2022北京网络安全大会
2022 BEIJING CYBER SECURITY CONFERENCE
全球网络安全 倾听北京声音

企业SRC建设与运营实践

姚亮 | 斗象科技

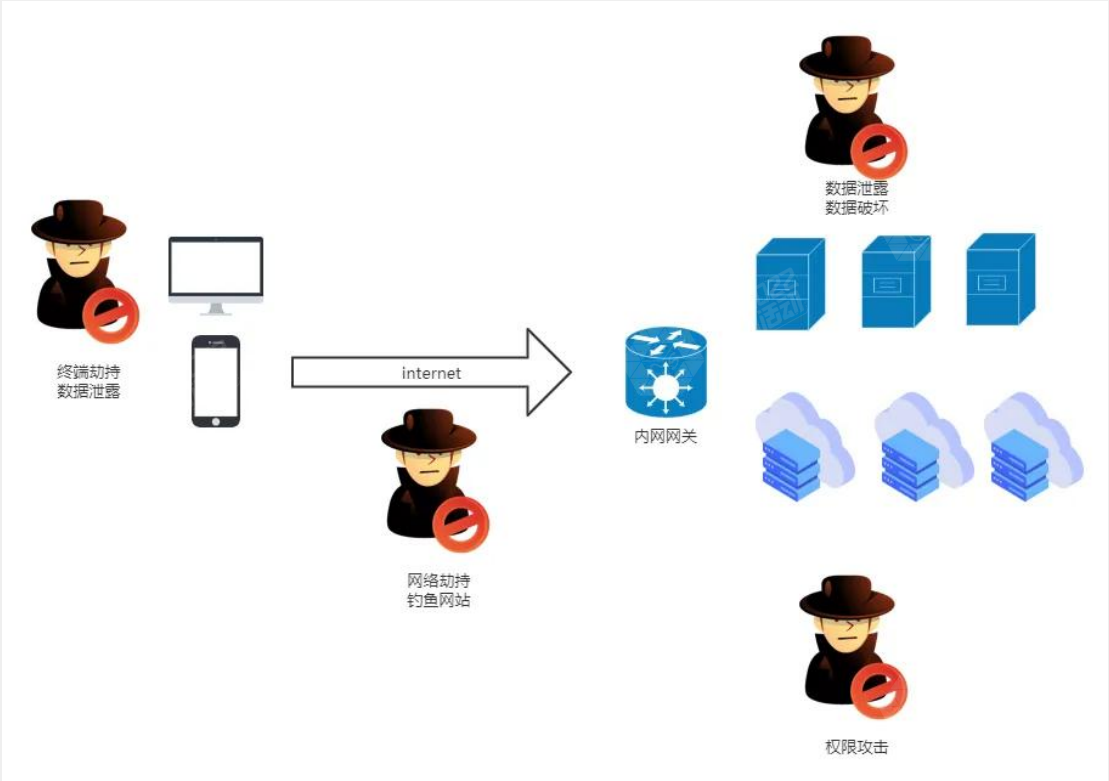
背景及需求

疫情影响下企业的安全隐患

◆疫情影响下，远程办公常态化。越来越多内网的业务被暴露到互联网，增加了暴露面，成为黑客攻击对象

系统软件更新不及时，安全漏洞未及时修补，易成为黑客攻击的跳板

为满足远程办公开启过多内部网络的对外访问权限，权限管理不规范，导致敏感数据泄漏层出不穷



背景需求

企业需求

- 从企业业务安全、安全运营角度出发，解决企业漏洞收集、漏洞管理、漏洞响应、漏洞闭环等实际需求
- 满足工信部、网信办、公安部联合发布的《网络产品安全漏洞管理规定》合规要求

WWW.CAC.GOV.CN

请输入检索关键词

首页 权威发布 办公室工作 网络安全 信息化 网络传播 国际交流 地方网信 执法督查 政策法规 互动中心 教育培训 业界动态 工作专题

当前位置：首页 > 正文

工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知

2021年07月13日 17:11 来源：中国网信网 【打印】 【纠错】

工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知

工信部联网安〔2021〕66号

各省、自治区、直辖市及新疆生产建设兵团工业和信息化主管部门、网信办、公安厅（局），各省、自治区、直辖市通信管理局：

现将《网络产品安全漏洞管理规定》予以发布，自2021年9月1日起施行。

工业和信息化部 国家互联网信息办公室 公安部

2021年7月12日

2021年9月1日生效的《网络产品安全漏洞管理规定》：

第五条 网络产品提供者、网络运营者和网络产品安全漏洞收集平台应当建立健全网络产品安全漏洞信息接收渠道并保持畅通。

第七条 鼓励网络产品提供者建立所提供网络产品安全漏洞奖励机制，对发现并通报所提供网络产品安全漏洞的组织或者个人给予奖励。”

