2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

AiLPHA大数据安全分析
应用于医疗网络安全闭环的实践

主讲人：杨锦峰 13515813551

信息安全三要素

机密性

Confidentiality

完整性

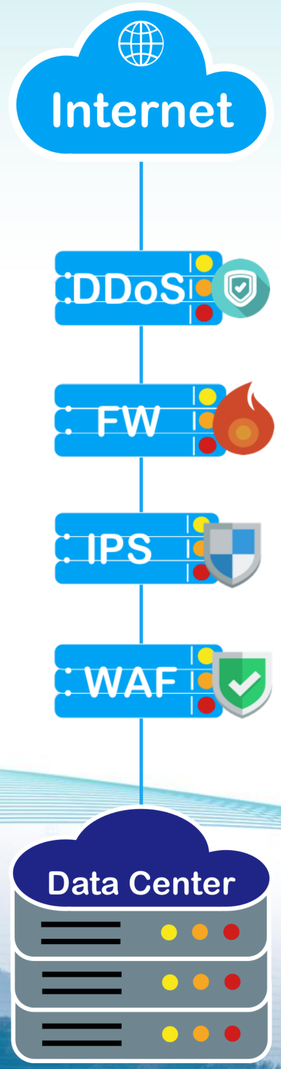
Integrity

可用性

Availability

数据安全

以防御为主的传统安全解决方案



传统以防御为主的安全解决方案，解决了90%以上的安全问题，但是.....

