互联网公司安全运营

01 安全运营

极客时间

扫码试看/订阅

《Web 安全攻防实战》视频课程

01 安全运营

定义&原理

业务安全

当一个产品功能有缺陷，用户体验极差，甚至整体宕机的时候，是谈不上安全性的，产品自身存活成了主要矛盾，当一个产品其他方面都做的好的时候，安全有可能成为产品的核心竞争力。

定义&原理

业务逻辑安全（逻辑漏洞）

- 登陆认证模块
- 业务办理模块
- 业务授权访问模块
- 输入输出模块
- 回退模块
- 验证码机制
- 业务数据安全
- 业务流程乱序
- 密码找回模块
- 业务接口调用模块

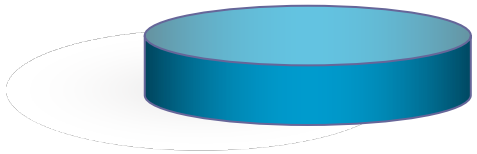
定义&原理

安全运营

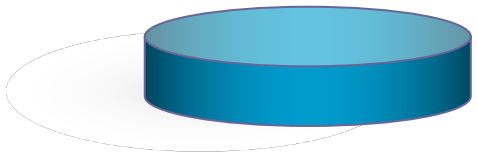
安全运营实践的主要目的是保障系统中资产的安全性，这些实践有助于确定威胁和漏洞，并实施控制来降低整个组织资产的风险。

知其所需&最小特权

极客时间



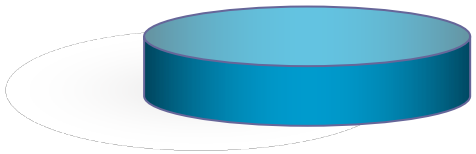
知其所需原则利用需求来给用户授权，仅仅根据为完成所分配任务而授权访问需要操作的数据或资源。



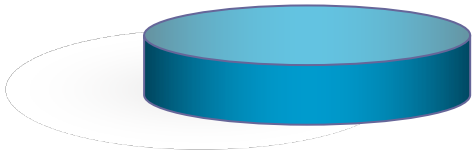
最小特权原则表明主体仅仅被授予执行已分配工作任务的特权，不会拥有超出其工作任务的特权。

职责和责任分离&双人控制

极客时间



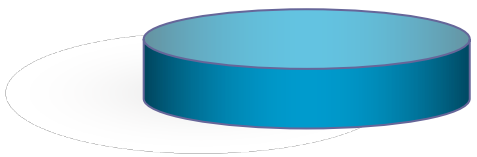
职责和责任分离确保没有人能控制某个关键功能或整个系统，能确保没有单个人能危害到系统和系统的安全性，如果两个或更多人必须共谋或串通，违反组织，这对于这些人增加了被发现的风险。



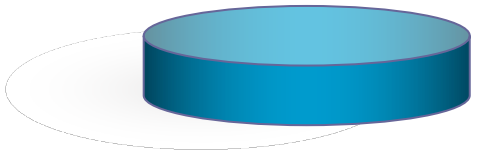
双人控制类似职责划分，关键任务需要两个人认同，并进行互审减少共谋和欺骗的可能性，也减少由于人精力问题出错的可能。

