



基于终端多维数据的攻防对抗与用户行为画像

赵灿辉

奇安信集团网络安全部安全运营总监

目录

1. 概述
2. 终端安全运营成熟度提升
3. 基于EDR的终端防守
4. 多维数据在运营中的应用

我们期待终端安全能做什么？



我们面临的安全问题：

根据B2B International 17年6月的一份研究，**46%**的信息安全事故是由**公司内部员工**导致的，占有原因的**第一位**。

奇安信威胁情报中心的全球高级持续性威胁（APT）2018年总结报告中指出：“在过去的APT威胁或者网络攻击活动中，利用邮件投递恶意的文档类载荷是非常常见的一种攻击方式，例如**鱼叉邮件攻击**，**钓鱼邮件**或BEC攻击”，可见许多APT行动背后的攻击者，**经常使用办公终端**，作为攻入一个组织的跳板。

TechRadar的一篇文章中写到，**29%**的员工承认他们将他们的用户名和密码给过其他同事。

而根据卡巴斯基19年5月的一份研究，**33%**的员工仍可以访问老东家的文件和文档.....根据调查，**72%**的员工承认他们终端上的文档有敏感信息，**37%**的员工曾经偶然在同事终端上看到公司的保密信息（如员工薪酬/股权等信息）。

终端安全就是人的安全，不仅限于终端自身，也不能仅依靠终端安全软件

从滑动标尺模型看终端安全



目录

1. 概述
2. 终端安全运营成熟度提升
3. 基于EDR的终端防守
4. 多维数据在运营中的应用

CMMI成熟度模型

优化级

量化管理级

已定义级

已管理级

初始级

奇安信内部终端安全评价基础指标：

1. 安装率：确保终端安全软件覆盖
2. 实名率：终端出现问题时快速定位
3. 正常率：确保终端安全软件基础功能正常运行
4. 合规率：确保终端符合公司的终端安全基线

