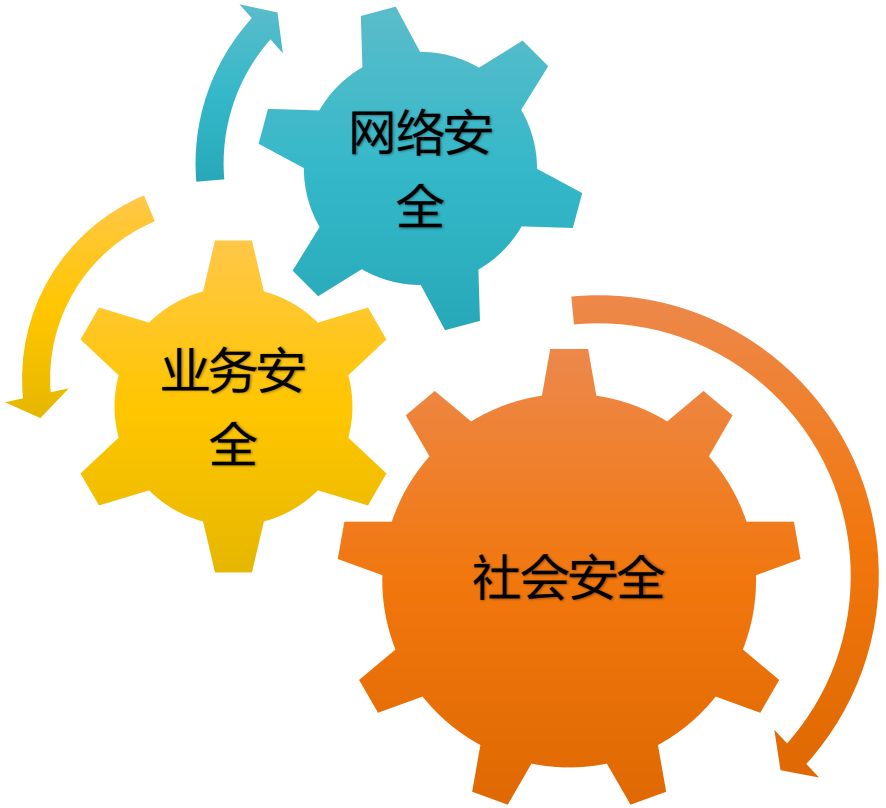
安全运营服务社会化精细分工发展观察

绿盟科技高级副总裁 叶晓虎

NSFOCUS

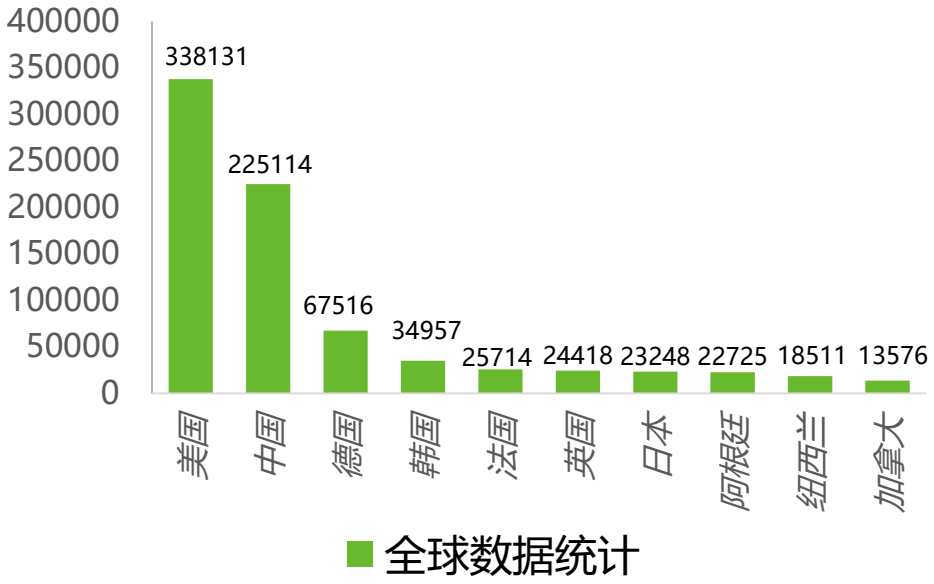
企业数字化变革与安全



NSFOCUS

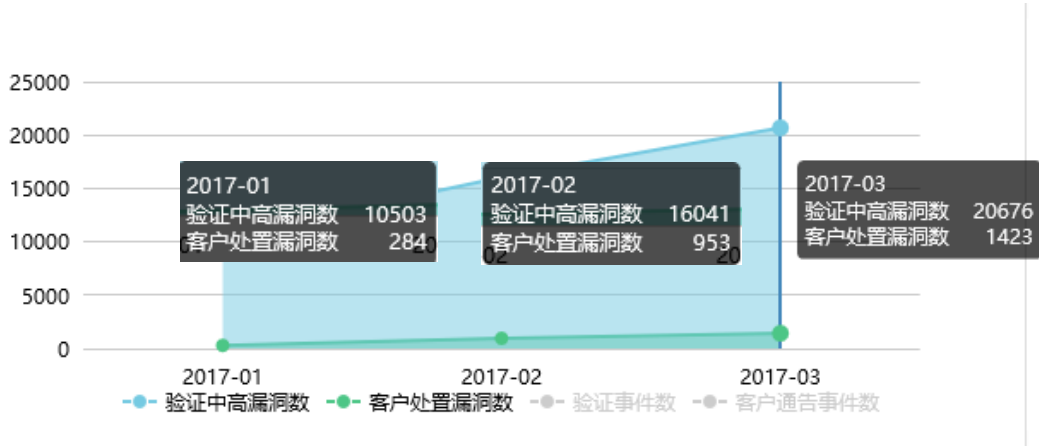
安全态势持续恶化

第三方代码的大量引入



（数据来源：绿盟威胁情报中心）

层出不穷的漏洞



（数据来源：绿盟网站安全检查数据　统计范围：14434个等保等级二级以上网站）

NSFOCUS

窗口期攻防能力差距在扩大

日内攻入和日内发现比例之时间窗口在扩大

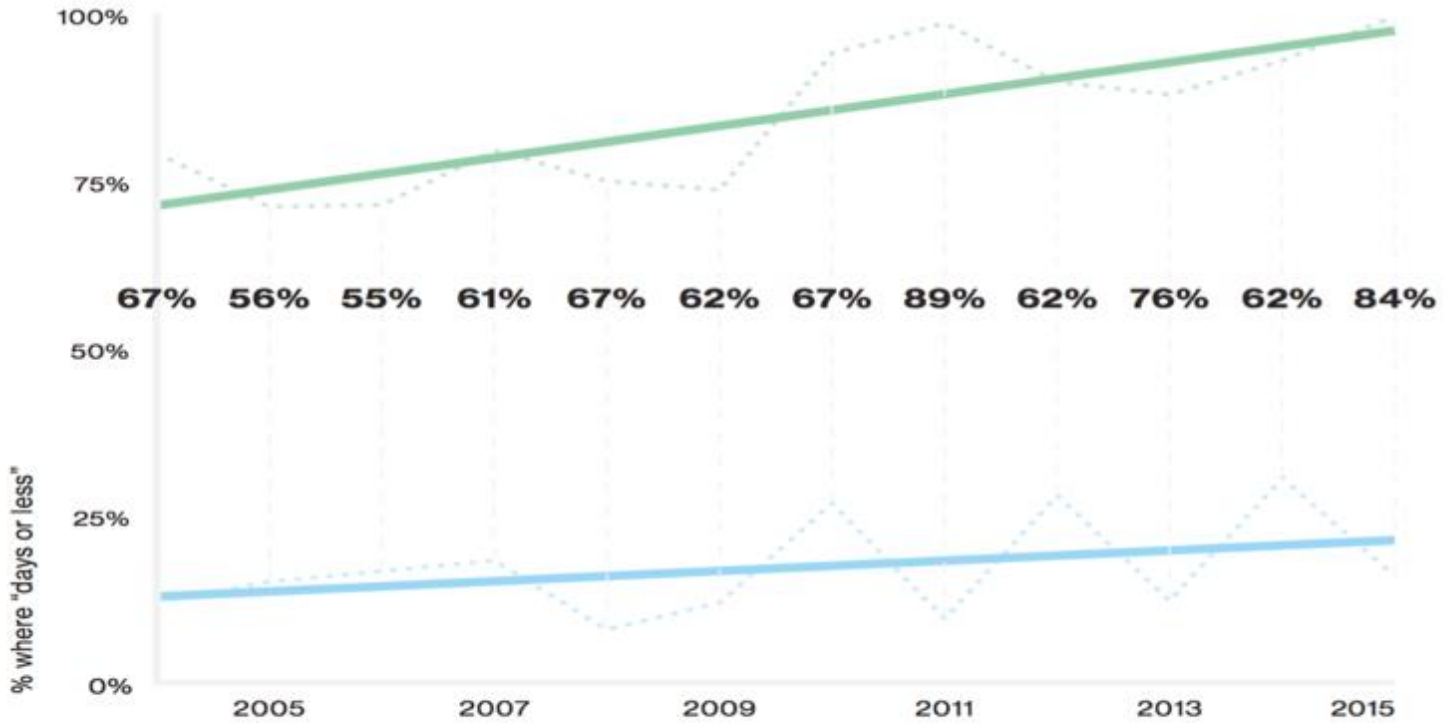


