，致使 9 人死亡数千人受伤

9 月 17 日综合消息，黎巴嫩真主党 17 日发表声明，该组织多名成员携带的寻呼机当天下午发生爆炸，已造成多名黎巴嫩真主党成员死亡，并在全国范围内造成大量人员受伤。黎巴嫩公共卫生部长阿卜亚德称，爆炸已造成 9 人死亡，约有 2800 人受伤，其中约 200 人伤情危重。据悉，黎巴嫩真主党武装人员近来较为普遍地使用寻呼机，以通过这种技术含量较低的通信设备，避免以色列追踪他们的位置。此次发生寻呼机爆炸的地点主要集中在贝鲁特南郊、黎巴嫩南部及贝卡谷地等地，这些都被认为是黎巴嫩真主党据点所在地。多方消息显示，可能是真主党采购的某批次寻呼机被以色列截获篡改植入炸药，真主党未发现继续分发使用。纽约时报称，这些寻呼机在当天下午同时收到一条看似来自真主党领导层的消息，发出振动 / 蜂鸣声几秒后发生爆炸，尚不确定引爆指令是这条消息还是其他信号。

## 因勒索攻击泄露患者敏感数据，美国医疗巨头赔偿超 4.6 亿元

9 月 12 日 The Register 消息，美国宾夕法尼亚州大型初级医疗集团利哈伊谷健康网络（Lehigh Valley Health Network，LVHN）将支付 6500 万美元（约合人民币 4.6 亿元），以了结其患者发起的集体诉讼，此次和解金额按每人计算或为医疗数据泄露案件最高。该机构于 2023 年 2 月 6 日发现其 IT 系统遭受入侵，随后确认 ALPHV（又称 BlackCat）团伙是这次攻击的幕后黑手。攻击者共窃取了 13.4 万名患者和员工的相关数据，数据量达数 GB。被窃取的数据包括姓名、地址、社会安全号码、州 ID 信息、医疗记录和手术照片等，甚至还有未经授权拍摄留存的患者裸露照片，并且部分已被公开发布到网上。

## 漏洞篇

微软本月共发布了 117 个漏洞的补丁程序，经研判有 13 个重要漏洞值得关注，包括 3 个紧急漏洞、9 个重要漏洞、1 个中危漏洞。鉴于这些漏洞危害较大，建议客户尽快安装更新补丁。

### Oracle 10 月补丁日多个产品高危漏洞安全风险通告

10 月 16 日，Oracle 官方发布了 2024 年 10 月的关键安全补丁集合更新 CPU（Critical Patch Update），修复了多个漏洞。其中 Oracle WebLogic Server T3/IIOP 远程命令执行漏洞（CVE-2024-21216）、Oracle WebLogic Server T3/IIOP 未授权数据访问漏洞（CVE-2024-21234）影响相对较大。奇安信 CERT 建议客户尽快自查，并应用本次关键安全补丁集合（CPU）。

| CVE 编号 | 影响组件 | 协议 | 可否远程未授权利用 | CVSS | 受影响版本 |
|---|---|---|---|---|---|
| CVE-2024-21216 | Oracle WebLogic Server (Core) | T3/IIOP | 可 | 9.8 | 12.2.1.4.0, 14.1.1.0.0 |
| CVE-2024-21274 | Oracle WebLogic Server (Console) | HTTP | 可 | 7.5 | 12.2.1.4.0, 14.1.1.0.0 |
| CVE-2024-21215 | Oracle WebLogic Server (Core) | HTTP | 可 | 7.5 | 12.2.1.4.0, 14.1.1.0.0 |
| CVE-2024-21234 | Oracle WebLogic Server (Core) | T3/IIOP | 可 | 7.5 | 12.2.1.4.0, 14.1.1.0.0 |
| CVE-2024-21260 | Oracle WebLogic Server (Core) | T3/IIOP | 可 | 7.5 | 12.2.1.4.0, 14.1.1.0.0 |
| CVE-2024-5535 | MySQL Connectors: Connectors: Connector/C++ (OpenSSL) | MySQL Protocol | 可 | 9.1 | 8.0.39 and prior, 8.4.2 and prior, 9.0.1 and prior |
| CVE-2024-21272 | MySQL Connectors: Connector/Python | MySQL Protocol | 否 | 7.5 | 9.0.0 and prior |

### Mozilla Firefox 释放后重用漏洞安全风险通告

10 月 12 日，奇安信 CERT 监测到 Mozilla 发布公告称 Mozilla Firefox Animation timelines 释放后重用漏洞（CVE-2024-9680）存在在野利用，远程攻击者能够通过利用 Animation timelines 中的释放后使用漏洞在内容进程中实现代码执行。目前，此漏洞已发现在野利用。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

### GitLab EE 权限绕过漏洞安全风险通告

10 月 10 日，奇安信 CERT 监测到官方修复 GitLab EE 权限绕过漏洞（CVE-2024-9164），攻击者可以在某些情况下，以其他用户的身份利用该漏洞在 GitLab 的任意分支上执行管道，从而可能执行恶意代码或泄露敏感信息。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 1,500,205 个，关联 IP 总数为 27,508 个。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

### cups-browsed 远程代码执行漏洞安全风险通告

9 月 27 日，奇安信 CERT 监测到官方修复 cups-browsed 远程代码执行漏洞（CVE-2024-47176），该漏洞是由于 cups-browsed 服务在处理网络打印任务时，会绑定到 UDP 端口 631 的 INADDR_ANY 地址，从而信任来自任何来源的数据包。这会导致未经身份验证的远程攻击

者可以利用该漏洞发送特制的数据包，触发恶意请求到攻击者控制的 URL，从而在目标系统上执行任意命令。利用此漏洞需要启用 cups-browsed 服务（Ubuntu Desktop 环境下默认启用），且需要受害者主动使用该恶意 IPP 服务器配置的打印机设备进行打印操作。目前该漏洞技术细节和 PoC 已公开，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

## 微软 10 月补丁日多个产品安全漏洞风险通告

10 月 9 日，微软本月共发布了 117 个漏洞的补丁程序，修复了 Microsoft Management Console、Windows MSHTML Platform、Microsoft Configuration Manager 等产品中的漏洞。经研判，以下 13 个重要漏洞值得关注（包括 3 个紧急漏洞、9 个重要漏洞、1 个中等漏洞），如下表所示。鉴于这些漏洞危害较大，建议客户尽快安装更新补丁。

| 编号 | 漏洞名称 | 风险等级 | 公开状态 | 利用可能 |
|---|---|---|---|---|
| CVE-2024-43572 | Microsoft Management Console 远程代码执行漏洞 | 重要 | 已公开 | 在野利用 |
| CVE-2024-43573 | Windows MSHTML Platform 欺骗漏洞 | 中 | 已公开 | 在野利用 |
| CVE-2024-43582 | Windows 远程桌面协议服务器远程代码执行漏洞 | 紧急 | 未公开 | 较小 |
| CVE-2024-43488 | Visual Studio Code extension for Arduino 远程代码执行漏洞 | 紧急 | 未公开 | 较小 |
| CVE-2024-43468 | Microsoft Configuration Manager 远程代码执行漏洞 | 紧急 | 未公开 | 较小 |
| CVE-2024-43583 | Winlogon 权限提升漏洞 | 重要 | 已公开 | 较大 |
| CVE-2024-43560 | Microsoft Windows 存储端口驱动程序权限提升漏洞 | 重要 | 未公开 | 较大 |
| CVE-2024-43556 | Windows 图形组件权限提升漏洞 | 重要 | 未公开 | 较大 |
| CVE-2024-43509 | Windows 图形组件权限提升漏洞 | 重要 | 未公开 | 较大 |
| CVE-2024-43615 | Microsoft OpenSSH for Windows 远程代码执行漏洞 | 重要 | 未公开 | 较大 |
| CVE-2024-43609 | Microsoft Office 欺骗漏洞 | 重要 | 未公开 | 较大 |
| CVE-2024-43581 | Microsoft OpenSSH for Windows 远程代码执行漏洞 | 重要 | 未公开 | 较大 |
| CVE-2024-43502 | Windows 内核权限提升漏洞 | 重要 | 未公开 | 较大 |

## GitLab SAML 认证绕过漏洞安全风险通告

9 月 19 日，奇安信 CERT 监测到官方修复 GitLab SAML 认证绕过漏洞（QVD-2024-40180），由于 GitLab 对 SAML 响应的不当处理，使得攻击者可以插入任意值，攻击者从而通过构造特定的 SAML 响应，绕过 GitLab 实例的身份验证机制，无需正确的凭证即可访问受保护的资源。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 1,372,328 个，关联 IP 总数为 24,944 个。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

## Ivanti Cloud Service Appliance 命令注入漏洞在野利用风险通告

9 月 19 日，奇安信 CERT 监测到 Ivanti Cloud Service Appliance 命令注入漏洞（CVE-2024-8190）技术细节与 EXP 已公开，该漏洞是由于后台未对传入的 TIMEZONE 参数做校验，而是直接传给 exec() 函数执行，从而导致拥有管理员权限的攻击者执行任意命令。奇安信鹰图资产测绘平台数据显示，该漏洞关联的全球风险资产总数为 11,321 个，关联 IP 总数为 2,249 个。奇安信威胁情报中心安全研究员已成功复现漏洞，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

## VMware vCenter Server 堆溢出漏洞安全风险通告

9 月 18 日，奇安信 CERT 监测到官方修复 VMware vCenter Server 堆溢出漏洞（CVE-2024-38812），VMware vCenter Server 在 DCERPC 协议实施过程中存在堆溢出漏洞，攻击者可发送特制的网络数据包来触发此漏洞，从而导致远程代码执行。奇安信鹰图资产测绘平台数据显示，该漏洞关联的国内风险资产总数为 13,314 个，关联 IP 总数为 3,017 个。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

注：使用公司邮箱发送企业名称和需开通订阅的邮箱地址至 cert@qianxin.com，即可申请订阅最新漏洞通告。

# 夺命寻呼机

## 黎巴嫩系列爆炸事件还原与解析

黎巴嫩寻呼机爆炸，是一场精心策划、利用各种技术实施的攻击行动，它是首个硬件篡改攻击，凸显供应链武器化的灾难后果，预示着“一切武器化”正成为现实。同时，这一事件使网络战和物理战争在冲突中深度融合，开启了网络战的新篇章，其影响可能将会极其深远。

# 事件还原：以色列如何打造现代特洛伊木马

黎巴嫩时间 9 月 17 日（星期二）下午 3 点 30 分左右，黎巴嫩真主党成员的寻呼机发出嘟嘟声，提醒其领导层有消息传来。

但这不是真主党领导人的信息，而是由真主党的死敌发出的。寻呼机信息提醒声发出几秒钟后，黎巴嫩贝鲁特南郊和其他真主党据点的数千台寻呼机同时发生爆炸。一时间，爆炸声和痛苦与恐慌的哭喊声，充斥着真主党据点的街道。

当天结束时，至少有十余人死亡，2800 多人受伤，其中许多人眼睛受伤、手指被炸断或腹部严重受伤而致残。

在寻呼机爆炸后的第二天，黎巴嫩再次发生爆炸，不过，这次爆炸的是真主党使用的对讲机，直接造成 20 余人死亡、600 多人受伤。

据路透社 10 月中旬披露，寻呼机和对讲机两次爆炸事件，在黎巴嫩共造成 39 人死亡、3400 多人受伤，其中包括真主党战士和伊朗驻贝鲁特特使。

据西方安全部门消息人士称，以色列情报机构摩萨德主导了此次寻呼机和对讲机爆炸事件。以色列既没有否认也没有证实其参与了袭击。袭击发生后的第二天，以色列国防部长约阿夫 · 加兰特称赞摩萨德取得了“非常令人印象深刻”的成果，以色列国内普遍将此解读为以色列承认该机构参与了袭击。

## 为何可能是以色列?

尽管以色列官员对相关指控不予置评，但大多数分析人士都认为，以色列很可能是此次袭击的幕后黑手。实际上，以色列也是少数拥有以这种方式渗透供应链的国家之一。

长期以来，真主党等伊朗支持的相关武装组织，一直受到以色列先进技术的攻击。

例如，2020 年，以色列使用通过卫星远程控制的人工智能辅助机器人，暗杀了伊朗顶级核科学家。此外，以色列还利用黑客手段阻止伊朗的核技术发展。2009 年和 2010 年，以色列与美国部署利用名为“震网”（ Stuxnet ）的计算机病毒 ，摧毁了伊朗核设施的大量离心机。

针对此次连环爆炸事件，美国国家安全局前情报分析员戴维 · 肯尼迪表示，这是其亲眼见过的规模最大、

> 以色列前军事情报部门负责人、著名战略专家阿莫斯 · 亚德林表示，此次袭击展示了“非常令人印象深刻的渗透能力、技术和情报”。

最有组织性的袭击之一。实施这一袭击所需的复杂性令人难以置信。人工情报(HUMINT) 是实现这一攻击的主要方法，同时还需要拦截硬件供应链，对寻呼机进行篡改。

以色列前军事情报部门负责人、该国著名战略专家之一阿莫斯 · 亚德林表示，此次袭击展示了“非常令人印象深刻的渗透能力、技术和情报”。

评论人士认为，袭击行动可能是为了在真主党成员中制造高度恐慌，削弱其招募人员的能力，并削弱人们对真主党领导层的信心，以及他们确保行动和人员安全的能力。

## 为何是寻呼机?

真主党长期以来一直宣称保密是其军事战略的基石，因此一直放弃使用高科技设备以避免以色列和美国间谍软件的渗透。与中东其他非国家组织不同，真主党部队据信通过内部通信网络进行交流。这被认为是该强大组织的关键组成部分之一，因此，长期以来该组织一直被视为国中之国。

根据美国情报评估，多年来，真主党领导人哈桑 · 纳斯鲁拉一直敦促真主党使用寻呼机。寻呼机功能有限，但可以接收数据却不会泄露用户的位置或其他信息。

据路透社报道，真主党组织在意识到手机通信遭以色列窃听后，于今年年初改用寻呼机。真主党领导人哈桑 · 纳斯鲁拉要求黎巴嫩南部的真主党成员及其家人交出手机，因为他认为以色列可以通过这些设备追踪到真主党成员的动向。

纳斯鲁拉的忧虑部分源于其盟友的报告。相关报告称以色列已经掌握了入侵手机的新手段，可以远程激活手机麦克风和摄像头来监视手机用户。真主党及其盟友之间流传着这样一种传言：任何手机通信，甚至加密短信应用，都已经不再安全。

