19th Asian Games Hangzhou 2022

杭州2022年第19届亚运会官方合作伙伴

Official Prestige Partner of the 19th Asian Games Hangzhou 2022

重保运营，是时候用MSS了

安恒信息 杨勃

2022年6月

www.dbappsecurity.com.cn 400-6059-110

实战化倒逼安全建设转向持续有效安全运营

01 从合规建设到实战化建设

- 安全合规是底线、是红线，但已难以应对当前复杂的网络安全形势

02 安全设备价值如何发挥

- 当前高校用户基本上安全设备已经齐全，面对持续迭代升级的安全设备，如何真正的发挥设备价值成为了一个难题

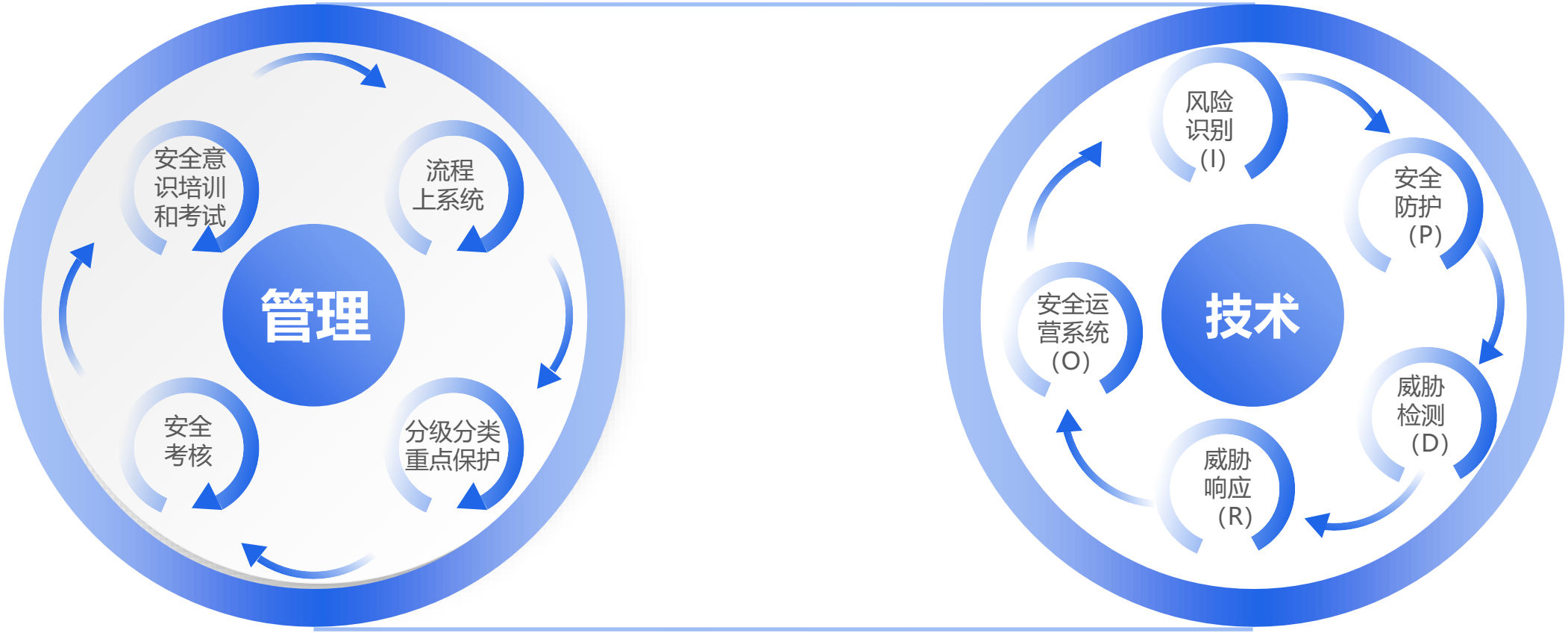
03 安全人才相对稀缺

- 网络安全工作一般由老师兼职
- 建制完备安全运营团队通常由5人组成，人工成本和管理成本学校难以承受

04 缺乏运营建设经验

- 安全运营工作落地成为难题，有设备难发挥价值，有制度难落地，安全工作零碎难以形成体系

管理指明方向，并解决技术无法解决的难题



技术促进管理制度有效落地

我们对网络安全工作中管理的几点思考

要做好网络安全意识宣传和培训工作

要得到领导层对网络安全工作的支持

要制度与管理办法，但**一定要有在线流程落地**

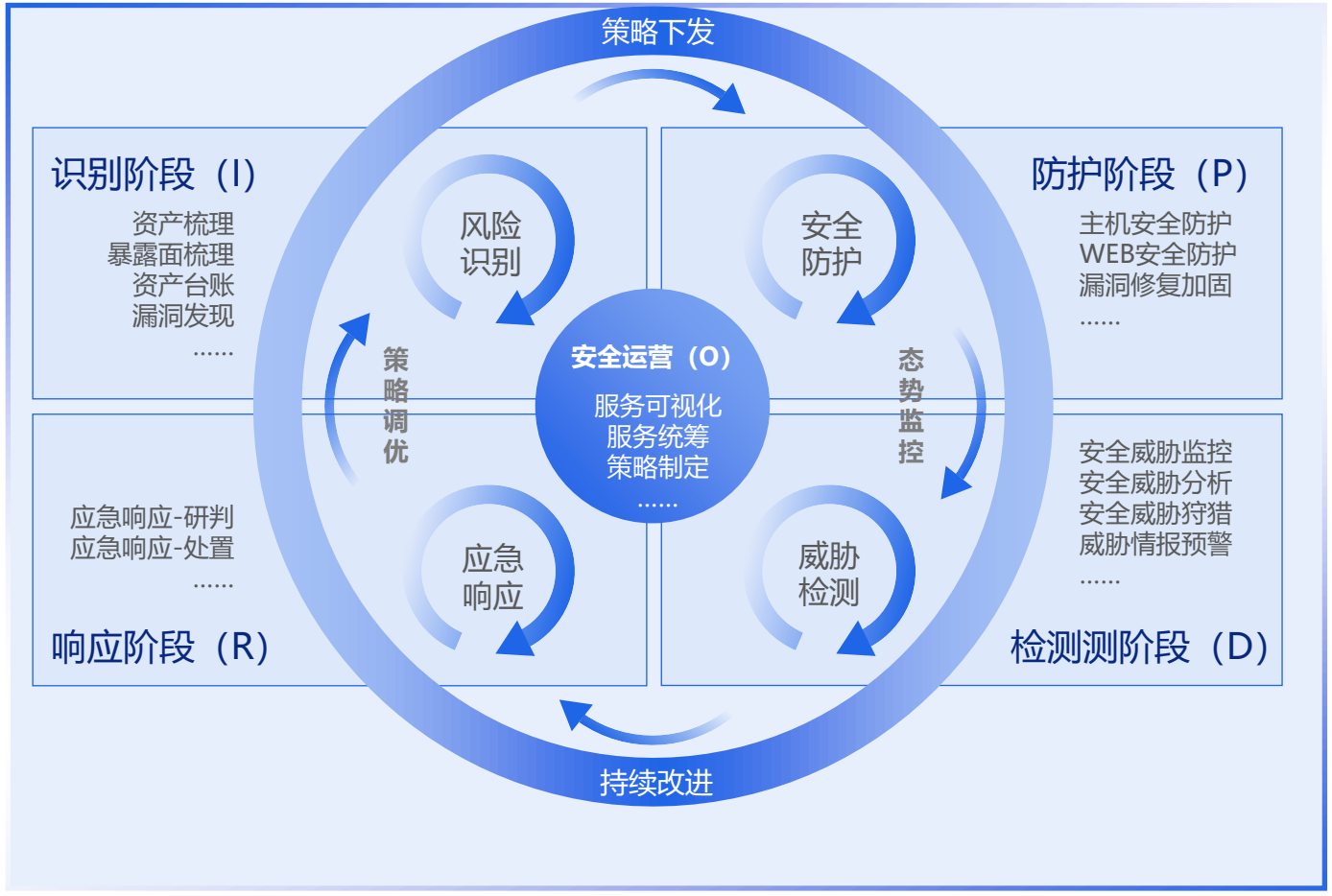
要做好**资产分级分类，落实重点资产重点保护**

要做好风险和事件分级，**实现动态清零**

要做好安全考核，以考促进各组织共同参与学校网络安全建设

