GOPS2017 Shanghai

GOPS 全球运维大会 2017 上海站

指导单位：数据中心联盟 Data Center Alliance

主办单位：高效运维社区 GreatOPS Community　开放运维联盟 OOPSA Open OPS Alliance

大会时间：2017年11月17日-18日

大会地点：上海光大会展中心国际大酒店（上海徐汇区漕宝路67号）

GOPS2017
Shanghai

企业内部风险的破冰探索

董晓琼

平安科技安全平台部

董晓琼

携程旅行网-信息安全总监
平安科技-　安全平台部

目录

企业风险聚焦


安全监控
业务安全
数据安全
客户端安全
应用安全
接口安全
未知风险
内部员工风险
终端安全
复杂事件管理和关联
安全适应及响应
外部攻击
内容安全
舆情与仿冒
市场活动
应用的生命周期管理
安全数据的查询与审计
员工风险

安全动因

行业内迫切度、重要度

- 金融行业管控驱动
- 行业竞争环境
- 用户信任、企业的价值驱动

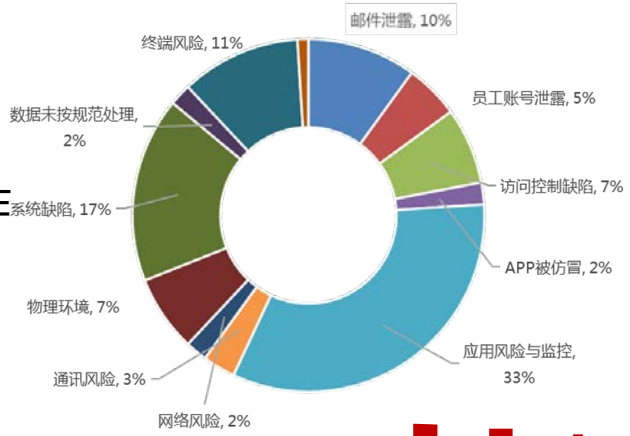
国内外监管标准趋严

- 《中华人民共和国网络安全法》于2016年11月7日发布，自2017年6月1日起施行
- 欧洲议会于2016年4月27日通过《一般数据保护条例》，该条例将对中国企业的移动应用安全，以及数据收集、处理和交易产生重大影响。

