NSFOCUS

TECHWORLD2019

绿 盟 科 技 技 术 嘉 年 华

探索 · DISCOVERY

NSFOCUS TECHWORLD

对抗下的服务能力提升

绿盟科技 曹嘉

国家级演习-Cyber Storm

- 美国Cyber storm
  - 国土安全部（DHS）-网络安全与基础设施安全局（CISA）执行，原则上每两年一次
  - 国会授权，重视和现实世界的互动，公私联合
  - 检查要点：网络安全准备情况、事件响应流程执行、社区程序和信息共享、以及相关整改

2006年

2006年 Cyber Storm I
首次国家级的全面演练，针对115个组织，主要考虑网络和通信降级以及关键基础设施的攻击

2008年

2008年 Cyber Storm II
审核检查个体的响应和决策能力，包括5个国家，18个联邦机构，40多家私营公司

2010年

2010年 Cyber Storm III
建立并执行国家网络事件响应计划（NCIRP），该计划成为国家级网络安全事件响应的蓝图，用于检查和管理国家网络事件响应的角色，职责，权限和其他关键要素。同时也增加了更多国家、部门以及公、私营企业
时长：5天

2011-2014年

2011-2014年 Cyber Storm V
15个小规模演习
环境：分布式

2016年

2016年 Cyber Storm IV
聚焦制造、运输部门、信息技术和通信部门以及执法，国防和情报机构
时长：一周，其中3天现场

2018年

2018年 Cyber Storm VI
聚焦情报与信息共享，包括阈值，路径，及时性，同时重点研究DHS与被攻击方的协调能力。

应急响应体系

• 国家级演练的首要目标

- 检验应急响应体系的有效性，制订流程和程序来识别和响应针对关键基础设施的攻击
  - 数据：Cyber Storm使得85%的组织具备了网络事件响应计划。

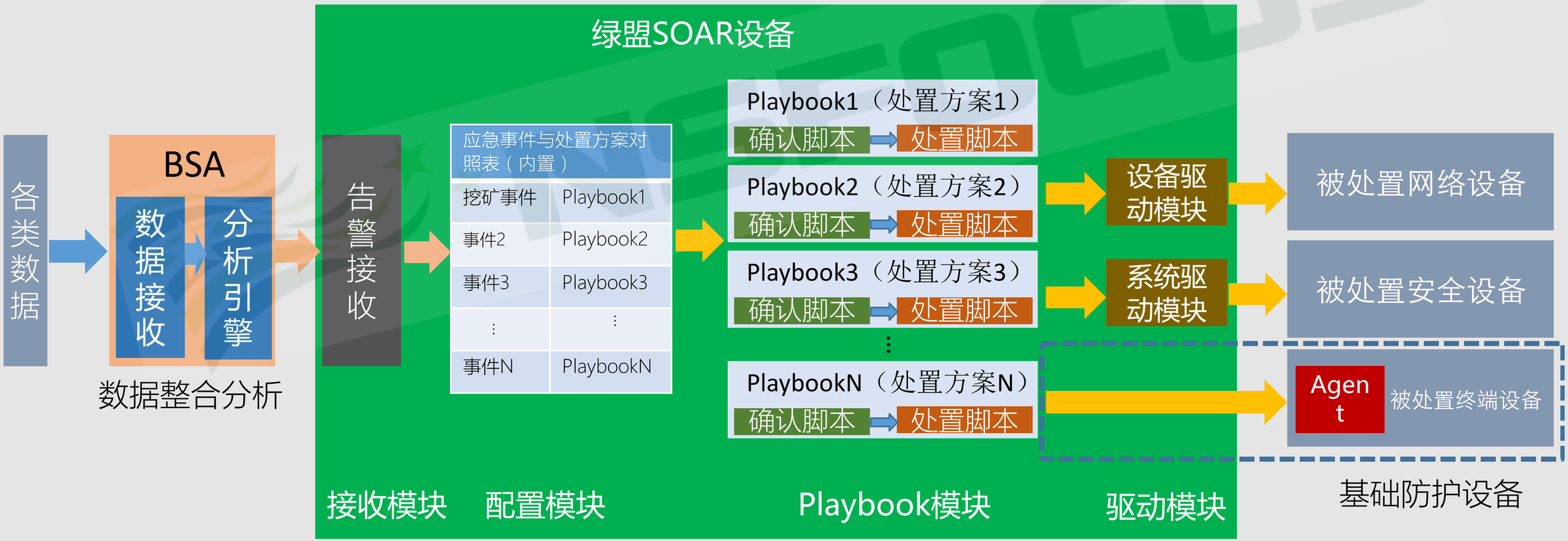
• 绿盟科技应急响应体系构建

- 建立单一的安全事件响应团队是启动运营的第一步
- 构建IR的事件库和知识库
  - 事件库：上下文、时间轴、IOC
  - 知识库：程序
- 基于场景的Playbook
  - SOAR