- 仅基于特征进行安全检测
- 严重依赖单点的处理能力
- 防护设备各自为战不协同
- 无法应对持续性安全威胁
- 告警量大安全运维效率低

Intrusion Kill Chain

Intrusion Kill Chain模型

Reconnaissance
侦查

Weaponization
组装

Delivery
投送

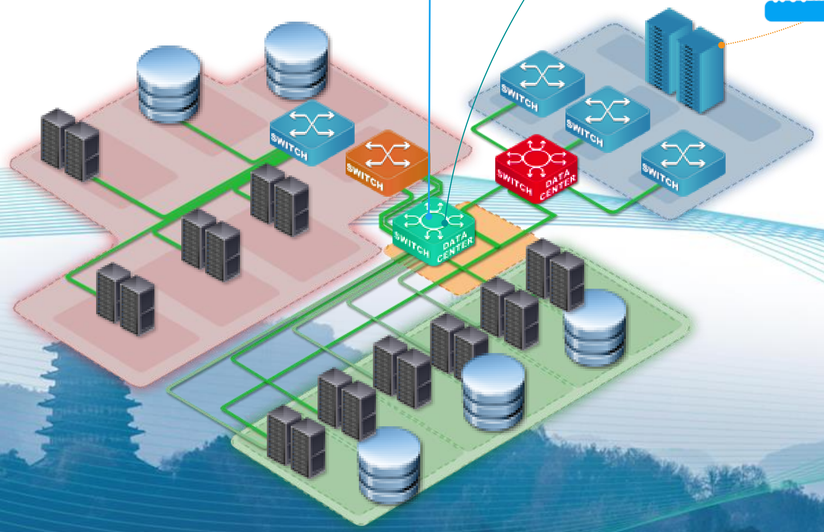
Exploitation
攻击

Installation
植入

Command & Crontal
C2 控制

Actions on Objectives
收割

AiLPHA大数据的最佳实践



知己： 基于机器学习发现**潜在的入侵**和**高隐蔽性攻击**，**回溯攻击历史**，**预测即将发生的安全事件**；

知彼： 结合威胁情报形成海陆空天一体的安全防御能力；

采集了关键安全设备的日志、告警，满足网络安全法不少于6个月的日志存储要求（第三章、第二十一条、3节）；

具备对内部失陷资产的发现与验证能力；

数据处理路径

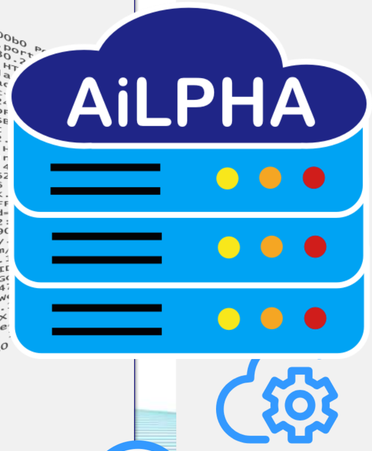
数据采集

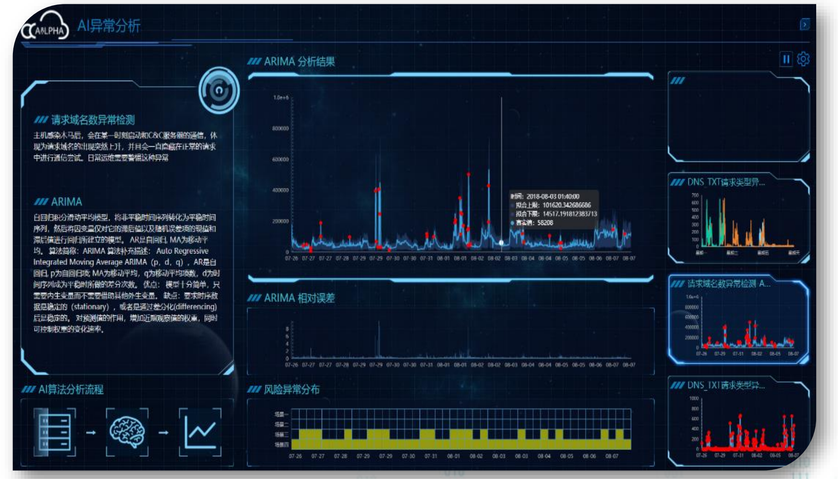
安全环境状态识别

已知安全事件监测

未知安全风险监测

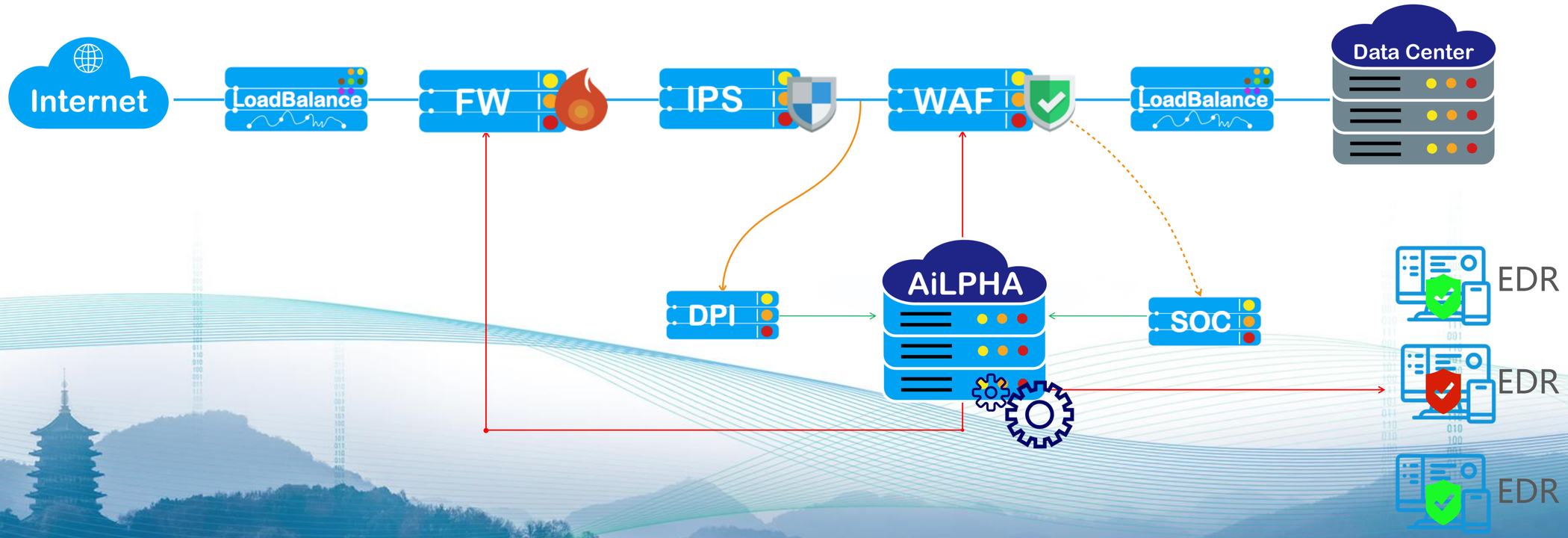
安全状态综合分析





实现从‘被动防守’到‘主动防御’的转型

树立正确的网络安全观，加强信息基础设施网络安全防护，加强网络安全信息系统统机制、手段、平台建设，加强网络安全事件应急指挥能力建设，积极发展网络安全产业，**做到关口前移，防患于未然。**



DER：Endpoint Detection and Response 终端检测和响应

安全的最核心问题

Intrusion Kill Chain模型

Reconnaissance
侦查

Weaponization
组装

Delivery
投送

Exploitation
攻击

Installation
植入

Command & Crontal
C2 控制

Actions on Objectives
收割

无侵入式被动发现资产

- 无侵入式被动发现，基于流量、日志、脆弱性等数据
- 采用实时流式计算框架，新入网资产，30秒内即可被识别加入资产管理
- 识别多种资产类型和指纹信息，如Web服务器、邮件服务器、数据库、终端等

EDR

病毒查杀

本地+云端双引擎查杀勒索、挖矿病毒

网站后门查杀

对网页木马进行查杀

漏洞管理

实时修复0day漏洞，加固系统

性能监控

实时监控系统资源，检测挖矿行为

微隔离

东西流量的防护

网站防护

防SQL流入、XSS、CC攻击、防恶意扫描、敏感信息泄露

登录防护

异常登录防护，防暴力破解、弱口令检测

防端口扫描

防恶意工具对侦听端口的扫描行为

溯源分析路径

- 掌握网络拓扑和安全边界态势，全局感知安全威胁
- 锁定风险资产和风险用户，画像分析异常行为和相关风险
- 异常行为举证，利用威胁情报和漏洞信息辅助验证
- 项目实践：20分钟内实现威胁溯源

