

安世加

Face the challenge, Embrace the best practice

EISS-2021

企业信息信息安全峰会

上海站 2021.11.19



Security Operations Center

企业自建SOC安全运营的探索实践

合合信息 廖超豪

安全运营-落实企业安全管理和治理目标

安全设备

安全漏洞

信息资产

安全需求

数据合规

知识库

应急响应

安全运营 ≠ 安全运维

随着企业安全建设进入一定阶段的时候，安全运营就显得尤为重要，安全运营常被认为是落实企业安全管理和治理目标的重要途径，那么安全运营到底都需要运营些什么呢？

SOC-落地安全运营的靠谱工具



建设思路-分阶段交叉同步建设

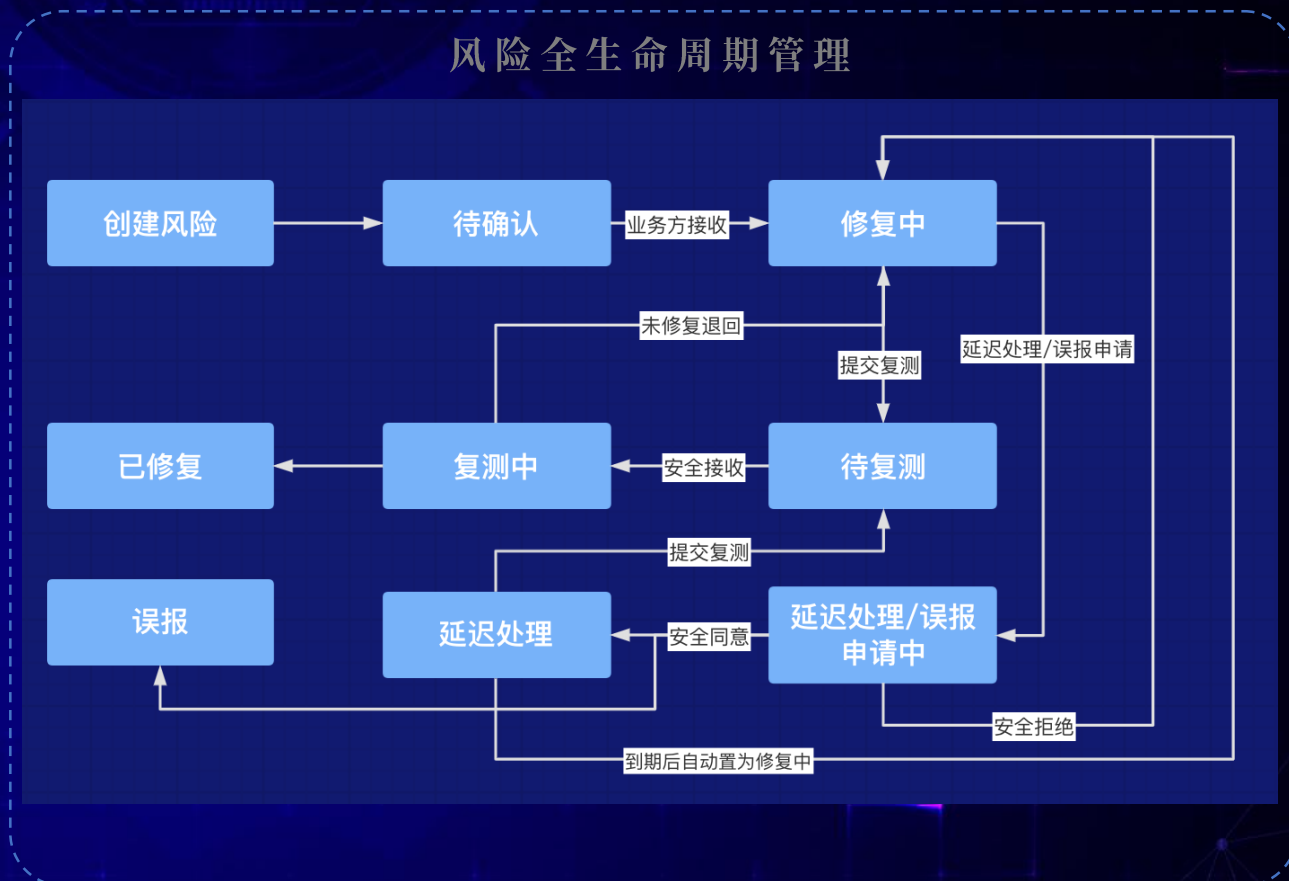
平台化建设

安全点位联动

智能化运营

高扩展和可持续性建设

平台化建设-工单&资产&风险全生命周期管理



INTSIG安全运营中心

风险管理-让系统替人跟进风险

➤ 风险超时未接受，系统催办



➤ 风险逾期未修复，系统催办



➤ 风险逾期未复测，系统催办



高危及以上风险关键节点系统自动抄送业务部门负责人

所有风险逾期未修复，系统自动抄送业务部门负责人

安全工单-通过安全服务提升企业安全性

INTSIG 安全运营中心

工单管理 / 全部工单

筛选面板

工单列表

工单名称	工单类型	业务线	创建人	处理人	处理状态	创建时间	完成时间	测试字段1	测试字段2	测试字段3	操作
定时工单提醒测试	其他测试	安全与合规			● 处理中	2021-11-17 09:37:18	--	--	--	--	完成 更多
测试	SDK安全检测	安全与合规			● 处理中	2021-11-15 10:50:09	--	--	--	--	完成 更多
