智能运营，安全赋能

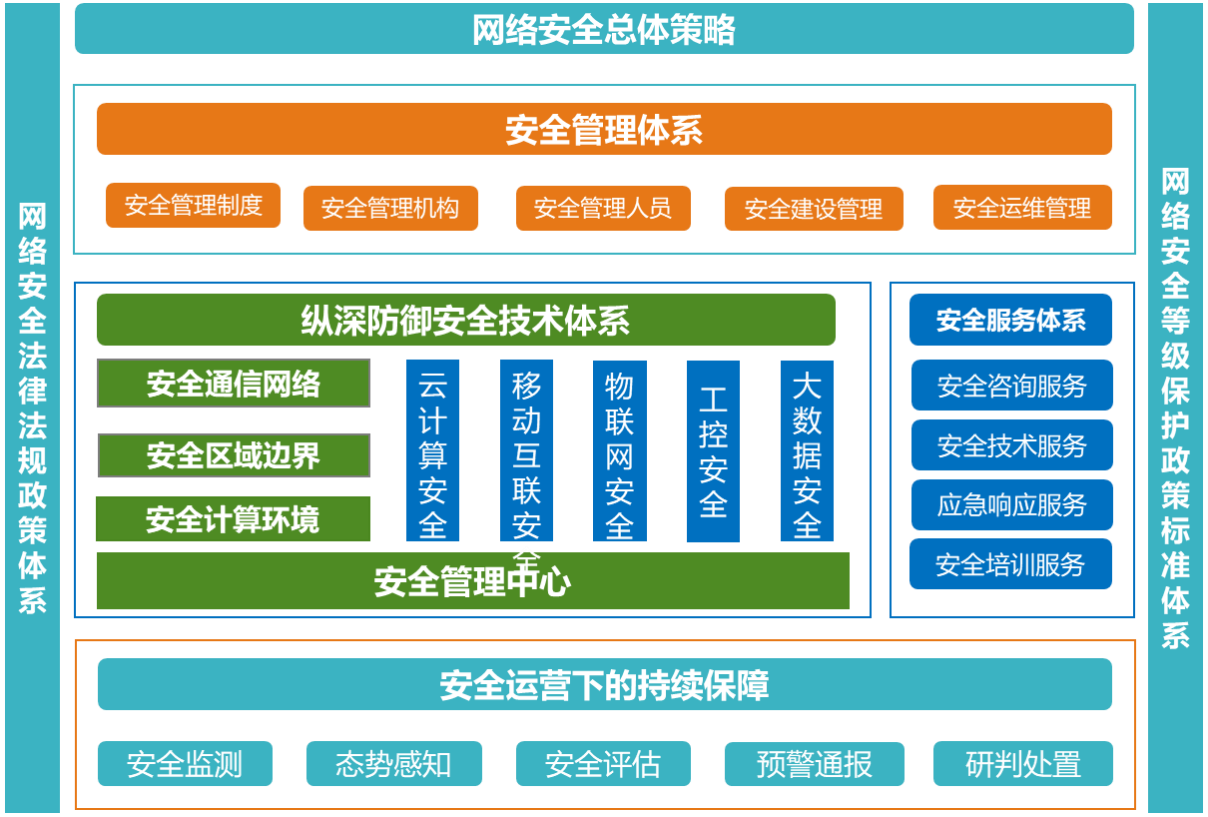
安全运营创新实践分享

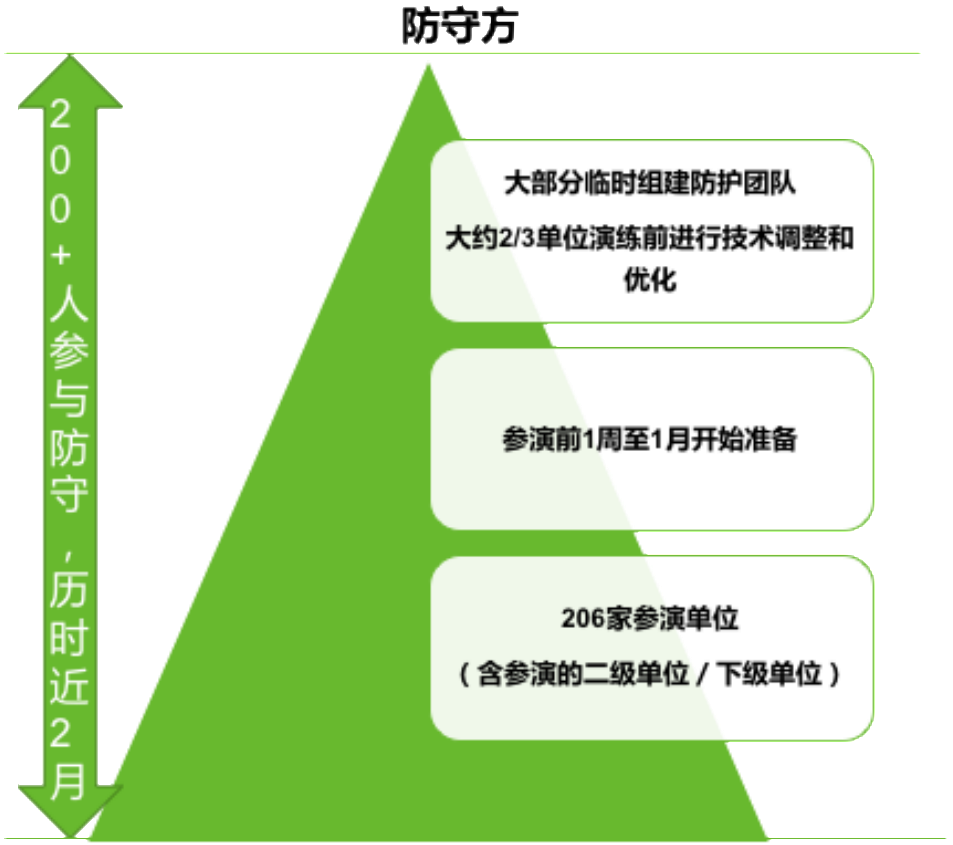
NSFOCUS

01

安全建设的机遇挑战

安全建设的长效机制与“临时工作”