以IPDRO的技术框架结合管理制度落地安全运营

IPDRO安全运营技术框架



管理制度

识别阶段

- 制定资产分级规则，重点资产重点保护
- 制定漏洞分级规则，聚焦重点
- 制定攻击面管理规则，减轻工作

防护阶段

- 制定防护设备维护规则
- 制定重点资产的防护链的规则

检测与响应阶段

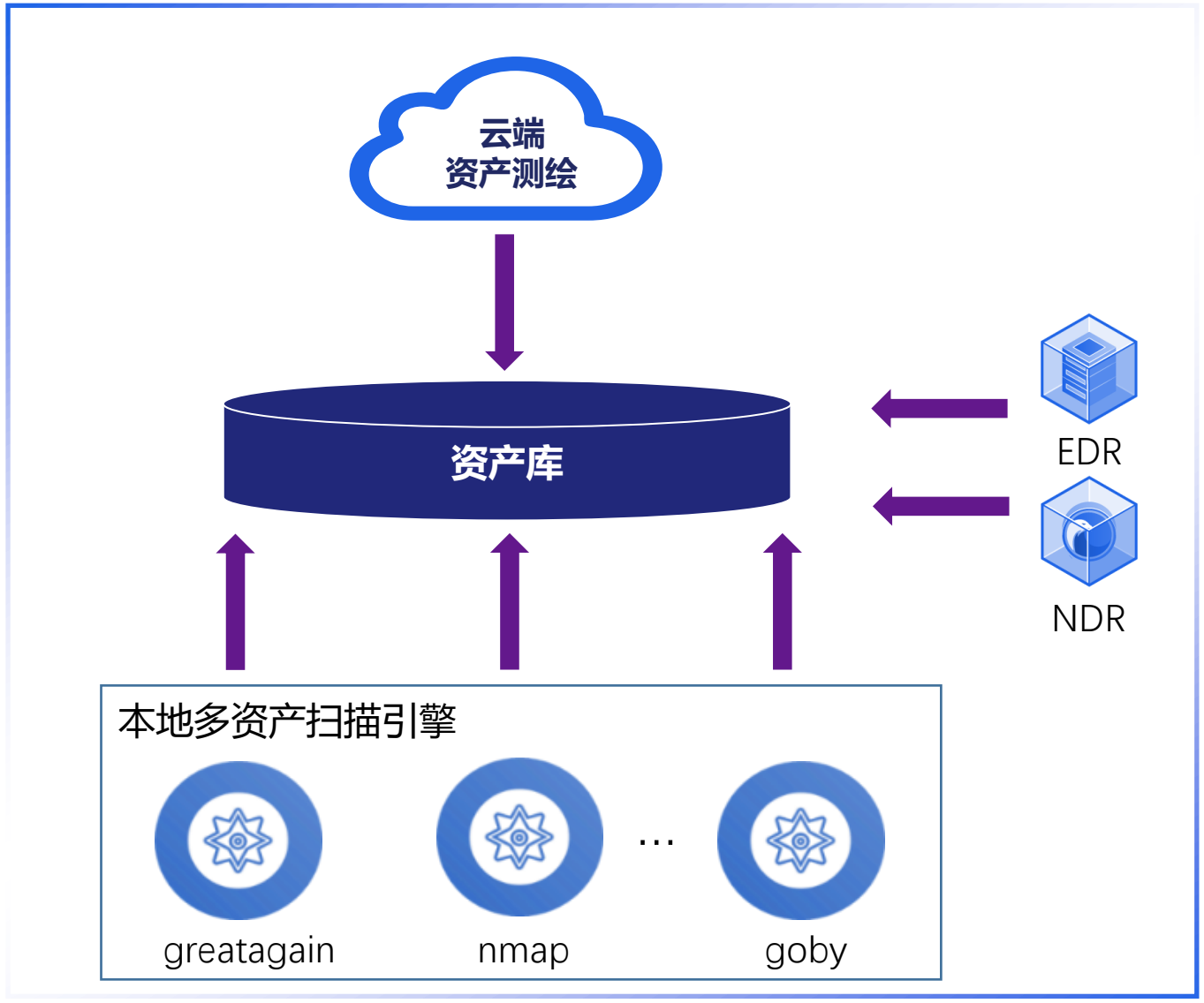
- 制定事件定级规则
- 制定威胁响应制度，紧急事件立马办，重要事件当天办

安全运营阶段

- 以PDCA原则持续优化制度与流程
- 坚持风险与威胁动态清零原则

做好资产管理是做安全运营的第一步（1/3）

从技术上做好资产探测是做好资产管理的前提



01

云端资产测绘

要通过云端资产测绘发现互联网暴露面资产。

02

本地资产扫描

本地多资产扫描引擎完成对内网资产的发现。

03

通过NDR+EDR获取资产

通过NDR从流量中提取资产信息，通过安装EDR获取安装agent的资产。

04

资产统一数据输出

云端资产测绘数据、本地资产扫描数据、NDR+EDR获取资产汇总到资产库中，进行统一的清洗和输出，形成统一格式的数字资产。

做好资产管理是做安全运营的第一步（2/3）

管理制度	对比校验	人员梳理	初步资产台账
制定制度要求二级学院等其他组织主动上报资产，说明用途。	将技术手段获取的资产与上报的资产进行对比校验。	结合用户组织和人员的梳理，将**资产与组织和人员关联**起来	■资产跟着部门走、风险跟着资产走。 ■发现风险或安全事件后，能够找得到人，找得对人。

做好资产管理是做安全运营的第一步（3/3）

