



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





GOPS2017
Shanghai

董晓琼

携程旅行网-信息安全总监
平安科技- 安全平台部



GOPS2017
Shanghai

目录



1

企业内部风险

2

解构-升维与降维

3

员工风险识别框架

4

技术内外的安全思考

企业风险聚焦



GOPS2017
Shanghai



员工风险

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。

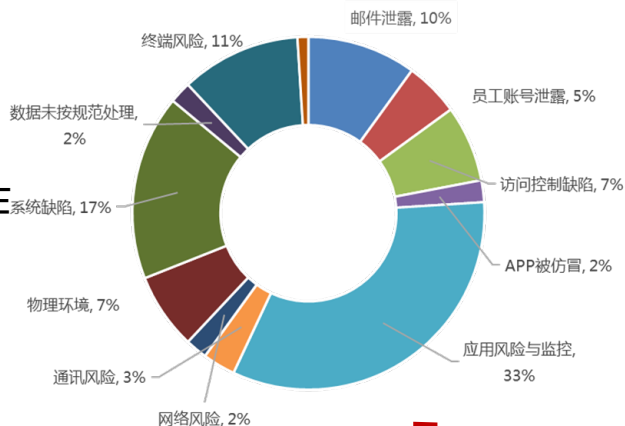
行业内迫切度、重要度

- 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

内部驱动

误操作
利用