从安全演练看企业安全防护现状

从日常安全运营角度看：人员、技术、管理都存在不足

没有落实安全监管职责

- 76%的二级单位对三级单位安全运营现状不了解；
- 100%采用外包运维的单位都没有对运维监管。

缺乏安全意识

- 61%的管理员低估系统存在的漏洞；
- 绝大部分安全管理员安全意识停留在业务可用性和企业形象上，不知道其他网络威胁和风险。

人员能力配置不足

- 仅有6%的单位配置威胁监控技术措施，能阻拦扫描和模拟攻击行为。

流程不规范

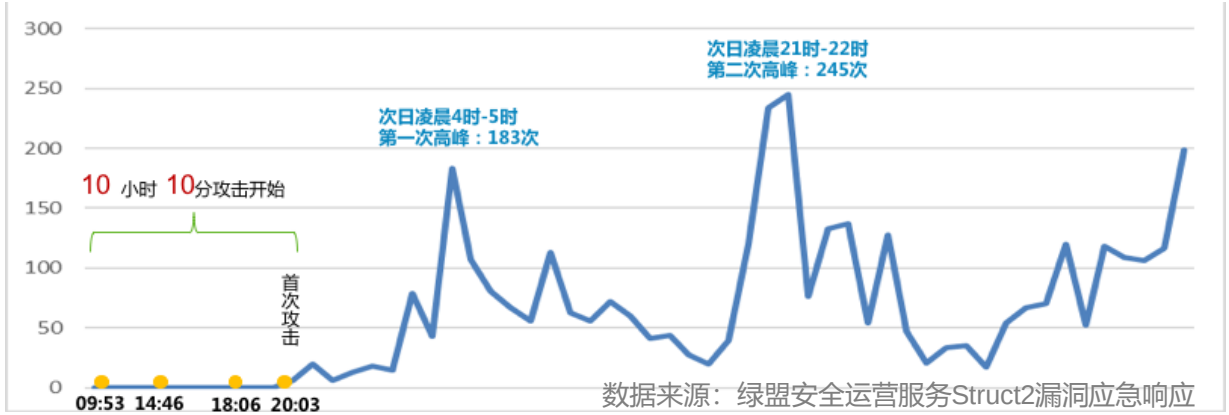
- 仅有4%的管理员知道对WEB漏洞采取预防措施
- 近一半的单位没有应急响应流程