驱动力

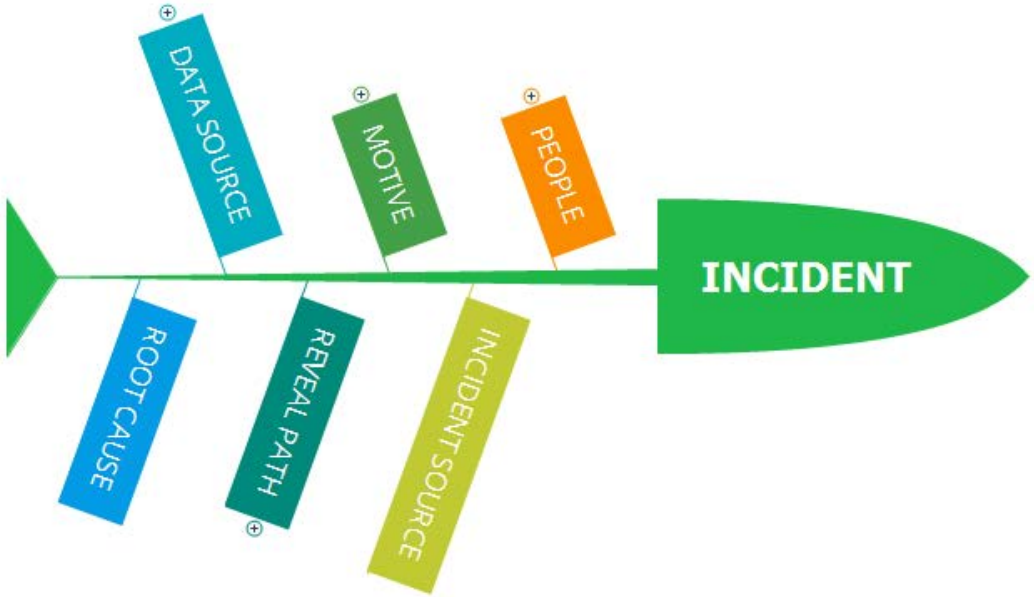
内部驱动

误操作
利用
滥用
违规



目录

多维解构


DATA SOURCE
MOTIVE
PEOPLE
INCIDENT
ROOT CAUSE
REVEAL PATH
INCIDENT SOURCE

01 员工风险事件的发现机制

1、客户投诉
2、监察部门
3、专业公司自查
4、安全监控工具

02 信息泄露的途径

1、邮件泄露　2、USB/Ukey　3、应用系统漏洞缺陷
4、文件打印　5、DB运营　6、IM传输
7、数据中转站-跳板机　8、蓝牙、红外
9、外部数据合作　10、GitHub、网盘等　11、大数据平台等

03 信息泄露的动机

1、经济利益驱动　2、员工操作不规范
3、员工不满恶意报复　4、员工滥用误用导致
5、员工跳槽资本

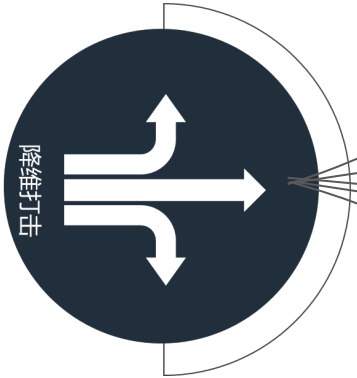
04 “敏感”信息获取来源

1、业务应用系统　2、接口、应用端
3、对外数据合作-违规获取、传输、及分析数据
4、数据库、大数据平台　5、来自跳板、打印
6、测试环境(存在真实用户数据）等

05 泄露的原因

升维思考


事件响应能力：
事件响应机制及方式
事件响应效率
数据丰富度及能力：
所需数据范围及来源
数据的Owner
数据采集及分析框架
基础管控能力：
检测规则-分析和运营
全局、一线安全运营现状
基础管控手段：
基础控制在泄露途径上的覆盖
部署灵活度、及扩容机制
所采用的产品是否能够检测
-检测机制、自定义能力
-产品的APIs支持等
组织管理/架构：
组织架构、职责是否明确
基础管控框架
安全管控策略/流程是否健全
现有奖惩体系
现状



