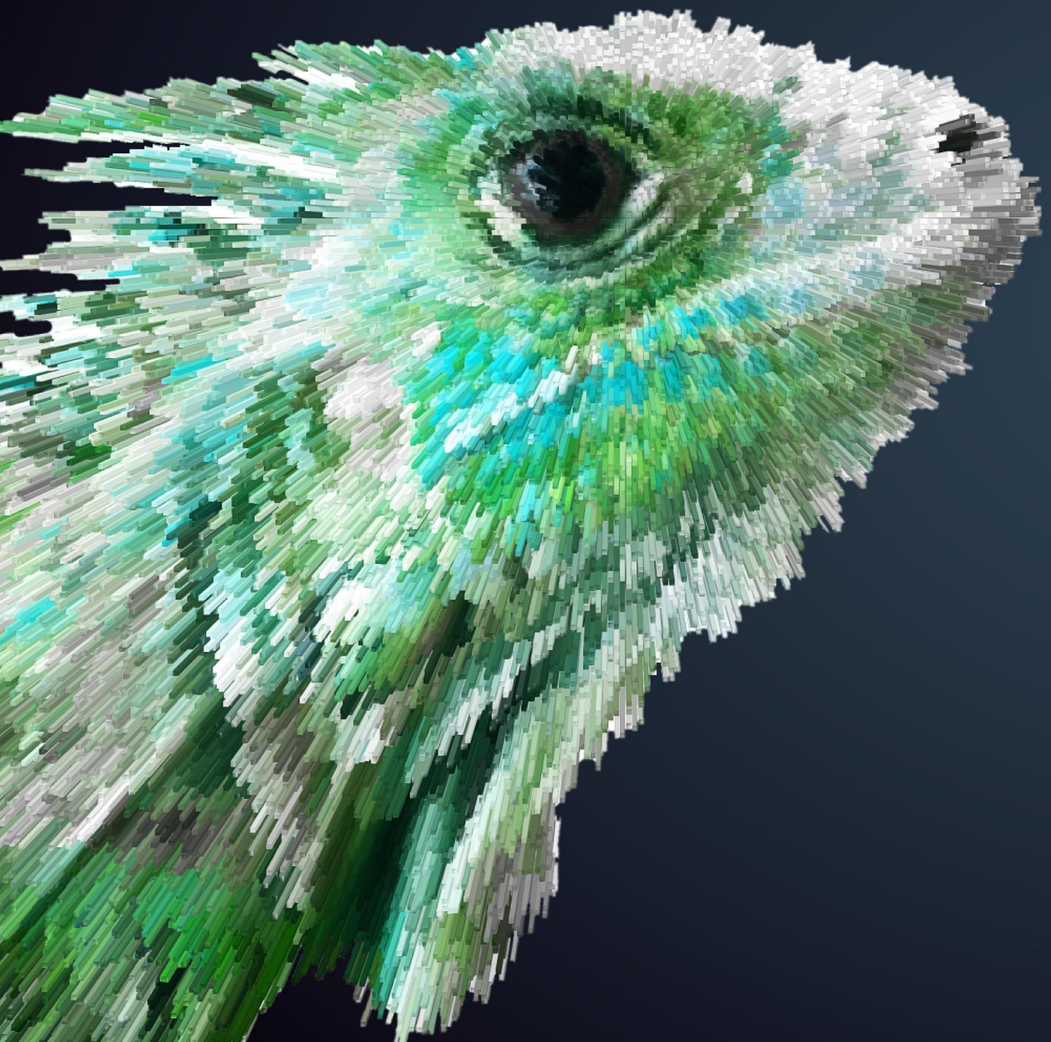
「融合·CONVERGENCY」

TECHWORLD 2021

绿 盟 科 技 技 术 嘉 年 华



基于情报驱动的实战化运营体系

绿盟科技 曹嘉

NSFOCUS TECHWORLD | NSFOCUS

「融合·CONVERGENCY」
TECHWORLD2021
绿 盟 科 技 技 术 嘉 年 华

2021年对抗趋势

2021年攻防演练攻击方

“从成长期走向成熟期”

0day为王，“人”者无敌

共监测到148个有效漏洞，69个0day漏洞，79个Nday漏洞，漏洞数量相较去年增长147%，应急的63起钓鱼事件中，包含热点事件钓鱼、利用浏览器内核漏洞对微信PC用户钓鱼等

更多资源投入漏洞挖掘、收集购买0day漏洞，以争取正面突破得分；愈趋成熟的钓鱼攻击结合0day漏洞利用，更加难以防护。

零日漏洞

伪装通信，隐匿行踪

接收到的恶意样本中反沙箱占19.5%，免杀占78%，流量伪造占46.3%，开展溯源的501个真实对象中，使用CDN/云函数相关隐蔽技术的达113个，同比往年大幅度增加

免杀、伪装、隐匿技术发展趋成熟，技术开放使相关技术得到更加广泛应用

隐蔽隐匿

2021年攻防演练防守方

“孤军奋战已不适应攻防趋势”

情报驱动，主动狩猎

基于情报的联防联控机制，完成了121个真实攻击者画像，形成了13个攻击组织画像，其中包括5个蓝军，并成功追踪多个APT/黑灰产组织

实战对抗瞬息万变，基于情报的联防联控机制，主动狩猎，提前防控，是应对规模化、武器化、自动化的攻击集团及境外势力的有效手段

联防联控

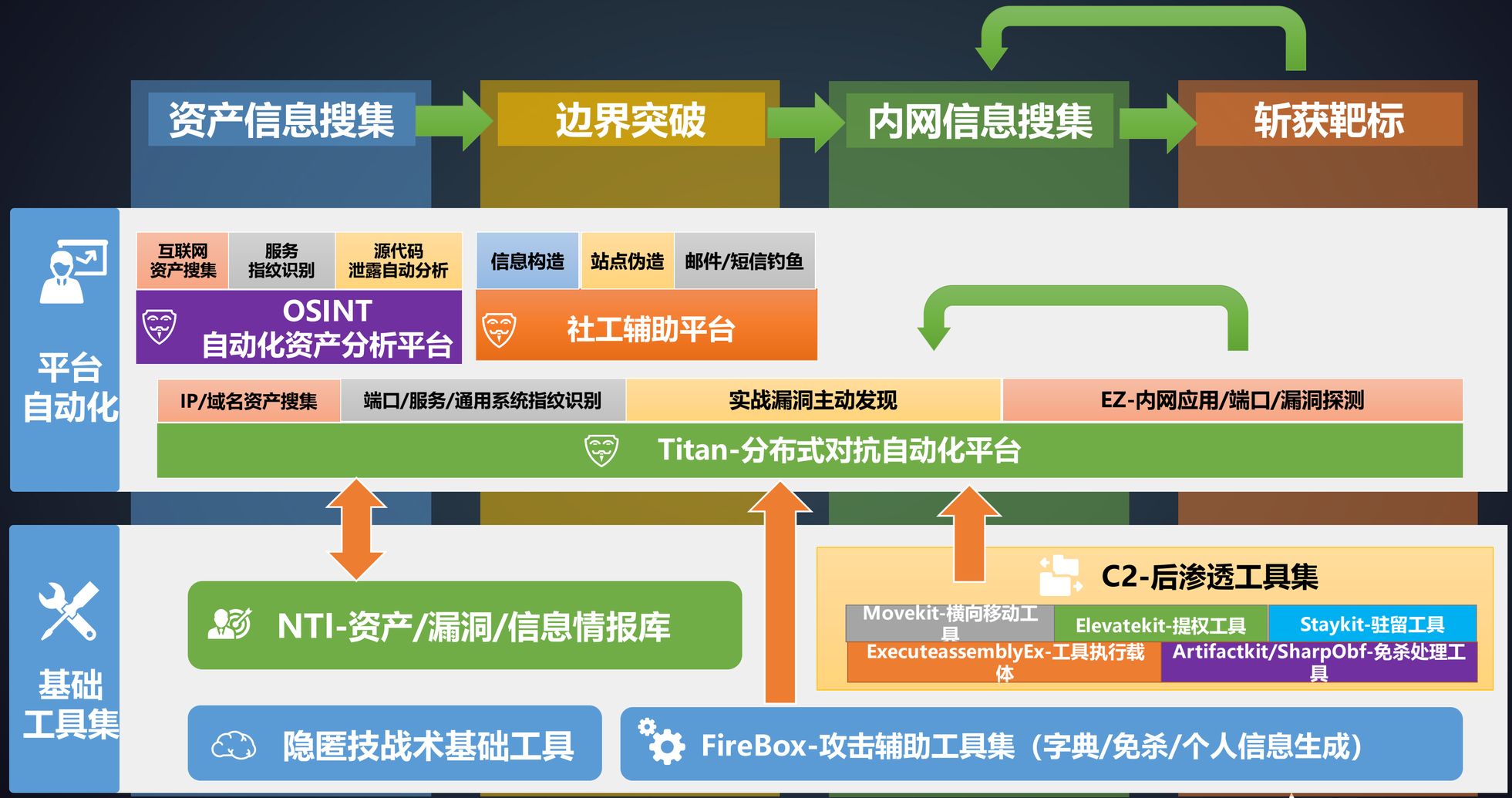
实战出发，归于常态

对全国防守单位的现状分析中发现，超过90%的单位未建立起成熟的安全运营体系，采取临时突击，或堆砌防护的方式应对实战，投入大量资金与人力均未能达到预期效果

有体系的建立起企业安全运营能力，通过运营实现对抗能力的常态化，在实战当中不断推动能力优化

运营三化

自动化能力


资产信息搜集
边界突破
内网信息搜集
斩获靶标
平台自动化
互联网资产搜集
服务指纹识别
源代码泄露自动分析
OSINT 自动化资产分析平台
信息构造
站点伪造
邮件/短信钓鱼
社工辅助平台
IP/域名资产搜集
端口/服务/通用系统指纹识别
实战漏洞主动发现
EZ-内网应用/端口/漏洞探测
Titan-分布式对抗自动化平台
基础工具集
NTI-资产/漏洞/信息情报库
C2-后渗透工具集
Movekit-横向移动工具
Elevatekit-提权工具
Staykit-驻留工具
ExecuteassemblyEx-工具执行载体
Artifactkit/SharpObf-免杀处理工具
隐匿技战术基础工具
FireBox-攻击辅助工具集（字典/免杀/个人信息生成）

「融合·CONVERGENCY」
TECHWORLD2021

驻留时间博弈

攻击者希望延长在目标网络的驻留时间以更好进行内网漫游，主要手段：

- **主动对抗（Anti）**：针对防护技术进行主动出击，避免查杀
- **检测绕过（Bypass）**：从自身特征出发绕过查杀
- **行为隐匿（Undetect）**：避免防御者发现样本行为

CONTENTS

演练期间：

- 样本中反沙箱占**19.5%**，免杀占**78%**，流量伪造占**46.3%**
- 溯源**501个**真实对象中，使用CDN等隐蔽技术的达**113个**，同比往年大幅度增加
- 非A.B.U. 通常驻留时间约**4小时**，A.B.U. 通常驻留时间约**4天或更久**

驻留的攻防博弈将会愈演愈烈

主动对抗

权限 | 进程 | 文件 | 设备

重点关注权限，监控以防护软件文件、进程、配置为目标的操作合法性

```
srand(v0);
sub_401B40(L"SeDebugPrivilege", 1);          // 使样本程序有访问其他进程的权限
for ( i = 0; i < 17; ++i )
{
  for ( j = 0; j < 17; ++j )
    byte_41D2F8[17 * i + j] = 42;
}
v2 = sub_402460(L"MpCmdRun.exe");
v3 = sub_402460(L"MsMpEng.exe");            // 检测是否存在WindowsDefender进程
```

权限提升与修改防护配置

检测绕过

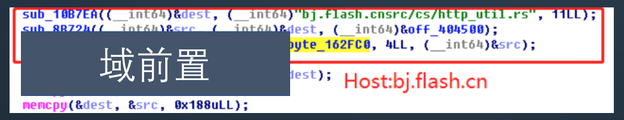
行为 | 文件

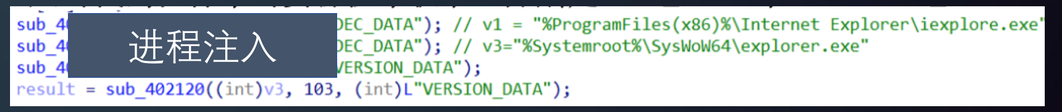
进行行为特征识别，依赖威胁情报指导静态特征识别（包括内存、文件特征）

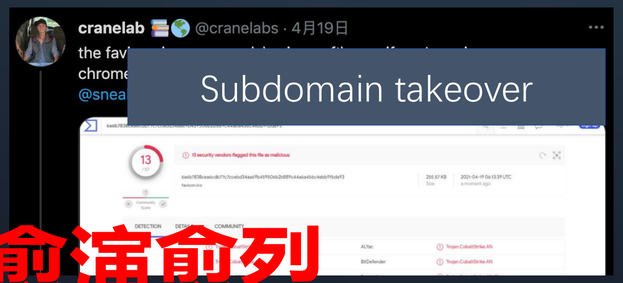
行为隐匿

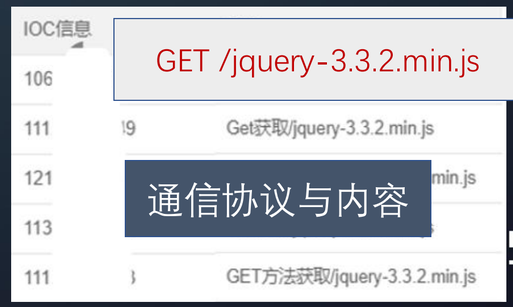
通信 | 进程

主要依赖于行为特征（进程）、流量学习、威胁情报进行狩猎



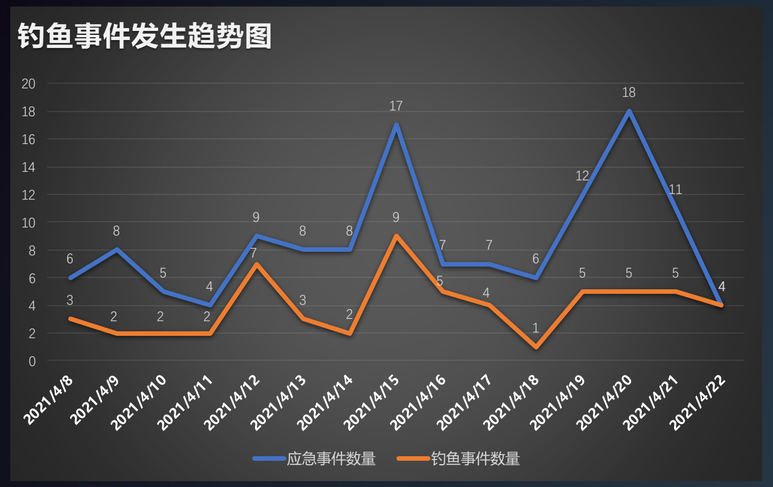






NSFOCUS TECHWORLD | NSFOCUS

钓鱼趋势变化



参演客户安全意识仍有待提高

- 捕获钓鱼攻击相关样本共**108个**，较2020年68个上升**58.8%**
- 钓鱼成功**23起**占比**21%**，较20年6起多近**3倍**，多起客户内部转发钓鱼事件，**单次传播范围达1000+人**

钓鱼攻击是攻击主要手段

- 今年供接收**59起**钓鱼事件，占应急事件 **46%**
- 钓鱼事件数与总数趋势基本一致，针对目标倾向于优先使用钓鱼攻击

钓鱼攻击专业化、专职化

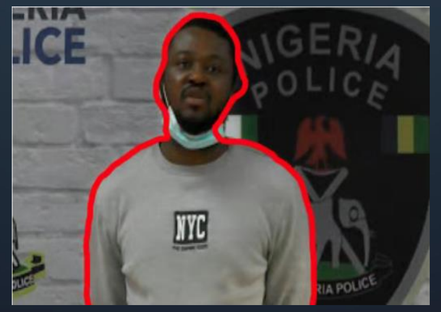
- 钓鱼攻击使用自动化工具，能够短时间内发送大量恶意邮件
- 团队作战，囊括**话术**、**漏洞**（如Chromium漏洞）、**免杀**等部分，扩大钓鱼成功概率

钓鱼攻击溯源以及钻石模型

在钓鱼事件中，我们发现存在境外组织对客户进行钓鱼，但是因为邮件通篇英文而被识别可能存在问题。

- 逆向分析
  - 使用了分发网络隐匿通信
  - AgentTesla为攻击载荷
- 联合威胁情报实验室进行溯源与情报关联分析得到大量该攻击组织信息

姓名	网名	身份
Onuegwu Ifeanyi	SSGToolz	负责人，主要开发者
Ikechukwu Ohanedozie	Dozzy	成员，受害者筛选
Onwuka Emmanuel Chidiebere	CeeCeeBossTMT	成员，提供攻击目标



对手（Adversary）

SSGToolz
Dozzy
CeeCeeBossTMT

功能（Capacity）

16个恶意代码
3466FDDCB**********69CEED
B0C728984**********D8B72A6
CE1295E2D**********67918AB
7A1C6CF**********D2BE4BC
....
1个攻击工具
AgentTesla
0个公开漏洞

基础设施（Infrastructure）

13个IP
208.91.199.224
....
10个域名
smtp.richieslogs.com
....
2个邮箱
ssgtoolz@richieslogs.com
....

受害者（Victim）

国家：中国
行业：金融

典型打点和内网环境下的钻石模型

除了钓鱼，攻击团队依然热衷于外围打点进行边界突破，以进入目标内外——包括了使用漏洞、弱口令进行正面破防，针对供应链企业、兄弟企业侧面破防再漫游至目标内网。

- 应急响应分析得到入侵路径

分支机构→集团VPN→关键信息收集→精准钓鱼→边界安全设备（代理）→内网横移→靶标

- 将黑IP作为情报进行下发
  - 客户B进行流量告警回溯发现攻击队攻击
  - 进一步扩展情报（域名、IP）
- 整合情报再次下发，结合溯源前置方案捕获到攻击者真实身份

对手（Adversary）

GJD005（代号）

功能（Capacity）

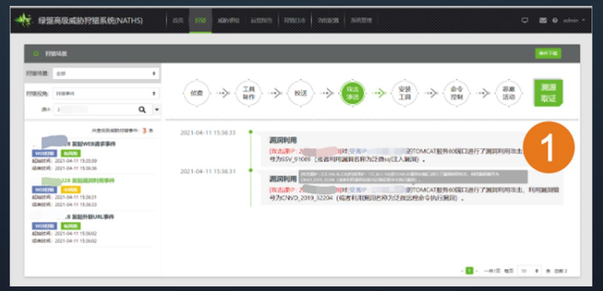
2个恶意代码（CS beacon）
4F7E0D**********E4D
B667D7**********DB9
4个攻击工具
FRP
CobaltStrike
Fscan
自改冰蝎（内存马）
1个公开漏洞
Fastjson 反序列化
2个非公开漏洞
某安全防护设备远程命令执行
某办公系统远程命令执行

基础设施（Infrastructure）

9个IP地址（多个同B段地址）
139.*.*.253
139.*.*.217
139.*.*.221
139.*.*.186
139.*.*.56
223.*.*.59
39.*.*.62
7. *.*.127
47. *.*.86
1个攻击域名
****n.com
0个邮箱账号

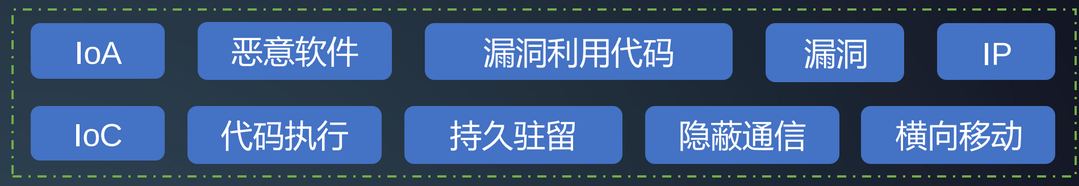
受害者（Victim）

国家：中国
行业：制造业



高烈度攻防对抗的决胜点，在于信息差

基于情报和威胁狩猎的实战化运营体系



漏洞情报

舆情通告

恶意IP情报

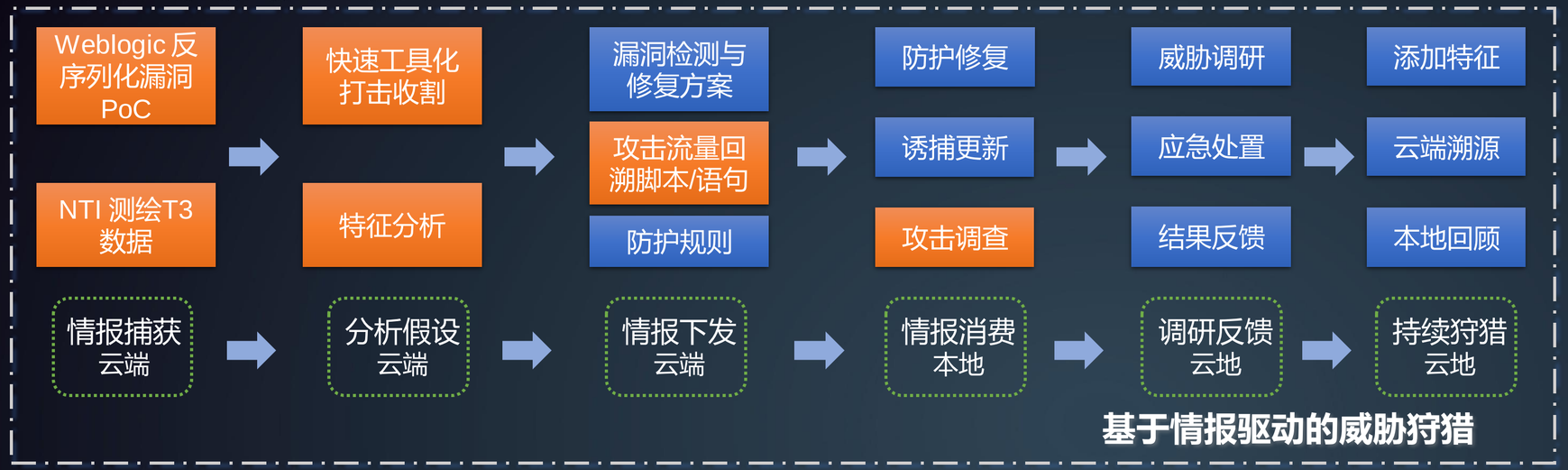
其他情报

观点

如何有效的进行情报的消费（分析和使用）是 运营能力提升的银弹，盲目消费情报是运营能力提升的毒药；

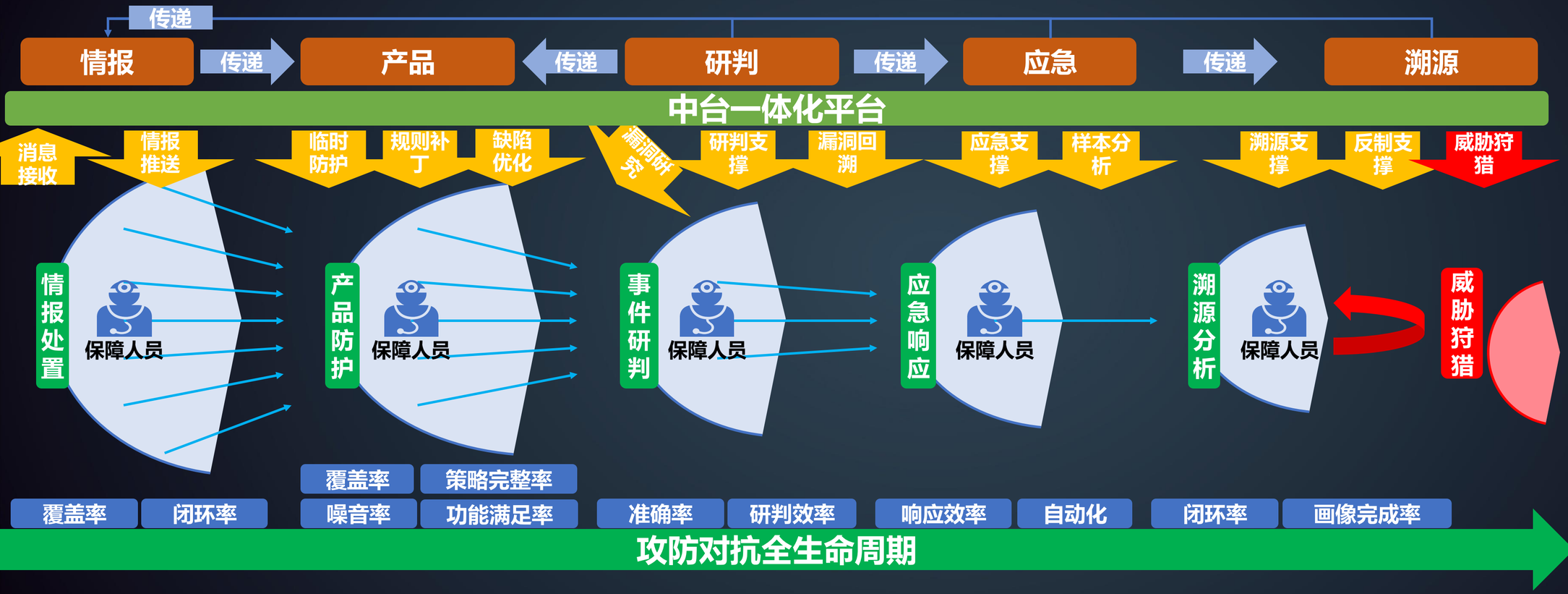
一个企业面临的威胁五花八门 多种多样，但对于一个具有庞大项目群体 庞大客户基础的安全生态，威胁的总量和攻击的手法相对稳定；

基于情报&&事件驱动的威胁狩猎



- 云地协同，事件、情报闭环率100%
- 联防联控，甄别4526个高可信威胁IP，捕获并画像121名攻击者
- 完成12个攻击画像，其中发现2个APT组织/黑灰产

实战化运营指标



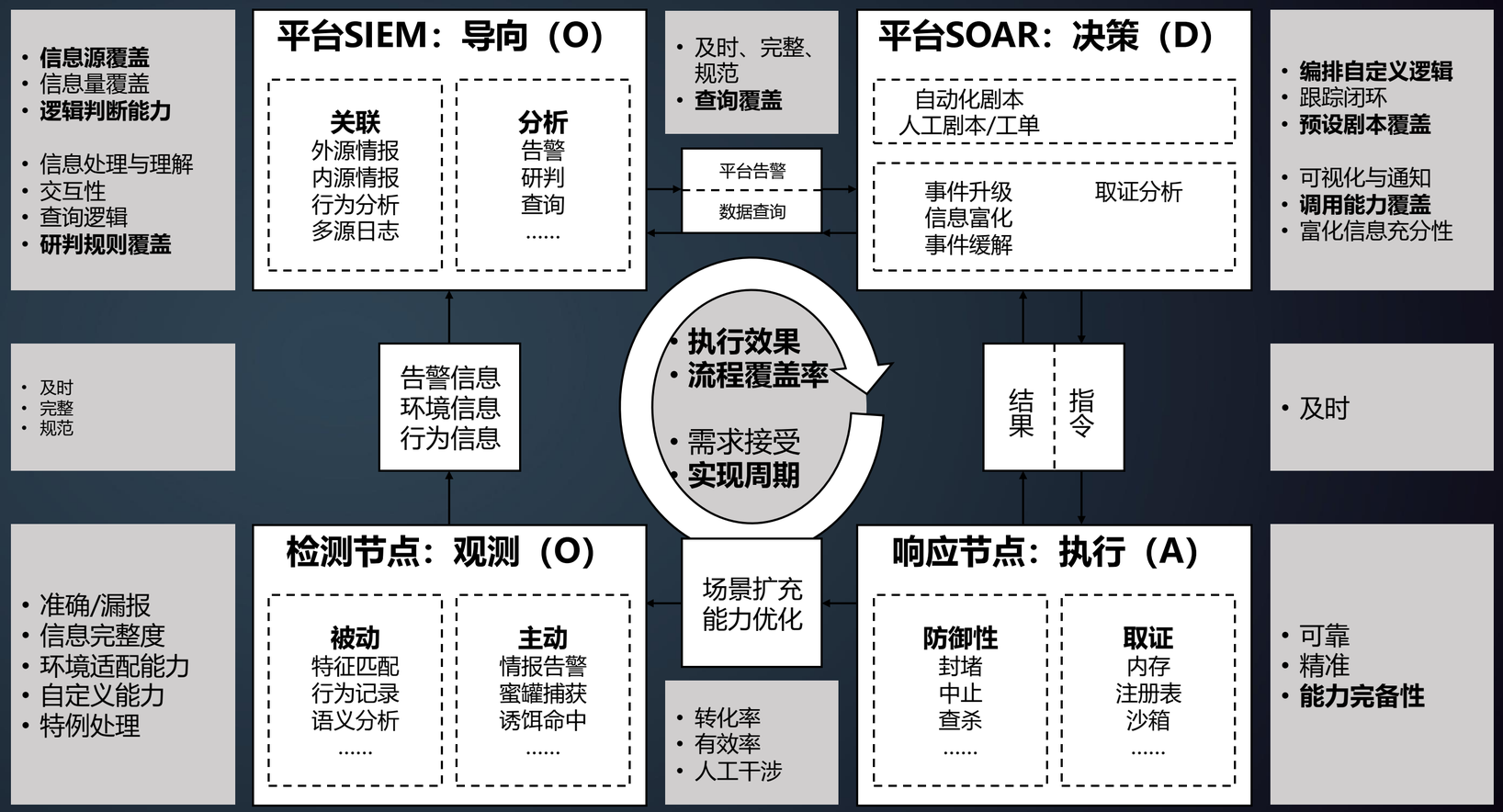
能力类型	指标
底座能力	已覆盖核心能力数/总核心能力数
流程能力	SOP关键流程自动化理论覆盖度
流程能力	自动研判规则对MDR分析规则集（有效）覆盖度
流程能力	SOAR剧本对MDR分析规则集（有效）覆盖度
执行效果	特定环境平均分析时长
执行效果	处置剧本有效性=某事件有效处置/该事件总数
执行效果	实际分析时长/预期分析时长
执行效果	特定流程使用自动化功能的项目数量/总项目数量
需求响应	平均需求实现周期

「融合·CONVERGENCY」
TECHWORLD2021
绿 盟 科 技 技 术 嘉 年 华

基于OODA运营自动化

1、驻留/检测/响应时间
2、Playbook覆盖度
3、自动研判覆盖度
4、标准化程度
5、人力资源优化
6、对抗性

步骤	指标参考	0-起步阶段（消费导向）	1-初级阶段（分享导向）	2-标准阶段（标准导向）	3-创新阶段（生产导向）	4-引领阶段（体系导向）
情报规划	情报内容维度 集团化程度	仅需求IoC	• 具备分享意识，知道大概分享目标 • 了解需要获取的情报	标准的情报获取及分享途径、内容、时间节点	需要包括战略性的情报	明确各方生产与消费需求，形成情报体系作战
情报收集	情报集中程度 情报覆盖程度 情报时效性	主要依赖被动接收 主动搜索一些情报	• 进行IoC以及少量IoA情报产出 • 通过分享、搜索、购买主动获取目标情报	明确落地情报收集来源、可信度、维度、内容、时效性	深挖情报产出，能够进行包括技术、战术、运营、战略情报产出	可以通过自动化平台收集与产生情报，运营人员仅需要进行情报调整即可进
情报处理	元数据完整度 情报有效率	没有情报分类 没有情报筛选	• 集中管理数据，很少进行情报筛选 • 简单进行数据分类，如IP、哈希等	落地情报数据管理方法，包括：元数据类型、情报分类、情报优先级	• 进行行业性等更深入以及针对性的分类 • 依据情报优先级以及相关性分类并赛选情报	自动分类、标志以及筛选情报，对情报进行入档处理
情报分析	情报分析占比 关联情报占比	无分析，直接使用情报	由人工进行情报正确性分析工作，只利用正确的情报	• 形成可复制的客观分析流程 • 分析情报正确性、准确性、有效性	• 具备关联分析方法论 • 能够调用历史情报数据进行情报关联分析工作	由自动化平台辅助完成情报判断与关联分析工作，产生分析结果
整合传播	分享范围 分享数量 分享有效率	• 对情报进行广泛下发 • 缺少情报分享	进行情报广泛分享与下发	规范下发与分享范围、SLA以及内容（包含情报与处置建议）	根据情报处理与分析结果针对性下发，提高情报有效率	利用自动化平台将情报下发到指定防护设备、运营人员进行快速验证
验证反馈	情报处置闭环率 情报处置时效性 情报回顾频率	缺乏验证反馈或被动收集反馈	主动收集情报下发与分享的验证结果反馈	• 形成反馈要求(模板、SLA） • 建立接口人，通过人工跟踪闭环	能够分析反馈数据，发现闭环问题与痛点，根据反馈完善情报和运营	通过自动化平台与流程进行情报处置与验证的反馈收集



NSFOCUS TECHWORLD | NSFOCUS

实战化运营和常态化运营的差异

攻防演习 v.s. 常规安全工作

开始、结束时间明确，可预先准备 实际对抗仅15天，个别问题可以“克服”	短时间	长时间	安全问题随时可能发生，需时刻警惕 无法一直“克服”问题，必须解决问题
规则明确，可针对性“押题”“刷分”“弃车保帅” 攻击队受到约束，风险可控	有规则	无规则	真实战，没有“得分技巧”，需直面真实风险 攻击者不受约束，安全事故将造成真正的业务损失
突击式安全建设，见效快，但细节难以照顾全面 基础薄弱，体系、制度的问题无法靠突击解决	突击	持续	可以持续完善安全能力 可以有计划、有节奏地建设、改进安全体系
为出成绩而在短期投入大量资源，力求“绝对安全” 获取跨团队合作、支持更容易	投入大	性价比	需考虑安全投入的性价比，达到“相对安全” 安全服务于业务，不应给业务造成过大阻力
有“分数”这一直观的结果 建设成果一目了然	显性成果	隐性成果	“安全”即为最终工作成果 难以直观体现出价值

常规安全工作需要以一种常态化、实战化、体系化的方式开展，以合理的投入达到相对安全，并直观展示出工作成果

「融合·CONVERGENCY」
TECHWORLD2021
绿 盟 科 技 技 术 嘉 年 华

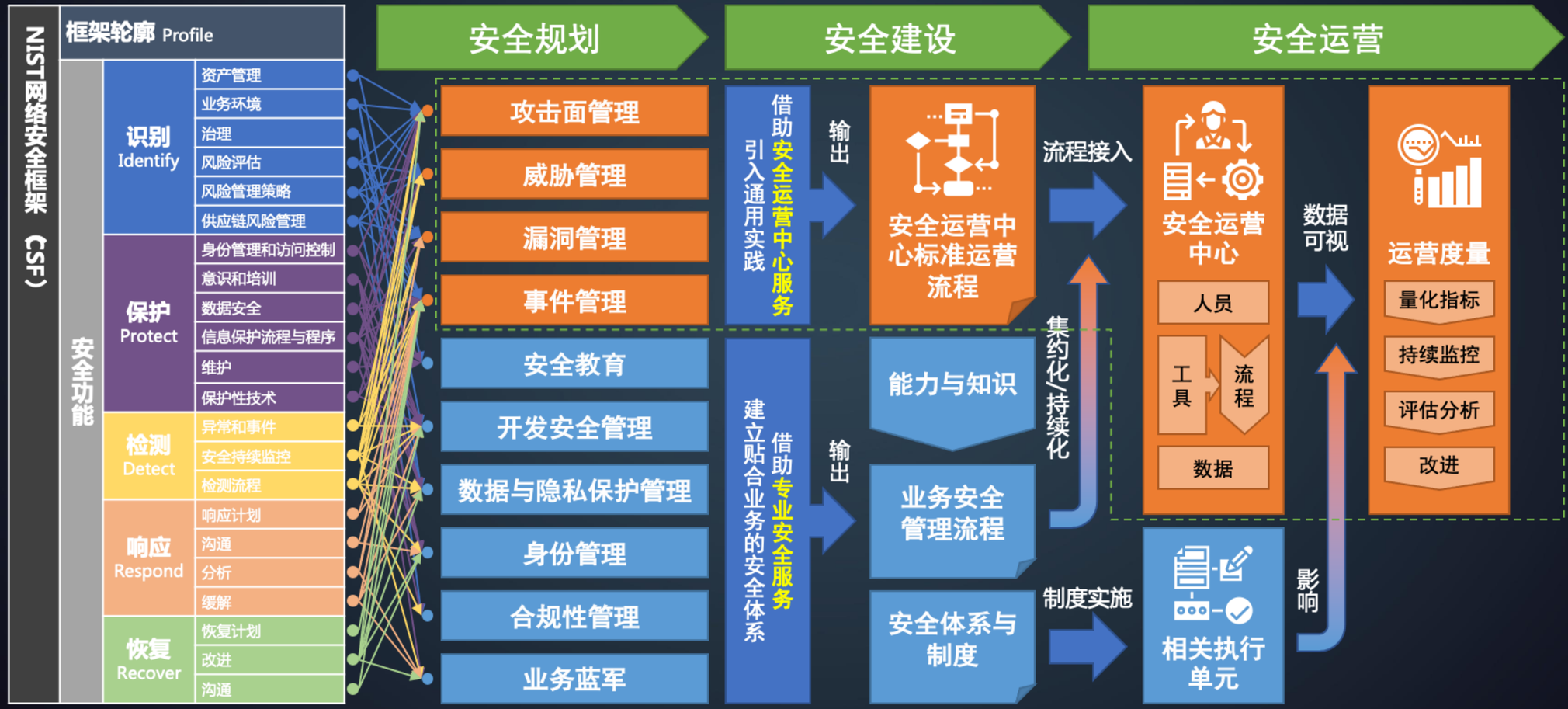
常态化和实战化的转化

- 借助安全运营服务将突击性的演习保障工作转化为常态化、实战化、体系化的安全运营能力。
- 运营工作覆盖演习保障范围，并扩充规划、建设与持续运营能力。在演习成果的基础上进一步提升安全水平，保障业务安全，并顺利应对各级演习、重保及安全检查。

演习保障				安全运营服务					
启动	塑团队 建共识	清资产 理边界	体系化	规划		安全咨询			
	演习保障团队规划	网络架构分析调优				企业安全规划	安全运营中心设计	信息安全风险评估	网络架构分析
	攻防演习基本同步	互联网暴露面治理				应用安全开发生命周期	企业安全培训方案设计		
	内网资产发现梳理			建设		运营管理	安全培训		安全演练
备战	梳路径 铸铁壁	排风险 除隐患				安全运营能力度量	安全产品培训	运营服务培训	安全演练服务
	攻击路径分析布防	高频高危专项检查				安全运营管理	安全服务培训	安全意识培训	钓鱼邮件演练服务
	安全设备能力优化	口令安全风险治理		运营	预测	资产管理	脆弱性管理	威胁管理	安全设备管理
	历史入侵痕迹排查	管控设备安全核查	实战化			资产梳理	紧急漏洞预警	紧急事件预警	设备维保
	敏感信息风险清查					资产上线安全检查	资产上线安全检查		
演练	砺精兵 强实战						代码审计		
	对抗场景仿真演练	安全意识专项强化			防护		安全加固服务	设备策略优化	平台系统加固服务
	红蓝对抗实战演练							云WAF/云清洗	MSS安全设备云端托管服务
保障	严防守 重对抗				检测	周期性资产稽查	Websafe网站安全监测服务	威胁分析	设备巡检
	战时保障安全巡查	攻击事件处置应急	常态化			互联网暴露面资产稽查	漏洞扫描&配置核查	平台及探针策略优化	
	战时情报联防联控	攻击事件溯源反制					弱口令扫描	网站后门扫描	
	攻击事件监控研判						漏洞验证&渗透测试	威胁事件建模	
总结	精复盘 优总结				响应		紧急漏洞响应	应急响应	设备策略优化
	演习缺陷补充闭环	演习保障工作总结						自动化编排与响应	

NSFOCUS TECHWORLD | NSFOCUS

常态化安全运营模式


NIST网络安全框架（CSF）
框架轮廓 Profile
安全功能
识别 Identify
资产管理
业务环境
治理
风险评估
风险管理策略
供应链风险管理
保护 Protect
身份管理和访问控制
意识和培训
数据安全
信息保护流程与程序
维护
保护性技术
检测 Detect
异常和事件
安全持续监控
检测流程
响应 Respond
响应计划
沟通
分析
缓解
恢复 Recover
恢复计划
改进
沟通
安全规划
安全建设
安全运营
攻击面管理
威胁管理
漏洞管理
事件管理
安全教育
开发安全管理
数据与隐私保护管理
身份管理
合规性管理
业务蓝军
借助安全运营中心服务引入通用实践
借助专业安全服务建立贴合业务的安全体系
输出
输出
安全运营中心标准运营流程
能力与知识
业务安全管理流程
安全体系与制度
流程接入
集约化/持续化
制度实施
安全运营中心
人员
工具
流程
数据
相关执行单元
数据可视
影响
运营度量
量化指标
持续监控
评估分析
改进

「融合·CONVERGENCY」
TECHWORLD2021
绿 盟 科 技 技 术 嘉 年 华

服务运营体系全景图

7x24小时集约化服务能力

- 自动化能力
- 数据能力
- 方案化能力

常态运营：风险管理 | 流程建设 | 攻击面分析 | 数据安全运营 | 指标度量

实战运营：情报预警 | 分析研判 | 威胁分析 | 事件响应 | 溯源反制

运营能力

对抗社区运营 | 成熟度运营 | 知识库运营 | 实战靶场运营 | 自动化能力运营

服务方法 / 最佳实践 | 客户画像 / 运营指标 | 情报 / 研判 | 数据 / 服务标准化

服务交付能力

安全服务项目
- 安全规划项目
- 驻场项目
- 实战保障项目
- 安全合规项目

常态化运营：TAC、EDR、SIEM、WAF、UTS

实战化运营
- 事件响应
- 威胁分析

工具运营
- 敏感信息泄露监控
- 风险评估
- 安全意识评估

项目管理 → 客户管理

SaaS服务

威胁狩猎 | 溯源反制 | 网站监测
专家研判 | 情报预警 | 云沙箱
云WAF | 云等保 | 威胁情报

绿盟安全云
绿盟城市运营中心
绿盟科技各分公司 | 合作伙伴

安全基础服务

渗透测试 | 应急响应 | 漏洞管理
代码审计 | 等保咨询 | 安全规划
风险评估 | 意识评估 | 基线核查

NSFOCUS TECHWORLD | NSFOCUS

NSFOCUS TECHWORLD | NSFOCUS

THANKS

欢迎关注绿盟科技
了解更多安全资讯

微信公众号

新浪微博