数据来源：某央企全集团安全检查

大型企业安全防护面临的主要威胁与挑战

慢

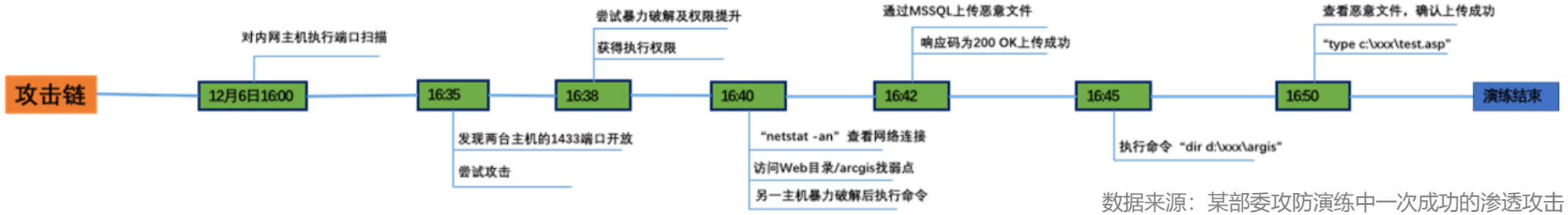
利用紧急漏洞的攻击行为在10-12小时被监测到



数据来源：绿盟安全运营服务Struct2漏洞应急响应

快

从扫描到非法获取主机权限只用了8分钟

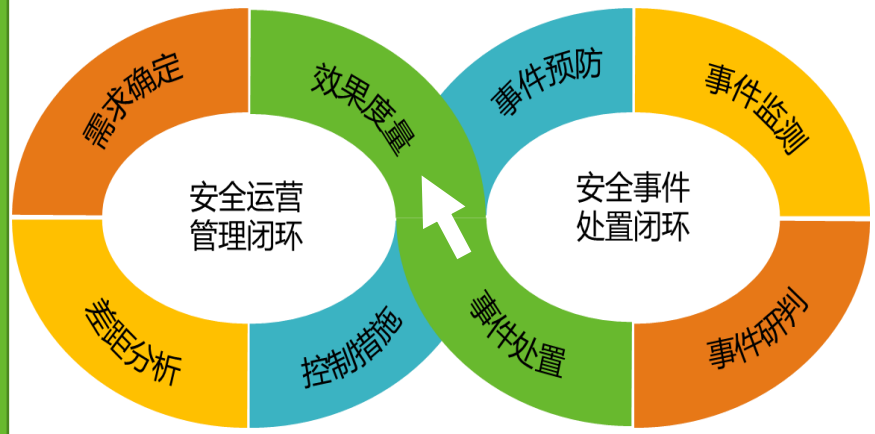


数据来源：某部委攻防演练中一次成功的渗透攻击

NSFOCUS

从攻防角度看企业安全防护的需求

2个闭环



2个高效

- 安全漏洞小时级闭环处置
- 安全威胁分钟级闭环处置

02

大型企业安全防护的运营思路

NSFOCUS

大型企业安全防护的运营规划体系

闭环的前提

第一步：安全需求分析

明确安全隐患与风险

- 现场调研访谈
- 安全咨询
- 攻防演练

资产变更产生的安全风险

- 主机 / 应用 / 端口 / 组件的变更导致的监控盲区

漏洞产生的风险

- 新曝光的重点高危漏洞导致的安全隐患
- 未修复及未防护的已知漏洞导致的安全隐患

威胁产生的风险

- 被攻陷主机产生的风险
- 漏洞利用等可疑行为导致的风险
- 威胁源导致的安全风险

第二步：安全能力差距分析

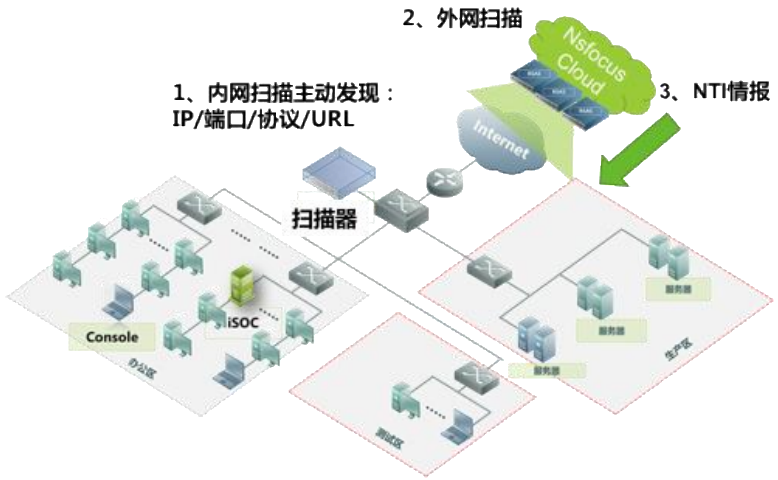
- 对照现有的标准与安全框架明确现存的能力差距

第三步：落实安全控制措施

- 根据安全能力差距分析的结果，明确技术、运维、管理上需要更新的内容与实施方案

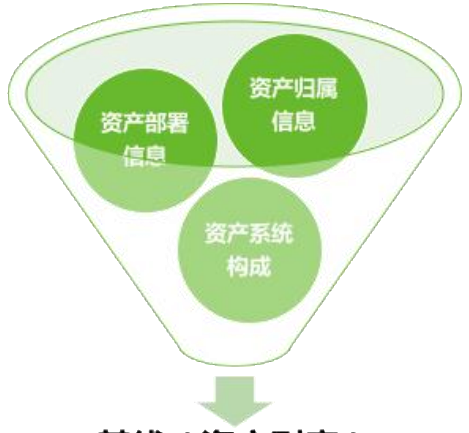
技术支撑方案

第一步：内网扫描 + 外网扫描 + NTI威胁情报补充



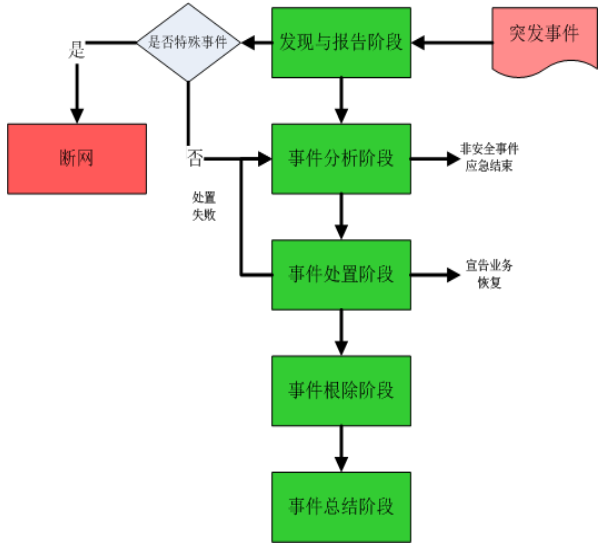
运维支撑方案

第二步：人工核实资产部署、归属和构成



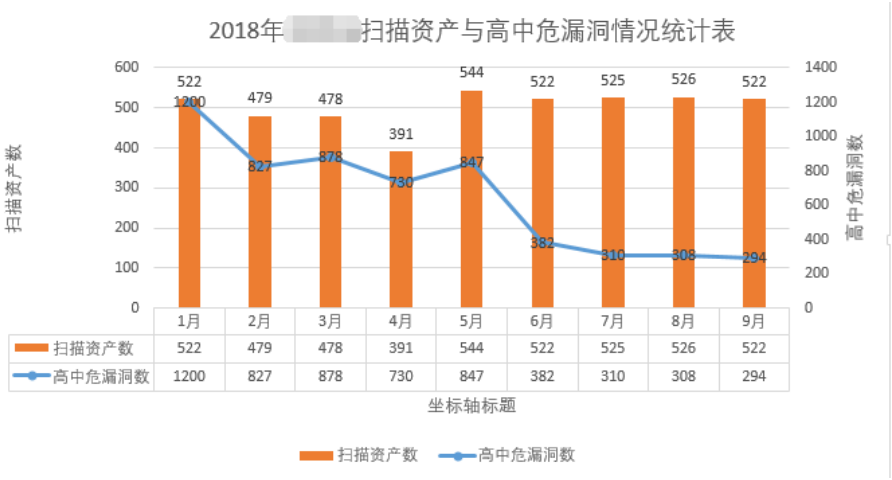
基线（资产列表）

配套的流程与职责分工



第四步：日常运营对控制措施进行度量和追踪

运营结果统计



	1月	2月	3月	4月	5月	6月	7月	8月	9月
扫描资产数	522	479	478	391	544	522	525	526	522
高中危漏洞数	1200	827	878	730	847	382	310	308	294