滥用
违规

驱动力





GOPS2017
Shanghai

目录

1 企业内部风险

➔ 2 解构-升维与降维

3 员工风险识别框架

4 技术内外的安全思考

多维解构

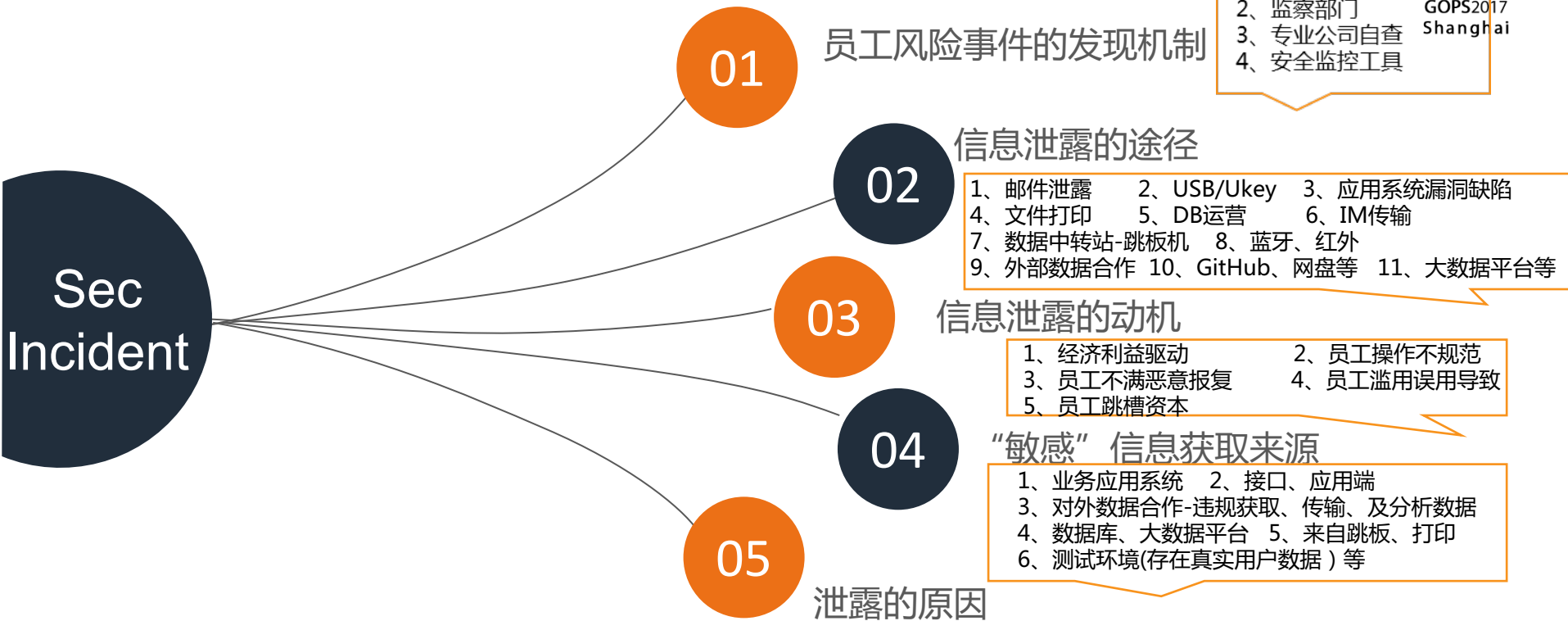


GOPS2017
Shanghai





GOPS2017
Shanghai





GOPS2017
Shanghai

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

基础管控手段：

- 基础控制在泄露途径上的覆盖
- 部署灵活性、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

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