据前以色列情报官员和中东分析师阿维 · 梅拉梅德称，正是在这样的背景下，真主党转而使用寻呼机等低端设备，认为这些设备比可能被具有 GPS 功能的手机更安全。

据两名美国情报官员透露，2024 年夏天，运往黎巴嫩的寻呼机数量有所增加，数千台寻呼机运抵黎巴嫩，分发给真主党军官及其战士。

对于真主党来说，这是一种防御措施，但以色列情报人员则将寻呼机称为可以在时机成熟时按下的“按钮”。

## 寻呼机是如何躲过检测的?

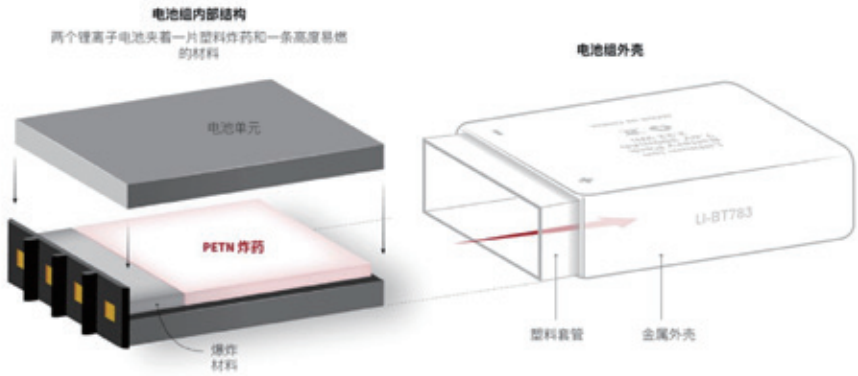
随着黎巴嫩遭受系列爆炸袭击，各界开始猜测，这些低端通信设备是如何躲过安全检测的。寻呼机炸弹和电池的秘密设计和精心策划表明，这是一次执行长达数年的长期行动。

据路透社报道，在真主党领导人纳斯鲁拉决定扩大寻呼机的使用范围之前，以色列就已开始实施这一计划。在真主党领导人要求其成员改用寻呼机之后，以色列特工看到了机会。

根据路透社发布的电池组拆卸照片，制造寻呼机的特工设计了一种电池：两个矩形电池之间暗藏了少量（6 克）但威力巨大的薄方形塑料炸药，以及一条高度易燃的物质作为雷管。由于不含任何金属成分，这种用于引爆的材料有一个优势：就像塑料炸药一样，无法用 X 光机检测出来。

据知情人士透露，在今年 2 月收到寻呼机后，真主党立即检查是否有爆炸物，并将其放入机场安检扫描仪中，看是否会触发警报。但并未发现任何可疑情况。

据电池专家表示，由于炸药和包装物占据约三分之一的体积，因此，电池



组的电量有所降低。消息人士称，真主党注意到寻呼机的电池耗电速度比预期的要快。不过，这个问题似乎并未引起重大安全担忧——真主党组织在爆炸前数小时，仍在向其成员分发寻呼机。

## 内部调查遭遇挫折

从外观来看，这款讯寻呼机的电源与消费电子产品中使用的普通锂离子电池组类似。然而，这种标有 LI-BT783 的电池在市场上并不存在，就像这款寻呼机本身一样。

据媒体报道，真主党的采购审查非常严格，以色列特工必须确保他们制造的寻呼机能够通过检查。

为了掩盖问题，即为这个新产品编造一个难以令人信服的故事，以色列特工建立了空壳公司，冒充寻呼机生产商，同时还创建了虚假的网上商店和页面，以欺骗真主党的检查。

为特工行动编造故事一直是间谍机构的核心技能。寻呼机的故事之所以不同寻常，是因为这些技能被运用到了无处不在的消费电子产品上。

为了欺骗真主党，以色列特工决定以合法品牌台湾金波罗公司的名义销售定制的 AR-924 型号寻呼机。爆炸事件发生后，金波罗董事长对外称，该公司是这一阴谋的受害者，对寻呼机的杀伤力及袭击真主党的行动一无所知。

该公司在声明中表示，AR294 型号寻呼机“由 BAC 咨询公司生产和销售。金波罗仅提供品牌商标授权，不参与该产品的设计或制造。”

从表面上看，BAC 咨询公司是一家总部位于匈牙利的公司，依据合同代表台湾公司金波罗生产这些通信设备。据情报官员称，事实上，该公司只是以色列特工的幌子。此外，至少还创办了两家空壳公司，以掩盖制造寻呼机者的以色列情报官员身份。

为此，BAC 咨询公司生产了一系列寻呼机。但它唯一真正重要的客户是真主党。这种暗藏 PETN 塑料炸药的寻呼机，于 2022 年夏天开始少量运往黎巴嫩，在 2024 年后产量迅速增加。

真主党领导人曾表示后悔购买了寻呼机，并展开内部调查，以了解安全漏洞是如何发生的，并找出可能的内奸。

这一仍在进行的内部调查遭遇挫折：寻呼机袭击发生 11 天后，即 9 月 28 日，负责领导采购调查的真主党高级官员纳比勒 · 卡奥克 (Nabil Kaouk) 本人在以色列空袭中丧生。

**电池电源**

质量类似为 35 克的电池的预期能量容量约为 8.75Wh，而不是 2.22Wh。

# 解读：寻呼机爆炸事件颠覆了哪些网络战传统认知？

本文撰稿　赵慧杰

黎巴嫩9月17日、18日连续发生寻呼机和对讲机爆炸事件，至少造成39人死亡，数千人受伤。黎巴嫩真主党指责对手以色列发动了这些攻击，称其已越过“所有红线”，并誓言将会实施“正义的惩罚”。外界分析普遍认为，以色列是此次爆炸行动的幕后主使，但以色列至今仍未承认对爆炸事件负责。

目前，公开来源信息还远未能揭示事件的全部真相，有关此次事件的内情可能需要有关情况解密或曝光才能完全为外界所知。本文尝试基于已经掌握的情况，从军事、政治、技术和法律角度出发，剖析事件疑点和谜题，分析攻击活动的创新性和颠覆性，并提出对新时代网络攻防态势的启示和思考。

## 一、事件疑点剖析

### （一）爆炸物载体是什么？

目前，关于此次事件的爆炸起因，媒体、学者和专家众说纷纭、说法不一。有多种方式可以导致寻呼机、对讲机爆炸，外界对爆炸载体分析主要集中在预置微型爆炸物和通信设备本身电池上。电池爆炸的原因有多种，主要包括内部压力过大、外部加热、化学反应过快等。有观点认为，袭击者可能设法通过化学反应使设备电池过热，从而引发爆炸。

笔者认为这种观点可能性不大，原因有三：

一是曝光的爆炸视频显示，爆炸的破坏范围和烈度显然超出了电池爆炸的威力。英国前陆军军官、爆炸物处理专家肖恩·穆尔豪斯表示，“从视频来看，爆炸的规模与单独使用电雷管或使用含有极小高爆炸药的电雷管引起的爆炸规模相似。”

二是电池过热爆炸前应该有过渡时间，会引起大量通信设备使用者的警觉，而此次事件造成大量人员伤亡，表明爆炸的启动时间较短，使用者没有时间做出反应。

三是通信设备电池通常都具有过

热自保护措施，包括嵌入保护板等，外因诱发化学反应导致的电池过热爆炸成功率不高，与事件的实际情况明显不符。英国陆军某退役拆弹人员表示，“爆炸装置主要有五个组成部分：容器、电池、引爆装置、雷管和炸药，寻呼机上已经有三个组成部分，你只需要加上雷管和炸药。”

综合分析认为，事件中的通信设备爆炸极有可能源于设备中被预先暗藏的微型炸弹。

**（二）是否源于网络攻击？**

目前曝光情况反映，真主党成员使用的寻呼机几乎同时于当地时间 9 月 17 日 15 时 30 分发生爆炸。针对通信设备爆炸物的引爆机制分析集中在两个方面：一是预先设置的定时炸弹；二是网电信号指令引发的爆炸。笔者认为定时炸弹的可能性不大，原因有二：

一是从地区冲突局势上看，自事件的嫌疑幕后主使以色列与哈马斯冲突 2023 年 10 月爆发冲突以来，其与跟哈马斯站在同一战线的真主党暴力冲突不断。此次事件的通信设备约于 5 个月前购置，而事件主使不太可能未来局势不明朗的情况下选择设置定时爆炸，更可能会选择“把引线留在手中”，将装置设定为收到特定指令时才会爆炸，从而掌握主动性并避免失控态势。

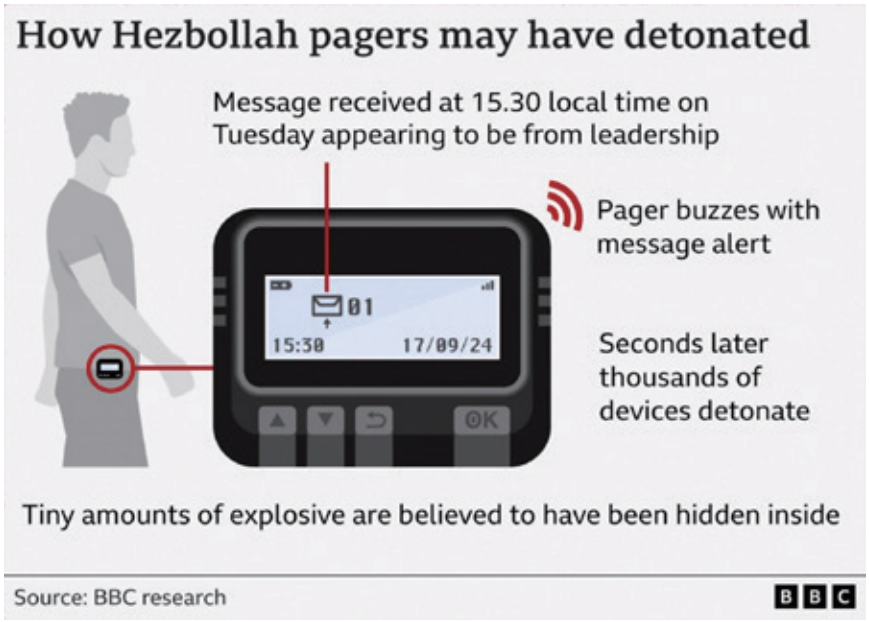
二是从技术原理上看，寻呼机、对讲机均可接收网电信息，为择时引爆内置炸药提供了方便途径和渠道。情况反映，携带寻呼机的人员听到传呼机发出提示音，收到被认为来自真主党领导人发来的信息，当他们正在阅读这些信息时，寻呼机发生爆炸。

综合分析认为，事件中的通信设备爆炸促发机制很可能源于传呼机和对讲机的通信网络遭渗透，设备在接收到特定的信号或代码后发生爆炸，即“由比特数字触发的 PETN 爆炸”。

**（三）是否违反国际人道法？**

国际人道法基本准则涉及，“失去战斗能力、已退出战斗及未直接参与战斗的人士，其生命及身心健全均有权受到尊重。在任何情况下，他们都应受到不加任何不利区别的保护与人道对待。”“冲突各方及其武装部队成员选择战争的方法与手段均受到限制。使用具有造成不必要损失或过度伤害性质的武器或战争方法，均受禁止。”“冲突各方在任何时候均应将平民居民与战斗员加以区分，以避免平民居民及平民财产受到伤害。不论是平民居民还是平民个人，都不应成为攻击的目标。攻击应只针对军事目标。”

黎巴嫩真主党是伊朗资助成立的什



叶派黎巴嫩伊斯兰政治和军事组织，其宗旨是消灭以色列，并将西方势力逐出国内。该组织性质极具争议，其自创立以来即于国内属合法政党，但其同时被美国、英国、以色列、澳大利亚、加拿大、德国、欧盟、海湾阿拉伯国家合作委员会等国列为恐怖组织。

从结果事件影响来看，此次攻击行动显然违背了国际人道法，原因在于：此次攻击爆炸针对是真主党订购的数千台寻呼机、数百台对讲机的拥有者，行动的针对性只能说是“相对集中和精准”，体现出控制范围和烈度意图，但未充分考虑设备拥有者的身份（是否战斗人员）、所在位置（住宅、汽车、杂货店或咖啡馆）和周围环境（周围是否有平民人员或目标），在动用武力手段实现军事目标过程中未区分平民目标和军事目标，也未采取有可行措施预防平民伤害，不符合国际人道法规定的攻击中的“区分”“相称”“预防”等关键原则。

联合国人权事务高级专员福尔克尔·蒂尔克表示，国际人道法禁止使用诱杀装置，这种装置是看似无害的便携式物体，经过专门设计和制造，可以装载爆炸材料。其中，所指的“诱杀装置”是指其设计、制造或改装旨在致死或致伤，而且在有人扰动或趋近一个外表无害的物体或进行一项看似安全的行动时出乎意料地发生作用的装置或材料。

综合分析认为，此次行动针对数千台设备持有目标人员实施无差别爆炸攻击，导致非战斗人员甚至平民伤亡及平民财产损失，在适用情况下违反了国际人道法。

## 二、此次特别网络行动的创新性和颠覆性

### （一）从行动方式来看，通过软硬供应链攻击，实现现代“特洛伊木马”计划

此次行动极有可能是某种供应链攻击，即在制造或运输过程中对寻呼机和对讲机进行篡改。供应链攻击涉及使用第三方工具或服务（统称为“供

应链”）来渗透目标系统或网络，可能针对由第三方管理的硬件、软件、应用程序或设备。

供应链攻击在网络安全领域日益受到关注，最近很多重大网络安全事件都是黑客在产品研发过程中获得访问权限导致的，如 SolarWinds 攻击、Kaseya 勒索软件攻击等。但此类攻击通常局限于软件，硬件供应链攻击则相对少见，因为这涉及对设备的人工物理接触。

美国智库“新美国安全中心”的高级研究员维韦克·奇尔库里表示，“两轮攻击都可能起源于所谓的供应链攻击：在寻呼机和对讲机的生产节点，就被渗透了。少量的爆炸性物质被添加到这两种设备中，让它们在特定时间被远程引爆。”前英国军队弹药专家表示，这些设备可能在假电子元件中隐藏了 10~20 克的军用级高爆炸药。1996 年和 2000 年，哈马斯的主要炸弹制造者叶海亚·阿亚什及法塔赫活动家萨米赫·马拉比均死于“手机炸弹”，以色列军事和情报机构被认为是事件的幕后策划者。上述两次猎杀行动可被视为此次爆炸事件的“先锋”，而此次爆炸袭击的不同之处在于其规模更庞大。

除硬件篡改外，此次行动还可能涉及对设备应用程序的操纵及通信渠道的入侵。

综合来看，此次爆炸事件可被视为基于供应链渗透和设备武器化的成功网电攻击行动，其行动方式新颖且大胆，具有与“震网”攻击、“手机炸弹”攻击相类似的元素，如人力介入、硬件接触和设备篡改等，符合以色列军情和情报机构的行事风络，也反映出以色列网电攻击手段的创新和发展。

