甲方视角之外的安全运营思路

郭亮

北京数字观星科技有限公司

观点

“安全运营是多方协作的体系化工程，不是单纯的技术和流程体系，甲方（安全运营者）对影响安全运营协作方的工作思路的理解程度，是安全运营工作思考的分水岭。”

分享的核心观点：

一、基础：梳理好资产，是甲方与各方协作安全运营的基础；

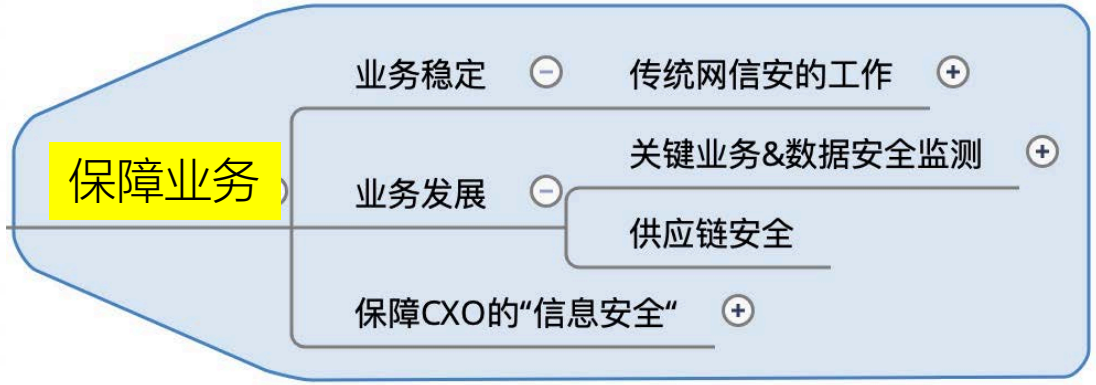
二、本质：关注业务，业务才是安全运营的宿主，安全运营的技术是手段；

三、趋势：数字化转型浪潮的趋势下，非受控区是安全运营需要关注的新重点；

目录

安全运营的三基色

安全运营的三基色： 合规 保障业务 体现价值