CMMI成熟度模型

优化级

量化管理级

已定义级

已管理级

初始级

每日由专员计算当天各项安全指标，并形成统计数据：

各位好，

以下是8月15日（周四）的指标数据：

安装率：97.35%

实名率：93.06%

正常率：93.94%

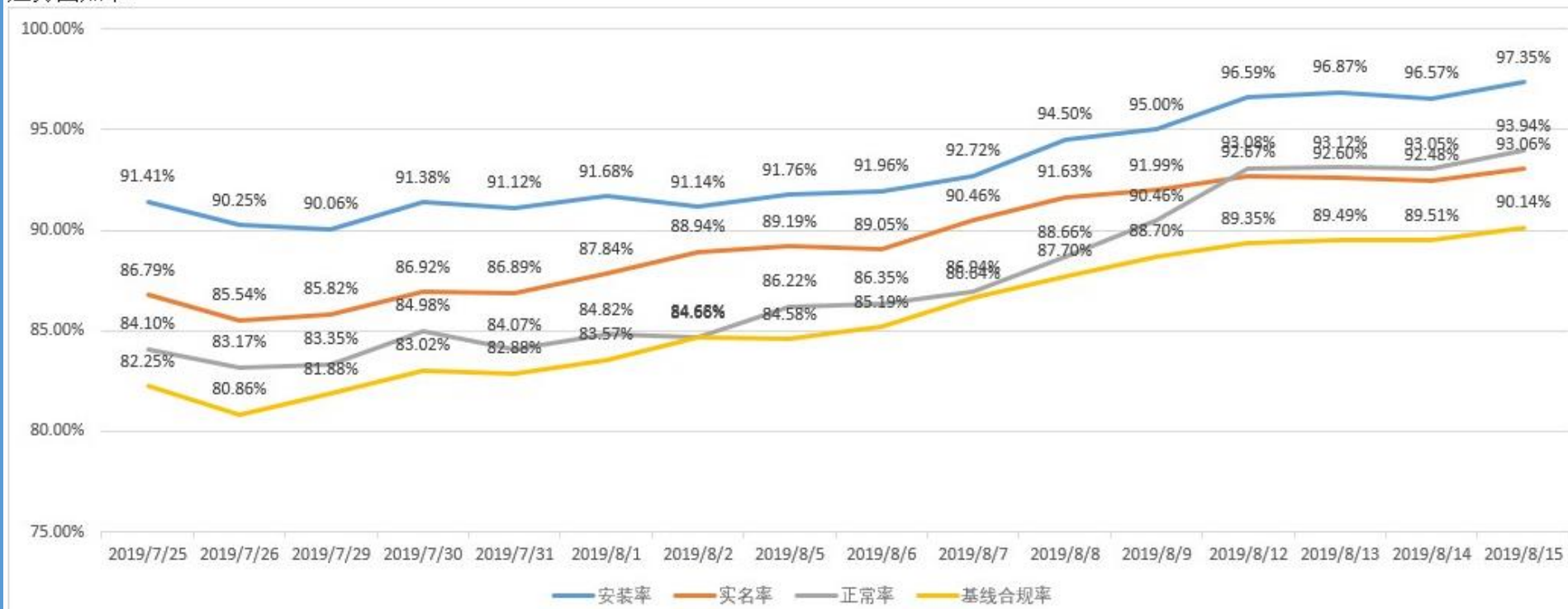
基线合规率：90.14%

CMMI成熟度模型

优化级

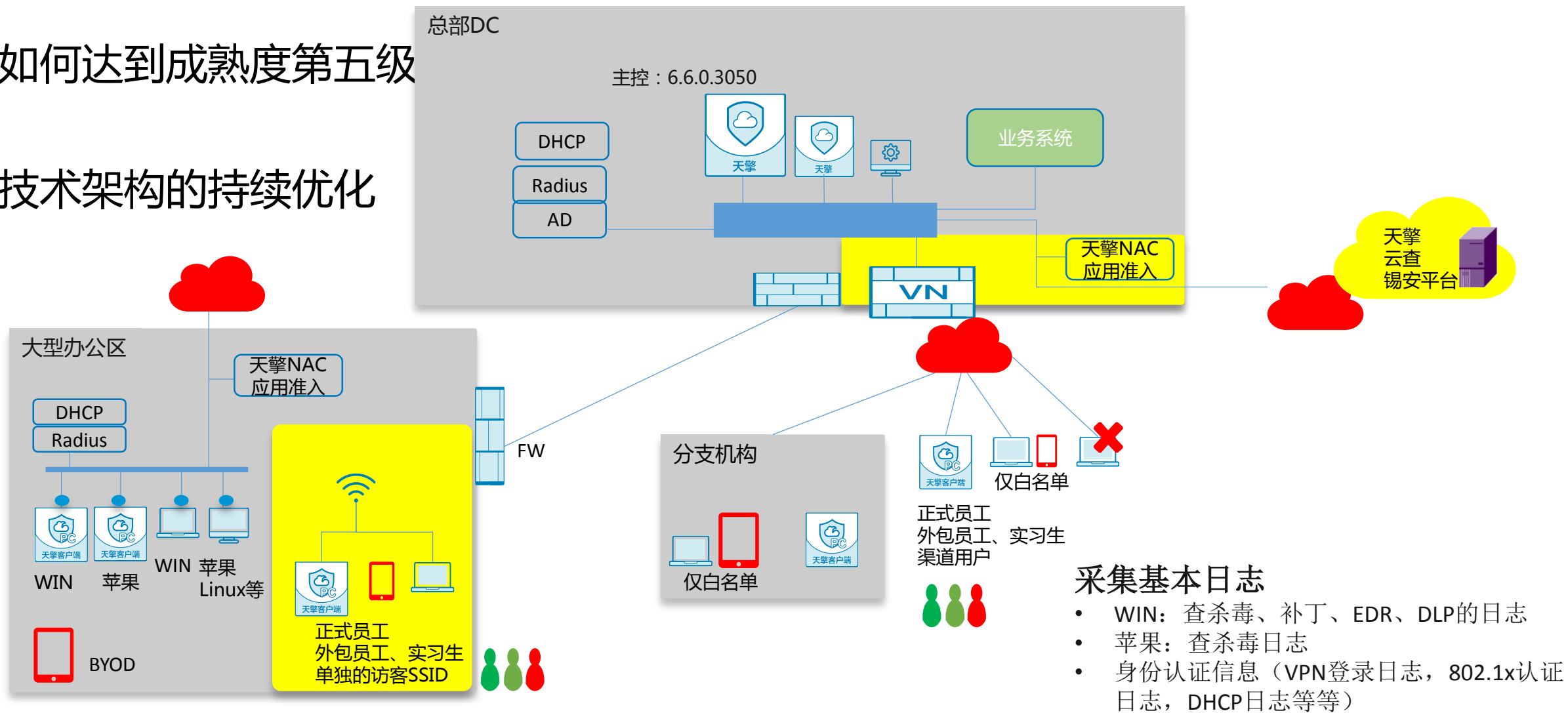
通过规章制度，流程改善，技术管控，安全运营来持续提升各项指标。

趋势图如下：



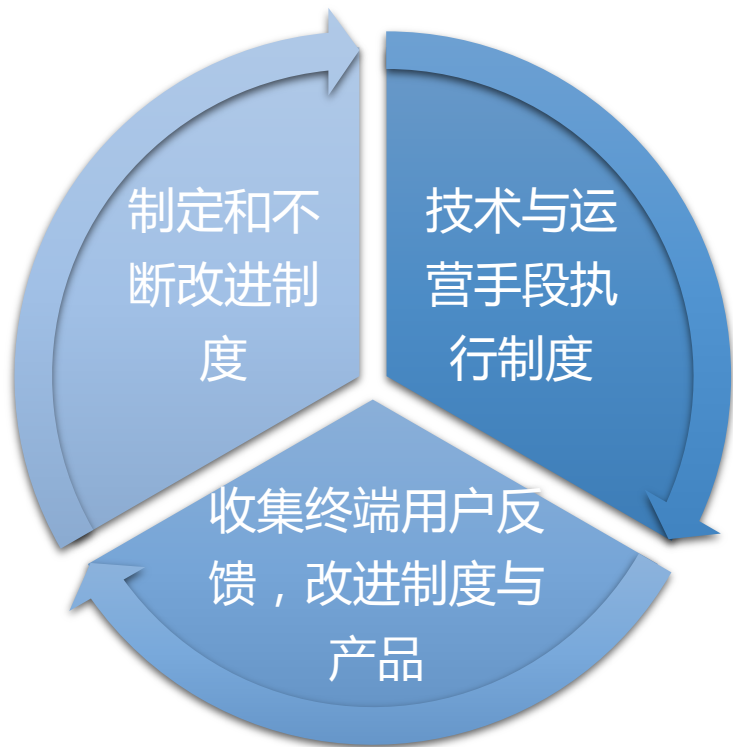
如何达到成熟度第五级

技术架构的持续优化



如何达到成熟度第五级：持续优化？

管理层面的持续优化



目录

1. 概述
2. 终端安全运营成熟度提升
3. 基于EDR的终端防守
4. 多维数据在运营中的应用

WHAT EDR ?

终端检测与响应（Endpoint Detection and Response，简称EDR）是一个用来持续检测与响应高级威胁的新型终端防御技术。EDR通常会在终端安装一个agent，将终端的各类日志回传至分析平台，供规则引擎和分析人员进行进一步的分析，检测，调查和统计。

WHY EDR ?

发现高级威胁.....



.....after all of this

In the end, it still runs on your computer.

A TRUE STORY

运营团队收到wmic白
利用告警，调查后发现
该终端从内网某服务器
拉取样本，注入到wmi
中运行，
创建svchost并挂起，
解密payload后注入到
svchost中继续运行

Use signed exec to load
a stageless payload. 常
见的避免杀毒软件主
动防御模块的方法。
Smart!