测试1	SDK安全检测	安全与合规			● 处理中	2021-11-11 18:06:23	--	--	--	--	完成 更多
测试工单2	专项安全测试	安全与合规			● 处理中	2021-11-11 18:06:23	--	--	--	--	完成 更多
测试工单3	材料说明	安全与合规			● 处理中	2021-11-11 18:06:23	--	--	--	--	完成 更多
测试工单4	安全意识培训	安全与合规			● 处理中	2021-11-11 18:06:23	--	--	--	--	完成 更多
测试工单5	安全技术培训	安全与合规			● 处理中	2021-11-11 18:06:23	--	--	--	--	完成 更多
测试工单6	源代码硬编码扫描	安全与合规			● 处理中	2021-11-11 18:06:23	--	--	--	--	完成 更多
测试工单7	资质证书	安全与合规			● 处理中	2021-11-11 18:06:23	--	--	--	--	完成 更多

共148项 < 1 2 3 4 5 ... 15 > 10条/页 跳至 页

意见反馈

平台共支持安全测试、合规评估、安全调研等50+种工单类型供业务方选择

安全工单-通过安全服务提升企业安全性

工单管理 / 添加工单

测试类工单

* 工单类型: 安全测试-合规检测

* 工单名称:

▼ 安全测试

* 业务线: 合规检测

* 测试域名:

* 测试账号:

版本迭代测试

SDK安全检测

APP合规检测


APP加固测试

专项安全测试

抄送: 选择抄送人

需求说明:

文件 编辑 插入 格式

B *I* U ~~S~~ sans-serif 12pt A 

工单管理 / 添加工单

非测试类工单

* 工单类型: 选择工单类型

* 工单名称:

* 业务线:

抄送:

需求说明:

