掌数
PAMADATA

智能安全运维解决方案

PART 01

我看到的痛点

The Difficult Problem

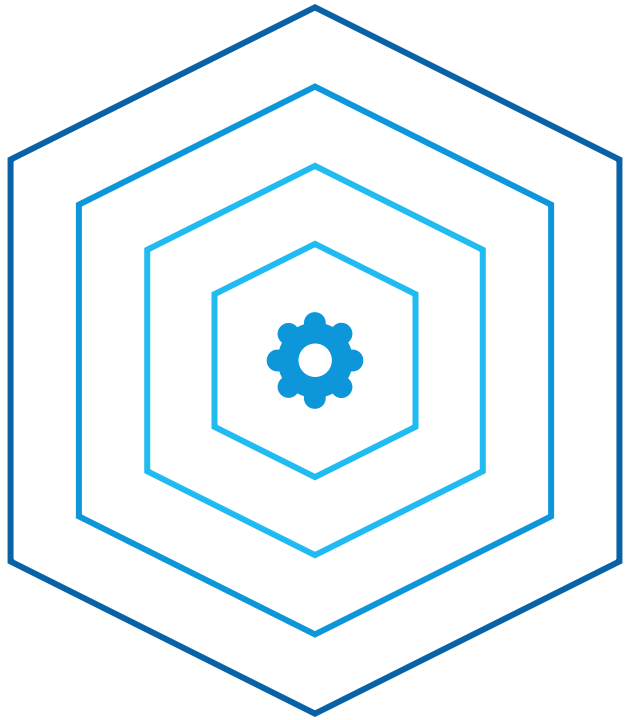
安全能力失效的根源是什么？

生活中安全能力失效的场景

带来安全能力失效的几个问题

无法闭环安全事件

安全事件无法定位，系统更新频繁无法定位资产，运维或安全部门背锅。



安全产品使用效率较低

当安全产品数量超过用户安全团队的运维能力时，安全管理面临着极大的挑战，安全工作效率会伴随产品增加而降低。

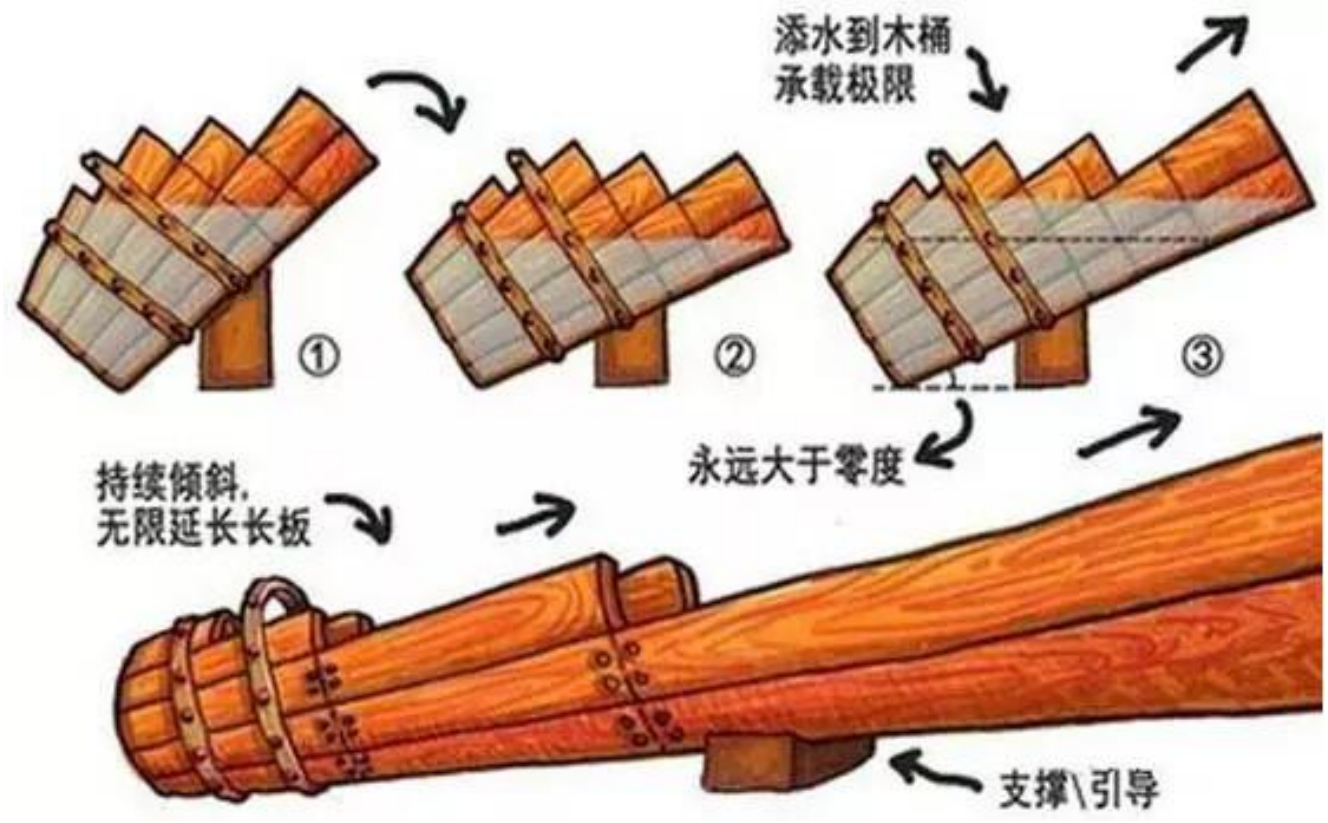
安全事件处置效果欠佳

安全事件处置效果严重依赖执行者的能力和状态，有些误操作甚至会放大安全事件的影响面。

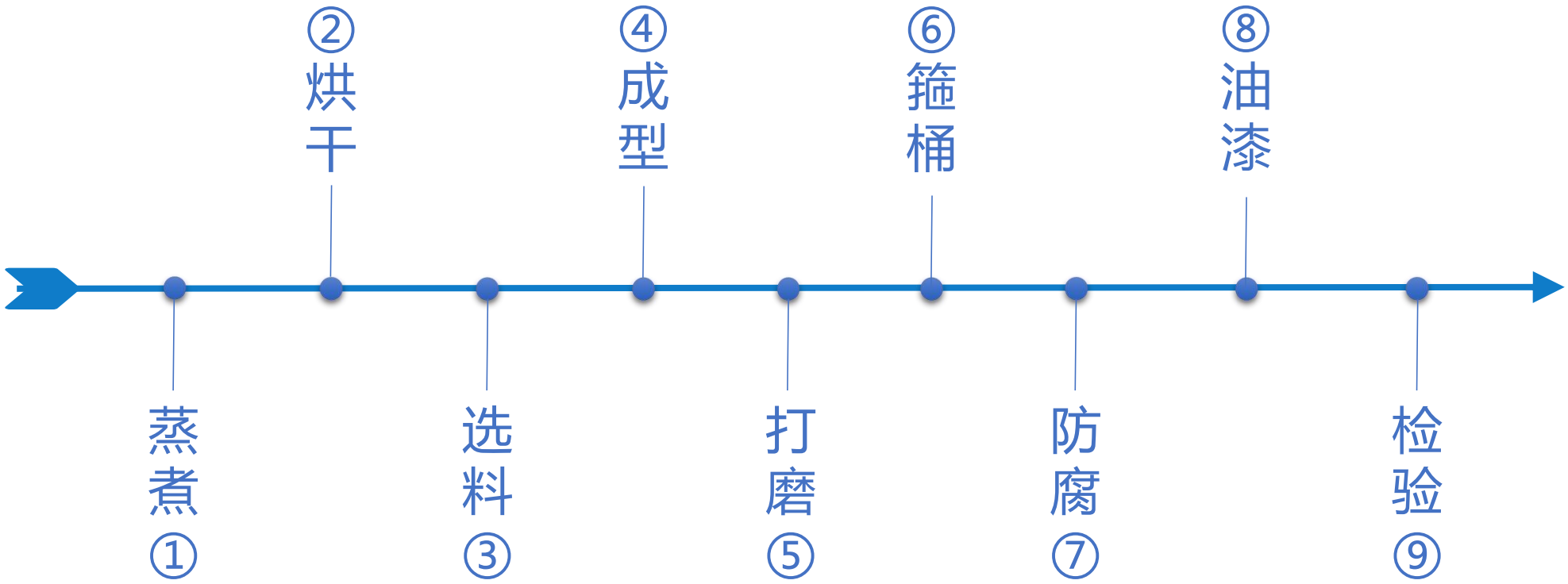
团队变动对运维能力影响较大

团队或关键岗位出现变化，对用户整体的安全能力会有较大的影响。

对木桶理论的第N+1种解释



对木桶理论的第N+1种解释



PART 02

解决方案