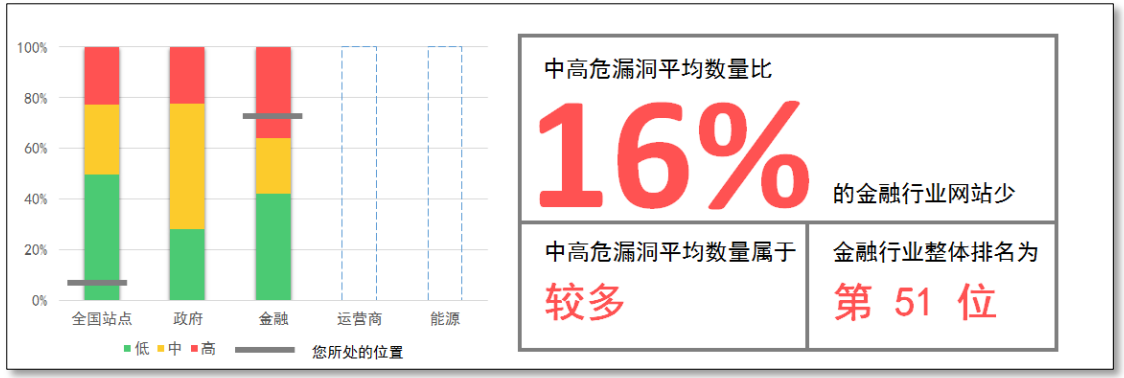
风险点处置追踪

漏洞定级建议　漏洞修复建议　漏洞修复验证　漏洞防护策略建议　漏洞状态跟踪

编号	资产域名	资产别名	所属单位	行政归属地域	待处理高危漏洞数	待处理中危漏洞数
1	w.net	河北 源信息网		(石家庄市)	6	49
2	ww .com.cn/	秦皇		(秦皇岛市)	6	0

ID	资产URL	漏洞名称	扫描类型	漏洞发现时间	漏洞处理时间	漏洞状态	详情
1	http://ww .com.cn/default.php	检测到目标URL存在跨站漏洞	web漏洞	2016-09-02 07:31:25	2016-09-08 21:38:30	待修复	查看
2	http://ww .com.cn/default.php	检测到目标URL存在跨站漏洞	web漏洞	2016-09-02 07:31:23	2016-09-08 21:38:30	待修复	查看
3	http://ww com.cn/default.php	检测到目标URL存在跨站漏洞	web漏洞	2016-09-02 07:31:25	2016-09-08 21:38:31	待修复	查看
4	http://ww com.cn/default.php	检测到目标URL存在跨站漏洞	web漏洞	2016-09-02 07:31:25	2016-09-08 21:38:31	待修复	查看
5	30.114	Microsoft Secure Channel 远程代码执行漏洞(CVE-2014-6321)(MS14-066)【原理扫描】	系统漏洞	2016-09-02 07:29:41	2016-09-08 21:38:36	待修复	查看
6	121.22.	Microsoft远程桌面协议RDP远程代码可执行漏洞(CVE-2012-0002)(MS12-020)【原理扫描】	系统漏洞	2016-09-02 07:29:41	2016-09-08 21:38:36	待修复	查看