**（二）从毁伤效果来看，通过动能与非动能打击相结合实现“目标斩伤”**

从历史来看，军事战争主要是通过使用物理力量来破坏或摧毁物质资产，所使用主要是动能武器。进入现代信息化战争时代，网络战、电子战、定向能和信息战等非动能效应手段也在不断发展，并为动能攻击手段提供了补充。网络攻击通常造成的影响是非动能数字损害，包括系统停转、信息被资、数据泄露，以及由此衍生的服务停顿、物理损害、经济损失、名誉受损等，鲜见由网络攻击直接引发的人员伤亡和财产物理损失。美军联合出版物 JP 3-0 号《联合作战》认为，网络空间攻击是一种可产生非致命效果的能力，能产生这种效果的还包括电子攻击、军事信息支援作战及非致命武器。

对比来看，动能攻击与网络攻击的主要区别包括：

一是动能攻击的介入和效果具有瞬时性（如发射导弹并摧毁目标），而非动能网络攻击手段则具有跨时性，如需要长时间来对目标开展情报侦察、研制网络攻击武器、获取目标访问权限、渗透并植入攻击载体、实施攻击行动等；

二是动能攻击产生的物理损伤效果几乎是不可逆的（如射杀人员、炸毁建筑物等），而网络攻击的效果则可以产生完全可逆的效果（如恢复系统运转等），可逆性既是网络武器的优势、也是其局限性；

三是动能攻击影响具有局限性，通常限定于一定范围的物理区域内，而网络攻击则具有广泛性和衍射性，可对广域分布式目标实施攻击并产生级联效应；

四是动能攻击的效果具有量化可预测性（如导弹的毁伤半径等），而网络攻击的效果可能因目标软件、硬件和用户配置的变化而具有不确定性。

此次爆炸行动开创了动能攻击与网络攻击深度融合的先河，展现出俄乌网络战争从未呈现的新型网络技战术，并取得了“先发制人”式闪击效果，除造成大量真主党成员伤亡外，还破坏了真主党指挥通信网络，是一次现代战争的成功网络战战例。

此次爆炸行动还彰显出网络攻击在现代战争中的威力还远未得到挖掘释放，其不仅是军事行动的一种火力形式，在与动能攻击相结合的情况下，还能产生“互相补充、力量倍增”的效果，在保留动能攻击效果不可逆、量化可预测的基础上，还能突破时空限制，瞬时对广泛、大量目标实施打击，以达到最大作战效果。

未来，动能与网络攻击手段的结合可能在常规战争冲突的重要军事战略工具，为国家实现军事目标提供新的渠道。

**（三）从资源统筹来看，通过情报、人力和技术相结合实现缜密部署**

此次通信设备爆炸行动是一次特种作战行动，事先必然经过长期和缜密的策划，并对情报、人力和技术等大量资源进行综合性、精准性统筹和调度。专家认为，此次爆炸的策划准备可能需要数月到数年的时间，需要动用大量人力、物力资源。前美国网络司令部司令保罗·中曾根表示，此次爆炸行动展示“令人震惊”的情报收集能力，肇事者“拥有令人难以置信的情报定位能力，能够真正了解这些号码，知道谁拥有这些号码，并且知道他们使用这些号码的频率”；对真主党的秘密袭击表明了对其成员的“透彻了解”，并且对目标“非常熟悉”。纽约大学学者尼古拉斯·里斯认为，此次攻击的复杂程度表明，肇事者长期以来一直在收集情报。英国皇家国际事务研究所的莉娜·哈提卜表示，此次袭击表明，以色列已经“深度渗透”了真主党的通信网络。

从攻击的规模来看，策划实施此次攻击需要几个方面：

一是精确的情报信息。需要获取目标人员使用的设备信息（型号、配置等）、采购设备的渠道，以及通信设备操作机制和所运行网络，开发能够确认目标携带设备的情报来源。

二是成功的人力介入。需要建立必要的人力关系和渠道，获得寻呼机、对讲机的物理访问权限，并对设备进行物理篡改及在设备系统中建立立足点。

三是可行的技术操作。需要对目标设备开展技术分析，开发将爆炸物

嵌入设备的技术及通过网信手段引爆爆炸物的技术，具备在执行前不被发现地渗透和操纵该通信设备网络的能力，且极可能提前对整体行动进行了技术测试和验证。

此次复杂爆炸攻击行动涉及环节众多，资源协调统筹及相互配合的难度极大，任何环节或要素出错都可能导致行动失败，在部分要素上完全可以与“震网”攻击行动相媲美，是一次网络战、渗透战和情报战的成功结合。网信攻击手段可能只是此次爆炸行动的“最后扳机”，由人力、情报手段支撑的设备改造、行动决策、部署实施则为行动成功实施奠定了基础。

此次行动体现出，现代网络战并非单纯的技术战，还必须要有精确的情报作为支撑，并在适用的情况下结合人力特种行动，才能保障网络行动的成功实施。

（四）从行动影响来看，通过热战、网战和心战相结合实现跨域辐射。

两轮爆炸袭击粉碎了真主党煞费苦心建立的低技术通信网络，而以色列在事件前就已经破坏了真主党其他形式的现代通信网络。此次爆炸行动既削弱了真主党力量，也对该组织士气造成极大打击。事件不仅让真主党感到危机四伏，也让黎巴嫩民众人人自危，担心任何电子设备都可能被外敌动了手脚。有报道称，爆炸开始后的最初时刻，众多黎巴嫩民众惊慌失措，拔掉了家里的路由器甚至电视机的插头，担心爆炸物可能已经渗透到家用电器。

网络风险咨询公司 SecDev Group 联合创始人罗布·穆加表示，“这次史无前例的袭击，削弱了真主党对其通信电子设备和更广泛的第三方供应链的信心。这也严重削弱了真主党的沟通能力。”美国智库“新美国安全中心”的高级研究员维韦克·奇尔库里表示，“我认为以色列发出的信息是，即使真主党试图转向技术含量较低、本以为更安全的通信替代品，也仍然很容易受到攻击。‘我们仍然可以在你的口袋里找到你，无论你在哪里。’这对真主党的安全感产生了巨大的心理影响。”美国东北大学国际安全问题专家麦克斯·亚伯拉罕表示，“以色列的寻呼机袭击是一次非常有效的心理作战。它传达了一个信息：‘我们比你聪明。我们可以以你甚至没有意识到、甚至不理解的方式攻击你。如果你越界，你会以闻所未闻的方式付出代价，悔恨不已’。”

可见，此次爆炸行动集成了动能战、网络战和心理战，攻击发生在网信域，作用发生在物理域，影响发生在认知域。行动在物理域、信息域和认知域均对真主党造成了破坏性影响，达到了“一举三得”的效果。

在物理域，通过动能爆炸杀伤了真主党成员并破坏了其所用通信设备，影响了该组织的组织动员能力和指挥控制网络；

在网信域，渗透了真主党通信渠道，并瓦解了其通信网络，造成其内部互相猜疑，并迫使其另行布建新的通信网络；

在认知域，打击了真主党的士气，并干预了真主党成员的感知、认知、情绪、情感、观念、信念等意识活动，影响了真主党高层的决策权衡。

## 三、启示与思考

### （一）网络攻击形式创新性或将开启网络战新篇章

此次爆炸行动可以被视为网络战争和物理战争原则在当今冲突中融合的经典创新案例，或将开辟网络战的新致命前沿，开启网络战争的新篇章，并预示着网络战争将发展成为比黑客攻击和间谍活动更致命的战争活动。

此次行动还标志着军事战略的一个重要转折点，表明现实世界和虚拟世界间不再有明确的界限，网络和物理元素在战争中可以无缝集成，为更致命的混合威胁敲响了警钟。此次袭击行动不仅仅是一次战术打击，还代表了战争模式的深刻转变，数字和物理领域不仅相互联系，而且融合成一个单一的、强大的战线。先前的网络战例通常破坏性较低，用于实现非关键性的动能目标，主要涉及间谍活动、数据盗窃或基础设施破坏。但能够造成物理伤害的网络攻击的能力则完全将破坏性提升至更高层次，源自数字世界的攻击威胁不再像以前那样是虚拟的、跨时的、可逆的，而是有能力对现实世界造成实际的、即时的、不可逆的影响。

此次事件体现了网络物理系统的巨大潜力和固有风险，为未来的军事行动提供了蓝图，表明网络能力不仅可用于间谍活动或破坏，还可以用作直接动能武器；或将打开网络战的“潘多拉魔盒”，启示民族国家开发新的网络战技战术，进一步推动网络空间军事化程度。

### （二）国家网络安全防线建设需要树立体系化思维

此次事件将促使全球重新思考国防和安全战略，凸显强有力的网络安全措施的迫切需要，以及在数字和物理基础设施界限日益模糊的时代，不断创新以保护相互连接的数字和物理基础设施的紧迫性。

在新的时代，网络安全威胁的来源将不再局限于单个漏洞、系统或设备，构成最严重网络威胁的主体将是国家级对手。与普通黑客组织或个人相比，国家级对手能够安排、调动、整合国内人力和资源，甚至可能联合利用国际盟友力量，来实现“数字军火的大融合”。其技术能力强大，拥有成熟的网络攻击技战术，且渗透渠道多样、手法更加隐蔽。尤其是国家级对手还能动用间谍情报机关，通过对目标开展侦察获取敏感信息，通过拉扰策反等手段打入目标内部，甚至派遣特工直接实施人工操作，导致网络安全威胁更趋严峻复杂。

因此，要应对国家级对手构成的严峻威胁，必须树立体系化网络安全建设思维，变“单打独斗”为“联合作战”，集成和发挥政产学研军等各方力量，构建实战化网络安全防御体系，筑牢数字时代安全基石。

此次爆炸行动可以被视为
网络战争和物理战争原则在当今冲突中融合的
经典创新案例，
或将开辟网络战的新致命前沿，
开启网络战争的新篇章。

**（三）网络安全防护需要跳出“重软轻硬”传统误区**

此次攻击可能会催生一个防御创新的新时代，重点是保护供应链和通信设备免受复杂的网络物理威胁。

相比于保护网络系统、软件应用、信息数据等的复杂网络安全机制相比，终端硬件的供应链物理安全获得的关注较少。此次事件告诉我们几方面信息：

一是高科技设备和低科技设备都可能被此类袭击破坏，即使是寻呼机、对讲机等已过时的通信设备经过篡改后也可能成为发动网络攻击的致命武器；

二是电子设备遭物理入侵可能会为间谍活动、破坏行动和网络攻击打开方便大门，对国家安全造成潜在的灾难性影响；

三是网络安全防护不仅仅要保护网络、软件和信息，还要保护通信设备中的物理系统，尤其需要加强设备供应链的监察和保护。

供应链风险无法通过单一措施来消除，但多种策略相结合可以大大降低风险，包括加强国内制造业、减少外国设备依赖、强化进口检验和测试规程、采用尖端安全技术（如基于区块链的跟踪系统）、实施硬件完整性检测等，确保从原材料到生产和运输的每个阶段都受到保护，以免受到渗透。

**（四）万物互联时代需扩大网络安全的内涵和外延**

当今社会已进入万物互联时代，大量智能设备和基础设施都与互联网紧密相连，智能手机、无人机、物联网设备已经成为当今社会不可分隔的一部分。上述设备如果遭受攻击，可能引发更大的灾难，对军队和平民都可能造成严重致命的影响。本次黎巴嫩爆炸事件表明，网络物理攻击领域的威胁较以前认知的更加多样化，汽车、家用电器、智能手环、耳机、智能门禁、医疗设备、军用电台、关键基础设施、太空飞行器都是潜在的攻击对象。相比于应用范围较小的传统的寻呼机、对讲机，对未来更先进、更复杂、更广泛应用的技术设备的网络物理攻击，在未来网络战争中具有潜在的更大破坏性。

可以预见，万物互联将催生更多前所未有的安全问题，把网络攻击面扩大到新维度，使网络攻击场景更加多样化，导致网络安全风险程度也将上升到新高度。伴着新风险、新隐患，需要并行探索和扩展网络安全的内涵和外延，不断丰富和创新安全理念和思维，加快推动网络安全技术的研发和实践落地，构建全方位、多维度的网络安全监测与防御体系。

# 分析：黎巴嫩寻呼机爆炸三个特点

黎巴嫩寻呼机爆炸事件，可能是一场精心策划、利用各种技术实施的攻击行动，包括硬件供应链攻击、软件漏洞和数据窃取，显示网络攻击将发展成为比黑客攻击和间谍窃密更致命的形式。

随着网络空间和传统物理领域的战场越来越模糊，网络安全防护除了保护传统的网络、信息和隐私安全，还需要考虑保护硬件供应链的完整性。

## “一切武器化”正成为现实

此前，以色列曾被指控使用篡改通信设备实施暗杀，包括 1996 年通过装有炸药的手机杀害哈马斯炸弹制造者叶海亚 · 阿亚什 (Yahya Ayyash)，但此次袭击的规模之大是前所未有的：数千部设备同时引爆。

因此，分析人士预计，以色列实施的真主党通信设备爆炸，可能开启网络空间地缘政治竞争的新阶段。

在过去数十年里，以色列经常通过利用非常规的战术和先进技术来攻击对手。2009 年，以色列和美国利用震网病毒（Stuxnet ）恶意软件针对伊朗核计划实施网络攻击。根据国际原子能机构的数据，震网病毒造成严重的破坏，2009 年至 2010 年年初，伊朗因震网病毒造成的破坏而被迫更换约 1,000 台离心机，严重打击了伊朗的核计划发展。这一事件在全球首次展示了网络武器对物理空间的重大影响。

随后，以色列国防军于 2019 年 5 月轰炸加沙地带的哈马斯技术部门，以阻止潜在的网络攻击。以色列的反应开创了先例，成为地区冲突中首个以军队实时应对网络攻击的案例。

此外，以色列还被指责针对伊朗科学家实施了长达数十年的秘密行动。据报道，以色列情报机构于 2021 年使用人工智能遥控狙击机枪杀死了顶级核科学家 Mohsen Fakhrizadeh。这是首次有记录的远程遥控此类设备。

这次攻击事件所展示的战略创新应该引起更多人的关注。它提出了一个令人不安的问题：只需要跳出固有的思维模式，像寻呼机这样简单的东西都可以武器化。长期以来，真主党一直依赖过时但安全的寻呼机通信系统，来保护敏感信息免受现代黑客技术的攻击。当这

> 爆炸事件证实了许多人猜测即将发生的事件：21 世纪冲突将出现日常物品的武器化。“一切武器化”，这种好莱坞电影惊悚片的情节，正在成为现实。

些曾用于协调军事行动的设备成为毁灭性武器时，这种看似安全的局面被打破了。信号很明确：无论多么过时或看似安全，没有哪个系统能够免受网络操纵。

可以说，黎巴嫩寻呼机和对讲机爆炸是许多人猜测即将发生的事件之一：21 世纪冲突中日常物品的武器化。“一切武器化”，这种好莱坞电影惊悚片的情节，正在成为现实。

奇安信观星实验室负责人龚玉山认为，寻呼机爆炸事件可能是未来时代战争的先兆。因为从理论上来说，所有的智能硬件设备，都能通过生产链大规模预先安装爆炸装置。

智能手机、无人机、物联网 (IoT) 设备已成为当今社会的一部分。相比寻呼机，智能手机要复杂几个数量级、电池更大、电路更复杂、传感器也更多，完全可能作为未来网络战的攻击途径。试想一下，如果所有这些更高级、更复杂的设备受到攻击，可能造成什么样的灾难?

