"Face the challenge,Embrace the best practice"

EISS－2019
企业信息安全峰会
之深圳站

2019.8.16

企业安全建设实践与调查那些事

一加OnePlus　安全负责人　郭惠龙

一加OnePlus公司简介

NEVER SETTLE

2013年12月17日，我们诞生了，总部位于深圳。
我们选择智能手机作为实践梦想的第一步，
秉承“不将就”的理念。
成立不到一年，
我们就入围“科技界奥斯卡”—— Crunchies Awards “全球最佳新创公司”。
我们发布的产品已走进美国、英国、印度等30多个国家和地区，
并获得《时代周刊》、《福布斯》、《华尔街日报》等国际主流媒体的高度评价

愿景 成为更健康 、更长久的企业

使命 与世界分享品质科技

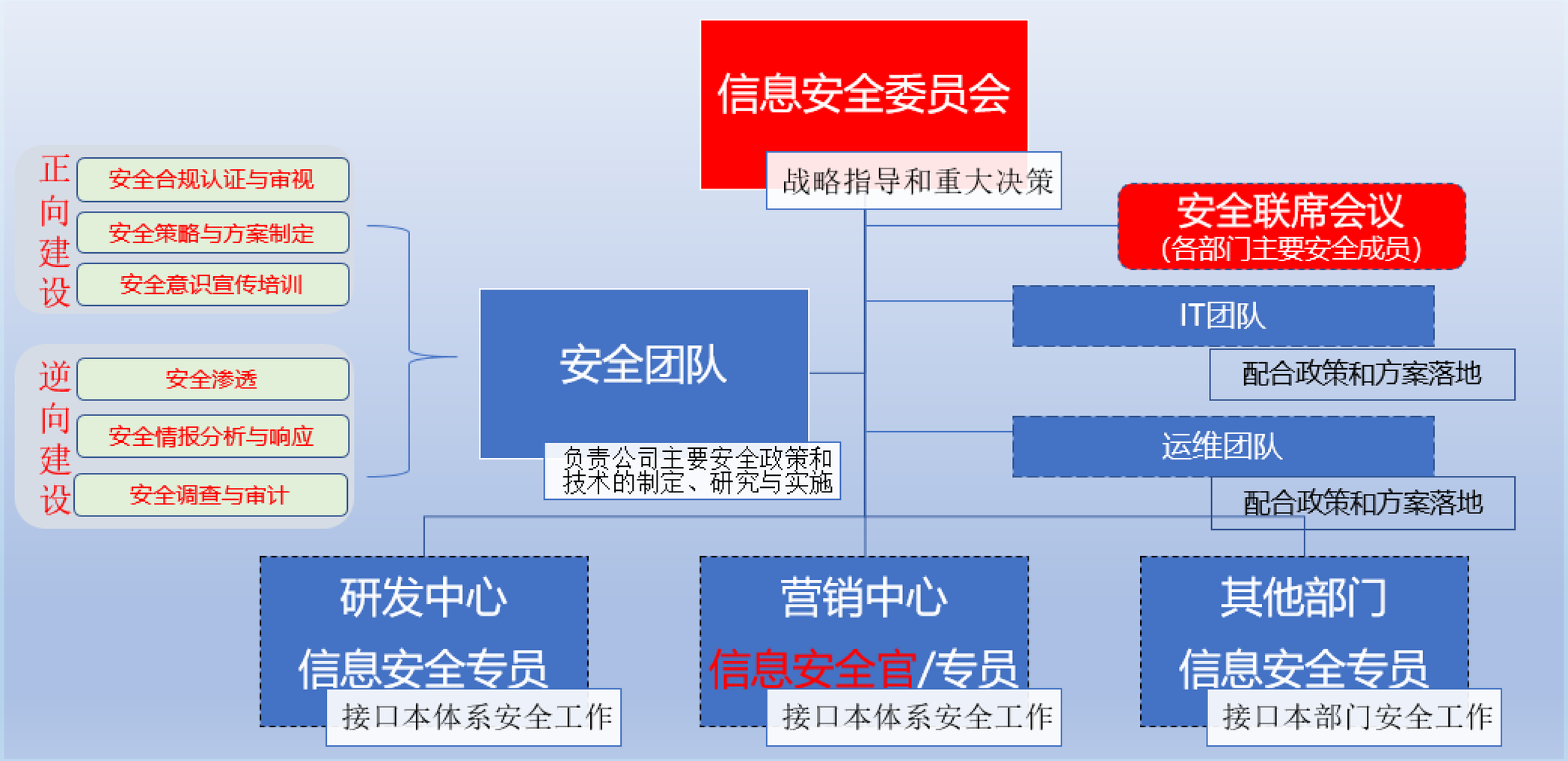
OnePlus 7 Pro 全网首销 1 分钟破亿

企业安全关注点

始于业务、服务于业务、终于业务

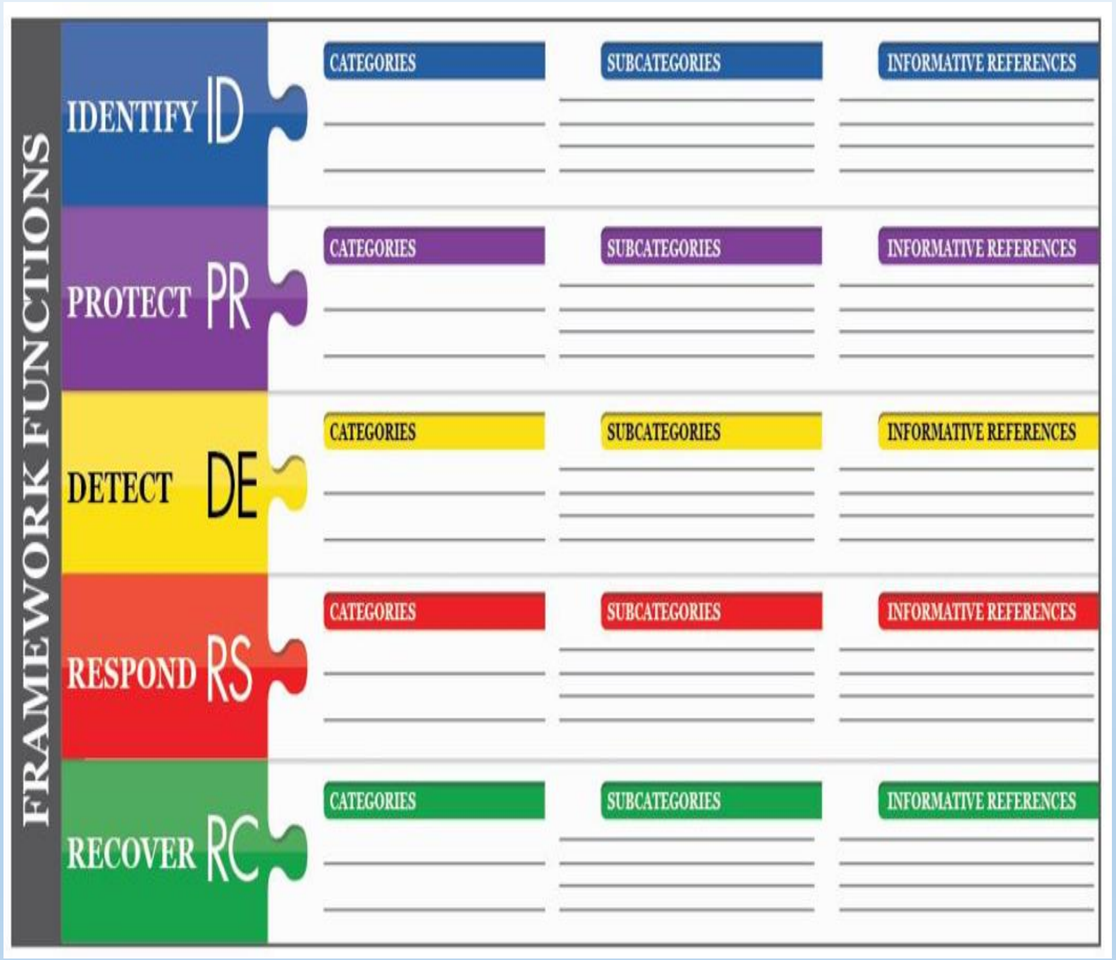
企业安全治理

组织建设（谁来治理：建组织）



安全治理（怎么治理：治理框架）

安全技术能力架构---IPDRR介绍