安全运营的本质是保障业务，除了保障“业务稳定”，推动业务发展提升业务品质，是安全运营的发展方向。而CXO的信息安全，将是安全运营的新热点。

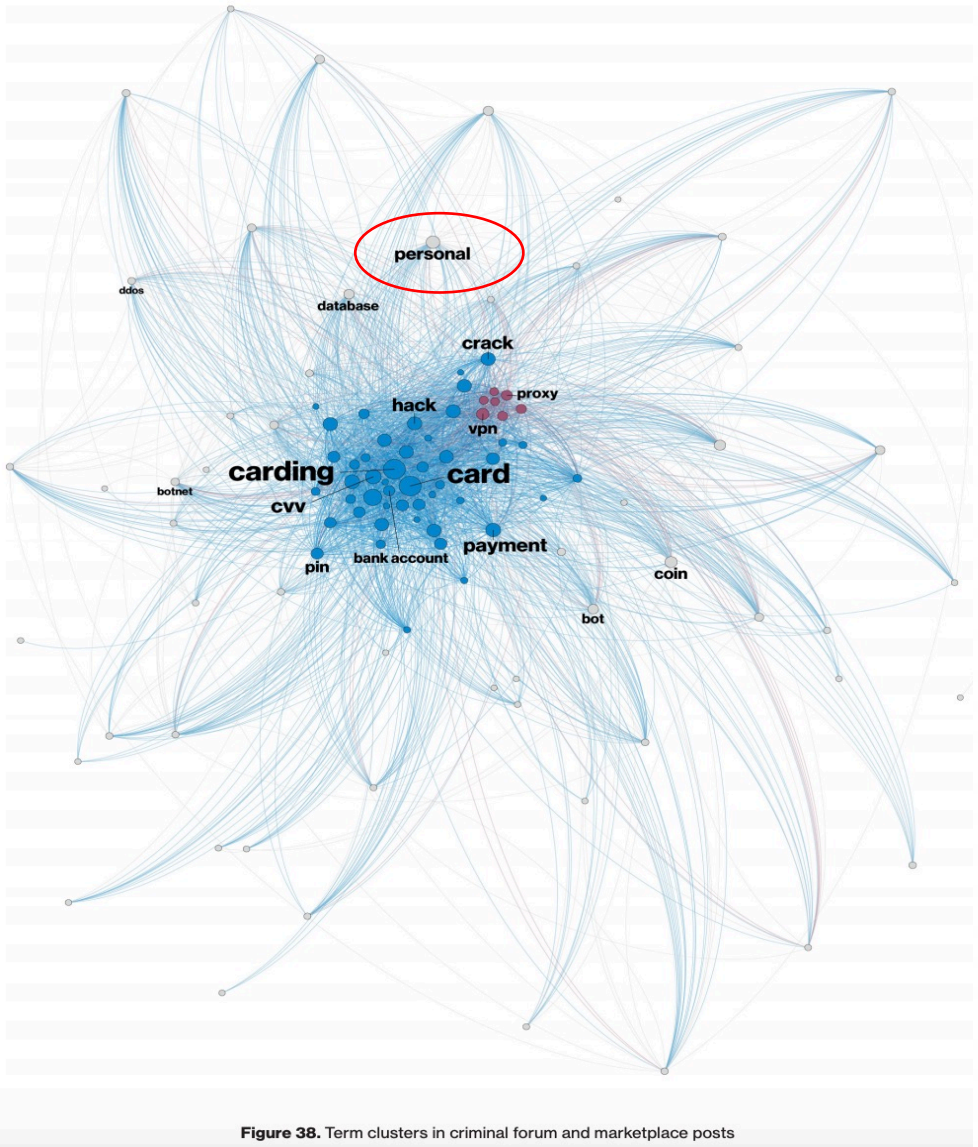


Figure 38. Term clusters in criminal forum and marketplace posts

Verizon 2019数据泄露调查报告(DBIR)中分析了31686个安全事件，60%的事件涉及高层目标。保障CXO的信息安全，是安全运营的新重点

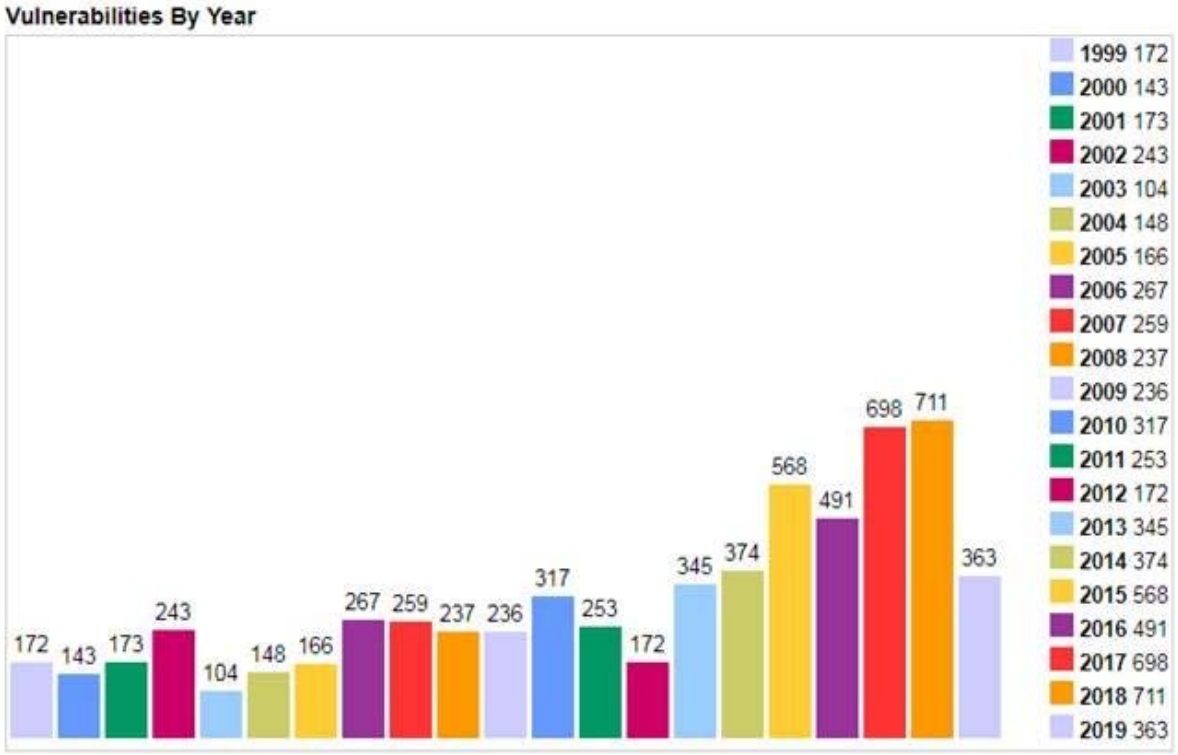
安全运营的“三基色”