因此，降低物联网设备、智能电子和通信设备的攻击可能性，将成为网络安全面临的一大挑战。

## 首个硬件篡改攻击，凸显供应链武器化的灾难后果

在网络空间，敌对各方会一直试图破坏对方的关键基础设施，包括通信网络。

尽管近年来各国互相指控对方在设备中植入后门漏洞，但黎巴嫩真主党寻呼机遭篡改，是已知的第一起在生产层面篡改硬件的案例。这暴露出供应链漏洞被武器化后将会灾难性的后果。武器和弹药情报专家、咨询公司 Armament Research Services 主任任詹森 · 琼斯( Jenzen-Jones )表示:“事件的规模表明，这是一次复杂的供应链攻击，而不是设备在运输过程中遭拦截和修改的场景。”

供应链攻击在网络安全领域越来越常见，但通常以软件为目标；针对硬件的攻击则少见得多，因为需要能够实现对设备的物理访问。对于缺乏国家背景的攻击组织，可能难以获得对设备制造阶段的深入访问权限，但具有国家背景的攻击者则可以通过适当的资源实现这一目标。

利用供应链漏洞的战略利益尚待商榷。但鉴于其可能造成的巨大破坏和损失，至少在短期内，将会导致更多的攻击者试图利用供应链漏洞来攻击对手。考虑到硬件供应链遍布全球各地，且缺乏严格监管，其不透明性显示了供应链的脆弱性，无意会加剧相关担忧。

科技行业和供应链分析师表示，科技公司可能会将此次攻击视为一次强烈的提醒，提醒他们确保供应链安全的重要性，而公众对科技的信任也可能受到打击。

加州州立理工大学伦理与新兴科学组主任帕特里克 · 林（Patrick Lin）表示，不知何时，数千个装置被制成武器，却无人察觉。这些爆炸装置分布有多广？爆炸物是如何进入装置或装置供应链的？这次袭击引发出了一些以前从未考虑过的可怕问题。

牛津大学数字伦理与防御技术教授马里亚罗萨里亚 · 塔德奥表示，攻击开创了一个令人担忧的先例，因为其中对供应链的干扰“不是出于特定的破坏行为，而是为了进行分布式、影响深远的攻击”。

迪拜科技公司 Ombori 首席执行官安德烈亚斯 · 哈塞洛夫 (Andreas Hassellof) 表示，爆炸事件为我们敲响警钟，“提醒我们需要彻底改革应对供应链安全的方法。”

阿布扎比网络安全公司 Cypherleak 的首席执行官穆罕默德 · 贝拉比 (Mohamed Belarbi) 表示：“如果一部手机或设备在到达你手中之前，在制造商或供应链层面遭到篡改，你什么也做不了。因为即使打开了一部 iPhone 或三星手机，你也难以发现问题。”

与保护当代设备的复杂机制相比，终端硬件安全却鲜受关注。美国康奈尔科技大学数字和信息法教授詹姆斯 · 格里梅尔曼表示：“每家生产或销售数字设备的公司都会担心其供应链的完整性。”“他们可能会考虑增加额外的保障措施和验证措施，以便能够更好地检测和阻止此类举动。”

惠普公司发布的一项全球调查显示，针对硬件供应链的攻击和设备篡改预计会增加，研究强调，企业需要关注设备硬件和固件的完整性。

安全专家认为，要减轻终端硬件安全风险，需要进一步加强电子设备的反破坏措施、确保供应链安全、建立更严格的敏感技术转让出口管制措施，并加强对网络空间负责任行为的问责制。

帕特里克 · 林（Patrick Lin）则认为，攻击事件会进一步加速“在一国境内自主研发技术，以加强对供应链安全控制的努力”。 澳大利亚新南威

尔士大学供应链专家米拉德·哈加尼(Milad Haghani)预计，（数字设备）将会看到一场“广泛的清算”，导致制造企业加强其供应链安全协议。 对于整个科技公司来说，这种情况的规模是前所未有的，许多公司以前可能没有如此重视其生产流程的安全性。因为许多公司可能还没有完全配备应对此类威胁的设备。

## 网络攻击和物理战深度融合的经典案例

寻呼机爆炸事件表明，网络战争将发展成为比传统黑客攻击和间谍窃密更致命的战争。这次攻击可以被视为网络战争和物理战争在冲突中融合的经典案例，开启了网络战争的新篇章，其影响可能远远超出当前事件。

黎巴嫩真主党通信设备爆炸，将网络战的后果带到物理领域。如果引发其他攻击者效仿，将对网络空间的稳定产生更广泛的影响。

网络战主要被定义为窃取机密信息、进行间谍活动或使主要设施失灵。这一事件以物理形态的影响展现出网络攻击的巨大威胁，表明数字世界的威胁不再像以前那样是虚拟的——它们非常有能力对现实世界造成巨大影响。此外，现实世界和虚拟世界之间不再有明确的界限，这次袭击可能是对更致命混合威胁的警告。

更令人难以置信的是，这些爆炸是通过一种越来越被视为过时的通信设备实施的。将寻呼机改装成简易爆炸装置的案例表明，即使有人认为这些装置已经过时，它们也可能具有未知的负面能力。

在大多数关于网络安全的讨论中，我们经常听到保护新的复杂系统——在此次事件中，攻击者却成功破解和利用了古老的系统，将一种简单而无害的工具变成了致命武器。真主党维护和使用这种原始系统是为了避免复杂网络攻击，但这样做却正好落入了为其设置的陷阱。

寻呼机爆炸事件表明，网络攻击的威胁比以前考虑的更加多样化。在这个几乎所有设备都相互关联的时代，通信设备故障的影响不仅对军队，而且对平民都可能造成严重致命的影响。

安全专家警告称，我们正面临一种新的威胁，这种威胁模糊了数字和物理漏洞之间的界限。信息很明确：要么适应，要么成为攻击目标。坚持使用过时安全模式的组织不仅落后，而且还会面临灾难性的后果。安

（本期黎巴嫩系列爆炸事件专题由奇安信威胁情报中心、网络空间安全军民融合创新中心、奇安信观星实验室等联合供稿。）

> 这次攻击可以被视为网络战争和物理战争在冲突中融合的经典案例，开启了网络战争的新篇章，其影响可能远远超出当前事件。

规划快一步

奇安信 | BEIJING 2022

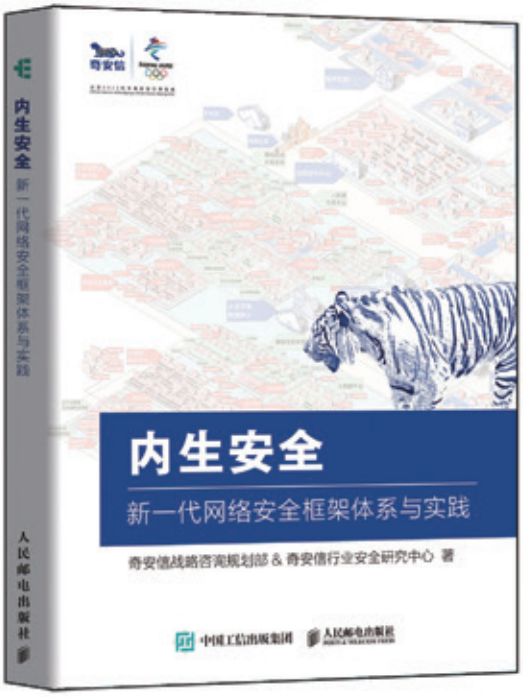
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

# 新书发布

## 内生安全权威解读

19支团队、37位专家倾力打造

政企“十四五”网络安全规划必读书籍




- 什么是内生安全
- 内生安全从何而来
- 为什么要内生安全
- 内生安全如何落地
- 新一代网络安全框架
- “十工五任”建设要点

扫描二维码
专享内购价

# 厦门国际银行安全编排与自动化响应系统的创新实践

作者 厦门国际银行 沈忱 林建庭

随着业务的持续发展，新的业务需求和技术应用可能带来新的安全漏洞和风险点，使得商业银行面临的安全风险也在不断增加。为了有效防范和应对各种内外部安全威胁，商业银行需要不断提高安全运营效率，以确保业务的持续稳健发展。

近年来，厦门国际银行对网络安全、金融科技、数字转型等领域的前沿技术进行了积极地探索与实践，持续强化网络安全建设，并将其视为银行经营和发展的关键。基于此，厦门国际银行通过引入奇安信提供的安全编排与自动化响应（Security Orchestration, Automation and Response,SOAR）技术，建设SOAR系统，实现了安全运营过程中人员、流程和工具三大要素合一，逐步迈向安全运营自动化时代。

## 一、安全运营工作面临的挑战

经过多年的安全运营建设，厦门国际银行现有安全防护设备较为齐全，并通过安全监控平台建设实现了日志和告警数据统一化处理，同时实现了安全事件的闭环管理。随着攻防对抗的日益激烈，现有的安全运营模式逐渐显现出弊端，如大量的安全告警、过长的响应时间、缺乏标准化的响应流程等。具体而言，安全运营工作面临如下挑战。

### 1. 人工分析时间过长

此前，厦门国际银行完全依赖工程师人工进行威胁分析。在威胁分析

过程中，往往会涉及大量原始日志查询等操作，工程师要频繁访问、来回切换不同的安全设备和系统，以判断告警的真实性，导致分析效率较低。

**2. 处置自动化程度有限**

此前，厦门国际银行仅少数安全攻击场景可通过联动安全检测和处置设备执行策略，实现秒级自动化响应；绝大部分场景需要协调网络管理员或值班人员人工执行策略，自动化程度较低，处置时间较长。

**3. 重复性基础工作量较大**

安全运营往往涉及大量重复性工作，如策略配置、权限变更、日志检索等，由于重复性工作通常需要大量时间，占据安全运营人员大量精力，导致有限的人员无法聚焦真正有威胁的安全事件，难以快速提升银行实战攻防能力。

**4. 缺乏标准化应急处置流程**

以人工为核心的安全运营模式主要依赖安全运营人员的经验，容易因为人员的业务熟悉程度、攻防技战术水平，以及人员变化等因素产生不确定影响，导致事件响应时间及事件处置完成程度不可控，甚至发生运营安全风险。此外，安全运营人员的经验缺乏体系化的积累和传承，难以复制和传递，不利于拉升银行整体安全运营水平基线。

## 二、SOAR 系统建设思路

为贯彻厦门国际银行安全运营的体系化、实战化、常态化建设理念，需要通过可编排、自动化的方式，整合现有工具、人员及流程，将面向分散的设备和系统的一系列操作串连起来，并根据不同的威胁响应将工作流程加以固化，使得响应的过程更加顺畅，并能够复制与传递。

SOAR 是近年来信息安全领域的一个新概念，它以安全编排和自动化为核心，将人、流程、技术和工具进行高效整合，辅助安全运营人员完成日常工作，可显著提升安全运营效率；能够自动化处理安全事件，减少人工干预，缩短响应时间，降低安全风险；同时，还能通过案例集管理和协作，提升威胁分析效率，实现安全能力的可视化编排与自动响应。

总体而言，通过构建 SOAR 系统，商业银行可实现场景体系化梳理、流程标准化落地，以及安全能力归一化资源池建设，初步形成自动化安全运营体系。

**1. 建设目标**

在参考大量实践案例、进行多项产品调研后，厦门国际银行与奇安信公司达成合作，并结合实际业务需求和现阶段网络安全建设特点，构建了 SOAR 系统，具体建设目标包括但不限于以下几点。

一是告警研判自动化。SOAR 系统应按照既定规则，定期主动从各类安全设备中拉取告警数据，自动或半自动地执行告警分析与智能分诊，将安全运营人员从处理海量告警的工作中解放出来，使其能够更加专注于更高级别的威胁。

二是响应处置闭环化。SOAR 系统将大量标准化应急处置动作固化成剧本，在完成告警分诊后，可根据已有的标准自动化处置大量同类告警，从而大幅缩短响应时间，提升响应效率，并且完成从告警分诊、分析研判、响应溯源到弱点加固的闭环流程。

三是安全运维剧本化。SOAR 系统基于剧本编排功能，将重复性高的安全运维工作固化成剧本，使大量设备的安全运维工作按照标准化的剧本执行。

四是事件管理知识化。安全事件处理的案例可保存在 SOAR 系统并形成案例库，后续形成统一共享的知识库，以便供他人按照以往的经验快速解决问题。

**2. 功能架构**

SOAR 系统是以安全告警为输入内容、以内置的剧本为基础、以自动化处置为主，辅以人工判断，协助安全运营人员进行威胁分析和响应处置的平台。SOAR 系统作为连接中枢和调度中心，支持 RestAPI、Kafka、SSH、TELNET、SYSLOG 等多种远程调用方式，集成上游系统如安全监控平台、日志系统和应用系统，下游系统如安全设备、网络设备、情报服务等。SOAR 系统功能架构如图 1 所示。