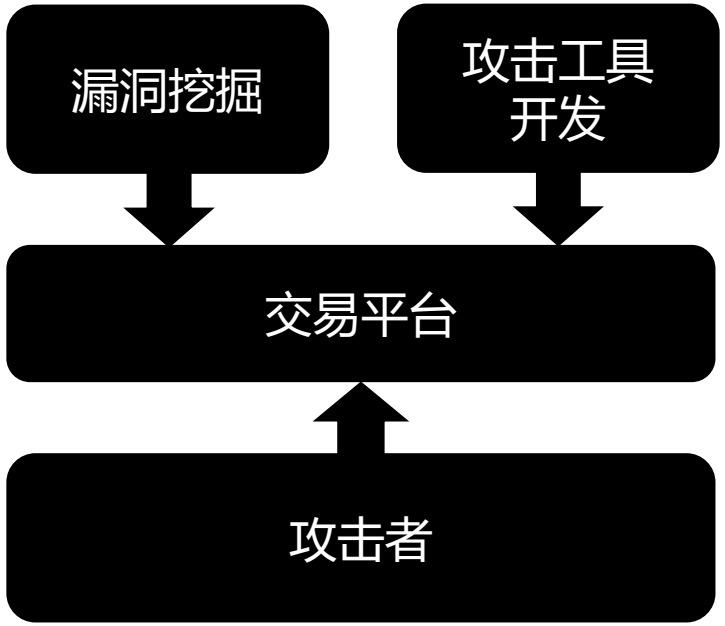
Figure 8.

Percent of breaches where time to compromise (green)/time to discovery (blue) was days or less

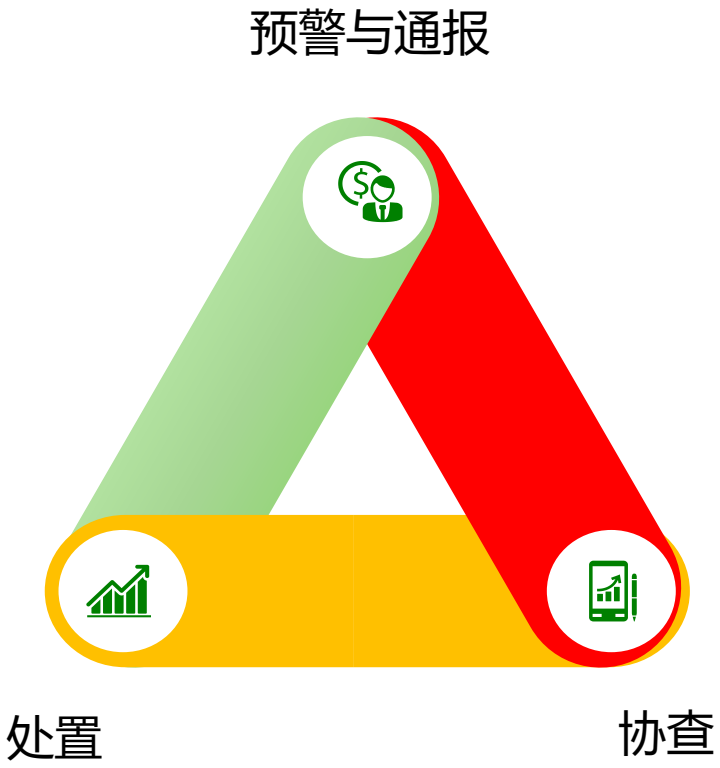
Verizon 2016 Data Breach Investigations Report

NSFOCUS

攻防双方的社会化分工对比



VS



分工和协作是企业持续保持高水平安全状态的必要条件

NSFOCUS

struts2-S-045的战斗

预警/通报/指挥

政府和媒体

- 网际威胁情报
- 社区情报交换
- 设备采集
- O2O互动
- ...