资源管理

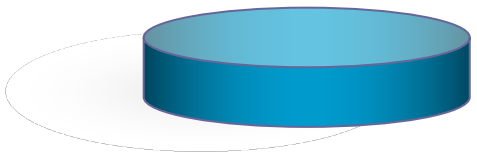
极客时间



硬件资源，如计算机、服务器、外设，如使用条形码系统，在硬件资产上贴上条形码，并在条形码数据库中保持设备相关信息。

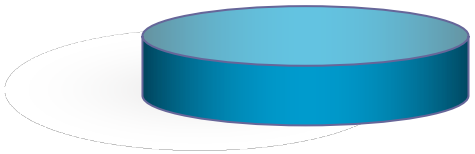


软件资源，操作系统和应用程序。组织购买软件，并使用许可密钥来激活软件，如未激活，保存好激活码。

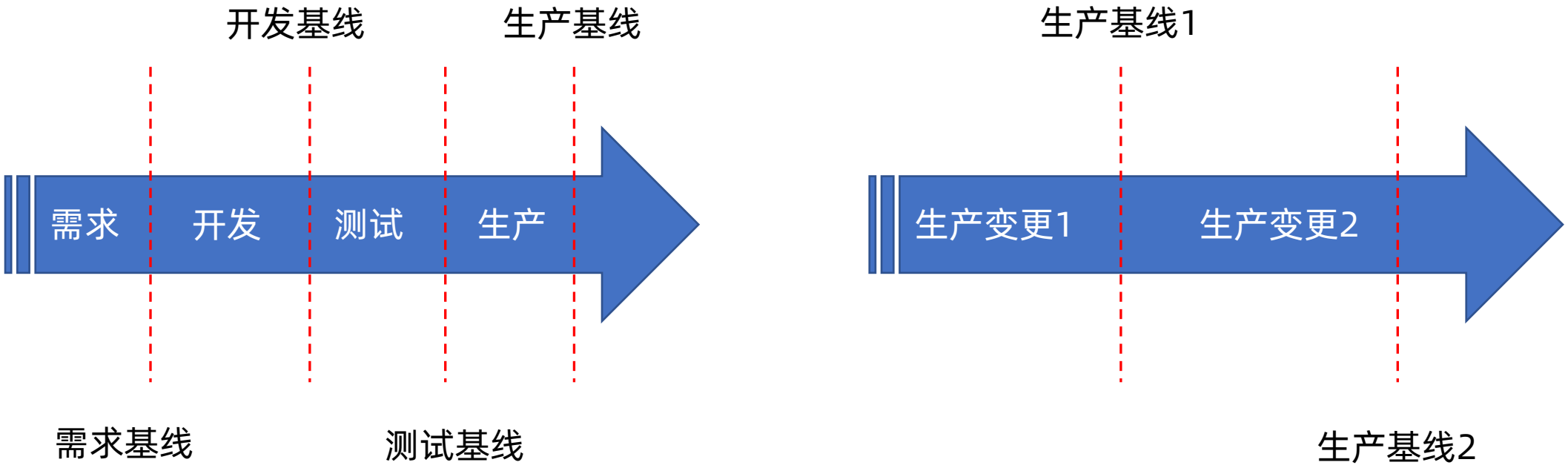


云资源，当企业数据存储在云上的时候，企业或组织必须确保安全控制能防止未授权访问。或由于挖矿病毒导致的服务使用受限。

配置管理（基线）



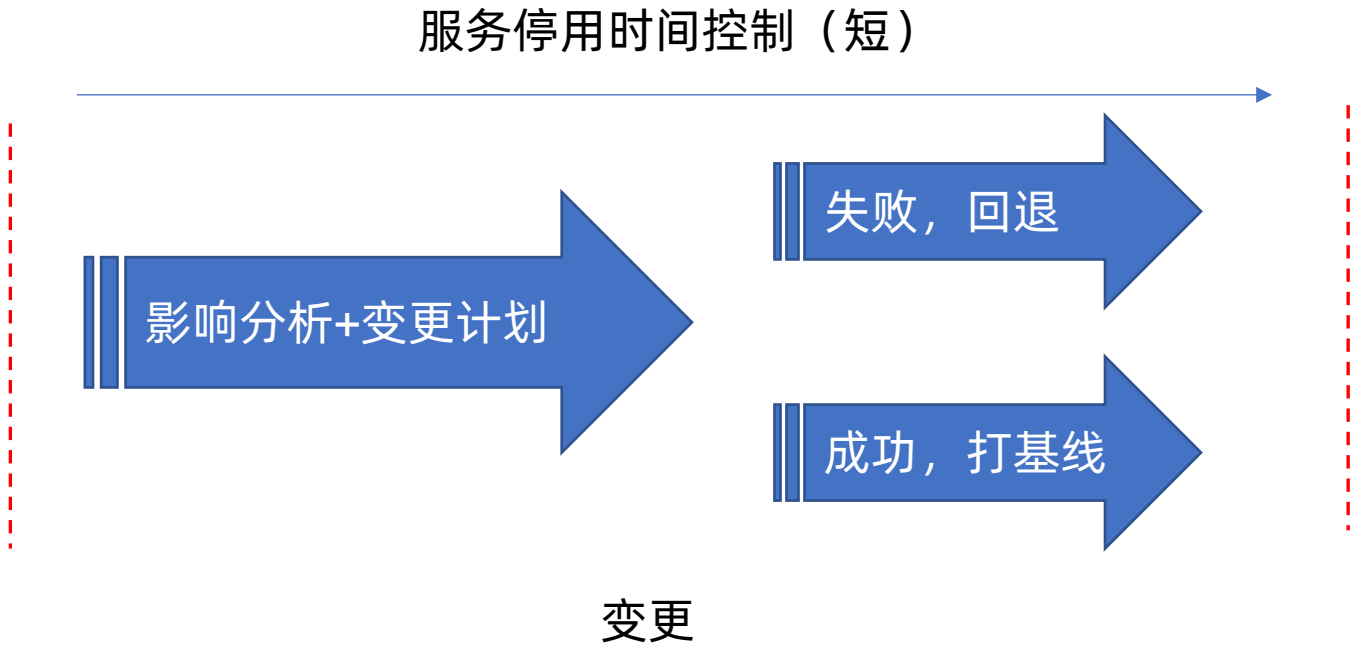
基线是一个起点，代表此时处于安全状态，达到通过变更达到下一个安全状态时候，打下下一个基线，保证系统或应用处于安全状态或符合项目流程进度。基线也用作版本控制，防止由于变更导致的网站瘫痪。