（Framework for Improving Critical Infrastructure Cybersecurity V1.1）

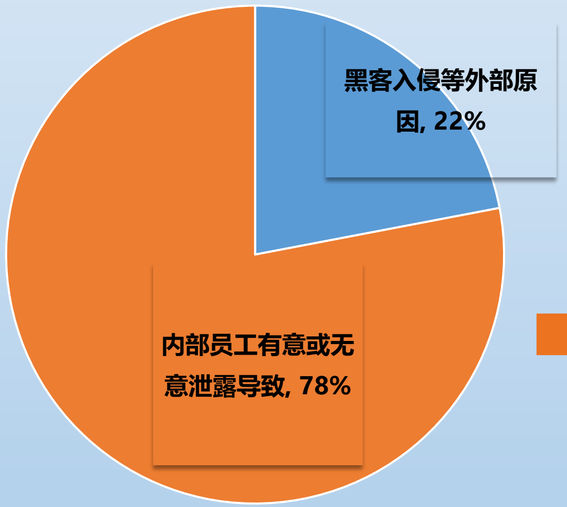


I	**识别**——发展组织理解，以管理系统、人员、资产、数据和功能的网络安全风险。 识别功能中的活动是有效使用框架的基础。了解业务环境，支持关键功能的资源以及相关的网络安全风险，使组织能够根据其风险管理策略和业务需求集中精力并确定其工作的优先级。此类别中的功能包括：资产管理；商业环境；治理；风险评估；风险管理战略
P	**保护**——制定并实施适当的保障措施，以确保提供关键服务。 保护功能支持限制或遏制潜在网络安全事件的影响的能力。此类别中的功能包括：身份管理和访问控制；意识和培训；数据安全；信息保护流程和程序；维护；保护技术。
D	**检测**——制定并实施适当的活动，以确定网络安全事件的发生。 检测功能可以及时发现网络安全事件。此类别中的功能包括：异常和事件；安全连续监测；检测过程。
R	**响应**——制定并实施适当的活动，以便对检测到的网络安全事件采取行动。 响应功能支持控制潜在网络安全事件的影响。此类别中的功能包括：响应计划；通信；分析；保持；改进。