技术开发

厂商

- 威胁技术分析
- 业务影响分析
- 规则补丁升级
- 应急操作方法
- 应急App
- 应急通告

协查

厂商

- 漏洞检测服务
- 漏洞检测工具升级
- 防护设备升级
- 提供防护设备策略建议
- 提供防护设备策略调优

研判与处置

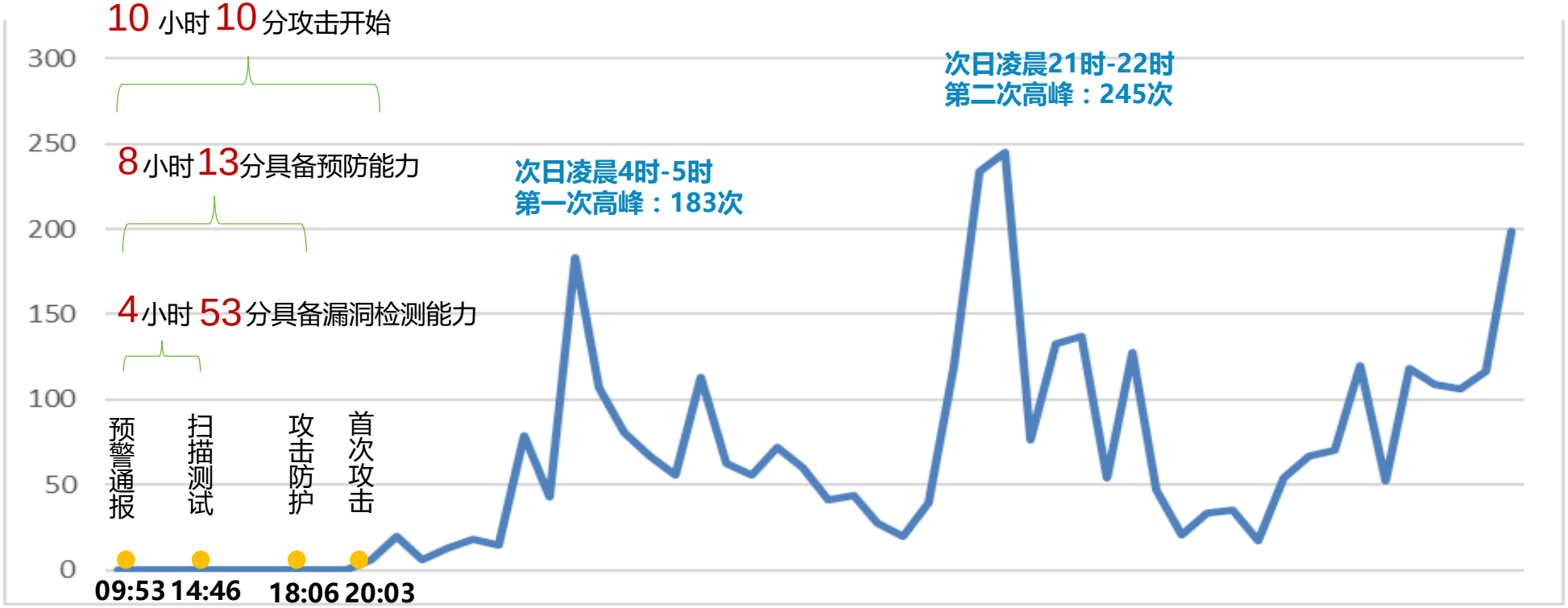
企业与组织机构

- 漏洞分析与研判
- 制定处置策略
- 执行修复或采取临时措施
- 复查

NSFOCUS

以1小时57分的差距险胜

3.7 -3.9日观测到的针对struts2-S-045漏洞攻击的数量，数据来源：绿盟网站安全监测与防护服务，防护站点数：458



协同存在的问题

大部分客户还在采用基于线下的、传统的模式效率低下，在时效上无法与线上客户对抗

流程上：

线下方式通告过程繁琐，周期长，风险高 VS 线上执行预案和预授权，先检测后通告

技术上：

线下方式在技术上更低效，先做页面分析，后进行页面检测，
线上方式在日常中建立资产档案和基线，直接对目标页面进行检测
线下方式设备升级部署效率低下，线上方式大规模自动部署

线下检测方式：厂商内部通告客户代表->客户代表通告企业客户和工程人员->工程人员下载升级保->对扫描设备升级->获取扫描授权->扫描页面分析->漏洞检测->反馈结果->执行修复>对修复结果复验