Security Operation Solution

通过平台及产品以及托管式服务，加强安全产品间的关联关系，将安全产品间的“缝隙” 减少甚至消除。

智能安全运维管理平台整体架构

运维能力层

- 工作台
- 资产管理
- 脆弱性管理
- 标准处置流程
- 服务质量管理
- 自动化报告管理

场景化能力层

- 防御策略管理
- 动态蜜网
- 页面可用性监测
- 页面篡改监测
- 内容安全分析
- 自动化应急处置

数据处理层

- 任务调度算法
- 服务指标算法
- 基础资源（Mysql+ES）
- 机器学习模块（训练+推理）

基础安全能力

- 资产发现引擎
- 漏洞扫描引擎
- 威胁分析引擎
- 能力联动引擎

IT信息安全成为企业发展关键点

掌数信息帮助企业通过标准化、自动化和智能化的方式
实现安全事件的全面闭环和企业运维知识的落地

标准化

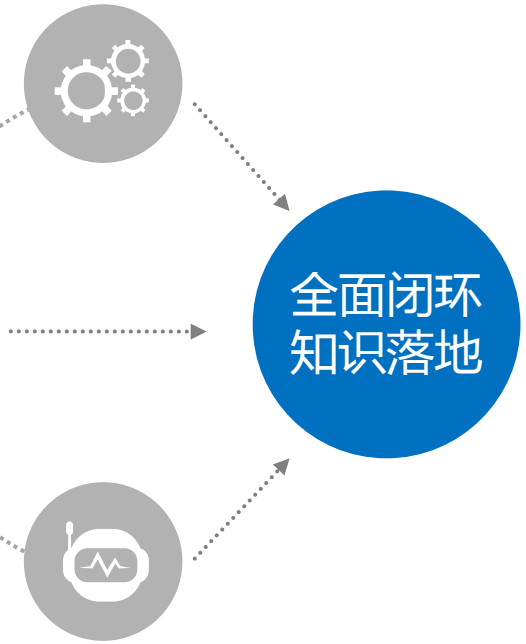
日常事件标准处置流程、标准应急流程、标准渗透测试矩阵

自动化

自动化应急处置、基础安全能力联动

智能化

标注、训练、推理一站式机器学习系统



全面落地闭环

