真正可靠，安全运营体系的规划、建设与落地

陈 然

奇安信网络安全部安全运营经理

目录

安全运营是什么


```
Starting Nmap 7.30 ( https://nmap.org ) at 2016-11-02 20:39 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00020s latency).
All 1000 scanned ports on 192.168.56.1 are filtered
MAC Address: 0A:00:27:00:00:00 (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.56.100 are filtered
MAC Address: 08:00:27:98:62:C4 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.00025s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:34:58:53 (Oracle VirtualBox virtual NIC)
```

现在很多公司都有安全部，也有很多优秀的安全工程师

他们可以搞定防御很高的系统
他们可以写出很棒的扫描器

But ...我们的公司真的安全了吗?

当然没有，我们依然有漏洞，依然被搞定，为什么

安全运营到底是什么?

那就是不断地发现问题、分析问题、解决问题、检验效果，持续跟踪不停优化迭代的过程。

最终目的是持续保护企业安全

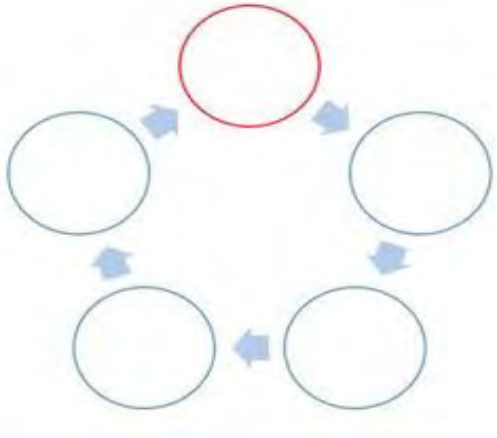
目录

安全运营解决什么

安全设备失效
(没上架、BYPASS、默认PERMIT、...)

检测能力低下
(缺少规则、漏误报、部署失位、...)

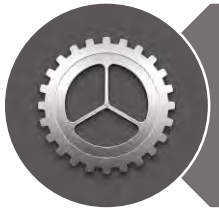
安全能力缺失
(不会干、干不完、量太大、...)



流程闭环缺失
(漏洞发现没修、端口开放没关、...)

安全运营解决什么

解决这些安全问题，建设好安全最后一公里，需要...