线上服务检测方式：预授权->建立资产档案->云端引擎自动升级->直接获取目标页面进行检测->通告->修复->复验

NSFOCUS

中美企业机构在安全运营上的细微差异

中国

企业和机构的安全运营

厂商

专业安全服务提供商

美国

企业和机构的安全运营

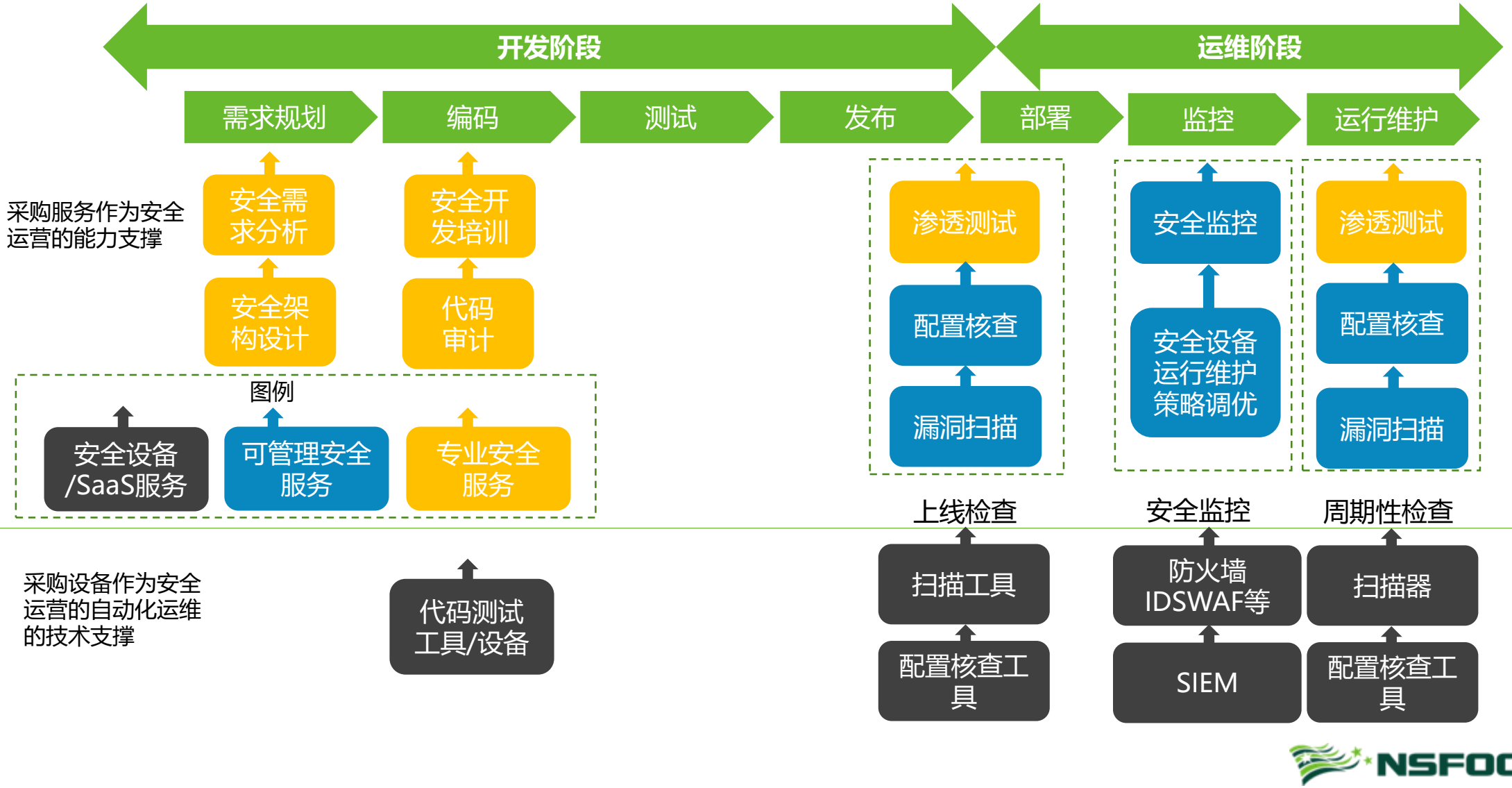
专业的运维支撑

MSSP

厂商

专业安全服务提供商

美国企业在安全运营支撑上的选择



NSFOCUS

MSS在欧美等发达国家的发展情况

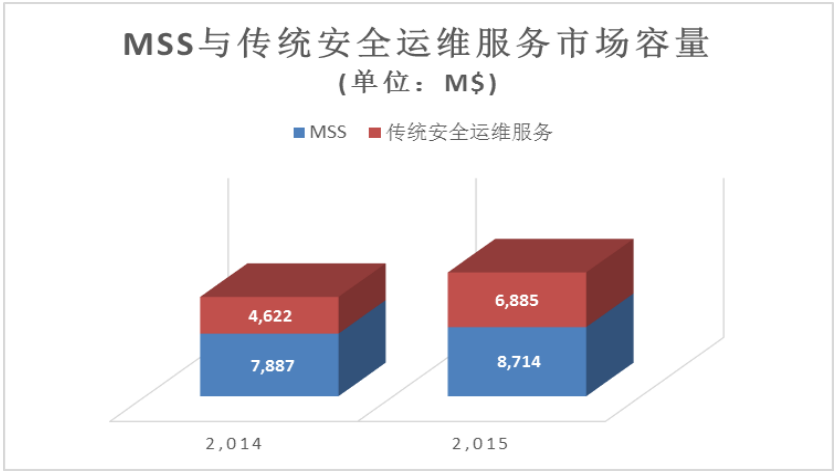
Gartner 认为 可管理安全服务 是一种 远程的IT安全监测与管理服务，该类服务必须是通过 远程运维中心（即SOC）提供的服务，而不是工程师在现场提供。MSS 不包含人员外包、咨询、实施和集成服务。

Market Definition/Description For the purposes of this research, Gartner defines managed security services (MSSs) as "the remote monitoring or management of IT security functions delivered via shared services from remote security operations centers (SOCs), not through personnel on-site." Therefore, MSSs do not include staff augmentation, or any consulting or development and integration services.

——Garnter，2015,23,December Magic Quadrant for Managed Security Services, Worldwide

2015年，全球市场容量8,714M$,是全球安全领域中最大的一个细分市场。

到2019年前，复合增长率15.4%，在产品与服务类排名第一，增长排名第二的security testing 基数只有MSS的十六分之一。



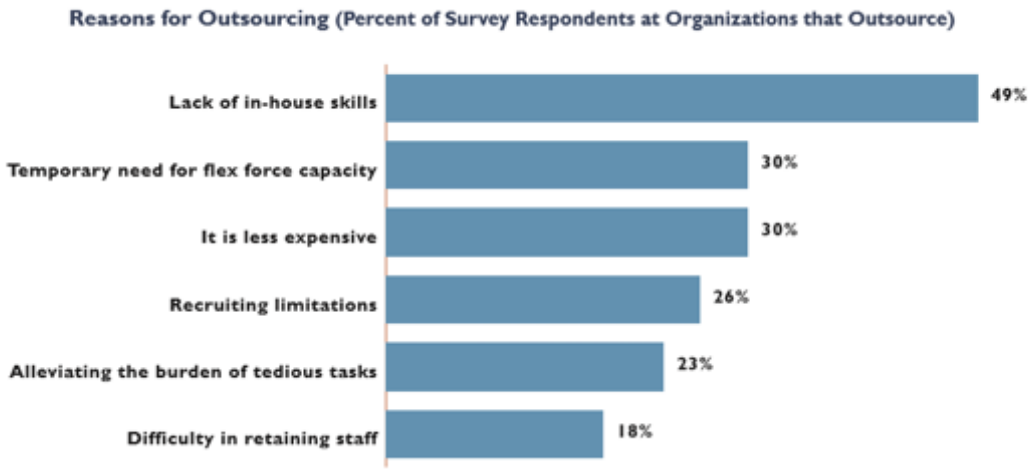
NSFOCUS

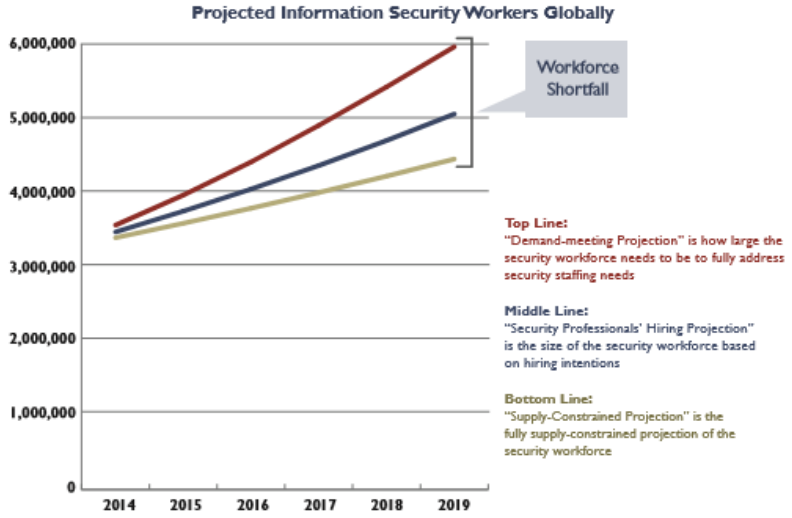
(数据来源:Gartner ,<Forecast Information Security, Worldwide, 2014-2020, 2Q16 Update>,<Market Share Managed Security Services, Worldwide, 2015>)