对项目流程确保流程全闭环管理，确保数据安全性

确保结果质量

快速响应、高效协同推进信息安全工作

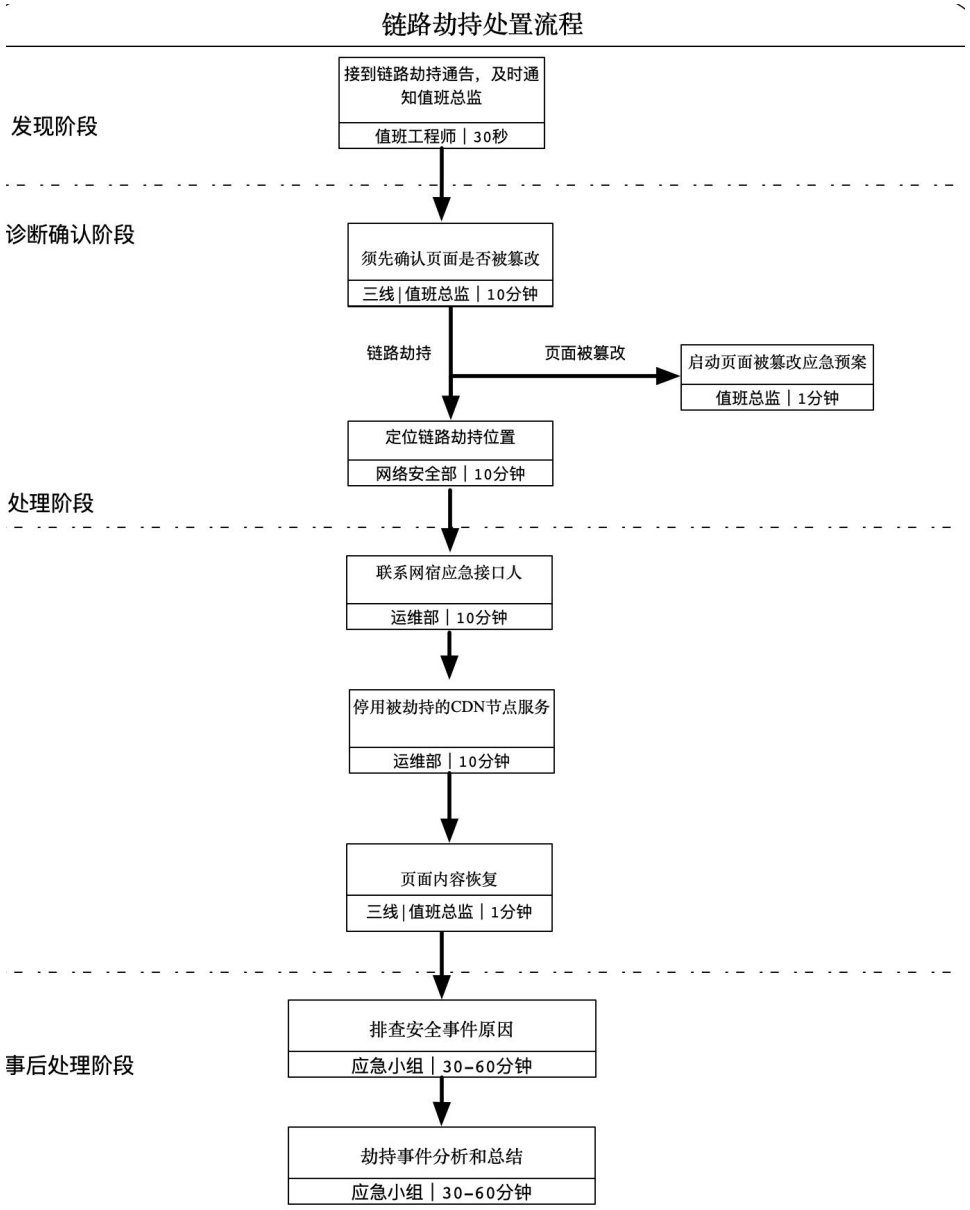
标准化--网络安全标准处置流程

侦查阶段	大规模扫描探测事件
武器化阶段	攻击样本投递
	Webshell上传事件
攻击阶段	RLOGIN弱口令事件
	FTP弱口令事件
	TELNET弱口令事件
	NNTP弱口令事件
	IMAP弱口令事件
	SMTP弱口令事件
	POP3弱口令事件
	MS-SQL弱口令事件
	MySQL弱口令事件
	Oracle弱口令事件
	针对性漏洞利用事件
	DDOS攻击事件
	持续性攻击事件
	MySQL暴力破解事件
	Oracle暴力破解事件
	Rdp暴力破解事件
	SSH暴力破解事件
	TELNET暴力破解事件
	MS-SQL暴力破解事件
	POP3暴力破解事件
	FTP暴力破解事件
	SMTP暴力破解事件
	IMAP暴力破解事件
	Webshell连接事件
	HTTP_Redis命令注入攻击
	HTTP_Linux命令注入攻击
	WindowsRDP远程命令执行（CVE-2019-0708）