SOAR 系统功能模块总体上分为三部分：安全编排与自动化、事件管理和作战室。

**（1）安全编排与自动化**

安全编排与自动化是 SOAR 系统的核心功能，可实现安全能力的集成、

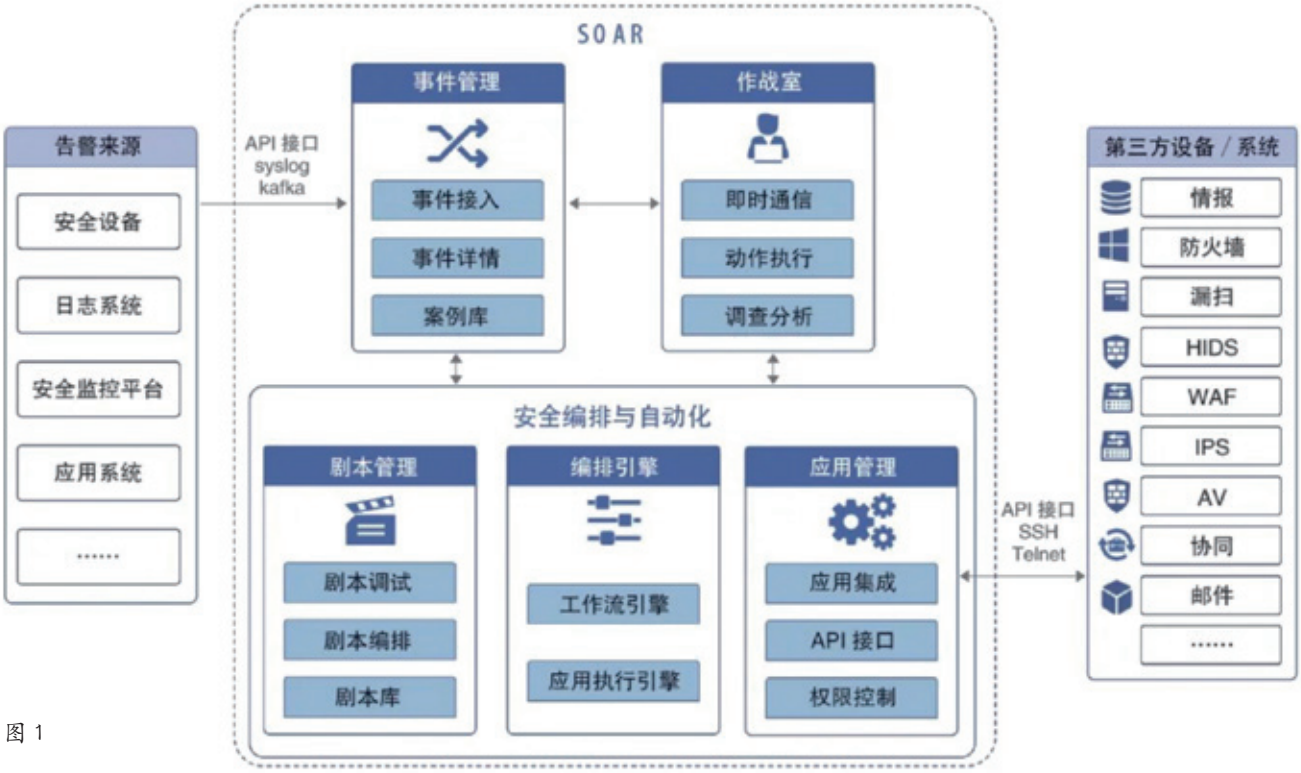



图 1

安全流程的编排与自动化执行，包括剧本管理、编排引擎和应用管理功能。

剧本管理功能为安全运营人员提供统一的剧本库，支持剧本的增删改查、导入导出，SOAR 系统内置可视化剧本编辑器，支持安全运营人员进行剧本编排创作，同时提供剧本执行详情，方便安全运营人员进行剧本调试。

编排引擎功能是安全编排与自动化的中枢，其中工作流引擎实现了剧本的编排调度和活动执行，应用执行引擎实现了安全处置能力的自动化调用。

应用管理功能为系统提供可扩展的集成框架。安全运营人员可以通过应用集成将安全设备能力封装成应用，提供给安全剧本调用。同时可提供基于角色身份的 FINANCIAL COMPUTER OF CHINA 应用动作权限控制功能，并实现权限最小化。

**（2）事件管理**

事件管理功能模块包括事件接入、事件详情和案例库三个功能模块。其中，事件接入功能模块通过采集多种来源的告警信息，为 SOAR 系统输入告警事件。事件详情功能模块提供整个事件处置过程中的各项关键信息记录，并为安全运营人员提供直观的展示，安全运营人员可以将整个事件处置过程转化成案例，以积累知识和经验。

**（3）作战室**

作战室提供一套面向安全运营人员的协同化响应处置工具，对应用、剧本和应对措施进行融合。安全运营人员可针对重要案例，以聊天运营的

方式进行实时沟通与响应处置。作战室可促进团队协作、贴近实战，并能生成作战报告，便于安全运营人员进行复盘和经验总结。

## 三、SOAR 系统建设成效

经过约 7 个月的部署、调试、开发与试运行，厦门国际银行 SOAR 系统实现了包括运维类、分析研判类和处置类的 20 个剧本场景，对接 14 个系统或安全设备，聚焦全局一键封禁 IP、终端中毒处置、多源情报聚合查询、弱口令检查通知、阶梯化 IP 封禁等剧本场景，实现典型场景剧本流程日常运营效率平均提升10倍以上（见表1）。

在告警方面，SOAR 系统可从安全运营中心（SOC）定期自动获取告警信息，实现告警解析、归并、信息富化，并衔接响应处理流程，完成自动化响应，体现出系统的灵活扩展能力，实现以最小的工作量完成自动化数据处理，从而高效驱动安全运营场景下的告警响应。

在处置方面，SOAR 系统通过自定义设计的阶梯威胁评分模型进行动态封禁处置，将安全运营精细化展开，替代原来粗犷的应急处置逻辑，更加契合实际业务流程和安全运营逻辑，展现出了系统更具弹性的安全策略拓展能力。

| 典型场景 | 原有（人工）处置方式 | 使用 SOAR 的处置方式 | SOAR 效率提升 |
|---|---|---|---|
| 全局一键封禁 IP | 20 分钟起 | 调用《全局一键封禁剧本》纯封禁 10 秒 + 人工确认，合计 3 分钟 | > 7 倍 |
| 终端中毒处置 | 20 分钟起 | 调用《终端中毒通知和处置剧本》纯处置 30 秒 + 人工审批，合计 3 分钟 | > 10 倍 |
| 多源情报聚合查询 | 逐个平台登录查询分析 5 分钟起 | 调用《威胁情报收集剧本》自动化分析查询 15 秒 | 20 倍 |
| 弱口令检查与通知 | 检查和通知 1 小时起 | 调用《弱口令通知剧本》自动化检查，通知到责任人，合计 5 分钟 | > 12 倍 |
| 一键巡检电子银行区安全设备 | 15 分钟 | 调用《一键设备巡检剧本》自动检查 20 秒 + 人工判断，合计 2 分钟 | > 7 倍 |
| 基线检查 | 人工导入漏扫生成报告 30 分钟起 | 调用《基线配置核查剧本》不考虑蓝鲸执行时间，5 分钟 | > 6 倍 |
| 主机高危告警通知 | 查找责任人发送告警详情 10 分钟起 | 调用《青藤高危告警通知剧本》短信邮件通知，合计 20 秒 | > 30 倍 |
| 阶梯化 IP 封禁 | 人工判断查询 10 分钟起 | 调用《攻击 IP 威胁评分封禁剧本》自动化分析查询 10 秒 | > 60 倍 |

表 1

在运维方面，SOAR 系统通过调用协同办公平台或科技服务台获取输入信息，将重复性高的安全运维工作固化成剧本，实现堡垒机配置、Web 应用防火墙配置、安全扫描和基线检查配置、设备巡检等安全运维工作的自动化，将安全运营人员从繁重的重复工作中释放出来。

在知识管理方面，安全运营人员通过 SOAR 系统提供的作战室进行协作化、流程化调查分析与响应处置，同时，SOAR 系统将过程中的各种数据与痕迹信息进行记录、管理和保存并形成案例库，后续通过安全运营人员的使用和完善形成知识库。

## 四、未来展望

厦门国际银行通过引入 SOAR 技术，突破传统安全运营的效率瓶颈，成功构建了一个高效、智能的安全运营体系，有效应对了日益复杂的网络安全威胁，保障了银行业务的安全稳定运行。

未来，厦门国际银行将继续与奇安信合作深化 SOAR 技术的应用，不断探索新的安全运营模式和策略，并持续扩展集成新的设备能力，推进已有场景流程的迭代，推动新场景流程的开发落地，保持 SOAR 系统的与时俱进；同时，在运营工作效能方面，以整体运营报告、日报等形式进行呈现，通过对处置时效和闭环状态的管理，跟踪工作成效，统计人员绩效，挖掘更高的自动化运营能力，展现更全面的运营效果，持续提升安全运营的效率和质量。安

奇安信

# 敏感信息泄露情报服务

- 攻击队视角的全网敏感信息情报
- 急需补上的防守盲点
- 供应链安全的管控抓手
- 预防性进攻反制利器

## 纵深防御的马奇诺防线，为什么会被攻破？

- 完整的防御体系，既要考虑正面防御，侧翼的情报收集和对抗也必不可少！
- 忽视全网视角的情报，是防守的重大盲点！

### 服务定位 SERVICE POSITIONING

- **攻击队视角**：使用渗透专家交付，不是简单的信息收集。
- **全网视角**：核心功能是从外部探测全互联网第三方应用中的敏感泄露数据；而非只关心自己的网络和应用。
- **情报级**：专家梳理的情报级信息，而不是简单数据抓取：给出利用思路和可能的攻击链，更有详细的整改建议。

奇安信安服团队

大事记

## 2024 补天白帽黑客大会举行：多方共话白帽黑客实网攻防能力培养

10 月 18 日，2024 补天白帽黑客大会在上海举行。活动以“Hack for Security Together”为主题，来自政府、厂商、高校的专家学者和顶尖白帽黑客汇聚一堂，共同解读数智时代网络安全形势和安全威胁，探讨攻防前沿技术，助力白帽黑客群体成长发展。

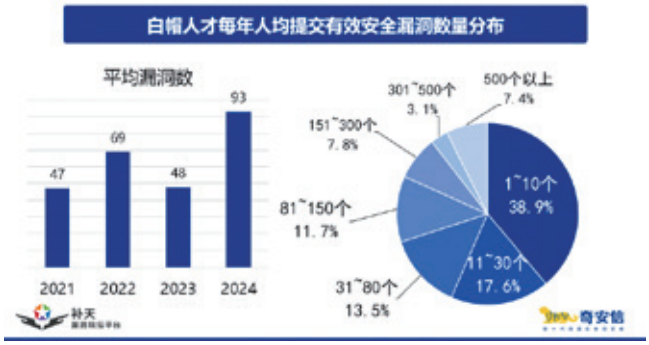
为进一步推动相关领域安全建设， 本次大会还专门组织了“实网攻防演练”和“人工智能安全”两个分论坛，并邀请主管单位、信息化企业、网络安全及数据安全专家，围绕实网攻防演练和人工智能安全对网络安全产业及白帽黑客人才的影响，进行了深入研讨和分享。十余家企业 SRC、近百个国内外优秀的安全实验室及安全团队参与了大会。

## 白帽驱动安全，实战化白帽人才能力图谱 160 项能力发布

10 月 18 日，2024 补天白帽黑客大会在上海召开。补天漏洞响应平台负责人田朋在会上发布了《2024 中国实战化白帽人才能力白皮书》（以下简称：《2024 白皮书》）和《2024 中国白帽人才能力与发展状况调研报告》（以下简称：《2024 发展报告》），全面阐述了当前国内白帽黑客人才的实战化能力核心框架与发展现状。

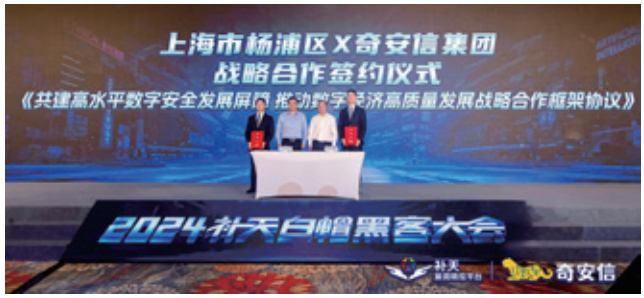
《2024 白皮书》首次将网络安全实战攻防演习中防守侧人员需要掌握的 5 大类、12 小类、52 项能力，纳入“实战化白帽人才能力图谱”；同时，将攻击侧人员需要掌握的能力图谱，从原有的 87 项能力扩充为 7 大类、17 小类、108 项能力。攻防合计包含 160 项具体能力。

《2024 发展报告》对白帽黑客人才的能力现状、生活现状、职业现状、社会认同、社会交往等方面，都进行了全面分析。报告指出：2024 年，国内白帽黑客人均向各大平台提交各类安全漏洞 93 个，与前几年相比均有所提升，创历年新高。




## 上海市杨浦区与奇安信集团签署战略合作协议

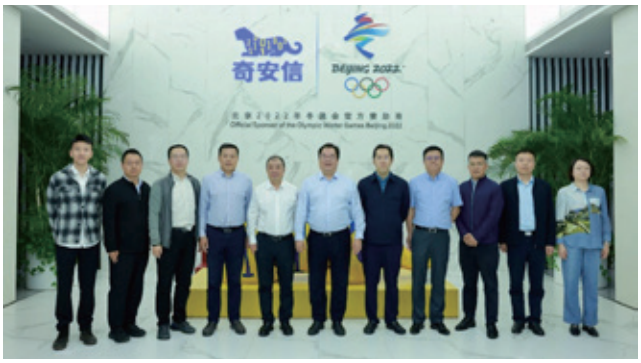
10 月 18 日，在上海五角场举行的 2024 补天白帽黑客大会上，上海市杨浦区人民政府与奇安信集团举行战略合作签约仪式，杨浦区委书记薛侃，全国工商联副主席、全国政协委员、奇安信集团董事长齐向东出席签约仪式，杨浦区副区长刘晋元、奇安信集团副总裁孔德亮代表双方签署合作协议。双方将共同打造“奇安信数据安全总部”，支撑上海乃至全国数据要素价值充分释放，助力数字经济健康发展。



## 国家信息中心主任徐强莅临奇安信集团调研

10 月 14 日，国家信息中心主任徐强带队赴奇安信科技集团股份有限公司开展调研。

徐强一行听取了奇安信集团核心技术能力及网络安全大模型的实践与应用情况。他强调，AI 时代的到来给网络安全工作带来了新的风险挑战，要以高度的使命感和责任感对待网络安全事业。徐强主任充分肯定了双方前期合作中取得的成果，并对构建“攻防一体化网络安全体系”提出四点要求：一是要进一步提高全民网络安全意识；二是要加强国家层面的网络安全专业人才队伍建设；三是要建立网络安全热线服务；四是要开展网络安全领域的关键技术和重要服务研究。




## 齐向东与李克强院士共议智能网联汽车信息安全发展之路

10 月 9 日，奇安信集团董事长齐向东一行与李克强院士团队就车路云一体化发展与智能网联信息安全议题展开了深入交流与探讨。

李克强院士对未来智能网联汽车的信息安全高度重视。他强调，在汽车产业变革浪潮中，智能网联汽车信息安全问题是国内外都在密切关注并深入研究的课题，需加强技术研发，提升安全防护能力，确保车辆系统不被非法入侵和攻击；同时，要建立健全信息安全管理体系，规范数据的收集、存储、使用和共享流程，保障用户信息和车辆数据的安全与隐私。未来，智能网联汽车信息安全体系的建立与完善，将为实现

汽车产业的智能化、网联化、安全化，提供有力支撑。

展望未来，双方将在智能网联新能源汽车的安全领域展开更为广泛而深入的合作，共同应对数据安全、网络安全、自动驾驶系统可靠性及车辆与基础设施协同安全等核心挑战，携手推动智能网联汽车产业健康、安全、可持续发展。

## 吴云坤：立足加速攻防 OODA 闭环 探索 AI 驱动安全

10 月 10 日 ~11 日，由中国计算机学会主办的第 39 次全国计算机安全学术交流会在西安举行。中国计算机学会计算机安全专委会常委、奇安信集团总裁吴云坤在主论坛发表主题演讲时表示，基于 AI 的创新在网络安全行业由来已久，须紧扣加速网络空间 OODA 循环闭环寻找方向，同时，国内厂商也需要加强在体系建设方面的资源投入和产业协作。