PDCERF是安全事件应急的通用过程

SOAR是IR必经之路

- 利用SOAR的价值：基于剧本，使用最直接最简单的手段（例如封禁IP）阻止尚且在攻击之初的攻击行为
  - SOAR内置剧本（playbook）基于人工经验、知识库、事件库编写



NSFOCUS

TECHWORLD2019 绿盟科技技术嘉年华

2018年应急事件SOAR处置可行性分析

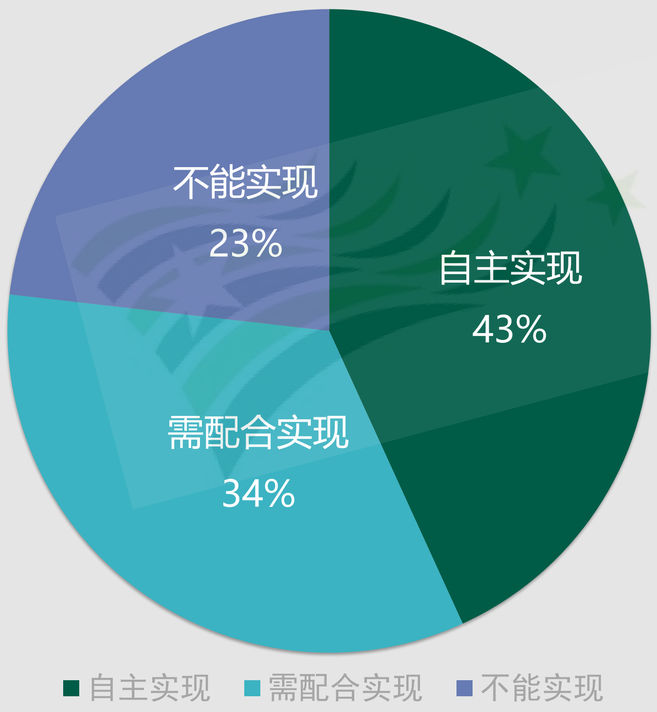
346件

2018年应急事件总数

SOAR能处置77%的事件

且能对几乎100%的事件进行干预。

2018年所有事件



自主实现

在公司已有的安全设备、SOAR按照预期设想实现全部功能、被保护环境完全按照严格设置的情况下，实现完整防御。
例如所有我司IDS、IPS能检测的攻击和漏洞，WAF、NF能发现的行为。

需配合实现

在"自主实现"基础上需要增加组件、模块、安装额外功能才能实现完整防御。轻度依赖人工。
例如针对特定程序攻击（例如最近的Jenkins 远程代码执行）。

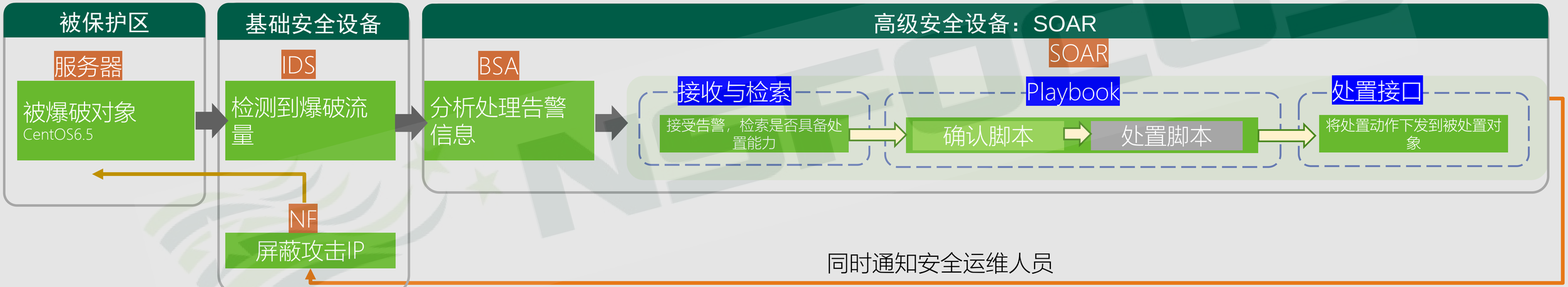
不能实现

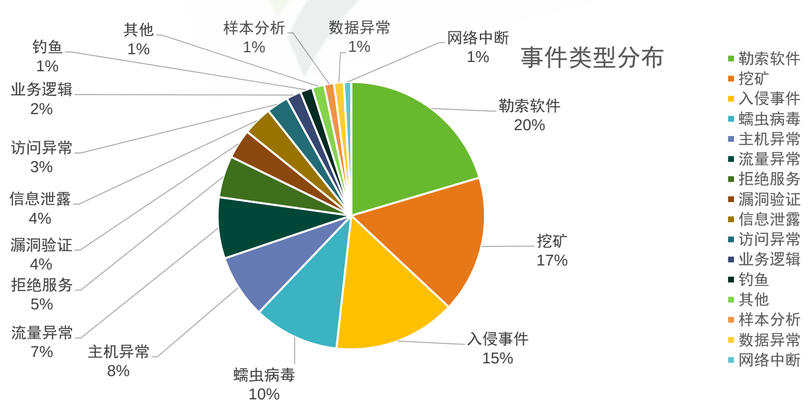
目前条件不具备该类事件的防御能力或者实现开销较大。主要依赖人工。但SOAR能干预并降低损失和危害。
例如APT、逻辑漏洞、复杂的攻击场景。

*基于2018年绿盟IRT数据以及其发布的《绿盟科技安全事件响应观察报告》

典型场景——SSH爆破：全自动处置

- 攻击效率提升明显，合理利用SOAR可以对冲掉攻击者的效率能力提升
- SOAR基于高置信度的威胁，适合轻量级的运营体系
- SOAR需要全网节点的密切配合才有发挥最大的作用





勒索病毒
- 侦测手段：从病毒传播途径下手，一般会通过内网密码爆破、溢出漏洞（永恒之蓝等）等途径传播。
- 处置手段：在防火墙上隔离被感染主机。

挖矿
- 侦测手段：挖坑流量有明显特征，已经能被主流IDS、IPS识别。
- 处置手段：封禁矿池IP地址。

蠕虫病毒
- 侦测手段：蠕虫病毒流量有明显特征，已经能被主流IDS、IPS识别。
- 处置手段：在防火墙上隔离被感染主机。

主机异常
- 侦测手段：根据主机日志，包括CPU占用率、单个进程占用率、内存占用率等资源数据分析。
- 处置手段：告警，提示人工介入处理。

利用F3EAD思想衔接“事件”与“情报”

IR可产生

- 高置信度的威胁情报
- 基于场景的Playbook
- IOC：IP、URL、HASH、Email等
- 样本
- CVE

查找-定位-消除-利用-分析-传播

- 查找：暗网上的信息泄漏、POC
- 定位：锁定事件
- 消除：服务关停、加固等
- 利用：IOC、样本等
- 分析：时间线、事件分析
- 传播：能力传递

- 威胁情报作为典型情报体系的输入，可以关注其情报成熟度

  - 设备消费
  - 内/外部情报整合
  - 结构化团队
  - 正式定义的工作流，基于SOC体系，将从被动事件响应转变为由主动情报驱动
  - 其他：暗网情报补充

情报体系-漏洞预警流程

- 源自Wannacry
  - 应遵循漏洞发布基本原则
  - 闭环能力是关键
    - 恶意IP-TI
    - 漏洞/利用-检测/防护能力
  - 情报团队独立运营

（二）不得刻意夸大漏洞的危害和风险；

（四）应当同步发布漏洞修补或防范措施。

——引自《网络安全漏洞管理规定》

0606
- Apache Shiro 反序列化漏洞
- Weblogic远程代码执行漏洞

0612
- 蓝方总结钓鱼文章预警

0613
- Axis远程代码执行漏洞

0614
- Coremail配置信息泄露

0619
- 帆软报表插件漏洞预警

0620
- 致远OA通用漏洞预警通告

NSFOCUS

TECHWORLD2019 绿盟科技技术嘉年华

基于“事件”和“情报”的运营体系建设

协同

流程顺畅，各司其职

解决问题，保障业务

预警，应急组织体系

情报

广收，精准，共享

高效，闭环

情报闭环流程

数据

过程数据展现态势

服务报告深挖价值

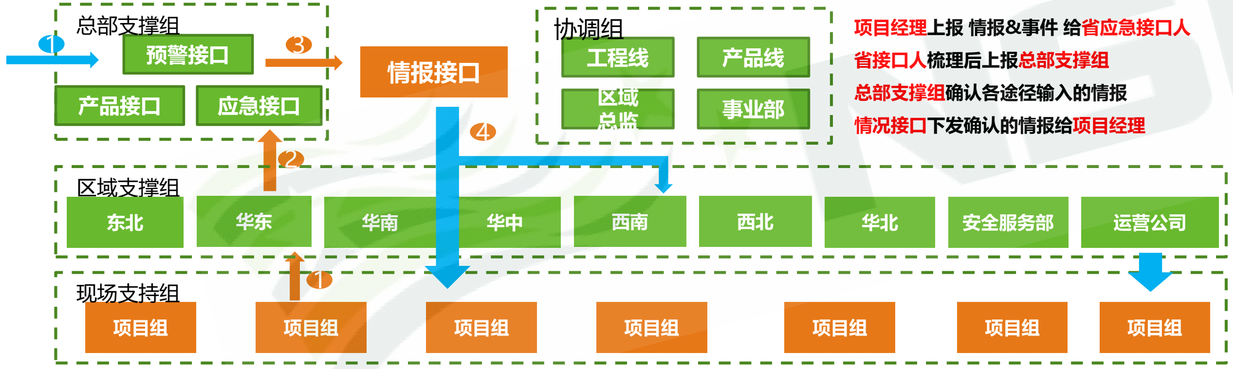
项目管理报告模板

知识

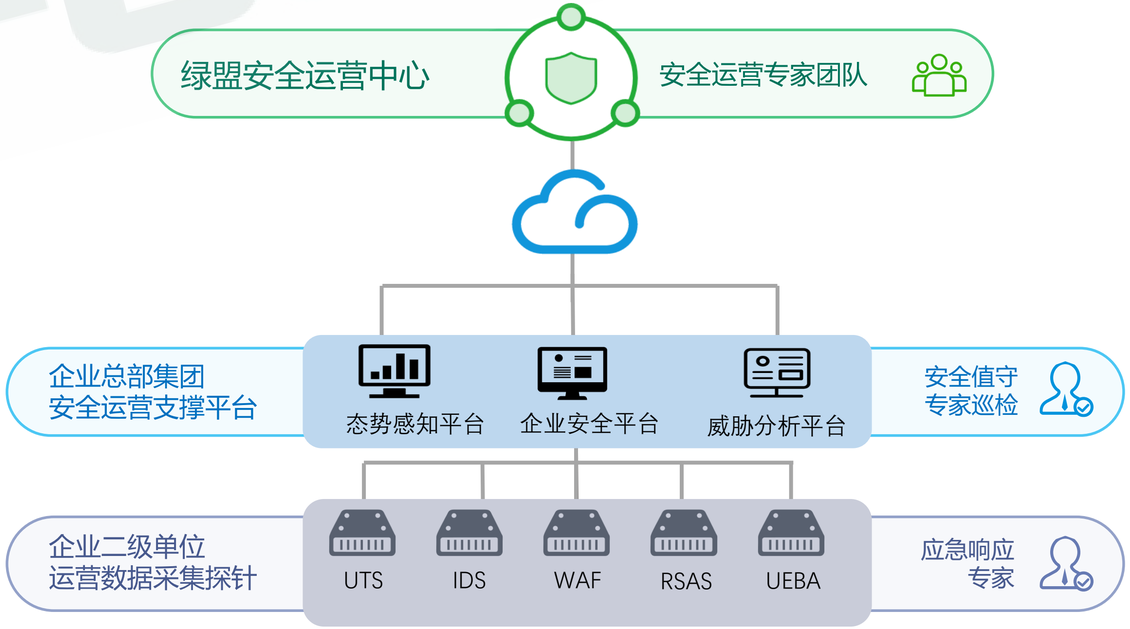
沉淀知识，分享经验

持续改进，能力扩展

复盘，整理，固化



应急处置	共处理应急事件57起,75%的平均的闭环时间在63.57小时，约2.64天处理一个应急事件
预　　警	25个攻防场景中，转化为预警情报共有12个;产品功能共升级32次，提供临时方案23次，平均闭环时间：21.61小时
情报处理	上报情报1885条，经研判，有效情报1645条，归类合并后下发情报195条



集成SOAR和TI等能力的协同平台

基于“事件”和“情报”的运营体系建设

某国产OA应急事件·

阶段一：某客户发现被挂webshell，发起应急

阶段二：应急过程，结合WAF拦截日志进行攻击路径分析，成功还原攻击者攻击入口点（某OA伴生安装决策系统），可直接设置管理员账户密码

事件响应体系

运营体系 Axis 0day

预警体系

对应产品规则	
WAF	自定义规则 update_rule.p6.0.4.1.41873.wcl update_rule.v6.0.5.1.41873.wcl update_rule.v6.0.6.1.41872.wcl update_rule.v6.0.7.0.41869.wcl update_rule.v6.0.7.1.41871.wcl
IPS	5.6.10.20521 5.6.9.20521 5.6.8.784
UTS	5.6.10.20521

对应产品规则	
WAF	自定义规则
IPS	自定义规则

阶段一：客户侧防篡改设备发起告警，触发应急流程

阶段二：从全流量设备上抓取完整漏洞利用细节，复现POC

阶段三：应急分析过程形成技术分析及处置手册，发布至现场，并同步产品团队完成产品规则更新

安全运营与红蓝对抗

ROI作为主要运营指标，驱动了对抗性服务的发展

- 安全运营是一项重大投资，从来不乏检出率超过99.9%的产品存在...

蓝队服务与渗透测试的区别

- 除了常规的测试导向、测试深度、隐蔽性等决定性因素
  - 业务侧重：利用真实有效的模拟攻击来评估因为安全问题所造成的潜在的业务影响，为企业管理者提供有效的数据来量化安全投入的ROI。
  - 决策影响力
  - 范围更广
    - 时间：持续性更强
    - 空间：业务线以及地域更广
  - 入侵假设
    - 假设黑客已经经过认证和授权
    - 假设所有数据都可以访问

NSFOCUS

TECHWORLD2019 | 红蓝对抗与ATT&CK

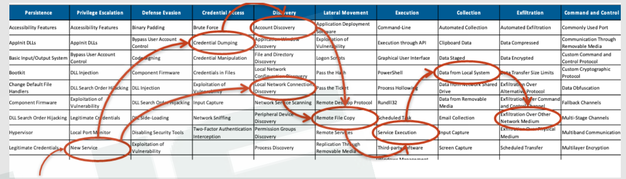
绿 盟 科 技 技 术 嘉 年 华

- 面对网络空间环境、监管手段的升级，“红蓝对抗”将会发展成精英化服务
- 基于MITRE ATT&CK的最佳实践
  - 基于真实攻击场景
  - 统一且结构化的呈现方式
- 产出物
  - 攻击剧本（playbook）
  - 差距分析报告
  - 企业防护手册

检测分析

持续的研究ATT&CK威胁设计模型

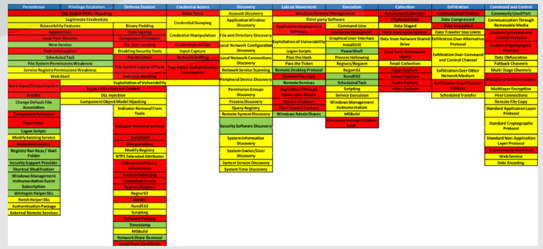
开发适用自己企业的用例-技术，战术及策略



模拟攻击

从防御角度验证和模拟攻击者行为

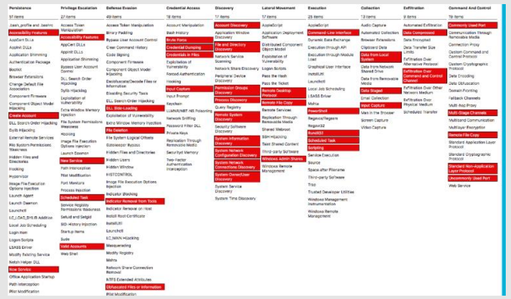
Red-Team/Blue-Team测试



防御措施差距评估

验证现有防护措施策略和技术效果

明确优先改进措施及手段



网络威胁情报使用

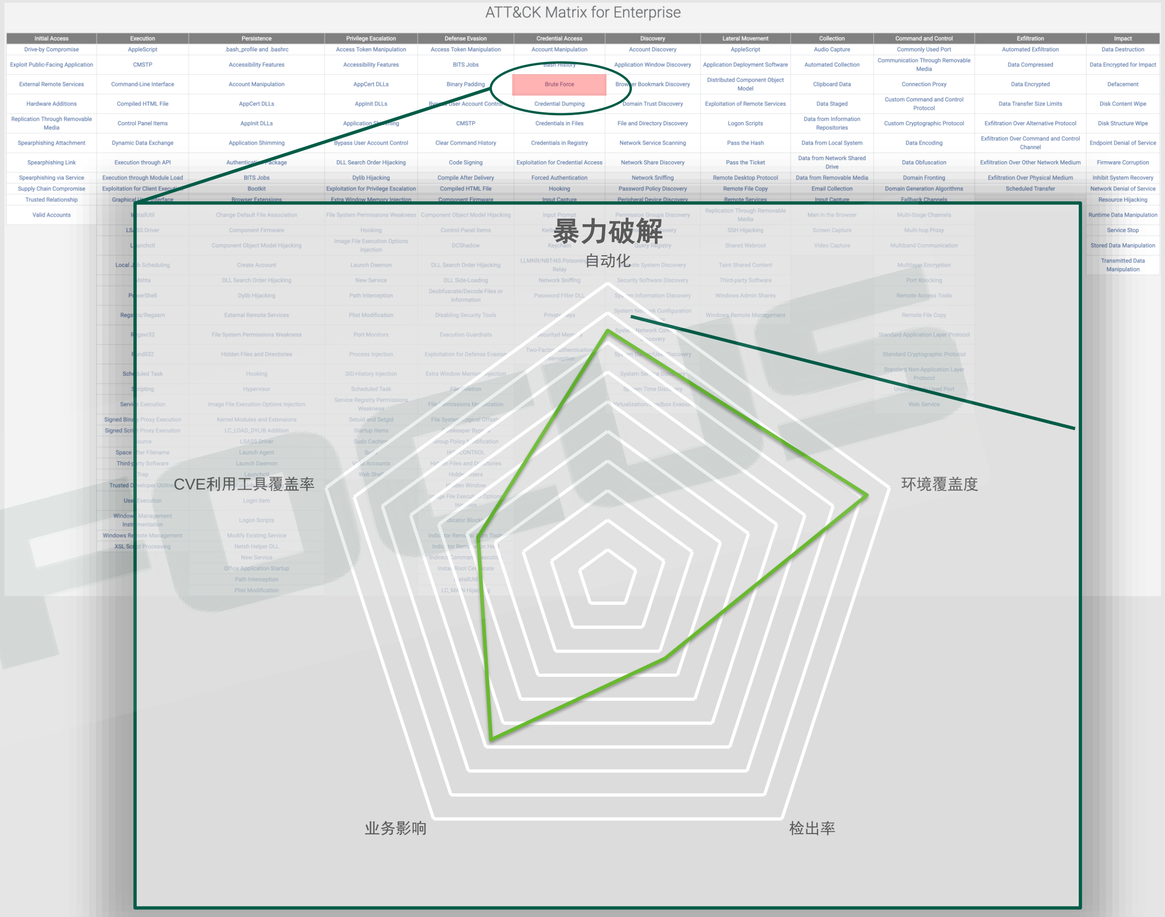
未知行为检测方法开发

安全运营成熟度评价分析

ATT&CK度量

- 以ID: T1110（暴力破解）为例

维度编号	衡量维度
1	自动化程度
2	CVE利用工具覆盖率
3	业务影响程度
4	检测率
5	环境条件覆盖度
6	持久度
n	…



对某团队从五个维度进行评估，通过计算，该团队84%的场景可以使用自动化工具完成，可以覆盖92%的爆破环境，在实战中33%的概率可以被检出，67%的场景下会对业务有影响，掌握46%暴力破解相关CVE利用工具，那么通过上述公式计算，得出该团队在该项能力上的成熟度为68.90%

每项技术成熟度由各个不同的衡量维度结合技术成熟度模型来构建

$$T=\sum_{t=1}^{n}(W_t \times C_t)$$

长期对抗能力建设-精英化之路

NSFOCUS

▶▶ 绿盟科技四大战队重装上阵

FIRE HAWK 烈鹰战队

TIGER-WARRIOR 虎贲战队

M01N 模因战队

M-KING 梅花K战队

行业对抗性升级

- Cyber Storm过程中的0/N day
- 团队协同性增强
- 自研武器库
- 对抗长期性

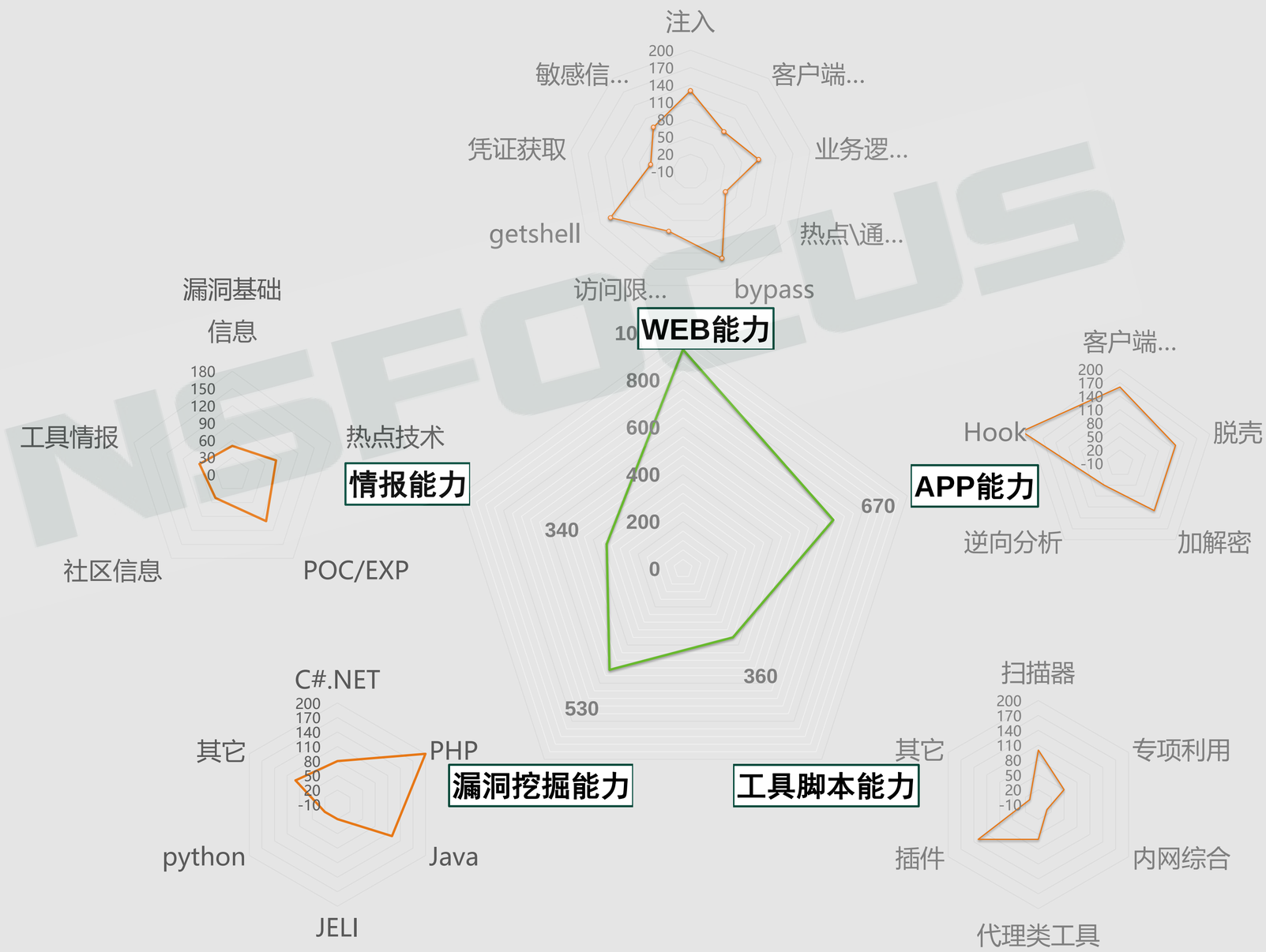
考核导向

- 对抗性服务业绩指标
- 人才培养指标
- 核心能力支撑指标

草根的力量-社区化之路

社区化目标

- **丛林式管理**：通过参与项目和参与社区进行双重考核（主动被动），创造基于“丛林法则”的生态运营模式。
- **建立内部技术圈**：促进纵向技术交流，扩充测试人员之间的“交友”范围。
- **人员能力画像**：统一考核维度，针对不同人员的不同能力，进行定量分析及展示，最终结合业务进行定向培养及人才遴选。



安全服务能力、体系与业务的构建

	培养体系	流程建立	知识管理	服务化/产品化能力	商业痛点	示例
能力	✓		✓			IR能力
体系		✓	✓			情报与预警体系
业务			✓	✓	✓	红队对抗服务

服务化业务的转型

- 单独服务模块→全面解决方案
- 定制需求多，个性化高成本→标准产品
- 本地化资源→统一资源

服务创新能力

服务产品的创新一般不具备研发过程，而是通过改善流程，优化运营来实现

- 产品创新：NSCTF
- 过程创新：方法论创新
- 组织创新：Red Team
- 市场创新：Cyber Storm

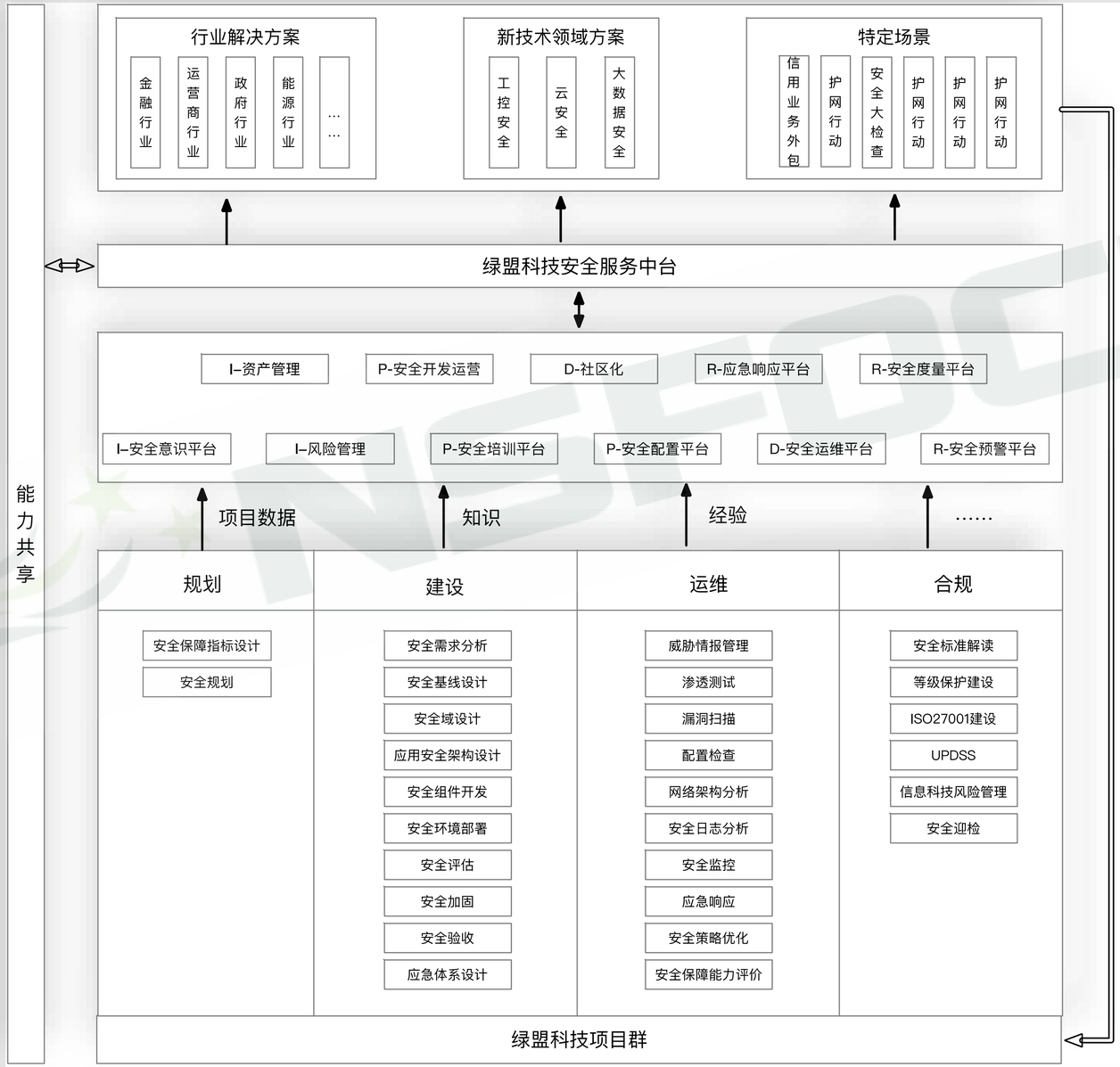
NSFOCUS

TECHWORLD2019

绿 盟 科 技 技 术 嘉 年 华

绿盟科技安全服务体系2.0

- 关注客户安全ROI
- 关注能力和业务的平衡
- 建立各项业务的数据管道、运营管道、知识管道



服务解决方案设计岗位

服务产品经理

安全运营岗位
安全架构师

安全交付岗位

项目经理

总结-国家级应急演习

应急响应体系

应急响应组织、程序和路径

- 具有清晰的应急响应时间线和SOP程序
- 建立区域-中心的应急响应机制
- 基于SOAR的知识能力构建

情报社区

- 威胁情报+预警，实现内外部闭环

蓝队能力

能力将会加速向红队转移

- 对安全运营的ROI
- 基于ATT&CK的评估和度量体系
- 精英化、武器化、持久化

面向结构化团队的角色能力、运营体系和服务业务的讨论

- IR：事件响应
- 情报：本地/云端运营人员
- 红队：内外部对抗团队
- 威胁狩猎……

改变设备堆砌（安全基础设施）、厂商堆砌（能力异构、情报共享）、驻场服务（日志分析、本地化响应、报表能力）的低效现状

改变简单将安全人才分为研究、开发和工程类人才的基础分类，而改为按照场景划分

NSFOCUS

TECHWORLD2019

绿 盟 科 技 技 术 嘉 年 华

探索 · DISCOVERY

NSFOCUS TECHWORLD

感谢聆听！