把安全设备用起来

- 让设备有效果

提高威胁检测能力

- 让异常被发现

提高安全对抗能力

- 让异常能处置

工作流闭环

- 让事项被完成

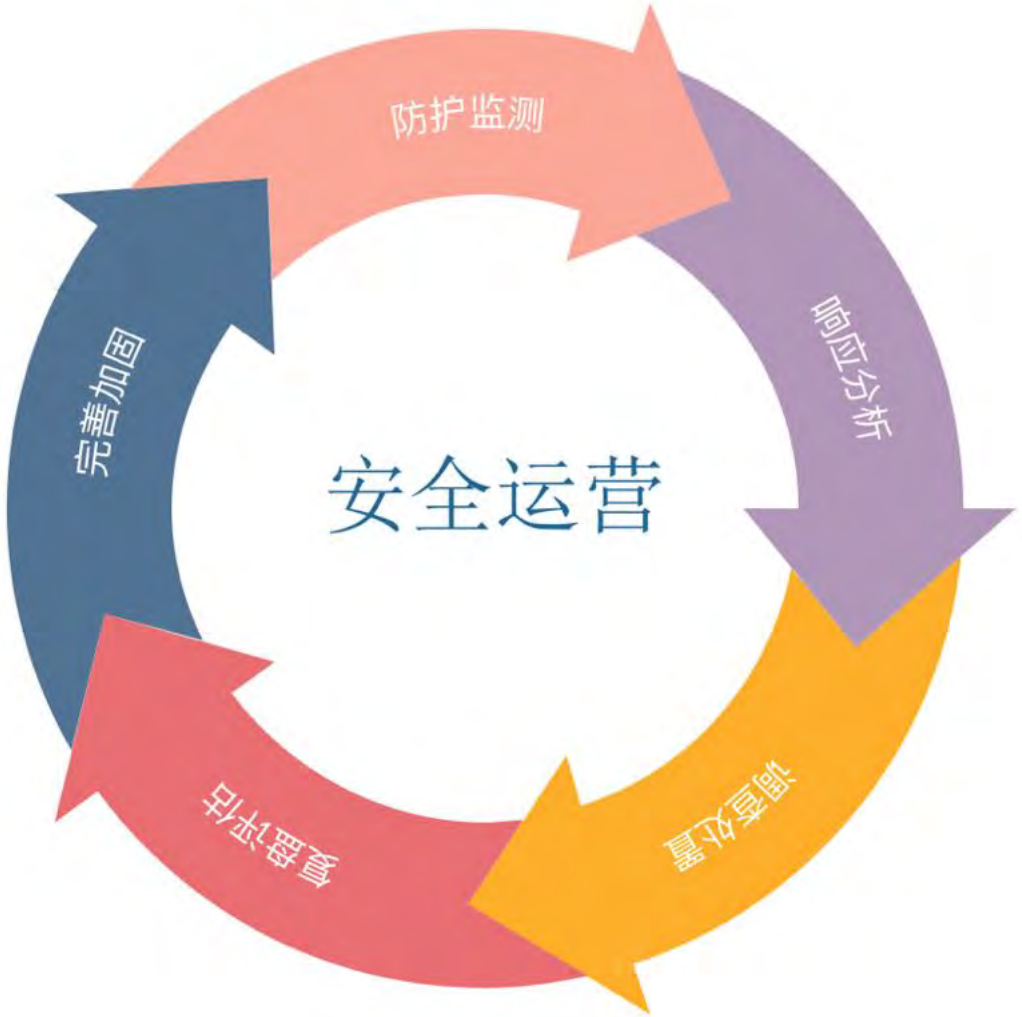
安全运营解决什么

- 总结下来就是不断提高安全能力和内部服务质量，并保持在稳定的区间：
  - 标准化（制定SOP，保证人员能力足够解决发现的问题）
  - 流程化（制定运营流程，保证所有的问题被响应、被处理、被解决）
  - 工程化（把能力工具化，保证安全能力快速输出给设备和员工）
  - 自动化（解决海量的问题，结合工程师安全能力与机器快速处理能力）