变更管理（影响分析&版本控制&配置文档）

极客时间

变更管理提供一个过程来控制，文档化，跟踪和审计所有系统的变化。主要目标是，以及变更失败的回退操作，确保变更过程不会导致长时间中断。



事件预防与响应

预防

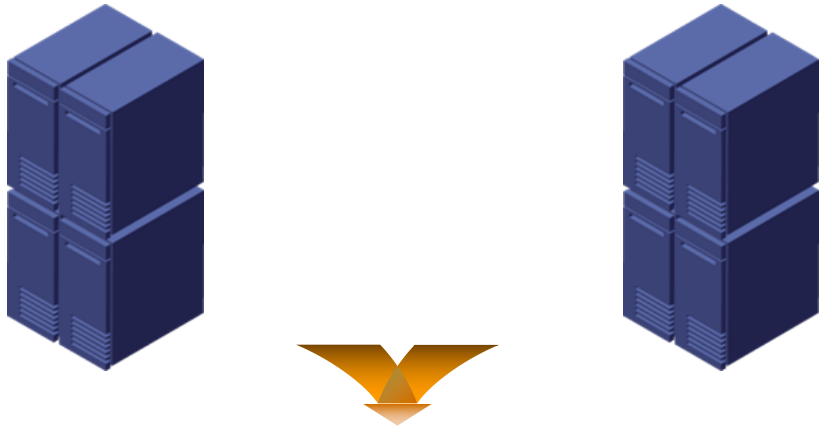
- 防火墙
- 入侵检测和防御系统
- 白名单/黑名单
- 第三方安全服务
- 沙箱
- 蜜罐
- 防恶意软件

响应

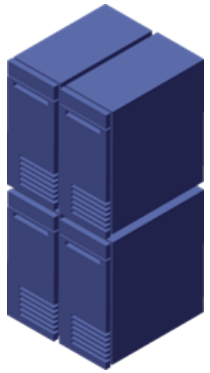
- 入侵检测+安全事件持续监控+出口监控
- 响应
- 缓解
- 报告
- 恢复
- 纠正

经验教训

灾难恢复（两地三中心）



同城



异地

如何做好隐私保护

01 隐私保护

01 隐私保护

定义&原理

隐私保护

互联网在带给人们带来便捷的的同时，也放大了负面事件的影响。

随着大数据的发展，企业试图谋求更多的个人信息，以提供更好更优质的服务作为理由，但同时，广告根据个人信息精准投放，给企业带来了丰厚的利润，甚至个人信息本身也成了一种商品。

诱导个人信息填写

- 完善个人资料，获得奖励。
- 授权个人信息，开启应用使用。

如何保护用户隐私

极客时间

- 用户应该拥有知情权和选择权。
- 网站应该妥善保管收集到的用户数据，不得将数据用于任何指定范围以外的用途。
- DNT(Do Not Track)header

用户应该拥有知情权和选择权

极客时间

应该清楚的展示询问完成 APP 自身功能所需要的权限：

合理：

地图类的 APP 询问授予定位权限

通讯类的 APP 询问授予语音权限

不合理：

字典类的 APP 需要定位权限？

通讯类的 APP 需要系统权限？

运动类的 APP 需要手机通讯录权限？

用户信息仅用于指定用途

腾讯新闻 | 打开眼界

李开复：早期帮助旷世科技拿到蚂蚁金服大量人脸数据做分析

大千世界 2020-09-12 22:48:52

https://view.inews.qq.com/wxn2/20200912V0KHSU00

DNT(Do Not Track)header

极客时间

随浏览流量一起发送“不跟踪”请求

不跟踪

如果您启用了“不跟踪”，即意味着您的浏览流量中将会包含一个请求。所造成的任何影响均取决于网站是否回应该请求以及如何解读该请求。例如：某些网站在收到该请求后，可能会向您展示广告（这些广告并不是根据您访问过的其他网站展示的）。许多网站仍会出于一些目的收集并使用您的浏览数据，例如，为了提高安全性，为了提供相关内容、服务、广告和推荐内容，以及为了生成报告统计信息。了解详情