R	**恢复**——制定并实施适当的活动，以维护弹性计划，并恢复因网络安全事件而受损的任何功能或服务。 恢复功能支持及时恢复正常运行，以减少网络安全事件的影响。此类别中的功能包括：恢复计划；改进；和通讯。

National Institute of Standards and Technology（NIST）
美国国家标准与技术研究院
April 16, 2018

信息安全工作自身业务的突破口（人员安全意识）

世界上**每分钟都有**信息安全事件发生。
究其原因，分类统计如下：



员工信息安全意识的薄弱正在成为企业面临的**最大风险**，
忽视信息安全意识教育，可能使企业遭受灾难性的打击。

安全意识松土 → 安全技能培养 → 人员意识从被动接受变为**主动思考与求助**

调查哪些事（案例1）

总结：
1、获取线索的及时性：找到嫌疑人（历史信息获取），而非发帖人。
2、嫌疑人网络信息搜索相关信息：（如相关昵称、其他帖子，进而推测活动城市、职业、年龄等）。
3、图片所有数据点分析：（时间、日期、手机联网状态等，后台可采集到的数据比对）。
4、综合分析：文字信息找人物、图片信息找数据，调查相关方，可能的组织和人。
5、坚持、注意每一个细节、相信自己的判断、发动内部团队力量。
6、不是所有人都有时间在意和坚持、不臆测、用事实来分析和判断。