漏洞处置率统计与排名（下级单位绩效评价参考）



中高危漏洞平均数量比

16% 的金融行业网站少

中高危漏洞平均数量属于	金融行业整体排名为
较多	第 51 位

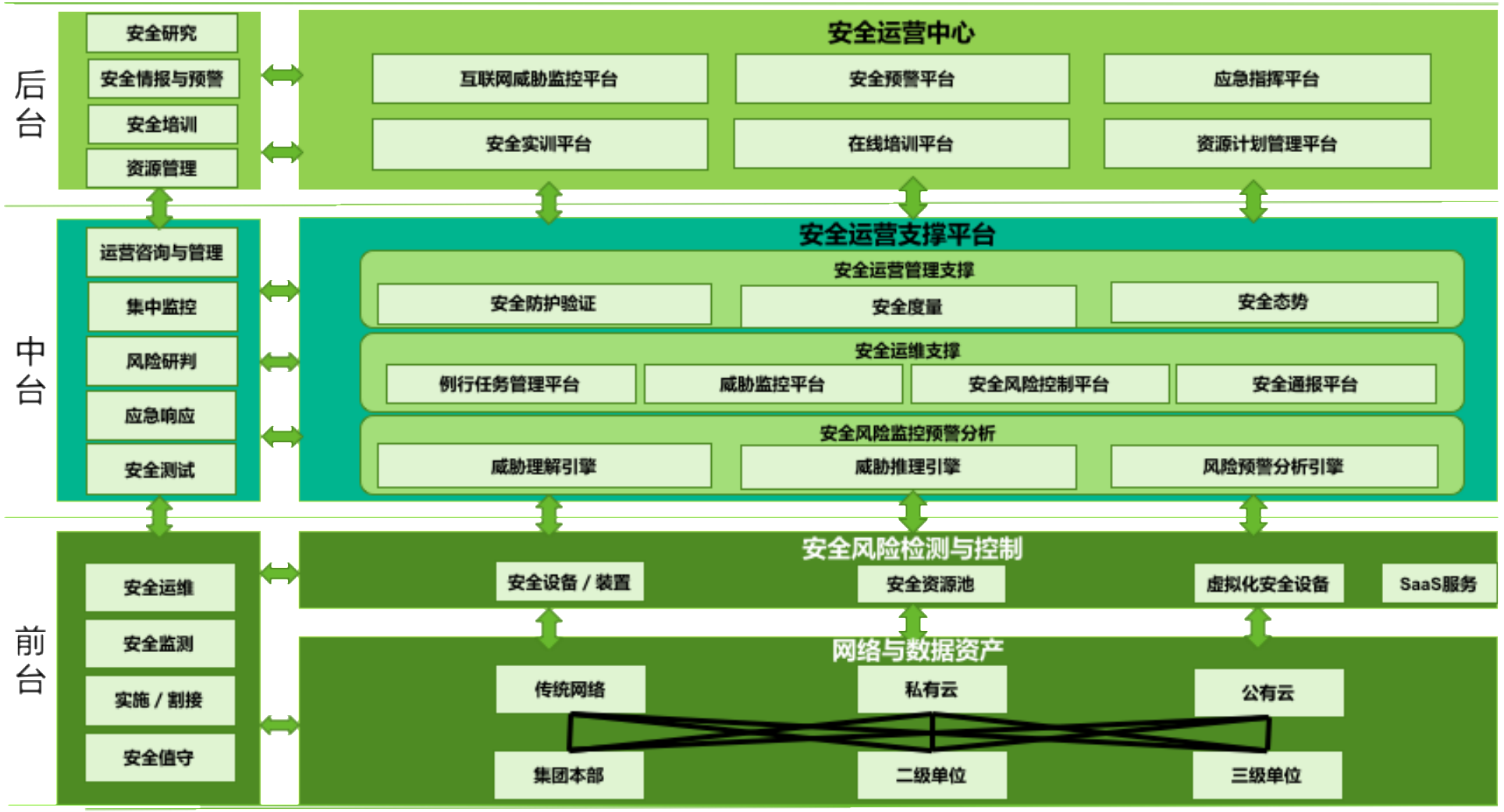
漏洞处置周期与排名（下级单位绩效评价参考）

网站漏洞平均存活周期比

95% 的金融行业网站更长

金融行业内漏洞修复时间	金融行业整体排名为
较长	第 56 位

大型企业信息安全防护的技术支撑体系



NSFOCUS

安全运营支撑中心

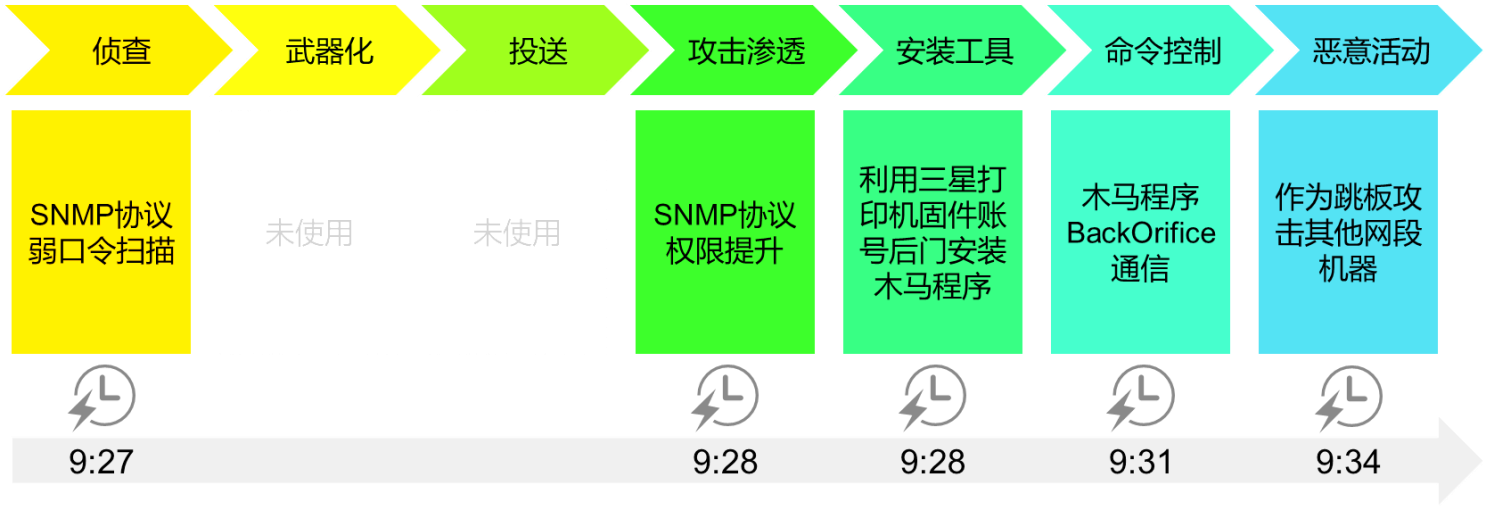
- 智能安全运营平台
  - 安全威胁快速发现
  - 安全风险闭环管理
  - 安全事件快速处置
  - 日常运营持续监控
- 安全运营技术支撑平台
- 安全响应效率提升平台

NSFOCUS

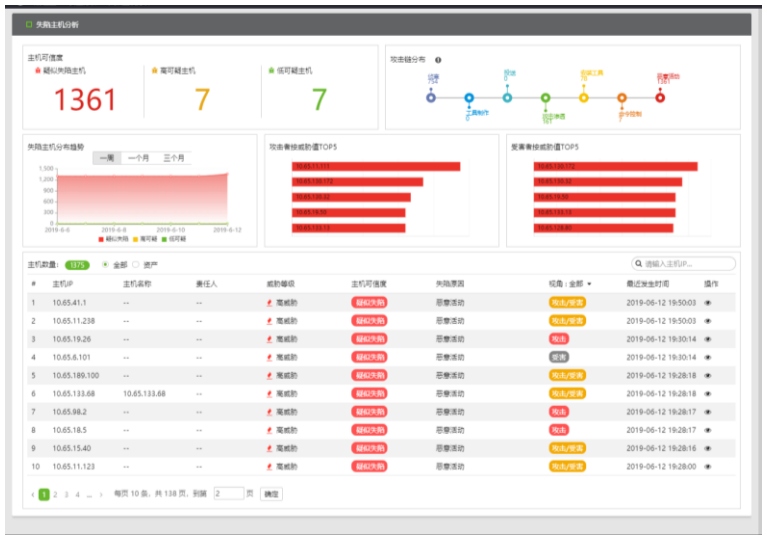
提高运营精度、告警准度、响应速度

面向网络运营和安全攻防的大数据分析

- 资产安全核查，全面发现脆弱性问题，对安全风险闭环管理，提高运营精细化水平。
- 基于攻击链的网络攻击分析，准确发现失陷主机，提高告警准度。
- 通过安全运营自动化编排，快速对攻击行为进行响应抑制，提高攻击响应速度。



某地客户发现攻击行为：7分钟内 数千万告警日志中 5条日志



准确告警高危资产，快速闭环响应

03

绿盟的运营实践

NSFOCUS

数字广东安全运营实践

建设“数字广东”

- 建设全省基础传输网络和宽带无线移动通信网络，实现粤港澳网络一体化；
- 建设网络民生、网络创新创业、公共服务在线化三大工程，实施数字家庭普及计划，实现信息技术和互联网在政务、商务、生产、生活中的普及应用，推进“信息兴农”工程，实现“泛珠”区域信息共享；
- 大力建设国家电子信息产业基地和国家级产业园，形成优势信息产业集群。

数字广东 Digital Guangdong　腾讯云　NSFOCUS

数字广东安全运营内容

01

安全评估

- 云平台安全评估
- 上线安全评估
- 业务安全评估
- …

02

重大保障

- 安全值守
- 日志分析
- 安全监控
- …

03

应急机制

- 应急预案编制
- 应急演练组织
- 应急事件响应
- …

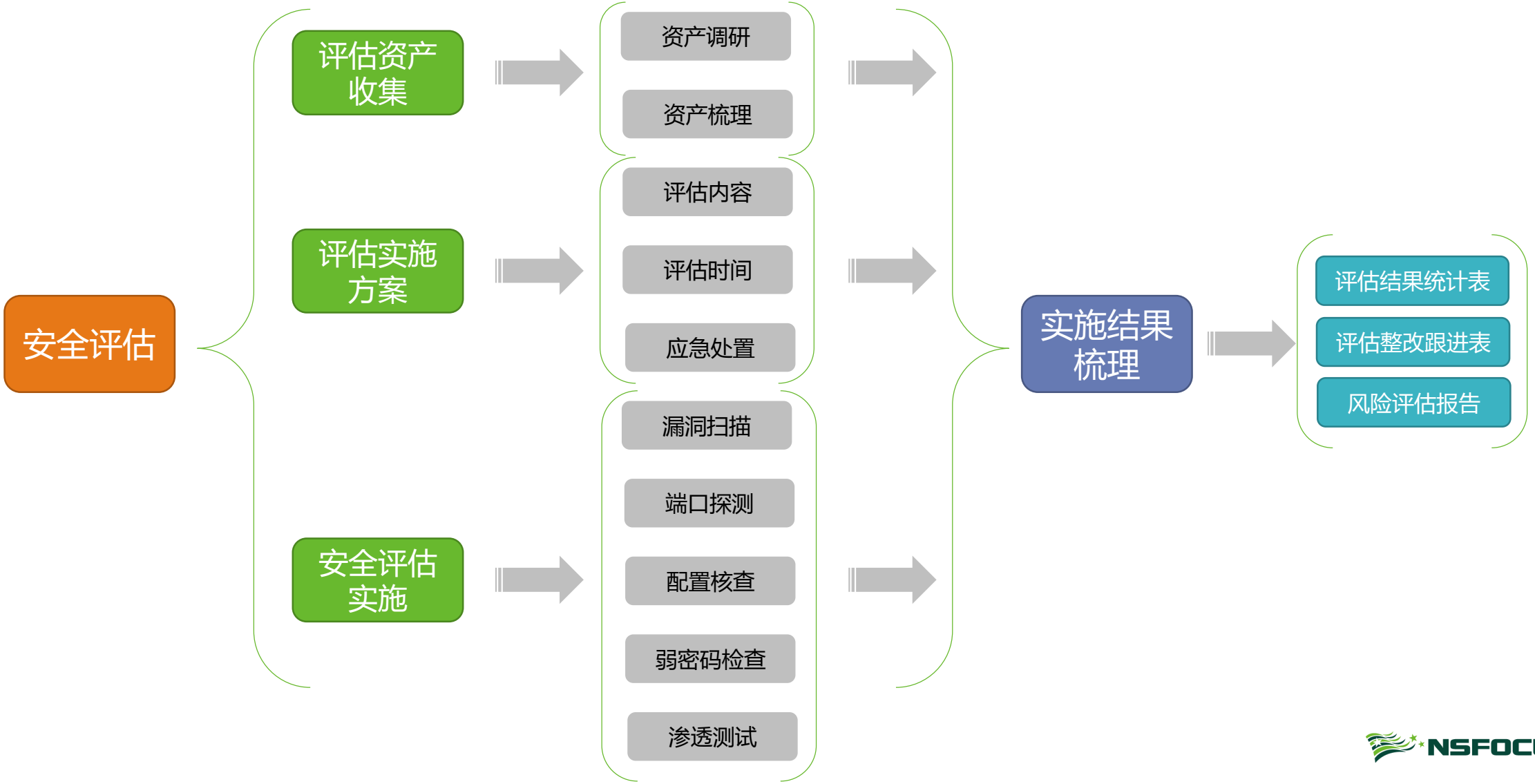
04

威胁预警

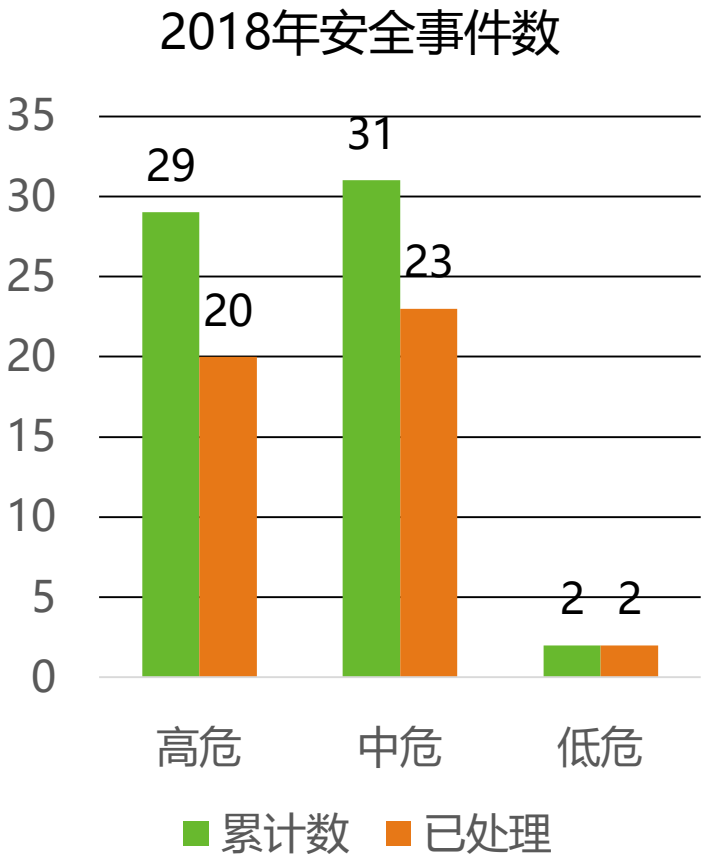
- 网站监控
- 安全通告
- 威胁预警
- …

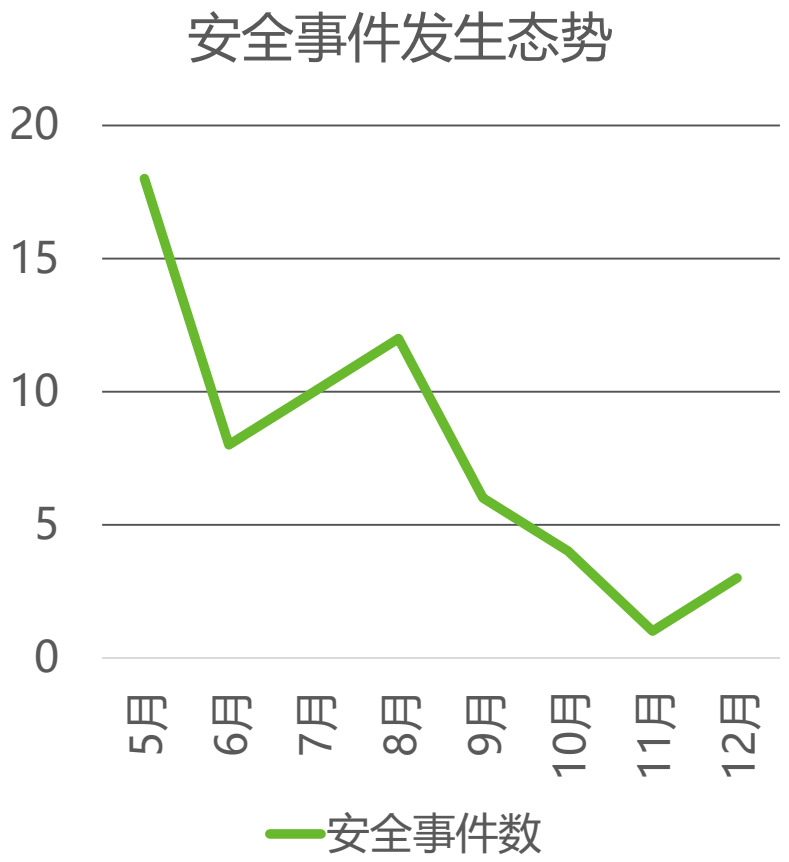
NSFOCUS

安全评估与差距分析



安全事件闭环处置





重保团队5月份入场开始，累计发现安全事件62起，闭环事件43起，事件处理率为70%，在团队努力下，政务云平台安全事件持续下跌。