体现价值

A. 在组织内部树立正确的安全观

B. 体现和度量安全运营的价值

当前在国家大型“红蓝”对抗常态化的基础上，比赛好名次，是体现价值很重要的手段，而传统的安全运营侧重于防，而溯源分析将是体现安全运营水平和价值的建设重点。



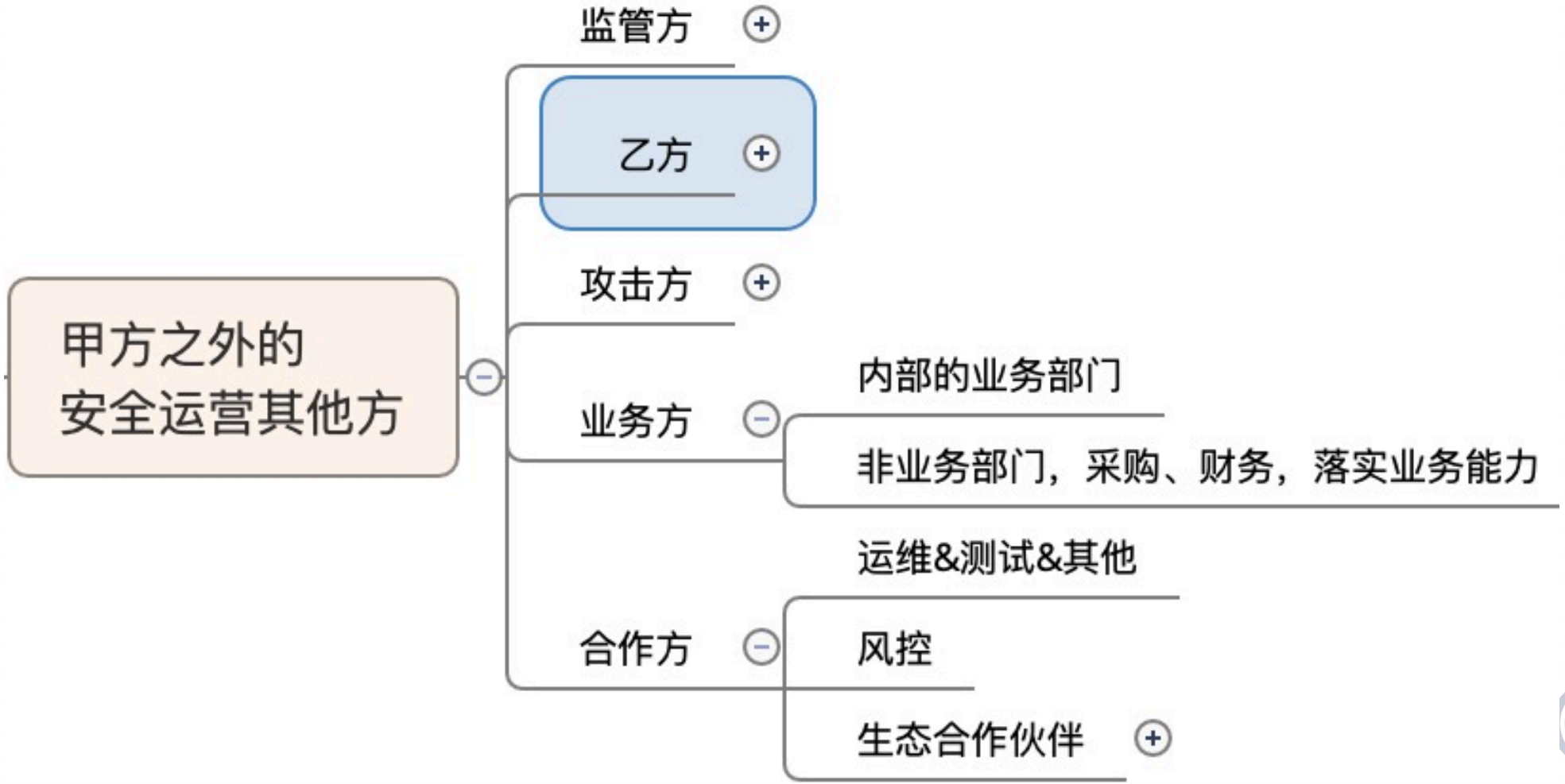
https://www.cvedetails.com/vendor/26/Microsoft.html