通过管理手段完成资产分级，结合先前资产台账形成最终资产台账，同时资产台账要动态定期更新。

资产分级四要素

01 是否等保备案

02 是否暴露面

03 系统访问量

04 是否核心系统

资产分级示例

资产分类	资产重要性
DMZ区核心业务	核心资产
DMZ区非核心业务	重要资产
办公网段	一般资产
测试网段	一般资产

资产属性示例

资产名称	资产IP	资产级别	归属安全域	资产类型	等保信息	服务开放情况	授权访问对象	IT维护负责人	业务责任人	安全防护链

做好漏洞管理同样也需管理与技术的结合（1/3）

已知漏洞管理五个动作

要工具	要人	要在线流程	要管理制度	要人
➢ 全量漏洞扫描	➢ 漏洞结果验证	➢ 通告并提供建议	➢ 漏洞整改修复	➢ 复测&关闭问题
• 需要扫描的快 • 需要扫描的准	• 需要安全专家对漏洞扫描结果做人工验证	• 需要在线流程直接通告給资产最终责任人，高效	• 需要安全考核制度提升组织对漏洞整改的积极性	• 需要安全专家对漏洞进行复测，并关闭问题。

同时需要系统看到漏洞趋势，历史整改情况，整改时长等，提升漏洞管理水平

做好漏洞管理同样也需管理与技术的结合（2/3）

0day漏洞管理五个动作

要工具	要人	要在线流程	要管理制度	要人
➢ 漏洞情报	➢ 匹配资产信息	➢ 通告并提供建议	➢ 漏洞整改修复	➢ 复测&关闭问题
• 需要准确漏洞情报	• 需要将漏洞信息与资产库属性进行匹配，扫描出哪些资产受影响	• 需要在线流程直接通告給资产最终责任人，高效	• 需要安全考核制度提升组织对漏洞整改的积极性	• 需要安全专家对漏洞进行复测，并关闭问题。

