紫军攻防演练实战

张驰
平安银河实验室

行业现状

2021年11月16日，国家发布的《“十四五”信息通信行业发展规划》，工信部提出“在安全保障体系和能力建设方面，着力完备网络基础设施保护和网络数据安全体系，持续提升新型数字基础设施安全管理水平，打造繁荣发展的网络安全产业和可信的网络生态环境，全面提升行业网络安全应急处置，构建国家网络安全新格局，以支撑国家网络安全新格局形成。”

目前在**政策**与常态化**护网**的双重促进下，各关键行业，企业的**安全防御体系**的**基础建设**已经基本**完成**

紫军演练是安全验证的极大补充

工具平台

- 漏洞扫描工具
- 攻击面管理运营
- 代码审计工具
- 入侵和攻击模拟

应用测试

- 安全测试
- SRC平台
- 众测
- 第三方服务

蓝军攻击

- 实战对抗
- 攻击手段多样
- 准许内网渗透
- 结果导向

紫军演练

- **攻击技术真实**
- **演练透明实时**
- **演练全面深入**
- **成本低效率高**

人工

什么是紫军演练

国际信息系统审计协会

紫方定义为通过将**攻击防御双方**（红蓝两军）集中起来，带着一定**目的**进行有**针对性的演练合作**，验证防御方的检测和响应能力。

微软

紫军以MITRE 的ATT&CK框架等构成的单元测试方式进行评估，利用这些对攻击者行为特征的积累来识别网络中的漏洞，并围绕企业关键资产建立更好的防御。**采用攻击者的技术并与企业信息系统一起构建更全面的评估，从而使得演练攻击方拥有了外部攻击者所没有的优势**

XM Cyber

XM Cyber 认为红队和蓝队在设计之初就是对立的实体，可能会造成**竞争摩擦**。而为了确保红蓝团队本着合作精神运作，可以创建（或雇佣）紫色团队，**分析流程，促进沟通，并帮助双方朝着共同目标努力**。紫色团队充当了调解人和促进者的角色，可以从**更超然的角度提供见解**，最终使企业更清楚地了解其应对安全攻击的准备情况

紫军演练是对蓝军攻击的有效补充

	蓝军	紫军	
攻防对抗	• 聚焦高危风险发现，攻防对抗模拟		
合作共建		• 具体实施场景，技术为双方确认（流程技术+企业实际情况）	
黑盒攻击	• 真实对抗使得双方只能在复盘阶段进行有限的沟通和确认		
攻防透明		• 攻击技术实施与防守方同步，可在事中进行防御有效性验证	
最短路径	• 因时间短，权限有限，攻击方专注向靶标进行渗透，渗透结果为最短有效路径		
全面路径		• 企业可提供需要权限，资产范围，从而获得开展更全面的内网环境防御有效性验证	
自建价值	• 蓝军服务可以通过采购第三方进行，自建蓝军价值未最大化		
自建价值		• 蓝军加入到安全防御建设，补充攻击视角的建设维度	

紫军演练攻击技术更全面,更深入

侦察	资源开发	初始访问	执行	持久化	权限提升	防御绕过	凭证访问	发现	横向移动	收集	命令控制	数据窃取	影响
收集可用于规划后续行动的相关信息	创建可用于支持星等的相关资源	进入内网环境的相关技术	运行恶意代码的相关技术	维持内网权限的相关技术	获取更高级别权限的相关技术	避免被防御设备发现的相关技术	窃取有有效用户名和密码的相关技术	内部环境发现，侦察相关技术	穿透环境获取其他服务系统权限的相关技术	收集目标感兴趣数据的相关技术	控制相关系统并通信的相关技术	窃取数据并外传的相关技术	能供操作，中断，破坏的相关影响

V13 2023.04.25（411技术项）

01 业内APT覆盖度：Lazar**（155），Tur**（88），Wizard Sp****（69）

02 紫军演练覆盖度：目前平安紫军演练ATT&CK技术覆盖度可达80%（300+）（根据剧本选择）

紫军演练相比蓝军攻击,效率更高,成本更低

01

时间周期短

- 蓝军攻击模拟为APT攻击，长周期持续为其重要特点，周与月为周期进行
- 紫军演练根据剧本选择，可以天为单位进行

02

资产覆盖范围广

- 蓝军攻击受时间，目标，权限影响，测试的资产范围有局限
- 紫军演练因为合作方式，可直接提供环境等信息，直接开展

03

投入人力少

- [初始访问]蓝军攻击人力投入最多为外网打点，平均占总投入人力70%，关注高风险漏洞
- [初始访问]紫军演练访问入口可提供，关注防御情况
- [人员技能]蓝军攻击重点为发现未知风险，漏洞挖掘，对人员要求高
- [人员技能]紫军演练在准备梳理演练项时对人员要求高，但演练项实施过程中，对于人员要求较低，可根据指引复现即可，复用度高

紫军演练大幅提高事件响应能力

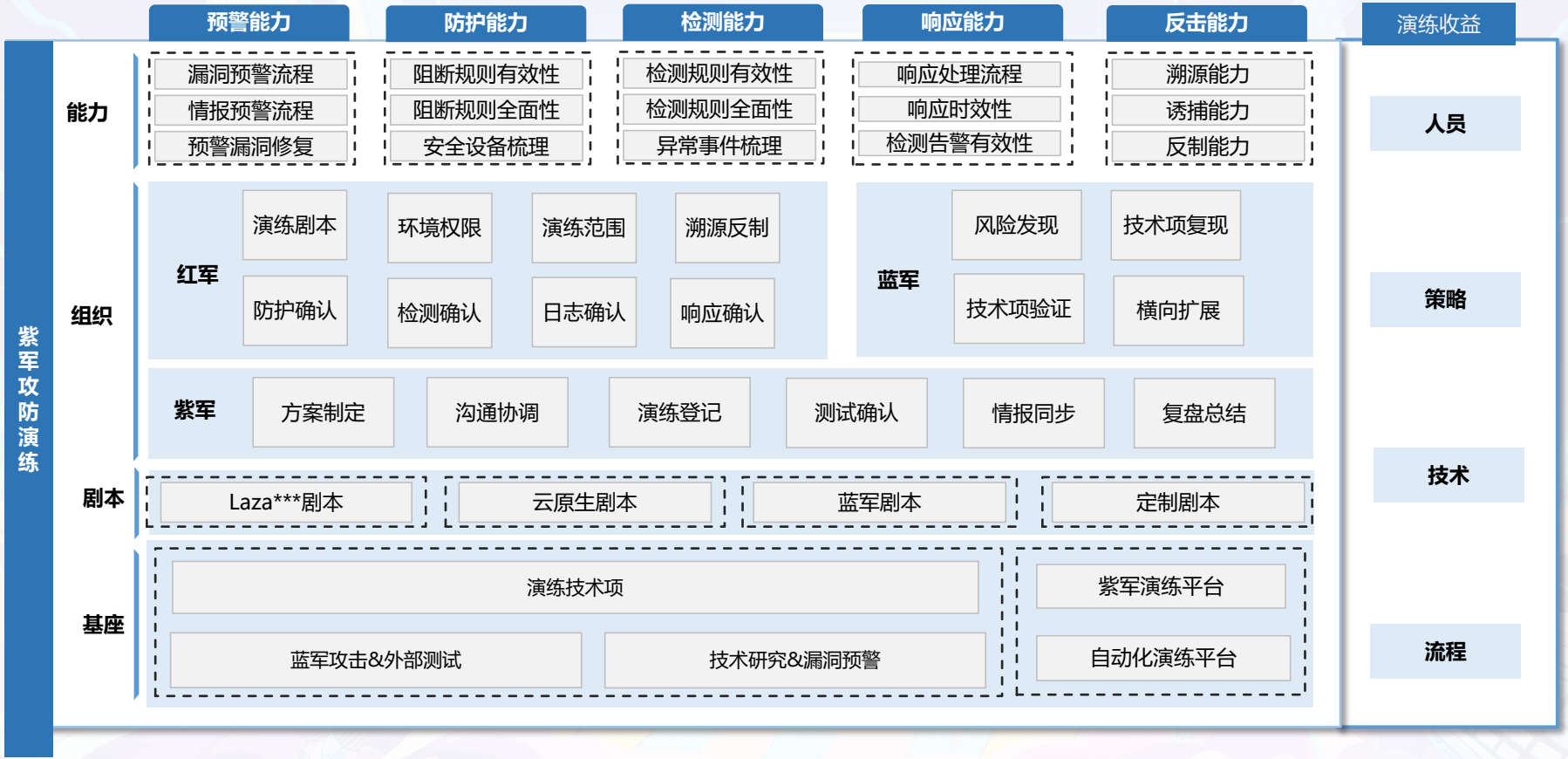
01 **攻击技术原子化：**将攻击技术分解到单项可执行，可细粒度对技术项进行防护有效性验证

02 **全方位应急响应经验提升:** 可进行实时的应急响应对抗处理，并根据实际情况可进行攻击复现，重复处理

03 **事件响应处理机制全流程验证:** 检验有效性，可行性，总结可优化方向

04 **全方位处置方案有效性验证:** 演练测试项为实战性，可用性总结而成,透明的防守措施验证

平安紫军攻防演练 架构


预警能力
防护能力
检测能力
响应能力
反击能力
演练收益
紫军攻防演练
能力
漏洞预警流程
情报预警流程
预警漏洞修复
阻断规则有效性
阻断规则全面性
安全设备梳理
检测规则有效性
检测规则全面性
异常事件梳理
响应处理流程
响应时效性
检测告警有效性
溯源能力
诱捕能力
反制能力
人员
组织
红军
演练剧本
环境权限
演练范围
溯源反制
防护确认
检测确认
日志确认
响应确认
蓝军
风险发现
技术项复现
技术项验证
横向扩展
策略
紫军
方案制定
沟通协调
演练登记
测试确认
情报同步
复盘总结
剧本
Laza***剧本
云原生剧本
蓝军剧本
定制剧本
技术
基座
演练技术项
蓝军攻击&外部测试
技术研究&漏洞预警
紫军演练平台
自动化演练平台
流程

平安紫军攻防演练 剧本设计

Laza***剧本

Laza***是有十多年历史，并一直保持活跃的黑客组织，涉及政治、军事、经济、情报等领域
攻击手法（130+）
涉及ATT&CK全战术覆盖
验证企业对于国际黑客组织的防御能力

云原生剧本

根据平安银河实验室原创云原生攻击矩阵，除攻击手法归类，还关注安全梳理，防御有效性验证
攻击手法（100+）
云原生（重点），云计算，云服务
验证企业云原生环境的防御能力

数据泄露剧本

根据平安银河实验室试试的敏感数据外发专项提升项目提炼而成，可对企业内网数据泄露风险进行有效验证
攻击手法（20+）

蓝军剧本

根据平安银河实验室蓝军团队5年攻击成果手法整理，并增加业内流行的新技术模式汇总而成
侧重于漏洞风险发现
多场景选择：办公，生产，测试，域，关键核心系统等

平安紫军攻防演练方案及流程

演练概况	红军	紫军	蓝军
参演团队	• 企业安全运营团队 • 企业相关部门团队	• 紫军 • 红军负责人 • 蓝军负责人	• 蓝军 • 企业安全人员（可选）
团队职责	• 监控阻断 • 应急响应 • 分析溯源 • 问题整改	• 演练设计 • 演练复盘 • 演练组织 • 红蓝提升 • 协同双方 • 演练记录	• 模拟攻击 • 技术实现 • 工具开发 • 漏洞挖掘 • 渗透测试

沟通

- 关注重点
- 剧本选择
- 测试范围
- 敏感资产
- 注意事项

准备

- 资产权限
- 目标资料
- 实施培训
- 红军组件

演练

- 剧本演练
- 3方协同
- 演练项实施

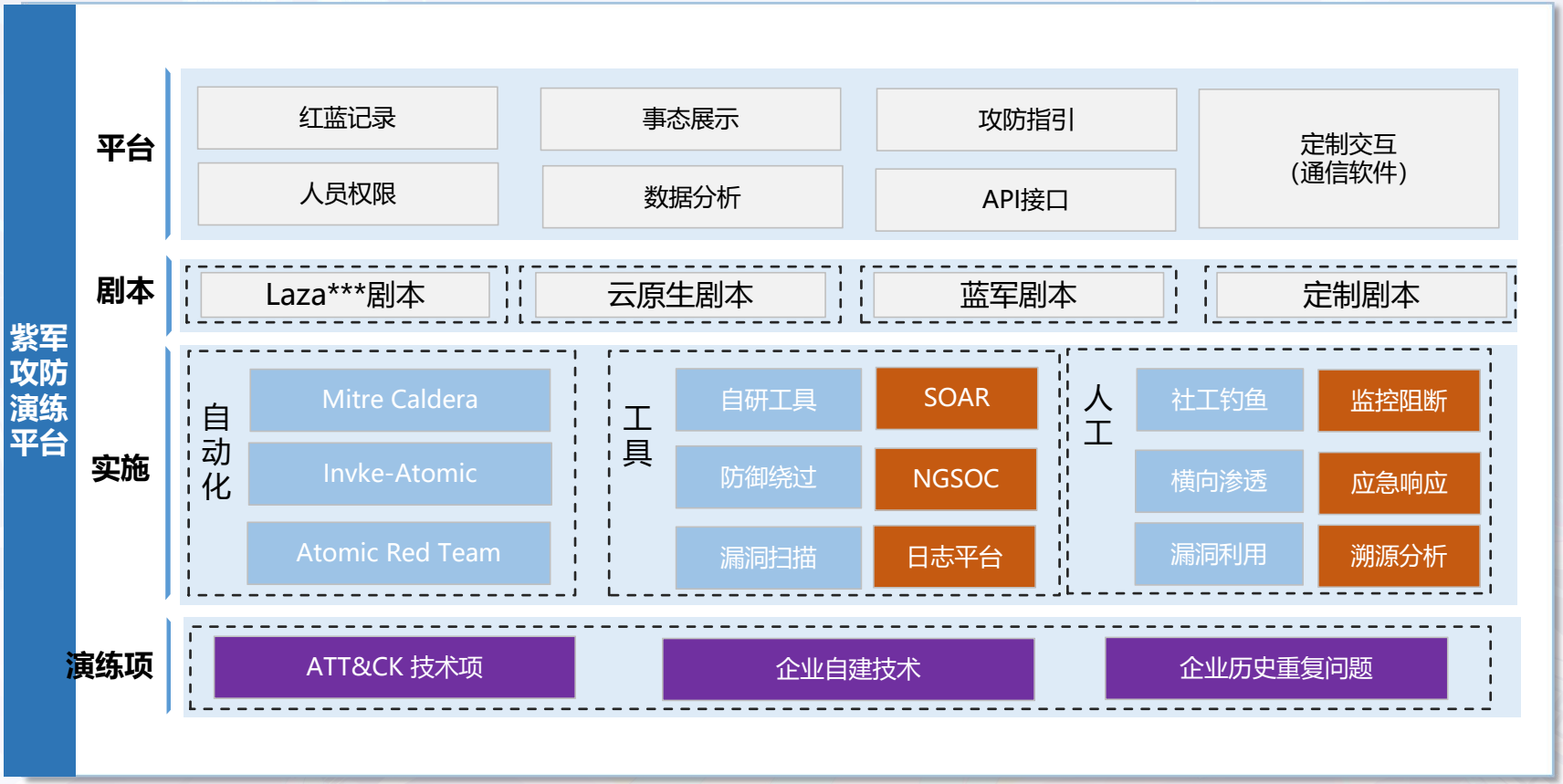
复盘

- 资料汇总
- 报告解读
- 提升探讨
- 规划建议

提升

- 提升落地

平安紫军攻防演练平台及工具



评估指标与提升方案

评估指标

综合安全覆盖率	去重（应急数 + 失败数） / 攻击覆盖项	评估目前应急流程中需要提升的对应技术项
安全设备告警率	告警数 / 需告警数	评估安全设备后续重点升级规则方向

提升方案

漏洞风险	响应流程	设备规则	设备覆盖	人员技术
历史问题修复 风险修复 风险抑制	流程可行性 流程完整性 流程人员责任	规则有效性 （阻断，检测）	规则有效性 （阻断，检测）	设备使用 响应技术 抑制溯源


THANKS