以微软为例，主动报每年发现的漏洞数据，不仅保持了产品在安全性方面的公开透明度，在公司和全球树立了正确的安全观。

目录

甲方之外-安全运营的其他方

甲方安全运营团队之外的甲方高层领导，乙方（厂商&服务商），还有监管方、攻击方、业务方（内部业务部门、非业务部门）、合作方等多个角色，各方都围绕业务资产，发挥其在安全运营中的作用。



安全运营的其他方-监管方

作用：结合政策导向和单点事件影响，驱动安全运营方向和阶段性工作重点。

策略：根据国家网络安全相关机构的监测与统计数据，形成有针对性的监管及检查要求，成为监管驱动安全运营发展的新趋势；

漏洞类型	漏洞数量	漏洞等级	漏洞数量	占比
IoT	11	高危	5	45.50%
		中危	5	45.50%
		低危	1	9%
WEB应用漏洞	1249	高危	407	32.58%
		中危	700	56.04%
		低危	142	11.38%
安全产品漏洞	48	高危	11	22.91%
		中危	29	60.41%
		低危	8	16.68%
应用程序漏洞	2808	高危	764	27.20%
		中危	1866	66.45%
		低危	178	6.35%
操作系统漏洞	343	高危	186	54.22%
		中危	142	41.39%
		低危	15	4.39%
数据库漏洞	69	高危	36	52.17%
		中危	30	43.47%
		低危	3	4.36%
网络设备漏洞	405	高危	158	39.01%
		中危	227	56.04%
		低危	20	4.95%

CNVD 2019年1至6月漏洞统计

01 应用程序、WEB应用漏洞多

02 基础应用高危害漏洞多

根据CNVD统计的漏洞数据，某监管机构下发通知，要求重点整治基础应用高危害漏洞；

安全运营的其他方-乙方

作用：不管是传统设备与服务供应商，以及基础资源服务商，都是安全运营的支撑方和基础，其自身安全直接影响安全运营的质量水平；

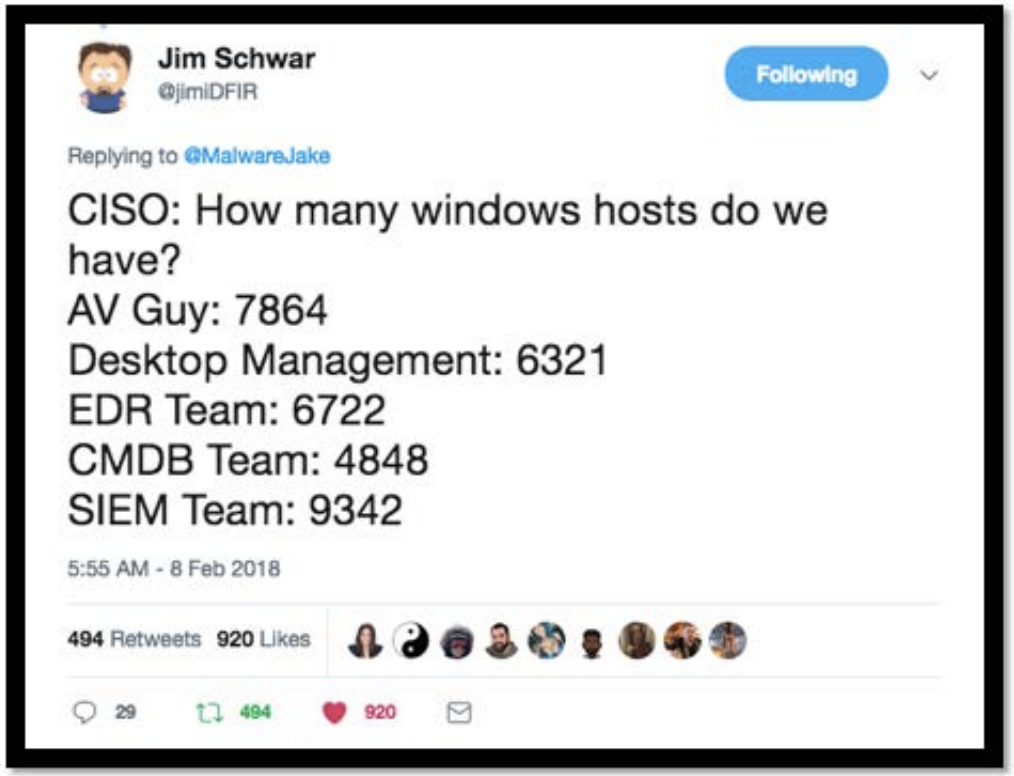
策略：及时和甲方形成安全运营数据的交换，是提高安全运营水平的重要趋势，例如：美国银行CapitalOne因为亚马逊AWS云平台出现的安全问题，其部分用户数据在GitHub泄漏了4个月，导致其上亿用户的数据受到影响。