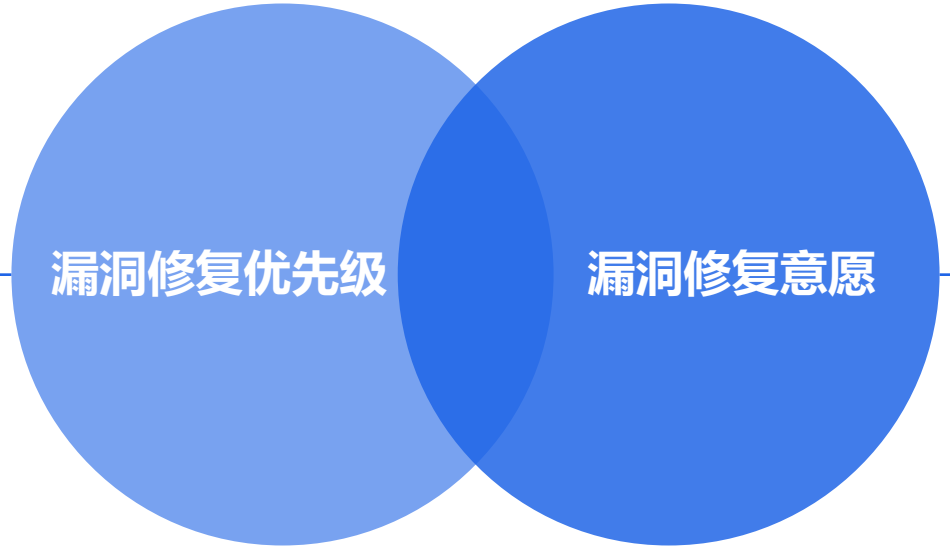
做好漏洞管理同样也需管理与技术的结合（3/3）

总结做好漏洞管理两个关键点

如何定义漏洞优先级

- 资产重要性
- 是否有EXP
- 是否有暴露面
- 利用复杂度
- 漏洞后果
- 披露时间
- 风险等级

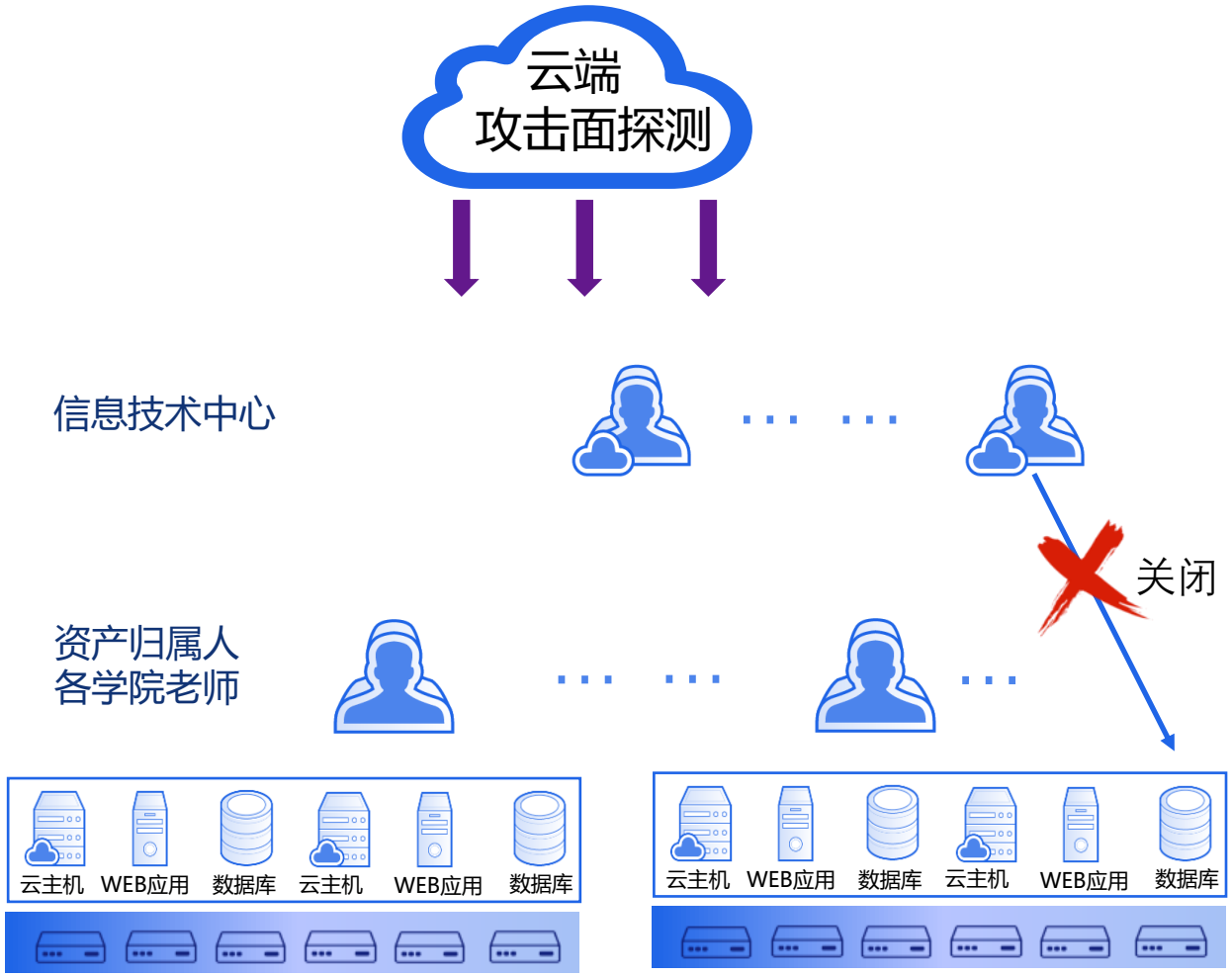
应该通过这些综合因素一起判断，给出资产漏洞的优先级，优先级高的立马修复。



如何让其他组织积极修复漏洞

- 安全考核管理制度，让学校其他组织共同参与进来进行安全建设，提升修复整改漏洞的积极性
- 需要在线系统可以量化各组织修复漏洞的数据，比如修复周期，剩余漏洞数等

日常做好攻击面治理，重保前从容应对



通过与资产上报情况，并与资产责任人进行沟通，当资产不应该有暴露面的应该关闭对外端口。

01

周期性攻击面探测

发现攻击面信息，至少包含IP、端口、中间件等其他资产指纹信息

02

确认服务对外必要性

根据资产责任人上报的资产信息结合攻击面的探测信息，沟通对外必要性。如无必须关闭对外服务。

03

出现影子资产先关停

出现没有责任人的资产，先关停。

04

结合漏洞和攻击面分析

结合漏洞优先级，漏洞优先级高的资产要优先关闭对外服务，或者上防护手段。

通过管理手段用好安全防护设备

定期更新规则库

- 形成定期更新安全防护设备的规则库的保障制度
- 形成定期删除无效配置的保障制度

拓扑图真实反映网络架构

- 要好持续更新的拓扑图真实反应安全保护设备的位置

安全防护链与重要资产相关联

- 重要的资产需要知道经过了哪些安全设备的防护，明确是否上了安全策略

聚焦核心矛盾，对威胁实现动态清零（1/2）

安全事件的定级是动态清零前提，将安全事件严重性与资产重要性关联，输出事件定级标准。

事件定级示例

序号	事件类型	资产类型	安全事件定级
1	web攻击/Webshell上传	**重要资产**	**紧急**
2	web攻击/文件上传	重要资产	紧急
3	web攻击/越权访问	重要资产	紧急
4	横向移动/远程执行	重要资产	紧急
5	web攻击/Webshell上传	**一般资产**	**重要**
6	web攻击/文件上传	一般资产	重要
7	web攻击/信息泄露	重要资产	重要
8	web攻击/远程代码执行	重要资产	重要
9	web攻击/越权访问	一般资产	重要
10	恶意程序/僵尸网络	重要资产	重要
11	恶意程序/挖矿软件	重要资产	重要
12	横向移动/远程执行	一般资产	重要