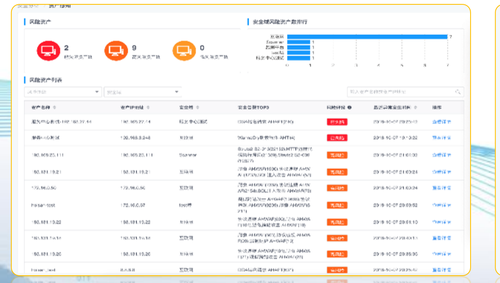
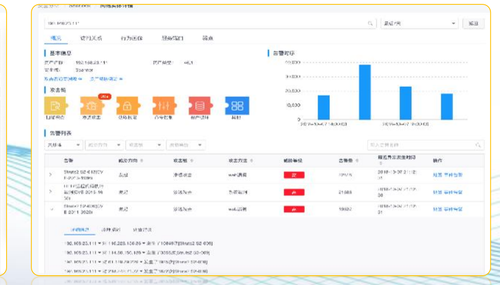
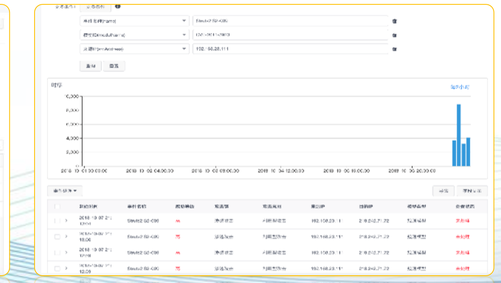
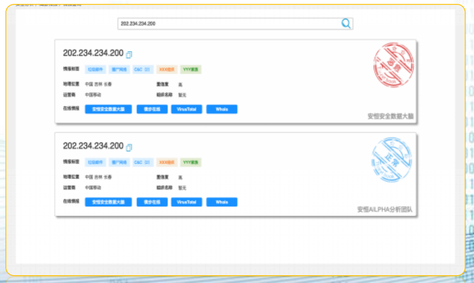
网络拓扑监控
跨安全域行为检测