## 奇安信集团副总裁韩永刚：新思维构建车路云一体化网络安全体系

10月9日，2024车路云50人年度发展论坛在重庆开幕。在10日举行的主旨论坛上，奇安信集团副总裁韩永刚深入分析了车路云的业务特点及安全需求，并提出用系统工程与内生安全方法，构建车路云一体化网络安全体系，为“车路云”保驾护航。

他强调，车路云安全能力内生的核心在于，将网络安全能力和业务逻辑及数字化环境紧密结合，确保安全防护与车路云业务的每个环节同步设计、建设和运营。这种内生安全方法涵盖了从车端到路侧，再到云控平台的全面安全建设，且安全建设能够与车路云系统的快速变化同步成长，实现安全能力的动态适应，以便于在遭遇复杂网络攻击时，能够及时发现、响应和消除威胁，保障车路云一体化业务的平稳运行。

## 南京市数据安全创新实验室正式揭牌

近日，以“秦聚金秋 畅淮WE来”为主题的2024秦淮区暨南部新城新质生产力创新发展招商活动，在南京成功举办。会上，由南京市数据局、奇安信集团牵头发起并组建的“南京市数据安全创新实验室”正式揭牌。

实验室成立后，将重点聚焦数据要素授权交易安全、数据跨境规则机制、AI生成内容安全检测技术等领域，对标DEPA等高标准国际规则要求，在科学研究、标准制定、体系认证等方面积极展开能力建设，打造城市级数据安全典型示范标杆，确保先进技术的实战管用。

## 齐向东：用一体化安全体系护航一体化算力体系

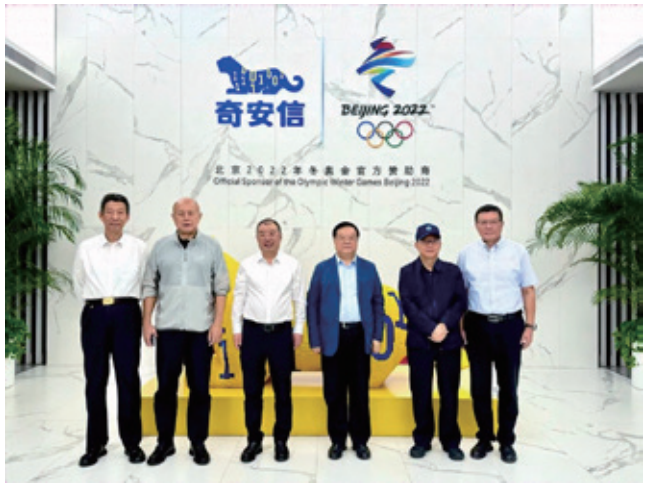
9月27日至29日，以“聚智向新 算领未来”为主题的2024中国算力大会在河南郑州举行。全国政协委员、全国工商联副主席、奇安信集团董事长齐向东在主论坛演讲中表示，全国一体化算力网络加速布局，带来更多安全威胁，必须加快贯彻国家对于提升算力网络安全保障能力的要求，努力实现算力发展与安全保障一体化。他提出，需要抓好体系化防护，确保安全无死角；做好一体化运营，确保实现动态防护；实现三级联动指挥，确保提升实战化安全能力。

## 中国电子外部董事莅临奇安信安全中心调研

9月23日，中国电子外部董事李正茂、左群声、陈书堂、李本正、王伟一行莅临奇安信安全中心调研，详细听取集团

经营发展情况的汇报，并在座谈会上展开深入交流。

在座谈中，外部董事就国内网络安全市场情况、公司未来市场定位、经营规划及海外市场布局等多个方面，提出了宝贵意见与指导。




## 产品动态

### 信创新标杆！奇安信中标中国移动 2024 年至 2026 年终端安全集采项目

日前，中国移动正式公布了 2024 年至 2026 年终端安全软件产品集采结果，经过多家供应商的综合评估和严格审核，由奇安信提供的终端安全管理系统最终脱颖而出，以最高评分获得本次采购高达 70% 的份额。该项目的中标，为奇安信在运营商行业信创安全建设树立了新标杆，将进一步加速中国移动集团的信创替代进程。

### 奇安信防火墙中标中国电信安全大脑 2024 年集采项目

近日，奇安信中标中国电信安全大脑（防护型）产品（2024 年）集中采购项目，产品包括智慧防火墙等边界安全产品。该项目的中标，意味着奇安信智慧防火墙继连续 3 年中标中国移动集采项目，并中标中国联通集采项目之后，再次在中国电信集团采购中斩获大单，这也使得奇安信成为唯一一家全部入围三大运营商总部防火墙集采的安全厂商。

### 云数据安全资源池发布：一键升级实现云上数据安全快速落地

10 月 8 日，奇安信凭借多年的云安全资源池积累，正式对外发布数据安全资源池，以解决日益严峻的云上数据安全问题。对于已建设过云安全资源池的客户，数据安全资源池支持一键升级，快速落地云上数据安全解决方案。

数据安全资源池主要解决云上数据安全的三大难题，即动态弹性匹配云上业务难题、数据安全能力适配云环境难题、云数据安全运营问题。

### All in 国产 | 奇安信集团渠道发布 15 款防火墙产品与标杆案例

10 月 8 日，奇安信集团渠道 CBG 面向全国的代理商正式发布 15 款防火墙产品与标杆案例，主要面向中小微企业、党政、卫生、教育与交通等细分领域，进行重点的市场部署与开拓，帮助渠道代理商解决客户的网络安全等需求。此次发布的 15 款防火墙产品，具备高性能，高性价比及多型号

等特点，涵盖了国产化型号，同时保证在下单后的 1 周内快速供货，满足代理商及客户需求。

## 数千万！奇安信中标“东数西算”某数据中心集群一体化安全项目

日前，奇安信成功中标“东数西算”某算力枢纽数据中心集群一体化安全保障项目，项目规模为数千万元。该项目不仅为奇安信助力“东数西算”工程网络安全建设打造了重要标杆，同时还入选了国家数据局首批全国一体化算力网应用优秀案例集。项目涵盖奇安信云平台基础安全、云平台租户安全、云原生及应用安全、数据安全、密码安全等多线产品。

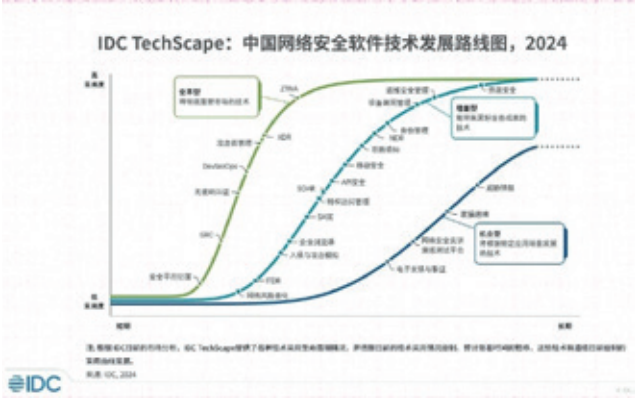
荣誉墙

## 奇安信天擎 V10 全项满分通过 AV-TEST 测评

日前，国际权威测评机构 AV-TEST 公布了最新一期的企业终端安全产品测试结果，奇安信天擎终端安全管理系统（简称“天擎”）以防护能力满分（6 分）、性能表现满分（6 分）、可用性满分（6 分）、总成绩 18/18 的优异成绩通过了测试，标志着奇安信天擎在企业级安全防护领域达到了国际领先水平，展现了其在保护企业免受网络威胁的卓越能力。

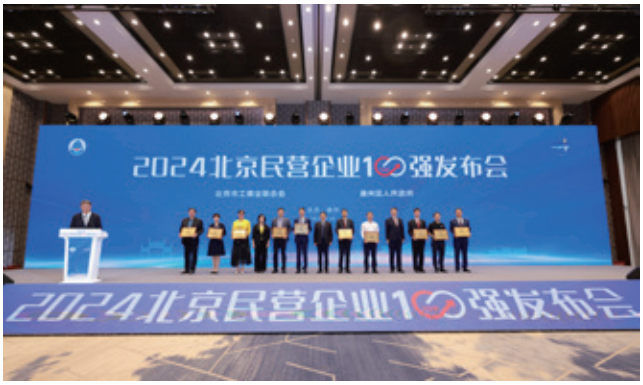
## 入选领域最多！奇安信七项技术获全球权威机构推荐

近日，全球领先的 IT 市场研究和咨询公司 IDC 发布《IDC TechScape: 中国网络安全软件技术发展路线图，2024》（Doc#CHC52608824，2024 年 10 月）（以下简称：《报告》）。奇安信凭借在 ZTNA（零信任网络访问）、NDR（网络检测与响应）、企业浏览器、态势感知、特权访问管理、终端安全、电子发现与取证等七项技术的推荐，成为本次《报告》中入选领域最多的推荐厂商。




## 奇安信集团连续六年入选“民营企业百强”“科技创新”及“社会责任”三大榜单

9 月 26 日，北京市工商联在京召开 2024 北京民营企



业百强发布会，发布了北京民营企业“1+4”百强榜单及《2024百强调研报告》。凭借在行业引领、技术创新、人才培养等多个方面的优异表现，奇安信集团入选“民营企业榜单”“科技创新”“社会责任”三大榜单，这也是奇安信集团连续第六年入选三大榜单。

在颁奖现场，奇安信集团作为百强企业，还与工商联系统相关单位进行了签约。接下来，奇安信将以实际行动，发挥百强企业示范引领作用，坚持创新驱动，为推动行业发展、促进经济增长贡献力量，为首都高质量发展贡献更大力量。

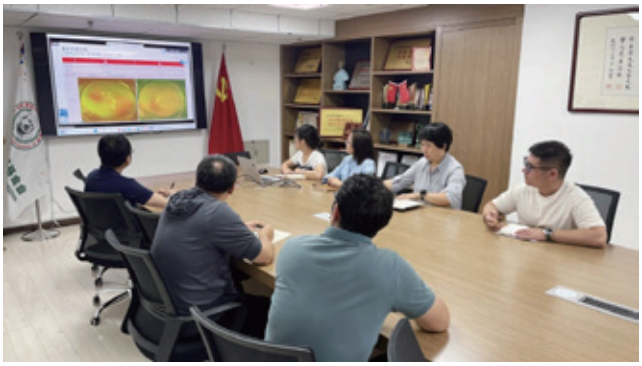
## 奇安信入选攻击面管理报告推荐供应商

日前，IDC 发布《IDC Technology Assessment：中国攻击面管理厂商技术评估，2024》报告（Doc#CHC51516424，2024 年 9 月），从网络资产攻击面管理 (CAASM)、外部攻击面管理、威胁情报、入侵与攻击模拟（BAS）、综合管理和可视化、应用场景适配、平台开放性 7 个维度进行评估，奇安信凭借综合实力和技术优势入选攻击面管理推荐厂商。

社会责任

## “眼明心安”公益项目线上培训开讲

9 月 19 日，由北京白求恩公益基金会、北京奇安信公益基金会和北大医学眼科专家共同发起，旨在提升西藏眼科医生眼病诊疗能力，满足西藏儿童及青少年基础眼健康需求的“眼明心安－西藏儿童盲及低视力诊疗能力提升项目”（以下简称“眼明心安”项目）“西藏儿童眼病诊疗技术二期培训班”线上培训正式开启。此次线上培训是 2024 年“西藏儿童眼病诊疗技术二期培训班”的重要内容，旨在借助科技之力，跨越地理阻隔，持续为西藏的眼科医生输送前沿医疗知识与技能。



在前期深入调研西藏当地医生技术水平与实际需求的基础上，朱雪梅教授精心筹备了《葡萄膜炎与儿童》的课程内容，西藏各地多名眼科医生在线听取了本次培训。

## 重庆移通学院举办“奇安信奖助学金”颁发仪式

近日，重庆移通学院信息安全学院举办了“心安助学 · 高校教育助学项目”2023 至 2024 学年“奇安信奖助学金”颁发仪式，表彰了在社会化实践中表现出色的信息安全专业学生，并对品学兼优的困难学生提供了助学支持。本年度“奇安信奖助学金”共有 25 名学生获得了支持，其中奖学金 10 人、助学金 15 人。

# SOAR 的未来

作者 叶蓬

## Gartner 一句“SOAR 已过时”引发热议

2024 年 7 月底，Gartner 发布了 2024 年度的安全运行（SecOps）技术与服务成熟度曲线（Hype Cycle）。报告中，Gartner 正式表示 SOAR“已经过时（obsolete）”，进而在业内引发热议。

之前主打 SOAR 现在改打“安全自动化”的厂商 Swimlane 的 CEO James Brear 在 X 上表示：“任何有关 SOAR 已死的提法都是我听过的最愚蠢（dumbest）的事情——绝对愚蠢（absolutely asinine）。”

IBM 产品管理副总裁及 SOAR 产品 Resilient（被 IBM 收购）的联合创始人 Ted Julian 在 LinkedIn 上愤怒的表示：“鉴于 Gartner 正在取消 SOAR，我要……取消 Gartner”。Ted 更是直言 Gartner 的分析和业务模式已经过时。

而针对 Ted 在 LinkedIn 上的发言，有人赞同，有人反对。有人表示，这对于正在进行下一代 SOAR（AI SOAR）创业的公司来说是一个打击。

D3 Security 的一位产品市场经理表示，尽管 Gartner 将 SOAR 归为过时产品，并且出现了一些不再使用 SOAR 缩写的新 SOAR 公司，但 SOAR 市场仍在增长，并估计每年有超过 10 亿美元的交易，这说明 SOAR 有市场。

这类声音的核心意思是认为 SOAR 技术依然存在，虽然遇到很多问题，但依然有其市场空间，并且还在不断改善和演进。

还有不少公司也在官网博客上发表观点，赞同 Gartner 的观点。

号称下一代 SOAR（超级自动化）的厂商 Torq 表示，“SecOps 专业人员对过时的、传统的 SOAR 产品深感不安”，“基于 GenAI 的安全自动化是现代企业的发展方向”。

标榜“安全自动副驾”的 Blink 表示，“SOAR 已经过时”，“网络安全的重点显然正在转向更先进的自动化工具，尤其是那些由 GenAI 驱动的工具”。

StrikeReady的首席客户官表示，“SOAR 就不是一个产品类别”，“作为一个功能集合，它早就失败了。”

网络上，还有很多“XX 已死，XX 永生”的言论。

Google 云安全首席营销官及前 Siemplify 首席营销官 Nimmy Reichenberg 表示赞同 Gartner 关于 SOAR 已经过时的提法，认为 SOAR

> LinkedIn 上有不少声音认为 SOAR 技术本身并未过时，SOAR 还是很有价值的，他们认为 Gartner 想要表达的意思主要是独立 SOAR 市场已经过时了。