MSS解决的问题

对企业：远程方式帮助企业提供安全运维能力、解决预算和编制不足的问题

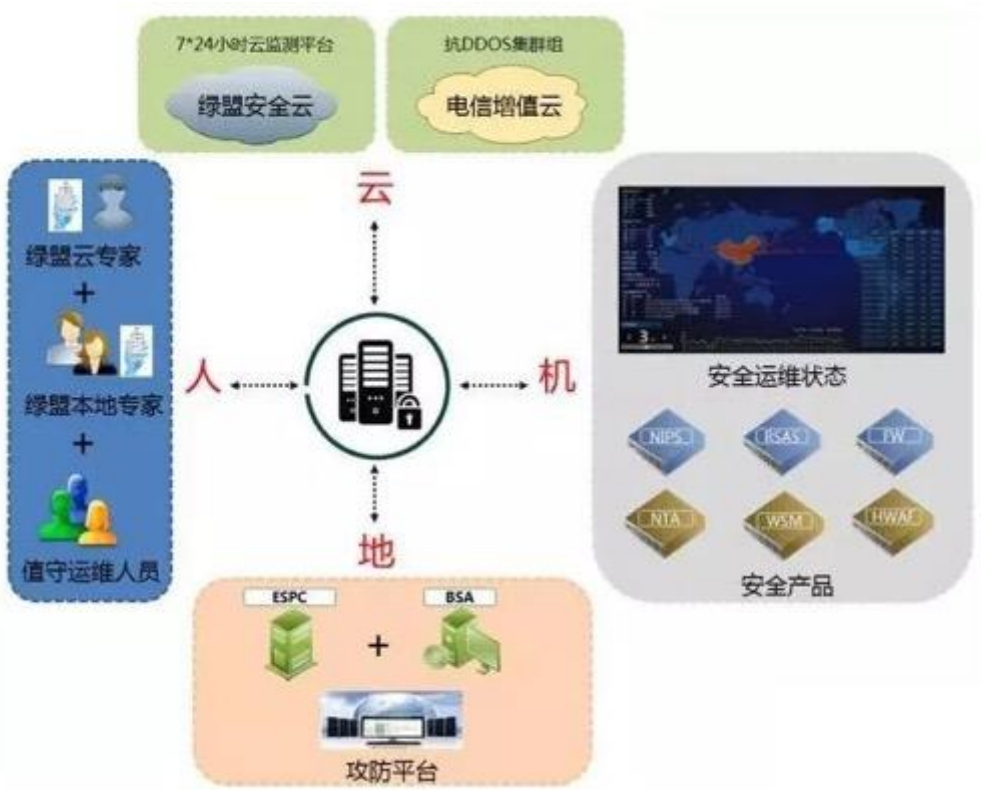
对社会：MSS是一种集中化的运维和管理模式，可以有效缓解全球安全人才不足的问题，根据Frost&Sullivan的预测，全球安全人才缺口在5年内达到150万，这个数据是指企业有编制情况下的缺口