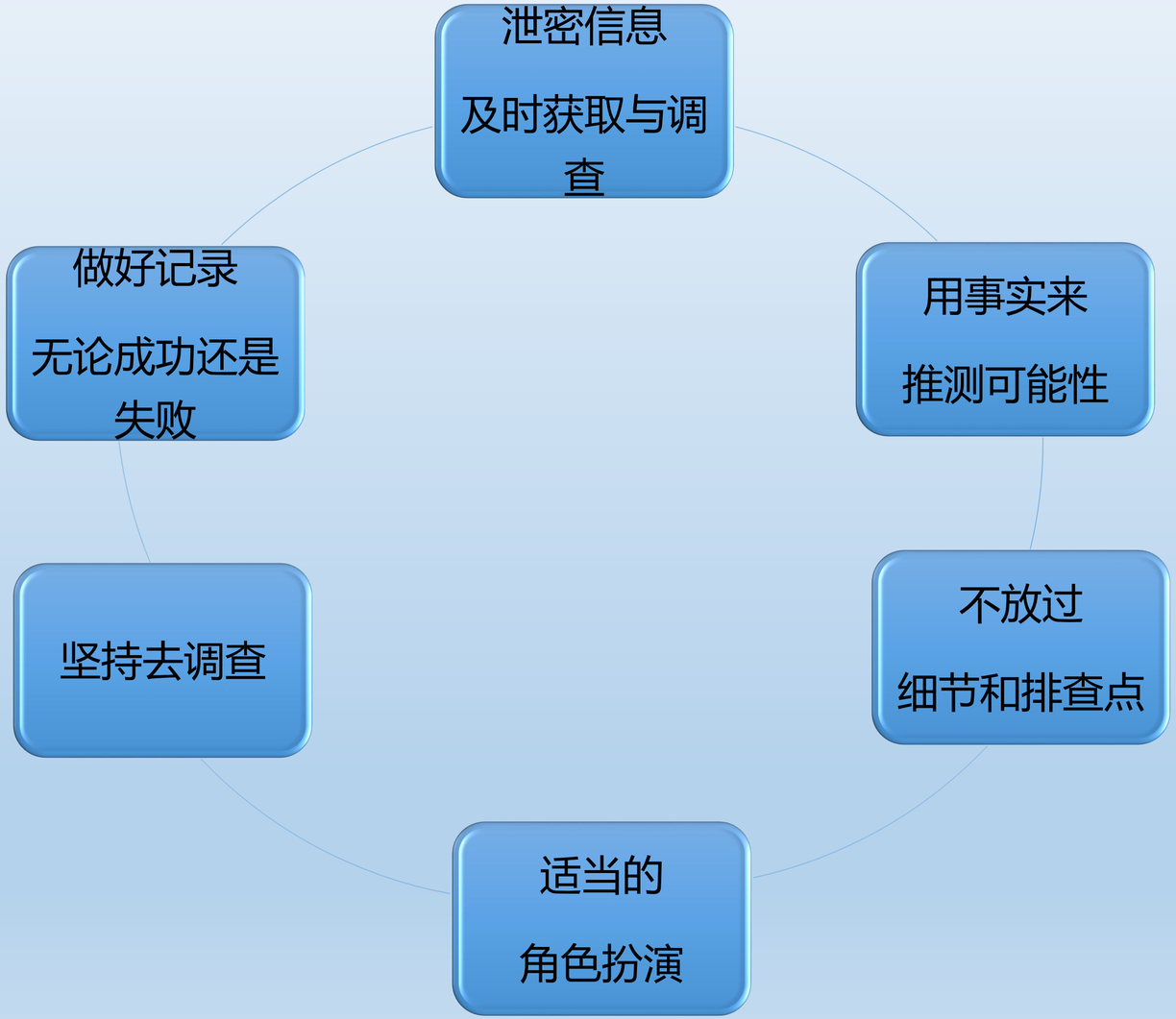
调查哪些事（案例2）

总结：
1、尽可能联系当事人（可能无果、也可能有线索）
2、明确表明身份和态度
3、泄密人信息搜集、分析、整理
4、按资产接触的环节、流程工序来逐一排查
5、中间可能有误伤，但要查到流程所有节点