企业SRC介绍

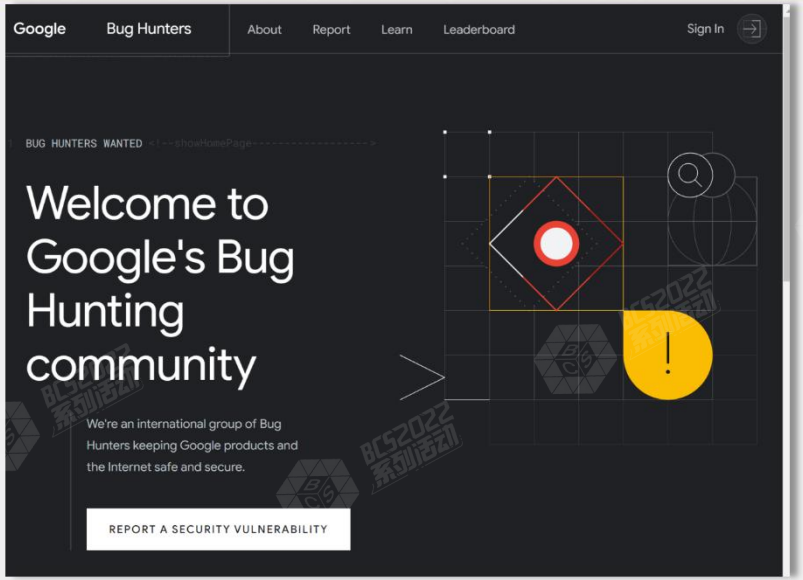
企业SRC概念

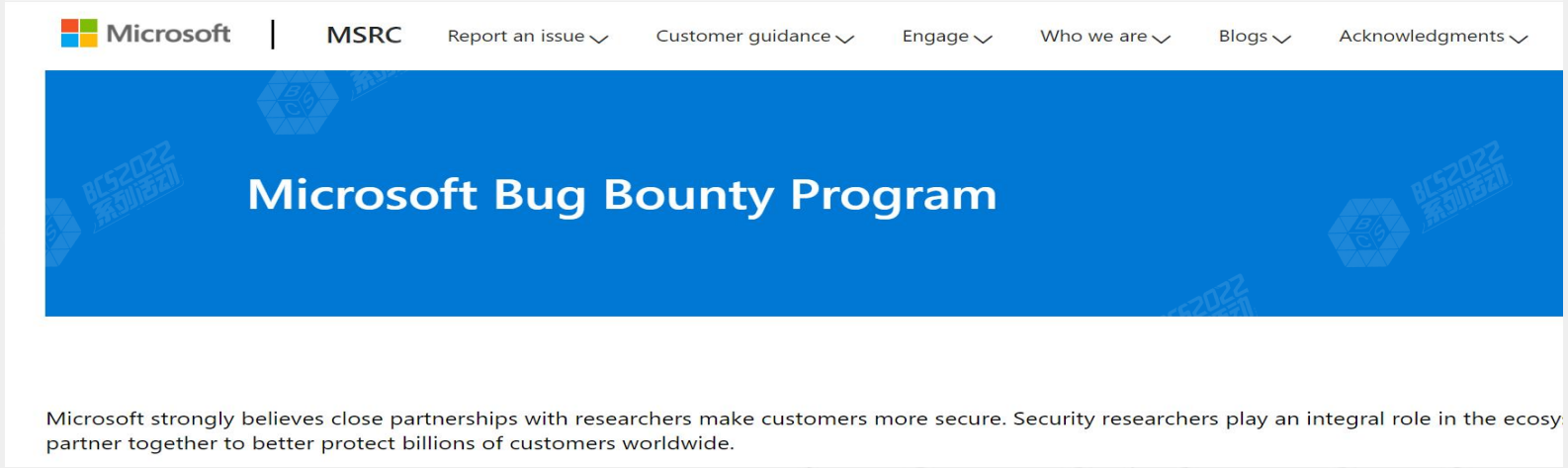
安全应急响应中心（SRC, Security Response Center）是企业安全团队对外接收来自安全领域的个人、团队发现并报告安全缺陷、安全漏洞的桥梁，以及企业对外发布突发安全事件处理动态的平台，旨在聚集多方安全领域力量帮助企业共同发现潜在安全威胁、并及时响应，同时也借助SRC平台加强与安全业界同仁的合作与交流。