目录

安全运营体系设计

所以你需要的是一个完整的安全运营体系



防护监测：
持续性动态监测
设备阻断

响应分析：
对事件进行快速响应
对告警或信息进行确认

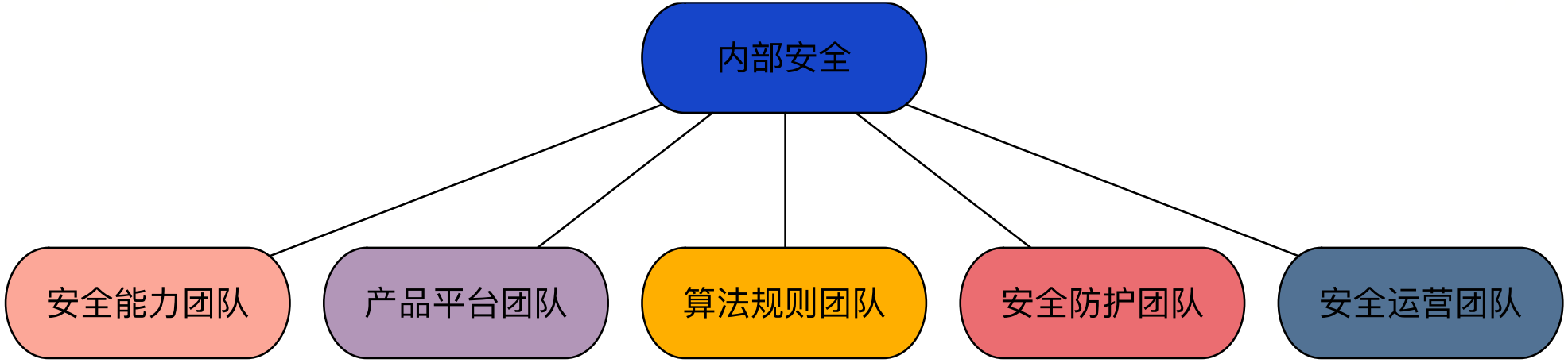
调查处置：
对安全事件分析还原
快速进行止损、善后

复盘评估：
复盘事件原因
提出完善修复方案

完善加固：
执行修复方案
增强防护和监测能力

安全运营体系设计

组织架构设计1



安全能力团队：攻防渗透、样本分析、威胁情报、漏洞研究等核心安全能力的支撑团队；

产品平台团队：让机器智能复制工程师经验，解放人力，解决安全中的“海量”难题；

算法规则团队：解决攻击无法被检测的“规则困境”，让攻击被感知；

安全防护团队：推动项目建设，实施防护措施，提高安全防御能力；

安全运营团队：狭义的运营，发现攻击、解决事件、处置威胁，让工作闭环；

安全运营体系设计

组织架构设计2

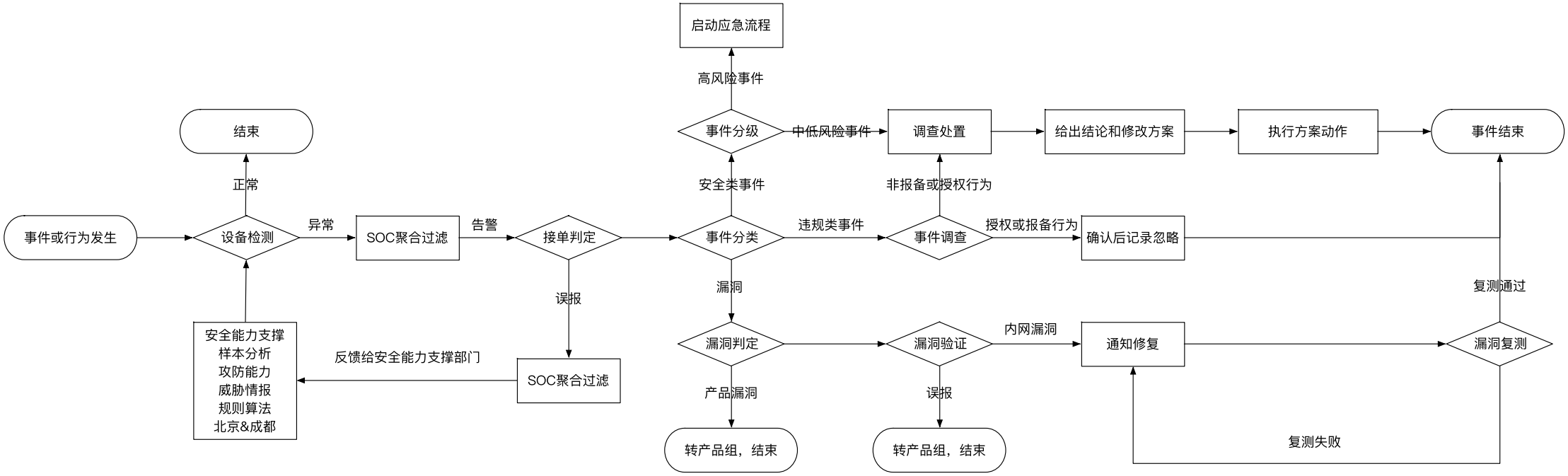
组织分类	人员能力定位	目标
一线运营	基础事件响应处置 沟通协调能力	完成工作闭环 解决基础问题 承接对外沟通任务
二线运营	高级威胁发现与跟踪响应 应急响应 具备一定的攻防能力	满足技术要求 处置高级或严重威胁
安全能力团队	样本分析威胁情报（逆向、动态调试、大数据） WEB渗透、内网渗透（红队性质） 安全研究能力	提高安全能力 检验安全运营效果
算法规则团队	制定算法规则，提高检测率、减少误报	构建攻击或者异常检测规则
安全防护团队	项目推进管理（产品部署、调整网络架构、域）	
产品平台团队	采购、自研、利用开源平台搭建必要的系统、产品、工具	

安全运营体系设计

安全防护设计

安全分类	功能定位	产品
安全总控	日志、告警、事件等数据聚合 管理中心 数据分析中心	SOC类产品
服务器与终端安全	终端管控、补丁修复、 病毒查杀、基线合规	终端安全助手 HIDS
	终端行为管控 高级威胁发现 攻防规则制定数据来源	EDR
网络安全	全流量分析 流量攻击匹配 IOC过滤阻断	全流量分析系统
应用安全	应用层安全加固 日志收集、存储与检测	NGSOC
数据安全	数据防泄漏、防篡改等	DLP、云平台监控等
APT对抗	样本沙箱 杀伤链聚合归并	SandBox