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

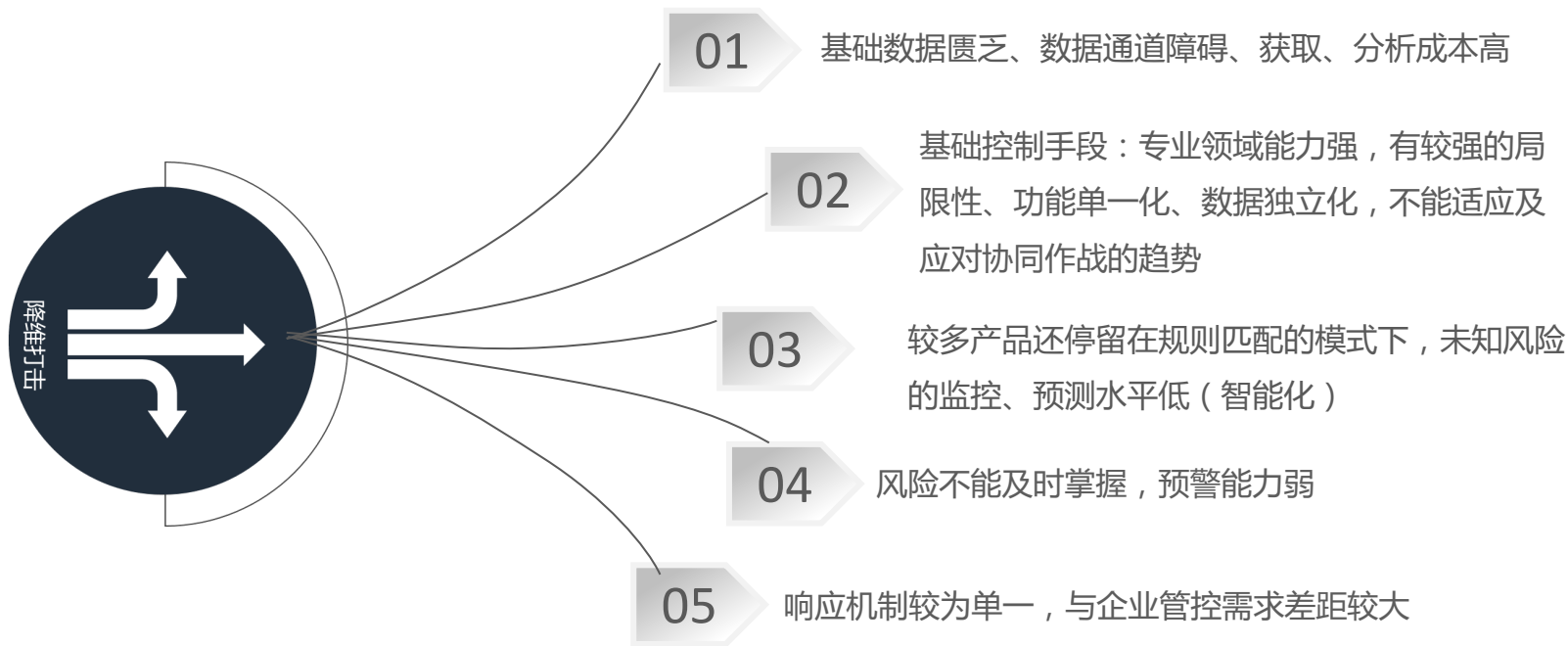
基础管控能力：

- 检测规则-分析和运营
- 全局、一线安全运营现状

现状



GOPS2017
Shanghai





GOPS2017
Shanghai

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；



GOPS2017
Shanghai

目录

1 企业内部风险

2 风险解构-升维与降维

➔ 3 员工风险识别框架

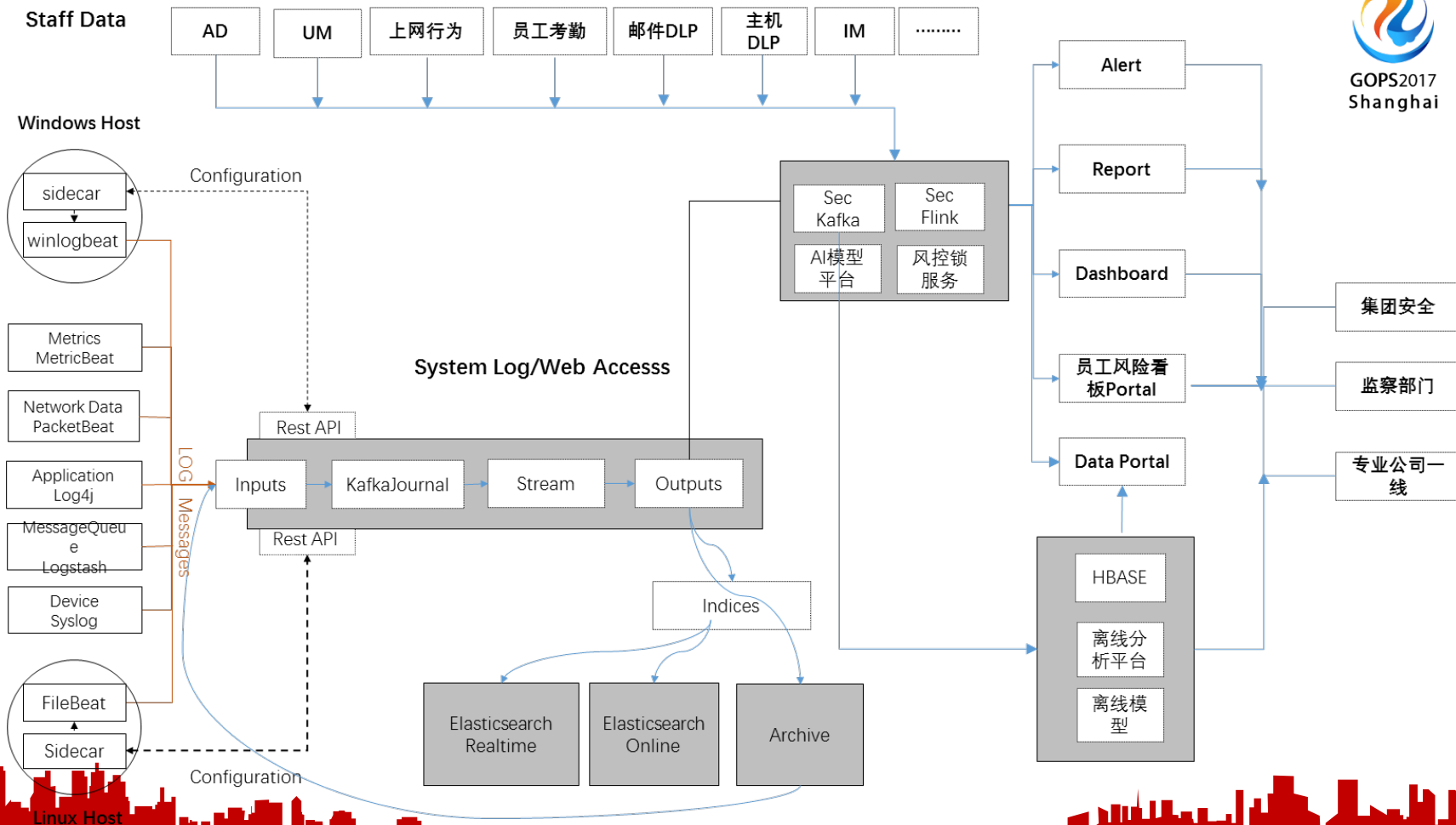
4 技术内外的安全思考

员工风险识别框架



GOPS2017
Shanghai

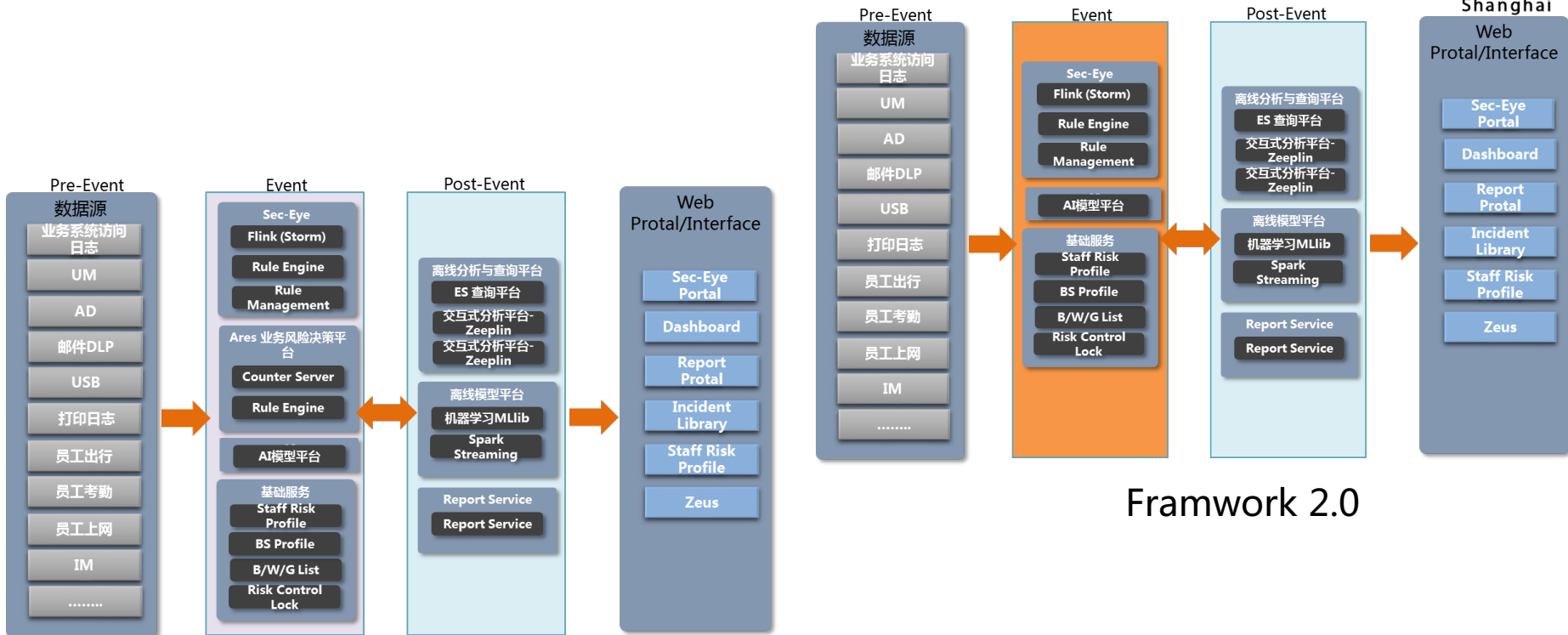