- ▶ 安全培训
- ▶ 合规材料
- ▶ 合规评估
- ▶ 资质认证
- ▶ 安全加固
- ▶ 安全报告需求
- ▶ 安全调研
- ▶ 安全运营

▼ A 

安全工单-提升用户体验



安全工单-增加应用场景

INTSIG 安全运营中心

工单列表 定时工单提前录入，到期提醒 导出

工单名称	工单类型	业务线	创建人	处理人	处理状态	创建时间	操作
2022年一月合小安合规期刊	合小安合规期刊	安全与合规		--	待接收	2021-11-11 19:58:01	接收 更多
2022年二月合小安合规期刊	合小安合规期刊	安全与合规		--	待接收	2021-11-11 19:58:01	接收 更多
2022年三月合小安合规期刊	合小安合规期刊	安全与合规		--	待接收	2021-11-11 19:58:01	接收 更多
2022年四月合小安合规期刊	合小安合规期刊	安全与合规		--	待接收	2021-11-11 19:58:01	接收 更多
2022年五月合小安合规期刊	合小安合规期刊	安全与合规		--	待接收	2021-11-11 19:58:01	接收 更多
2022年六月合小安合规期刊	合小安合规期刊	安全与合规		--	待接收	2021-11-11 19:58:01	接收 更多
2022年七月合小安合规期刊	合小安合规期刊	安全与合规		--	待接收	2021-11-11 19:58:01	接收 更多
2022年八月合小安合规期刊	合小安合规期刊	安全与合规		--	待接收	2021-11-11 19:58:01	接收 更多
2022年九月合小安合规期刊	合小安合规期刊	安全与合规		--	待接收	2021-11-11 19:58:01	接收 更多

< 1 2 3 4 > 40条/页 跳至 页

意见反馈

安全运营中心

Hi, [用户名]

定时工单已到达处理时间，请及时接收，详情如下：

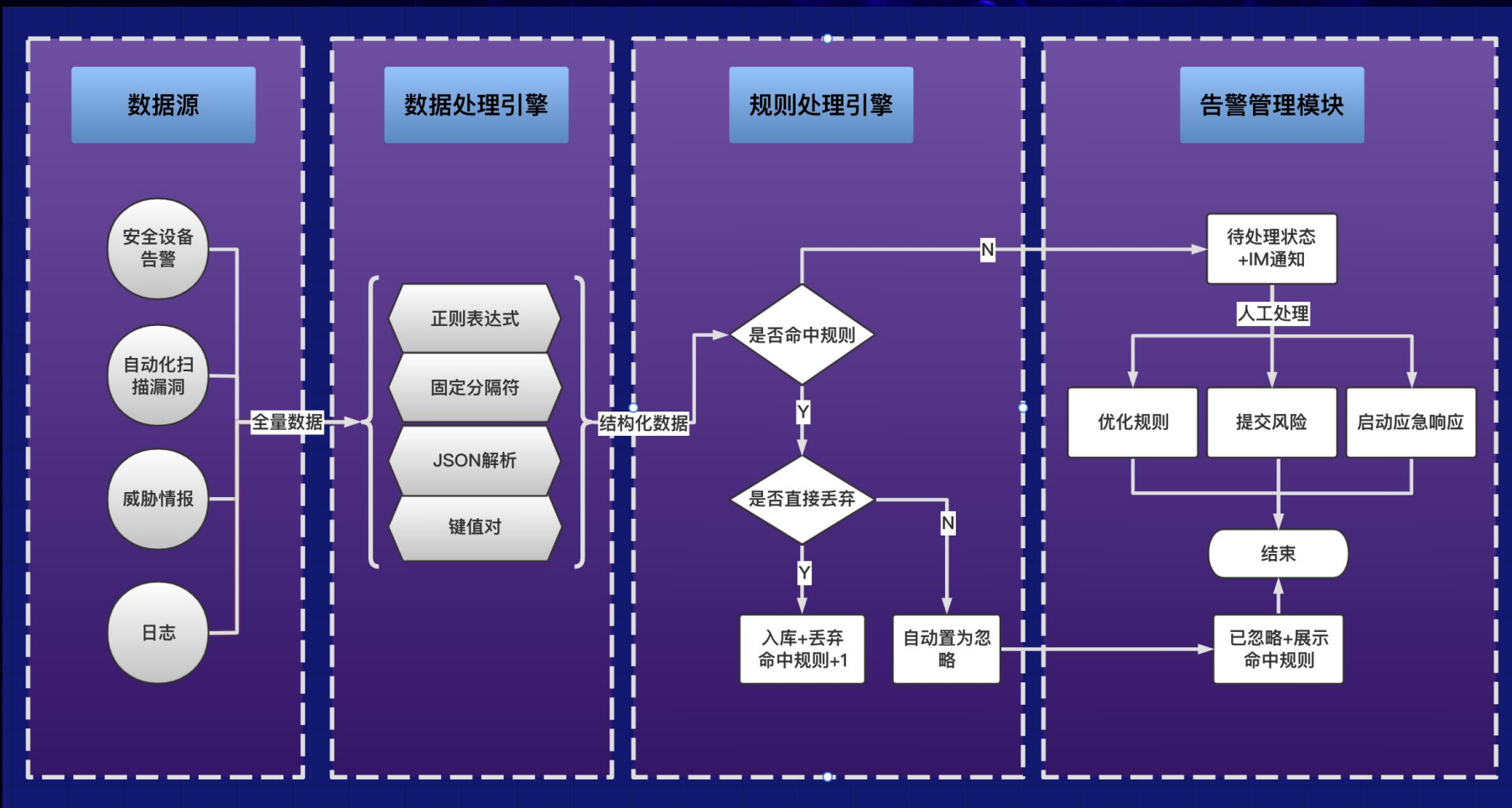
工单名称：[工单名称]
业务线：[业务线]
创建人：[创建人]
处理时间：2021-11-27 15