	FastJson反序列化漏洞攻击
	泛微E-cologyOA代码执行漏洞攻击
	PHPStudy后门事件
	ApacheSolr远程代码执行漏洞（CVE-2019-0193）
	Coremail敏感信息泄露漏洞
	Harbor任意管理员注册漏洞
	iTerm2远程代码执行漏洞（CVE-2019-9535）
	泛微e-cologyOA前台SQL注入漏洞
	WebLogic反序列化漏洞
	Kibana代码执行漏洞
	泛微e-cologyOA数据库配置信息泄露漏洞
	Apache solr velocity模版注入远程命令执行漏洞

	感染CryptON（x3m）勒索病毒
	感染Sodinokibi勒索病毒
	感染AUCHENTOSHAN（GlobeImposter变种）勒索病毒
	感染GlobeImposter3.0勒索病毒
	感染GlobeImposter5.0勒索病毒
	感染sherhagdomski（GlobeImposterV2）勒索病毒
	感染Crysis（Dharma）勒索病毒
	感染Phobos勒索病毒
	感染PRCP（Matrix变种）勒索病毒
	感染Clop勒索病毒
	感染ITLOCK（Matrix）勒索病毒
	永恒之蓝事件
后渗透阶段	Windows系统帐户密码被重置事件
	Windows系统创建用户帐户事件
	Windows系统添加账号到管理组事件
	Windows系统日志被清除事件
	windows系统杀毒软件关闭事件
	windows系统存在恶意进程事件
	系统存在恶意进程事件
	SNMP弱口令事件
	SMB暴力破解事件
	VPN暴力破解事件
	DGA域名访问事件
	内对外扫描探测事件
	内对内扫描探测事件
	外对内WEB弱口令事件
	内对内外WEB弱口令事件
	VPN单账号短时间内用多个IP登陆
问题管理类 PlayBook	违规扫描行为
	内网异常应用
	广告软件/VPN等客户端程序访问DGA域名
	广告软件/VPN等客户端程序进行敏感端口扫描
	广告软件/VPN等客户端程序访问恶意域名
	主机用途变更
	下载安装受感染工具软件
	失陷主机--处置脚本
	互联网大规模扫描探测事件
	互联网持续性扫描探测事件
	分支机构访问总部高危端口
	敏感端口扫描探测事件
	内网大规模扫描探测事件
	内对内漏洞攻击事件
	系统存在异常连接事件
	感染病毒木马事件