【SOC 报警】| 极高(10)| BF07| Windows| Windows 系统白文件利用| wmic ↵



2019/3/19 (周二) 16:09

网络安全部

【SOC报警】| 极高(10)| BF07| Windows| Windows系统白文件利用| wmic

收件人

如果显示此邮件的方式有问题，请单击此处以在 Web 浏览器中查看该邮件。

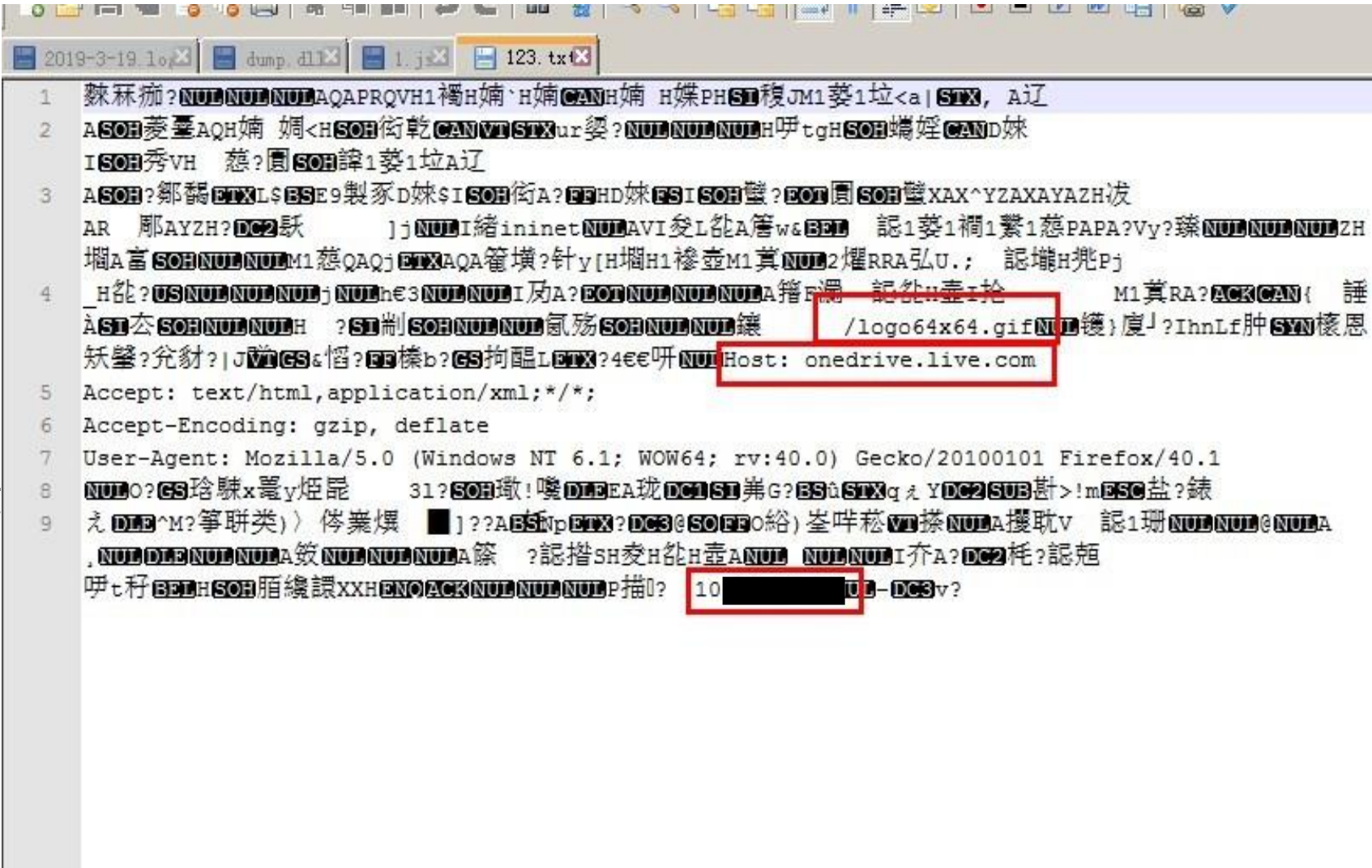
原始EDR触发的告警

【SOC报警】| 极高(10)| BF07| Windows| Windows系统白文件利用| wmic

名称	数值
设备记录时间	18 Mar 2019 19:45:33 CST
设备地址	
设备资产名称	天擎终端安全管理系统_172.24.0.99
设备所在网段	172.24.0.0_24
设备主机名称	NULL
设备管理人	
父进程名	c:/windows/sysnative/svchost.exe
父进程Hash	32569e403279b3fd2edb7ebd036273fa
子进程名	c:/windows/syswow64/wbem/wmic.exe
子进程Hash	79a01fcd1c8166c5642f37d1e0fb7ba8
命令行	C:/Windows/SysWOW64/wbem/WMIC.exe os get /format:"/scripts/1.xsl"
终端MID	5ff6369992f944f096f73ae5f2763db6

发现攻击者使用了 domain fronting 技术，防火墙，IDS看到的流量都是终端与 onedrive.live.com 进行通信，尝试下载一个gif。实际上...

Use white domain to relay transmit. 成功的规避开了IDS, IPS, 防火墙的检测和管控。



对样本进行分析

在沙箱分析，发现样本含反沙箱检测无法正常运行；二进制分析后，发现是CobaltStrike生成的免杀远控脚本。

规避沙箱分析

免杀样本生成，无特征码，内容混淆加密

```
C:\Users\Administrator\Desktop>wmic os get /format:"1.xml"
os get /format:"1.xml"Win7-2019TOLHYKroot\cimv2root\cliIMPERSONATEPKTPRIUACYms
804EN 样本回传信息，明显为远控信息 01Multiprocessor
FreeM ComputerSystemSe
rvice Pack 1Win7-2019TOLHYK480TRUETRUETRUE2FALSEFALSE256232760844193784745199620
190125125546.000000+48020190130114757.109999+48020190319184722.344000+4800804Mic
rosoft Corporation-18589934464zh-CNMicrosoft Windows 7 旗舰版 !C:\Windows!\Devic
e\Harddisk0\Partition10431164-bit205225618TRUE1Windows 用户00426-OEM-8992662-000
061041937840K272\Device\HarddiskVolume1C:\Windows\system32C:838569241937846.1.76
01C:\Windows
```


WITH EDR

天擎 EDR 相关查询信

hi.DST:C:\Wind

hi.SRC:C:\WIND

hi.SCL:-k netsvcs

hi.CLE:os get /fo

奇安信网神
终端安全管理系统

24小时内 process_name="wmic.exe" AND cmdline:"format*" AND cmdline:"esg.360es.cn/scripts*" 检索 筛选 历史

终端进程信息

过滤字段

- ☐ 分组名称
- ☒ 终端名称
- ☐ 终端MID
- ☐ 文件版本
- ☐ 产品版本
- ☐ 版本信息
- ☐ 进程描述
- ☒ 进程PID
- ☐ 产品名称
- ☒ 父进程PID
- ☒ 父进程路径
- ☒ 运行命令
- ☒ 进程路径
- ☐ 运行权限
- ☒ 进程状态
- ☒ 进程名称
- ☐ 进程MD5
- ☐ 公司名称
- ☐ 运行身份
- ☐ 原文件名
- ☐ 事件时间
- ☐ 程序签名
- ☐ 父进程MD5