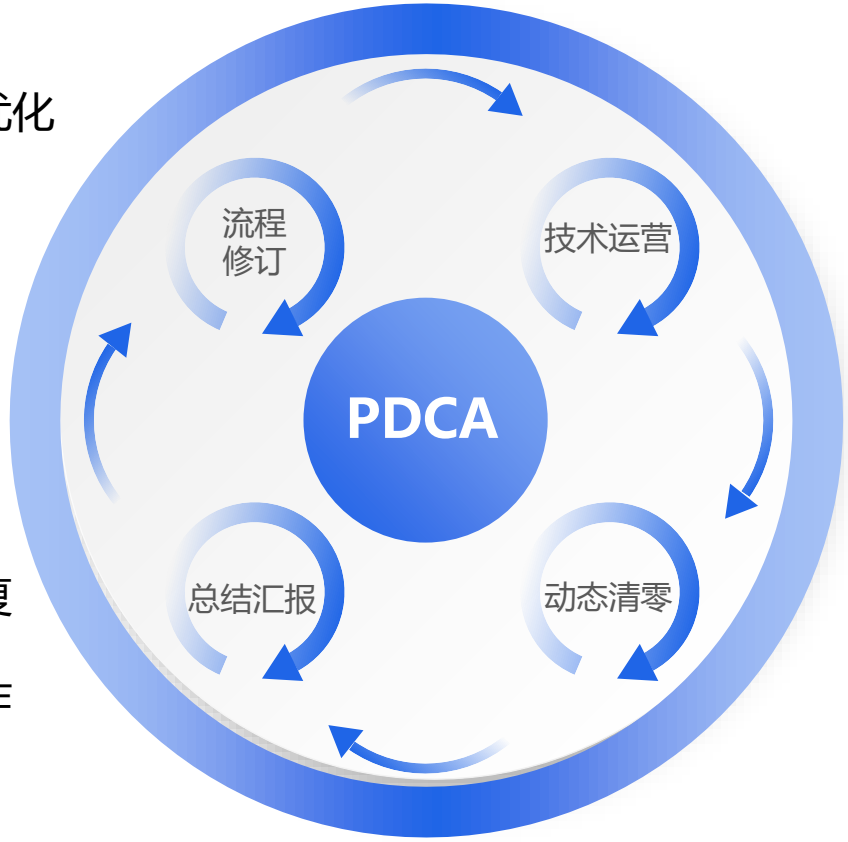
聚焦核心矛盾，对威胁实现动态清零（2/2）

马上办　　当天办　　周期性闭环

以PDCA为原则不断优化安全运营流程

■ 结合实际的安全运营效果，动态优化资产分类、事件定级、响应流程等

■ 每个季度对运营成果和问题进行复盘，明确后续工作计划
■ 对领导层进行工作汇报，展示工作成果获得网络安全工作的支持



■ 持续做好定期资产管理、漏洞管理、攻击面治理
■ 持续做好威胁检测与响应

■ 动态清零是根据资产分类、事件定级的最佳实践，紧急威胁和漏洞当日闭环，重要威胁和漏洞周内闭环，一般威胁和漏洞季度闭环

不定期的安全演练是检验安全运营效果的手段

通过实际攻防或者不定期安全演练检验安全运营效果

反挖矿演练

演练流程：

1. 靶场环境模拟该场景下内网挖矿行为；
2. 安全设备检测挖矿流量采集后平台进行分析，按照资产分类，定义为重要或一般事件；
3. 业务责任人进行事件响应处置，信息中心老师进行协助处置；
4. 处置完成，信息中心老师确认风险消除，在系统上结束事件；

反勒索演练

演练流程：

1. 靶场环境模拟该场景下勒索病毒行为；
2. 安全设备检测勒索病毒行为流量采集后平台进行分析，按照资产分类，定义为紧急或重要事件；
3. 业务责任人进行事件响应处置，信息中心老师进行协助处置；
4. 处置完成，信息中心老师确认风险消除，在系统上结束事件；

重保演练

演练流程：

1. 靶场环境模拟该场景下口令爆破行为；
2. 安全设备检测攻击流量采集后平台进行分析，按照资产分类，定义为重要或一般事件；
3. 业务责任人进行事件响应处置，信息中心老师进行协助处置；
4. 处置完成，信息中心老师确认风险消除，在系统上结束事件；

除了管理与技术，人是安全运营的关键

在安全运营的工作中，人是安全运营的关键。

01.资产测绘

需要人将各种工具探测的资产进行去重分析处理

02.漏洞验证

将工具扫描的结果需要人工验证

06.应急响应

需要人对紧急安全事件进行应急响应

03.协助漏洞整改

需要人协助资产责任人进行漏洞整改

05.威胁研判

需要人对告警事件进行研判，确认是否是真实安全事件

04.攻击面治理

需要人结合漏洞优先级分析与暴露面指纹信息综合分析攻击面影响

除人的问题，还有不少问题让安全运营落地困难

安恒信息针对“管理、技术和人”的诸多问题，推出安全托管运营服务。

- 五分钟完成托管服务接入
- 云端专家7*24h持续守护
- 风险和威胁动态清零
- 安全数据和安全运营流程不出校，保障数据安全
- 充分利用云端安全算力和各种安全数据，如漏洞情报、威胁情报。