风险资产发现

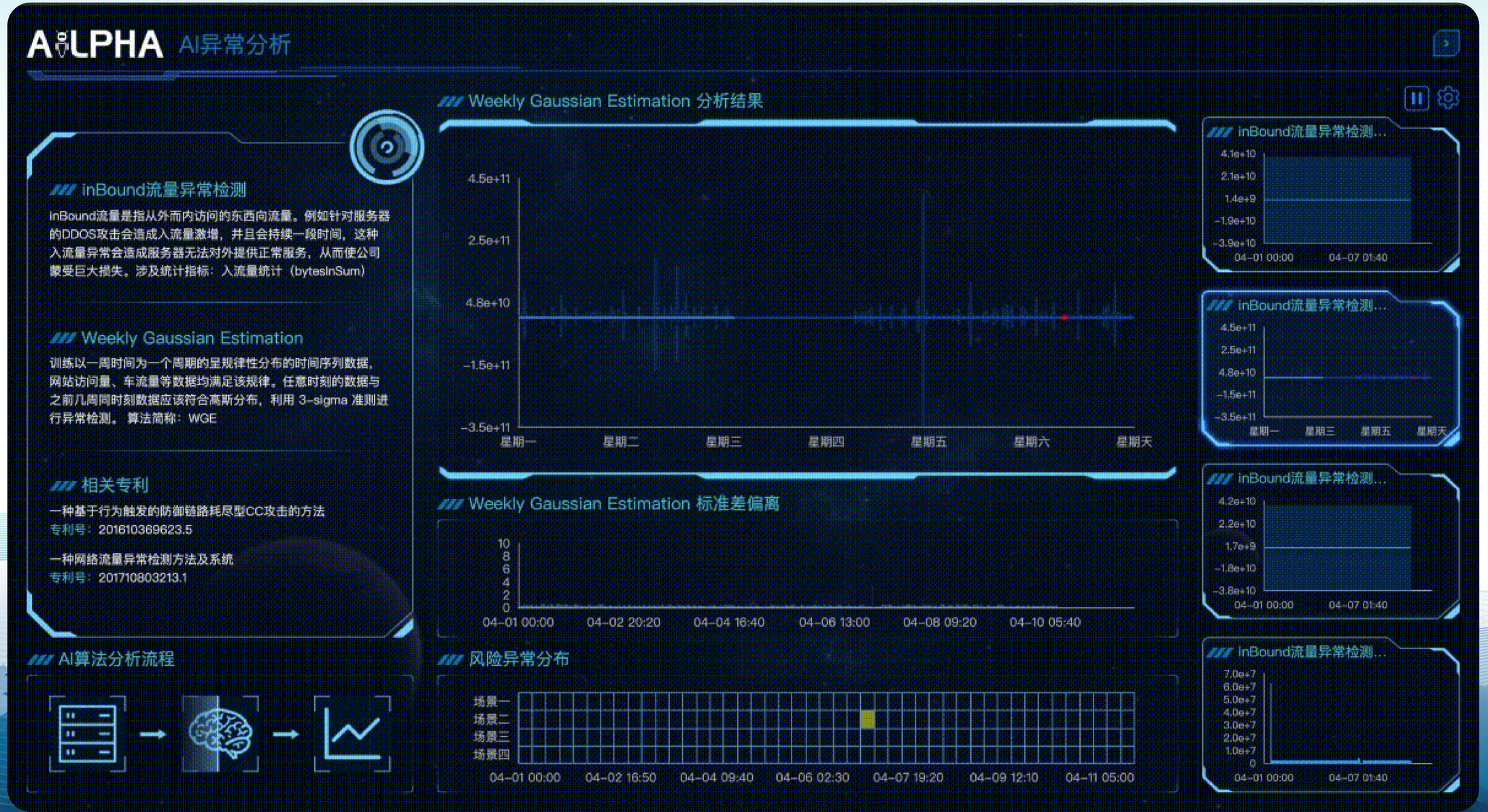
资产综合画像

异常行为举证
上下文分析

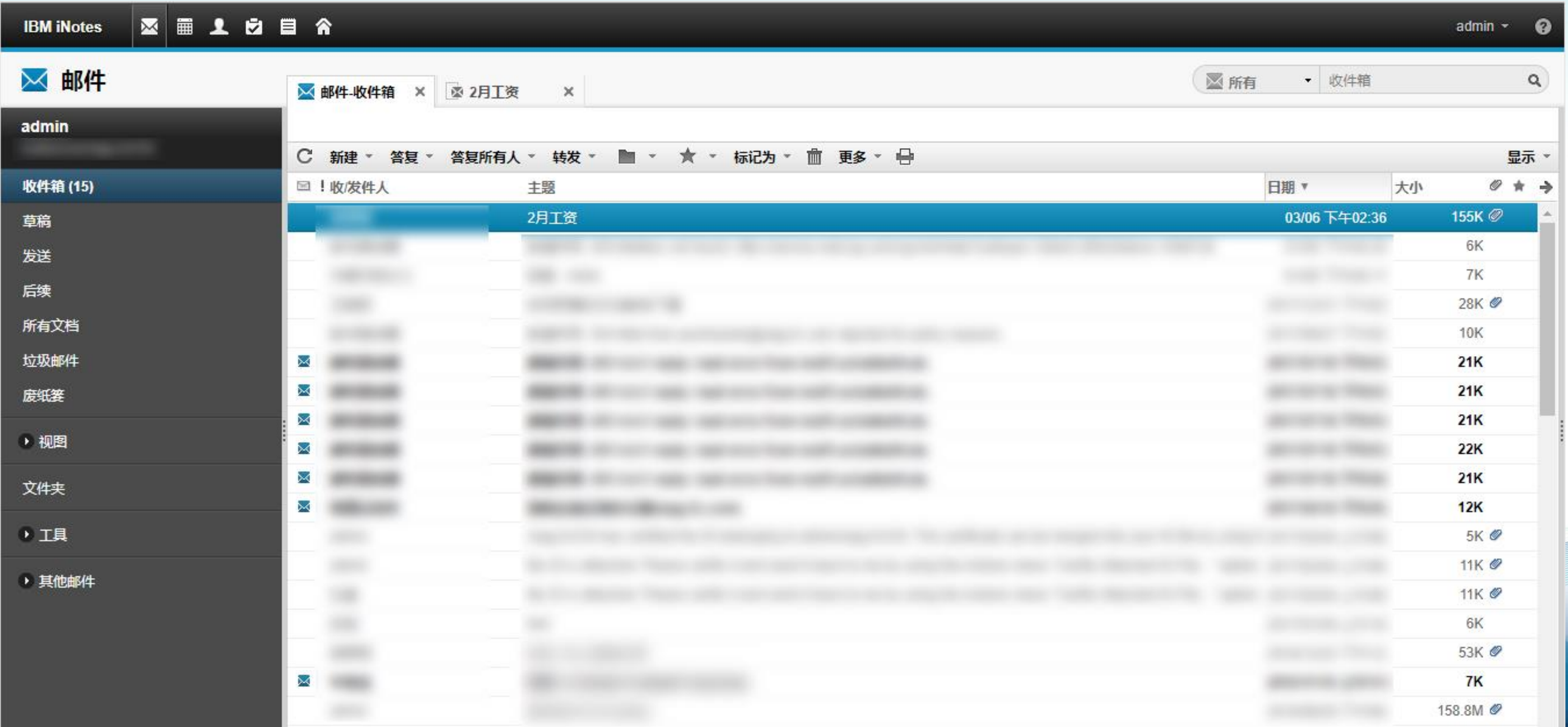
威胁情报查询
漏洞利用验证

可能是业内首创的AI智能引擎



AI智能的案例实践


IBM iNotes
admin
邮件
邮件-收件箱
2月工资
所有
收件箱
admin
新建
答复
答复所有人
转发
标记为
更多
显示
收/发件人
主题
日期
大小
收件箱 (15)
草稿
发送
后续
所有文档
垃圾邮件
废纸篓
视图
文件夹
工具
其他邮件
2月工资
03/06 下午02:36
155K
6K
7K
28K
10K
21K
21K
21K
22K
21K
12K
5K
11K
11K
6K
53K
7K
158.8M

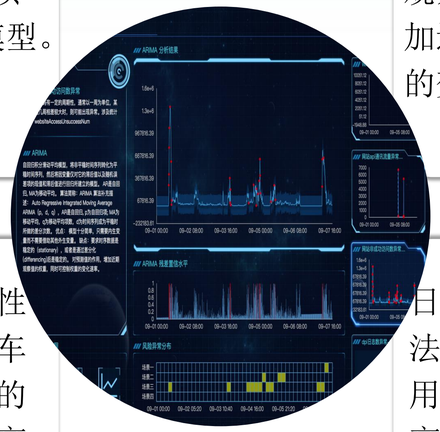
可能是业内首创的AI智能引擎

ARIMA

自回归积分滑动平均模型，将非平稳时间序列转化为平稳时间序列，然后将因变量 仅对它的滞后值以及随机误差项的现值和滞后值进行回归所建立的模型。AR是自回 归，MA为移动平均。