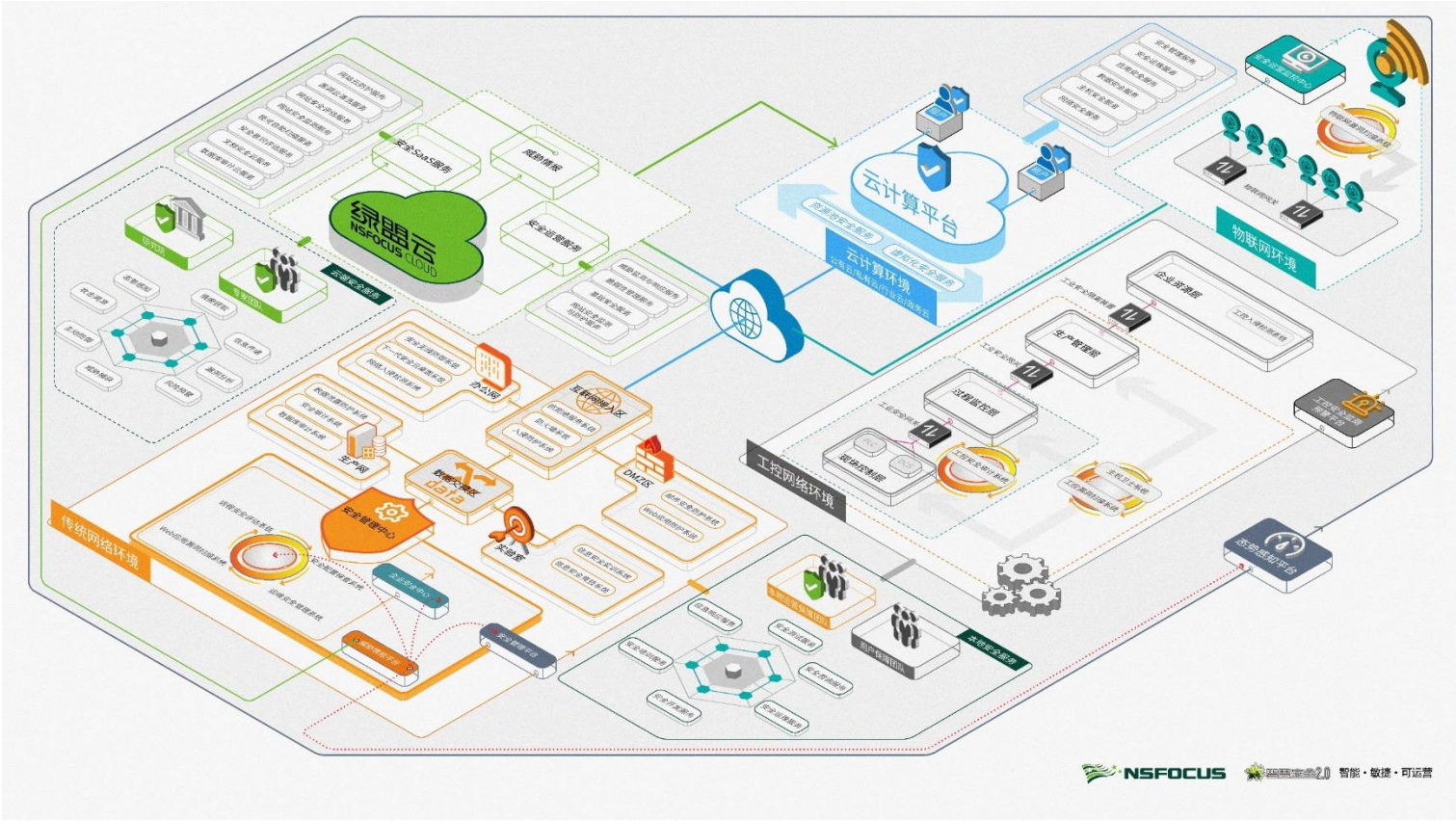
04

关于绿盟科技

NSFOCUS

绿盟科技

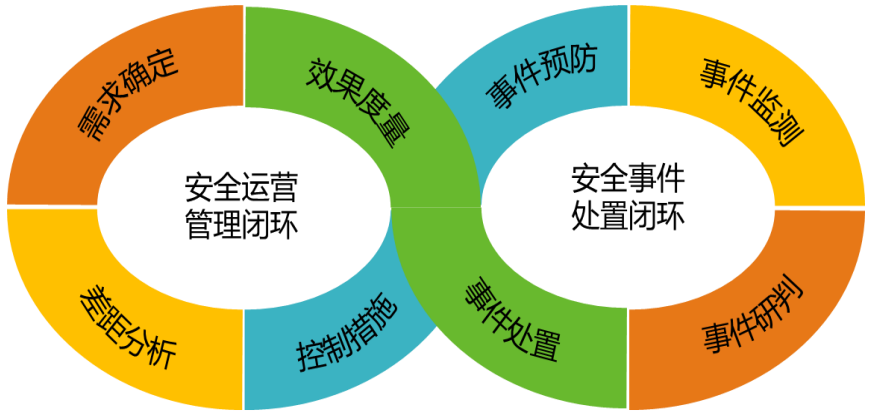
- 成立于2000年，全球40余个分支机构，3000+员工。
  - 网络攻击与防御
  - 云计算安全
  - 数据安全
  - 工控安全与物联安全
  - 安全运营
  - 漏洞挖掘与检测

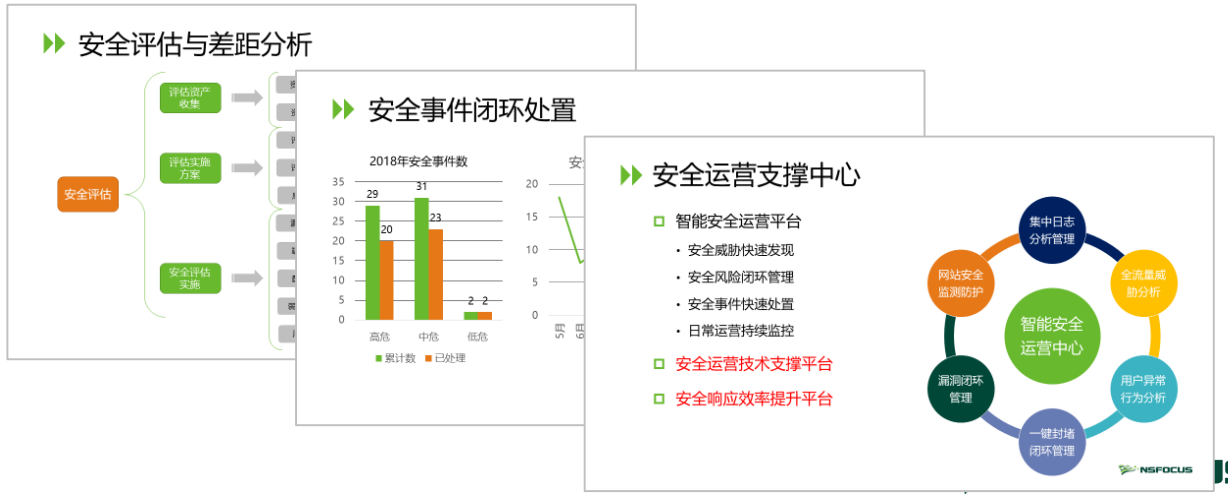


NSFOCUS

总结

- 关键信息基础设施保护工作的运营实践





谢谢！

NSFOCUS