- 从甲方安全运营角度出发，解决了企业漏洞管理与响应的环节
- 企业可以把更多资源专注于主线业务发展，根据自身发展需要逐步组建安全团队，从战略角度为企业争取生存空间。

国内外SRC平台

- 国内大型互联网公司都已陆续建立各自的SRC应急响应中心，并在推出以后取得了良好的效果，对企业安全有了巨大的协调和推动作用。
- 国外与之对应的是“Bug Bounty Program”赏金漏洞计划，比国内SRC起源更早，应用更为广泛。如Google，Facebook，Microsoft等大型互联网厂商都有独立的赏金计划。





企业SRC核心价值

企业SRC核心价值

- ➢《网络产品安全漏洞管理规定》相关合规要求
- 引入外部力量，更加高效、长期地提升企业安全壁垒，降低突发安全风险事件
- 节省成本、提升安全运营效率
- 漏洞全生命周期的闭环管理
- 宣传企业形象，吸引安全人才

企业SRC建设问题

资源投入

- 需要专业安全团队、运营团队、开发团队，以及财务支持。

1. **靠谱的安全团队**
   - 安全专家
   - 漏洞规范
   - 漏洞审核制度
   - 漏洞生命周期管理
2. **开发团队**
3. **运营团队**
   - 持续的宣传
   - 白帽子的KOL
   - 线上线下活动策划
   - 日常纳新、留存、促活
4. **财务支持**

平台建设投入

SRC平台是一个功能全面且业务复杂的平台，搭建一套完善的SRC平台需要花费大量的成本，多数中小型企业无力开发一套功能齐全的SRC平台。

首页

宣传众测平台与企业信息
发布最新活动资讯

注册/登录

多重机制防止恶意注册
防止暴力破解
校验用户真实性

项目大厅

支持通过VPN访问指定测试环境
解密VPN帐号加密流量，一对一流量审计

我的漏洞

统一记录用户历史提交的漏洞信息、获取奖金等信息。
便于用户查看漏洞审核状态、最新动态等信息
漏洞关闭后，白帽用户将不可见漏洞信息，保证漏洞私密性

排行榜

全平台榜单与项目榜单
有效激励测试人员，增加漏洞数量
提升企业系统安全

奖励提现

支持企业审核提现金额
导出账单等操作

系统公告

及时告知用户，企业发布的最新消息

平台落地运营经验缺乏

漏洞定级

平台规则

专业审核能力

生命周期闭环

沟通申诉渠道

白帽生态建设乏力

斗象科技 TOPHANT

2022北京网络安全大会
2022 BEIJING CYBER SECURITY CONFERENCE
全球网络安全 倾听北京声音

漏洞盒子企业SRC运营实践及解决方案

漏洞盒子企业SRC运营实践

筹备阶段

- 人员配备与分工：项目经理、漏洞审核人员、运营人员，财务，内部对接研发人员
- 奖励方案：确认核心资产、非核心资产，设定区分奖励规则
- 授权协议：制定白帽测试授权协议，约定测试边界，测试行为
- 漏洞规则：漏洞定级，收取规则，无效漏洞、已知漏洞、重复漏洞声明
- 资产范围：确认SRC收取的漏洞范围边界（本公司/单位/组织、子公司/单位/组织等）
- 应急处置：应急处置方案

试上线阶段

- 定向邀请：邀请小范围白帽测试，提交漏洞
- 流程磨合：从漏洞提交到审核、验证、转交、修复、复测、关闭全生命周期流程磨合
- 问题反馈：试运行过程中收集问题反馈及改进优化