通过EDR
日志发现
执行过该
有害脚本
的终端

终端进程信息-终端名称	终端进程信息-运行命令	统计数量
yanghaixia-A003849-NC01	C:\Windows\SysWOW64\wbem\WMIC.exe os get /format	> 40
	C:\Windows\SysWOW64\wbem\WMIC.exe os get /format	> 38
	C:\Windows\SysWOW64\wbem\WMIC.exe os get /format	> 38
	C:\Windows\SysWOW64\wbem\WMIC.exe os get /format	> 38
	C:\Windows\SysWOW64\wbem\WMIC.exe os get /format	> 38
	C:\Windows\SysWOW64\wbem\WMIC.exe os get /format	> 38
	C:\Windows\SysWOW64\wbem\WMIC.exe os get /format	> 38
	C:\Windows\SysWOW64\wbem\WMIC.exe os get /format	> 38
	C:\Windows\SysWOW64\wbem\WMIC.exe os get /format	> 36
	C:\Windows\SysWOW64\wbem\WMIC.exe os get /format	> 34
	C:\Windows\SysWOW64\wbem\WMIC.exe os get /format	> 30
	C:\Windows\SysWOW64\wbem\WMIC.exe os get /format	> 26
	C:\Windows\SysWOW64\wbem\WMIC.exe os get /format	> 26

In the end, it still runs on your computer.

WHY EDR

高级攻击快速检出

- 能监测MITRE ATT&CK 中大部分攻击
- 能有效补充常规安全设备防守不到的盲区

样本行为准确还原

- 准确记录终端的进程执行，子父进程关系，文件操作，IP访问等行为
- 通过hook底层API实现

影响范围快速确认

- 快速检索平台，基于各种关键字快速检索内部所有EDR日志，支持模糊搜索，全词搜索
- 样本->威胁情报（特征）
->快速定位失陷终端

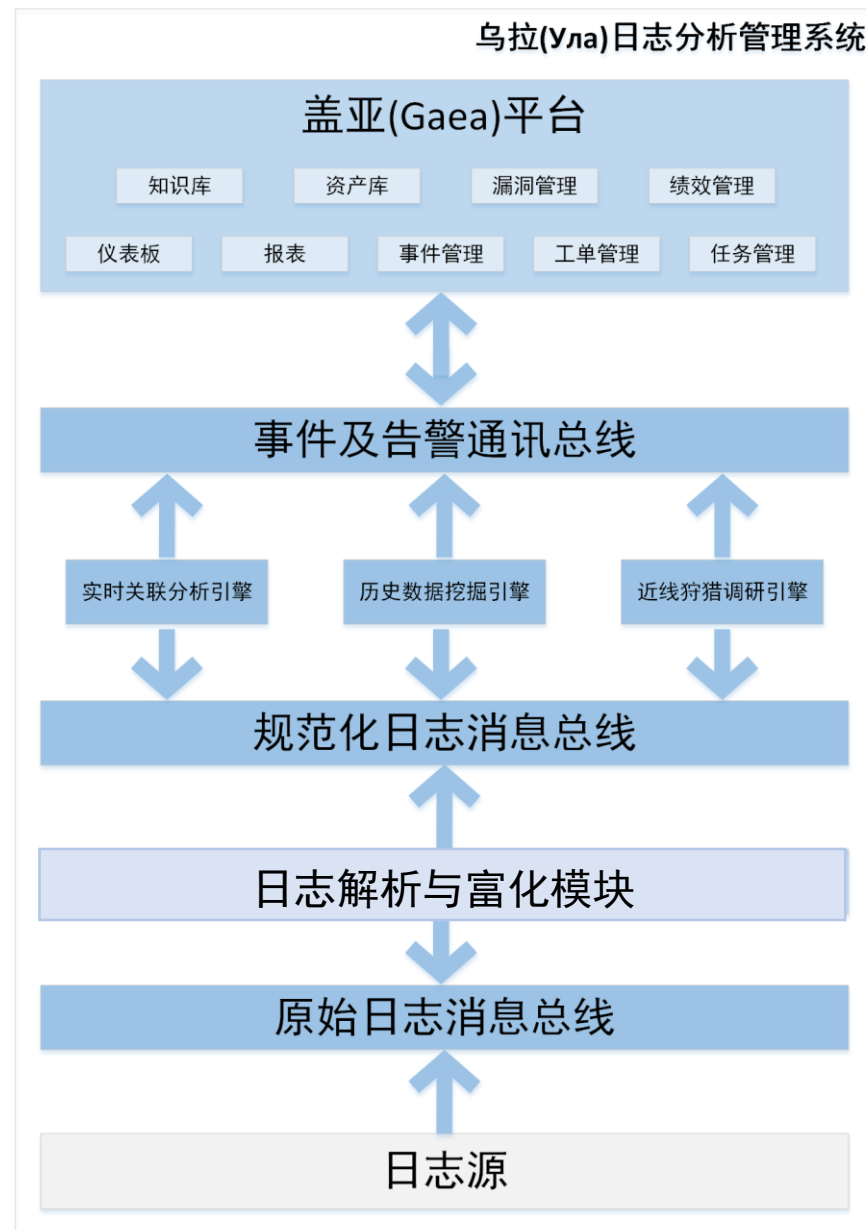
目录

1. 概述
2. 终端安全运营成熟度提升
3. 基于EDR的终端防守
4. 多维数据在运营中的应用

WITH EDR DATA
...AND MORE DATA!