7月29日，Capital One披露其数据遭泄露，影响1亿美国人和600万加拿大人，信息涵盖2005年至2019年的个人信息，其中包括大约12万个社会安全号码和77000个关联银行账号。经过FBI的调查，最终发现黑客是前AWS员工，Cpaital One存储在AWS S3中泄露的数据发生在2019年3月-7月之间，截止到7月17日被人邮件通知数据在Github泄露为止；

及时交互乙方安全动态，有助于优化安全运营应急响应基础；

安全运营的其他方-业务方&合作方

•**业务方**：理解安全运营的价值，并为安全运营提供沟通机制和资源保障。包括业务团队，以及财务、采购、审计等安全投入直接相关的部门，目前除了监管合规要求之外，通常是以业务资产自身价值来衡量安全运营及投入的必要性与价值，忽略安全运营价值和影响的隐形成本是常态。建立安全运营价值评价体系，需要业务方加强同业的沟通；



各方资产不一致的常态情况，安全能运营吗？

合作方：安全运维团队同级的运维、测试等团队，还有数据交互的生态链合作伙伴，都维护管理各自的资产系统以及数据，共同建立资产动态变更信息同步机制，是构建安全运营的关键基础；

目录

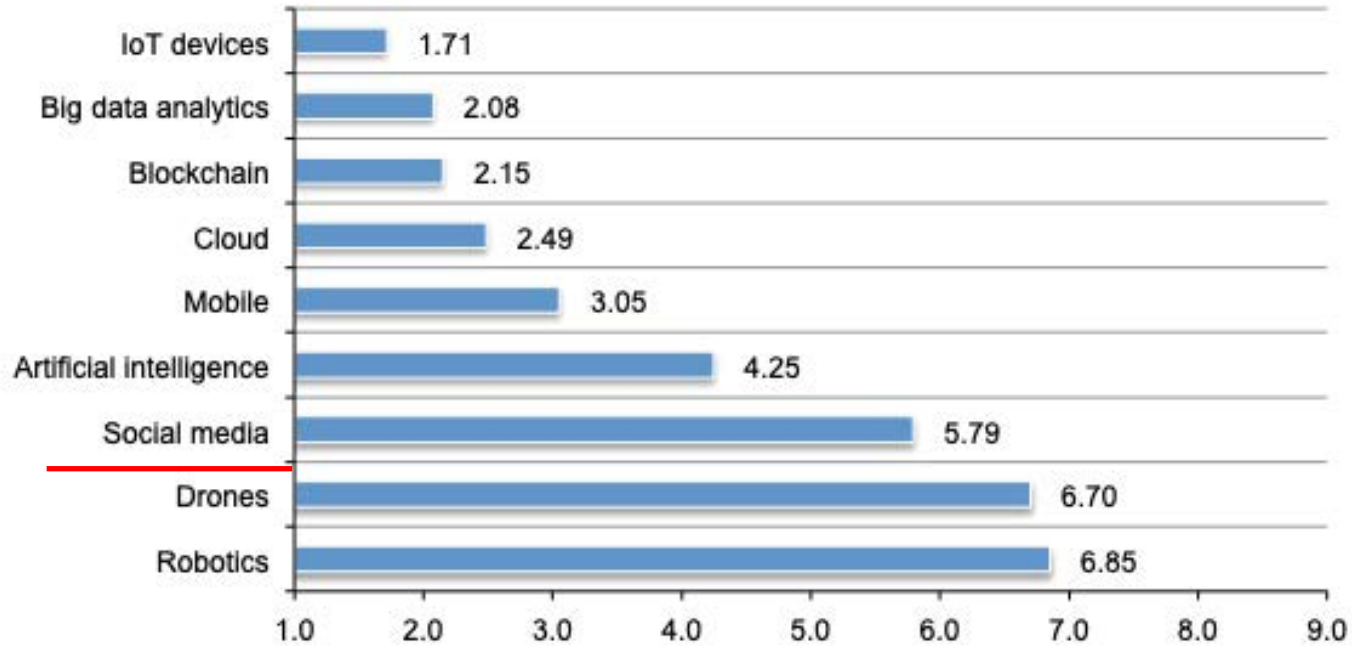
数字化转型浪潮下，新兴技术带来的风险

数字化转型浪潮趋势下，企业资产和威胁的维度越来越多。

传统的安全运营，不仅要关注传统IT资产的安全，还要为企业数字化转型提前奠定转型的安全基础。其中社交媒体的安全就是数字化转型浪潮趋势下安全运营的新重点。

Figure 13. The impact of disruptive technologies on the digital transformation process

1 = most negative impact to 9 = least negative impact



来源：https://www.ibm.com/downloads/cas/ON8MVMXW
标题：Leaders Must Balance Risk & Growth

传统安全运营-甲方视角之困

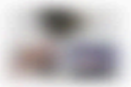
08:50
我们现在应该是被 深入 APT，

08:51
经常受到欺诈邮件，是冒充合作伙伴或者 LP发过来，要求打款，而且收件人是特别针对负责对应权限的人，

08:52
欺骗原地址还是我们的下属公司或者LP，邮件地址略微有区别，但是名字完全和下属企业或者LP里面的人一样，只能人为去识别，

08:53
我们正在考虑怎么解决，还没有特别好的对策，目前只能是通过培训提高人员安全意识，另外付款环节，内部增加了一些管控流程环节，不能仅仅依靠电子流信息。


郭亮 08:54
APT的问题

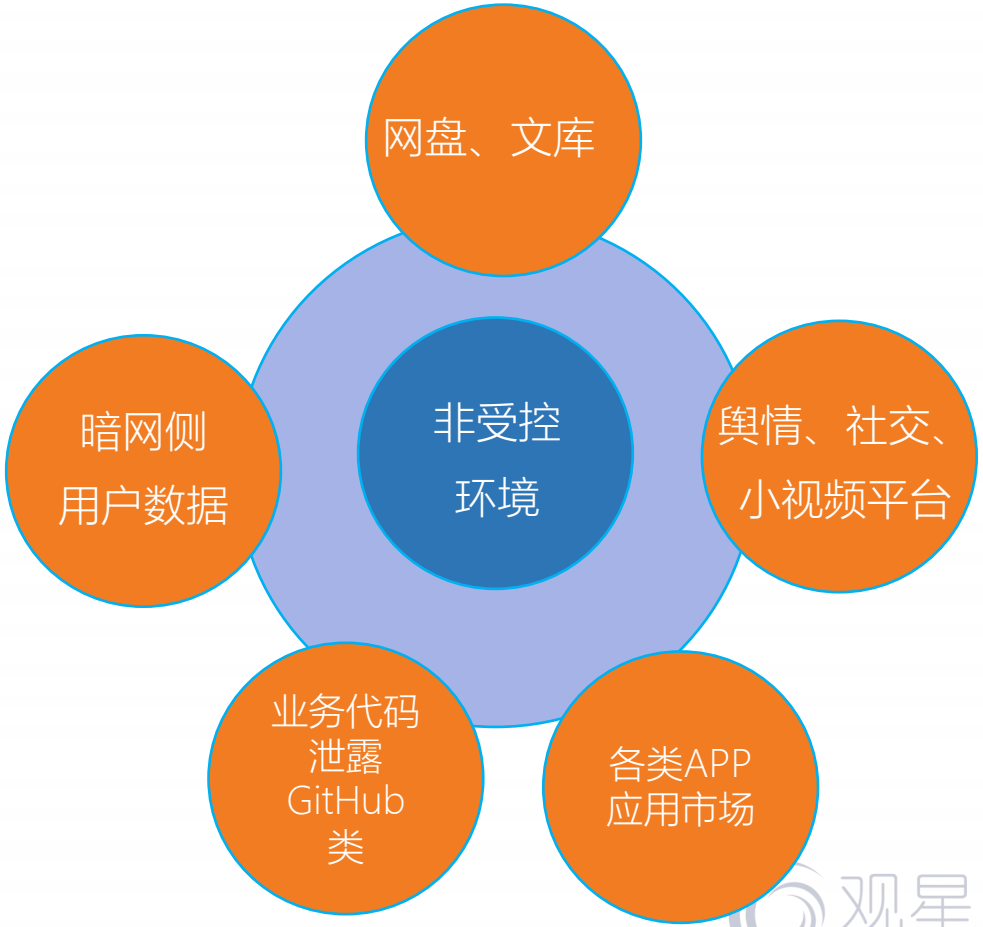

08:59
对，比较尴尬的是，我们 IT 对业务的理解深度一般，很多数据比较敏感，IT不可以接触的。

我们IT对业务的理解深度一般，很多数据比较敏感，IT不可以接触的

数字化转型趋势下，安全运营兼顾的二维资产场景

观星 Data Star Observatory

按照数字资产暴露面来看

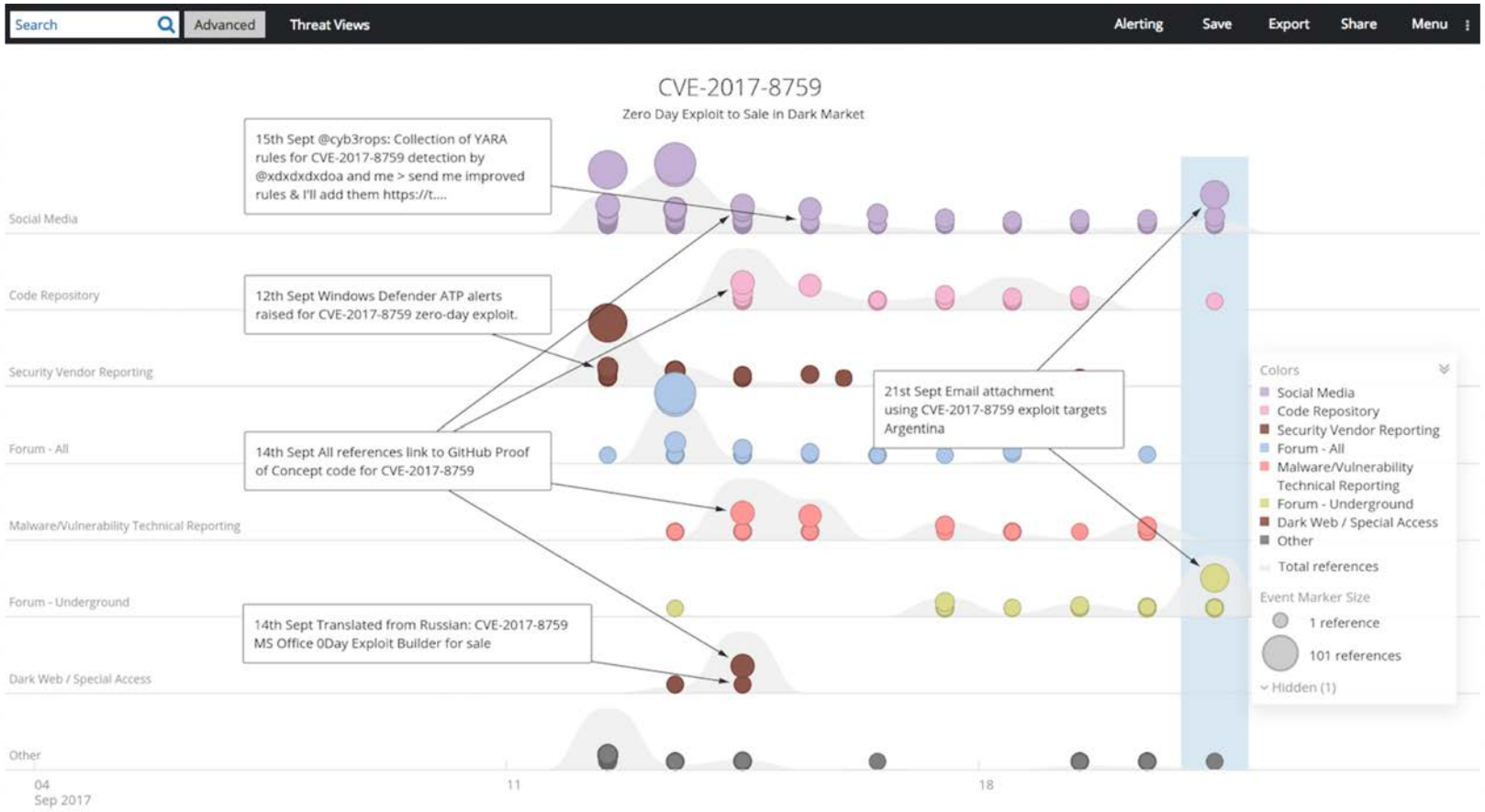


非受控环境-数字资产以及安全威胁的变化

及时监测非受控区，是数字化转型趋势下的安全运营新维度。

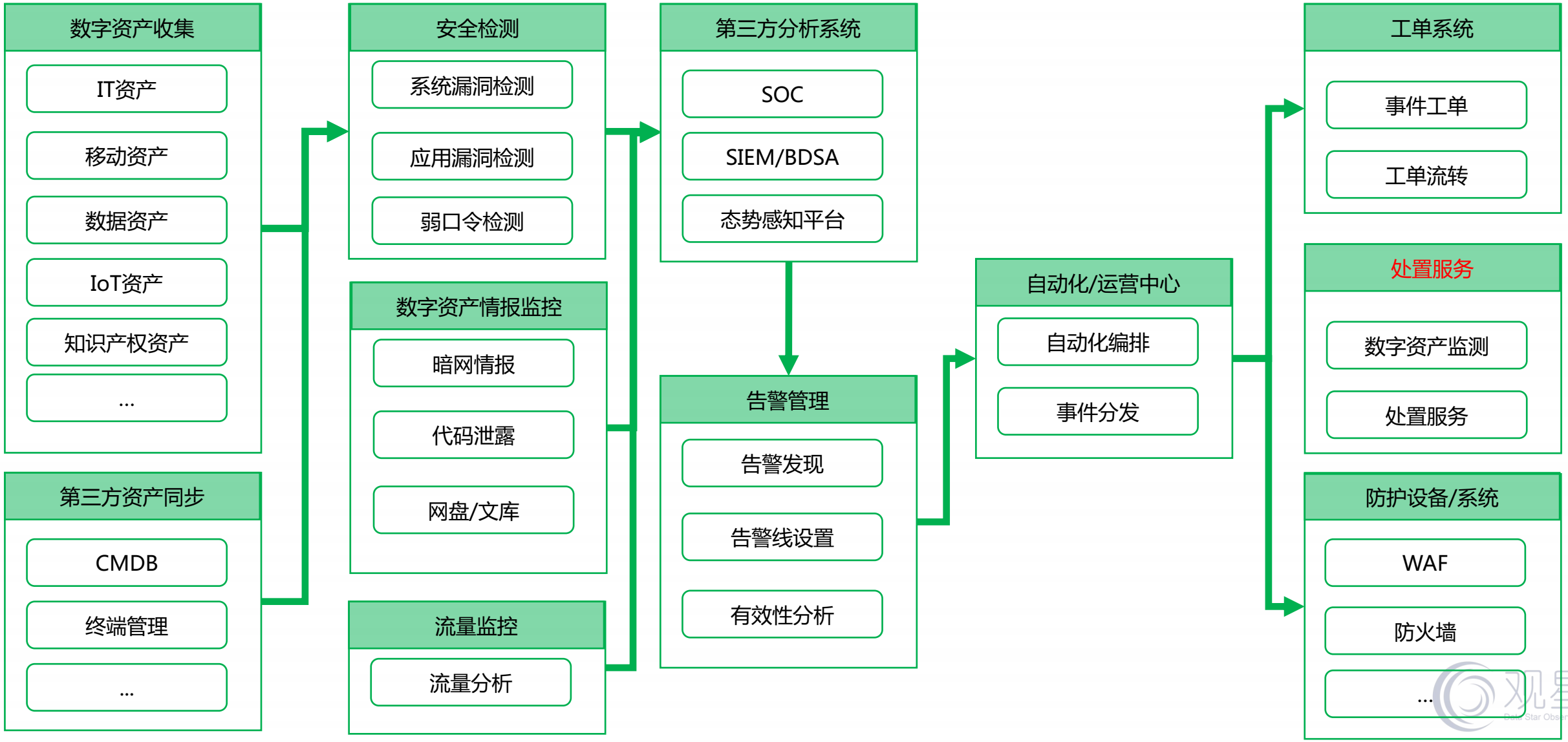
以暗网为例，不仅是用户数字资产贩卖的区域，也是安全威胁变化的发起来（漏洞在暗网交易中武器化、商品化）

2017年暗网出现CVE-2017-8759漏洞exp的交易，7天之后阿根廷某金融交易所就遭受了利用该漏洞的网络攻击。



源自： RecordFuture

基于数字资产的安全运营体系



数字化转型趋势下的安全运营

- 数字化转型趋势下安全运营的发展
  - 数字资产侵权
  - 行业视野～同业的经验情报交换
  - 增加上下游的视野
  - "杜绝猪队友"

THANKS

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE

感谢您的观星