Exponential Smoothing

指数平滑法常用于中短期趋势预测。是一种加权移动平均法。其特点是可加强观察期近期观察值对预测值的作用，增加近期观察值的权重，同时可控制权重的变化速率。



Weekly Gaussian Estimation

训练以一周时间为一个周期的呈规律性分布的时间序列数据，网站访问量、车流量等数据均满足该规律。任意时刻的数据与之前几周同时刻数据应该符合高斯分布，利用 3-sigma 准则进行异常检测。

RPCA-SST

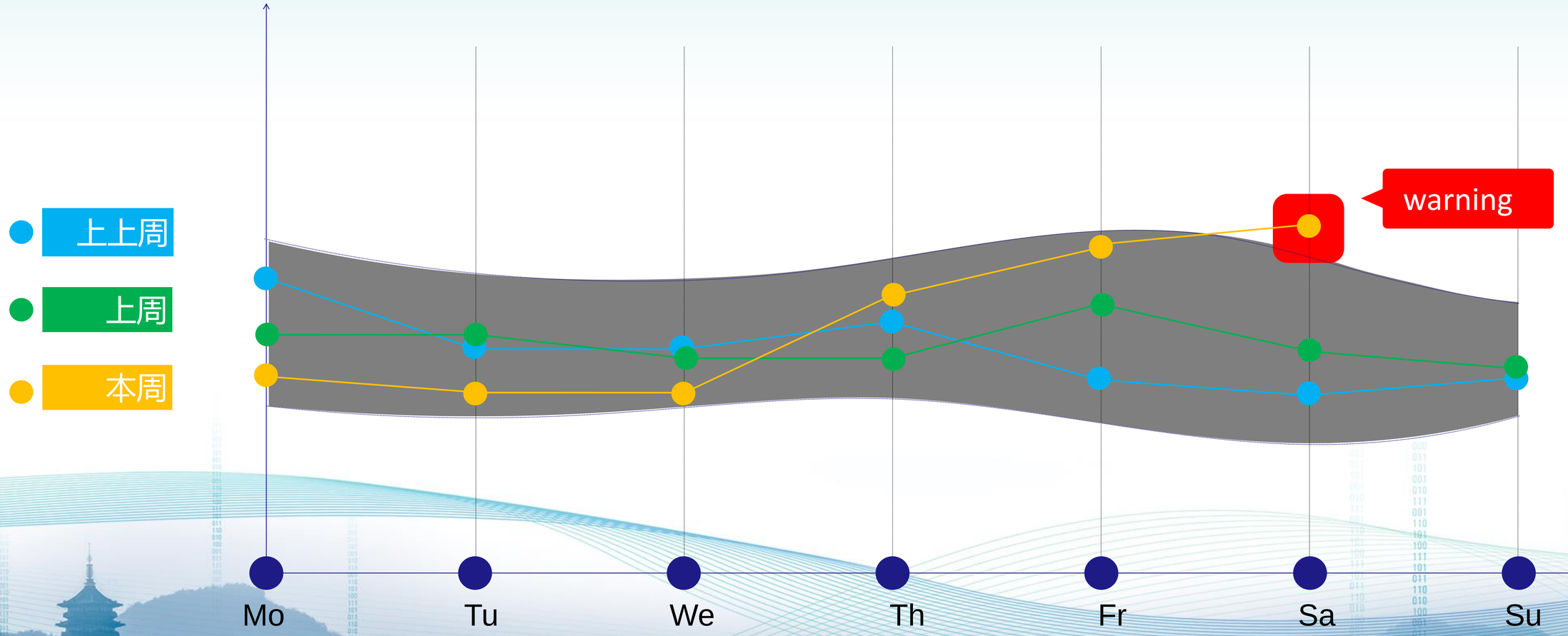
日常观测数据往往包含噪声干扰，该算法将时序数据片段转化为矩阵结构，利用RPCA重构矩阵剔除大幅值噪声，提高突变程度略低的异常点检测性能，发现掩盖在噪声下的异常信息。

论文：A Robust Change-point Detection Method by Eliminating Sparse Noises, IEEE DSC

专利：一种基于行为触发的防御链路耗尽型CC攻击的方法 专利号：201610369623.5

专利：一种网络流量异常检测方法及系统 专利号：201710803213.1

AI智能的基本原理



AiLPHA的颜值


AiLPHA 外部攻击态势
时间范围：本月
利用型攻击 483
恶意文件 9
拒绝服务 0
扫描探测 1
异常事件 0
APT 10
系统管理 0
资产破坏
命令控制
渗透攻击
扫描探查
其它
攻击来源排行
攻击来源国家排行
受攻击安全域排行


AiLPHA 横向威胁感知
时间范围：本月
办公网
研发区
DMZ
内部安全告警数 576
内部攻击者数 9
内部受害者数 18
安全域 7
被访问业务排行
最新内部安全告警
安全域威胁方向
内部攻击类型分布


AiLPHA 资产外连风险态势
时间范围：本月
外连主机数 32
外连告警数 4373
外连目的IP排行
外连目的国家排行
最新外连事件
外连安全域名排行
外连告警类型TOP10