01 基础数据匮乏、数据通道障碍、获取、分析成本高

02 基础控制手段：专业领域能力强，有较强的局限性、功能单一化、数据独立化，不能适应及应对协同作战的趋势

03 较多产品还停留在规则匹配的模式下，未知风险的监控、预测水平低（智能化）

04 风险不能及时掌握，预警能力弱

05 响应机制较为单一，与企业管控需求差距较大

员工风险监控平台：
1、建立一套通过多风险特征、结合员工日常属性特征、行为等进行风险决策依据的平台；

数据及数据平台通

1、员工相关数据源打通
2、数据采集、获取和存储-框架支持
3、数据查询与分析
-按集团维度
-按专业公司

员工风险可视化：

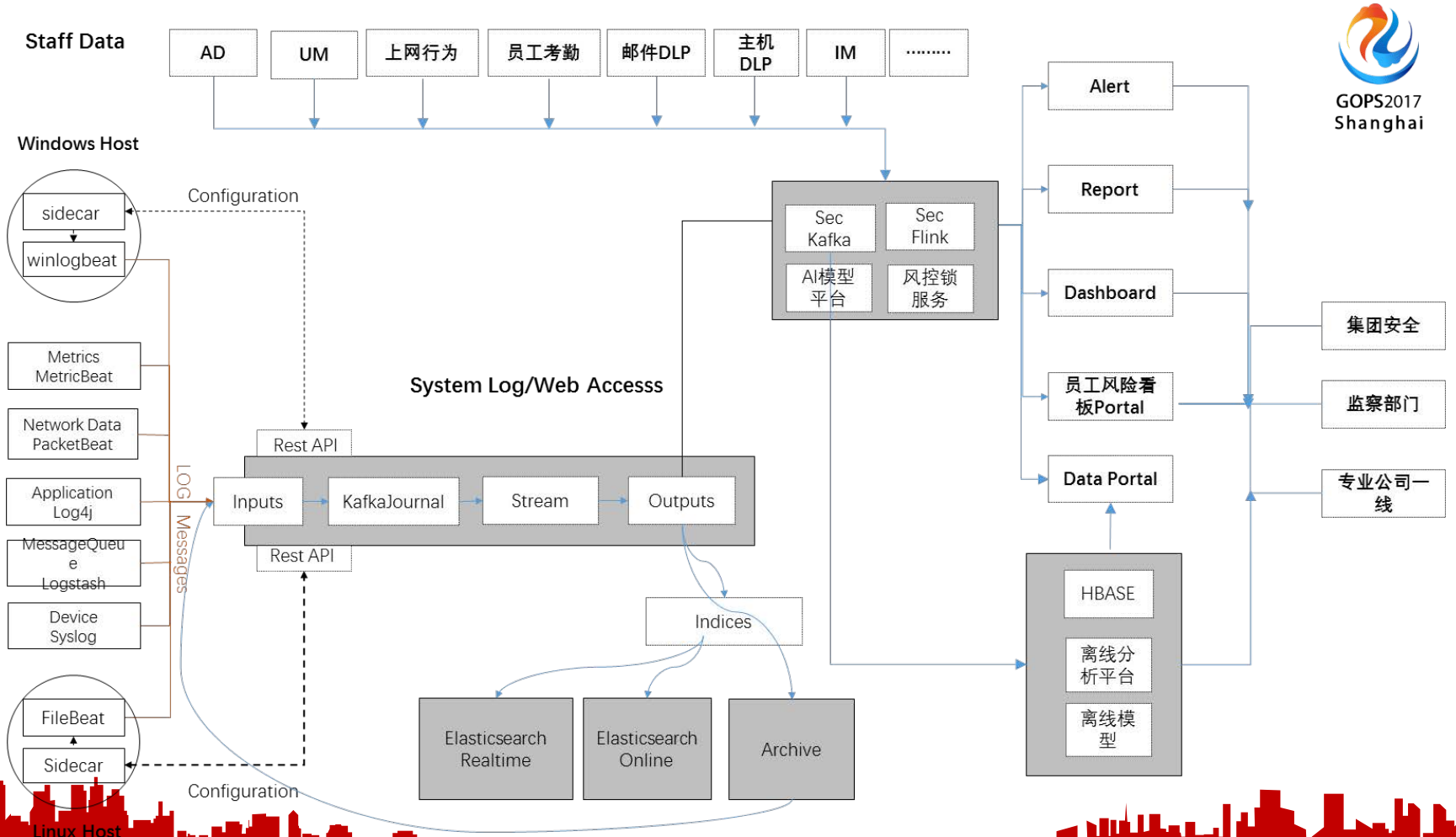
1、实时监控、自动预警
2、风险趋势仪仪表化
3、风险一目了然、全盘掌握；

目录

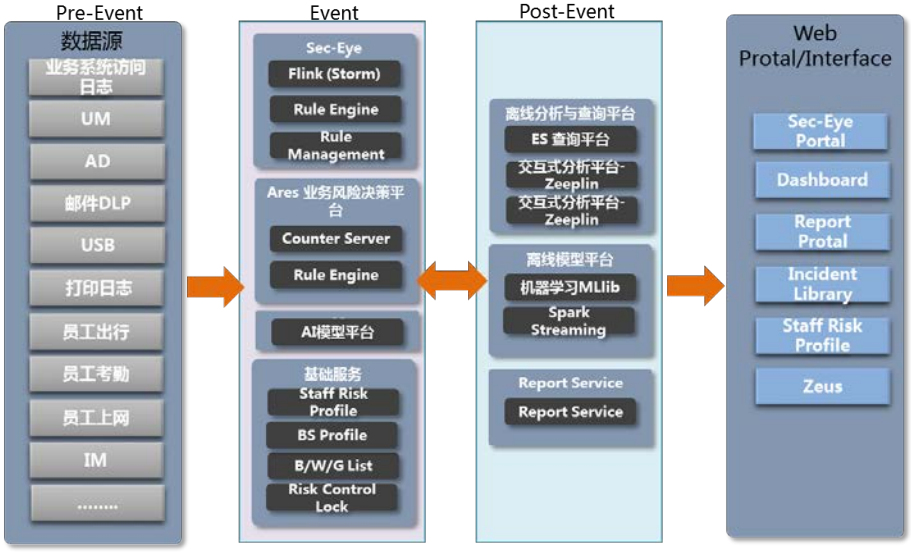
员工风险识别框架


事件层
员工风险看板
Dashboard
Report Protal
Incident Library
Staff Risk Profile
Zeus安全感知
分析引擎层
实时分析层
Flink (Storm)
Rule Management
Rule Engine
AI模型平台
离线分析与查询平台
ES 查询平台
交互式分析平台-Zeeplin
离线模型平台
机器学习MLlib
Spark Streaming
基础服务
BS Profile
B/W/G List
Risk Control Lock