漏洞盒子企业SRC运营实践

正式上线

- 上线时间选择：避开业务高峰期，研发做好漏洞修补准备
- 资产范围：根据企业实际业务大小，分批次公开，避免大流量扫描影响业务
- 宣传推广：公告、社群、海报、短信、推文……
- 社群维护：SRC白帽社群组建及维护，通过社区收集白帽意见反馈，保持沟通
- 活动运营：用户拉新、活动推广、PR宣传

持续运营

- 漏洞生命周期管理与闭环
- 活动运营：用户留存、排行榜、节假日活动、线上线下活动
- 申诉沟通：白帽漏洞申诉处理
- 白帽关系维护：定期意见收集反馈、礼品寄送、社群维护
- 数据统计：漏洞数据、奖金数据、用户数据分析统计

漏洞盒子解决方案：SaaS托管

企业SRC托管是指企业通过包年托管服务形式，将企业SRC创建于漏洞盒子平台，根据企业购买套餐，盒子平台的安全专家帮您完整管理

类型	服务内容	部署方式	特点	增值服务
SaaS服务-旗舰版	提供基础服务+漏洞完整审核+全套运营服务	无需部署产品，直接云端使用	云端部署，快速开通； 与盒子的白帽体系、白帽资源联动，在白帽引流白帽激励方面效果更佳	● 审核服务（审核、验证、复测） ● 客服服务（申诉、白帽子沟通、合同签订） ● 运营服务（白帽引流、线上线上活动运营、宣传推广、白帽社群、平台数据分析等） ● 驻场安全运营服务（驻场审核、驻场运营） ● 奖金代发
SaaS服务-专业版	提供基础服务+漏洞初审+部分运营服务			
SaaS服务-自助版	提供基础服务托管服务，厂商自助审核漏洞			

漏洞盒子解决方案：私有化部署

VMS(Vulnerability Management System)是斗象科技依托多年的安全服务经验、漏洞管理经验以及漏洞盒子漏洞情报积累，推出的一款集漏洞信息收集，漏洞生命周期管理，漏洞扫描调度为一体的平台系统。

漏洞盒子企业SRC提供服务

斗象科技 TOPHACT

2022北京网络安全大会 2022 BEIJING CYBER SECURITY CONFERENCE 全球网络安全 倾听北京声音

01 平台搭建及规则制定

➢通过SaaS或者本地化部署帮助客户搭建一套功能完备的SRC服务平台

➢为客户SRC平台制定科学的漏洞收取规则及漏洞定级标准

02 常态化平台运营

➢提供完整的漏洞审核服务：包括漏洞审核定级、漏洞复现验证、报告输出编写、漏洞复测等工作

➢提供优质的客服运营工作：包括白帽子申诉处理、白帽子问题解答以及白帽子奖金代发等服务

03 白帽运营及品牌宣传

➢企业SRC宣传

➢白帽子社群建立与维护

➢独家互动策划运营、联合平台运营活动

漏洞盒子核心优势

核心优势

白帽生态

领先的白帽生态，平台注册认证白帽超过100,000+

经验丰富

业界最早推出企业SRC托管服务，拥有多年运营经验，客户涉及各个领域行业

服务全面

多种套餐及单项服务组合，灵活定制切合企业需求，支持SRC平台私有化产品部署

服务全面

专业团队具备高效漏洞验证能力，代企业审核漏洞，节约企业人员成本

漏洞复测

提供专业漏洞复测服务，保证漏洞修复闭环

平台运营

平台白帽运营团队提供一站式运营服务，快速提升企业SRC影响力

盒子白帽生态及运营优势

A 庞大的白帽子群体

技术能力全面的白帽子群体

有效白帽子用户10w+

B 高效的漏洞管理能力

累计为企业提供漏洞100w+

高危、严重漏洞“小时级”响应速度

中低危漏洞24小时响应

C 各种线上线下活动

FreeTalk白帽沙龙

一年一度的CIS大会

漏洞马拉松活动

年度TOP白帽子出境游

D 白帽运营管理

白帽技能画像

白帽分级管理

白帽任务系统

盒子赛季体系

成熟的运营体系

➢ 新颖的赛季玩法：

赛季积分、赛季段位、赛季排行榜、赛季奖励玩法多种多样。

➢ 业内首创任务系统：

业界首创的白帽任务系统+白帽智能派单，引领业界风向标；白帽能力标签化，智能学习邀请。

➢ 丰富的运营互动：

全年举办超过20次线上线下各类型活动，举办漏洞马拉松、盒子梦想趴、FreeTalk、白帽LIVE等活动，打造盒子独特的白帽文化。

➢ 社群及内容运营：

依托漏洞盒子及「FreeBuf」的影响力，是安全垂直领域最有影响力的宣传渠道之一；漏洞盒子技术社区、FreeBuf知识大陆、白帽公开课、S级白帽分享沙龙等技术分享。