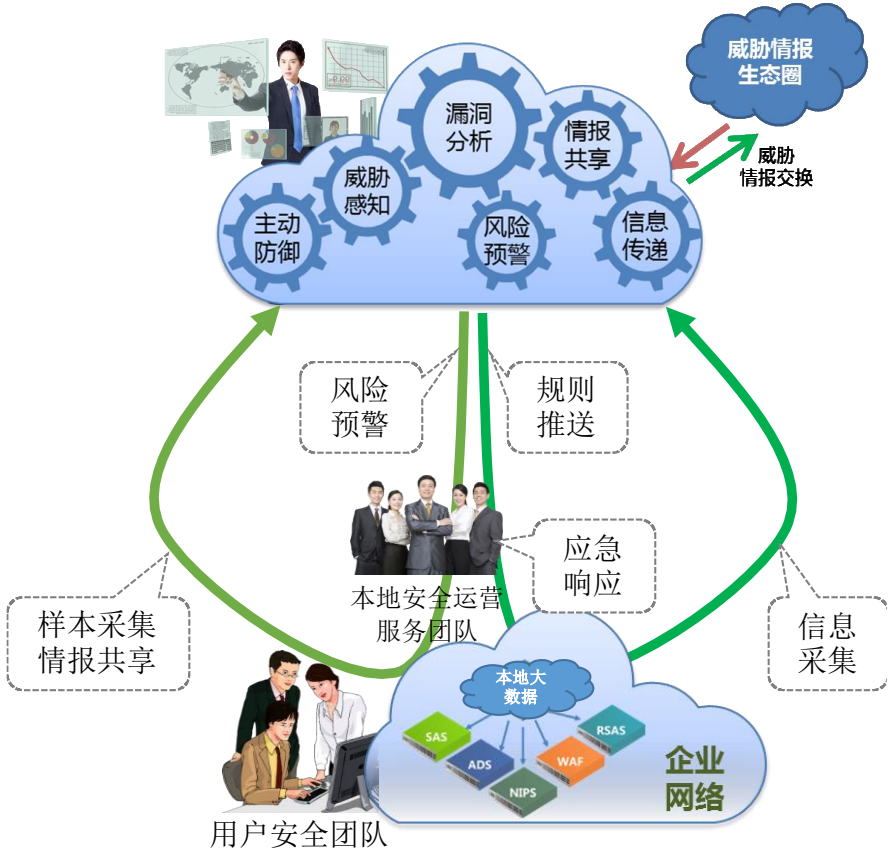




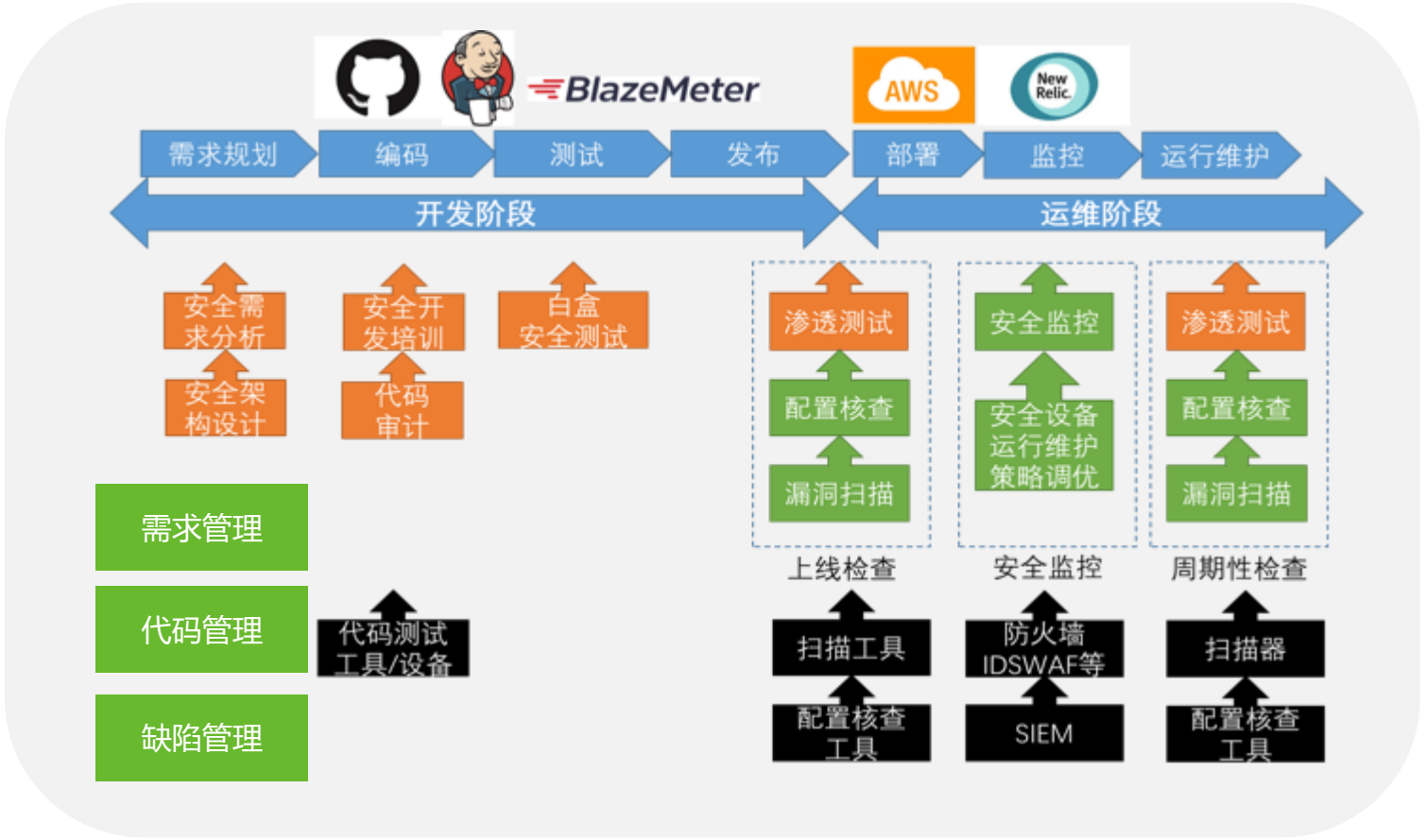
（数据来源：The 2015（ISC）²Global Information Security Workforce Study）

安全运营中的云地人机


7*24小时云监测平台
绿盟安全云
抗DDOS集群组
电信增值云
云
绿盟云专家
+
绿盟本地专家
+
值守运维人员
人
机
地
安全运维状态
NIPS
RSAS
DW
NTA
WSM
HWAF
安全产品
ESPC
BSA
+
攻防平台


威胁情报
生态圈
威胁
情报交换
漏洞
分析
情报
共享
威胁
感知
主动
防御
风险
预警
信息
传递
风险
预警
规则
推送
应急
响应
样本采集
情报共享
信息
采集
本地安全运营
服务团队
本地大
数据
SAS
ADS
NIPS
WAF
RSAS
企业
网络
用户安全团队

企业面临的挑战



Dev+Sec+Ops

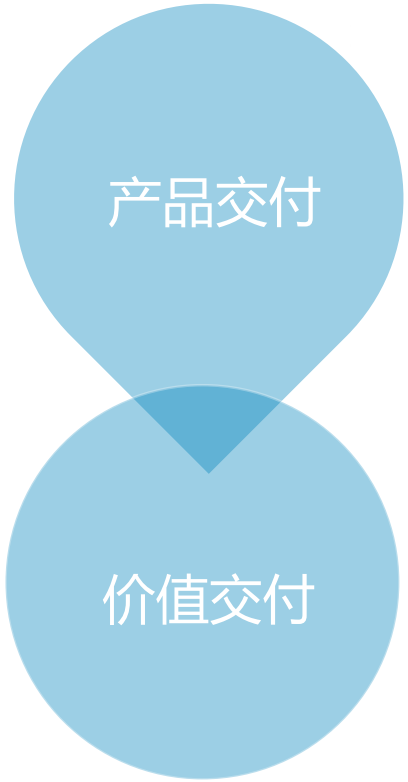
01 改变对服务的观念，改变预算决策机制及预算结构

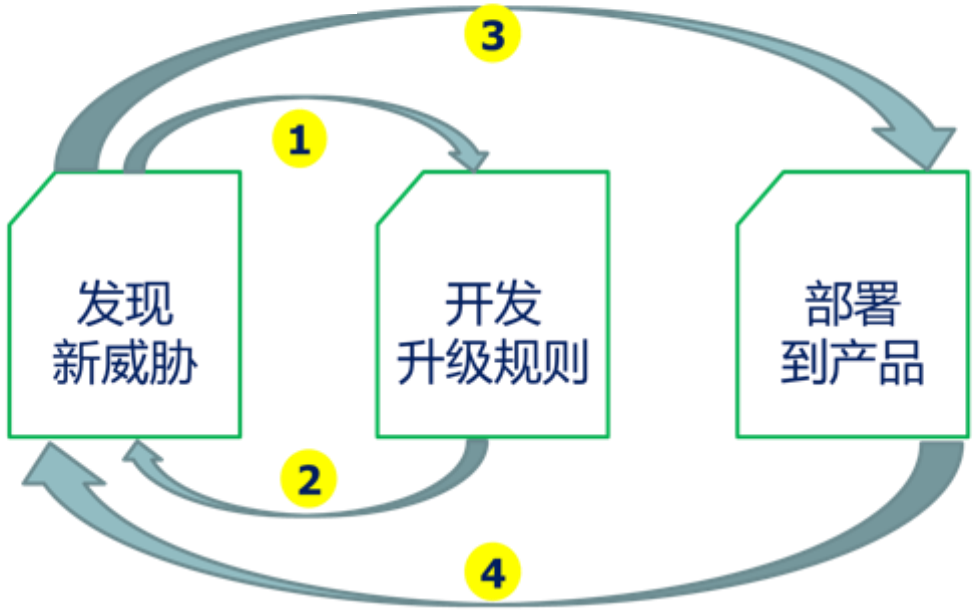
02 企业将安全运营能力、工具与现有的开发体系整合，实现高效自动化安全开发和运维