乌拉日志分析管理系统

- 统一收集，解析奇安信集团内部系统日志，应用日志，安全系统日志与告警。
- 对日志进行三份处理
 - 实时关联分析引擎（使用Spark编写），实时处理日志输出告警。由安全部二线运营团队进行维护，和奇安信威胁情报中心等其他部门一起编写攻击检测规则，业务安全规则。
 - 近线狩猎调研引擎（ELK体系），存储热数据，供安全分析团队进行安全事件调查，攻击行为溯源。
 - 历史数据挖掘引擎（HDFS），存储冷数据，供建立模型，进行模式发现，机器学习。同时进行日志富化，模型计算，来发现用户异常行为。
- 将告警，异常输出到盖亚安全事件处理平台，进行后续的事件追踪等处理。



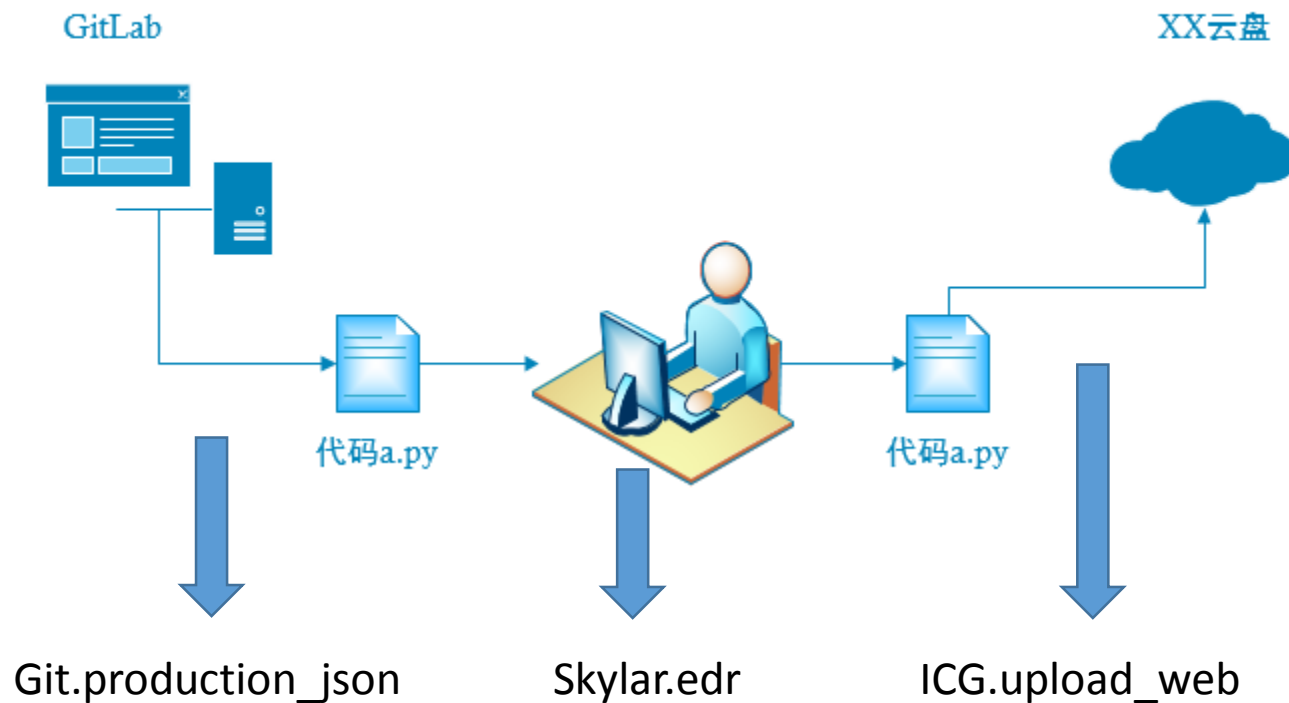
乌拉日志分析管理系统

- 支持Syslog，Beats系列输入
- 接入服务器与设备约1000台
- 平均EPS约1.5万，峰值EPS约4.4万
- 日志平均EPD约9亿，每天产出流量约1T

场景分析

一个常见的代码外泄场景：

- 行为散布在不同类型日志中，没有日志记录了完整过程
- 不同日志信息记录的信息都不完全
- 不同日志源对用户身份没有统一标识
- 不同日志源对于涉及数据没有统一标识
- 日志中描述的动作多样，难以使用统一规则对行为建模