典型客户案例

斗象科技 TOPHANT

2022北京网络安全大会
2022 BEIJING CYBER SECURITY CONFERENCE
全球网络安全 倾听北京声音

中国银联 China UnionPay

Lenovo 联想

Midea 美的IoT

中國東方航空 CHINA EASTERN

SAIC 上汽集团 SAIC MOTOR

理想

金山云 WWW.KSYUN.COM

openEuler

泛微 weaver

airbnb

LEXIN 乐信

丁香园 WWW.DXY.CN

瓜子 二手车直卖网

嘀嗒出行

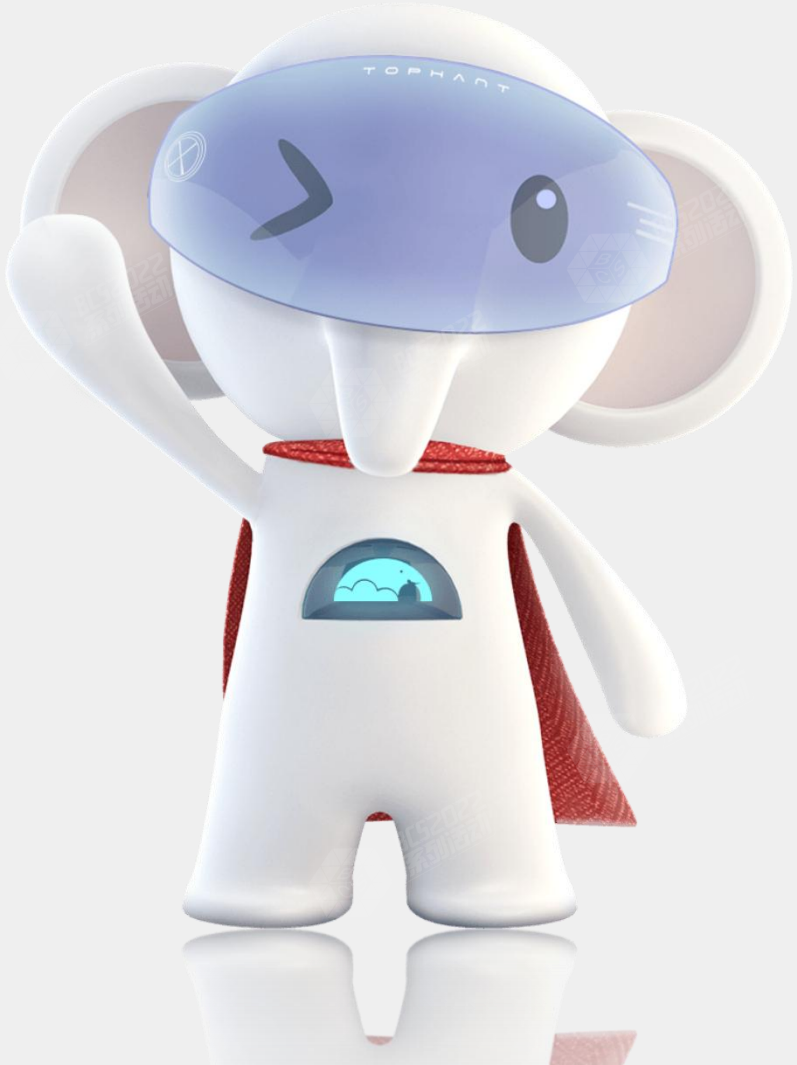
萤石 EZVIZ

漏洞盒子企业SRC试用

SRC试用版

斗象科技 TOPHACT

2022北京网络安全大会
2022 BEIJING CYBER SECURITY CONFERENCE
全球网络安全 倾听北京声音



申请试用

THANKS