[点击查看详情](#)

[不想接收该系统邮件消息？点此设置](#)

服务于公司各业务线的安全管理系统，实现安全风险的全生命周期响应管理。链接地址：[链接地址]

安全点位联动-注册制&数据范式处理



- 插件式注册接入，保证用户端充分灵活
- 全量数据范式处理，保证安全点位高扩展性
- 告警分类匹配半自动处理，避免海量告警淹没
- 全量信息入库，保证真实告警不丢失

安全点位联动-点位&规则可持续运营

INTSIG 安全运营中心

告警管理 / 安全点位管理

告警管理

安全点位列表

ID	名称	责任人	操作
29			编辑 删除 查看字段
28			编辑 删除 查看字段
15			编辑 删除 查看字段
5			编辑 删除 查看字段
4			编辑 删除 查看字段

注册安全点位

* 名称: 请填写名称

类型: 请填写类型

回调地址: 请填写回调地址

风险来源: 请选择风险来源

风险类型: 请选择风险类型

* 责任人: 请选择责任人

+ 添加告警字段

字段展示名称 字段存储名称 X

取消 确定

共5项 < 1 > 10条/页

意见反馈

注册

安全点位联动-点位&规则可持续运营

INTSIG 安全运营中心

告警管理 / 规则管理

平台: 请选择

规则列表

ID	平台	名称	命中次数	直接丢弃	操作
73		进程名	3	否	编辑 删除 查看规则
72		dba团	8	否	编辑 删除 查看规则
71		pytho	5	否	编辑 删除 查看规则
70		pytho	78	否	编辑 删除 查看规则
69		html文	22	否	编辑 删除 查看规则
68		txt文件	128	否	编辑 删除 查看规则
67		json文件	238	否	编辑 删除 查看规则

添加规则

* 平台: 请选择平台

* 名称: 请填写名称

* 描述: 请填写描述

* 直接丢弃: 是 否

+ 添加正则表达式

请选择字段 | 正则表达式

取消 确定

新建

查询 重置

意见反馈

安全点位联动-点位&规则可持续运营

INTSIG 安全运营中心

告警管理 / 规则管理 新建

平台: 查询 重置

规则列表

ID	平台	名称	描述	命中次数	直接丢弃	操作
73	双限监控	测试进程名忽略	确认改进程名非敏感应用, 无风险	3	否	编辑 删除 查看规则
72	双限监控	测试的python进程	非提供web等服务的python进程, 确认无...	8	否	编辑 删除 查看规则
71	双限监控	测试python爬虫进程	非提供web等服务的python进程, 确认无...	5	否	编辑 删除 查看规则
70	双限监控	测试python爬虫进程	非提供web等服务的python进程, 确认无...	78	否	编辑 删除 查看规则
69	安全监控	测试html文件	html文件	22	否	编辑 删除 查看规则
68	安全监控	测试txt文件	txt文件	128	否	编辑 删除 查看规则
67	安全监控	测试json文件	json文件	238	否	编辑 删除 查看规则