架构调整



GOPS2017
Shanghai
Web
Protal/Interface



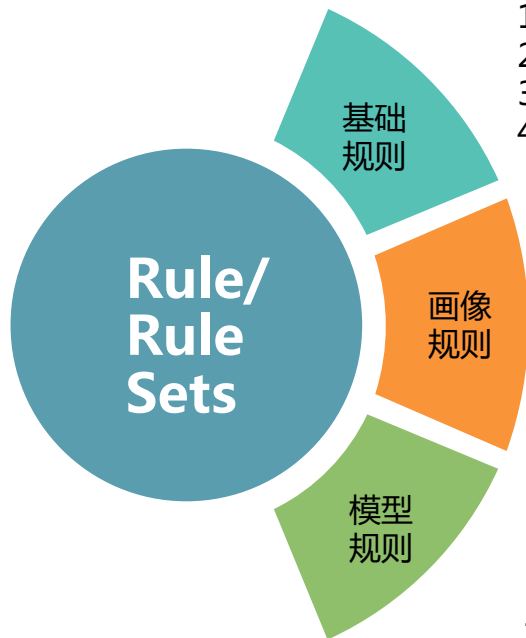
Framework 2.0

Framework 1.0

规则引擎-规则类型



GOPS2017
Shanghai



- 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



GOPS2017
Shanghai

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

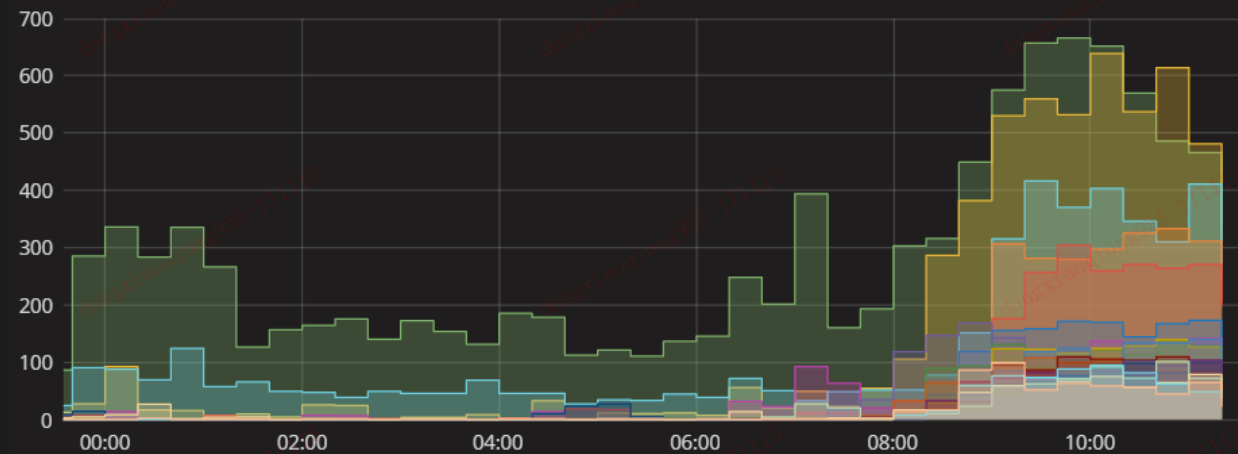
◎ Last 24 hours



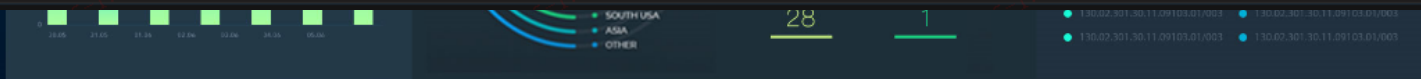
	total
YN [redacted] 01	1.2080 K
DL [redacted] 01	758
YN [redacted] 03	641
CZG [redacted] 001	516
LIA [redacted] 001	516

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





GOPS2017
Shanghai

目录

1 企业内部风险

2 风险解构-升维与降维

3 员工风险识别框架

➔ 4 技术内外的安全思考



GOPS2017
Shanghai

- 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



GOPPS2017
Shanghai



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