03 监管合规的限制

NSFOCUS

对安全厂商的挑战



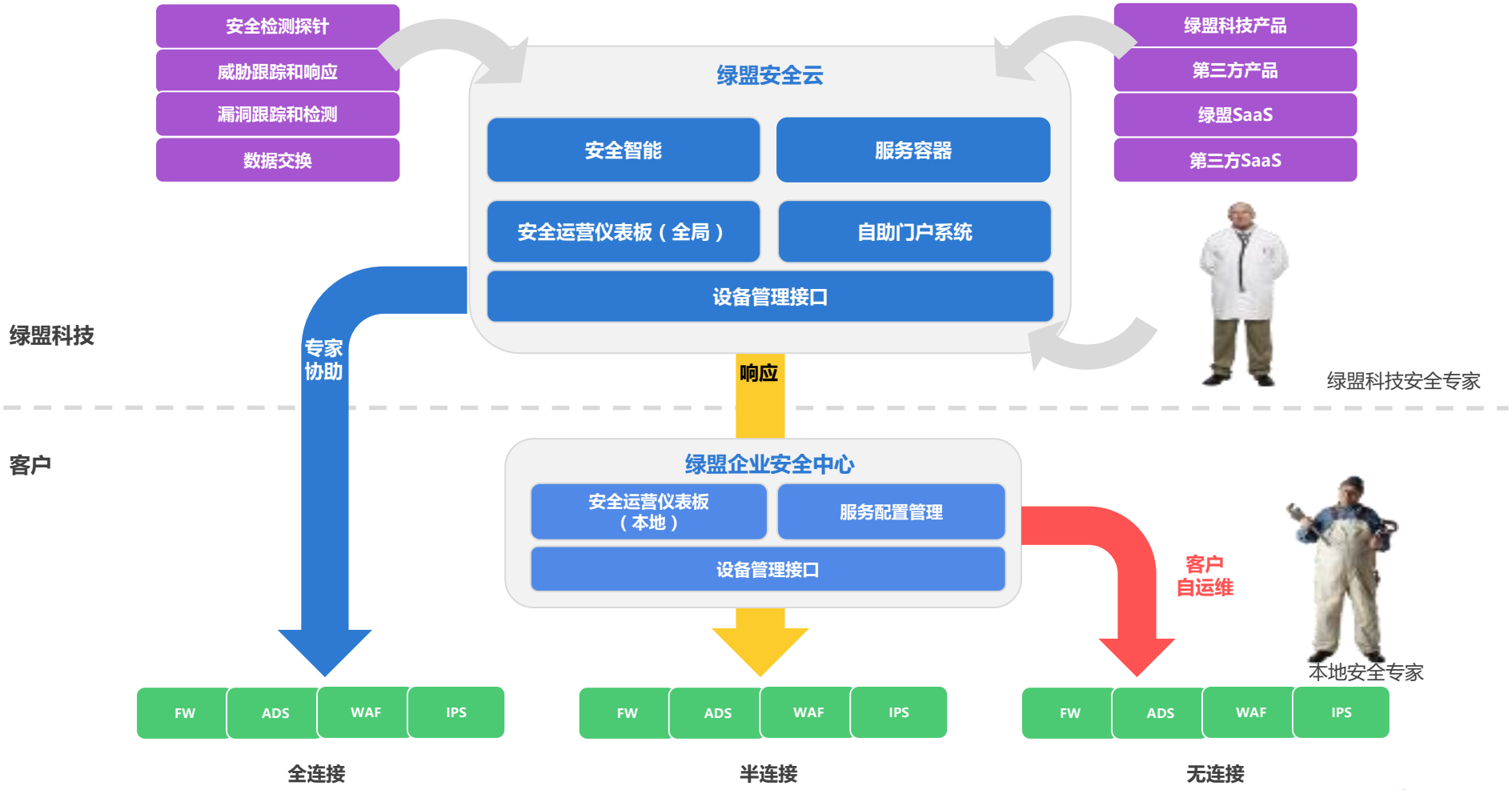


小闭环：从发现威胁到开发出相应的规则或升级补丁到发布

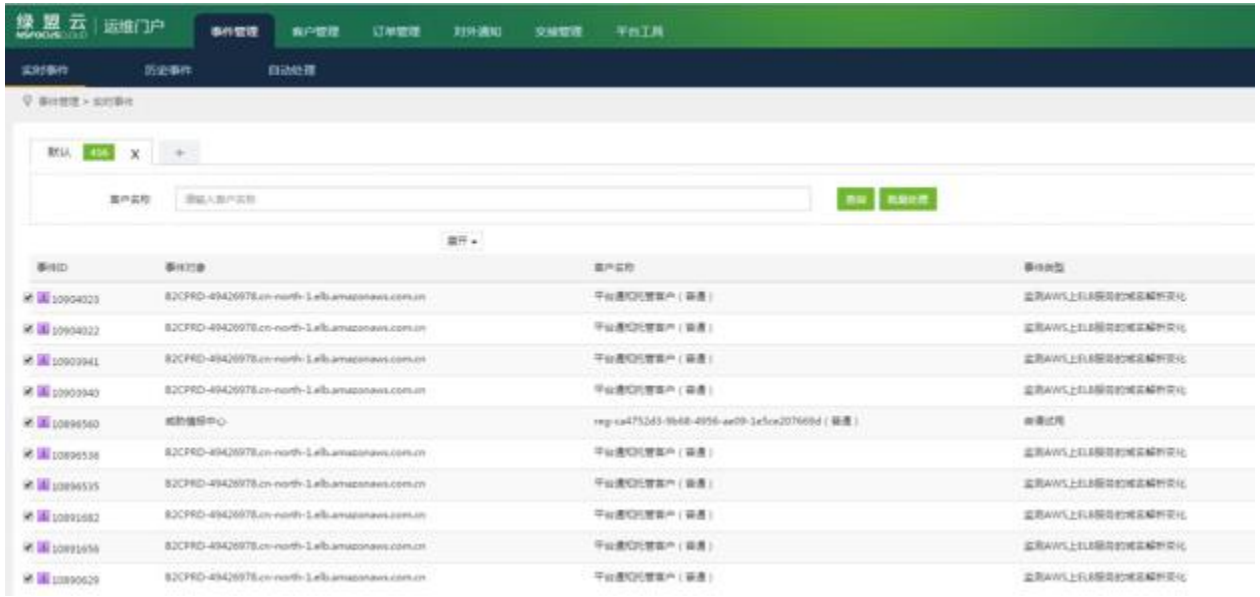
大闭环：从发现威胁到部署到产品，到确保防护效果

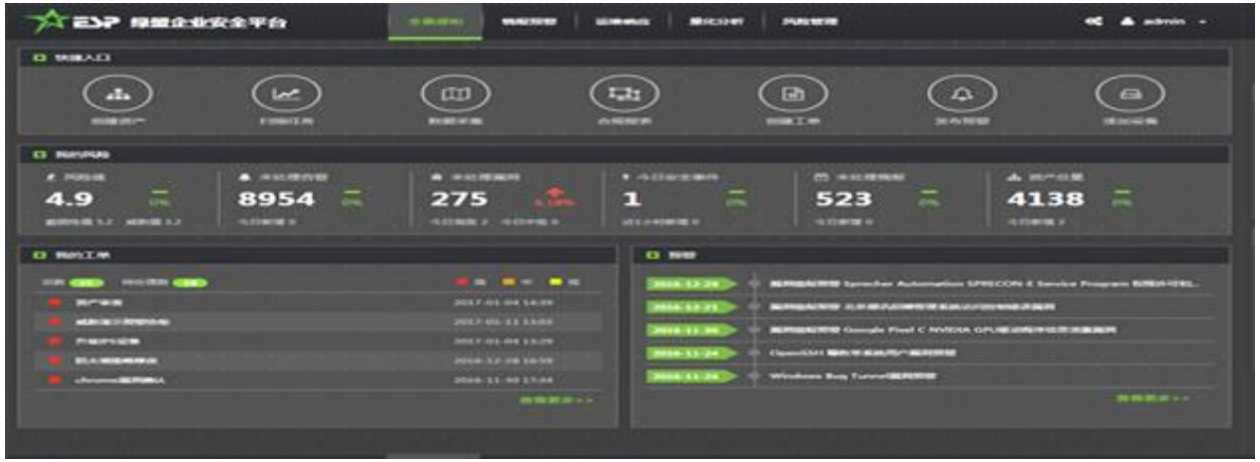
NSFOCUS

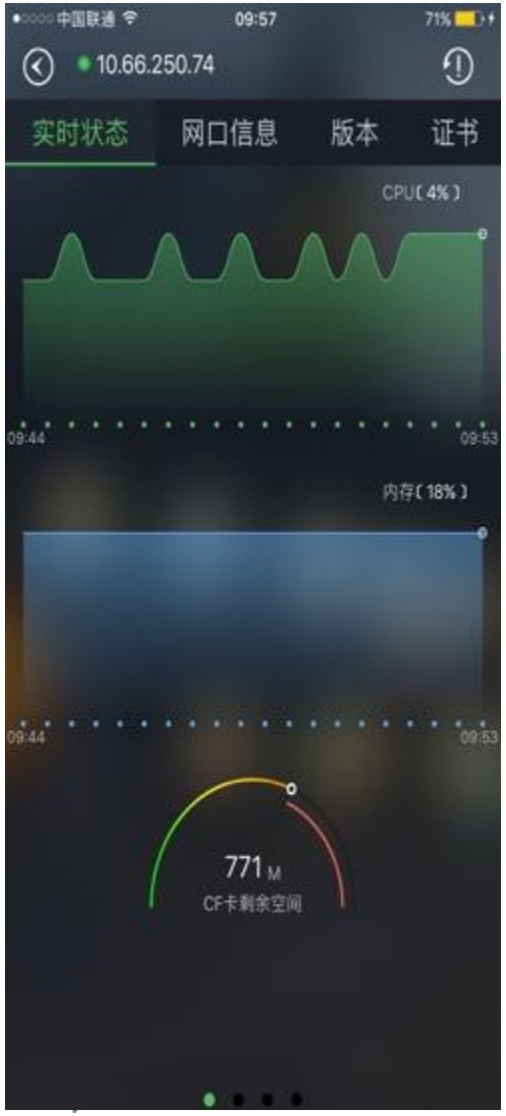
实践：网站安全监测与代维服务