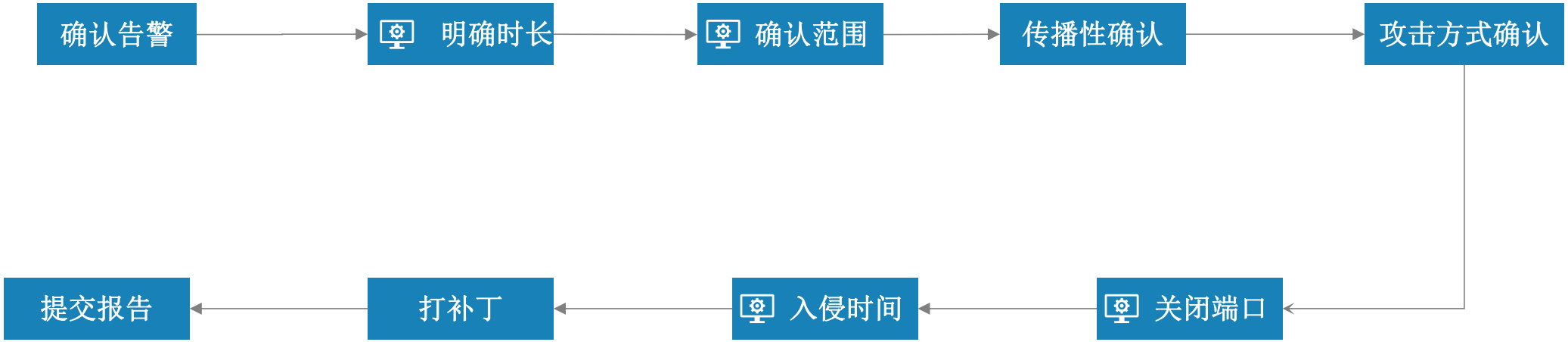
标准化--业务安全标准处置流程

除了网络安全事件处置流程，我们还根据媒体行业场景集成了大量安全事播出件的处置流程，包括**页面篡改**，**直播故障**、**直播信号马赛克**、**视频源站故障**等十余种处置流程。每个处置流程都涉及到多人甚至多团队的协作。