已经是大多数安全运营平台的一部分，不再值得作为独立产品类别了，就像以前的 UEBA 那样，并不是说不需要 SOAR 了，而是演变成了大平台的功能。

Exabeam 首席战略官及前 Gartner 分析师 Gorka Sadowski 发表了一篇题为《SOAR 已死，SOAR 永生》的文章，提及了 SOAR 的起源、繁荣和当前遇到的困境，表示 SOAR 就跟 UEBA 一样，作为独立市场基本消失，更多地融入到了其他市场（如 SIEM）中。他写道："是否还需要独立 SOAR 工具？有时需要，但更多组织可以利用他们技术栈中已有工具的 SOAR 功能，尤其是 SIEM 和 CloudSec 工具。"

Sumo Logic 的 Field CTO Chase Clawson 表示，SOAR 功能已经迁移到各种安全产品之中。

在 LinkedIn 上也有不少类似的声音。其核心思想就是说，SOAR 技术本身并未过时，SOAR 还是很有价值的，否则为什么 Gartner 的这份 Hype Cycle 依然详细分析了 SOAR 技术，并明确给出了其价值，以及用户应该如何选购 SOAR 的建议？Gartner 想要表达的主要是独立 SOAR 市场已经过时了。

在深入讨论 SOAR 是否已死之前，让我们先来回顾一下 SOAR 的发展历程，当前面临的困境和市场格局，以及发展趋势。

## SOAR 的发展历程

Gartner 在 2015 年发明了 SOAR 这个术语，并在 2017 年正式确立了现代 SOAR 的定义。目前，SOAR 的最新定义是：

SOAR 是一个将事件响应、编排和自动化及威胁情报管理功能组合成的单一解决方案。SOAR 工具可用于许多安全运营任务，例如，记录并实施流程，支持安全事件管理，向人类安全分析师和操作员提供基于机器的协助，以及更好地实现威胁情报实战化。

根据 Gartner 的定义，SOAR 是包含安全编排与自动化（Security Orchestration and Automation，SOA）、安全事件响应平台（Security Incident Response Platform，SIRP）和威胁情报平台（Threat Intelligence Platform, TIP）的三合一解决方案，主要旨在解决安全运营（SecOps）的事件响应环节的自动化和闭环，捎带进行自动化的威胁情报管理与利用，后来又发展到可以自动化处理安全运营各个环节的任务。

在 SOAR 之前，安全运营人员先是借助自定义的脚本实现原始的自动化，后来又借助 IT 运营自动化工具，以及 RPA 等面向跨系统工作流程的通用自动化平台。而 SOAR 正是基于之前这些实践基础上专门面向安全运营的自动化技术。

在 SOAR 技术处于 Gartner 技术成熟曲线炒作高峰的那段时间，人们对 SOAR 的期待很高，给人感觉 SOAR 自动化能力"没有上限"。

## SOAR 面临的困境

随着 SOAR 实践的深入，SOAR 暴露的问题也越来越多。

首先，人们再次认识到安全运营作为一种人、技术和流程相结合的产物，不存在技术上的银弹。SOAR 技术也一样，它严重依赖组织的安全运营流程和规程，需要投入资源进行剧本的设计与开发，并且要持续投入。人们发现，对于中小型组织或者安全运营成熟度不高的组织而言，部署 SOAR 的投入产出比可能不高。

其次，基于预置剧本的编排更适合那些机械式重复的、相对简单和固化的工作任务的自动化。对于一些复杂的、时常变化的工作过程，采用剧本编排则很容易陷入无止尽的开发和修改过程之中。而不幸的是，网络安全领域的攻防变化太快，响应过程分支情况太多。

再次，与各类第三方系统和工具的对接和集成也成为了制约 SOAR 发展的瓶颈。

## SOAR 的演进

为了应对上述挑战，SOAR 厂商们也在尽力改善。当前，所谓的"下一代 SOAR"的主要功能都反映在如何改善上述问题上。现在的"下一代 SOAR"主要有两个发展方向。一个是向所谓"超自动化 SOAR"方向发展（如 Torq），旨在将安全编排自动化技术的应用领域向安全运营之外扩展，成为通用安全自动化工具。同时，充分采用低代码－无代码开发技术，降低剧本开发难度和成本。此外，预先开发好大量第三方应用接口，并内置大量剧本模板，再以应用市场和社区的形式进行发布，降低用户的使用门槛。另一个发展方向则是"AI SOAR"或"AI SOC 助理"（如 DropZone.AI），使用 GenAI 技术实现一个"网络 AI 助理"，用智能化改造基于剧本的编排自动化。

此外，SOAR 厂商们也逐步总结了一套剧本设计开发的方法论，并不断将 SOAR 的价值聚焦到基于剧本的编排技术能够驾驭的应用场景上去。

## SOAR 市场格局巨变

在 SOAR 技术不断演进的同时，SOAR 市场格局也经历了巨变。

从安全运营的角度来看，正是由于自动化和响应如此重要，响应技术（包括自动化响应）已经不再是 SOAR 的专属。检测类产品纷纷布局响应，出现了各种 DR（检测与响应）类产品，从 NDR、EDR 到后来的 XDR，纷纷内置（简化的）SOAR 能力。而作为 SOC 核心的 SIEM 产品也在朝 TDIR 方向前进，大力发展响应自动化技术，并成为 SOAR 厂商的最大买家群体。

如图一所示，入围 Gartner 2024 年 SIEM 魔力象限的所有 SIEM 厂商都有 SOAR，要么收购（主要方式），要么自研，要么是 SIEM 产品中的一个模块，要么是 SIEM 产品套件中的一个子产品。

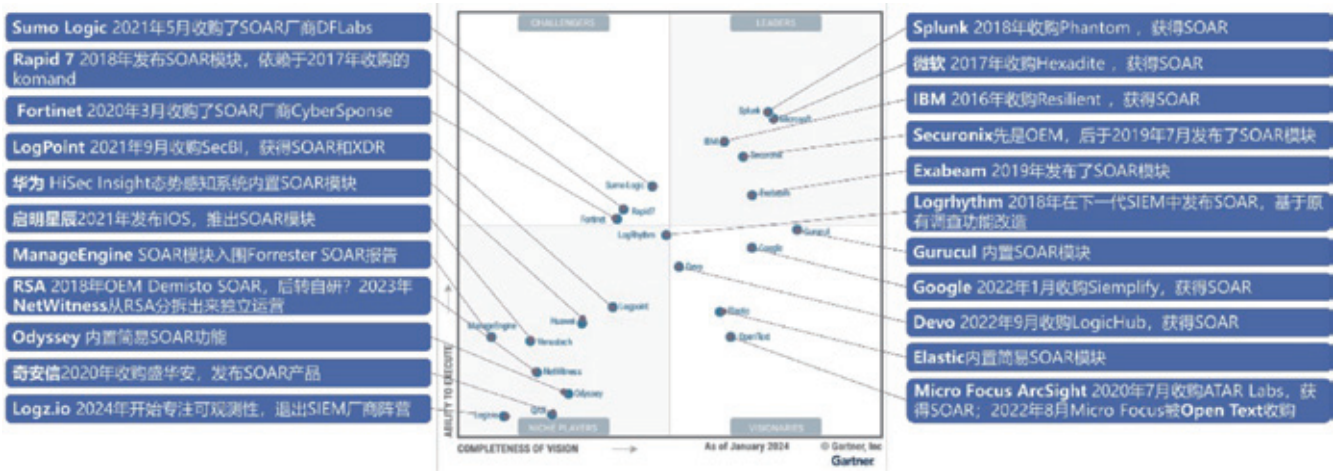
Gartner 在 2023 年的 SOAR 市场指南报告中就指出，SOAR 整合到各种 TDIR 类产品中的趋势已经十分明显。

## Gartner 的观点解读

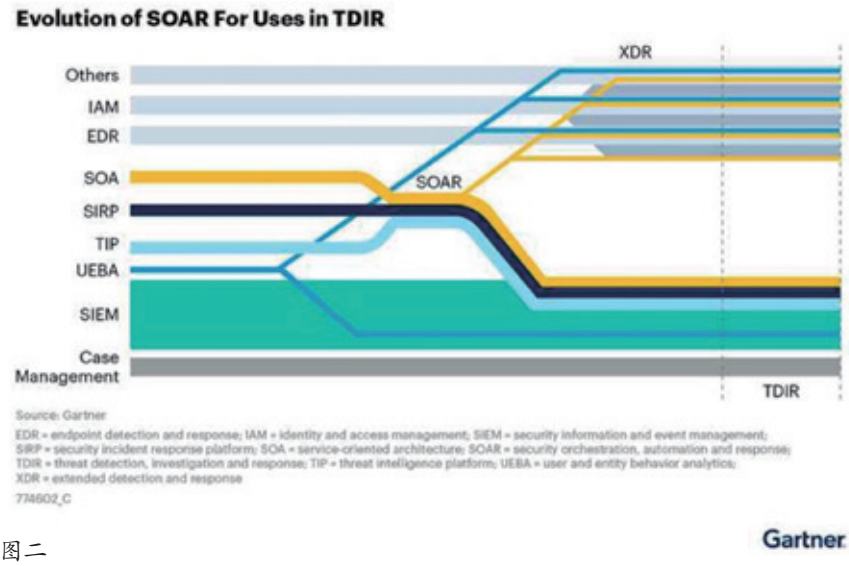
对 SOAR 进行了全面审视之后，我们再回过头来研究 Gartner 的观点。

在 2024 年 2 月份的时候，笔者跟 Gartner 分析师 Pete Shoard 进行了一次 Inquiry，当时就询问他对 SOAR 未来的看法，SOAR 市场是否会消失。Shoard 当时就委婉的表示，SOAR 将更多的融入 SIEM 中，但独立 SOAR 还存在于某些缝隙（niche）市场。同时，Shoard 表示，Gartner 对 GenAI 应用于安全（包括 SOAR）持审慎态度。笔者理解，GenAI 作为革新 SOAR 或者安全自动化的技术，还有较长的路要走。GenAI 是变革 SOAR 的重要因素，但不是 Gartner 把 SOAR 标记为“过时”的关键因素。

今年 8 月份，Dark Reading 对 Gartner 的 SOAR 过时论点进行了专门的文章报道。文章引述了 Gartner SecOps Hype Cycle 报告中 SOAR 词条的主笔分析师 Eric Ahlm 的话。他表示，将 SOAR 标记为过时，是因为该类产品的组件已经被其他产品和服务所取代。当前，自动化越来越成为




图一




图二

一种众人期待的功能，SOC 需要编排作为一项单独的功能，将分散的产品集成到单一的运营中心。同时，由于企业客户越来越倾向于简化运营，因此供应商纷纷将 SOAR 与他们的产品和服务进一步整合到一起。Ahlm 进一步表示，Gartner 真正要传递的信息，不是说 SOAR 这个概念过时或者自动化已经终结，而是有很多不同的方法可以增加自动化（以提升效率、扩大规模），而无需去购买独立的 SOAR 平台。

总结一下，笔者认为 Gartner 的观点是：

基于三方面原因——（1）随着自动化技术越来越渗透到各类安全产品（尤其是 SIEM）中，独立 SOAR 厂商和产品越来越少；（2）SOAR 自身面临各种落地障碍，需要将 SOAR 与其他产品能力相结合来化解其中的一些障碍；（3）用户对于供应商和产品能力整合的呼声越来越高——Gartner 呼吁用户更多考虑在 SIEM 等其他 SOC 核心产品平台中考虑使用 SOAR 功能，而不要使用独立 SOAR。因此，Gartner 将 SOAR 标记为过时，独立 SOAR 产品将不再是主流产品，独立 SOAR 市场将逐步萎缩，仅存在于某些缝隙市场，但 SOAR 技术将在其他产品和市场中继续发展演进。

## SOAR 在中国的未来

那么，中国 SOAR 市场未来走势如何？笔者认为，其实在国内尤其更加需要独立 SOAR 产品。因为当前国内大部分客户的 SOC/SIEM 平台都不具备 SOAR 能力。在用户彻底更换为下一代具有 SOAR 功能的 SOC 平台之前，还需要购买独立 SOAR 来弥补现有平台的这部分不足。而鉴于当前的中国经济不利局面，用户花费大量资金投资下一代 SOC 替换以前大额投资的意愿不高，反而更倾向于采用“向存量投资要效益 " 和 " 查漏补缺 " 的方式来完善其 SOC。因此，在中国，独立 SOAR 的机会仍然很多。

不论 SOAR 是否独立存在，还是被整合到 SIEM 或其他产品中，SOAR 技术都必须继续演进。

在技术发展趋势方面，需要让 SOAR 更加易于实施和维护，要降低用户使用成本，例如，积极引入低代码－无代码开发技术，降低用户设计开发剧本的难度，积极探索利用 GenAI 增强现有的 SOAR 能力。功能上，应该继续深化作战室功能，把 SIRP 平台做好。对于 Gartner 提及的 TIP 部分，鉴于国内的实际情况，建议由专门的 TIP 承接，在 SOAR 产品中更多考虑如何利用威胁情报即可。此外，应内置尽可能多的剧本和 App，提升产品开箱即用的程度。同时，要优化剧本开发方法论，教育用户树立正确认知，聚焦投入产出比高的应用场景，避免造成“SOAR 万能自动化”的假象。

最后，作为中国 SOAR 厂商，应该在继续发展独立 SOAR 的同时，将 SOAR 与 SOC 平台进行整合。

关于作者

**叶蓬**

虎符智库专家、北京盛华安信息技术有限公司联合创始人、副总裁。具有 20 余年 SIEM、安全管理（SOC）平台和态势感知领域从业经验，并对 SOAR 有较深入研究。

# 加拿大建立武装部队网络司令部以整合军事网络能力

作者 赵慧杰

**编者按：**9月26日加拿大正式宣布成立加拿大武装部队网络司令部，从而将武装部队的网络能力整合为一个统一的专门实体，提高军队应对网络领域威胁的准备程度。

加拿大武装部队网络司令部的成立对加拿大国防部和加拿大武装部队来说是一个重要的里程碑，体现了加拿大建立专门的网络作战架构的承诺，凸显了网络能力在现代军事行动中日益增长的重要性。该司令部将成为加拿大国防部和武装部队网络行动的唯一管理机构，负责网络部队的维持、管理和发展，通过集中资源来推进与行动、人员、政策和能力相关的网络空间现有活动；包括信号情报和联合电子战，能够执行和支持一系列网络任务；除对保卫加拿大和推进其利益至关重要外，还将帮助国防团队履行北约承诺及加拿大印度－太平洋战略的网络和防御部分，如虚拟网络事件支持能力和盟国自愿提供的主权网络效应；将支持加拿大武装部队过渡到全域战场，具有更高的灵活性和对恶意网络活动的响应能力。