数据层
终端控制层-基础数据
衍生数据-员工画像
衍生数据-系统画像
基础控制层
账户认证
权限认证
门禁与考勤
系统访问控制
上网行为
终端HDLP
邮件DLP
数据脱敏与加密
文件打印
邮件DLP
IM监控
水印跟踪
行程管理
人脸识别等

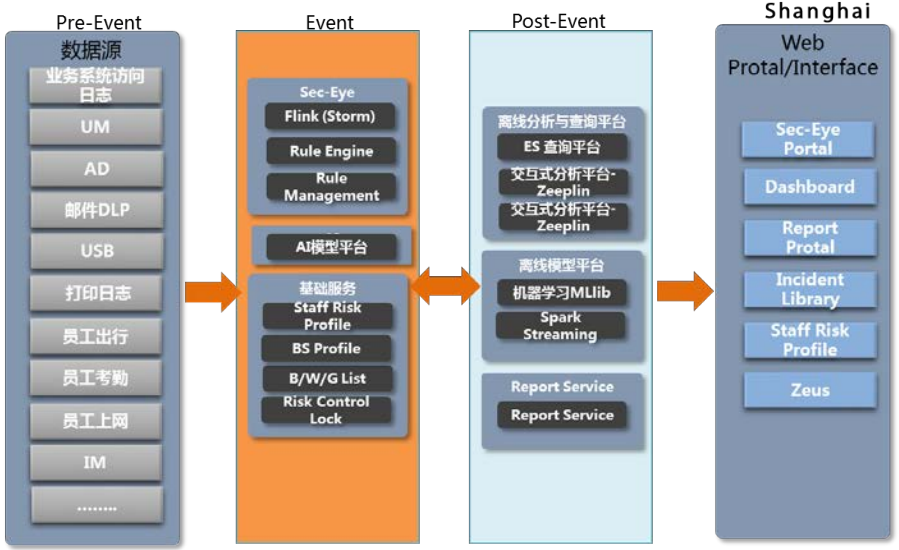
员工风险看板平台架构


Staff Data
AD
UM
上网行为
员工考勤
邮件DLP
主机 DLP
IM
.....
Windows Host
sidecar
winlogbeat
Configuration
Metrics MetricBeat
Network Data PacketBeat
Application Log4j
MessageQueue Logstash
Device Syslog
LOG Messages
FileBeat
Sidecar
Configuration
Linux Host
System Log/Web Accesss
Rest API
Inputs
KafkaJournal
Stream
Outputs
Rest API
Indices
Elasticsearch Realtime
Elasticsearch Online
Archive
Sec Kafka
Sec Flink
AI模型平台
风控锁服务
Alert
Report
Dashboard
员工风险看板Portal
Data Portal
HBASE
离线分析平台
离线模型
集团安全
监察部门
专业公司一线