安全运营流程


事件或行为发生
设备检测
正常
结束
异常
SOC聚合过滤
告警
接单判定
误报
SOC聚合过滤
反馈给安全能力支撑部门
安全能力支撑
样本分析
攻防能力
威胁情报
规则算法
北京&成都
事件分类
高风险事件
启动应急流程
安全类事件
违规类事件
事件分级
中低风险事件
调查处置
给出结论和修改方案
执行方案动作
事件结束
非报备或授权行为
事件调查
授权或报备行为
确认后记录忽略
漏洞
漏洞判定
产品漏洞
转产品组，结束
漏洞验证
内网漏洞
误报
转产品组，结束
通知修复
漏洞复测
复测通过
复测失败

安全运营体系设计

安全运营验证与度量

度量维度	度量指标	检测手段	检测意义
基础指标	终端安全软件安装率 终端安全软件正常率 安全设备覆盖度 规则数量	数据统计	基础数据是进行安全运营地基，没有这些也就没有安全运营的可能性
安全运营效果	规则覆盖度 平均响应时长 平均处置时长 检出率（漏报率） 误报率 对抗成功率	实战结果 红蓝对抗 渗透测试（黑、白、灰） 漏扫等	检验运营效果、发现未检出的漏洞，未发现的威胁，提升高度可靠性
价值维度	满意度 对业务支撑能力	走访座谈 调查问卷	安全最终要服务于业务，为业务正常开展保驾护航

目录

安全运营的落地实践

基础数据平台建设与数据积累

- 运营需要足够的基础数据
- 基础数据需要一个合适的系统进行存储查询（S_CMDB）

- 员工表和组织架构表一般相对容易
- 资产表：
  - IP、OS、PORT、SERVICES、API、…
  - MIDWARE、LANGUAGE、FRAME、…
  - SOFTWARE、…
- 资产与员工表的关联