实践：安全态势与运维平台







企业安全的生态圈

迎合国家发展IT服务业的战略，提供IT安全运营保障

社会

能让企业和组织机构能用更低成本引入专业安全能力

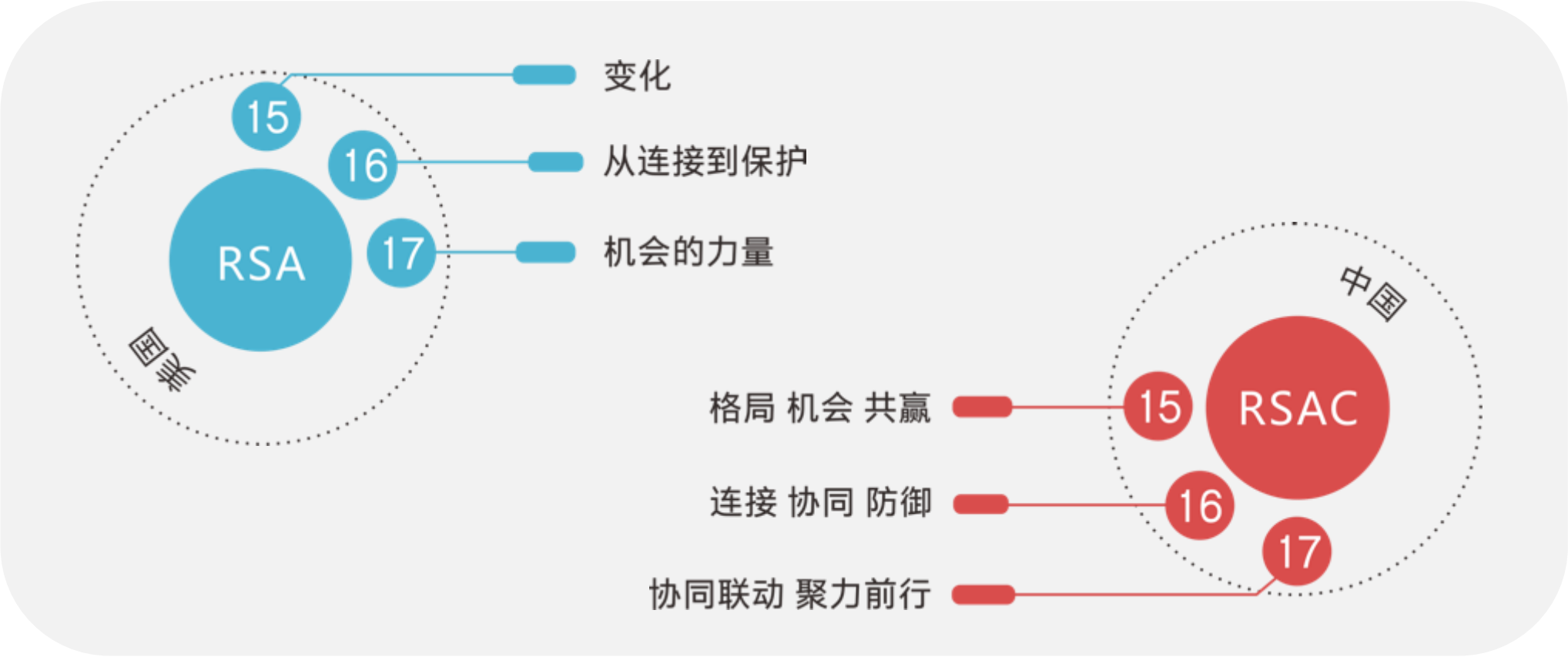
企业

构建一个分工更加精细化的相互协作的生态圈

产业

NSFOCUS

挑战、改变、共赢


15
16
RSA
17
美国
变化
从连接到保护
机会的力量
中国
15
RSAC
16
17
格局 机会 共赢
连接 协同 防御
协同联动 聚力前行

谢谢！

NSFOCUS