AiLPHA AI异常分析
Weekly Gaussian Estimation 分析结果
inBound流量异常检测
Weekly Gaussian Estimation
相关专利
AI算法分析流程
Weekly Gaussian Estimation 标准差偏离
风险异常分布


AiLPHA 内网安全态势
DDGMining挖矿木马 AHTI
攻击者基本信息
告警
资产告警
实时场景分析


AiLPHA Sherlock
请输入IP地址

永无止境


AView 网络安全可视化分析
AView 大数据可视化重磅发布
无需任何编程能力，0基础轻松玩转酷炫大屏
二十分钟快速完成大数据可视化
提供100+可视化组件，满足您个性化需求
Ai助力可视化 让可视化更简单更便捷
大幅提高可视化制作效率
满足不同需求节约成本
多类型炫酷界面
0基础轻松制作大屏
AiLPHA大数据实验室出品

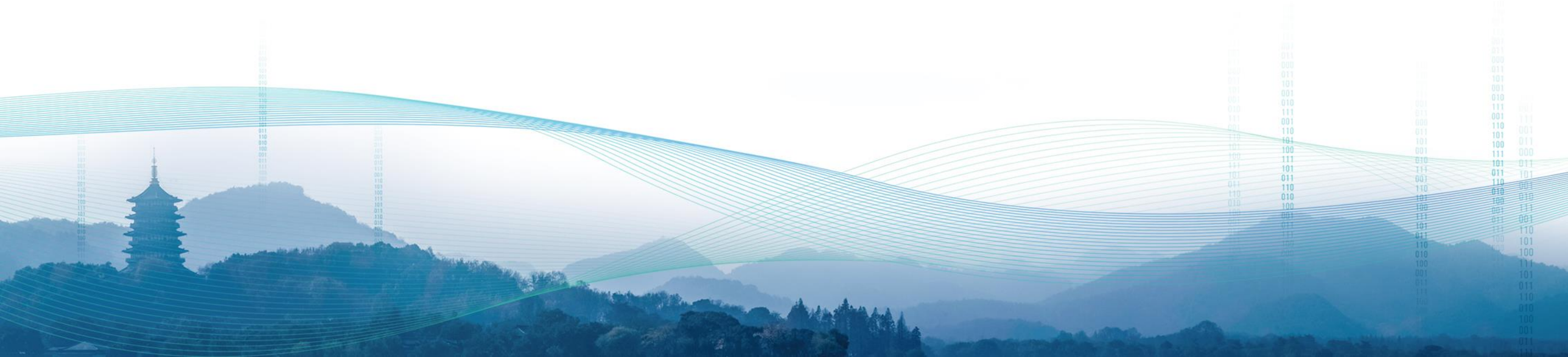
AI | 洞 | 见 | 未 | 来

大数据可视化平台

用户名

密码

案例分享



安全分析案例

3月5日15:03该单位财务部门一台设备出现蓝屏。

3月5日15:37内网爆发蓝屏现象。

3月5日16:00安恒信息安服赶到客户现场确认勒索病毒爆发，并协助该单位进行病毒查杀。

该单位有2000+台设备，没有很好的网络规划，安服处置十分困难，只能是那里有蓝屏去哪里

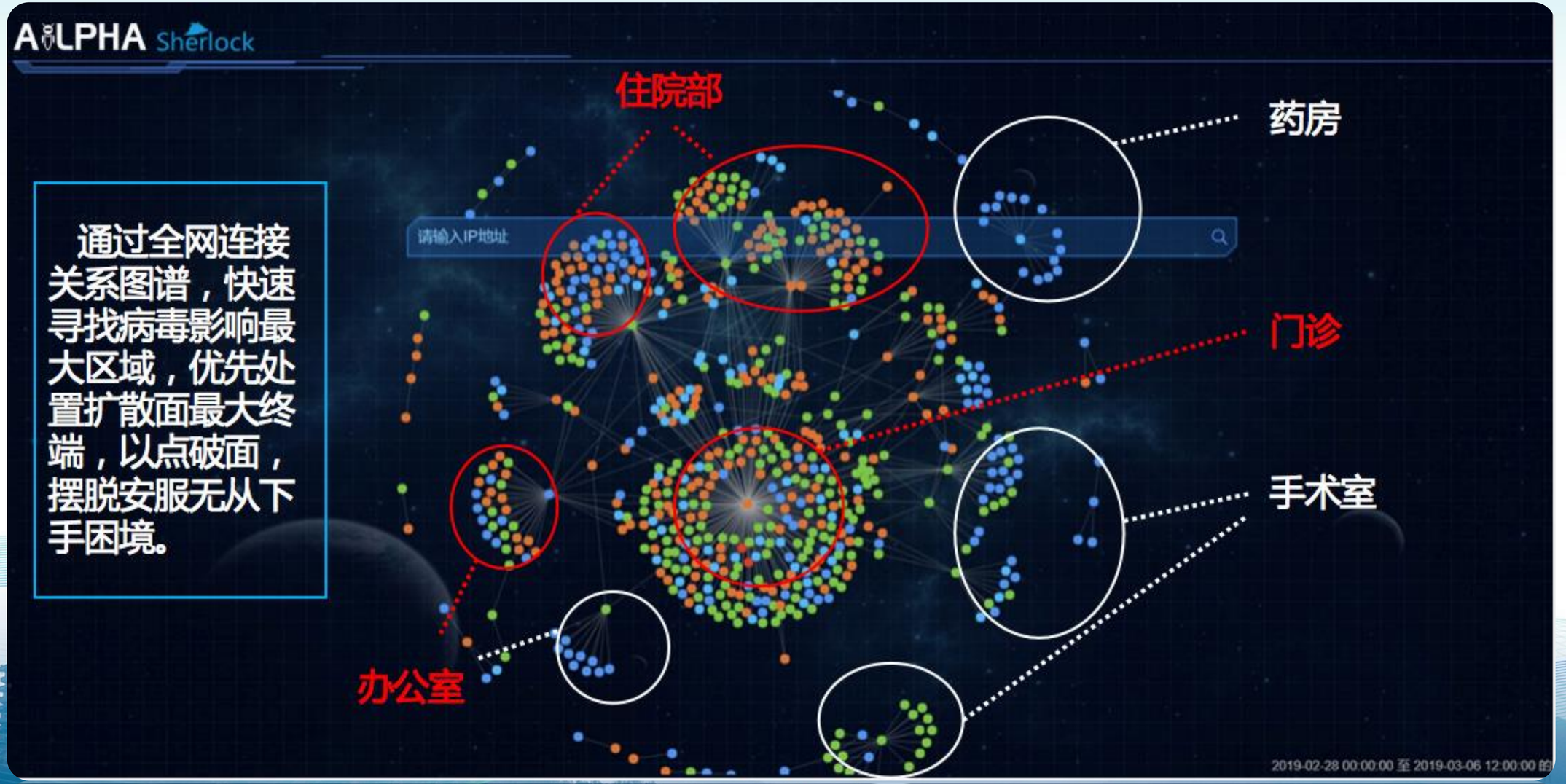
3月6日7:00AiLPHA大数据平台+APT+SOC设备部署。

3月6日采用大数据发现传播源发工单给安服处理方式，成功抑制病毒爆发与扩散

3月7日，根据大暑平台告警，彻底完成内部勒索病毒清理工作

5 5 5 6 6 7

安全分析案例



通过全网连接关系图谱，快速寻找病毒影响最大区域，优先处置扩散面最大终端，以点破面，摆脱安服无从下手困境。

安全分析案例

风险资产

5
已失陷资产数

419