以上这些都是我们进行运营的基础支撑

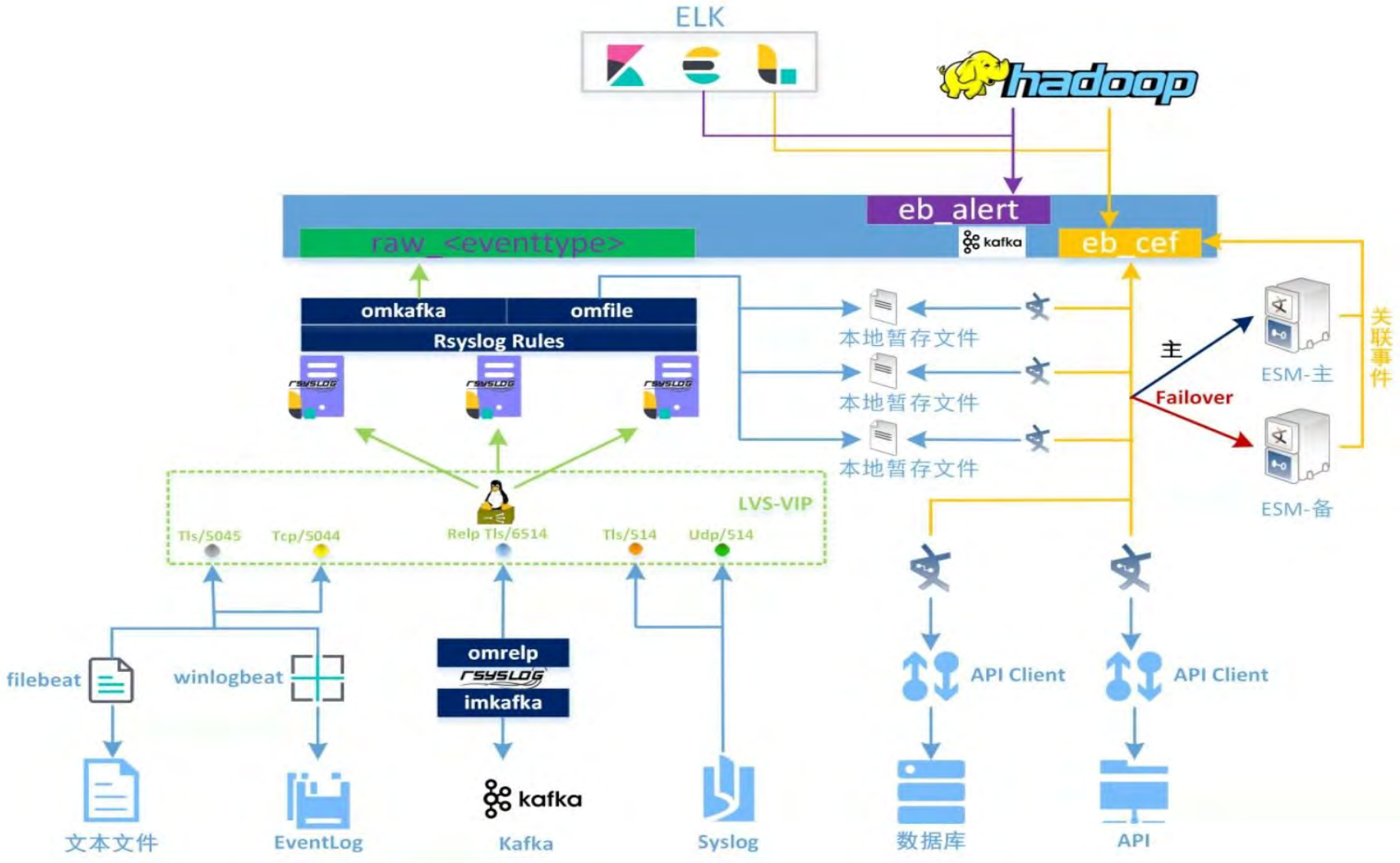
需要的基础数据	数据来源部门
员工表	行政或人力资源部门
资产表	IT部门与安全部门
组织架构表	行政或人力资源部门
网络拓扑	网络运维部门与安全部门
系统信息	研发管理中心
组件信息	研发管理中心
编程语言信息	研发管理中心
框架信息	研发管理中心
终端软件信息	主机运维中心

安全运营的落地实践

安全能力支撑

能力	部门	备注
威胁情报	安全能力中心 community.riskiq.com	提供情报、IOC库
样本分析	安全能力中心 virustotal	进行样本判别、逆向分析等
攻防渗透	安全部、安服、红队	进行攻防对抗、实战演练
漏洞研究	安全部、安全能力中心、漏洞库	挖掘0DAY、挖掘已知漏洞
应用安全	产品与内部系统安全团队	WEB、移动端进行安全保障

分析中心系统平台搭建


ELK
hadoop
eb_alert
kafka
raw_<eventtype>
eb_cef
omkafka
omfile
Rsyslog Rules
本地暂存文件
本地暂存文件
本地暂存文件
主
Failover
ESM-主
ESM-备
关联事件
LVS-VIP
Tls/5045
Tcp/5044
Relp Tls/6514
Tls/514
Udp/514
filebeat
winlogbeat
omrelp
imkafka
API Client
API Client
文本文件
EventLog
kafka
Kafka
Syslog
数据库
API