新司令部的成立与加拿大在北美防空司令部、“五眼”联盟和北约的主要合作伙伴和盟友的类似投资相一致。通过增强其网络能力，加拿大正在支持与其盟友的更大互操作性，更好地应对各种网络威胁，并正在推进北约的任务目标和目的。加拿大国防部长比尔·布莱尔表示，新司令部的成立向盟友、合作伙伴和对手展示了加拿大持续致力于在充满挑战的网络领域开展行动的承诺，将通过加强加拿大在网络领域的工作并推进与合作伙伴和盟友合作，来发现、阻止和防御针对加拿大和利益关切的网络威胁和恶意行为者。加拿大国防参谋长珍妮·卡里尼昂表示，加拿大国防部和武装部队将通过网络司令部继续与通信安全局密切合作，开发和扩大进攻性和防御性网络行动能力，支持战术和战略层面的网络行动。加拿大武装部队网络司令部首任司令戴夫·雅克表示，在网络领域建立决定性优势需要速度、信任、敏捷和团结的努力。

奇安网情局编译有关情况，供读者参考。

加拿大国防部长比尔·布莱尔和国防参谋长珍妮·卡里尼昂9月26日正式宣布成立加拿大武装部队网络司令部（CAFCYBERCOM）。该新司令部将把加拿大武装部队的网络能力整合为一个统一的专门实体，这将提高军队应对网络领域威胁的准备程度。

加拿大武装部队网络司令部（CAFCYBERCOM）的成立对加拿大国防部和加拿大武装部队来说是一个

重要的里程碑。该司令部体现了加拿大在“强大、安全、参与”战略中提出的建立专门的网络作战架构的承诺，凸显了网络能力在现代军事行动中日益增长的重要性。

该新司令部将由戴夫·雅克少将领导，负责网络行动及网络部队的维持、管理和发展。戴夫·雅克将利用他担任联合网络部队指挥官和通信安全局（CSE）顾问的经验，利用他的专业知识指导该机构在网络领域取得新的战略进步。

通过加拿大武装部队网络司令部（CAFCYBERCOM），加拿大武装部队继续与加拿大通信安全局（CSE）密切合作，开发和扩大其进攻性和防御性网络行动能力。加拿大武装部队和加拿大通信安全局（CSE）长期合作，开发先进的技术和专业能力，为军事行动提供情报。在过去十年中，双方的伙伴关系不断发展，包括网络安全、防御性和进攻性网络行动领域的合作。

新的加拿大武装部队网络司令部还使加拿大能够履行对北约的承诺，如虚拟网络事件支持能力和盟国自愿提供的主权网络效应。新司令部的成立与加拿大在北美防空司令部、“五眼”联盟和北约的主要合作伙伴和盟友的类似投资相一致。通过增强其网络能力，加拿大正在支持与其盟友的更大互操作性，更好地应对各种网络威胁，并正在推进北约的任务目标和目的。

**高官言述**

加拿大国防部长比尔·布莱尔表示，“加拿大武装部队网络司令部的成立向我们的盟友、合作伙伴和对手展示了加拿大持续致力于在充满挑战的网络领域开展行动的承诺。通过加强我们在网络领域的工作，并继续与我们的合作伙伴和盟友合作，我们可以发现、阻止和防御针对加拿大和我们利益的网络威胁和恶意行为者。”

加拿大国防参谋长珍妮·卡里尼昂表示，“通过加拿大武装部队网络司令部，加拿大国防部和武装部队将继续与通信安全局密切合作，开发和扩大进攻性和防御性网络行动能力。这一举措支持战术和战略层面的网络行动。新机构将集中资源，以便我们能够推进与行动、人员、政策和能力相关的网络空间现有活动。”

加拿大国防部副部长斯蒂芬妮·贝克表示，“我向雅克少将表示祝贺，祝贺他担任加拿大武装部队网络司令部司令。他为司令部、国防团队和所有加拿大人带来了丰富的知识、经验和领导才能。”

加拿大武装部队网络司令部司令戴夫·雅克少将表示，“在网络领域建立决定性优势需要速度、信任、敏捷和团结的努力，我很自豪被任命为致力于实现这一目标的组织的负责人。”

加拿大通信安全局局长卡罗琳·泽维尔表示，“自成立以来，加拿大通信安全局一直是加拿大武装部队的重要合作伙伴。合作对我们来说是自然而然的事情，加拿大武装部队网络司令部也不例外。这就是为什么我们要联合我们已经世界一流的外国网络作战能力，以在复杂的世界中保护加拿大。即使在和平时期，我们也面临网络战，这种伙伴关系将使加拿大人民及加拿大的盟友受益，并让我们所有人更好地了解我们每天面对的不断变化的威胁形势。”

**简要事实**

- 加拿大武装部队网络司令部（CAFCYBERCOM）将成为加拿大国防部 / 武装部队网络行动的唯一管理机构，负责网络部队的维持、管理和发展。
- 加拿大武装网络司令部包括信号情报和联合电子战，能够执行和支持一系列网络任务。
- 加拿大武装部队网络司令部的建立除了对保卫加拿大和推进其利益至关重要，还将帮助国防团队履行北约承诺及加拿大印度－太平洋战略的网络和防御部分。
- 加拿大武装部队网络司令部将支持加拿大武装部队过渡到全域战场，具有更高的灵活性和对恶意网络活动的响应能力。
- 自 2010 年以来，戴夫·雅克少将一直担任盟友和合作机构的关键参谋和联络职位，以及部队和编队级别的指挥职位。戴夫·雅克于 2022 年被任命为联合部队网络部分指挥官。

关于作者

**赵慧杰**

虎符智库专家、网络空间安全军民融合创新中心高级研究员。长期从事网络安全、互联网发展等领域研究工作，对外军网络战、国际网络安全态势、全球网络空间竞合及新技术新应用发展等具有深厚研究造诣，先后获得军内成果奖七项。

# “定期更换密码”是最愚蠢的密码规则？

作者 GoUpSec

数十年来，消费者和企业员工经常被灌输一些“强密码规则”，如定期更换密码，在密码中使用特殊字符等。虽然，近年来此类密码规则的有效性遭到安全专家的广泛质疑，但是新一代密码规则（如用长度换强度、非必要不更新等）由于企业界的强大惯性和阻力（如大多数互联网服务和企业系统都不支持 64 位长密码）而难以普及推广。

近日，美国国家标准与技术研究院（NIST）发布了最新的数字身份指南草案（SP800-63-4 第二版），彻底颠覆了人们对密码安全的认知。指南提议取消一些最流行的、同时也是“最荒谬”的常识性做法，例如：

- 强制用户定期更改密码
- 强制或限制用特定字符
- 强制要求混合多种类型字符
- 使用安全问题作为验证手段

**破除密码安全的陈规陋习**

在数字时代，密码是保护用户隐私和数据安全的关键要素。然而，NIST 指出，许多传统密码管理规则不仅没有增强安全性，反而适得其反。最典型的例子是强制用户定期更改密码的要求。

几十年前，密码安全性认知尚未普及，人们往往选择容易被破解的常见词汇或简单字符组合，因此定期更改密码被认为是防止被盗用的一种策略。但是，随着密码管理技术的进步和随机生成密码的普及，强制更改密码的做法不仅增加了用户的负担，还可能导致密码复杂性下降。

NIST 给验证服务和管理者的“颠覆性”密码建议如下：

- 密码长度至少为 8 个字符，建议不少于 15 个字符。
- 应允许最大密码长度至少为 64 个字符。
- 应该接受所有打印 ASCII（RFC20）字符，或在密码中添加空格字符。
- 应接受密码中的 Unicode（ISO/ISC 10646）字符。评估密码长度时，每个 Unicode 代码点应计为一个字符。
- 不得对密码施加其他组合要求（如要求混合不同类型的字符）。
- 不得要求用户定期更改密码，

> 美国国家标准与技术研究院（NIST）指出，许多传统密码管理规则不仅没有增强安全性，反而适得其反。
> 最典型的例子是强制用户定期更改密码的要求。

除非有证据表明账户被盗用。

• 不得允许订阅者存储未经身份验证的用户可访问的提示。

• 不得提示订阅者在选择密码时使用基于知识的身份验证 (KBA)（如“您的第一只宠物的名字是什么？”）或安全问题。

• 验证者应当完整验证所提交的密码（即，不要截断它）。

**特殊字符与安全问题是一对“卧龙凤雏”**

NIST 还质疑另一项广受诟病的规则——要求密码必须包含大小写字母、数字和特殊字符。NIST 认为，在密码足够长且复杂的情况下，这类字符组合规则并没有实质上的安全提升作用，反而会导致用户选择更容易记忆且相对脆弱的密码。

许多用户为了满足这些复杂的规则，往往倾向于使用重复的字符或常见组合，如“Password123!”之类的“伪强密码”。

同样，NIST 建议废除使用安全问题（如“您的第一只宠物叫什么？”）作为密码验证手段。研究表明，安全问题容易被破解或通过社交工程攻击获取答案，难以真正保障用户隐私（有时反而会导致隐私泄漏）。

**用长度换取强度**

NIST 在新指南中建议，密码验证系统应接受至少 64 个字符长度的密码，并支持所有 ASCII 字符和 Unicode 字符的使用。这意味着用户不仅可以设置更长的密码（如 wo xihuan chi gobelieve baozi），还可以使用更广泛的字符集，进一步增强密码的复杂性与安全性。

同时，NIST 强调，密码验证应当检查用户输入的完整密码，而非截断处理，确保密码的每一个字符都被考虑在内。

**密码安全新趋势：回归常识与用户体验**

NIST 的最新指南草案不仅在技术层面上进行了优化，更重要的是，它体现了密码安全领域的一种回归——回归常识、回归用户体验。正如 NIST 在声明中指出的，许多密码管理规则之所以存在，是因为早期网络安全认知不足，然而，随着技术的进步和攻击手段的复杂化，许多看似“安全”的做法其实已经不再适用，甚至成为安全隐患的源头。

以密码长度为例，NIST 建议的 8~15 字符的最低密码长度既确保了密码的基本安全性，又避免了过度复杂的字符组合规则，让用户可以在增强安全性的同时减少记忆负担。这一理念与近年来密码管理软件（如密码管理器）和生物识别技术的普及相呼应，进一步提升了整体用户体验。

**未来展望：安全管理需要以人为本**

尽管近年来不少专家一再批评现行密码规则的弊端，但银行、互联网平台和政府机构大多依然固守这些过时、无效甚至有害的规则。NIST（美国国家标准与技术研究院）发布的新指南草案尽管并不具备强制性，但被业界广泛看作是终结“无效”密码规则的一个标志性历史事件，也是全球密码安全标准演进的重要一环，有望在更广泛的领域内被采纳和应用，带动密码安全领域的深层变革。

未来，随着量子计算等新技术的发展，密码学的基础原理也可能发生变革。目前来看，这一提议对于密码管理和用户安全的提升是显而易见的，但其最终效果仍有待观察和验证。

“人的因素”是网络安全最重要的环节，NIST 密码新规的提出代表了一个重要的网络安全趋势——有效的安全管理需要更多地依赖技术创新和用户友好的安全设计，而不是机械地强制用户遵循陈规陋习。安

关于作者

GoUpSec

以国际化视野服务于网络安全决策者人群，致力于成为国际一流的调研、分析、媒体、智库机构。

奇安信

新一代网络安全领军者

# 聚焦安全运营，构建智能平台

奇安信网神态势感知与安全运营平台（简称NGSOC）以大数据平台为基础，通过收集多元、异构的海量日志，利用关联分析、机器学习、威胁情报等技术，帮助政企客户持续监测网络安全态势，为安全管理者提供风险评估和应急响应的决策支撑，为安全运营人员提供威胁发现、调查分析及响应处置的安全运营工具。

## 国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

## 首款分布式关联分析引擎 - Sabre

国内首款具备分布式关联分析能力的安全运营平台，提供多元异构数据关联分析、灵活威胁建模、丰富的告警上下文信息展示及分布式横向扩展能力，已获得数十个相关专利。

## 将平战结合进行落地

演练态势监测攻防演练中防守方管理信息、系统建设、威胁运营等信息的总体状况，平战结合，全面提升安全防御能力。

## 重大安全事件的威胁预警

当出现重大网络安全事件时，帮助用户第一时间掌握是否遭受到攻击？首个被攻击的资产？影响部门？影响面趋势？事件处置情况？

## 专业的安全运营服务

奇安信集团具有专职产品运营服务团队，可提供原厂一线驻场、二线分析、运营方案咨询及培训服务，帮助客户解决无人运营困难。

## 市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证

态势感知解决方案市场领导者——IDC认证

态势感知技术创新力和市场执行力双第一——数世咨询认证

网安26号院

# 征稿启事

当下，网络空间态势日趋严峻，关基设施成为重要攻击目标，因网络攻击导致的系统瘫痪、数据泄露现象频发。网络安全建设和运营需时刻因应形势变化进行创新。分享行业趋势、交流建设与运营之道成为提升安全防护水平的重要途径。

为此，奇安信《网安 26 号院》联合虎符智库、安全内参联合征稿。具体要求如下：

## 一、征稿对象：

投稿人为政企网络安全负责人、从业者，以及研究人员。

## 二、征稿时间：

本次活动活动长期有效。

## 三、征稿要求：

投稿论文应为投稿人原创，且尚未被任何期刊接受或发表。投稿人应对所投稿件的著作权及其他法律责任负责。

## 四、稿件说明：

来稿主题包括但不限于网络安全合规解读、网络攻防态势分析、网络安全建设经验、安全运营最佳实践，创新安全技术及应用等网络安全领域相关的议题。

稿件字数（含注释）原则上应控制在 4000 ~ 8000 字。

## 五、评选及奖励：

来稿经专家组评审入选刊登后，即获得相应的稿费（不低于 2000 元人民币）。

优秀获奖作者将有机会受邀参加 “BCS 北京网络安全大会”，发表主题演讲并分享研究心得。

## 六、其他荣誉：

长期供稿作者可以获聘“虎符智库”专家，授予聘书和徽章。

## 七、投稿方式：

投稿以附件形式通过电子邮件

发送至 lijianping@qianxin.com;

或者微信添加 security4 咨询联系。

扫码咨询

# 奇安信连续四年位居
# “中国网安产业竞争力50强”
# 第一名

9月6日，中国网络安全产业联盟（CCIA）
公布“2024年中国网安产业竞争力50强”榜单，
凭借扎实的技术实力和领先的市场表现，
奇安信连续四年高居榜单第一名。

## “2024年中国网安产业竞争力50强”榜单

| TOP15 | 公司名称 |
|---|---|
| 1 | **奇安信科技集团股份有限公司** |
| 2 | 启明星辰信息技术集团股份有限公司 |
| 3 | 深信服科技股份有限公司 |
| 4 | 华为技术有限公司 |
| 5 | 天融信科技集团股份有限公司 |
| 6 | 新华三信息安全技术有限公司 |
| 7 | 杭州安恒信息技术股份有限公司 |
| 8 | 亚信安全科技股份有限公司 |
| 9 | 绿盟科技集团股份有限公司 |
| 10 | 三六零安全科技股份有限公司 |
| 11 | 天翼安全科技有限公司 |
| 12 | 中电科网络安全科技股份有限公司 |
| 13 | 杭州迪普科技股份有限公司 |
| 14 | 北京山石网科信息技术有限公司 |
| 15 | 中孚信息股份有限公司 |