自动化--人机协同机制

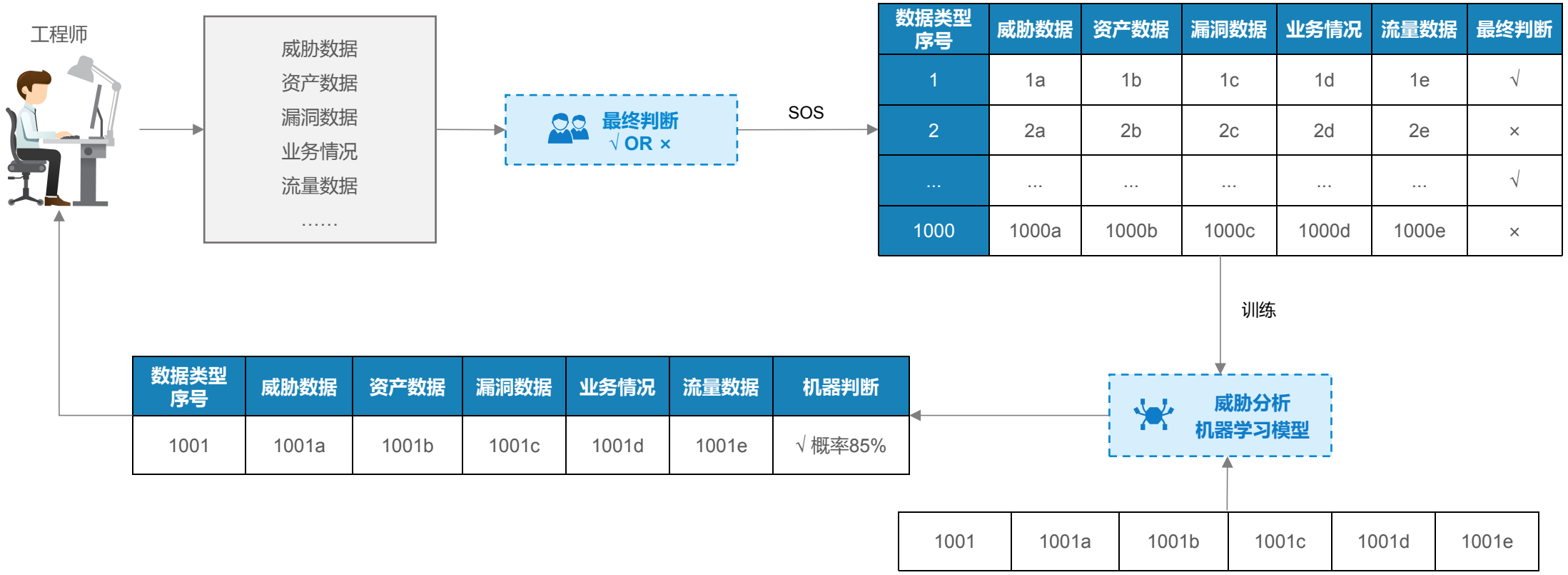
勒索病毒标准处置流程



20+ 全自动 & 120+ 人机协同

结构化数据是安全运维工作关注最多的数据类型

标准的数据分析逻辑是人通过收集多个维度的数据，给出最终判断，而掌数信息会将这些查询和判断的信息放入机器学习模型训练。当出现新告警时，系统会根据之前的训练模型给管理员一个判断概率，辅助管理员分析。



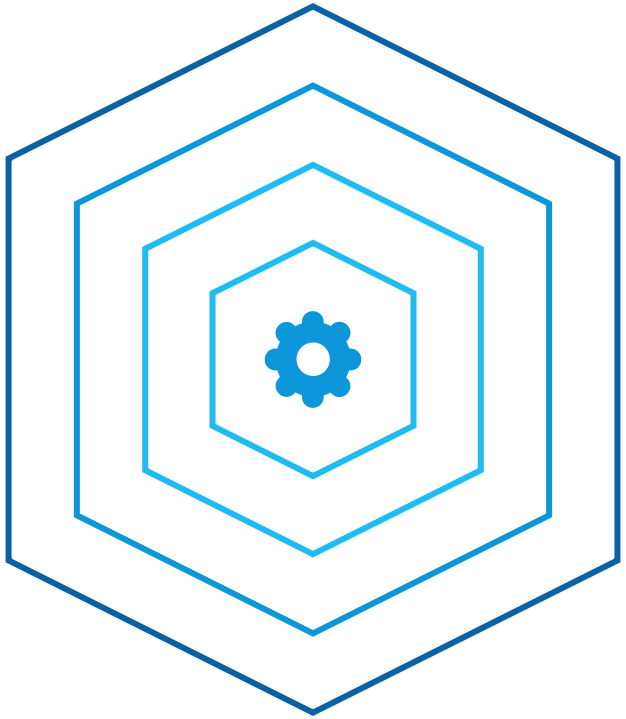
数据类型序号	威胁数据	资产数据	漏洞数据	业务情况	流量数据	最终判断
1	1a	1b	1c	1d	1e	√
2	2a	2b	2c	2d	2e	×
…	…	…	…	…	…	√
1000	1000a	1000b	1000c	1000d	1000e	×

数据类型序号	威胁数据	资产数据	漏洞数据	业务情况	流量数据	机器判断
1001	1001a	1001b	1001c	1001d	1001e	√ 概率85%

1001	1001a	1001b	1001c	1001d	1001e

闭环安全事件

通过标准处理流程全面闭环安全事件



提高安全产品使用效率

一站式机器学习与自动化处置模块有效提升了运维团队对安全产品的使用效率。

提升安全事件处置效果

通过人机协同的标准处置流程，提升安全事件处置的效率和准确性

运维团队知识落地

通过一站式机器学习模块与标准处置流程，将用户运维团队知识落地。

车杂而乘之，卒善而养之，是谓胜敌而益强。

创始人介绍

孙东

- ✓ 武汉大学通信与信息系统博士
- ✓ 中欧国际工商管理学院EMBA
- ✓ 曾任职于国家广播电影电视总局
- ✓ 曾任职启明星辰政府事业部技术总监、媒体和教育行业总经理、数据运营事业群副总经理、副总裁

黄乐

- ✓ 曾任央视网网络安全负责人
- ✓ 《企业安全建设之道》作者
- ✓ 清流派企业安全沙龙创始人
- ✓ 诸子云企业安全联盟北京负责人

孙大凡

- ✓ 曾任广电总局中国广播电影电视协会技术工作委员会秘书长助理
- ✓ 14年加入北京启明星辰信息安全技术有限公司，任媒体事业部销售总监

谢谢观看！

PAMADATA INFORMATION

掌数
PAMADATA