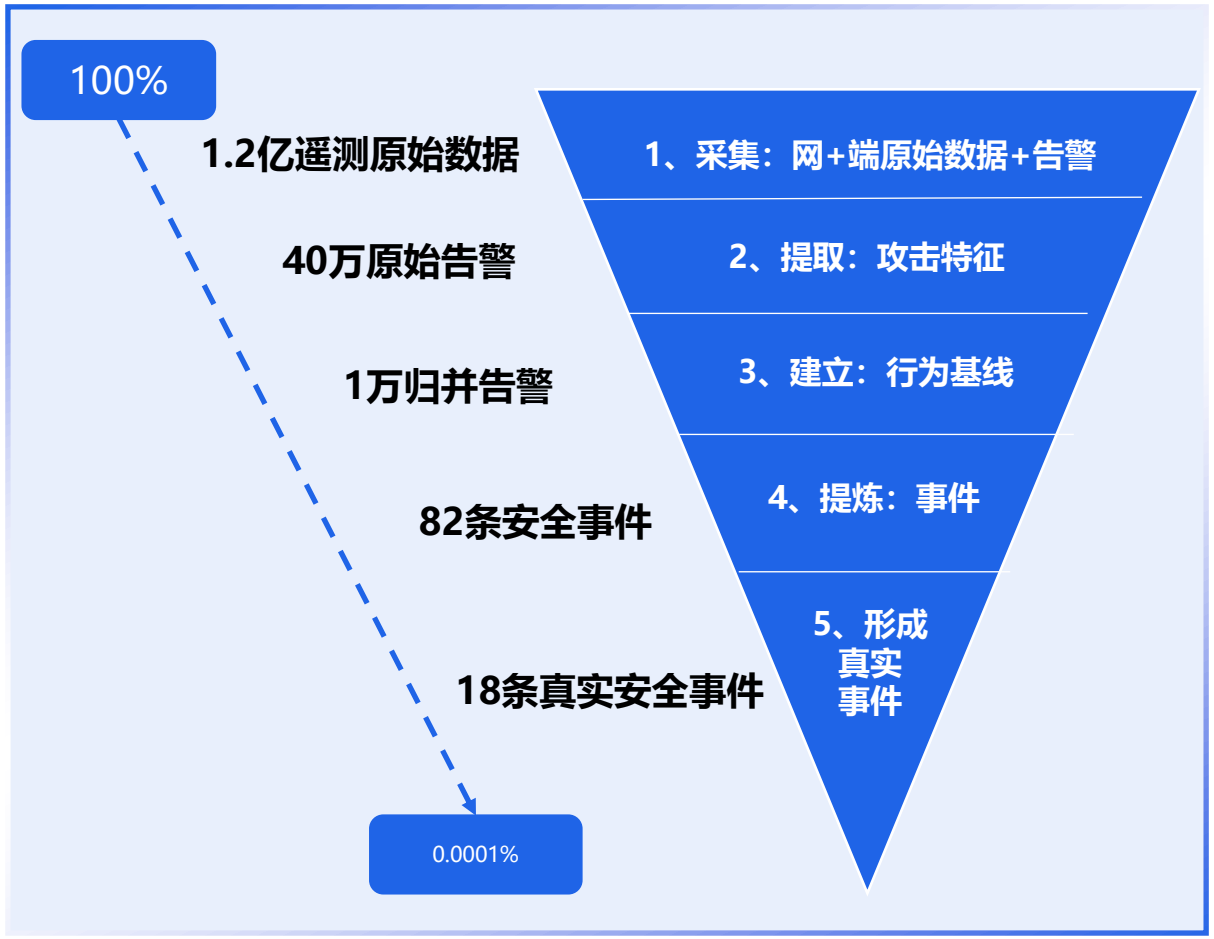
做好安全运营服务三个关键技术（1/3）

全方位采集攻击信息不遗漏

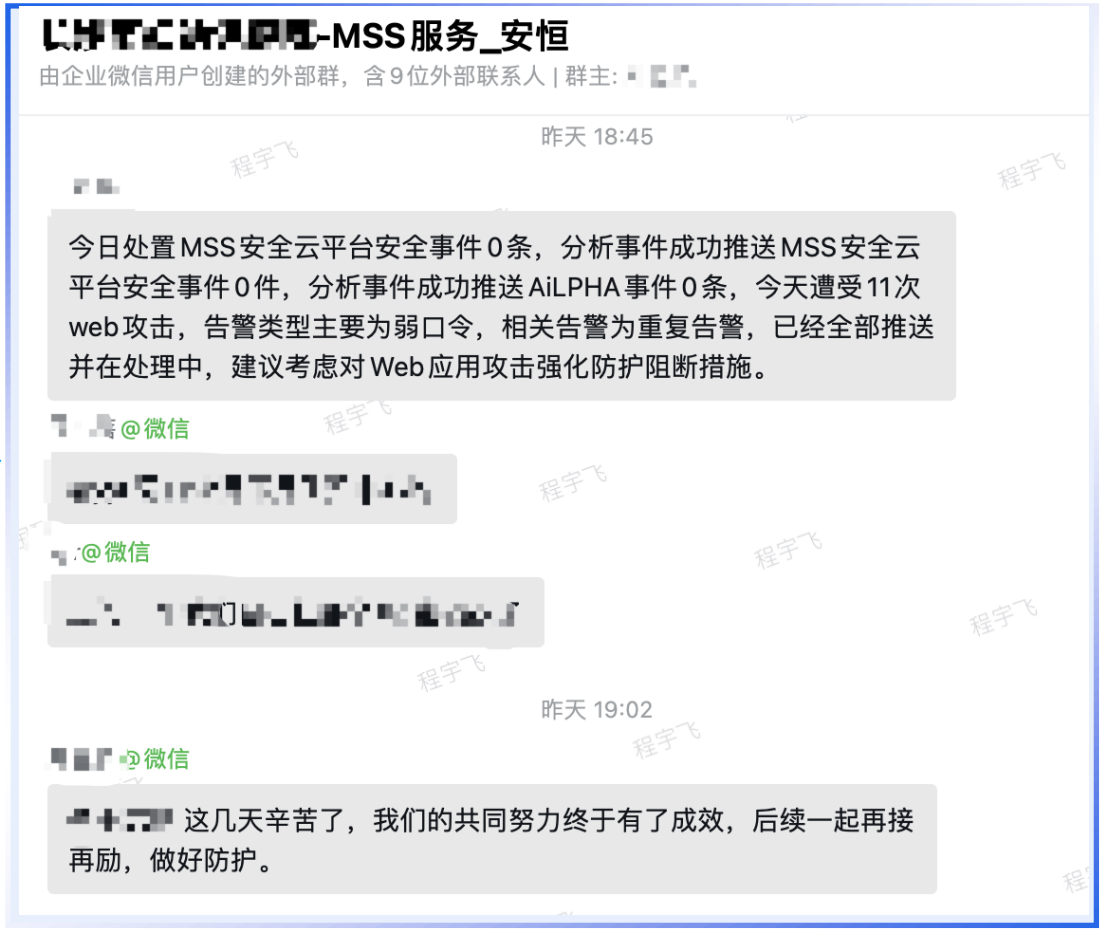
采集能力涵盖ATT&CK中331项中的187项，TTP高覆盖

做好安全运营服务三个关键技术（2/3）

海量告警降噪、锁定真实攻击



安全运营常态化≠ 常态化告警
不为用户带来告警焦虑



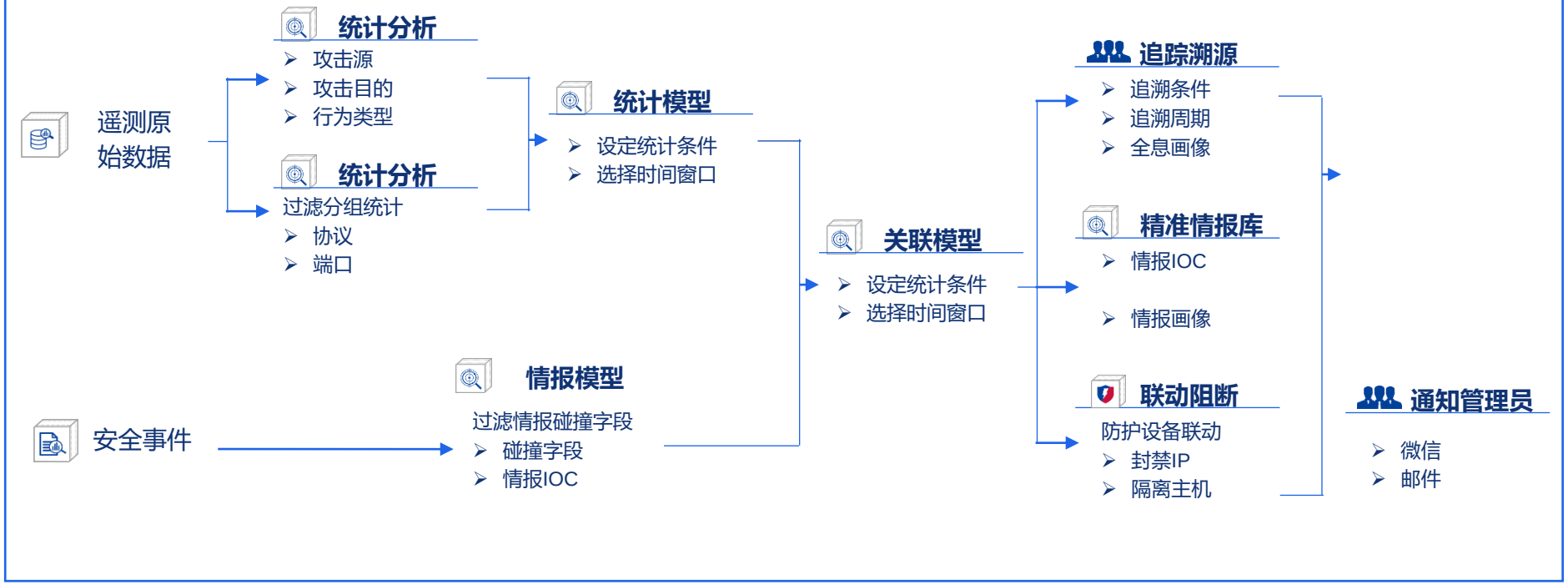
做好安全运营服务三个关键技术（3/3）

丰富UseCase+SOAR是关键

安全要素

- 安全原始数据
- Usecase模版
- 威胁分析能力
- 威胁阻断能力
- 服务专家研判

UseCase提炼与规范化处置示意



有丰富Usecase，当出Usecase库中事件时，调用安全工具实现自动化响应处置，如封禁IP、隔离主机等

三级运营人员紧密协同，打造高级专家运营团队

安全研究专家
（名医团队会诊）

- 安全研究
- 情报专家

云端安全专家
（门诊专家7*24h坐诊）

- CSIRT
- 漏洞管理组
- 分析研判组
- 威胁处置组
- 威胁监测组
- 应急响应组

一线安全运营经理
（家庭医生贴身健康管理）

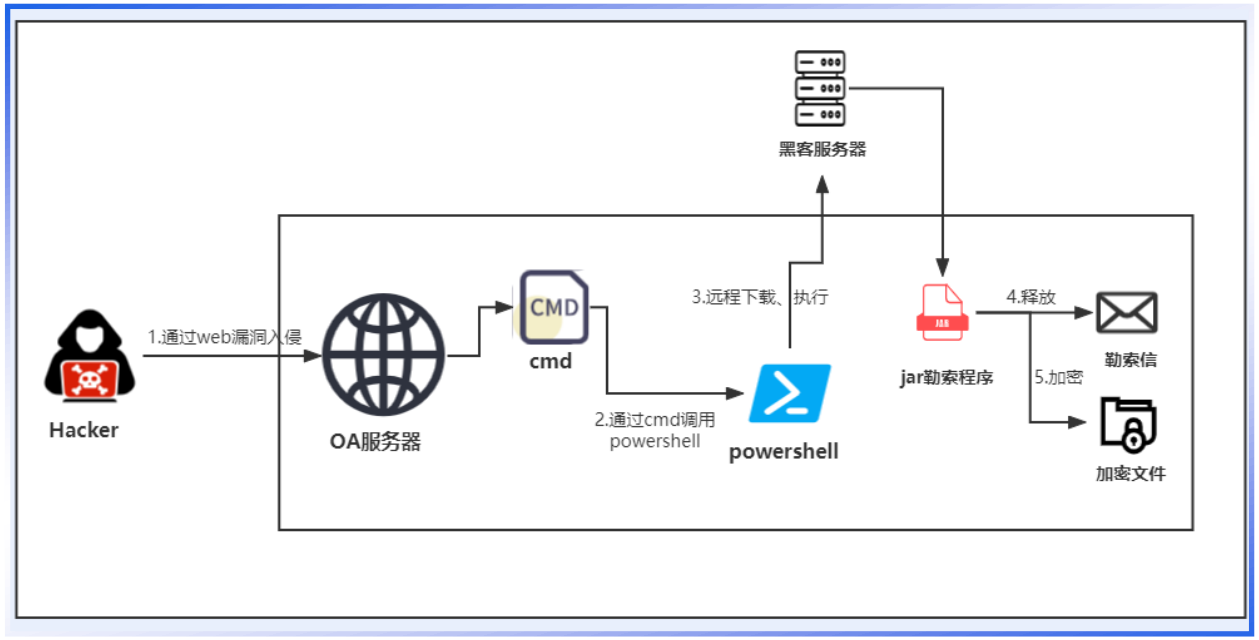
- 安全运营经理
- 现场安全服务

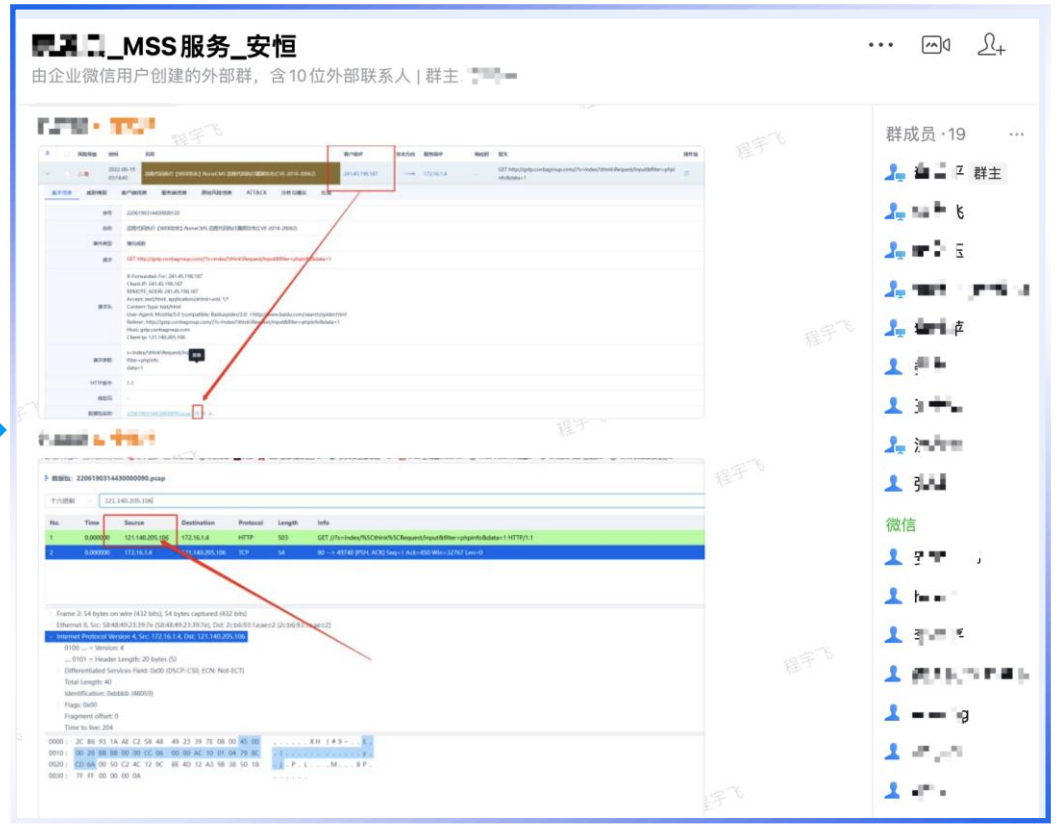
聚焦核心矛盾，帮助高校用户对威胁实现动态清零

安恒信息 DAS-Security 安全中国 | 数字经济的安全基石 The security cornerstone of the digital economy

网络安全工作井然有序

高校老师只需要将精力投入到关键的安全事件中实现各类风险和威胁的“动态清零”





13：58
云端运营专家通知用户

14：00
开启应急响应

14：05
攻击阻断

14：10
溯源分析

14：50
完成溯源 找到秘钥

服务指标度量 效果看得见 用户可感知

为高校提供全程监测、精准预警、主动服务、快速响应、闭环管理的安全托管运营服务

平均响应时长

< 5min

重大事件闭环率

100%

重大事件平均处置时长

< 1H

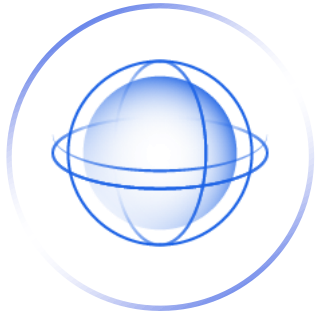
0day漏洞预警时长

< 24H

一般事件平均处置时长

< 2H

安全托管运营服务对学校安全运营的价值



资产台账清晰可视

理清学校网络中现有数字资产，并建立资产管理流程，减少资产暴露面；同时建立资产与资产责任人对应关系，责任到人，便于资产管理

7*24H主动化服务

7*24小时安全值守服务，协助学校持续了解单位当前网络安全动态，第一时间协助学校处置各类安全事件如被通报、外部恶意攻击等

风险和事件动态清零

安全专家持续对学校网络安全进行监控，协助学校动态调整防护策略，紧急风险和事件当天办、一般风险和事件周期性闭环

安全运营流程标准化

安全运营专家协助学校将资产发现、漏洞扫描、漏洞整改、安全通报、应急响应等安全流程规范化，打磨出适合学校自身的流程管理体系，让学校能从容应对各类安全事件

19th Asian Games Hangzhou 2022

杭州2022年第19届亚运会官方合作伙伴
Official Prestige Partner of the 19th Asian Games Hangzhou 2022

联系我们

Contact Us

浙江省杭州市滨江区西兴街道联慧街188号安恒大厦
www.dbappsecurity.com.cn
400-6059-110

安恒信息官方服务号
网安人的干货充电站