青藤云安全

2022攻防演练蓝队防守指南

目　录

背 景

网络安全攻防演练自 2016 年首次开展以来，经过 6 年的发展，已经成为检验网络安全防御能力最重要的手段之一，也是当下检验对关键信息系统基础设施网络安全防护工作的重要组成部分。在攻防演练中，红队通常以实际运行的信息系统为攻击目标，在既定规则下最大限度地模拟真实网络攻击，以此来检验目标系统的安全防护能力。

随着数字化与信息化进程的不断加快，网络安全逐步走入大众视野，并引起各行各业的重视。网络安全攻防演练逐渐发展成为涉及多个行业、多家单位的大型事件。从 2016 年至今，攻防演练的参演单位数量和覆盖的行业数量都大幅提升。此外，除了国家级的攻防演练，各省市、各行业的监管机构，也会在各自管辖范围内筹备和组织实战演习。

时间长、规模大并不能说明这一活动发展得足够成熟，尤其是对蓝队来说，任何人或产品都不能保证绝对的网络安全，它只能通过一次次的攻防对抗来不断完善自身的防护能力，从而更好地防御蓝队攻击。这是一个以攻促防的过程。

青藤云安全编写本指南的主要目的在于以蓝队的视角，阐述攻防演练中防守工作的注意事项，并针对如何提高防守效率给蓝队提出了相应的建议。本文默认蓝队为防守方，红队为攻击方。

概　述

在实战环境中，无论是面对常态化的一般网络攻击，还是面对组织化、规模化的高级攻击，蓝队都需要按照事前准备、事中实战、事后收尾三个阶段来开展安全防护工作。

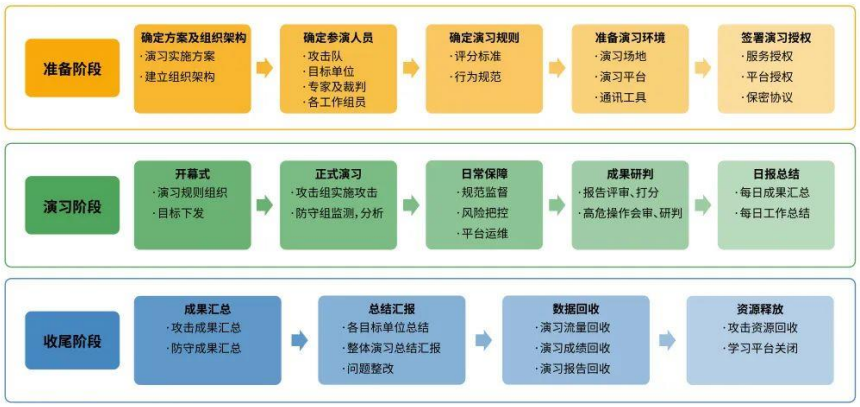

图 1 攻防演练的三个阶段

一、事前准备——查漏补缺，做好战前准备

在攻防演练开始之前，蓝队首先应当充分地了解自身安全防护状况与存在的不足，找出自身的脆弱点并及时进行加固，为后续工作提供能力支撑。这就是准备阶段的主要工作。

在攻防演练中，前期的准备工作包括安全团队组建、演练流程制定，以及未知资产排查、安全设备 0day 排查、系统漏洞排查、系统弱口令排查、系统配置缺陷排查、内网集权系统排查、协助安全加固等技术性工作。

二、事中实战——监控处置，对抗安全攻击

红蓝两队在实战阶段展开正面对抗。蓝队需要集中人力、物力，力求达到系统不破，数据不失。在实战阶段，从技术角度看，应重点做好以下三点：

- **监控全面、持续。**在资产细粒度清点的基础上，从多个路径持续、全面、透彻地发现潜在风险及安全薄弱点，包括弱密码、安全补丁、应用风险等，对网络、主机侧的动态进行持续监测，以发现是否有入侵行为。

- **研判快速、准确。**在攻防演练中，分析研判上承攻击行为的确认、分析及溯源，下接安全人员对攻击行为的响应处置，是整个防护流程技术含量最高的一步，也是对速度、准确度要求最高的环节之一。
- **响应及时、有效。**确认安全事件后，最重要的是在最短时间内采取技术手段遏制攻击的影响范围，并消除攻击发生的所有要素，确保攻击者无法进一步攻击。

三、事后收尾——总结复盘，提升安全能力

演练的结束也是防护工作改进的开始。在实战工作完成后，应对各个阶段的工作进行充分、全面的复盘分析，总结经验、教训。并针对复盘中暴露出的不足之处，立即着手整改，修复或加固安全漏洞及隐患，完善安全防护措施，优化安全策略，提高安全人员技术能力，最大程度提升整体网络安全防护水平。

对于蓝队来说，想要达到高水平的防护效果，需要从“知己”和“知彼”两个方面同时着手。既要了解自身的安全脆弱点，也要了解红队的思路与打法，这样才能结合自身实际网络环境、运营管理情况，制定相应的防御措施和响应机制，以在防守过程中争取到更大的主动权。

在攻防演练实战中，蓝队的主要工作包括红队演练、风险收敛加固、安全监控，以及攻击研判等。这些工作模块并不是彼此孤立的，而是各部分协同工作，形成一条完整的防守工作链。

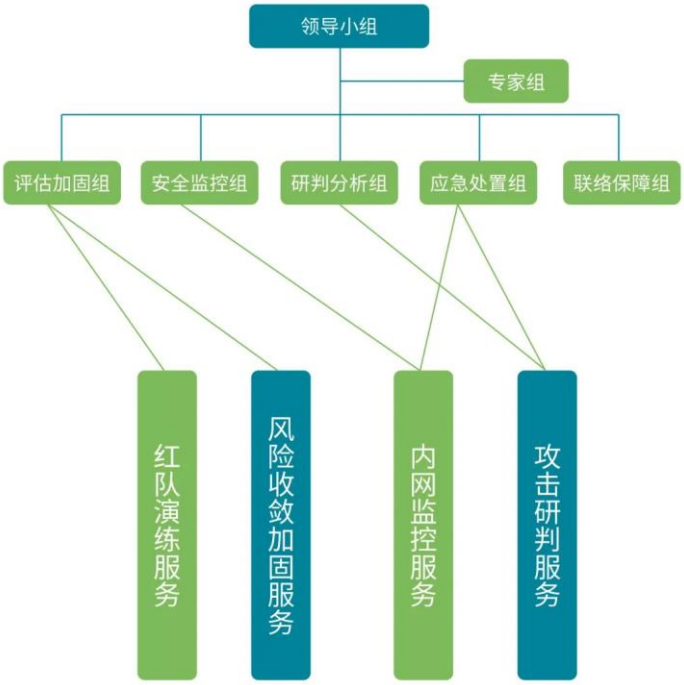

图 2 蓝队的主要工作模块

第一章 红队演练篇

在网络犯罪分子不断更新网络攻击技术和工具的时代，安全人员必须不断完善防御战略，以跟上不断变化的威胁形势，加强检测和响应能力，争取领先攻击方一步。

对于大多数企业组织而言，真正的纵深防御战略应该包括红队演练这个环节。这些企业组织只有经过不断的红蓝对抗演练，形成漏洞发现、修复闭环，才能构建强有力的安全防御体系。

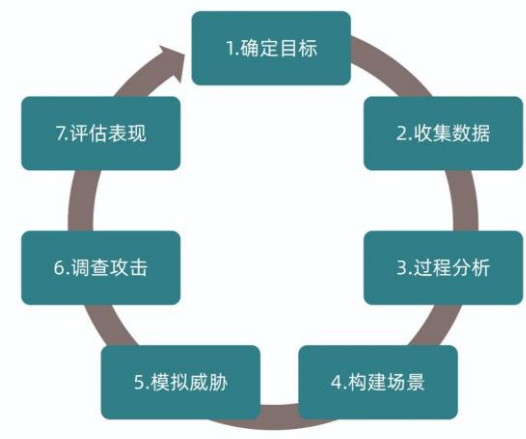

图 3 红蓝对抗的流程闭环

1.1 什么是红队演练?

红队演练是测试企业对网络攻击检测和响应能力的最终方法。它专注于攻击模拟，通过采用与真实攻击相同的各种策略、技术和程序（TTP）来评估企业在整个攻击生命周期中每个阶段的防护能力。红队演练服务为安全运营团队提供了一种安全的方式来测试其威胁检测和事件响应能力。

红队演练的目的在于通过攻击模拟揭示公司安全中的漏洞，发现网络安全防御中的暴露面及盲点，帮助企业深入了解自身安全体系的状态以及安全技术、流程和人员的有效性，并确定需要改进的领域。

通过红队评估，用户可以测试以下内容：

1. 攻击面的大小；
2. 威胁检测技术的有效性；
3. 响应过程的效率；
4. 内部人员的安全意识。

1.2 为什么需要红队演练?

网络安全不是一个短暂的事件，而是一个持续的过程。网络攻击技术和工具不断进化、企业的攻击面不断扩大、企业并购带来的新用户和新政策……所有这些变化都会产生新的安全问题。

解决这些安全问题意味着需要进行定期的安全评估和持续的侦察活动，而红队演练就是最好的安全评估方式之一。它的主要价值在于帮助企业：

- **衡量关键资产的风险。**了解外部或内部攻击者接触企业核心资产的难易程度，并明确通往这些资产的各种关键路径。

- **发现未知的攻击路径。**发现未知的载体和弱点，了解其潜在的业务影响，并基于此提前制定准备、检测、响应和恢复方案。
- **确定优势和劣势。**对自身安全策略进行广泛而深入的分析，获得对团队优势和劣势的客观评估。
- **推进安全防护策略的改进。**为用户提供持续改进所需的洞察力，并促进其有针对性地提高特定能力。

红队演练鼓励安全团队以主角的身份思考，帮助他们识别和修复所有已识别或未识别的漏洞，使其在网络安全防护中始终处于准备就绪的状态，促进团队协作能力的提升和批判性安全思维的养成。红队演练是识别漏洞的绝佳途径，它能在漏洞发展成为安全问题之前彻底将其发掘出来。

以下这些企业组织非常有必要进行红队演练：

- 上市公司及经常被攻击的资本密集型组织；
- 拥有大量数字资产的组织；
- 以信息安全为企业形象的组织；
- 拥有需要保护的敏感数据的组织；
- 想在攻防演习中取得好成绩的组织。

1.3 如何开展红队演练?

在演练服务期间，红队会使用任何必要的手段，就像真实的攻击者所采取的措施一样，包括网络攻击、社会工程攻击、近源攻击、钓鱼邮件、安全设备攻击、供应链攻击、分支机构攻击，不过这些手段不会对客户的基础设施或资产造成损害。

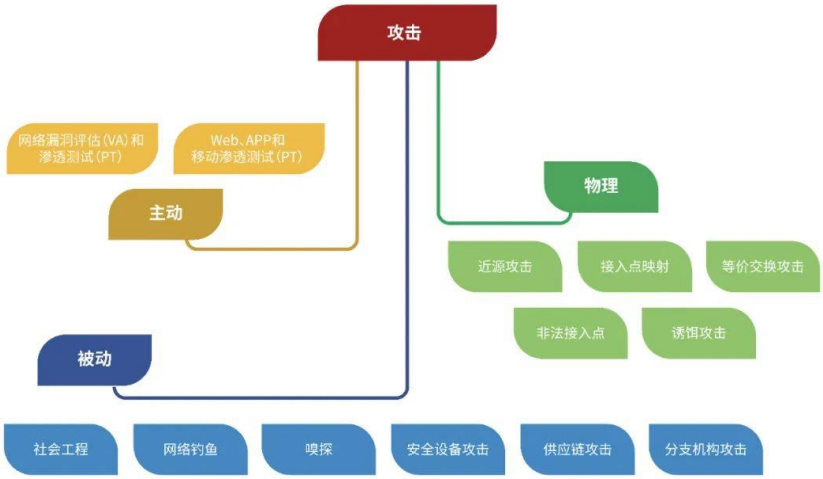

图 4 红队演练涉及到的攻击方式

红队演练遵循结构化方法，根据攻击者传统的策略进行攻击模拟。在每次演练服务开始时，红队人员与客户一起确定项目的目标。客户可以根据他们个性化的要求，选择针对已知或未知威胁进行测试。一旦红队与用户的红队演练目标达成一致，演练服务将分为四个步骤进行：

第一阶段——侦察

采用一系列网络威胁情报技术来尽可能多地收集有关用户的信息。这可能包括开源情报、金融情报、技术情报和人员情报等等。红队人员使用这些信息来识别和确定攻击目标及方法。

第二阶段——武器化和交付

在这个阶段，红队利用获取到的情报对用户发起攻击。根据之前确定的范围和目标，红队可以执行诸如钓鱼邮件、社会工程攻击、物理入侵或命令和控制活动等方法来利用漏洞并获得对用户网络的访问权限。

第三阶段——开发、安装、指挥和控制

一旦红队建立了立足点，他们的接下来目标就是实现与用户共同商定的演练目标。这也意味着在真实攻击中，攻击者能否成功实现他们的最终目标。在这个阶段，红队人员还可以模拟不同类型的攻击者，包括心怀不满的员工或获得用户网站访问权限的攻击者。

第四阶段——输出报告

红队人员需要针对演练的每个阶段为用户提供清晰的报告。这使用户可以全面了解系统或人员中可能存在的任何漏洞或弱点，以便其可以采取行动加强防御。报告的内容通常包含两大部分：

- **执行摘要：**概述演练涉及的范围、主要发现，以及这些发现所造成的业务影响。
- **技术分析：**详细阐述发现的漏洞和风险，分析其形成原因，并给出具体补救建议。

在网络安全防护方面，没有企业是万无一失的。通过练习对模拟攻击的事件响应，安全运营团队可以提高他们的威胁检测和响应能力，在威胁追踪方面变得更加高效，还能发现之前可能未被注意到的漏洞，从而在攻击发生之前或攻击早期阻止攻击进程，避免对业务造成重大损害。

1.4 渗透测试和红队演练有什么区别?

基于对自身安全防护能力进行检测的目的，用户在进行安全服务选型的时候，可能会面临这样一个问题：既然都是测试系统的防御能力，那红队演练与渗透测试有什么区别呢?

虽然红队演练和渗透测试都旨在通过模拟真实攻击的技术和流程来改善企业的安全防御策略，但两种评估的形式和方法不尽相同。

渗透测试是在指定的时间内，对给定的目标系统进行安全测试，比如指定的 web 系统或 APP，找出用户安全系统的漏洞或风险，渗透测试过程中对漏洞的利用一方面可以证明漏洞是真实存在的，另一方面也能基于这些漏洞揭示目标系统所面临的安全风险。在渗透测试的过程中，企业的安全防护团队一般不会参与，为了配合渗透测试的进行，企业还会关闭某些安全防护软件或策略，以方便渗透测试团队发现更多的漏洞。

与渗透测试不同，红队演练的任务往往是完成某个特定业务目标的攻防演练，例如获取用户某个项目的源代码等。它不局限于单个应用程序或系统，而是着手利用包括社会工程在内的

多种攻击手段，对整个环境都在范围内的多个系统进行攻击，全面模拟真实世界中具有明确目的且避免被检测到的攻击者。红队演练某种程度上可以看作是合法的高级持续性攻击（APT）。这种完全贴合真实攻击环境的演练过程，能够反映出企业安全防护体系的检测和响应能力。

两者之间的主要区别可以直观地概括为下表中的 7 点：

渗透测试	红队演练
是短期评估	是长期的评估
使用一种攻击方法	使用广泛的攻击方法
旨在识别和利用漏洞	旨在测试组织检测和响应攻击的能力
企业员工知道要进行渗透测试	企业员工通常不知道发生了红队演练
寻找漏洞是测试人员的核心任务	寻找漏洞是测试人员实现目标的手段之一
测试目标是事先确定的	测试目标不确定且覆盖多个领域
各个系统独立进行测试	各个系统同时进行测试

图 5 渗透测试与红队演练的区别

1.5 国内红队演练最佳实践剖析

红队演练属于网络安全服务领域的一个分支，其质量主要取决于人员与工具两个方面。青藤作为国内网络安全的技术引领者，凭借经验丰富的专业红队团队和猎鹰等安全产品，成为1000+头部用户红队演练的首选合作伙伴。

- 专业的团队：青藤红队的队员全部来源于网安一线大厂，对网络攻防模式有深入和广泛的了解，这意味着他们可以提供最优质的红队演练服务。
- 广泛的经验：拥有多年攻防演练实战经验，在全套安全评估方面的专业知识，包括电子邮件网络钓鱼、物理入侵和命令和控制活动，这意味着青藤可以测试大量的攻击方法。

- 高效的工具：青藤自主研发的猎鹰•威胁狩猎平台，为红队演练服务提供了高效的工具，可以帮助用户更好了解地红队演练的效果，以及整个模拟攻击的过程，例如攻击者是怎么进来的、拿走了什么、留下了什么。
- 红队专家安全咨询：根据用户的红队演练结果，青藤的安全专家会提供清晰、详细、有见地的报告以及针对性的建议，帮助用户准确了解如何补救和降低风险。

第二章 风险收敛加固篇

通过攻防演习，参演单位能够充分检验自身的安全防护、攻击监测和应急处置能力。参演单位作为防守方，面对“隐蔽”的网络攻击，只有了解攻击方是如何开展攻击的，才能根据攻击特点建立完善的安全防护体系，有效抵御网络攻击。

那么从防守方的角度来看，在网络安全攻防演练中应该采取哪些措施提升安全防护水平呢？本篇将要讨论的就是对攻防演练结果至关重要的的事前准备阶段。

2.1 风险收敛加固是攻防演练前序阶段最重要的环节之一

在攻防演练中，前期的准备工作包括安全团队组建、演练流程制定，以及未知资产排查、安全设备 0day 排查、系统漏洞排查、系统弱口令排查、系统配置缺陷排查、内网集权系统排查、协助安全加固等技术性工作，我们可以把这些技术性工作概括为风险收敛与安全加固两个方向。

风险收敛与安全加固服务作为攻防演练前序阶段最重要的环节之一，聚焦于安全的多维度精细化提升，从而收敛自身攻击面，满足企业对于前期内外网资产风险测评、安全意识提升、风险事件精准捕获、防御范围最大化等多种类安全需求，全方位巩固安全防线，增强防御效果。

2.2 如何进行风险收敛加固?

对攻防演练的防守方来说，可以从资产评估、安全策略检查、安全防线加固三个方面实现风险收敛与安全加固，做好攻防演练前期风险管理。

2.2.1 资产评估

大多数情况下，蓝队对于自己的资产情况把控不够，导致部分资产未能纳入有效监测、防护范围，形成了防护薄弱点。红队在发起进攻前，会先收集这些薄弱点，并以此为跳板攻入企业关键系统。所以，提前对资产进行评估，及时关闭“老旧”、“无主”、“无用”资产，收敛对外暴露的攻击面变得尤为重要。

公网资产评估:通过收集企业暴露在公网的资产信息和敏感信息,分析存在的未知公网资产、以及业务系统源码、账号密码暴露等安全风险，协助企业在攻击者发起信息收集前收敛外部攻击面，提升企业对自身资产的掌握程度以及应对突发安全事件的能力。

内网资产评估：从内网安全维度对主机安全产品核心功能模块的检测结果进行详细分析，从而发现操作系统、业务系统存在的风险隐患，为客户解读并持续跟进风险整改期间各类技术问题，协助企业提升操作系统、业务系统本身的健壮性，进而提高内网横向攻击门槛。

2.2.2 安全策略检查

安全策略可以简单理解为一组用于保护网络安全的既定规则。其目的在于控制进出网络的访问行为，保护特定网络免受攻击，同时保障网络之间的合法通信。安全人员可以结合业务需求在系统中配置合适的安全策略，对通过设备的数据流进行检验，放行符合安全策略的合法流量，阻断非法流量，实现访问控制，保证网络安全。

传统的安全策略与业务的结合度不高，难以进行高细粒度的安全分析。在攻防演练中高强度的攻击下，很容易出现策略的检测盲区，进而导致被攻破的局面。因此，在攻防演练前期对安全策略的检查、优化非常重要。

2.2.3 安全防线加固

安全加固和优化是实现网络安全的关键环节。通过安全加固，可以在安全系统的网络层、主机层、软件层及应用层等不同范围建立起符合安全需求的安全状态，并基于此实现对企业组织安全系统的保护。

安全加固是配置软件系统的过程，针对服务器操作系统、数据库及应用中间件等软件系统，通过各种不同的方法修复可能被攻击者利用的漏洞，加强系统安全配置，增加攻击者入侵的难度，提升安全防范水平。它与攻击面收敛、漏洞修复、安全策略优化及等工作形成了完整的风险管理闭环。

2.3 风险收敛加固面临的挑战

攻防演练中，企业在提升蓝队安全防护水平的主要方法之一是缩小攻击面、加固原有脆弱点。但这件事说起来容易做起来难，安全人员在试图进行风险收敛加固时，常常会面临以下挑战：

- **网络不具备可见性。**软件漏洞和网络盲点是常见的安全挑战。随着攻击面的扩大，减少这些漏洞和盲点需要洞察和控制所有流量，以及监控未经授权的设备或请求网络访问的用户的能力。但大部分网络活动或资产处于“隐藏”的状态，安全人员难以实现即时可见。
- **网络环境复杂。**随着云环境、虚拟机、容器等新名词的涌现，网络安全面临的局面越来越复杂，风险收敛加固同样无法实现“一招鲜吃遍天”，安全人员必须针对保护对象的特质制定个性化防护策略，这对有限的安全防护资源与技术人员来说，都是巨大的压力。
- **难以进行集中策略管理。**当今的企业网络高度分散，网络攻击发生的概率大幅度提升。企业需要通过分层访问和策略控制功能来实现集中统一管理所有用户、设备和网络的网络访问策略，以更好地保护网络。

- **难以实现主机间的隔离。**网络攻击隐藏的时间越长，造成的伤害就越大。一旦攻击者通过网络入口，他就会在受信任区域内横向移动以避免被发现，并在整个企业范围内传播以危及数据和系统。企业需要通过主机间的隔离将网络划分为多个区域以防止横向移动来降低这种风险。

企业想要解决这些问题，不仅需要具备专业安全知识的技术人员，还需要特定的安全工具，以「产品+服务」相结合的形式，从多个角度来实现攻防演练前期的风险收敛与安全加固。

2.4 最佳实践：青藤风险收敛加固服务

根据多年攻防演练经验，青藤将前序阶段的工作聚焦于安全的多维度精细化提升，从而收敛攻击面，并凭借经验丰富的专业安全团队和主机安全、容器安全及微隔离等安全产品，实现了细粒度的资产清点、多种类型的风险发现，以及安全加固等多个功能。

- **专属精细化梳理加固：**青藤安全服务团队从资产评估、安全策略检查和安全防线加固三个方面，对企业安全系统的被攻击面和脆弱点进行全面、细致的梳理，最大程度从事前阶段保障攻防演练的防护能力。
- **专家级风险评估、策略配置：**青藤安全团队人员拥有多年攻防演练实战经验，对攻防流程和细节有全面的认识，具备风险评估和策略配置方面的专业知识。
- **攻击队视角多维度分析、收敛：**青藤安全团队从攻击队视角出发，结合企业个性化特征进行多维度分析，基于可能的攻击方式发现隐藏风险，包括网络、软件系统、Web 应用等多个攻击途径和后门、社工、近源等多种攻击方式。

第三章 安全监控篇

近几年的攻防演练显示，攻击方的手段越来越隐蔽，经常通过 0Day、NDay 漏洞快速侵入靶标系统并取得控制权限。这种隐蔽性的攻击给防守方的工作带来了很大的难题。

与攻击方尽量隐蔽痕迹、防止被发现的意图相反，防守方需要尽早发现攻击痕迹，并通过分析攻击痕迹，调整防守策略、溯源攻击路径甚至对可疑攻击源进行反制，而建立全方位的安全监控体系是防守方最有力的防卫武器。

3.1 什么是网络安全监控?

网络安全监控是持续观察用户网络中所发生事情的过程，目的在于监测潜在的网络威胁和及早发现系统被入侵的风险。安全监控可以理解为网络安全界的“吹哨人”，它在检测到网络攻击时发出报警，并在造成严重损害之前帮助用户做出响应，及时检测和管理潜在威胁，有助于保护用户的业务应用程序、数据以及整个网络。

安全监控的工作通常需要包括以下几个方面：

1. 收集和分析数据以识别网络变化或异常行为
2. 利用威胁情报来识别最新的风险
3. 确定需要注意的特定行为类型
4. 在威胁成为安全事件之前采取行动
5. 生成详细的网络安全报告

网络攻防演练中，监控工作主要由安全监控和应急处置小组完成。他们一般将监控重点放在三个端上：网络端、服务器端和个人终端。

- **网络监控。**当攻击者通过网络发动攻击，就会产生网络流量。防守方通过对企业外部与内部间的所有流量进行监控和分析，结合安全人员的深入分析，可快速发现攻击行为，并提前做好针对性防守准备。
- **主机监控。**通过在每台主机（服务器）上安装代理（Agent）来进行对操作系统层面的日志监控，日志信息是帮助蓝队分析攻击路径的一种有效手段。蓝队通过分析用户系统的行为和配置状态，并结合网络全流量监控措施，从而准确、快速地找到攻击者的真实目标主机。
- **终端监控。**除了网络与主机以外，对终端的监控同样必不可少。红队很容易从终端发起攻击，然后逐步渗透到核心服务器。因此，持续监控终端的日志和行为也是安全监控的重点之一。

安全监控不是攻防演练的目的，它只是蓝队进行安全防护的手段之一。安全监控应该覆盖攻防演练的全流程，除了流量和日志，防守方通常还会安排专门的安全人员对互联网上新披露的漏洞进行持续监控，防止其成为红队的入侵点。

3.2 为什么需要安全监控?

不同于传统的渗透测试，攻防演练中红队完全按照攻击者的思维，发起高强度、高水平的网络攻击，专注于攻击和暴露网络安全漏洞。因此，对蓝队来说，监控是能够及时发现攻击的至关重要的一步。虽然预防性安全技术能够应对已知的基于签名的威胁，但蓝队仍需要网络安全监控来识别更复杂的威胁，它可以帮助蓝队：

1）缩短响应攻击的时间

网络攻击可能会在最意想不到的时候发生，用户必须在检测到威胁后立即进行控制和补救。

持续的网络安全监控可以让用户在攻击造成广泛破坏之前做出响应。

2）检测到新的未知威胁

由于网络安全形势在不断变化，新型攻击层出不穷。因此，防守方不能仅仅依赖于对已知威胁的特征值来进行安全防护，他们需要基于对流量、主机上异常行为痕迹等监控来发现新的未知威胁，例如 0day 攻击。

3）限制红队攻击造成的损害

在攻防演练中，攻击方往往通过某一漏洞进入内网，继而横向移动，最终拿下靶标系统。这种情况下，通过网络安全监控，用户可以及时发现并阻止攻击者在内网的移动。安全监控会自动检测用户网络中的任何异常活动，并阻止它威胁蔓延到其他区域造成广泛破坏。

3.3 实施安全监控的 4 大要点

虽然安全监控对蓝队做好安全防护来说至关重要，但建立有效监控机制的过程并不简单。笔者整理了用户在实施安全监控时涉及的基本步骤。

1）确定监控范围和要重点保护的靶标系统

攻防演练中，防守方的监控范围可以概括为外网、内网两个维度，外网代表企业资产在互联网中的暴露面，比如 IP 地址、端口的数量等；内网代表企业内部各部门联通或远程办公人员访问内网服务等情况。

另外，在确定监控范围之后，蓝队还需要明确保障目标系统（靶标系统）和重点资产，并对重点监测资产进行监测优先级排序，这样才能将有限的资源用在重点资产监控上。

优先级	系统类型	重要资产
高	靶标系统	目标系统、域控、邮件系统等
中	重点数据服务器	集中管理平台、证书认证中心、云桌面
低	非核心业务资产	一般应用设备资产等

图 6 攻防演练中资产监控优先级排序

2）创建一个识别用户行为变化的流程基线

针对潜在内部威胁，需要通过持续的安全监控。首先，必须为整个企业组织的标准用户行为设置基线，了解大多数员工通常如何使用网络中的应用程序和数据。随后，就可以通过安全监控和行为基线来识别一些可能存在潜在安全威胁的可疑行为变化。

3）确保持续监控所有端点

当攻击者侵入内网之后，为了获取更多的资产信息进行下一步行动，他会进行横向渗透。因此，用户必须持续监控所有端点，包括台式机、笔记本电脑、服务器和其他设备。

4）与应急处置组协同工作

攻防实战阶段监控人员需具备基本的安全数据分析能力，根据监测数据，情报信息能基本判断攻击有效性。一旦确定攻击事件，应立即协同应急处置人员采取技术手段遏制攻击、防止蔓延。事件处置环节，应联合运维和安全等多个岗位人员协同处置。

3.4 攻防演练中安全监控最佳实践

考虑到技术和人员等方面的原因，很多企业并不具备独自实施安全监控的能力，这就需要选择一个靠谱的安全厂商提供托管式的安全监控服务。

青藤作为有 6 年多攻防实战经验的安全厂商，将专业的安全监控服务与主机安全、容器安全、微隔离等多款安全产品相结合，形成了「产品+服务」的安全监控服务模式，可以创建

针对不同用户的独特需求定制专家策略。从识别漏洞到修复漏洞，青藤的安全服务为用户的提供全流程的安全保护。

1）持续性监控分析，及时发现最重要的风险

主动、持续性地监控所有主机上的软件漏洞、弱密码、应用风险、资产暴露性风险等，并结合资产的重要程度进行风险分析，准确定位最急需处理的风险，帮助企业快速有效解决潜在威胁。另外，安全团队持续关注国内外最新安全动态及漏洞利用方法，不断推出最新漏洞的检测能力，实现紧急安全事件快速响应。

2）多锚点、全方位攻击监控

通过对攻击路径的每个节点进行深入监控，提供了多平台、多系统的全方位、高实时的攻击监控，对进程变化、文件变化、登录登出等事件了如指掌，做到了实时监控“全”方位，保证了能实时发现失陷主机，对入侵行为进行告警。

3）只告警“成功的入侵”，减少告警量

由于网络安全监测设备原理机制的原因，误报在所难免。当有大量误报时，网络安全监测人员只能通过经验进行排除，难度很大。但青藤安全监控服务只对“成功的入侵”行为发出告警，有效减少告警量，提升了告警有效性。

第四章 攻击研判篇

响应作为遏制攻击、缩小攻击影响面的具体执行阶段，被视为攻防演练中的关键一步。但在对检测到的事件进行处置之前，有一个对事件从识别到评估的过程。这个过程被称为“攻击研判”，攻击研判相当于整个事件响应流程的“军师”，承担分析判断安全事件和决定处置方式的任务。

4.1 攻击研判的定义及重要性

网络安全中的攻击研判，可以理解为人工层面对攻击事件进行再分析的行为。安全人员针对安全系统或工具发出的告警，通过结合已有的经验和相关工具，来判断其是否为真实存在的攻击，并根据判断结果做出响应的响应、给出处置建议。

一般来说，对攻击事件的分析研判通常从以下 4 个维度进行：

- 对已发现攻击的来源进行研判；
- 综合分析攻击技术、工具和路径，判断其威胁性大小；
- 攻击意图研判；
- 处置方式判断。

攻击研判可以看作安全防护流程最为关键的一环。它上承安全告警的分析，下接安全处置的实施，是安全防护过程中技术含量最高的一步。

一个企业组织，拥有攻击研判能力是至关重要的。这样在发生告警的时候，它可以做出正确的判断，进而实施有效的措施，使情况恢复控制。攻击研判，同时也是事件响应过程中最具挑战性的环节：确定是否发生了事件，事件影响面有多大，后续如何遏制或根除异常、可疑活动。

4.2 攻击研判中的团队角色分类

为了有效地处理网络安全事件，企业组织需要一个专门从事攻击研判的团队。这个团队的任务是当安全告警发出时，按照既定计划对事件及时进行分析和判断。

以下是一个组织内进行全面、协调的攻击研判所需的角色列表。用户可以根据企业组织的规模、结构以及监管和行业要求来定制此列表。例如，一个人可以担任几个角色，或者几个人可以协调分担一个角色的责任。

角色	主要任务
安全运营中心	对每个安全警报进行分类、收集证据并确定适当的行动
研判管理团队	向利益相关者提供证据、建议和意见，并确定事件的节奏
安全专家团队	参与重要和高优先级的事件
威胁狩猎团队	确定事件的根本原因，还原攻击路径

图 7 攻击研判中的人员角色与任务

攻击研判团队由专业安全人员组成，每个人在处理事件时都发挥着重要作用。

- **安全运营中心。**对每个安全警报进行分类、收集证据并确定适当的行动。轮班工作的分析师必须对网络安全威胁有广泛的了解，他们能够访问各种安全平台和工具，例如 SIEM 和 EDR 解决方案。这些工具会生大量的警报，安全分析师需要能够理解和解释这些数据。如果事件为高优先级或超出技能范围，则需上报事件管理团队。
- **研判管理团队。**管理团队向相关人员提供证据、建议和意见，并确定事件的节奏，确定需要完成哪些任务、谁来完成，以及应该在什么时候完成。所有事件流转和通信也都由管理团队完成。
- **安全专家团队。**他们只参与重要或高优先级的事件。与运营中心的分析师拥有广泛的技能组合不同，专家团队由具有专业技能的个人组成，例如恶意软件分析师和数字取证专家。该团队提供专家技术建议和分析，并由管理团队分配任务。
- **威胁狩猎团队。**尝试确定事件的根本原因并还原攻击路径，为后续响应工作提供信息。确定对手能够在环境中访问和操作的条件。这些条件将为事件分类和事件后续活动提供信息，以调整网络和系统，使其实现更好的安全防护功能。

4.3 攻击研判的 6 个步骤

攻击研判属于安全事件响应的一部分，为了更好地了解攻击研判在整个事件响应过程中的作用，我们可以把列出包括攻击研判在内的事件响应全流程，其中蓝色部分属于攻击研判的流程部分。

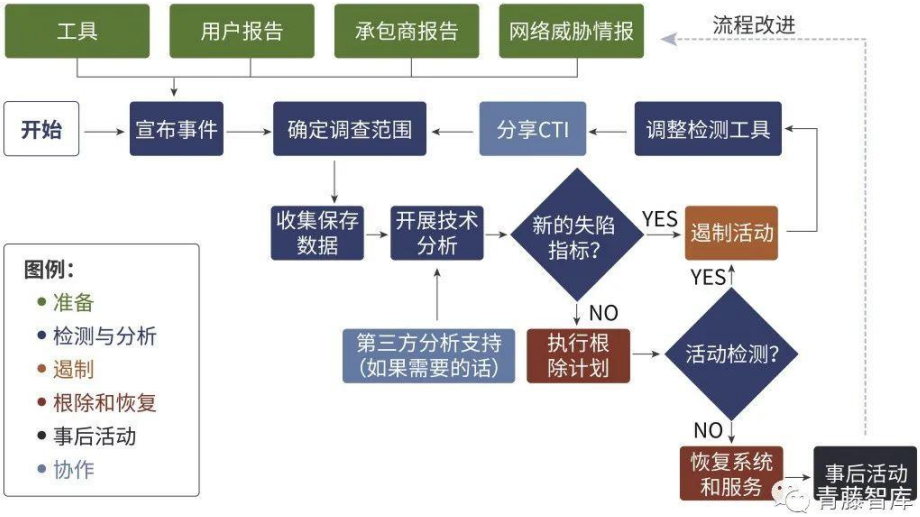

图 8 安全事件响应的完整流程

在攻防实战中，根据告警发生后防守方的响应流程，我们可以把攻击研判服务，划分为以下 6 个步骤：

1）攻击告警真实性研判

在接到告警研判服务请求后，安全专家通过内置的研判溯源模型并结合实际环境，快速分析告警主机的进程和操作审计事件，确认告警的真假以及攻击者还做了其他哪些操作，明确告警主机是不是已被入侵，安全专家进行系统性的梳理并给出详细的研判分析报告。

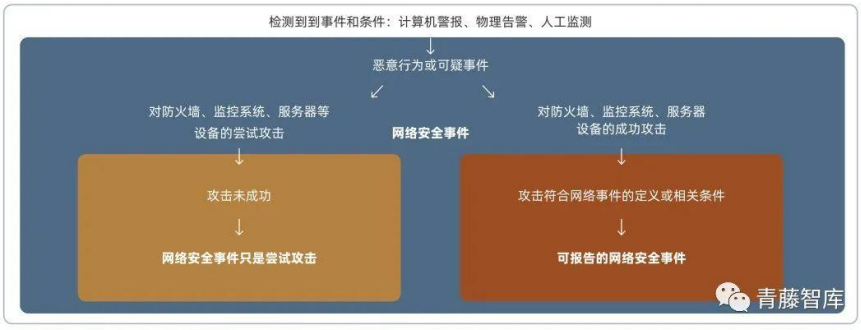

图 9 攻击研判的结果分类

如上图所示，对在系统发出警报后好做出响应的处置以前，需要对警报进行确认，是误报，还是真的有告警事件发生？如果告警是真实的，那么攻击者是正在试图入侵的过程中，还是已经成功入侵？只有确认告警事件为攻击者已经成功入侵后，才会启动响应处置。

告警研判的结果和对应措施也可以用下表直观地展示出来：如上图所示，对在系统发出警报后好做出响应的处置以前，需要对警报进行确认，是误报，还是真的有告警事件发生？如果告警是真实的，那么攻击者是正在试图入侵的过程中，还是已经成功入侵？只有确认告警事件为攻击者已经成功入侵后，才会启动响应处置。

告警研判的结果和对应措施也可以用下表直观地展示出来：

告警研判的结论	对应的响应措施
告警为误报不需要处置	需要进行策略优化
告警为尝试攻击，对系统无影响	需要后续持续关注
告警为真实告警，告警主机已被入侵	需要上报决策组进行应急响应

图 10 攻击研判的结果分类及响应措施

2）攻击事件调查

一旦确定了告警的真实性，安全专家要通过主机、流量侧的日志以及系统告警等信息，对攻击事件进行调查。并根据攻击行为特征建立一套通用的方法论，生成《XXX 事件调查报告》。用户可以根据这套方法论在自己的安全设备中添加检测规则，以便在下次面对相同攻击的时候快速做出响应。

在这个过程中，请参阅以下关键问题以全面了解攻击事件：

- 最初的攻击媒介是什么？（即，攻击方如何获得对网络的初始访问权限？）
- 攻击方如何访问环境？

- 攻击方是否利用漏洞来获得访问权或特权?
- 攻击方如何维持指挥和控制?
- 攻击方在网络或设备上是否有持久性?
- 持久性的方法是什么（例如，恶意软件后门、webshell、合法凭证、远程工具等）
- 哪些账户已被盗用，这些账户是什么权限级别（例如，域管理员、本地管理员、用户账户等）?
- 使用什么方法进行侦察?
- 是否发生横向移动?如何进行横向移动（例如，RDP、网络共享、恶意软件等）?
- 数据是否被泄露，如果有，是什么类型的，通过什么机制?

3）失陷范围排查

安全事件发生时，对于横向移动主机，安全专家首先会根据现有信息找出一台确认失陷的主机，然后以这台失陷主机的数据以及它的互联关系为线索，在用户系统中展开内网溯源，确认是否存在被横向渗透的主机，并循环此过程逐步找出所有失陷主机，确认攻击影响面及具体的失陷范围。

图 11 根据攻击者 TTP 确定失陷主机范围

4）攻击过程还原

攻击溯源是事件响应的关键，也是安全能力提升的关键。通过对被攻击资产的分析与溯源，还原攻击路径与攻击手法，用户不仅能够有效提升攻防演练效果，还可增强常态化安全防御能力，将攻击事件转换为防御势能，避免二次攻击事件的发生。

5）防守方成果报告整理

在攻防演练中，防守方在完成攻击确认到调查、还原的整个流程之后，需要整理出一份防守报告，阐述攻击的真实性、攻击的覆盖范围、攻击者的攻击路径及行为。并将报告提交给组织方，即可得分。

6）攻击清除处置建议

最后，根据对攻击者所用技术和攻击路径的反向梳理结果，安全团队要综合分析对方的攻击动机和意图，以及用户自身的防护水平及目的，给出合理的处置建议。

以上 6 个步骤是安全专家在攻防演练或日常防护中所要实施的攻击研判流程，不同企业的攻击研判服务都大致如此。但虽然流程基本一致，不同企业组织的攻击研判质量却参差不齐，究其原因，在于研判模式的区别。

攻防演练是实战化的安全能力考验，各种高级、未知、高隐藏型攻击威胁，已成为攻防演练的主流攻击方式。一般情况下，攻防演练中的攻击不可能只持续一次，它一定是长时间、周期性、多 IP 的攻击。这时候要想在系统发出告警后，实现全面、高效率的研判和处置，研判模式必须由单纯的“服务型”向“产品+服务”型转变，除了专业安全人员的服务以外，还需要高可用、高易用的分析研判工具，两者有机结合，才能在面临不同攻击时实现准确、快速、有效的攻击研判。

4.4 基于网络安全“黑匣子”的攻击研判服务新模式

上文提到了攻击研判团队的角色分类，其实，安全人员除了自己的技能以外，还需要相应的安全工具来支持攻击研判工作。当然，这些工具不能取代安全人员本身。两者只有相互配合，才能更好地履行每个角色所担负的责任。青藤正是基于被称为“网络安全黑匣子”的青藤猎鹰·威胁狩猎平台才实现了更高效的攻击研判服务模式。

黑匣子，又叫做“飞行记录器”，是安在客机上用来记录客机飞行信息的重要载体。它可向调查人员提供飞机在失事前一段时间内的飞行情况，是事故分析的重要证据来源，找到黑匣子往往意味着离“真相”更近了一步。

与“黑匣子”的溯源取证功能类似，青藤猎鹰凭借其“溯源已知威胁、捕获未知威胁”的能力成为攻击研判的重要工具，并提供了「产品+服务」的攻击研判创新服务模式，可应用于告警真实性确认、攻击事件调查、攻击路径还原等多个流程。

图 12 青藤猎鹰在攻击研判中的作用机制

1.快速确定告警的真实性

根据收集的情报数据，青藤猎鹰会确定威胁狩猎的目标；界定调查范围，选择要进行狩猎的系统及相关的数据源；然后制定详细的狩猎计划，采用相关技术和工具来分析不同来源的数据，确认系统中是否存在威胁。

2.多种告警类型深入查询

青藤猎鹰可以通过青藤自研的一个类 SQL 查询引擎，使用统一的方式对所有数据进行检索，支持 10 余类告警查询，包括暴力破解、异常登录、反弹 shell、Web 后门、可疑操作、内存后门等。

3.全方位还原攻击路径和流程

在确认攻击事件后，青藤猎鹰可基于主机 Agent 的事件采集，对攻击事件进行快速溯源，回溯分析黑客攻陷了哪些机器及其横向移动的路径链条，进而切断攻击源头。

4.联合多种安全工具协同防御

青藤猎鹰还可与其他安全产品联动，通过连接 IPS/WAF/蜜罐等网络安全检测设备进行事件调查，实现了网络安全监控、事件研判、分析溯源、应急处置等各项工作的协同。青藤猎鹰的重点是完善内网层面的告警验证和主机层横向溯源，与流量平台形成了良好的组合。

作为有 6 年多攻防实战经验的安全厂商，青藤将专业的服务与多款安全产品相结合，形成了「产品+服务」的创新安全服务模式。目前已服务 1000+涉及金融、运营商、能源、电力、政府、军工等行业的攻防演练项目，实现所有关基行业的全面覆盖，并在省、市级及行业攻防演习中多次取得第一，受到了各个行业的广泛认可。

此外，通过对各行业各种类客户的服务经验的充分总结，青藤红队形成了一套快捷、简单的攻防演练服务运行模式。服务期间可基于专家团队与规范化流程保证服务的全面性、高效性、专业性、可靠性。

青藤云安全 | 让安全之光照亮数字世界的每一个角落

服务热线：400-188-9287
官网：www.qingteng.cn
总部地址：北京市海淀区创业路8号群英科技园1号楼5层

获取更多信息