安全运营的落地实践

标准动作SOP举例，做到标准化，快速复制安全能力

- SOP标准动作
  - ITS&VPN
  - Windows类
  - 暴力猜解
  - 漏洞利用
  - 漏洞运营
  - 资产隐患类

SOP名称	新增域名处置		
事件分类	互联网高危端口	事件小类	新增互联网高危端口处置
对应规则			
规则评价	误报低		
事件解释	确认IP负责人，关注新增高危端口是否可以关闭/潜入内网/ACL访问控制		
标准动作	（1）查看互联网高危端口变动邮件，主要针对新增高危端口处置。 （2）首先询问IP负责人该高危端口是否有特殊用途必须得开？ ①是必需业务——运营同事对必需业务做记录并邮件或蓝信反馈至王章政加白，case结束，否：进入下一动作 ② 不是必需业务——询问是否能关闭端口? ③可以关闭——运营同事进行具体原因记录，测试端口已经关闭或下次监控数据不再报，case结束，否：进入下一动作 ④不能关闭——询问是否能迁移到内网？ ⑤可以迁至内网——运营同事进行具体原因记录，待迁移到内网，测试端口已经关闭或下次监控数据不再报，case结束， 否：进入下一动作 ⑥不能迁至内网——询问是否能加ACL做访问控制？ ⑦能做ACL访问控制——运营同事进行具体原因记录，待加完ACL，测试端口已经关闭或下次监控数据不再报，case结束，否：进入下一动作 ⑧不能做ACL访问控制——做特殊事件处理，事件升级；反馈至网络安全部 （3）需要将询问结果记录在wiki当日的安全运营日报-高危端口部分，跟进高危端口处置进度，及时更新记录。		

流程闭环的确保

- 人不是机器，总会有能力高低、总会状态起伏，总会有责任心强弱，流程保障不能靠人
  - 一靠机制：
    - 日例会，每天对前一日的事件、漏洞等进行简要跟进和分析；
    - 周回顾，每周对当周事件进行跟进、催促未关闭事件和未修复漏洞；
    - 月总结，每月对重要运营问题进行总结复盘、跟进重大加固修缮方案的进度；
  - 二靠平台：
    - 把制度流程嵌入平台工单流转逻辑，使得流程步骤没办法绕过；
    - 重要流程审核机制，对忽略、复验完成、修缮进度结束、关闭等节点进行double check；

目录

实战效果检验下的安全运营

基础成果

成果分类	成绩
流量收集覆盖度	（1）所有办公区全覆盖； （2）所有IDC的互联网方向流量全覆盖；
终端覆盖度	（1）98.52%以上的终端安装率； （2）93.21%的实名率； （3）93.96%以上的基线合规率，补丁安装率 （4）基本消除重大终端漏洞和终端弱口令；
服务器覆盖度	（1）互联网侧服务器全部安装终端安全防护软件；
漏洞事件运维	（1）事件100%关闭； （2）漏洞（中危及以上）100%修复；
蜜罐	（1）完成蜜罐密网的部署；
SOP	（1）创建100+ SOP

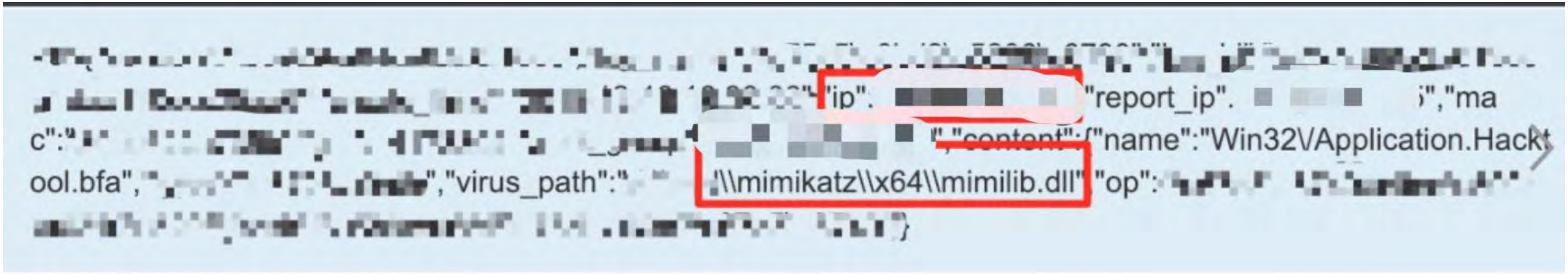
案例一 红队日常攻击被检测

背景：

AD服务器日志收集平台检测到关键字mimikatz 随即判定AD已经失陷，根据Workstation和地址信息在域内进行追踪溯源，最后判定攻击IP为 a.b.c.d ， 根据该IP地址的交互认证信息，找到其使用者，归属于公司红队成员 ， 其在进行授权渗透测试。

成果：

快速发现关键服务器被攻击，找出攻击者，阻断攻击行为，避免进一步损失。



案例二 攻防演习阻断攻击方进入内网

背景：

攻防演习期间，内部二次认证账号系统出现新的移动终端绑定事件。与帐号拥有者联系确定为非本人行为。立即意识到有其他人获取到了该用户的账后凭证，妄图通过二次认证进入内网。首先，立即停用该账号，然后排查移动终端唯一识别标识，最终根据移动设备终端标识发现攻击者。