[意见反馈](#)

智能化运营-基于平台&数据&规则探索运营模式



智能化运营-业务方安全建模

基于SOC平台的元数据，参考CVSS等专业安全模型，通过5个维度，20+项衡量标准，并且以向上延申一个季度为梯度进行建模，加权计算出各业务线在指定的时间内最终的综合安全系数及各个维度安全状况分布，以此反映各业务线该周期内的整体安全态势。

- 业务安全：主要从安全漏洞视角，根据业务线周期内各类测试及漏洞情况按照公式加权计算出最终分值；
- 应急响应：主要根据业务线周期内是否存在安全事件、漏洞逾期、专项整改等维度进行加权计算出最终分值；
- 监管合规：主要根据业务线周期内是否存在内外部合规隐患事件进行加权计算出最终分值；
- 安全防护：主要根据业务线周期内安全防护设备或安全防护机制覆盖率及有效性等情况计算出最终分值；
- 第三方评估：主要根据第三方专业安全工具进行应用漏洞、SSL健壮性、网站有效性等检测结果进行相关计算得出最终分值；



智能化运营-专项治理

安全运营中心

Hi,

近期多次出现“设计缺陷/逻辑错误”相关的漏洞，按照专项行动治理启动规则，安全团队和业务方将一起配合启动“设计缺陷/逻辑错误”类问题专项治理行动，详情如下：

专项治理名称：启信宝个人版第四季度测试

业务线：

实施方式： 1) 启动专项治理行动后，业务方梳理所有相关功能接口进行白盒代码Review；

2) 同时将这些接口通过安全运营中心提交安全测试，由安全团队对这些接口进行全面的黑盒测试；

历史漏洞：

工单名称	风险名称	风险等级	风险状态	风险类型	风险处理人	风险责任人	安全检测人	业务线	风险来源
		中危	已修复	设计缺陷/逻辑错误					安全团队
		中危	已修复	设计缺陷/逻辑错误					ISRC
		中危	已修复	设计缺陷/逻辑错误					安全团队
		中危	已修复	设计缺陷/逻辑错误					安全团队

创建人：

启动时间：2021-

专项行动治理规则详细如下：

启动规则：各业务线在1个自然年内相同类型中危及以上漏洞出现3次及以上启动专项治理行动；

实施方式：

1) 启动专项治理行动后，业务方梳理所有相关功能接口进行白盒代码Review；

2) 同时将这些接口通过安全运营中心提交安全测试，由安全团队对这些接口进行全面的黑盒测试；

漏洞后续跟踪：

1) 在1个自然年内，若经过专项治理行动的漏洞类型在同一产品再次出现，则由安全团队对该业务所有相关研发人员进行一次整体的专项培训，同时业务方需全面分析再次出现的原因，并将原因分析通过填写复盘报告邮件抄送该产品线及安全团队leader；

➤ 基于SOC的应用漏洞数据，同一业务线在1个自然年内相同类型中危及以上漏洞出现3次及以上即启动专项治理行动；

➤ 专项治理行动由业务方和安全团队共同配合完成；

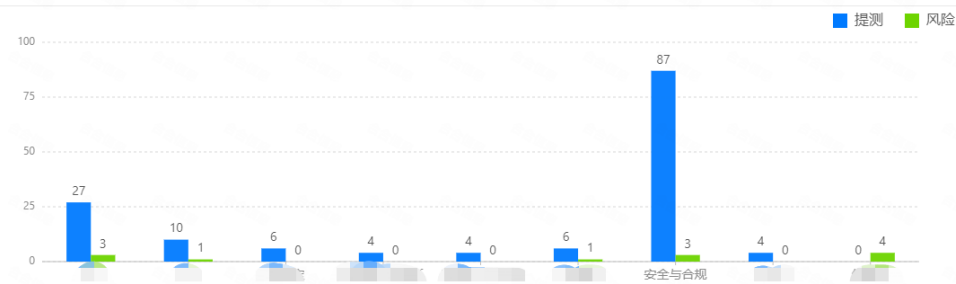
➤ 经过专项治理后若仍继续发生，则需进行专项安全培训+深度复盘；

智能化运营-态势分析

测试环境用于演示，非真实数据

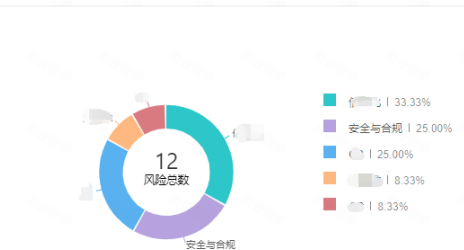
业务线提测/风险分布

2021/08/17 ~ 2021/11/17



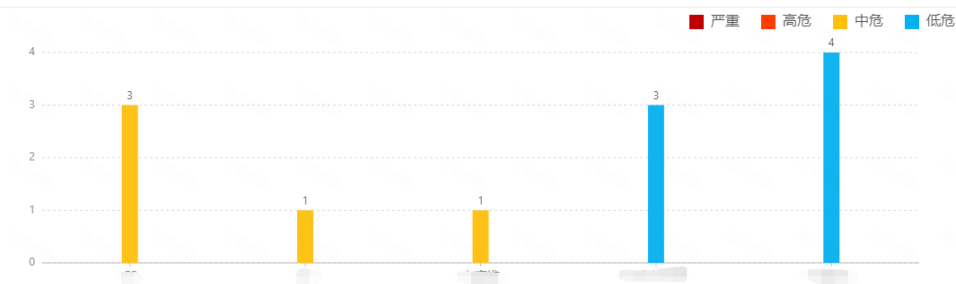
业务线风险占比

2021/08/17 ~ 2021/11/17



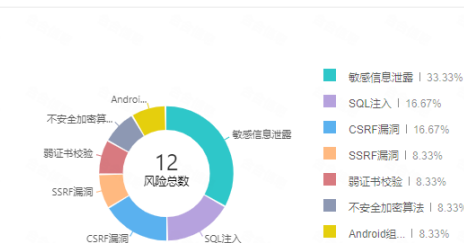
业务线风险分布

2021/08/17 ~ 2021/11/17



风险类型占比

2021/08/17 ~ 2021/11/17

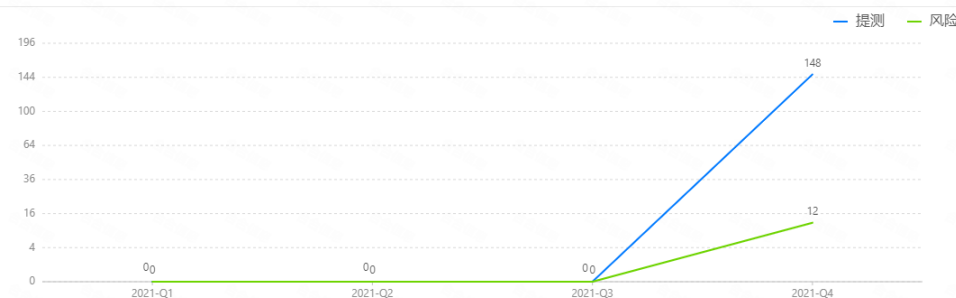


业务线提测/风险趋势

2021/01 ~ 2021/12

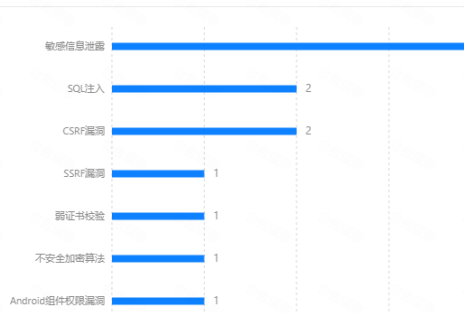
全部业务

按月份 按季度



风险类型Top10

2020/11/18 ~ 2021/11/18



- 业务线提测/风险分布
- 业务线风险占比
- 业务线风险分布
- 风险类型分布
- 业务线提测/风险趋势
- 风险类型Top10

智能化运营-安全巡检机器人

资产监控 BOT

公司资产概况

时间: 2021年 月 日
服务器: 个
机房分布:
1902
其他: 446
下线: 27 个
新增: 32 个
[查看更多>>](#)

域名: 个
下线: 0 个
新增: 1 个
域名: api-her.com
WAF状态: 已部署
责任人:
WAF 部署情况: 9/93
[查看更多>>](#)

网站: 个
新增: 1 个
url: https://ai.com
Title:
location: 无
CSP状态: 已部署
责任人:
漏洞数量: 12 个
CSP 部署情况:
[查看更多>>](#)

资产监控 BOT

外网IP高危端口及服务

今日共发现高危端口 4 个, 涉及IP 4 个

101. 检测
端口:
服务: mysql
版本: -log

52. 检测
端口:
服务: ftp
版本: 2.2