高风险资产数

0
低风险资产数

安全域风险资产数排行

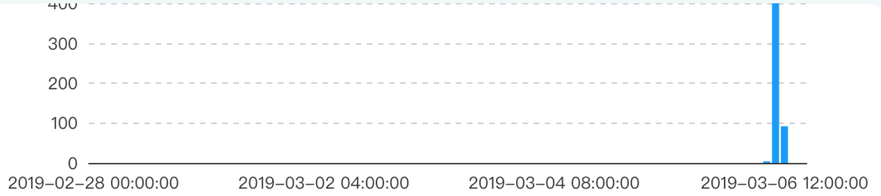
风险资产列表

风险评级 | 安全域 | 输入资产名称或资产IP地址

资产名称	资产IP地址	安全域	安全告警TOP3	风险评级	最近异常发生时间	操作
内网-132.147.1.182	132.147.1.182	内网	SMB远程溢出攻击 AHAPT(294),勒索病毒尝试(292),SMB远程命令执行成功（MS17-010） AHAPT(16)	已失陷	2019-03-06 13:49:54	查看详情
内网-172.16.103.65	172.16.103.65	内网	SMB远程溢出攻击 AHAPT(76),勒索病毒尝试(76)	已失陷	2019-03-06 13:21:43	查看详情
内网-132.147.1.216	132.147.1.216	内网	SMB远程溢出攻击 AHAPT(39),勒索病毒尝试(37),SMB远程命令执行成功（MS17-010） AHAPT(16)	已失陷	2019-03-06 13:21:31	查看详情
内网-172.16.106.122	172.16.106.122	内网	SMB远程溢出攻击 AHAPT(62),勒索病毒尝试(23)	已失陷	2019-03-06 11:01:16	查看详情
内网-172.16.106.125	172.16.106.125	内网	SMB远程溢出攻击 AHAPT(112),勒索病毒尝试(23)	已失陷	2019-03-06 11:00:48	查看详情
内网-172.16.122.101	172.16.122.101	内网	SMB远程溢出攻击 AHAPT(2),勒索病毒尝试(2)	高风险	2019-03-06 13:54:43	查看详情
内网-172.16.161.92	172.16.161.92	内网	SMB远程溢出攻击 AHAPT(31),勒索病毒尝试(30)	高风险	2019-03-06 13:54:43	查看详情