成果：

阻止攻击方进入内网，并追溯到攻击者。最终防御方在攻防演习中取得了胜利。

案例二 攻防演习阻断攻击方进入内网

[redacted]用户绑定设备成功|有新绑定设备

名称	数值
原始日志时间	29 Mar 2019 16:21:36 CST
日志源设备地址	[redacted]
日志源资产名称	
日志源所在网段	[redacted]
日志源主机名称	NULL
日志源设备管理人	NULL
绑定账号	
设备ID	[redacted]
设备操作系统	iOS
设备型号	iPhone11,6
日志源	[redacted]
处置建议	请尽快与相关人员确认原因
说明	此报警每次均提醒

案例三 及时发现修复ThinkPHP5漏洞保护公司资产

背景：

TP5RCE 这个漏洞一出来，随即安全运营小组对内网资产进行了盘点扫描和检查，发现部分系统存在该问题，立即推进修复，并最终紧急修复完成。后面即发现公网利用TP5RCE漏洞执行mstha 命令反链cobalt-strike的批量攻击，由于及时跟进修复完成，公司没有造成损失。

成果：

及时修复了漏洞，避免了公司的损失。

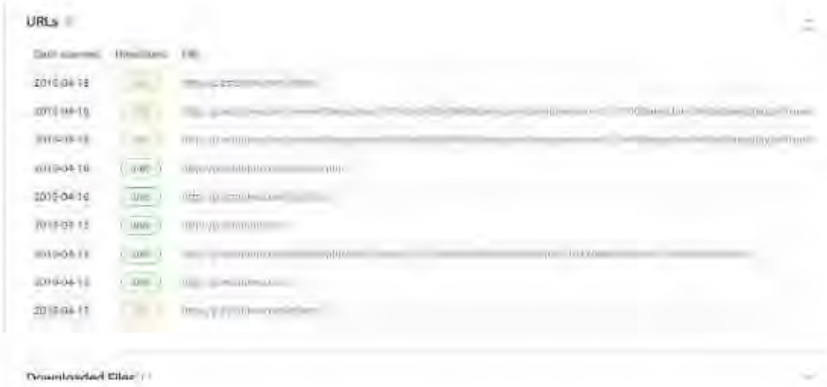
案例四 终端安全运营发现感染无文件永恒之蓝变种

背景：

公司服务器出现异常流量，排查进程之后却没有找到对应文件，进行深入分析日志后，并根据流量进行排查，结合威胁情报IOC，终于发现这是一类无文件落地的永恒之蓝变种。

成果：

按照SOP知道，登录服务器，进行修复查杀等工作，避免了公司的进一步损失。



2、检查进程中是否存在其他挖矿木马，如果存在，就先结束进程，以独占系统资源挖矿。一般挖矿木马都具体的行为，此次更新为更好的独占系统资源

3、PowerShell进程中注入执行矿机，若失败就释放PE文件（用被发现的风险换取执行机会），继续执行挖矿，通过成功的进程注入，来避免PE文件的释放，达到无文件落地，同时也能在内存中持续的挖矿。

下载相关powershell脚本，可以发现脚本已被混淆，无法直接分析代码。

通过其他相关分析，基本能判定powershell脚本实现整个挖矿木马的功能。

目录

未来展望

- 目前安全运营的理念还没有统一：

就像读者读哈姆雷特，不同的人对安全运营有不同的理解和认识，更没有统一的标准，这是问题也是机遇。

问题是没有统一的理念和标准，难以保障有效的、快速的推进安全运营的发展与普及；机遇是我们各有想法，一起碰撞可以互相激发，取长补短；相信最终会形成博采众家之长的安全运营标准。

- 缺乏足够的有效的产品、工具、平台：

我们不缺乏各类安全产品，无论是终端的、流量的、态势感知的等等，但是互相之间不能互联互通，标准化SOC的发展总是不能适应各家复杂的情况，缺乏一个高效率的稳定的安全综合管控运营平台。

THANKS

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE