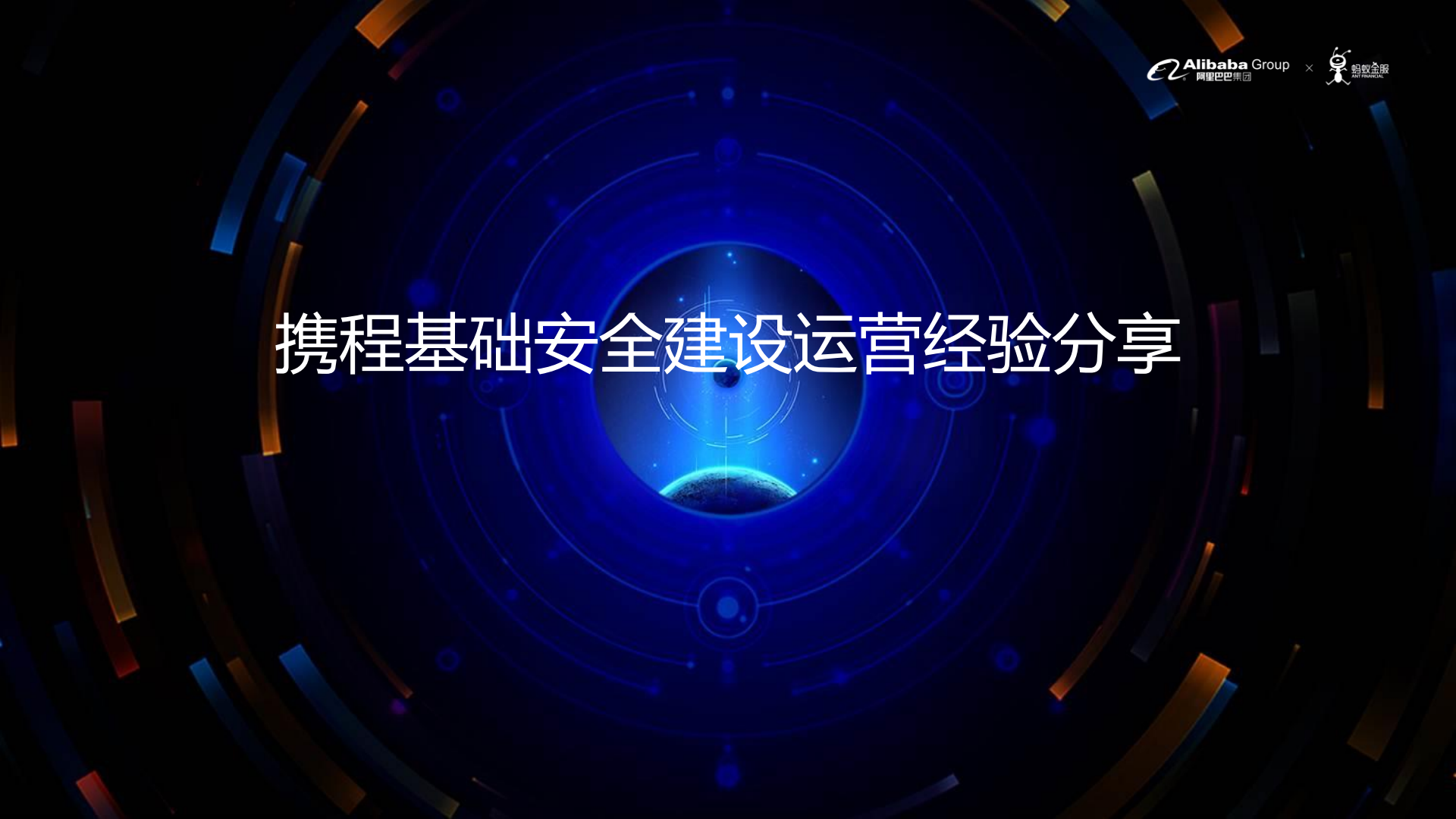

Alibaba Group
阿里巴巴集团
×
蚂蚁金服
ANT FINANCIAL
携程基础安全建设运营经验分享

目录

范围目标

风险识别

体系建设

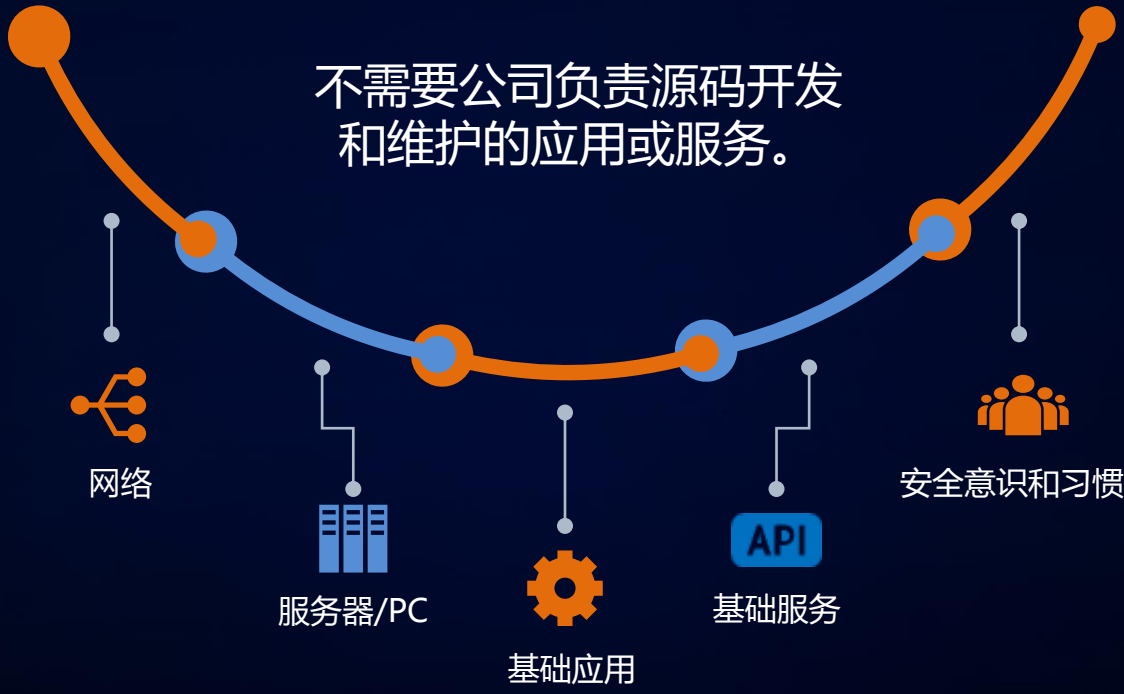
我们已实现的

我们将要做的

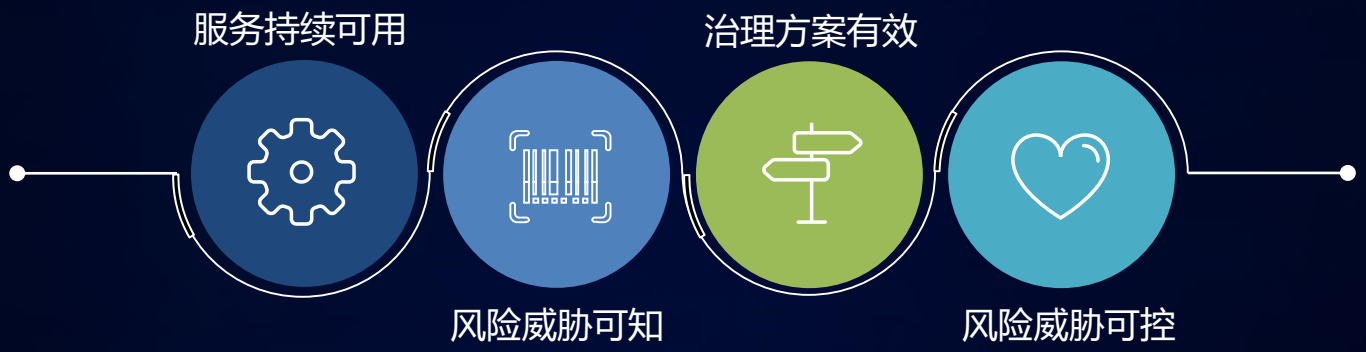
范围和目标

基础环境的范围及其安全目标。

基础安全范围



基础安全目标



降低内外部威胁对基础环境的影响，增强其服务持续可用的属性。

风险识别

基础环境中存在的安全风险点。

风险

内部风险

意识：安全规范基准缺乏
习惯：高风险操作、违规越权、数据泄漏

服务：不安全配置、权限不当、弱口令、关键日志

应用：漏洞、不安全配置、弱口令
权限：权限不当

OS：漏洞、补丁、帐号权限、弱口令、恶意程序、webshell
远程：漏洞、远程管理卡、桌面、命令终端、认证授权

设备：弱口令、漏洞、不安全配置、权限管控不当
边界：策略不当、策略失效、安全例外

外部威胁

体系建设

基础环境中已识别的安全风险，通过有效的治理和监控方案以及安全事件响应流程，实现基础安全的目标。

体系运营

规范基准

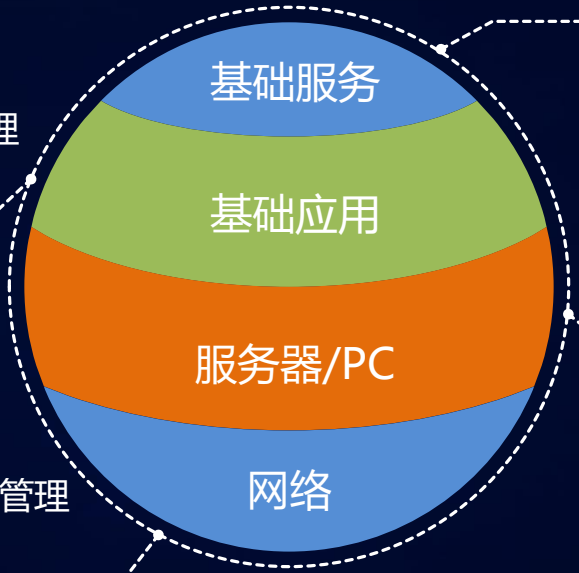
培训分享

威胁情报

事件响应

检测监控

基准规范



- ✓ 安全基线
- ✓ 帐号和漏洞补丁管理
- ✓ 关键日志异地集中

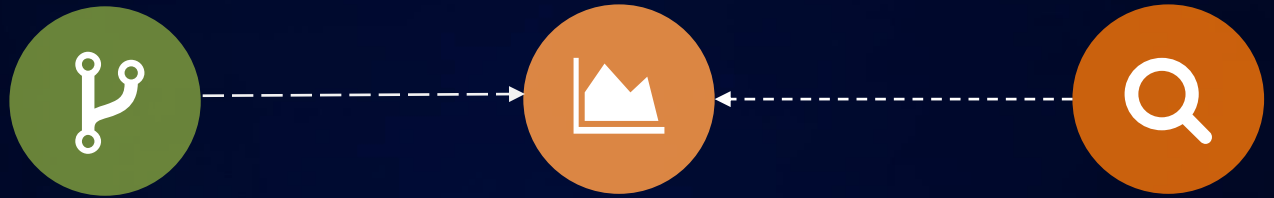
- ✓ 安全基线
- ✓ 接口授权
- ✓ 关键日志异地集中

- ✓ 安全基线
- ✓ 帐号和漏洞补丁管理
- ✓ 边界和策略
- ✓ 关键日志异地集中

- ✓ 安全基线
- ✓ 漏洞补丁管理
- ✓ 防病毒
- ✓ 帐号管理
- ✓ 关键日志异地集中

威胁情报

检测监控



网络和流量

- ✓ 内外边界日志
- ✓ 公网端口扫描
- ✓ 跨边界流量检测
- ✓ 核心内网横向流量检测
- ✓ 内外网埋点蜜罐

事件监控

- ✓ 基础环境日志
- ✓ 频率
- ✓ 单维度安全类别事件件
- ✓ 多维度关联

扫描器

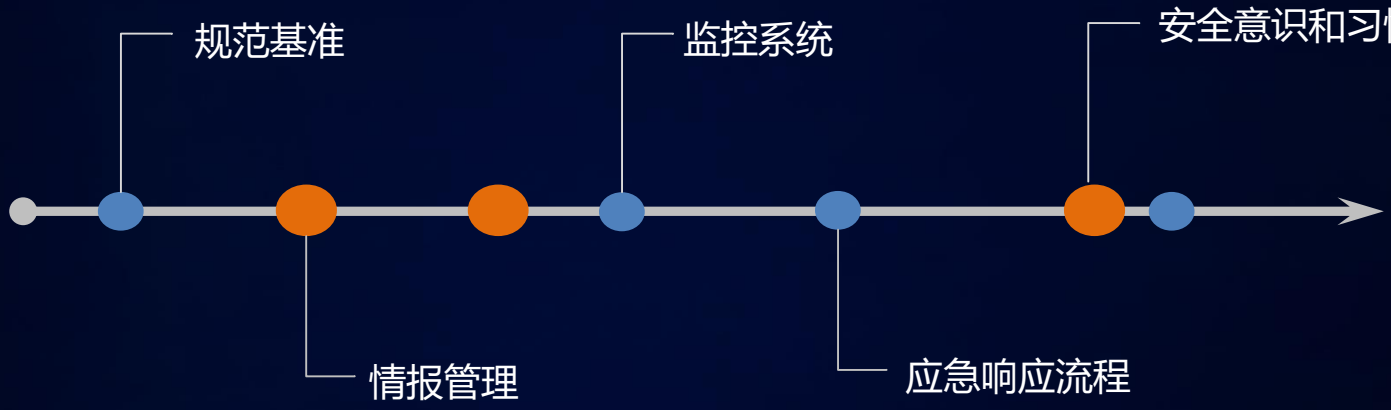
- ✓ 指纹
- ✓ 弱口令
- ✓ 漏洞
- ✓ 授权

事件响应

培训分享

良好的安全意识和习惯

体系运营

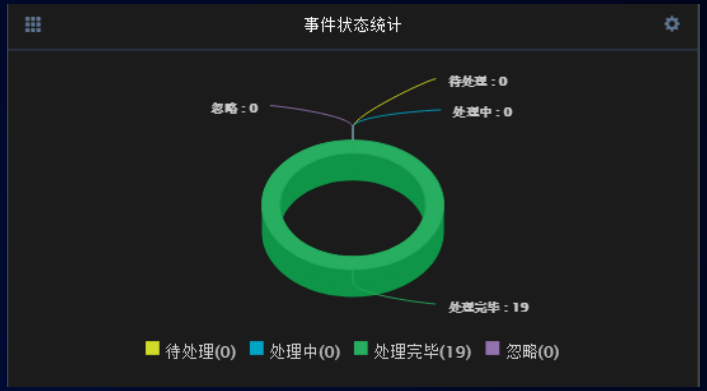


我们已经实现的

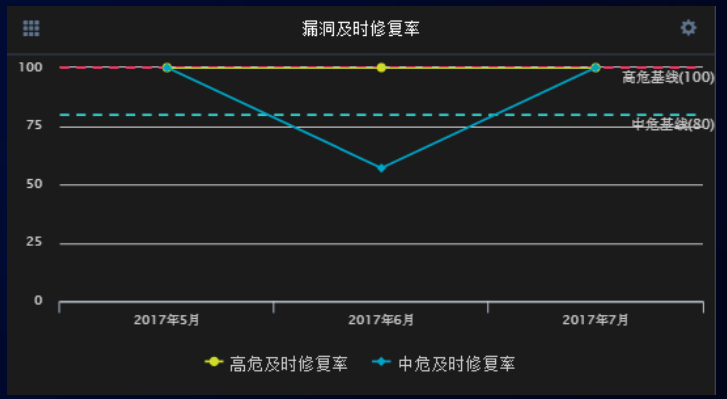
简要分享携程基础安全建设已实现的内容。

SOC

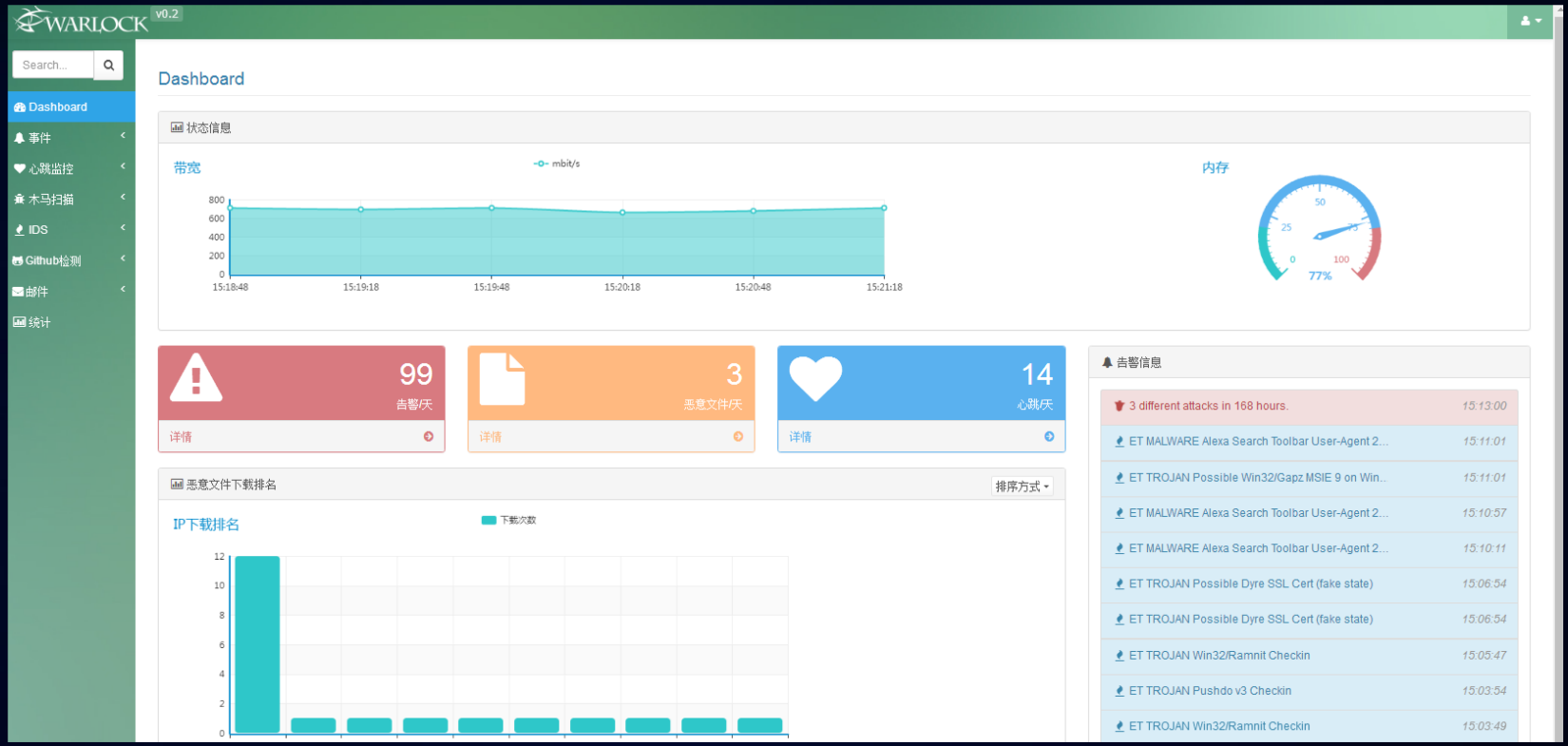

安全威胁状态
0
2
4
6
8
0
10
风险低
2017-07-24 17:54:13[idc-linux]
ip(10)10分钟内登录失败8次
2017-07-24 14:21:13[idc-mhn]
sourceip( )5分钟内发起内网攻击19次
2017-07-24 19:02:13[it-webmail]
webmail IP( ) 30s内登录错误用户数超过4个


事件状态统计
待处理 : 0
忽略 : 0
处理中 : 0
处理完毕 : 19
待处理(0)
处理中(0)
处理完毕(19)
忽略(0)


安全事件分布
it-windows
idc-linux
it-webmail
idc-windows
it-vpn
idc-ossec
idc-mhn (7)
idc-mhn
idc-nids
portscanner


漏洞及时修复率
100
75
50
25
0
高危基线(100)
中危基线(80)
2017年5月
2017年6月
2017年7月
高危及时修复率
中危及时修复率

APT

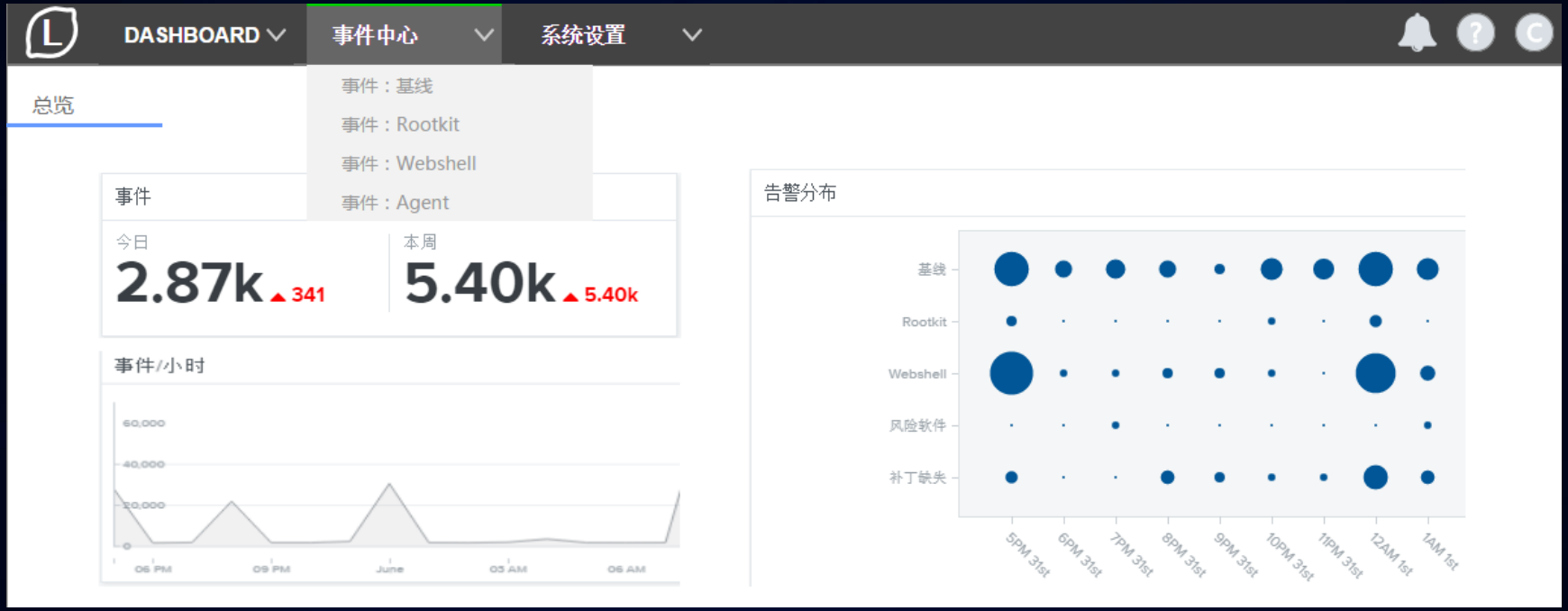

WARLOCK v0.2
Search...
Dashboard
事件
心跳监控
木马扫描
IDS
Github检测
邮件
统计
Dashboard
状态信息
带宽
mbit/s
800
600
400
200
0
15:18:48
15:19:18
15:19:48
15:20:18
15:20:48
15:21:18
内存
50
25
75
0
100
77%
99
告警/天
详情
3
恶意文件/天
详情
14
心跳/天
详情
告警信息
3 different attacks in 168 hours. 15:13:00
ET MALWARE Alexa Search Toolbar User-Agent 2... 15:11:01
ET TROJAN Possible Win32/Gapz.MSIE 9 on Win.. 15:11:01
ET MALWARE Alexa Search Toolbar User-Agent 2... 15:10:57
ET MALWARE Alexa Search Toolbar User-Agent 2... 15:10:11
ET TROJAN Possible Dyre SSL Cert (fake state) 15:06:54
ET TROJAN Possible Dyre SSL Cert (fake state) 15:06:54
ET TROJAN Win32/Ramnit Checkin 15:05:47
ET TROJAN Pushdo v3 Checkin 15:03:54
ET TROJAN Win32/Ramnit Checkin 15:03:49
恶意文件下载排名
排序方式
IP下载排名
下载次数
12
10
8
6
4
2
0

我们将要做的

携程基础安全体系的实际思考反思以及后续我们将去实现的内容。

反思：
当前安全体系的规划建设和运营，能有效治理当前基础环境的安全风险，为基础环境的可用性和安全性提供保障。对于实际基础环境中，数据处理的最小运算环境（主机、容器）的实时安全性如何保障？

To Do：
✓ 在不断完善当前安全体系建设的基础上，自研Luhn-HIDS


DASHBOARD
事件中心
系统设置
事件：基线
事件：Rootkit
事件：Webshell
事件：Agent
总览
事件
今日
2.87k
341
本周
5.40k
5.40k
事件/小时
60,000
40,000
20,000
0
06 PM
09 PM
June
03 AM
06 AM
告警分布
基线
Rootkit
Webshell
风险软件
补丁缺失
5PM 31st
6PM 31st
7PM 31st
8PM 31st
9PM 31st
10PM 31st
11PM 31st
12AM 1st
1AM 1st

Thank you