架构调整

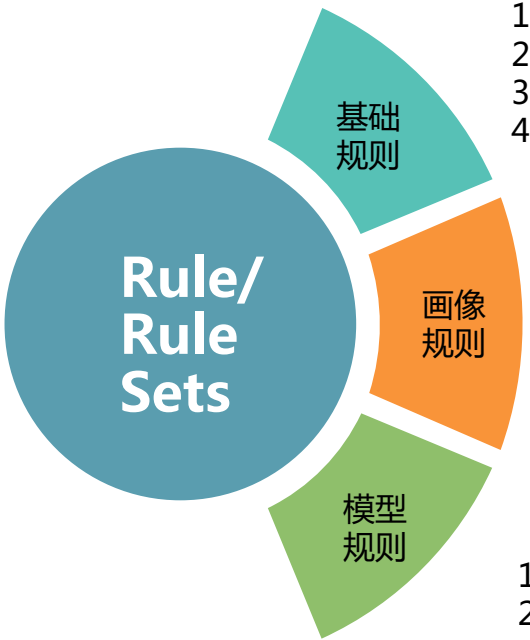


Framwork 1.0



Framwork 2.0

规则引擎-规则类型



1、单位时间内流量规则
2、多场景的组合关联规则
3、匹配规则
4、复杂规则（自定义条件匹配类）

1、员工画像规则: 如常用设备、员工常出入职场、员工工作时长、员工在岗状态、离职倾向、系统访问频度等
2、系统画像规则：系统所属公司、访问量、访问高峰、访问频率、应用访问类型、活跃用户数量区间、用户分布区域等

1、在线模型规则
2、离线模型分析

画像服务的应用

- 业务系统画像

  业务系统访问量、访问用户属性、访问用户量、访问区域等以标签方式进行抽象描述

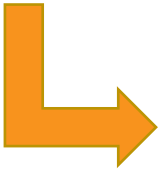
- 员工风险画像

  将员工的自然属性、社会属性、工作习惯、访问习惯、兴趣度等以标签方式进行抽象描述

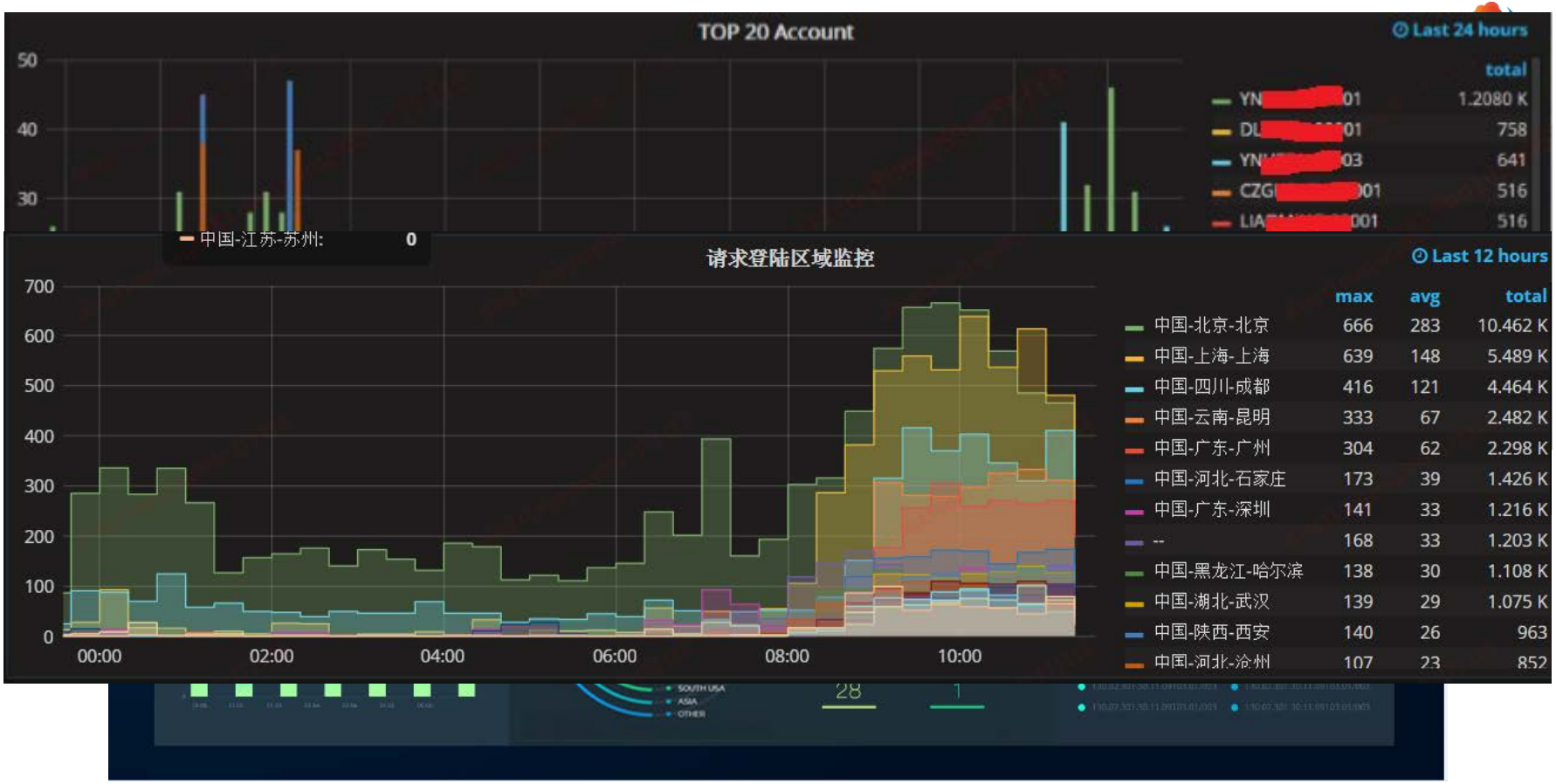
应用举例：
AD账户监控： 现有规则所用的数据维度，登陆时间、登陆IP、登陆账号、登陆状态、账号锁定或修改密码的操作行为