Git.production_json:{1565183482458, git-upload-pack, wangming03, simple-python-demo.git}

Skylar.edr:{1565183482475, 文件操作审计, a6752aec22a54b2bb57351184deedcc5, 10.110.42.142, write, a.py, c:/users/wangming03/desktop, a88afc559fa07ad2bdfdc1bec433e14a, git.exe}

ICG.upload_web:{1565183484235, 文件外发审计, pan.baidu.com, 10.110.42.142, 111.206.37.70, 53345, 443 , c:/users/wangming03/desktop/a.py , 1kb}

数据富化（关联计算部分）——补全信息，统一标识

Git.production_json:{1565183482458, git-upload-pack, wangming03, simple-python-demo.git}

Skylar.edr:{1565183482475, 文件操作审计, a6752aec22a54b2bb57351184deedcc5, 10.110.42.142, write, a.py, c:/users/wangming03/desktop, a88afc559fa07ad2bdfdc1bec433e14a, git.exe}

ICG.upload_web:{1565183484235, 文件外发审计, pan.baidu.com, 10.110.42.142, 111.206.37.70, 53345, 443 , c:/users/wangming03/desktop/a.py , 1kb}



用户身份富化

Git.production_json:{1565183482458, git-upload-pack, **wangming03**, simple-python-demo.git}

Skylar.edr:{1565183482475, 文件操作审计, a6752aec22a54b2bb57351184deedcc5, 10.110.42.142, write, a.py, c:/users/wangming03/desktop, a88afc559fa07ad2bdfdc1bec433e14a, git.exe , **wangming03**} (由天擎ODP接口 , 查询mid后获得)

ICG.upload_web:{1565183484235, 文件外发审计, pan.baidu.com, 10.110.42.142, 111.206.37.70, 53345, 443 , c:/users/wangming03/desktop/a.py , 1kb , **wangming03**} (由sip+VPN日志联合查询得到身份)

数据富化（关联计算部分）——补全信息，统一标识

Git.production_json:{1565183482458, git-upload-pack, wangming03, simple-python-demo.git}

Skylar.edr:{1565183482475, 文件操作审计, a6752aec22a54b2bb57351184deedcc5, 10.110.42.142, write, a.py, c:/users/wangming03/desktop, a88afc559fa07ad2bdfdc1bec433e14a, git.exe, wangming03} (由天擎ODP接口, 查询mid后获得)

ICG.upload_web:{1565183484235, 文件外发审计, pan.baidu.com, 10.110.42.142, 111.206.37.70, 53345, 443, c:/users/wangming03/desktop/a.py, 1kb, wangming03} (由sip+VPN日志联合查询得到身份)

文件特征富化

Skylar.edr:{1565183482475, 文件操作审计, a6752aec22a54b2bb57351184deedcc5, 10.110.42.142, write, a.py, c:/users/wangming03/desktop, a88afc559fa07ad2bdfdc1bec433e14a, git.exe, wangming03, a88afc559fa07ad2bdfdc1bec433e14a} (文件md5)

Git.production_json:{1565183482458, git-upload-pack, wangming03, simple-python-demo.git, a88afc559fa07ad2bdfdc1bec433e14a} (关联相近timestamp, EDR)

ICG.upload_web:{1565183484235, 文件外发审计, pan.baidu.com, 10.110.42.142, 111.206.37.70, 53345, 443, c:/users/wangming03/desktop/a.py, 1kb, wangming03, a88afc559fa07ad2bdfdc1bec433e14a} (由文件路径在EDR路径中查询得文件hash)

数据富化（打TAG）—— 将复杂多样的信息模型化，用于规则检测或模式检测

行为类tag：

- 下载
Gitlab: git-upload-pack
Jowto: curl
Jowto: wget
Linux: curl
Linux: wget
Windows: downString
ICG: 文件下载审计
EDLP: 文件下载审计
Nginx: GET end with file extension
- 上传
Gitlab: git-download-pack
ICG: 文件上传审计
ICG: IM外发审计
EDR: 邮件附件审计
.....