121. 检测
端口:
服务: ssh
版本: 3

52. 检测
端口:
服务: ssh
版本: .1

[查看更多>>](#)

SOC安全点位监控-测试 BOT

昨日安全点位日报

2021年11月12日

检测
24小时内未收到该点位告警, 判断已离线, 请排查
监控
告警总数: 25

待确认: 3
跟进中: 0
已忽略: 22
已提交风险: 0
已提交工单: 0

告警
该点位还未有告警接入, 请安排处理
监控
24小时内未收到该点位告警, 判断已离线, 请排查
监控
告警总数: 26

待确认: 6
跟进中: 0
已忽略: 20
已提交风险: 0
已提交工单: 0

➤ 基于资产管理模块, 每日对公司全量信息资产进行盘点和安全巡检后, 通过机器人发送消息至安全团队, 再由运营人员判断是否需要对相关风险或异常进行跟进

➤ 对所有接入SOC的告警进行日报统计及异常情况跟进

所有数据均为用于演示的测试环境, 非真实数据

智能化运营-其他场景的运营探索



合小安



昨天 11:00

合小ai

7:22 PM

个人电脑可以用于办公么

- 1 禁止使用私人电脑用于办公
- 2 禁止将私人电脑、私人存储（U盘、移动硬盘等）带入公司
- 3 禁止使用私人电脑、私人存储（U盘、移动硬盘等）保存公司资料
- 4 禁止私人电脑接入公司网络

- 1、员工入职后都会为每一位员工配备办公电脑，请大家在公司办公时使用公司配备的电脑进行办公。
- 2、如因岗位调整、所配电脑使用年限过长等影响办公使用的情况，请通过 OA 《IT 资产领用/采购申请流程》提交申请，经过所属部门审核通过后，IT 将在符合制度规范内为申请人采购/替换新设备。

公司代码可以上传到 github 么

员工工作过程中创造的代码、文档等属于公司财产，禁止任何人员非授权对外公开，如上传到 GitHub、网盘及私自拷贝到个人 U 盘等。

基于SOC的安全体系全景图



感谢聆听

合合安全应急响应中心：

<https://security.intsig.com/>

微信公众号：合合安全应急响应中心



安世加专注于网络安全行业，通过互联网平台、线下沙龙、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，以培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站：

<https://www.anshijia.net.cn>

微信公众号：asjeiss