安全分析案例

攻击链



风险详情

安全告警 | 未处理 | 威胁方向 | 攻击链 | 威胁等级 | 输入告警名称

告警	威胁方向	攻击链	攻击方法	威胁等级	告警次数	最近异常发生时间	操作
SMB远程溢出攻击 AHAPT(smbRemoteCmdExe)	发起	扫描探查	系统漏洞	中	290	2019-03-06 13:56:52	处置 告警详情
勒索病毒尝试(AHAPT1)	发起	资产破坏	勒索软件	高	290	2019-03-06 13:57:22	处置 告警详情
SMB远程命令执行成功（MS17-010） AHAPT(successExeSMBRemoteCmd)	发起	渗透攻击	系统漏洞	高	10	2019-03-06 12:27:59	处置 告警详情
勒索病毒攻击成功(AHAPT2)	发起	资产破坏	勒索软件	高	10	2019-03-06 12:27:59	处置 告警详情
SMB远程命令执行成功（MS17-010） AHAPT(successExeSMBRemoteCmd)	遭受	渗透攻击	系统漏洞	高	6	2019-03-06 11:02:37	处置 告警详情
SMB远程溢出攻击 AHAPT(smbRemoteCmdExe)	遭受	扫描探查	系统漏洞	中	6	2019-03-06 11:02:37	处置 告警详情
勒索病毒尝试(AHAPT1)	遭受	资产破坏	勒索软件	高	4	2019-03-06 11:02:00	处置 告警详情
勒索病毒攻击成功(AHAPT2)	遭受	资产破坏	勒索软件	高	4	2019-03-06 11:02:00	处置 告警详情

3月6号12:27
被感染成功后
成为新的病毒源头

3月6号11:02
正在遭受病毒感染

安全分析案例

290 开放端口 （不常用：288个）　0 风险端口

47 MB 流出总流量　1013 MB 流入总流量　0 KB 风险流出流量　0 KB 风险流入流量　0.00% 风险流量占比

开放端口详情

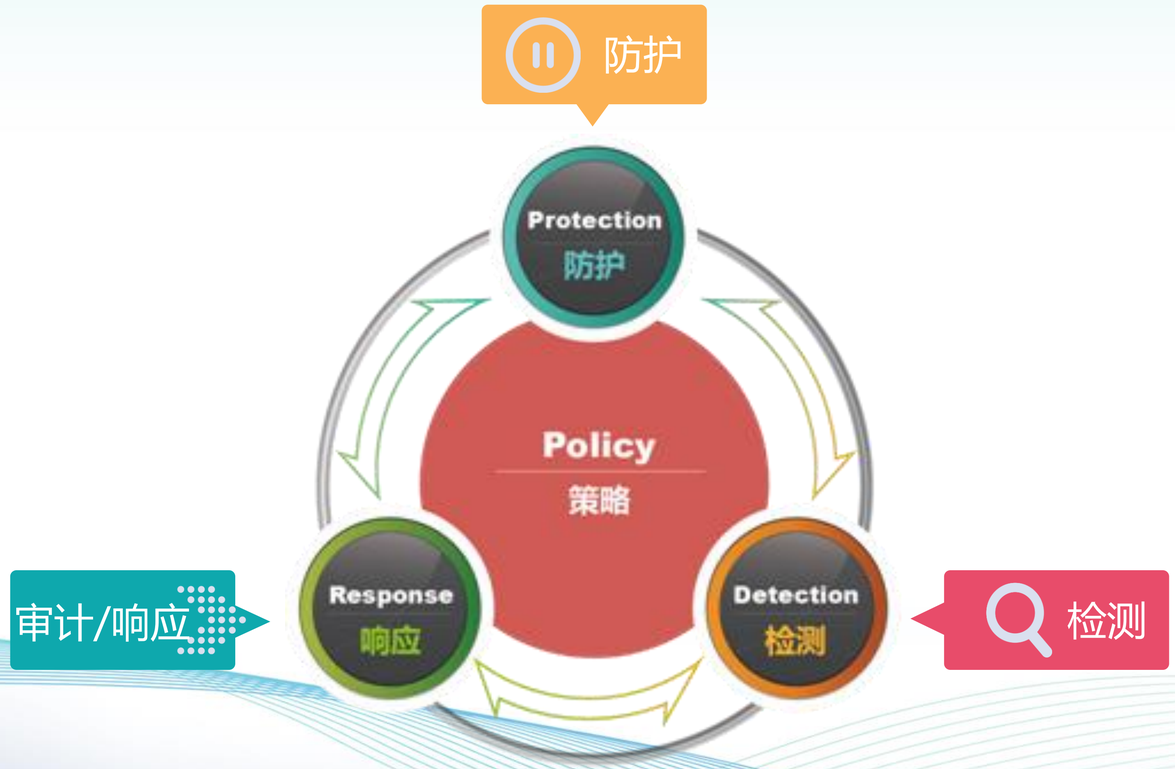
全部　　端口号

开放端口	端口类型	流出流量	流入流量	被访问次数	操作
445	不常用端口	43 MB	858 MB	67	流量日志
139	在红帽企业 Linux 中被 Samba 使用的NET BIOS 会话服务	7 KB	10 KB	46	流量日志
80	用于万维网（WWW）服务的超文本传输协议（HTTP）	49 KB	12 KB	26	流量日志
22105	不常用端口	1 KB	1 KB	2	流量日志
49834	不常用端口	23 KB	1 MB	2	流量日志
57801	不常用端口	23 KB	1 MB	2	流量日志
57803	不常用端口	23 KB	1 MB	2	流量日志
57844	不常用端口	25 KB	1 MB	2	流量日志
62911	不常用端口	25 KB	1 MB	2	流量日志

1. 资产自动开放445，22105，49834等不常用端口288个。

2. 445端口流入流量858MB，基本可以确认是通过445端口感染。

可持续的安全能力



THANK YOU

谢　　谢　　观　　看