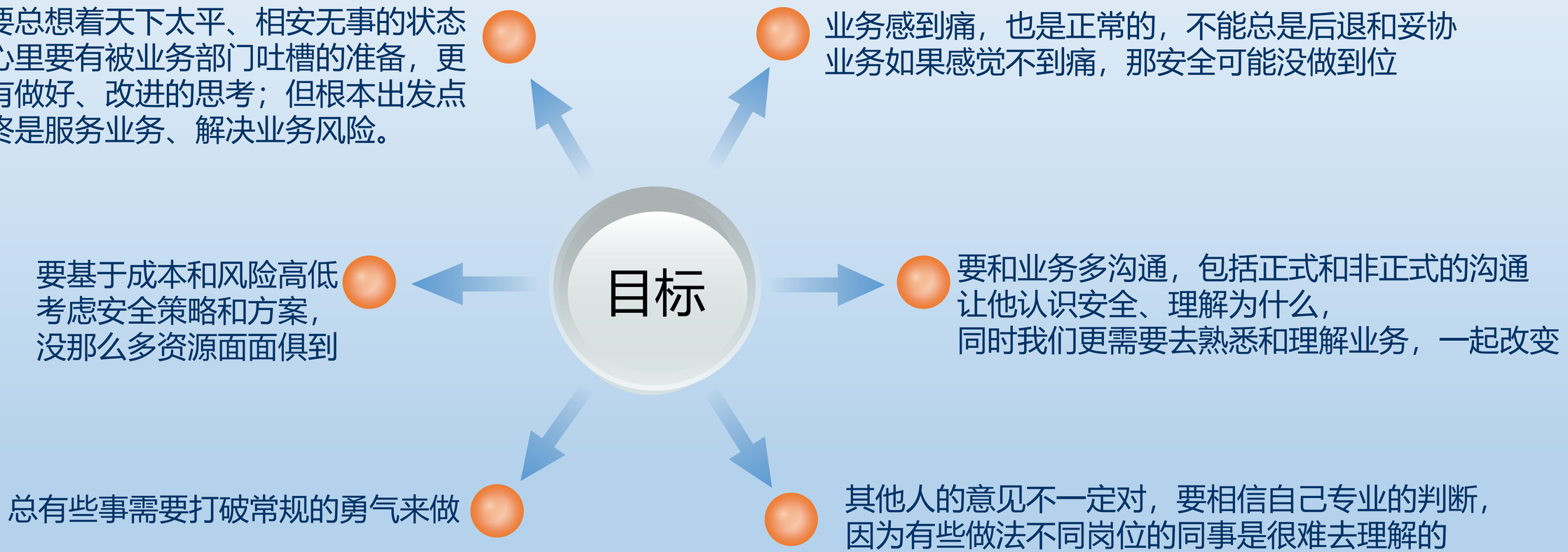
调查哪些事（案例3）

总结：
1、关注泄密信息本身的价值点（业务部门可能会甩包袱）
2、泄密时效性（关注最近几天内的活动）
3、核查接触信息的对象（如第三方），不用担心对象多
4、找一两天内的接收记录
5、找相关背景图：查怀疑对象的官方公开信息和互联网主流站点中相关方的公开信息

调查哪些事（要点总结分享）



企业安全建设的一点经验分享



ONESRC
一加安全应急响应中心
OnePlus Security Response Center

公司官网：https://www.oneplus.com

SRC网址：https://security.oneplus.com

郭惠龙 15019425416

Thank You !