取消 确认

DNT(Do Not Track)header

极客时间

× Headers Preview Response Initiator Timing

:path: /api/v2/za/logs/batch
:scheme: https
accept: */*
accept-encoding: gzip, deflate, br
accept-language: zh-CN,zh;q=0.9,en;q=0.8
content-encoding: gzip
content-length: 722
content-type: application/x-protobuf
dnt: 1
origin: https://www.zhihu.com
referer: https://www.zhihu.com/question/20615448
sec-fetch-dest: empty
sec-fetch-mode: cors
sec-fetch-site: same-site
user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) App
7.36

国家集中整治

公安网安部门专项整治违法违规APP取得初步成效

发布时间：2020-05-16　字体：[大 中 小]

索 引 号	000000000/2020-00121	发布机构	公安部 > 网络安全保卫局
名　称	公安网安部门专项整治违法违规APP取得初步成效		
生成日期	2020-05-16		
主题分类	重要工作 > 网络安全管理		
内容概述			

今年第一季度，全国公安机关网安部门充分发挥职能作用，加大公民个人信息保护力度，依法查处违法违规收集公民个人信息APP服务单位386个，涉及信息咨询、辅助学习、文学小说、新闻资讯、娱乐播报等多个类型。其中，97个APP被予以行政处罚，192个APP被依法责令改正违法行为，51个APP被下架、停运，有效保护了公民个人信息。十大案例为：

国家集中整治

一、“猎豹清理大师”APP（版本号：6.13.5.1066）。经查，该款APP的隐私协议中对于索取用户通讯录、通话记录等权限的行为没有进行详细说明。北京市公安局朝阳分局已依法责令该公司改正违法行为。

二、“印象笔记”APP（版本号：10.5.5）。经查，该款APP隐私协议中未以显著位置、显著字体申明收集用户信息数据项，未明示各数据项收集用途。北京市公安局朝阳分局已依法责令该公司改正违法行为，并予以警告处罚。

三、“好孕帮”APP(版本号：3.4.8)。经查，该款APP在收集信息时未明示并征得用户同意，用户服务协议及隐私声明中未明示申请权限目的，未告知收集用户个人信息的目的及使用方式。北京市公安局西城分局已依法责令该公司改正违法行为，并予以警告处罚。

四、“不背单词”APP(版本号：3.2.2)。经查，该款APP在收集信息时未明示取得用户同意。北京市公安局大兴分局已依法责令该公司改正违法行为，并予以警告处罚。

五、“哈弗智家”APP(版本号：3.4.7)。经查，该款APP无收集信息明示且未取得用户同意，未向用户明示收集、使用个人信息的目的、方式、范围。河北省保定市公安局已依法责令该公司改正违法行为。

国家集中整治

六、“完美校园”APP（版本号：v5.0.6）。经查，该款APP在部分第三方SDK组件中存在调用获取任务信息和读取联系人等两项权限的情况。河南省郑州市公安局已依法责令该公司改正违法行为。

七、“天然工坊”APP（版本号：3.5.0）。经查，该款APP的用户隐私协议中未向用户明示获取用户信息的详细用途及业务关联。湖南省长沙市公安局已依法责令该公司改正违法行为，并予以警告处罚。

八、“随手借”APP（版本号：4.11.11）。经查，该款APP应用隐私政策中未明示第三方SDK插件以及收集使用个人信息的目的、方式和范围。广东省深圳市公安局已依法责令该公司改正违法行为。

九、“每日瑜伽”APP（版本号：7.15.1.1）。经查，该款APP未以显著位置、显著字体申明收集用户信息数据项。陕西省西安市公安局高新分局已依法责令该公司改正违法行为。

十、“Paintly”APP（版本号：V2.1.6.3）。经查，该款APP存在超范围收集用户信息问题。陕西省西安市公安局已依法责令该公司改正违法行为。

极客时间

扫码试看/订阅

《Web 安全攻防实战》视频课程