应用举例：
AD账户监控： 现有规则所用的数据维度，登陆时间、登陆IP、登陆账号、登陆状态、账号锁定或修改密码的操作行为

监控规则：
1）单位时间内的同一账号的认证次数
2）单位时间内同一IP访问不同账号的认证次数
3）单位时间内不同IP同一账号的认证次数
4）单位时间内同IP的认证失败次数
5）单位时间内同IP不同账号的密码修改次数
6）非工作时间段的账号认证频度及次数（基于整体AD用户，而非个人属性）
7）离职员工的账号登陆认证成功监控等



通过画像产生的衍生规则：
1）基于每个员工的工作时长、勤奋指数的规则
2）常用设备、IP、主机、职场区域、常登陆系统等的监控规则
3）离职倾向指数超高的员工行为监控
4）基于涉敏指数的员工高风险监控等


TOP 20 Account
Last 24 hours
total
50
40
30
中国-江苏-苏州: 0
请求登陆区域监控
Last 12 hours
max avg total
中国-北京-北京 666 283 10.462 K
中国-上海-上海 639 148 5.489 K
中国-四川-成都 416 121 4.464 K
中国-云南-昆明 333 67 2.482 K
中国-广东-广州 304 62 2.298 K
中国-河北-石家庄 173 39 1.426 K
中国-广东-深圳 141 33 1.216 K
-- 168 33 1.203 K
中国-黑龙江-哈尔滨 138 30 1.108 K
中国-湖北-武汉 139 29 1.075 K
中国-陕西-西安 140 26 963
中国-河北-沧州 107 23 852
700
600
500
400
300
200
100
0
00:00
02:00
04:00
06:00
08:00
10:00

目录

- 技术内番外
  - 架构平滑切换-适应业务场景
  - 数据维度-数据资料的再加工
- 技术外番外
  - 技术之外安全人员关注重点
    - 安全思维/业务思维 冲突
    - 打开双赢局面：业务需求为导向，寻求平衡及角色转换
    - 安全人员：价值输出

想第一时间看到
高效运维社区公众号
的好文章吗？

请打开高效运维社区公众号，点击右上角小人，如右侧所示设置就好