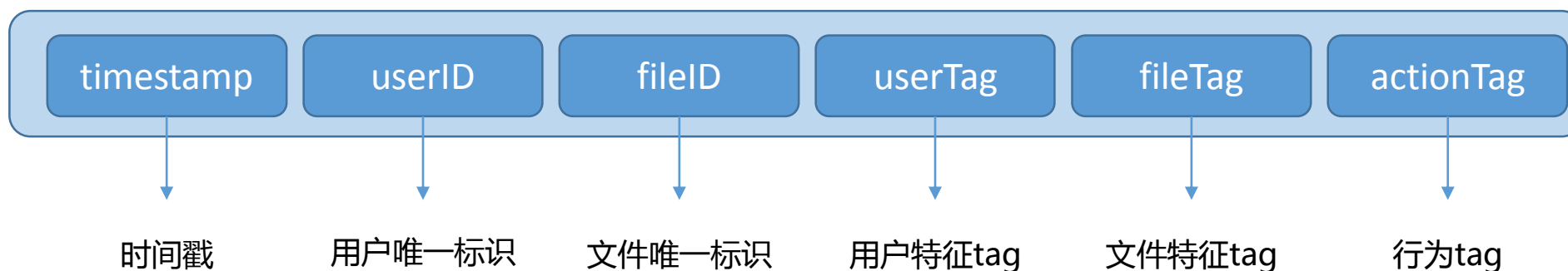
人员类tag

- 部门（LDAP数据）
人力资源部
财务管理部
研发一部
研发二部
销售一部
销售二部
.....
- 部门类型
研发部门
服务部门
管理部门
职能部门
.....
- 其他信息
如正在办理离职中
.....

文件类tag：(依托DLP引擎)

- 研发类数据
 - 源代码
 - 项目文档
 - 产品文档
 - 运行数据
 - 测试结果
 - 配置用信息
 - ...
- 人力类数据
 - 人员基本信息
 - 人员敏感信息
 - 组织架构信息
 - 人员薪酬信息
 - ...
- 财务类数据
.....

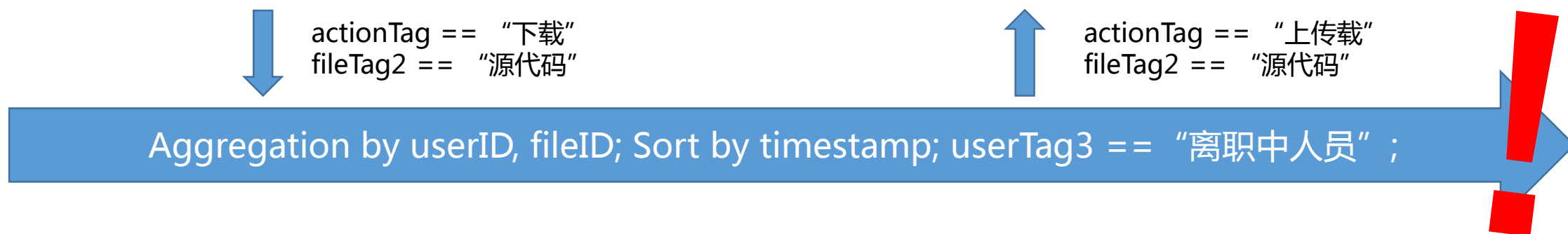
转换为行为帧 —— 格式统一化，并将复杂日志抽象为人的一个行为



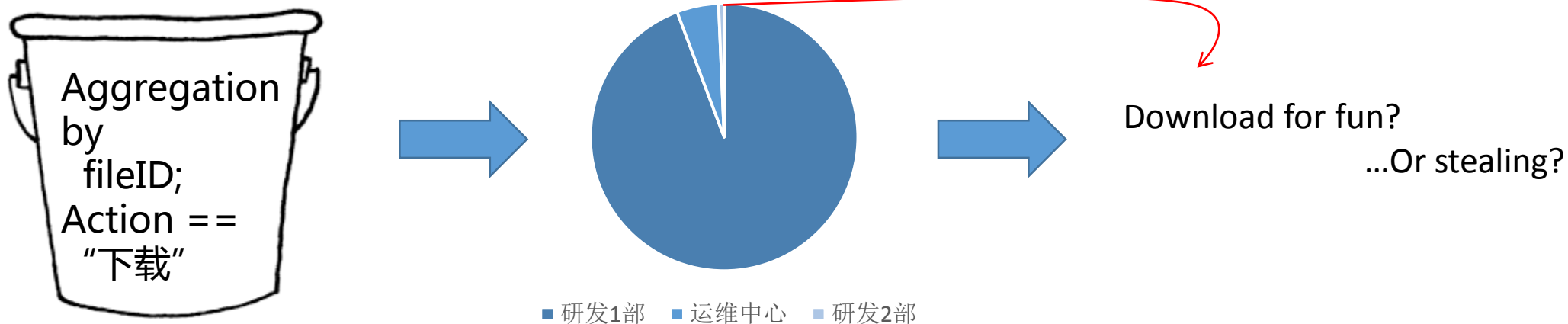
Git.production_json:{1565183482458, git-upload-pack, wangming03, simple-python-demo.git , fb87f1ae6059c052f196a8cdd3483669, “人员tag1”: “研发3部”, “人员tag2”: “研发部门”, “人员tag3”: “离职中人员”, “文件tag1”: “研发类数据”, “文件tag2”: “源代码”, “行为tag”: “下载”}




行为帧序列规则告警



行为“离群”模型告警





THANKS

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE