安全牛
AQNIU.NET

入侵与攻击模拟 BAS应用指南（2025版）

构筑数字时代坚韧防线：BAS 驱动主动防御安全



版权声明

本报告为北京谷安天下科技有限公司（以下简称“本公司”）旗下媒体平台安全牛研究撰写，报告中所有文字、图片、表格均受有关商标和著作权的法律保护，部分文字和数据采集于公开信息，所有权为原著者所有。未经本公司书面许可，任何组织和个人不得将本报告内容作为诉讼、仲裁、传媒所引用之证明或依据，不得用于营利或用于未经允许的其他用途。任何未经授权的商业性使用本报告的行为均违反《中华人民共和国著作权法》及其他相关法律法规、国际条约。未经授权或违法使用者需自行承担由此引发的一切法律后果及相关责任，本公司将依法予以追究。

免责声明

本报告仅供本公司的客户或公司许可的特定用户使用。本公司不会因接收人收到本报告而视其为本公司的当然客户。任何非本公司发布的有关本报告的摘要或节选都不代表本报告正式完整的观点，一切须以本公司发布的本报告完整版本为准。

本报告中的行业数据主要为分析师市场调研、行业访谈及其他研究方法估算得来，仅供参考。因调研方法及样本、调查资料收集范围等的限制，本报告中的数据仅服务于当前报告。本公司以勤勉的态度、专业的研究方法，使用合法合规的信息，独立、客观地出具本报告，但不保证数据的准确性和完整性，本公司不对本报告的数据和观点承担任何法律责任。同时，本公司不保证本报告中的观点或陈述不会发生任何变更。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。

本报告所包含的信息及观点不构成任何形式的投资建议或其他行为指引，亦未考虑特定用户的个性化需求或投资目标。用户应结合自身实际情况独立判断报告内容的适用性，必要时应寻求专业顾问意见。报告中涉及的评论、预测、图表、指标、理论等内容仅供市场参与者及用户参考，用户需对其自主决策行为负责。本公司不对因使用本报告全部或部分内容所产生的任何直接、间接、特殊及后果性损失承担任何责任，亦不对因资料不完整、不准确或存在任何重大遗漏所导致的任何损失负责。

目录 contents

引言 4

关键发现 5

第一章 背景概述

1.1 当前网络安全威胁的趋势 7

1.2 网络安全政策法规要求 8

1.3 企业安全管理面对挑战 11

第二章 BAS 的基本概念

2.1BAS 的基本概念和发展 13

2.2BAS 价值体现和必要性 18

2.3BAS 与安全框架的关联 20

第三章 BAS 的能力框架和关键技术

3.1BAS 的能力框架 24

3.2 关键技术 26

3.3BAS 量化指标体系 36

第四章 国内外 BAS 市场和技术现状

4.1 国外 BAS 市场和技术应用现状分析 43

4.2 国内 BAS 市场和技术应用现状分析 48

第五章 AI 赋能 BAS 验证

5.1AI 赋能 BAS 验证应用现状 57

5.2AI 赋能 BAS 验证的不足与未来展望 65

第六章 BAS 的十大应用场景

场景一：安全产品有效性与防护覆盖度的持续验证 67
场景二：纵深防御体系与攻击链的整体效能评估 69
场景三：BAS 驱动安全运营优化 72
场景四：合规保障与安全产品采购决策 73
场景五：提升人员安全意识与洞察未知威胁 74
专项场景六：护网演练前沿预演与实战化准备 76
专项场景七：高级 APT 威胁与 0day 漏洞的防御验证 77
专项场景八：分子公司/上下级单位的安全能力验证 78
专项场景九：云环境与复杂异构网络安全验证 80
专项场景十：数据安全防护能力验证 81

第七章 BAS 实施部署与建议

7.1BAS 实施原则 82
7.2BAS 实施路线图 83
7.3BAS 实施：常见挑战和策略 97

第八章 BAS 场景应用实战指南

8.1 场景一：安全产品防护能力验证场景 110
8.2 场景二：纵深防御体系防护能力验证场景 112
8.3 场景三：安全运营验证场景 115
8.4 场景四：合规保障验证和安全产品采购场景 118
8.5 场景五：钓鱼演练与风险洞察验证场景 121
8.6 专项场景六：攻防演练前验证场景 123

8.7 专项场景七：高级 APT 威胁安全防护验证场景 126
8.8 专项场景八：分子公司安全防护能力验证场景 129
8.9 专项场景九：云环境安全防护能力验证场景 132
8.10 专项场景十：数据安全防护能力验证场景 135

第九章 BAS 优秀案例研究

9.1 优秀案例一 电力行业安全有效性验证案例（塞讯科技提供） 138
9.2 优秀案例二 某大型金融机构有效性验证案例（矢安科技提供） 143

第十章 厂商推荐

10.1 厂商选型建议 149
10.2 推荐厂商－长亭科技 151
10.3 推荐厂商－华云安 151
10.4 推荐厂商－绿盟科技 152
10.5 推荐厂商－墨云科技 153
10.6 推荐厂商－塞讯科技 153
10.7 推荐厂商－矢安科技 156
10.8 推荐厂商－知其安科技 159
10.9 其他特色厂商 160

第十一章 未来趋势与建议

11.1 未来趋势 161
11.2 建议 163
参考文献： 166

引 言

随着全球数字化转型进程的加速，使网络边界快速向外拓展，攻击面不断扩大。与此同时，网络安全威胁正日趋复杂且持续升级，攻击者不再专注于单一手段，而是利用人工智能、零日漏洞以及供应链缺陷及社会工程学等多种方式，构建定制、多级化、组合化的攻击工具链，对目标系统进行渗透与破坏。不断演变的威胁格局使传统基于签名或规则的被动防护系统难以有效应对，尤其是面对未知威胁时的力不从心，对企业构成了严峻的挑战。我国高度重视网络安全工作，构建了《网络安全法》《关键信息基础设施安全保护要求》（GB/T39204-2022）、等保 2.0（GB/T22239-2019）等较为完善的网络安全法律法规，并明确提出了对安全防御措施有效性进行验证的要求。此外，常态化护网行动和实战化攻防演练的普及，也促使企业从安全建设转向实战化验证阶段。

但是，尽管国内企业在网络安全建设方面投入了大量资源，部署了多种安全产品，构建起复杂的安全体系，但普遍存在投入与安全实际效果难以准确计量和有效评估的困境，在攻防演练及中屡屡失守，安全事件频发。企业亟需实战化、常态化的验证工具，以实现从被动防御向主动免疫的转型。

在此背景下，入侵与攻击模拟（Breach and Attack Simulation，简称 BAS）技术应运而生，并迅速成为提升企业网络安全态势的核心驱动力。BAS 技术采用自动化、常态化、无害化的方式，从攻击者视角出发，进行高度仿真的攻击模拟，能够精准揭示防御体系中的薄弱环节，量化安全防护的实际效果，进而驱动安全运营的持续优化。为企业开辟了一条从被动响应转向主动免疫、从依赖经验判断走向数据驱动的实践路径，正在深刻改变网络安全的攻防博弈模式。

针对上述背景、挑战与实践需求，本报告深入探讨入侵与攻击模拟的重要性、应用面临的挑战及应对策略，详细介绍 BAS 的概念、能力框架、国内主要应用场景、具体实施落地方法，对近期优秀案例进行研究，并推荐优秀厂商。旨在为组织提供实用、可落地、可实操的应用指南，助力企业利用 BAS 提升网络安全防护和实战能力，显著提高企业的安全防护水平与运营效率，实现安全与业务的共赢发展，共同推动中国网络安全从有到优、从被动防御到主动出击的战略跨越。

关键发现

一、政策和实战化驱动

- 政策驱动与实战化转型并行驱动：随着中国网络安全法律法规体系的不断完善，以及常态化护网行动和实战化攻防演练的普及，企业安全建设逐渐从传统的合规建设向强化实际成效和实战化对抗转型，BAS 技术作为新兴技术，凭借其独特优势，成为保障网络安全运行的关键工具。

二、BAS 的技术能力

- 无害化测试作为核心基础：所有厂商均将无害化测试技术作为产品核心特性，通过仿真模块、数据包标记、流量控制或沙盘隔离等创新方式实现，在模拟攻击时不会对生产系统造成实际损害、数据破坏或业务中断，有效消除用户顾虑。
- 闭环管理实现价值的关键路径：BAS 的价值不仅在于发现问题，更在于与 SIEM/SOC、SOAR、工单系统等现有安全生态深度集成，实现日志统一回传和结果分析，并通过自动化任务下发和自动化复测，构建攻击模拟－发现分析－修复优化－复测闭环，助力企业从被动安全防御转向主动安全防御。
- 确保模拟攻击的高仿真性和有效性成为竞争点：领先的 BAS 产品将海量威胁情报（特别是 APT 组织的 TTPs）转化为可执行的攻击场景和用例，并将实战攻防经验、工具积累沉淀为 BAS 知识库，经第三方威胁情报验证其真实性，确保模拟攻击的高仿真性和有效性。
- 量化指标体系驱动价值：BAS 提供多维度、可量化的评估指标，包括防护覆盖度、检测率、阻断率、攻击链阻断率、MTTD/MTTR 以及 ATT&CK 模型覆盖率等，使安全投入效果可视化，为安全管理决策提供数据支撑，辅助评估投资回报率。
- AI 深度赋能 BAS 全周期：AI 技术深度集成到 BAS 各环节，目前主要用于智能生成攻击向量、优化攻击策略、分析评估结果、提供修复建议等。未来，AI 将贯穿 BAS 整个流程，实现自主智能攻击路径生成和动态决策，推动威胁预测和智能动态决策。

三、BAS 的市场和技术应用

- 护网演练前预演的重要应用场景：BAS 凭借高强度、多轮次、自动化的攻击模拟能力，成为攻防演练备战阶段的重要工具，帮助企业动态感知攻击面，提前发现并修复防护盲点，提升实战防御能力，应对常态化攻防演练压力。

- 应对高级威胁的独特作用：BAS 深度模拟 APT 攻击和新型/0day 漏洞利用，健全和验证防御体系对已知和未知威胁的抵御能力，提升人员意识，并提供量化指标指导防御优化，助力企业从被动响应转向主动免疫。
- 国内 BAS 市场快速兴起：市场参与者包括传统安全厂商、人工智能驱动型企业等，市场发展迅速，用户认知度不断提升。本土厂商凭借对国内政策、监管要求、实战需求的深刻理解及技术创新，形成中国特色竞争优势。
- 用户集中在重点行业：国内 BAS 市场用户主要集中在金融、运营商、互联网企业，这些行业安全建设完善，监管要求高，利用 BAS 应对高级网络威胁和攻防演练挑战。政府、工业制造、教育、医疗等行业也在积极应用 BAS 技术。
- 用户困惑阻碍市场普及：企业在 BAS 应用中面临不敢跑不会用看不懂等痛点，厂商需在产品易用性、运营服务和呈现价值上持续发力。

四、BAS 的不足和趋势

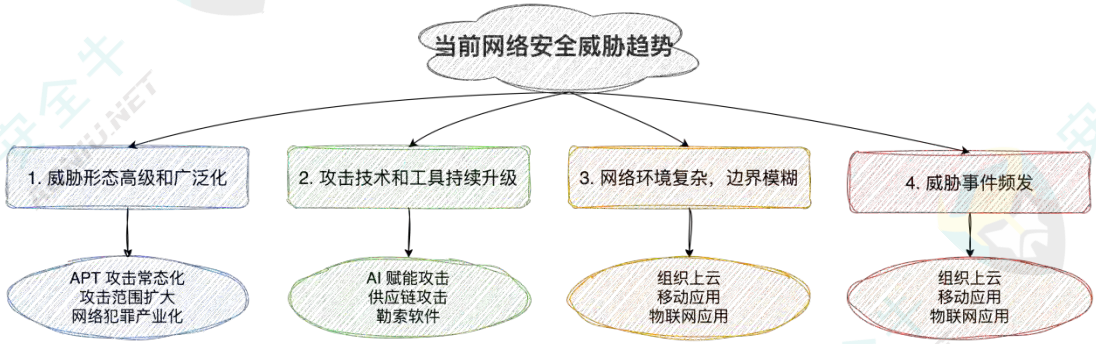
- 缺乏行业统一标准：当前国内 BAS 市场缺乏统一的行业标准，包括攻击剧本、攻击向量和量化指标评估方法，导致不同厂商产品能力和评估结果存在差异，给用户选择带来困难。
- 市场迈向广泛应用阶段：随着国内用户认知度提升和技术成熟推动，BAS 正向整体防御体系实战化验证等方向发展。
- 数据安全和大模型安全防护验证成未来方向：随着《数据安全法》等法规的落地，以及大模型广泛应用带来的安全隐患，BAS 正拓展能力，加强对 DLP、API 安全、供应链安全的有效性验证，同时探索对大模型安全产品的有效性评估。
- BAS 演进为威胁暴露管理框架：BAS 未来将向对抗性暴露管理（CTEM）或对抗性暴露验证（AEV）核心组件演进，与攻击面管理等技术融合，实现从发现暴露面到动态风险收敛的完全闭环。

第一章背景概述

当前，全球数字化转型进程加速，信息技术广泛且深入地渗透到社会经济的各个领域。然而，与此同时，网络安全威胁也随之持续升级并不断泛化，给国家安全、社会稳定以及企业运营带来了极大的挑战。在这样的背景下，威胁的演进趋势以及日益严格的法规要求，成为推动入侵与攻击模拟（BAS）发展的重要因素。

1.1 当前网络安全威胁的趋势

在网络安全领域，企业和政府机构正面临多重严峻挑战，威胁趋势呈现高级化、广泛化、智能化和产业化特点，传统安全防护体系受到严峻考验。企业和机构亟需一种能持续、自动化、实战化验证防护体系有效性的新方法，以激发主动性，实现主动安全治理。



当前网络安全威胁的趋势

1.1.1 网络安全威胁高级化、专业化

网络安全威胁的高级化和专业化表现明显。如今，网络攻击不再是简单的病毒感染或脚本行为，而是高度复杂且专业。高级持续性威胁（APT）已常态化，国家支持的攻击者和高水平犯罪组织常利用其攻击，具有强度高、潜伏期长、攻击链复杂、规避检测能力强等特点，攻击链条变得复杂多级，不再单一，包含多个阶段组成的杀伤链，攻击者利用多种漏洞和技术组合绕过防护，增加检测难度。并且目标明确，主要针对关键信息基础设施、核心技术企业等高价值目标，意图窃取敏感数据、破坏关键系统或长期渗透。同时，勒索软件的商业化与精准化趋势凸显，从广撒网转向精准勒索，开展数据窃取和双重勒索，并通过 RaaS 模式降低攻击门槛，威胁各行各业。

1.1.2 威胁技术和工具持续升级

威胁技术和工具也在持续升级。攻击者在技术和工具的创新迭代速度已超防守手段。他们利用 AI 和大模型提升攻击效率和精准性，如自动生成钓鱼邮件、恶意代码变种，辅助自动化渗透测试和漏洞挖掘，使攻击者能力指数级增长。同时，攻击者发现并利用 0-day 漏洞绕过传统防护，供应链攻击也频繁发生，通过侵害供应商或篡改合法软件分发渠道植入恶意代码，实现大规模感染，给防护者带来更高要求。而且，攻击工具的认知性和规避检测能力增强，采用无文件攻击、内存驻留等手段，使传统特征检测方法难以奏效。

1.1.3 网络环境复杂，范围边界模糊

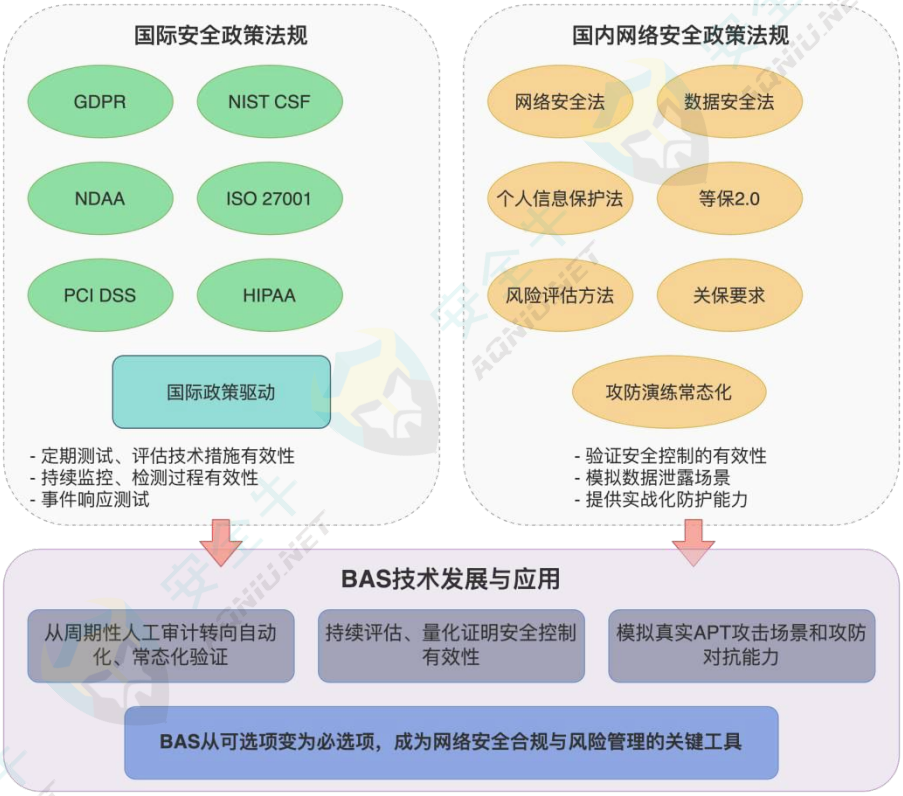
网络环境的复杂化和边界模糊也带来诸多挑战。企业数字化转型使 IT 架构变化，网络环境急剧复杂，传统边界模糊。云计算与多云环境下，企业上云采用多种架构，资产分布广，安全责任边界模糊，云环境的动态性和弹性增加了安全配置和策略管理复杂性。物联网和工业互联网普及，智能安全产品、传感器、工控系统接入网络，使攻击面从 IT 领域扩展到 OT/ICS 领域，带来新安全挑战，尤其对生产运营的潜在物理影响大。远程办公与移动互联常态化，员工通过远程接入点和移动安全产品访问企业资源，企业边界转移，安全和身份验证复杂性增加。攻击面管理（ASM）也面临挑战，资产动态变化和多源性使企业难以全面准确识别管理暴露资产，包括物理资产、云资产等，导致攻击面扩大且难管理。

1.1.4 威胁事件频发，安全形势严峻

网络安全形势严峻，威胁事件频发。全球范围内，数据泄露事件常态化，敏感数据等泄露给企业带来巨大损失和风险。勒索攻击、DDoS 攻击等导致业务中断和关键基础设施受损，威胁社会经济运行和国家安全。网络战和地缘政治风险使网络空间成为国家间对抗新战场，网络攻击与地缘政治事件交织，对国家安全稳定形成战略性挑战。国内网络安全事件频发，企业和组织遭受巨大经济损失和社会影响，甚至引发法律纠纷和监管处罚。如 2022 年 6 月 22 日，国内某大学遭境外网络攻击，源头为美国某组织，使用多种攻击武器，窃取大量高价值数据，还渗透电信基础设施窃取隐私数据。又如 2020 年 2 月 23 日，国内某集团运维人员因个人原因删除业务数据，致业务瘫痪，影响众多商户，造成重大经济损失，相关责任人被判刑。

1.2 网络安全政策法规要求

网络安全威胁的升级，推动各国政府和国外组织不断完善网络政策安全法规，定期提升国家和企业的网络安全防护水平，这些政策法规推动 BAS 从可选项变为必选项，驱动安全实践从周期性验证转向自动化、常态化、数据驱动的验证模式。



网络安全政策法规要求

1.2.1 国外安全政策法规要求

近年来，各国对网络安全的重视程度不断提高，各国纷纷出台一系列网络安全法律法规、监管要求和政策，国外上的法律法规和行业框架正共同推动企业网络安全实践从传统的周期性、人工化审计，转向自动化、常态化、数据驱动的验证模式，这有力推进了企业从部署安全控制向持续验证其有效性的转变，进而驱动了 BAS 技术在全球范围内的需求增长和应用深度。BAS 作为一种能够持续评估、量化证明安全控制有效性的工具，在全球合规和风险管理语境下的重要性日益凸显。

欧盟的《通用数据保护条例》（GDPR）在第三十二条处理的安全中明确要求，企业应采取确保处理系统和服务的持续保密性、完整性、可用性和韧性的技术和组织措施，并特别指出需要定期测试、评估和评价技术和组织措施有效性的流程。这直接推动了企业对持续性验证工具的需求，以自动化、常态化的方式证明其对个人数据的保护是真实有效的。美国的《国家标准与技术研究院网络安全框架》（NIST CSF）在其检测和响应功能中，强调了持续监控、检测过程的有效性以及事件响应测试的重要性，而保护功能则要求对已实施的安全控制进行验证，BAS 通过自动化模拟攻击和验证，为企业提供了量化实现 NIST CSF 各项功能要求的手段。

美国《国防授权法案》（NDAA）：对美国的网络安全能力建设提出明确的要求，包括提升网络安全产品、威胁情报分析、安全事件响应等能力。NDAA 推动美国加强安全运营中心的建设，并积极采用人工

智能、大数据分析等先进技术，提升安全运营的智能化水平。美国国家网络战略要求将提升国家网络安全能力作为重要目标，强化加强网络安全信息共享、公私合作、主动防护等，该战略推动美国和组织加强安全运营中心的建设，并积极采用威胁情报、自动化安全响应等先进技术，提升安全运营的效率和效果。ISOC 的建设与该战略的目标高度契合。

国外权威标准如 ISO 27001（信息安全管理体系）也对技术漏洞管理和安全措施有效性测试提出了要求，如控制项 A.12.6，BAS 作为一种持续性的技术控制验证工具，能够为 ISO 27001 体系的检查环节提供量化证据，并推动改进过程。再如，《支付卡行业数据安全标准》（PCI DSS）规定了每年进行一次外部和内部渗透测试，并在发生重大基础设施或应用升级修改后进行，同时要求进行漏洞扫描。BAS 作为一种持续性、自动化预渗透测试的工具，能够帮助企业在正式测试前识别并修复潜在漏洞，有效辅助提高合规通过率，并为漏洞扫描结果提供实际可利用性的验证。类似地，美国的《健康保险流通与责任法案》（HIPAA）也要求对医疗保健机构的电子保护信息采取技术保障措施并进行评估，BAS 通过对这些技术措施的持续验证，确保了敏感医疗数据的安全性。

1.2.2 国内网络安全政策法规要求与 BAS 的发展

我国高度重视网络安全工作，已初步构建起较为完善的网络安全法律法规和政策体系，不断提高网络安全监管力度，为国内 BAS 市场的发展提供了强劲而独特的驱动力，对网络安全的有效性验证提出了明确且严格的要求，使 BAS 从可选项变为必选项。

《中华人民共和国网络安全法》，作为国家网络安全领域的基础性法律，确立了网络安全等级保护制度，为网络安全保护的必要性提供了基本依据。并要求网络运营者采取技术防范、监测、记录等措施保障网络安全。BAS 通过持续验证安全控制的有效性，帮助企业确保满足等级防护要求，并发现技术措施的不足，从而提升整体防护能力。

《中华人民共和国数据安全法》建立数据分类分级保护制度，明确了重要数据和核心数据的保护要求，包括应通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力，并要求数据处理者履行数据安全保护义务，开展数据安全风险评估，建立数据安全监测预警机制。BAS 能够模拟数据泄露场景，验证数据分级策略、数据防护措施以及评估数据安全防护效果，并可视化泄露路径，从而支撑企业进行数据安全合规治理，验证数据分类分级制度的效果。

《中华人民共和国个人信息保护法》确立了个人信息处理的合法、合理、必要和诚信原则，对信息处理活动制定了个人规范，强调个人信息处理者需采取个人信息安全技术措施，并定期进行合规审计。BAS 可以通过模拟敏感数据泄露路径和社工攻击，或模拟个人信息非法获取或破解场景，验证个人信息保护措施和自动化决策的安全性，确保数据处理活动的合规性。

《GBT22239-2019 信息安全技术网络安全等级保护基本要求》（以下简称等保 2.0）要求加强积极防

护、动态防护、整体防护和精准防护，并纳入云计算、物联网、工业控制系统、大数据等新型环境，如 8.1.7.5 检查，应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性；9.1.10.7，恶意代码防范管理，应定期验证防范恶意代码攻击的技术措施的有效性。BAS 提供验证各项技术措施的实际防护效果和策略效果，并覆盖云、物联网、工控等新兴场景，直接验证等保障 2.0 中技术措施和安全管理要求的落地效果。为等保障评估提供有力的实战证据，帮助企业从符合性效果检查走向实际评估。

《GBT20984-2022 信息安全技术信息安全风险评估方法》针对各类组织开展信息安全风险评估工作的实施流程和评估方法进行了明确，并明确应根据脆弱性访问路径、触发要求等，以及已实施的安全措施及其有效性确定脆弱性被利用难易程度；要求评估人员应对已采取的安全措施和有效性进行确认。安全措施的确认应评估其有效性，即是否真正地降低了系统的脆弱性，抵御了威胁。如 4.2 风险分析原理，应根据脆弱性访问路径、触发要求等以及已实施的安全措施及其有效性确定脆弱性被利用难易程度;如 5.2.3 已有安全措施识别，评估人员应对已采取的安全措施和有效性进行确认。安全措施的确认应评估其有效性，即是否真正地降低了系统的脆弱性，抵御了威胁。

《关键信息基础设施安全保护条例》明确要求运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对可能影响国家安全的网络产品和服务进行安全审查等。BAS 作为自动化、持续性的安全验证工具，能够为关键信息基础设施运营者履行定期测试和风险评估义务，提供可靠的数据支撑。

《GB/T39204-2022 关键信息基础设施安全保护要求》（以下简称《关保要求》），《关保要求》为全面开展关保提出了更加全面、更加细致的操作性要求。明确提出应检验安全防护措施的有效性，对面临的安全威胁态势进行持续监测和安全控制措施的动态调整，形成动态的安全防护机制，及时有效地防范应对安全风险。提升关键信息基础设施应对大规模网络攻击能力。如主要内容及活动检测评估，为检验安全防护措施的有效性，发现网络安全风险隐患，应建立相应的检测评估制度，确定检测评估的流程及内容等，开展安全检测与风险隐患评估，分析潜在安全风险可能引发的安全事件。主动防护，以应对攻击行为的监测发现为基础，主动采取收敛暴露面、捕获、溯源、干扰和阻断等措施。

攻防演练常态化与实战化需求：国家政府常态化组织网络安全攻防演练（如护网行动），极大地推动了企业实战化防护能力建设的重视。BAS 在帮助组织进行实战的有效性验证方面发挥关键作用。使国内市场对 BAS 的需求更加侧重于模拟真实的 APT 攻击场景和攻防对抗能力。

1.3 企业安全管理面对挑战

根据安全牛对十多家的安全厂商的访谈，国内企业在网络安全建设中普遍面临四大难题并陷入困惑。

在安全建设层面，企业尝试从合规驱动转向主动防护，却因成效评估与关键点定位模糊而难以落地；攻防演练中，企业对防护体系的有效性缺乏验证手段，难以摆脱被动挨打的困境；在安全产品运维层面，防护失效后的优化部署成为难题，高级持续性威胁的持续有效性保障更是挑战重重；安全运营方面，团队因人力不足陷入人少事多的泥沼，关键风险的精准识别与防护效果的自我验证能力不足。

目前企业的十大高频故障场景包括：边界防火墙拦截失效、防病毒软件启动故障、SOC 告警积压、终端防护软件覆盖不足、关键资产审计缺失等，均严重威胁企业网络安全。如安全产品已经部署但是规则配置错误或日志丢失导致安全产品能力失效；防护未覆盖导致安全漏洞，暴露管理盲区。

网络安全团队同样深陷困境，面临执行力波动、评估体系不完善、人才短缺等多维度挑战。人员水平参差不齐导致 7x24 小时持续验证难以实现，团队规模与任务量的倒挂现象普遍，优化整改缺乏动态指导依据，安全投入与防护效果难以量化呈现，最终难以向决策层证明安全工作的价值。

企业迫切需要摆脱被动防护的应急响应模式，构建主动防护体系。当前的被动模式下，安全团队普遍存在缺乏感知攻击能力的焦虑，往往在攻击者已深入内网后才发现问题，导致事后补救成本高昂。这暴露了网络安全建设的根本性缺陷：只有在事前主动发现并消除潜在风险，才能真正实现从被动防护向主动免疫的转型升级。

第二章 BAS 的基本概念

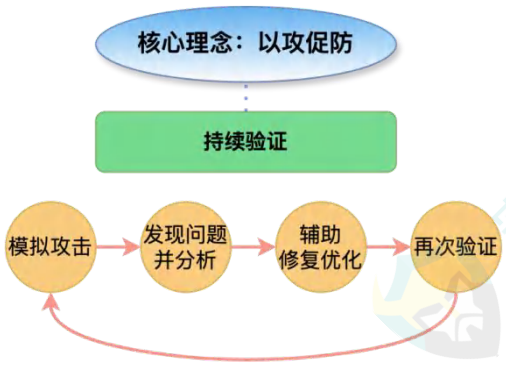
在当今数字化时代，网络安全威胁日益复杂多变，传统安全测试方法在应对复杂、动态的网络环境时逐渐显得力不从心。入侵与攻击模拟（BAS）在这样的背景下应运而生，并迅速发展成为安全防护体系中至关重要的一环。

2.1BAS 的基本概念和发展

网络安全威胁的演进，使传统安全测试方法在应对复杂、动态的网络环境时力不从心。入侵与攻击模拟在这样的背景下应运而生，并迅速发展成为安全防护体系中舵机的一环。

2.1.1BAS 的定义和理念

入侵与攻击模拟（BAS，Breachand Attack Simulation）是一种创新的网络安全验证方法。借助自动化、持续性的软件工具，安全无害化地模拟多种黑客攻击行为，从攻击者视角出发，运用多样化攻击手段，查找并验证企业防御系统漏洞，并借助模拟攻击－分析－修复－复测的闭环流程，推动防御体系改进提升。



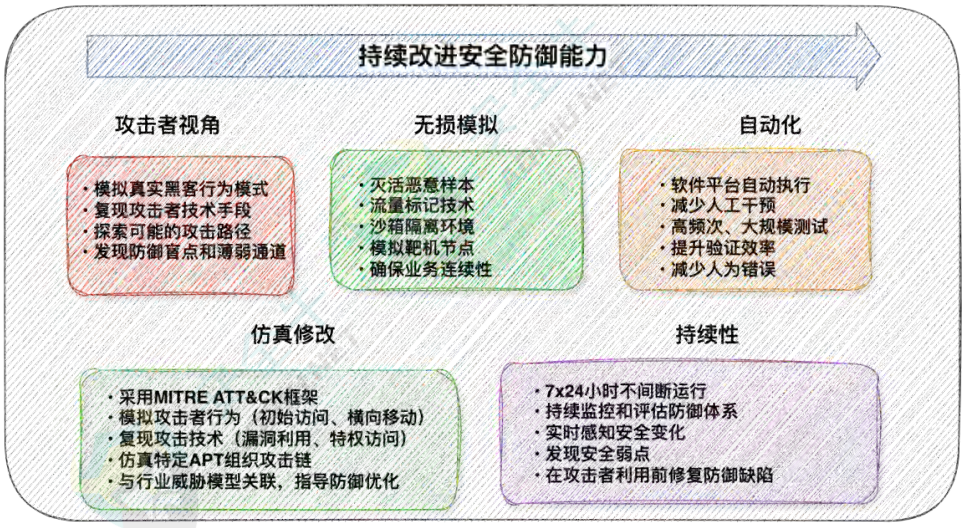
BAS 的理念

BAS 的核心理念

BAS 的核心理念是以攻促防，将安全评估从传统的点对点测试转变为贯穿安全建设全生命周期的持续验证，贯穿企业网络安全管理的各阶段和场景，验证安全产品有效性，发现防御体系的短板，评估攻击路径风险，强调持续进行模拟攻击－发现分析－修复优化－再次验证的闭环，确保安全防护能力在动态 IT 环境中持续有效，提升安全运营能力，满足合规要求，优化安全投资决策，进而促进企业安全能力提升。

2.1.2BAS 的特点

入侵与攻击模拟（BAS）利用自动化、持续性的软件工具，从攻击者视角出发，以安全且无害化的方式模拟多样的黑客攻击。核心目标是验证组织安全暴露面，发现防护盲点，提升安全态势，包括错误配置的安全控制、软件漏洞以及薄弱的安全漏洞。



BAS 的特点

BAS 的主要特点包括：

- 攻击者视角。BAS 的核心在于突破传统的防御思维，从攻击者视角出发，主动模拟真实攻击者的思维模式、攻击路径和技战术。从外部、内部以及横向移动等多个维度，全面探测企业防御体系中的漏洞、配置缺陷或策略盲区，助力企业实现知攻善防，在攻击发生前精准预判并弥补短板。
- 无害化模拟。无害化模拟是 BAS 广泛评估生产环境的关键特性，确保在高度仿真攻击行为的同时，不会对企业的业务系统造成任何实际破坏、中断或数据泄露。例如仅模拟攻击流量或行为而不实际利用漏洞，以及在受控环境中执行高风险操作后自动回滚，消除了企业在核心生产环境进行安全测试的顾虑，是其区别于传统渗透测试的显著优势。
- 自动化。自动化是 BAS 实现常态化和高效率的基础。BAS 通过自动化攻击模拟、日志收集、结果分析和报告生成，使企业能够摆脱传统人工测试耗时费力、更新缓慢、难以规模化的制约，显著提升安全验证的效率和覆盖范围，确保安全评估的及时性和一致性。
- 仿真模拟。仿真模拟是模拟攻击真实性的关键体现，能够高保真地复制真实攻击者的行为模式和网络流量特征，而非简单发送 PoC 代码，能在受控环境中还原真实攻击场景下的交互和响应，更准确地检验安全产品的检测和防御能力，确保验证结果能够有效指导防御策略的调优。
- 持续性。持续性是 BAS 实现动态安全的核心特性。BAS 通过常态化、自动化的验证，不间断地对企

业防御体系进行检测，可感知因网络配置变更、新业务上线、安全策略调整或外部威胁演进而产生的防御短板，并及时驱动安全能力的闭环优化，使企业的安全防护能力始终处于最新、最有效的状态，实现动态、实时的安全威胁防范。

2.1.3BAS 的演进

网络安全验证的历史是一个不断适应威胁、提升效率和追求真实性的过程。BAS 的出现是一演进的必然结果，主要是弥补传统安全测试的固有局限性。



BAS 的演进

安全验证早期背景（2007 年至 2016 年）：

我国等保 1.0 等法律法规的强制要求下，大部分企业开始了合规的网络安全建设，企业开始对安全建设的效果进行测试验证。早期的安全测试主要依赖于人工渗透测试和漏洞扫描，但是这些方法效率低下且无法提供持续的可见性。

BAS 的起源与初步发展（2016 年至 2023 年）：

2016 年左右，大部分企业随着安全建设的逐步完成，在重保、护网等网络安全实战演练的要求下，安全建设从合规阶段向实战阶段过渡。并且随着高级持续性威胁（APT）的兴起、网络攻击的紧迫复杂性以及越来越频繁的攻防演练过程中，安全暴露问题凸显，国内组织开始认识到需要一种验证网络安全控制是否有效的方法。BAS 的概念应运而生，Gartner 于 2017 年首次在其新兴技术成熟度曲线中提及 BAS，并以其作为独立技术类别的正式登场，并与 2018 年，正式将 BAS 纳入安全运营技术成熟度曲线，认可了 BAS 在安全运营中的重要性得到。

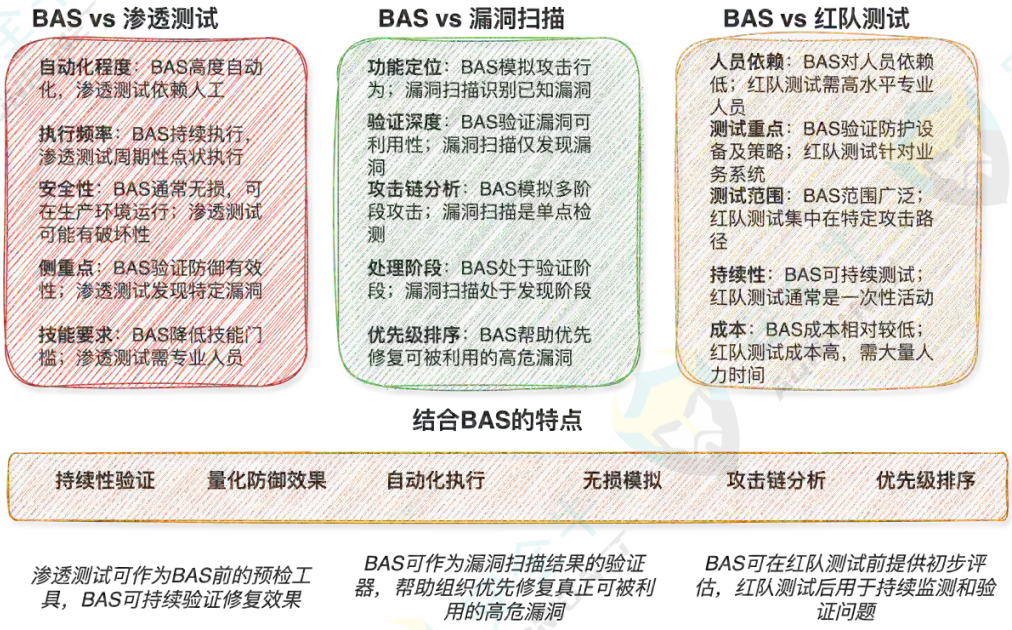
国内各厂商在 2018 年开始关注 BAS 技术，并积极布局 BAS 市场，国内厂商侧，如塞讯科技、矢安科技等厂商在 2022 年左右开展该领域业务，国内用户侧也开始关注 BAS，并积极对 BAS 的概念进行了解。2022 年，Gartner 发布 2022 年国家网络安全技术成熟度曲线，将 BAS 作为国家的新兴技术得到初步发展。

国内 BAS 市场快速发展（2024 年至今）：

BAS 技术逐渐成熟，产品功能十分丰富，能够覆盖更多的攻击和威胁场景。厂商开始提供 SaaS 化部署，降低使用门槛。国内一线城市的大部分头部组织已经理解 BAS 的概念和理念功能，特别是护网行动的开展，各组织积极进行试用，部分头部组织开始采购 BAS 并进行应用，国内 BAS 市场进入快速发展阶段。

2.1.3BAS 与传统安全验证技术的区别与结合

传统渗透测试和漏洞扫描在验证方面具有的局限性使组织在复杂多变的网络环境中缺乏持续性、全面的安全性，面临较大的网络攻击风险。BAS 不是替代传统安全验证技术，而是有效补充和延伸，BAS 凭借自动化、持续性、无害化模拟的特点，可以弥补传统渗透测试和漏洞扫描在验证方面的不足，形成更全面、高效的安全验证体系，帮助组织在复杂多变的网络环境中建立持续、全面的安全防护能力。



BAS 与传统安全验证技术的区别

1）与渗透测试的区别与结合

BAS 高度自动化，可实现持续、大规模的模拟执行。而渗透测试主要依赖人工，呈现周期性、点状执行的特点。BAS 侧重于持续验证安全控制的有效性，量化防护效果并进行监控；渗透测试则侧重于发现特定时间点、特定范围内的漏洞，提供详细的攻击路径报告。BAS 通常是无害化的，可在生产环境安全运行；

渗透测试可能具有破坏性，一般在受控环境或非生产环境进行。BAS 降低了对用户进行攻击模拟的专业技能要求；渗透测试则高度依赖于渗透测试人员的丰富技能。

渗透测试虽是长期以来常用的系统安全性评估工具，但其周期性特点、人工操作依赖、高昂成本，导致只能提供特定时间点的安全快照，难以持续反映不断变化的安全性，且验证范围受限于渗透测试人员的能力和时间，难以全面覆盖所有潜在攻击路径，还可能对生产环境造成不可控影响。

BAS 是渗透测试的有效补充和延伸，而非完全替代。渗透测试可作为 BAS 前的预检工具，发现显著业务风险，提高 BAS 验证的精准度和业务关联性；亦可在渗透测试后，利用 BAS 持续验证修复效果。二者结合，能形成更全面、高效的安全验证体系。

2）与漏洞扫描的区别

漏洞扫描主要识别已知漏洞的存在，基于漏洞库进行比对；BAS 则模拟真实的攻击行为，验证漏洞在实际环境中的可利用性以及攻击者能否利用该漏洞形成攻击链。漏洞扫描处于发现阶段，输出漏洞列表；BAS 则处于验证阶段，回答能否被利用和防护是否有效的问题。漏洞扫描是单点检测；BAS 能够模拟多阶段攻击，分析攻击路径。

漏洞扫描是攻击面管理和漏洞管理的基础，BAS 可作为漏洞扫描结果的验证器，借助 BAS 帮助组织优先修复那些真正可被利用的高危漏洞。

漏洞扫描已较为成熟，具备较高自动化能力，可识别已知漏洞，但无法验证漏洞在真实环境中的可利用性，也不能模拟攻击者利用漏洞后的多阶段攻击行为，输出的漏洞报告数量庞大，难以有效优先级排序。漏洞评估工具主要检查系统中是否存在已发布和已知的漏洞，但核心缺陷在于无法验证这类漏洞在实际生产环境中的可利用性，不能全面评估攻击者利用漏洞后可能经历的多个攻击阶段，存在知识库依赖性，无法全面覆盖所有潜在安全威胁，易造成资源浪费且不能为企业提供完整攻击链防护建议。

3）与攻防演练或红队测试的区别

红队测试通常需要高水平的专业人员组成红队，对人员的依赖程度极高；BAS 对人员依赖程度较低，主要依靠自动化系统执行。红队测试主要针对业务系统进行攻击测试；BAS 更侧重于验证防护安全产品及策略的有效性。红队测试的范围相对较窄，主要集中在特定的攻击路径和目标上；BAS 可以模拟多种攻击场景，测试范围更广，能够发现潜在的安全漏洞和风险。红队测试通常是一次性的活动，持续时间较短；BAS 可以持续不断地进行测试，及时发现新的安全威胁。红队测试的成本较高，需要投入大量的人力和时间；BAS 的成本相对较低，可以实现自动化的测试和监控。

BAS 和红队测试可以相互补充。在红队测试之前，可以使用 BAS 进行初步的安全评估，为红队测试提供参考；在红队测试之后，可以利用 BAS 对发现的问题进行持续监测和验证。同时，BAS 在日常的安

全监测中也可以模拟红队测试中的常见攻击手法，提高企业的安全防护能力。

红队测试具有较高的可靠性，能够真实地反映攻击者的行为和能力；BAS 虽然也可以模拟攻击行为，但在某些情况下可能会出现误报或漏报的情况。

2.2BAS 价值体现和必要性

BAS 不再是可选选项，而是企业和政府构建高效、可靠的网络安全防护体系的必要组成部分，是实现主动安全治理和应对未来威胁的关键基石。组织应高度重视 BAS 的应用和推广，充分发挥其价值，以提升自身的网络安全防护能力和运营效率，保障业务的持续稳定发展。



BAS 价值体现和必要性

2.2.1BAS 的核心价值

入侵与攻击模拟（BAS）的价值在于其能够提供传统安全测试方法无法提供的持续、自动化、确定的安全漏洞检测，从而显著提升组织的安全防护能力和运营效率。

1）持续验证安全控制有效性

传统安全产品部署后，其有效性容易因配置错误、策略老化或环境变化而下降。而 BAS 克服了传统渗透测试和漏洞扫描的局限性。能够持续、自动化地模拟攻击，验证防火墙、IDS、EDR、WAF 等各类安全产品的配置是否正确、是否按预期工作，及时发现防护盲点和薄弱环节。确保了安全投资能够真正产生预期的防护效果，使组织在不断变化的网络环境中始终保持高度的安全保障。

2）确定安全风险与实现量化评估

BAS 将抽象的安全风险和防护能力转化为可量化的指标，是组织量化安全评估框架的基石。提供数据驱动的洞察，揭示在独特的环境中，已识别的暴露面被攻击者实际利用的可能性。通过攻击成功率、漏洞利用成功率、检测率、阻断率、平均检测时间（MTTD）和平均响应时间（MTTR）等判断指标，BAS 能够精准洞察防护能力画像。种判断能力对于高层管理人员汇报安全绩效、证明安全投资回报率（ROI）至关重要，帮助决策者清晰了解组织的安全状况，为制定合理的安全战略提供有力依据。

3）促进风险主动治理

BAS 推动网络安全从被动响应向主动防护的根本性转变。使组织能够主动评估其安全预警，在攻击者利用暴露的事先识别并解决问题，从而实现现实风险的前置管理。通过持续监测和反馈，BAS 帮助企业发现潜在威胁，并提供可落地的缓解和修复建议，从而构建主动防护能力。不仅有助于防范安全事件的发生，还能降低安全事件对组织造成的损失和影响，保障业务的连续性和稳定性。

4）提升安全运营效率

BAS 的自动化功能显著减少了人工安全测试的成本和时间，将安全团队从繁琐的重复性任务中解放出来，能够专注于威胁狩猎、事件响应和战略性安全改进。自动化评估、攻击场景编排和日志闭环验证，极大提升了安全运营的自动化水平和协同效率。同时，BAS 可以辅助攻防演练，提升 SOC 团队的检测和响应能力，使安全团队能够更迅速、更有效地应对各类安全威胁，提高整体安全运营的效能。

5）提供满足合规要求的数据

BAS 能够提供证明安全控制措施实际效果的数据，是满足迫切严格的合规性要求（如国家等保 2.0、关键信息基础设施保护条例）的关键组成部分。帮助组织确保其安全措施持续符合法规要求，弥补仅遵循合规清单可能产生的盲点，降低潜在的法律和合规风险。在日益严格的监管环境下，BAS 为组织提供了合规保障，避免因合规问题而面临的处罚和声誉损失。

6）优化安全投资

BAS 能够准确评估不同安全控制解决方案的价值，帮助企业确定资金的最佳投入方向，从而证明安全投资的有效性。通过识别安全工具的优势或安全能力的不足，BAS 可以优化资源配置，确保安全投入能够产生最大的业务价值。有助于组织合理规划安全预算，避免资源浪费，实现安全投资的效益最大化。

2.2.2 应对网络安全挑战的必要性

在当今复杂的网络安全形势下，BAS 不再是可选选项，而是企业和政府构建高效、可靠的网络安全防护体系的必要组成部分，是实现主动安全治理和应对未来威胁的关键基石。

1）应对高级持续性威胁的紧迫性

现代网络攻击（如高级持续性威胁 APT、勒索软件、供应链攻击）呈现出高度复杂、聚焦和集中的特点。传统安全防护和验证手段难以有效应对动态演变的威胁。BAS 能够真实模仿攻击者格局、技术和程序（TTPs），主动发现并矫正防护盲点，帮助组织在实战中保持领先，有效抵御国家级网络战攻击。在复杂的网络威胁环境下，BAS 为组织提供了应对高级持续性威胁的有力武器，增强了组织的网络安全防护能力。

2）满足组织迫切的合规要求

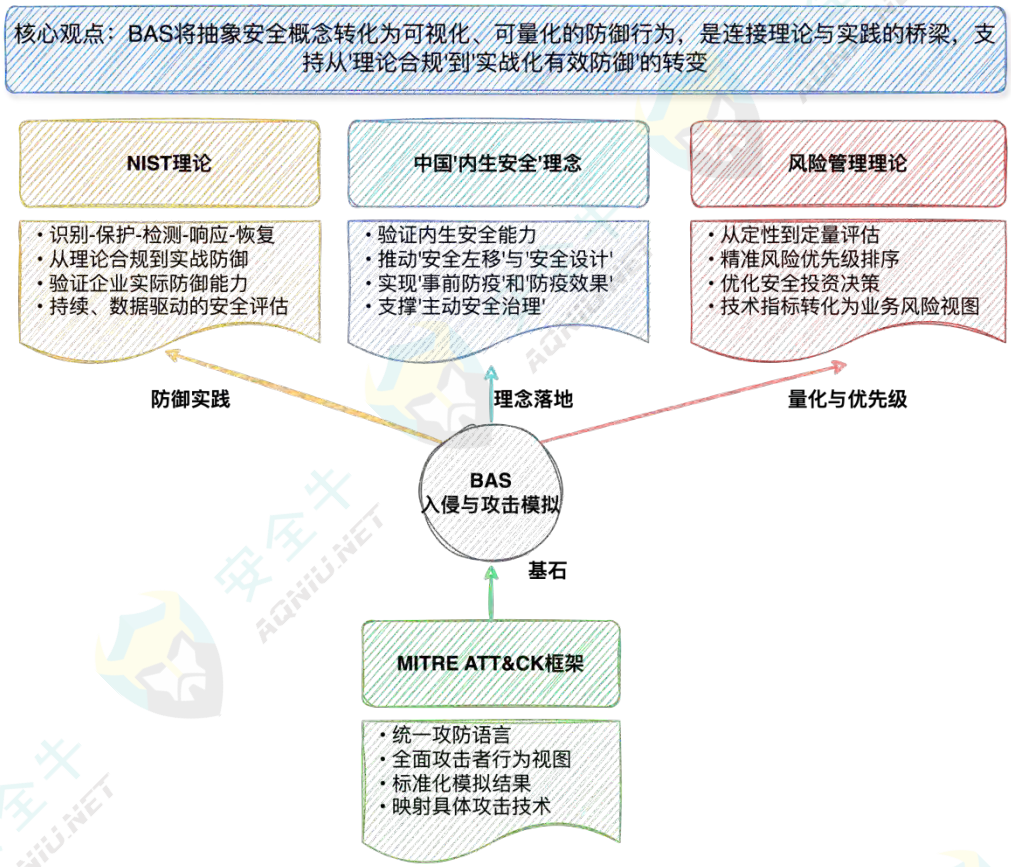
国家的网络安全法律法规对企业体系提出了明确的安全保护义务和持续验证要求。特别是在国家攻防演练常态化的背景下，组织需要具备实战级的防护能力，并提供可量化的合规证据。BAS 能够提供持续的、量化的、符合 ATT&CK 框架的验证数据，支撑组织满足法规要求，并降低潜在的法律和合规风险。使组织能够在合法合规的框架内开展业务活动，避免因合规问题而带来的不利影响。

3）提升安全投入回报率

大多组织配置了各种安全产品和控制措施，但往往不确定这些投资是否真正有效。BAS 通过提供量化的安全绩效指标，能够有效展示安全投资的实际效果，帮助组织进行科学的预算分配，优化资源配置，从而提高安全投入的投资回报率，将安全投入的成本支出转变为可量化的业务价值。帮助组织在有限的预算内实现安全效益的最大化，提升组织的整体运营效益。

2.3BAS 与安全框架的关联

入侵与攻击模拟（BAS）的理念和实践并非凭空，而是将抽象安全概念转化为可视化、可量化的防护行为，是连接理论与实践的桥梁，支持从理论合规到实战化有效防护的转变。该理论为 BAS 实践提供了指导框架、评估标准和技术方向，使 BAS 能够有效地抽象的安全概念转化为可视化、可量化的防护行为。



BAS 与安全框架的关联

2.3.1MITREATT&CK 框架是 BAS 的基石

MITREATT&CK 框架是基于真实世界观察的对抗性和策略知识库，包括攻击者的策略（如初始访问、横向移动）和技术（如漏洞利用、路径访问），提供了一个统一的语言和全面的攻击者行为视图。MITREATT&CK 框架作为 BAS 攻击模拟的基石，起到其在统一语言和评估中的作用。

一方面，MITREATT&CK 框架可以确保 BAS 模拟的全面性和标准化，使模拟结果能够清晰地映射到具体的攻击技术，从而深化安全团队对攻击的理解并优化响应流程。BAS 平台广泛采用 ATT&CK 框架来组织和映射攻击模拟场景，将理论的攻击者可能做的事转化为自动化、执行的模拟行为。例如，理论的横向移动规定，在实践中通过 BAS 模拟一系列基于 ATT&CK 的技术的安全技术验证平台产品，如获取权限－远程执行－扫描内网开放端口，确保 BAS 模拟的全面性和标准化，从而能够高保真地还原真实攻击场景。

另一方面，BAS 利用 MITREATT&CK 框架将复杂的攻击行为转化为可简化、可改进的防护指标。BAS 的评估报告通常会以 ATT&CK 矩阵的形式呈现防护覆盖率和检测效果。使团队、舰队以及不同厂商的安全产品之间，能够使用统一的语言来理解和沟通安全态势，并明确指出组织在哪些攻击区域或技术存在防护缺陷，从而指导有边界的策略调整和优化。

2.3.2NIST 理论是 BAS 的防护实践理论

NIST 网络安全框架（NISTCSF）提供了一套自主性的指导原则，旨在帮助组织管理和降低网络安全风险。包含识别、保护、检测、响应、恢复五大核心功能，是涵盖安全风险管理全生命周期的框架。NIST 强调组织需要持续评估其安全风险和应对能力。

BAS 是验证 CSF 理论在企业环境中落地效果的关键手段，将抽象的理论转化为可量化的实践效果，帮助企业实现从理论合规到实战化有效防护，并遵循 NIST 应持续的、数据驱动的原则。BAS 通过模拟攻击者行为，验证企业在 NIST 的检测（如安全信息和事件管理系统 SIEM、扩展检测与响应 XDR 的能力）和响应（如自动化响应流程、事件处理时间）功能上的实际能力。其发现的漏洞和防护缺陷直接指导保护功能的改进和优化，确保安全控制真正有效。

BAS 也可以推动组织提高 NISTCSF 成熟度的关键工具。通过 BAS 验证现有防护措施的有效性，指导安全策略和控制措施的优化，提升保护能力、通过模拟攻击，验证安全监控系统（如 SIEM、XDR）的检测能力和告警的准确性，提升威胁检测效率、并可模拟事件发生，测试事件响应流程和团队响应时间，提升响应效率和恢复能力。

2.3.3BAS 支撑风险管理理论的量化和优先级排序

风险管理理论关注风险的识别、分析、评估、处罚和监控。将风险划分为威胁事件发生频率和事件造成的损失程度等因素，以量化评估网络风险。而传统的风险评估方法难以精确的风险的真实影响，也难以支持基于成本实现的安全投资决策。BAS 不同于传统漏洞扫描基于 CVSS 评分，可结合漏洞在实际环境中的可利用性、资产的业务关键性以及已部署部分措施的效果。

BAS 通过持续模拟特定攻击计算场景，提示在当前防护下特定类型攻击成功的概率或频率，作为威胁事件频率和漏洞可利用性数据的重要来源，将风险管理从定性推向定量评估，帮助企业提供更精准的风险观点和优先级排序，从而优化安全投资决策，提升安全在企业战略层面沟通的效果。

并且，BAS 提供洞察的风险解析报告，将攻击成功率、暴露面等技术指标转化为业务可理解的风险视图，结合业务资产价值，提示潜在损失。使安全风险从定性方向定量评估，安全投资决策更加数据驱动，提升了安全在企业战略领域的话语权。

2.3.4BAS 契合和支持国家内生安全理念的落地

内生安全理论是我国独创的网络安全理论，旨在解决网络空间中普遍存在的未知威胁和系统固有的安全问题。强调其网络安全防护不应依赖于外部的安全产品，应从系统设计之初就通过动态、偶发、危机等机制，使系统具备自适应、自恢复、自防护的能力，从而构建高可靠、高可信、高可用的安全体系。将安

全植根到业务系统能力，实现事前防疫和防疫效果的统一。BAS 理念与内生安全理念高度契合，可以帮助企业将安全能力植根于业务系统中，实现事前防疫和防疫效果的统一，构建真正自主性、韧性的网络安全防护体系，是实现内生安全的重要实践路径，能够有效支撑国家特色理论的落地。

- 验证内生安全能力：BAS 通过持续面部模拟攻击，可以验证系统在各种攻击时（包括已知的 APT 组织的 TTP 和模拟的未知威胁）的免疫性和自适应性。能够评估内生安全机制的实际防护效果，提供量化数据，证明系统真正具备免疫能力。
- 推动安全左移与安全设计：内生安全强调安全外壳设计。BAS 可以支持在软件开发生命周期的早期阶段集成安全测试，持续验证代码和架构中的安全缺陷，将安全问题解决在成本最低的阶段，从而从源头上提升系统的内生安全性。
- 实现事前防疫和防疫效果：BAS 的以攻促防理念与境内生安全的事前防疫不谋而合。通过常态化的攻击模拟，BAS 能够帮助企业在威胁真正到来发现并补足防护短板，将安全关口前移。其量化评估能力则直接体现了防疫效果，使安全保卫的价值可被逐步实现，推动安全建设从有前向好不好转变。
- 支撑主动安全治理：内生安全主动治理。BAS 作为主动验证工具，能够持续提供风险安全洞察和防护反馈，赋能底层主动识别、评估和处置风险，从而实现风险前移、主动防护的战略目标，而不是被动响应。

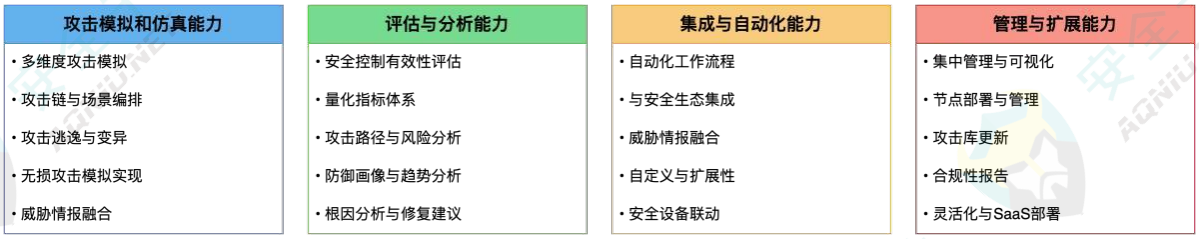
第三章 BAS 的能力框架和关键技术

入侵与攻击模拟（BAS）作为新一代安全验证工具，在企业整体安全能力建设中扮演着基石性的角色，能够提升组织在不同安全成熟度模型下的水平，并形成一套涵盖攻击模拟、评估分析、集成自动化及管理扩展的综合能力框架。

3.1BAS 的能力框架

3.1.1BAS 能力框架的构成

一个完整的 BAS 能力框架主要由攻击模拟和仿真能力、评估与分析能力、集成与自动化能力以及管理与扩展能力等核心要素构成。这些能力要素相互协作，共同赋予 BAS 强大的攻击模拟、评估分析、集成自动化及管理扩展功能，使其能够有效支持企业的网络安全防护工作。



BAS 能力框架

1）攻击模拟和仿真能力

攻击模拟和仿真能力是 BAS 的关键组成部分，涵盖了攻击样本库、威胁情报、攻击手法库以及 TTPs 编辑引擎等内容。其中，攻击手法库广泛覆盖了 APT 攻击、勒索软件攻击、Web 攻击、社会工程攻击等多种常见网络攻击类型。通过多维度攻击模拟功能，BAS 能够针对网络、端点、Web 应用、邮件、域、容器、工控系统以及数据等不同攻击面的攻击行为进行精准模拟，旨在全面评估企业安全防护体系在面对各类攻击时的应对能力。同时，BAS 支持攻击链与场景编排，能够将单个攻击行为组合成多级攻击链，例如基于 KillChain 或 ATT&CK 模型，模拟出如 APT 组织攻击、勒索攻击病毒传播以及内部横向移动等复杂攻击场景，并允许用户根据自身需求进行自定义编排，此外，BAS 具备攻击逃逸与变异能力，能够模拟诸如流量交互、分块传输、加密等攻击逃逸技术，并借助 AI 自动生成变异攻击，以此来测试防护系统对于新型或未知攻击的能力，BAS 还采用无害化流量模拟实现技术，通过沙箱隔离、标记、虚拟靶机、仿真接收端或灭活样本等手段，避免模拟攻击对企业的生产环境造成任何损害，以保障攻击模拟的安全性。

2）评估与分析能力

评估与分析能力以评估分析引擎、数据采集与日志关联为核心要素。在安全控制漏洞评估方面，BAS 可实时检测和评估各类安全产品，包括 WAF、FW、IPS、EDR、DLP 等的防护和检测能力、策略覆盖度以及稳定性。同时，BAS 能够构建量化指标体系（具体内容暂未详细阐述），帮助量化评估企业安全状况。攻击路径与风险分析功能使得 BAS 可以自动识别并可视化攻击路径，精准定位关键攻击点，评估攻击面的潜在影响，并结合业务属性对风险进行量化分析。防护画像与趋势分析功能则生成企业整体防护能力画像，提供包括检出率、爆发率、MTTD（平均检测时间）、MTTR（平均修复时间）等量化指标，并对安全形势变化趋势进行分析，助力企业及时发现安全威胁。此外，BAS 还具备根因分析与修复建议功能，能够深入分析攻击失败的根本原因，并为企业提供切实可行的修复建议和优化方案。

3）集成与自动化能力

BAS 的价值很大程度上取决于其与企业现有安全生态系统的集成能力，实现数据共享、流程互补和自动化。

集成与自动化能力是 BAS 价值实现的重要方面。BAS 与企业现有安全生态系统的集成能力至关重要，能够实现数据共享、流程互补以及自动化响应。

BAS 可与 SIEM/SOC/XDR 联动，通过与 SIEM/XDR 的集成，帮助企业发现安全运营中的盲点，优化检测流程降低，全局平均检测时间（MTTD）。借助模拟攻击，BAS 能够验证 SIEM/XDR 平台中的检测规则是否能有效识别威胁，并将模拟攻击的日志注入 SIEM/XDR，测试其关联分析和威胁危害的准确性。同时，BAS 的攻击模拟结果和威胁情报可以反哺 SIEM/XDR，帮助优化相关规则，减少误报和漏报，提升威胁检测的精准度。

与 SOAR 联动则可实现自动化的闭环响应。SOAR 接收 BAS 的验证结果后，能够自动化执行修复流程，形成从问题发现到响应、验证和修复的完整闭环管理。当 BAS 模拟攻击触发安全响应后，SOAR 平台可自动执行一系列基线响应动作，如自动封禁攻击源 IP、隔离受感染主机、发送通知等，而 BAS 则可对响应的效果和及时性进行验证。

此外，BAS 与 ASM（攻击面管理）的联动能够实现攻击面精准验证和风险可视化。一方面，BAS 可利用 ASM 提供的企业 IT 资产外部和内部暴露面信息、潜在漏洞数据等发现结果，对识别出的攻击面和漏洞进行精准的攻击模拟和验证，确认其真实可利用性，并根据攻击路径进行优先级排序；另一方面，结合 ASM 的攻击面视图和 BAS 的攻击路径分析，能够更全面地可视化企业的风险暴露状况。

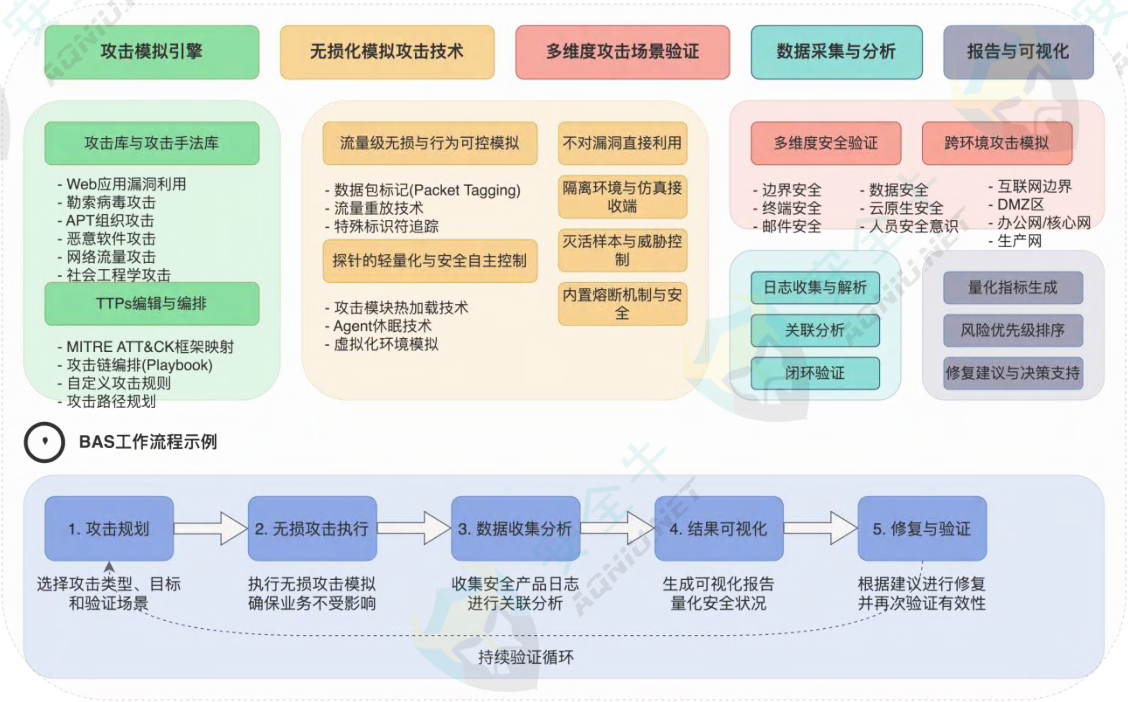
4）管理与扩展能力

管理与扩展能力为 BAS 的高效运作提供了有力支持。集中管理与可视化功能通过提供统一的 Web 管

理界面和仪表盘，使企业能够可视化展示安全压力、任务执行、评估结果等关键信息，并支持多角色视图，满足不同用户角色的查看和管理需求。节点部署与管理方面，BAS 支持攻击节点和目标节点（机器人/Agent）的灵活部署，包括本地、云端、SaaS 等多种部署方式，同时具备跨网络、跨硬件形态的兼容性管理能力。攻击库更新功能确保 BAS 提供持续更新的攻击库，使其能够与最新出现的攻击手段以及 APT 组织 TTP（战术、技术与程序）保持同步更新。在合规性报告方面，BAS 支持生成符合等保、关保等标准要求的报告，帮助企业满足相关法规的合规要求。同时，BAS 还具备原生化与 SaaS 部署能力，能够灵活满足大型企业对于原生化部署以及中小型企业对于 SaaS 化部署的需求。此外，BAS 还涵盖知识库管理功能以及安全和轻量化设计，进一步提升其管理与扩展的效能。

3.2 关键技术

BAS 的关键技术以攻击模拟引擎为核心，通过无害化化模拟攻击技术确保在不影响业务的前提下进行安全验证，通过多维度攻击场景验证能模拟各种安全维度和环境的攻击，并利用数据采集与分析对模拟过程中的数据进行高效处理和可视化展示，最后通过报告支持则将数据转化为可操作的洞察，提供量化指标、风险排序和修复建议，辅助安全决策。



BAS 的关键技术

3.2.1 攻击模拟引擎

攻击模拟引擎是 BAS 产品的核心中枢，主要承担攻击的生成与执行任务，确保攻击模拟具备真实性、多样性以及可控性等关键特性。

1）攻击库与攻击手法库

BAS 系统内置并持续更新海量的攻击载荷及攻击库。攻击库的来源广泛，包括最新威胁情报、APT 组织攻击报告、实战攻防经验、CVE 漏洞分析以及恶意样本研究等。库中涵盖了多种攻击类型，例如 Web 应用漏洞利用（如 SQL 注入、XSS、Webshell 等）、勒索病毒攻击（包括勒索全链条、加密行为等）、APT 组织攻击（如钓鱼邮件投递、恶意文件传播、命令与控制 C2、持久化驻留等）、恶意软件攻击（如后门、木马、挖矿程序等）、网络流量攻击以及社会工程学攻击（如钓鱼邮件、钓鱼网站）等。

部分国内领先的厂商，将 AI、机器学习以及大型语言模型技术应用于攻击载荷和手法库的生成过程。借助这些先进技术，实现攻击的智能化、变异以及动态适应能力，使得攻击模拟更具真实性和未知性，能够有效测试防护系统对于新型或变种攻击的抵御能力。

2）TTPs（战术、技术和过程）编辑与编排

目前，多数 BAS 产品以 MITREATT&CK 框架为基石，对攻击者的策略、技术和程序进行组织与映射。这种基于框架的标准化方式，为攻击模拟提供了统一且规范的语言和格式化方法。

在攻击链编排方面，可将单一攻击行为整合成多阶段的攻击链，即 Playbook，精准模拟复杂且真实的 APT 攻击路径，例如从最初的入侵访问直至数据渗出的完整杀伤链。

同时，用户能够依据自身业务环境特点以及最新威胁情报，自定义攻击规则和测试示例，实现全面且有针对性的安全验证。此外，攻击模拟引擎支持用户对 TTP 进行灵活地编辑和编排，构建契合特定安全测试需求的攻击场景。具体而言：

部分国内领先厂商的 BAS 系统能够基于对目标网络拓扑的自动分析并规划所有可行的攻击路径，通常运用攻击图理论进行建模。并且，依据攻击执行结果以及目标环境的动态变化，实时动态调整攻击路径和攻击手段，从而更为逼真地模拟攻击者的行为逻辑。

3.2.2 无害化化模拟攻击技术

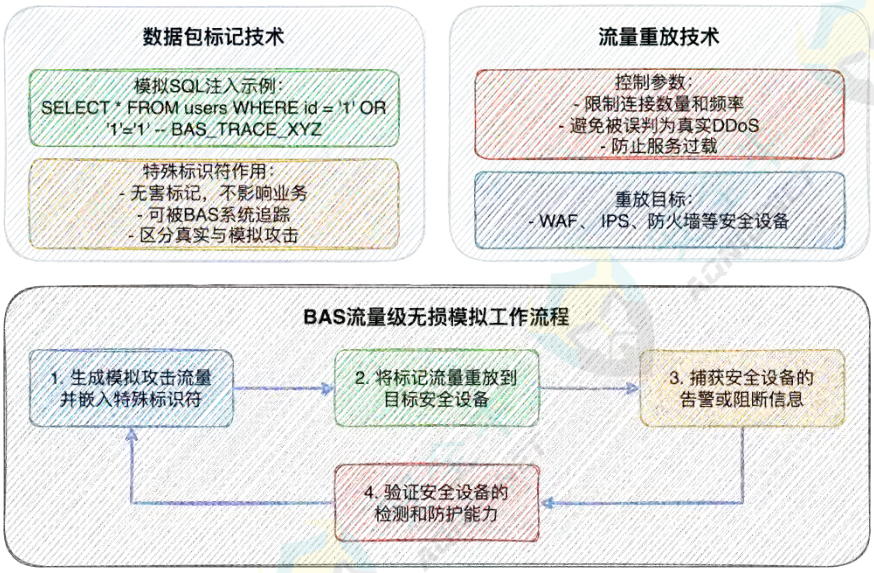
国内 BAS 厂商在实现无害化化模拟攻击方面，采取了多管齐下、创新并举的技术路线，共同构筑了安全可靠的验证环境，确保了攻击模拟过程既能有效验证安全防御能力，又不会对企业正常业务造成任何负面影响。



BAS 的无害化化模拟攻击技术

1）流量级无害化与行为可控模拟：通过数据包标记与行为精巧重构

BAS 产品通过数据包标记（PacketTagging）与流量重放技术，能够在不改变原有网络拓扑和不实际部署额外攻击设备的前提下，精确控制和追踪模拟攻击流量。其核心原理是，在生成的模拟攻击数据包中，系统会巧妙地嵌入特殊的的标识符，给模拟攻击流量打上一个独特的指纹。



BAS 的行为模拟

例如，在模拟 SQL 注入攻击时，BAS 系统并不会发送真正会破坏数据库的恶意代码。例如，在看似正常的 SQL 查询语句中，嵌入一个独特的、可被追踪的注释或参数值，如 SELECT * FROM users WHERE id = '1' OR '1'='1' --BAS_TRACE_XYZ。这里的-- BAS_TRACE_XYZ 就是无害的标记，对数据库执行无影响，

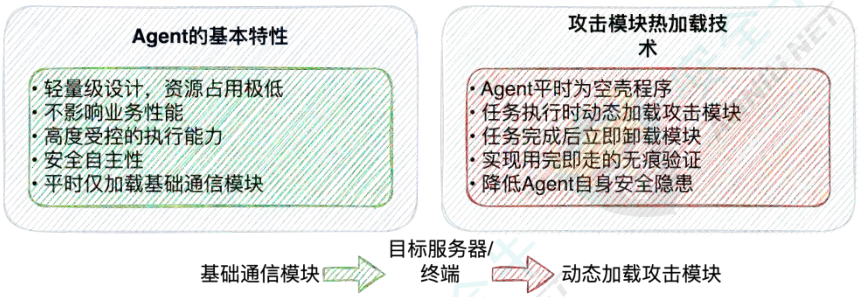
但能被 BAS 追踪。接着，BAS 系统会将带有这些特殊标识符的模拟攻击流量重放到目标网络中经过的安全设备（如 WAF、IPS、防火墙），这些安全设备会像对待真实攻击一样对其进行检测和阻断。如果设备识别到了攻击行为，BAS 的监控模块便会捕获其告警或阻断信息，以此来验证安全设备是否具有检测这个攻击的能力。类似地，在模拟网络端口扫描时，BAS 会发送探测报文，但会限制连接数量和频率，并通过标记区分，避免被误判为真实 DDoS 攻击或造成目标服务过载。这种技术实现了在不实际触发漏洞利用、不真实修改系统状态的前提下，对安全设备检测能力的精准验证。有厂商通过此方式，在模拟真实攻击效果的同时，避免对生产环境造成任何负面影响，保障业务连续性。

厂商案例

- 长亭科技通过对业务的仿真能力，模拟各种业务环境（如 Web 服务器、数据库）的响应行为和特征，无需部署靶机，规避了部署真实靶机可能引入新业务或潜在漏洞的风险。
- 绿盟科技采用流量标记技术，如在模拟 SQL 注入等场景中，将攻击载荷自动替换为测试语句，确保了流量层面的无害化。
- 墨云科技采用流量重放和插入动态 ID 技术，在实现快速部署与模拟真实攻击效果不造成危害的同时，轻松区分模拟攻击流量和其他流量。

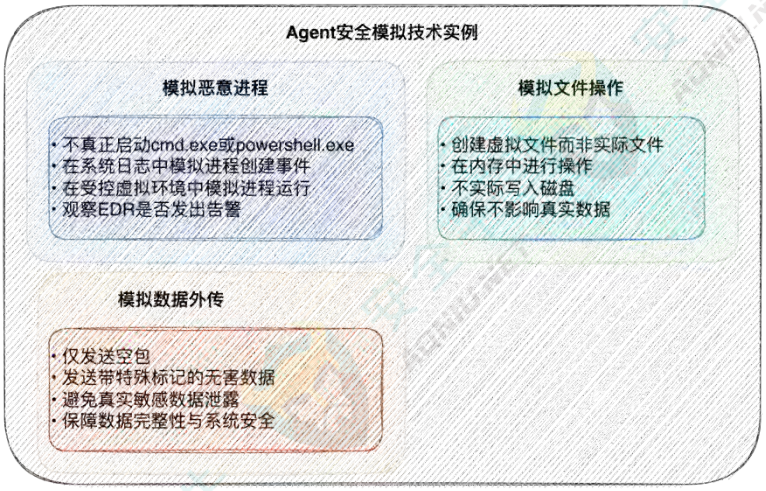
2）探针的轻量化与安全自主控制：Agent 端的“隐身”与“自愈”

BAS 通常需要在目标服务器或终端上部署轻量级的 Agent/探针，以模拟本地攻击行为。这些 Agent 对系统资源占用极低，确保不影响业务性能，并且具备高度受控的执行能力和安全自主性。



BAS 的轻量探针和热加载技术

攻击模块热加载技术核心原理是 Agent 平时只加载基础通信模块，就像一个“空壳”程序；仅在执行特定安全验证任务时，才会临时动态地加载相应的攻击或仿真模块，完成任务后这些模块会被立即卸载，降低了 Agent 自身可能存在的安全隐患，并避免了对生产环境的持续性干扰，实现了“用完即走”的无痕验证。另外，部分厂商采用 Agent 休眠技术，即 Agent 在没安全验证任务执行一段时间内自动进行休眠，而在被分配验证任务后由守护进程再次叫醒 Agent。



在模拟终端恶意行为时，例如模拟创建恶意进程，Agent 可能不会真正启动 cmd.exe 来执行 powershell.exe 并造成破坏，而是会在系统日志中模拟一个进程创建事件，或在受控的虚拟化环境中模拟进程的运行，并观察 EDR（终端检测与响应）软件是否发出告警。再如，模拟文件修改或创建，Agent 只会创建虚拟文件或在内存中进行操作，而不会实际写入磁盘，确保不对真实数据造成任何影响。同时，Agent 在模拟数据外传时，也仅发送空包或带有特殊标记的无害数据，避免真实敏感数据泄露，从而保障了数据完整性与系统安全。

厂商案例

- 华云安采用攻击模块热加载技术，其探针仅在执行安全验证任务时临时加载攻击和仿真模块，任务完成后立即卸载，大幅降低了资源占用，并避免了探针自身可能存在的安全隐患。这种设计实现了用完即走的无痕验证。
- 塞讯科技采用 Agent 休眠技术，其 Agent 在没安全验证任务执行一段时间内自动进行休眠，在被分配验证任务后由守护进程再次叫醒 Agent 进行攻作，这种设计降低了资源占用。
- 矢安科技采用攻击模块热加载技术，Agent 在没有安全验证任务执行时处于休眠状态，当被分配到任务时被唤醒执行相关安全验证任务，并且任务执行完成后 Agent 将自动还原清理执行痕迹，降低了资源占用与潜在的风险隐患。

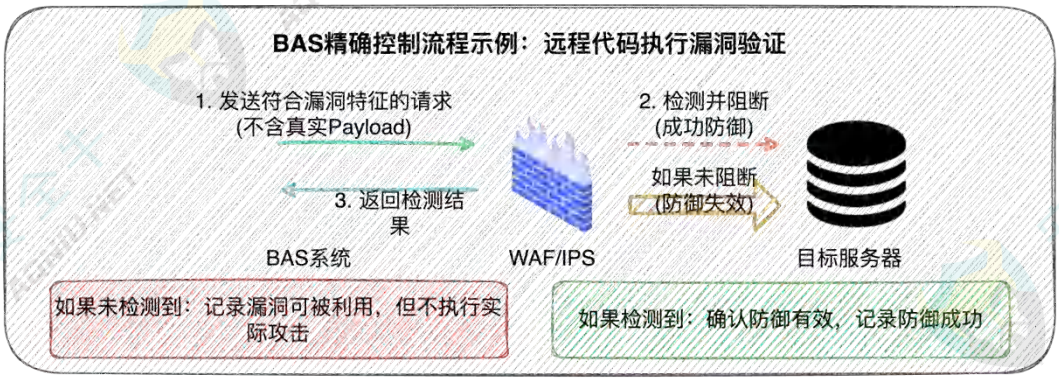
3）不对漏洞直接利用

不对漏洞进行直接利用是 BAS 与传统自动化渗透测试的核心区别，仅模拟攻击者尝试利用漏洞的行为（如发送特定格式的请求），但不会实际触发漏洞并侵入系统或修改目标数据，确保了验证的安全性。



不对漏洞直接利用

BAS 发送的请求仅仅是到触发安全设备检测的程度，这种精确控制，确保了在评估防御能力的同时，不为攻击者留下任何可乘之机。



BAS 精准控制

例如，对于一个已知的远程代码执行漏洞，BAS 会发送符合该漏洞触发特征的请求，但不会包含真正执行恶意命令的 Payload。发送后观察 WAF 或 IPS 是否能检测到此请求并进行阻断。如果防御设备未能检测到，BAS 仅会记录该漏洞可被利用，但不会发送真正能获取系统控制权或执行恶意操作的 Payload。这种精确控制可以探虚实，但不会伤筋骨，避免在生产环境中制造新的安全风险或留下可乘之机。部分领先的 BAS 产品采用专利技术实现这一点，通过特定的攻击向量、评估机制和算法，对业务进行无害化伤的风险评估。

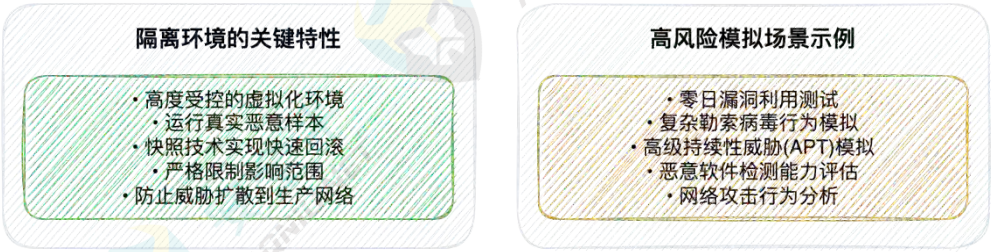
厂商案例

- 灰度安全不对漏洞直接利用，也不依赖实际生产设备作为落点渗透，而是通过特定的攻击向量、评估机制和算法，对业务进行无害化伤的风险评估，从而保障了验证过程的安全性。
- 塞讯科技实现不对漏洞直接利用，通过仅发送符合该漏洞触发特征的请求，对真实对外暴露业务的目标 URL 的防护检查与防护力验证。

- 矢安科技通过技术手段最大程度保留了漏洞利用的特征，在攻击模拟时实现了仅让安全设备对漏洞利用做出回应，后端的目标系统并不会真实响应。该技术手段让安全验证更彻底、更安全。

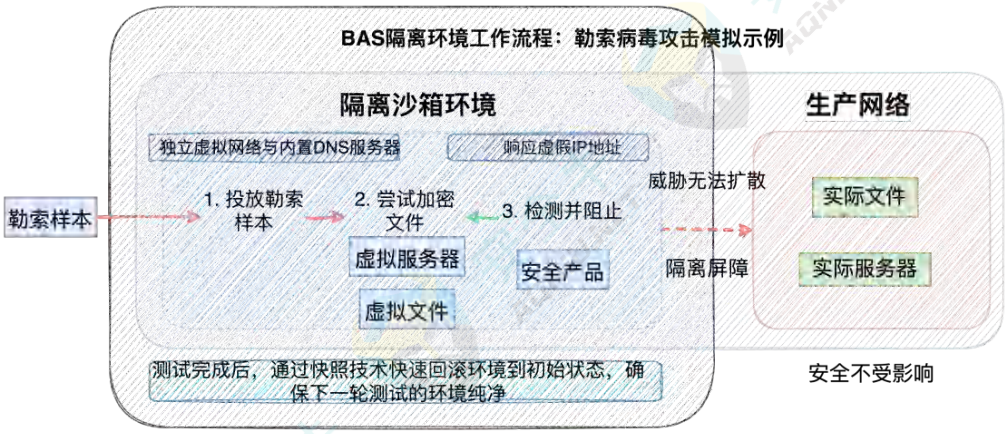
4）隔离环境与仿真接收端：高风险模拟的“安全气泡”与“虚拟替身”

为了安全模拟一些高风险或难以在生产直接执行的攻击行为（如零日漏洞利用、复杂勒索病毒行为），利用沙箱隔离技术，实现运行真实的恶意样本，测试安全产品的检测能力，确保任何恶意行为的影响范围被严格限制，不扩散到生产网络。



BAS 隔离环境

其工作原理是在一个高度受控的、虚拟化环境中，BAS 运行真实的恶意样本，测试安全设备的检测能力，并在测试完成后通过快照技术（对虚拟机状态的即时备份）快速回滚环境到初始状态，确保任何恶意行为的影响范围被严格限制在隔离区内，不扩散到生产网络。例如，在模拟勒索病毒攻击时，BAS 会在一个与生产环境完全隔离的沙箱中投放勒索样本，观察其是否能成功加密沙箱内的虚拟文件，以及终端安全产品是否能及时检测并阻止，而不会对生产系统造成任何实际加密。某些厂商的“受保护的沙盘”组件，拥有独立的虚拟网络和内置 DNS 服务器（响应虚假 IP 地址），能够隔离恶意软件的网络连接，阻止其真实外联。



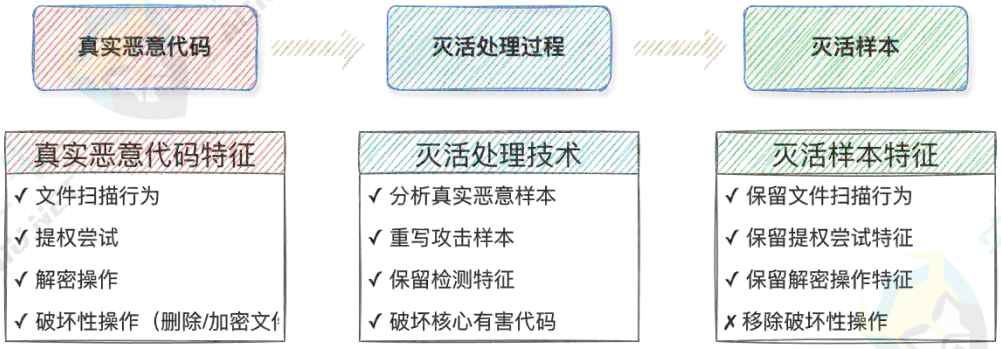
BAS 隔离环境工作原理

厂商案例

- 绿盟科技采用沙箱隔离技术，可以在沙箱中进行攻击模拟，确保真实资产无需感知系统检测分析过程，实现零侵入。
- 塞讯科技即采用受保护的沙盘，具有独立的虚拟网络和内置 DNS 服务器（响应虚假 IP 地址），能够隔离网络连接，并在运行恶意样本前后自动创建操作系统镜像的快照并回滚，确保实际环境不被感染。

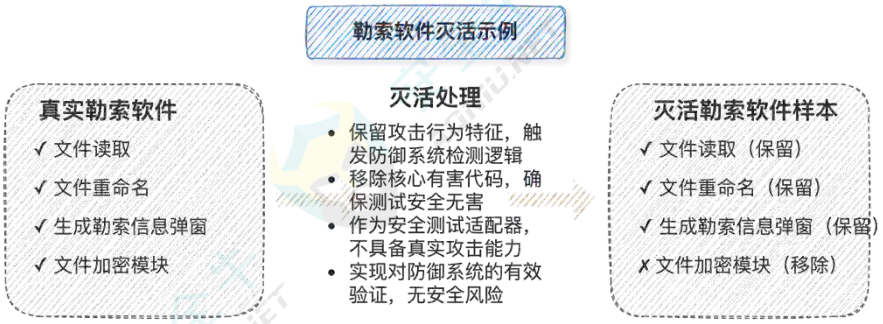
5）“灭活”样本与威胁控制：让“毒药”变“试剂”

“灭活”样本与威胁控制：对于涉及恶意代码的模拟，厂商会采用特定的技术手段确保其无害化。针对涉及恶意代码的模拟，BAS 厂商会采用特定的技术手段确保其无害化，这使得 BAS 能够安全地测试防御系统对病毒、木马、勒索软件等恶意代码的检测和阻断能力。



BAS 灭活技术

厂商通过分析真实的恶意修改样本，进行重写攻击样本处理，保留攻击行为特征（如文件扫描、提权尝试、解密等触发检测的关键模式）的同时，彻底破坏了其核心的有害代码和破坏性操作（如删除文件、加密硬盘、建立真实通信隧道等）由此产生的“灭活”病毒样本，仅作为安全测试适配器，只为触发防御系统的检测逻辑，不具备真实的攻击能力。



BAS 灭活示例

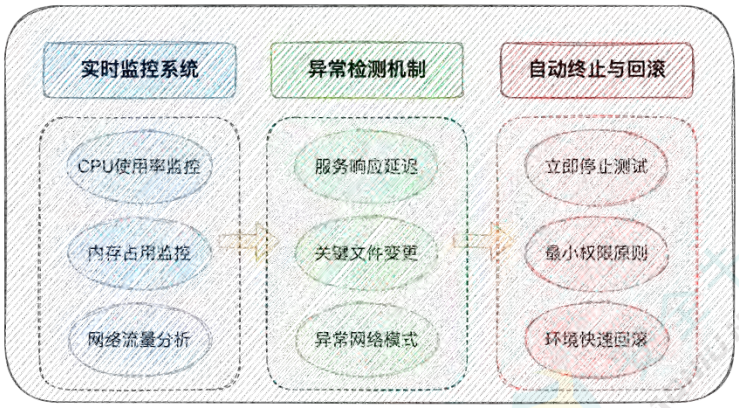
例如，在模拟一个勒索软件攻击时，灭活样本会模拟文件读取、重命名文件、生成勒索信息弹窗口等行为，但核心的加密模块会被删除，从而不会真实加密用户数据。去除不可控行为，例如不会激活运行病毒样本文件，只保留触发安全产品检测的特征，从而确保模拟的真实性和安全性。

厂商案例

- 塞讯科技对于无法部署沙盘环境的客户提供了无害化样本进行验证，也提供通过模拟恶意样本的行为实现检测，可在验证时不对部署环境造成影响。
- 矢安科技的攻鉴 BAS 产品在攻击样本处理时，通过分析真实恶意样本并重写攻击样本，在保留攻击特征的同时去除了危害性操作，从而得到了用于攻击的“灭活的病毒”样本。通过对样本的“灭活”不仅实现了从“毒药”变为“试剂”，更让“试剂”变的更可控，可用于各类验证场景。

6）内置熔断机制与安全：模拟攻击的“安全保险丝”

BAS 产品普遍内置自动化熔断机制作为安全防护的最后一道屏障，能够在模拟攻击出现风险时，立即自动终止测试任务，并将风险降至最低，这种机制构筑了最后一道防线。



BAS 熔断机制

BAS 系统在模拟攻击过程中会持续监控目标系统和网络的状态，通过实时监测系统资源（如 CPU、内存）的异常拓扑、服务响应延迟、关键文件突然变更、或异常网络流量模式等潜在信号，一旦检测到任何异常或超出预设安全阈值的情况，系统会立即自动终止测试任务，将风险降至最低。确保在极端或不可预见的情况下，能够迅速停止可能的影响，类似电路中的保险丝，在过载时自动切断。同时，BAS 系统在设计上会遵循最小权限原则，其通知和管理平台只需获取完成验证任务所需的最小权限，并提供完善的环境回滚机制，确保即使发生意外，也能快速环境到验证前的安全状态。

厂商案例

- 绿盟科技产品内置熔断机制，当模拟行为意外触发验证环境系统异常时（如 CPU 激增、服务响应延迟），会自动终止测试并回滚状态

3.2.3 多维度攻击场景验证：

BAS 支持针对不同安全维度和环境的攻击模拟，包括边界安全、终端安全、邮件安全、数据安全、云原生安全、人员安全意识进行多维度的验证，并且 BAS 能够模拟攻击者在不同网络区域（如互联网边界、DMZ 区、办公网、核心网、生产网、中继）之间的横向移动和攻击行为。并且支持跨安全产品类型（如 WAF、防火墙、IPS、EDR、NTA、DLP 等）的集中验证，评估不同安全产品在攻击过程中的协同防护效果。

例如通过模拟针对 Web 应用、网络安全产品（WAF、防火墙、IPS）的外部攻击，如 SQL 注入、XSS、DDoS、Webshell 上传，验证边界安全；通过模拟恶意文件执行、勒索病毒、后门入侵、提权、信息收集等，验证 EDR、HIDS 验证终端/主机安全等。

3.2.4 数据采集与分析

BAS 应对模拟过程中产生的大量数据进行高效地采集、分析和提供，从而提供有价值的洞察。

- 日志收集与解析。BAS 系统通过多种方式收集安全产品在模拟攻击过程中产生的日志和相关信息，包括 Syslog、API 接口对接或直接从 SIEM/SOC 平台获取日志。收集到的日志需要进行标准化解析和归一化处理，以便后续的统一分析。
- 关联分析。BAS 将模拟攻击的执行日志与安全产品生成的同类日志进行智能匹配和关联分析，以判断攻击是否被成功检测、爆发，以及是否触发了正确的对应或响应。部分厂商创新性地应用 AI 技术，实现对非契约安全日志的智能解析和关联分析，提升匹配的准确性和效率，有助于发现单点防护未触发但通过关联分析可识别的攻击链条。
- 闭环验证。BAS 通过日志闭环验证，确保攻击行为被安全产品识别并进而确认防护效果。
- 数据可视化。BAS 提供丰富、可分析的可视化仪表盘和报告，多维度展示安全威胁路径、防护效果和趋势。可视化内容包括攻击成功率、检测率、阻断率、ATT&CK 覆盖率、安全趋势、风险热力图、攻击路径图、相似时间线等，使安全状况一目了然，方便不同角色（如 CSO、安全运营人员）快速理解和决策。

3.2.5 报告与可视化

BAS 不仅提供原始数据，更重要的是能够将其转化为可操作的洞察，为安全决策提供科学依据。

- 量化指标生成。系统根据数据分析并生成量化指标，包括检测率、阻断率、穿透率、攻击成功率、漏洞利用成功率、爆发率、平均检测时间（MTTD）、平均响应时间（MTTR）、安全趋势、修复效率、ATT&CK 覆盖率等。这些指标使安全绩效可被量化，解决了传统安全评估难以量化的问题。
- 风险优先级排序。BAS 基于漏洞的实际可利用性、资产的业务关键性以及已部署部分控制措施的有效性，对发现的风险和漏洞进行优先级排序。这一功能使企业能够将有限的资源集中投入到最有影响且最易被利用的高风险点上，实现精准防护。
- 修复建议。BAS 系统会根据攻击模拟结果和分析洞察，提供详细的、可落地的修复建议和优化方案。这些建议通常包括安全产品策略调整、漏洞修复安装、配置优化、运营流程改进等，指导安全团队进行高效整改，形成发现－修复－验证的闭环。部分产品甚至能够提供修复建议，例如 AI 辅助生成优化策略。
- 决策支持。BAS 通过清晰、可量化、与业务分析相结合的报告，为安全管理人员和技术团队提供决策支持。能够将复杂的技术洞察转化为业务可理解的语言，帮助高层领导理解安全差距，推进安全投资的合理性，并制定长期安全战略。

3.3BAS 安全量化指标体系

在当今复杂多变的网络安全环境下，企业为安全建设投入了大量资源，然而如何加速这些投入的实际成效，如何彰显安全业务的真正价值和投资回报，始终是困扰安全负责人的一大难题。为了实现这一目标，企业需要针对安全业务的量化指标体系，形成具有说服力的评估结果。

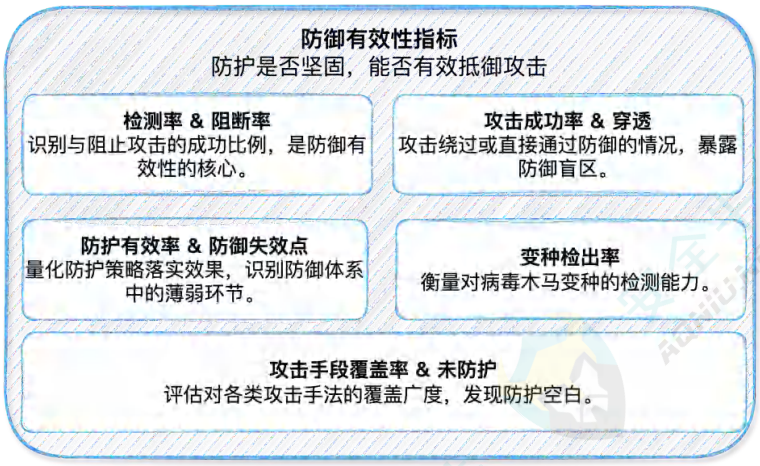
安全牛基于对网络安全实践的深刻理解、行业主流指标的借鉴，设计了安全量化指标，为企业提供全方位、系统化的模拟验证工具。企业可以利用入侵与攻击模拟（BAS）和量化指标，精准验证现有防御体系的效果，从而对自身的安全防护水平形成清晰的认知。这不仅有助于企业有效评估并提升安全防护能力，还能够推动安全运营效率的显著提升，最终以直观、量化的方式体现安全业务的工作价值和投资回报，助力企业实现从传统的基础安全建设到精准量化安全管理的跨越。



BAS 安全量化指标体系

1）防御效率指标：精准评估安全防护的实战能力与覆盖范围

防御效率指标体系是 BAS 的核心价值所在，反映企业安全产品和策略在面对模拟攻击时的实际防护性能和覆盖范围，可以帮助企业及时发现安全短板，并推进优化修复，避免安全防护的木桶效应。



防御效率指标

主要指标：

检测率。该指标是衡量安全产品基础感知能力的关键指标。具体而言，指在模拟攻击发生时，安全产品或系统能够成功识别并记录攻击事件的比例。BAS 通过自动化执行攻击事件并与安全产品的日志进行实时关联，判断设备是否按预期运行。高检测率表明安全产品对潜在威胁的感知能力强，是后续响应和处理的前提。反之，则意味着可能存在公共盲区或故障规则，需要及时进行策略调优或规则更新。

阻断率。该指标反映安全产品或系统在检测到攻击后，能够有效阻止模拟攻击，防止其达到目标或完

成攻击链的比例。BAS 会验证模拟攻击行为的目标（如文件执行、网络连接建立、数据传输）是否被安全控制成功阻止。高阻断率是企业期望看到的结果，意味着攻击在早期阶段即被有效遏制，直接降低风险。企业应优先强化拦截能力弱的关键控制点。

攻击成功率/穿透率。该指标揭示防御体系的根本缺陷。攻击成功率表示攻击者在模拟环境中成功绕过防御措施，达到攻击目标的比例；而穿透则明确指攻击行为未被检测且直接穿透防御的情况。BAS 通过真实模拟攻击路径，追踪攻击者是否能最终达成目的。较低的攻击完成率或零穿透率是企业安全防护的终极目标。任何非零值都意味着企业存在可被利用的风险，需立即启动应急响应和彻底的问题根源分析。

防护有效率。该指标评估全面防护策略的落地效果。通过定期的全面排查，确定安全策略在边界防护、流量安全、主机安全和终端安全防护等不同方面的实际落实效果及其提升百分比。BAS 能够自动化、常态化地执行跨方面的验证，其趋势变化反映安全策略的持续优化和落地情况，从而指导企业进行全面的安全策略审查和调整。

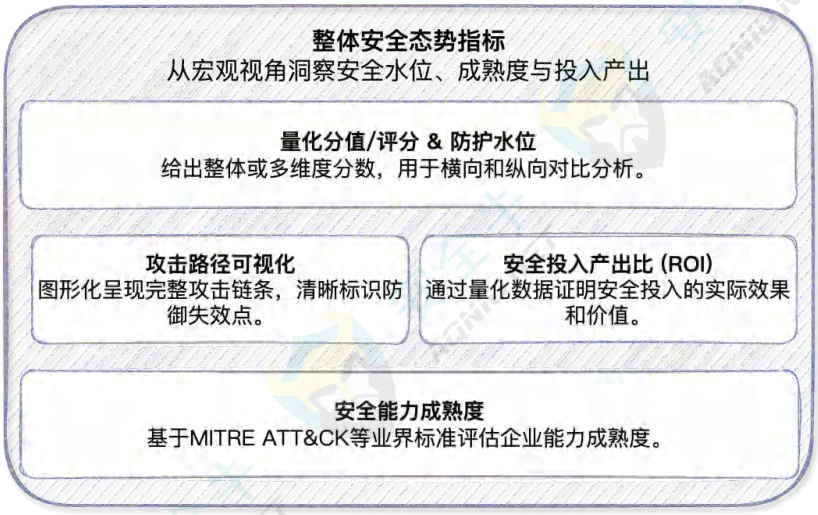
未防护弱点。指未被现有安全措施覆盖的场景或特定资产，揭示防护的空白区域。

防御薄弱点则识别在实际攻击场景下，防御体系中存在的薄弱环节或失效的控制措施。BAS 通过攻击路径可视化，明确指出这些具体的、可操作的改进点，促使企业优先解决这些显著的防御短板或配置错误。

变种检出率。该指标是衡量企业快速应对未知威胁能力的关键指标。专门指面对病毒木马等恶意软件的变种或新型攻击时，安全产品能够有效检测出这些变种的比例。BAS 通过模拟已知恶意软件的变种或利用 AI 生成新的、高度逼真的变种，测试防御系统对未知威胁的泛化识别能力，从而指导企业提升其高级威胁检测能力，例如增强行为分析、优化机器学习模型等。

2）整体安全态势指标：全面宏观战略指导

整体安全态势指标旨在从宏观层面全面评估企业的网络防御能力，为战略决策和长期规划提供清晰的安全方向和依据。



整体安全态势指标

整体安全态势量化评分。该指标是对整体安全态势能力的直观洞察。BAS 系统能够对企业整体安全态势防御能力进行自动化评估，并给出总分或各分项的分数（例如，采用 0-100 分制，并划分为低、中、高、严重风险等级）。这一评分通常基于多维度指标（如防护覆盖度、检测率、阻断率、攻击链成功率等）的权重计算结果。为企业管理者提供一个易于理解的安全健康指数，有力支持其进行战略性安全规划和经费分配决策。

防护水位。该指标动态反映企业整体防御能力的状态和成熟度。可用于横向对比（例如，与同行业平均水平对比，或与集团内部不同分子公司/部门进行安全能力对比）和纵向对比（例如，分析不同时间段内企业自身防护水位的变化趋势）。通过持续监测防护水位的变化，企业能够评估安全改进措施的实际成效，识别内部最佳实践，并指导资源在不同业务单元间的优化分配，推动安全能力的持续提升。

可视化攻击路径。提供直观的风险视图与行动路线。通过图形化方式，将模拟攻击中从初始预警、漏洞利用、横向移动到数据窃取等完整攻击痕迹呈现在网络拓扑图上，并准确标识防御失效点。这种可视化能力将复杂的攻击过程和防御失效点转化为直观易懂的信息，帮助安全团队和管理人员全面了解攻击者可能利用的渗透路径和潜在风险点。这有助于更精准地制定防御策略、优化网络架构（如实施微隔离），并指导安全资源的有效部署。

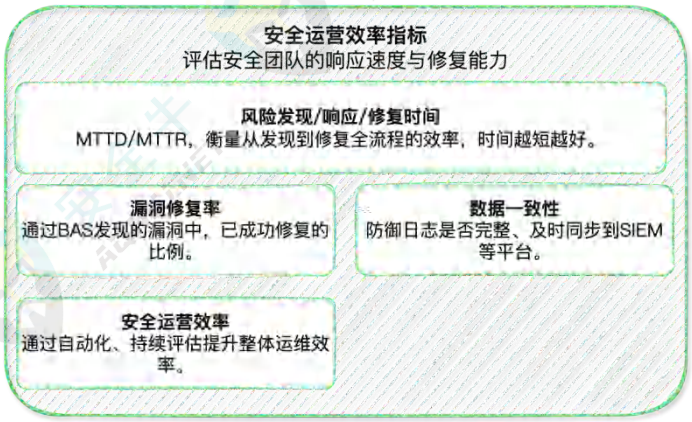
安全能力成熟度。该指标评估企业体系化安全建设的水平。该指标以 MITREATT&CK 框架等行业标准为基础，从识别、保护、检测、响应、恢复等多个维度，全面评估企业安全能力的成熟度。BAS 通过验证企业防御流程体系对 ATT&CK 框架中各项 TTP 的覆盖情况，详细分析企业在各阶段的防御能力。这有助于企业发现自身安全能力的短板，构建更加完善、体系化的防御体系，并推动安全管理和技术的持续优化。

安全投入增量比。该指标是衡量安全投资商业价值的核心指标。BAS 通过提供量化数据，直接论证安

全投入的实际效果。例如，通过 BAS 验证发现并修复高危漏洞的数量，以及避免的潜在安全事件次数，将安全成果与业务价值直接挂钩。这种能力能量化安全业务价值，验证安全战略的效果，并确保每一项安全布局都能转化为实际的业务价值。

3）安全运营效率指标：优化团队响应与管理绩效

安全运营效率指标旨在评估安全运营团队在风险发现、响应和修复流程中的表现，从而推动运营流程的自动化和效率提升。



安全运营效率指标

风险发现时间。该指标体现企业感知威胁的敏捷性。指从模拟风险事件出现到被 BAS 系统或 SIEM/SOC 平台成功发现并记录的时间。BAS 通过精准注入模拟流程并监测生成的数据，洞察企业对威胁的采集速度和日志上报的及时性。该时间越短，表明企业对威胁的采集能力越强，能够更迅速地启动后续响应。

平均响应时间/平均检测时间。该指标分别指安全团队从发现风险到采取响应或修复措施的平均时间，以及从风险出现到被检测的平均时间。BAS 能够模拟攻击并触发告警，测量从告警产生到问题响应（响应）或彻底解决（修复）的时长，从而评估 SOC、事件响应团队和自动化事件处理流程的效率。这些指标越短，表明企业的事件响应能力和运营效率越高，能够更快速地解决安全问题，减少损失。

风险问题修复时间。该指标评估问题解决的效率与闭环效果。指从发现问题到问题被彻底修复并经 BAS 复测确认所需的时间。高效的修复流程和问题解决能力是提升安全防护能力的关键。BAS 通过持续验证，能清晰地跟踪修复进度，确保问题真正得到闭环处理。

风险问题修复率。该指标直接反映漏洞管理的有效性。是通过 BAS 发现的漏洞或安全缺陷中，验证已成功修复并通过复测的比例。高修复率是降低整体风险的关键，表明企业具备强大的漏洞管理和策略优化能力，能够有效将测试成果转化为实际防御效果。

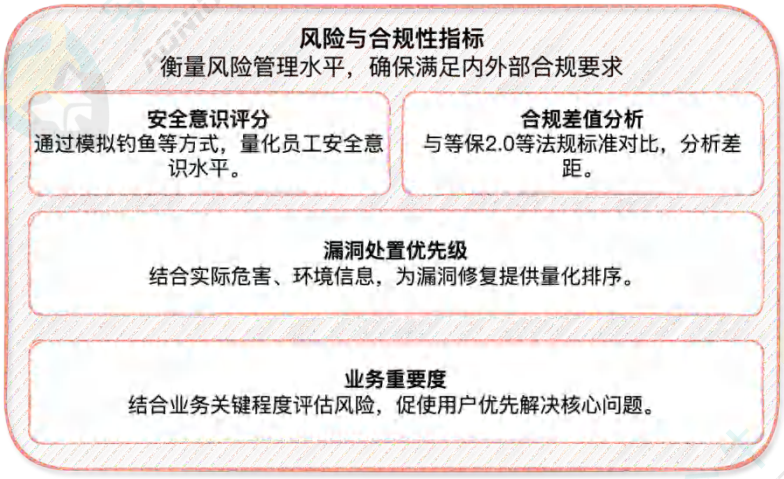
日志数据一致性。该指标是高效安全运营的基础，对于拥有复杂网络和海量日志的大型客户（如运营

商）而言尤为重要。指安全产品产生的日志是否完整、及时同步到 SIEM 等集中管理平台，以及不同日志源之间的时序和内容是否匹配。BAS 通过模拟攻击并比对各源日志的输出，能够发现日志传输过程中的断点、延迟或不一致等问题。这些问题可能导致安全分析出现盲区，以及影响分析安全事件的有效性。

安全运营效率。该指标确定安全运营的人力投入和时间成本，旨在显著降低安全运营团队的人力投入和时间成本。这使得安全人员能够从繁琐的日常事务中解脱出来，更加专注于高价值的威胁挖掘、高级分析和战略性决策。

4）风险与合规性指标：支撑管理决策与合规要求

风险与合规性指标旨在将安全验证结果与业务风险和法律法规要求相结合，为管理决策提供数据支撑，并帮助企业满足相关合规标准要求，实现从纸面合规到实战合规的转变。



风险与合规性指标

安全意识评分。该指标是通过模拟钓鱼邮件、恶意链接点击等社会工程学攻击，评估员工点击链接、打开附件、提交信息等行为，并结合行为结果，量化员工的安全意识水平。高分表明员工对常见社工攻击的识别和规避能力强；低分则凸显人这一防线的薄弱环节，需要开展有针对性的安全意识培训，以弥补人员方面存在的安全短板。

合规差距分析。该指标明确企业当前安全体系与合规要求的实际差距。通过将当前安全体系的实战现状与最新的行业标准、法规要求，如《网络安全法》《数据安全法》《信息安全技术-网络安全等级保护基本要求》等进行对比，针对合规条款对应的技术控制点进行实战模拟。例如，验证入侵防护、恶意代码防护、数据加密等措施的效果，并自动生成详细的合规性验证报告。报告中注明哪些合规项已通过实战验证，哪些仍存在风险，从而指导企业进行安全改进，确保从纸面合规迈向实战合规，降低法规处罚风险。

漏洞修复优先级。该指标通过评估其在当前防御体系下是否真正可被利用，并结合漏洞本身的利用难

度、受影响资产的业务重要性以及是否能被现有防御措施拦截等信息，为漏洞修复提供更精准的优先级评估。可以优化企业在风险管理中的资源分配。使企业能够将有限的安全资源投入到最能降低实际风险的修复工作中，提升漏洞管理的效率和效果。弥补传统漏洞优先级往往仅基于漏洞的 CVSS 评分，却未考虑其在企业实际环境中的可利用性和潜在影响的问题。

业务重要度。该指标将安全风险与核心业务价值深度关联。在评估安全风险时，能够将业务系统的关键程度纳入核心考量，例如，对业务关键性更高的系统赋予更高的风险权重，或者优先模拟针对关键业务系统和数据的攻击路径。这使得安全报告和决策支持更具业务说服力，促使企业和安全团队优先解决对企业核心运营和盈利能力影响最大的安全风险，从而实现安全与业务目标的紧密结合，确保安全工作能够切实保护企业的核心业务安全。

第四章国内外 BAS 市场和技术现状

在数字经济浪潮中，企业对网络安全实效的追求日益强烈，入侵与攻击模拟（BAS）技术作为以攻促防的关键工具，正逐步成为全球网络安全市场的新增长点。国外 BAS 技术应用正朝着更自动化、更标准化、更集成化、更关注面验证的方向发展，并紧紧围绕着云安全和 CTEM 等前沿安全管理理念进行创新。

4.1 国外 BAS 市场和技术应用现状分析

国外 BAS 技术应用市场已步入相对成熟的阶段，并持续演进，特别是在应对复杂威胁和集成化安全管理方面表现突出。

4.1.1 国外市场发展现状

国外 BAS 市场正呈现快速发展并趋于成熟的阶段，其市场规模持续扩大，这是多重复杂因素相互作用的必然结果。

1）国外 BAS 市场正呈现快速发展，市场参与者和创新解决方案层出不穷。

BAS 技术被越来越多的企业所接受和采纳，市场渗透率不断提升，新的市场参与者和创新解决方案层出不穷，主要原因是首先传统安全防护体系的局限性日益凸显：企业发现即使巨资部署了众多安全产品，仍然难以有效应对层出不穷的高级持续性威胁（APT）、勒索软件攻击和零日漏洞（0day），传统的年度渗透测试或周期性漏洞扫描因其稀疏性、高成本和无法常态化的局限性，无法满足动态验证的需求。其次，业务数字化转型加速，使得企业攻击面呈几何级数增长，云计算、物联网（IoT）和远程工作模式的普及带来了全新的安全挑战，这些复杂环境下的安全防护效果难以评估，亟须自动化、持续性的验证手段。

2）国外 BAS 市场正趋于成熟，向落地应用和价值实现的阶段迈进。

BAS 市场正在从早期概念验证向主流应用转型，趋于成熟。国外市场上涌现出 SafeBreach、Cymulate、XM Cyber 等一批技术领先、客户基础稳固的国外头部厂商，形成了相对稳定的竞争格局；BAS 产品更加标准化，例如自动化攻击模拟、标准化指标输出、无害化保障等已成为普遍共识；其与安全运营中心（SOC）、安全信息与事件管理（SIEM）、安全编排自动化与响应（SOAR）等现有安全生态的集成度日益加深；再者，企业对安全投资回报（ROSI）的量化需求日益迫切，管理者需要清晰地了解安全投入带来的实际防护能力提升和风险降低效果，而 BAS 提供了一种将抽象的安全效果转化为可量化指标的科学方法，使 BAS 的价值评估体系也日趋成熟。

3）BAS 显著增长的主要驱动

推动全球 BAS 市场实现显著增长的主要驱动因素可以归纳为以下几点。首先是网络攻击面的持续增长，随着企业数字化进程的深入，云计算、物联网和远程工作模式的普及，企业的攻击面不断扩大，传统边界防护难以覆盖所有风险，企业亟须一种能够持续、自动化验证所有暴露点的能力。其次是网络安全法规的不断演变，全球范围内对数据保护和网络安全合规性的要求日益迫切，例如欧盟的 GDPR、美国的 CCPA 以及 NIST 等框架，这些法规不仅要求企业部署安全控制，更强制性要求企业证明其安全控制措施的实际效果，从而推动了对 BAS 等验证工具的需求。再者，是对可扩展安全态势方案的诉求，传统的以人工为主的安全测试方法，如渗透测试和红蓝对抗，成本高昂、效率低下且难以规模化，无法满足企业不断增长的持续验证需求，因此，企业急需自动化、持续性的解决方案来提升验证能力。同时，高级持续性威胁（APT）的常态化也成了核心驱动力之一，面对 APT 组织、勒索软件等高级持续性威胁的复杂性和隐蔽性，企业需要更实战化的工具来验证自身防护体系的有效性，以确保能够抵御这些难以被传统手段发现的复杂攻击。

4.1.2 国外 BAS 技术应用现状

国外市场上的主要玩家，如 SafeBreach、Cymulate 和 XM Cyber 等，凭借其在技术创新和市场拓展方面的先发优势，已占据重要地位，并形成了各自独特的优势。这些厂商的产品普遍展现出以下显著的技术特点：



国外 BAS 技术应用现状

1）BAS 产品已经发展成熟

国外市场上已形成以 SafeBreach、Cymulate、XM Cyber 等技术领先、客户基础稳固的国外头部厂商，形成相对稳定的竞争格局。这些厂商共同推动了 BAS 核心功能和价值标准化的标准化，如自动化模拟攻击、标准化指标、无害化标准化工作等已成为行业共识，也代表 BAS 产品已经发展成熟的重要标志。

2）攻击模拟能力的全面性

国外 BAS 产品普遍具备对各种攻击技术（从 Web 应用攻击到网络层漏洞利用，再到高级恶意软件行

为）的全面模拟能力，并能高度仿真攻击链的各个阶段。其解决方案组合已涵盖各种攻击类型、广泛的环境（包括传统本地部署、复杂云环境，甚至工业控制系统/物联网），以及深度集成能力。例如，SafeBreach 拥有涵盖数万种攻击技术的攻击者行为库，持续更新最新的威胁，强调提供全面的攻击者视角，覆盖网络、终端到云环境，展示了其方案的广度和深度。AttackIQ 则在攻击场景覆盖的全面性、自动化验证能力以及与 MITRE ATT&CK 框架的深度集成方面具有显著优势，强调对安全控制的持续验证和优化。Cymulate 也提供广泛的攻击模拟能力，从网络应用到邮件安全，并强调持续验证安全控制、评估风险暴露和策略合规性。

3）高级的自动化与编排能力

国外上的 BAS 自动化能力已从简单的脚本执行演进到复杂的攻击链编排和智能决策，支持用户通过直观界面编排多阶段、多协议的攻击链。例如，Cymulate 凭借其模块化设计和高度自动化的测试流程，能够让用户灵活组合多种攻击模拟模块，其产品提供了多个独立的模拟模块，包括漏洞利用、钓鱼、Web 应用攻击、勒索软件、数据泄露等，企业可以根据自身需求选择和组合，并通过高度自动化的测试流程，显著降低了非专业安全人员的操作配置，使非安全专业人员也能快速上手。

4）深度集成融合和闭环修复

厂商也高度重视与其他安全产品和平台的集成，能够与企业现有的系统进行无缝集成，如安全运营中心（SOC）、安全信息与事件管理（SIEM）、安全编排自动化与响应（SOAR）、漏洞管理（VM）和 IT 服务管理（ITSM），这种深度融合使得 BAS 验证结果能够自动流入安全运营流程，驱动自动化响应和闭环修复。

5）量化评估体系与可视化报告

国外 BAS 产品普遍提供精细化的量化评估指标，如检测率、阻断率、ATT&CK 覆盖率，并通过直观的可视化仪表板、攻击路径图谱等形式呈现安全态势和风险评估结果，帮助企业明确安全投入的价值和风险优先级。例如，XM Cyber 侧重于攻击路径管理，其平台能够持续识别并模拟攻击者在企业网络中最可能利用的攻击路径，并通过可视化方式呈现攻击图谱，提供优先级排序的修复建议，将技术发现转化为业务风险洞察。Picus Security 也强调其能够持续验证安全控制措施的有效性，并与各种安全产品和 SIEM 平台无缝集成，提供实时反馈，从而实现防护策略的自动化调优。

6）威胁情报驱动的行为仿真

国外 BAS 产品普遍与全球威胁情报深度融合，将最新的 APT 攻击策略、技术和过程（TTPs）转化为可执行的模拟，并主要注重模拟攻击者的真实行为模式和绕过防护技术。例如，XM Cyber 更关注于攻击路径管理和暴露管理，其平台能够持续识别企业网络中最容易被攻击者利用的攻击路径（攻击路径），并模拟攻击者在这些路径上的横向移动行为，其独特之处在于强调基于假设被攻击的思维，帮助企业识别出

真实并最具风险的攻击路径。Google Cloud 则是通过收购 Mandiant 的威胁情报和安全响应经验，显著增强威胁情报驱动的验证能力，实现最新的攻击手段模拟。Picus Security 也强调最新威胁情报驱动的验证，提供最新的威胁库和可定制的攻击场景，以模拟高级持续性威胁（APT）和勒索软件攻击。

7）融合 AI 能力的创新应用

国外领先厂商积极探索 AI、机器学习特别是大型语言模型（LLM）在攻击模拟中的创新应用。AI 可以自动化生成更复杂的攻击场景、动态适应目标环境、生成多变攻击有效载荷（如利用生成式 AI 生成高度仿真的钓鱼邮件），从而显著提升攻击模拟的智能性和自动化程度。例如，FireCompass 等厂商利用 AI 对最新威胁情报的分析和学习能力来优化攻击库更新和场景编排。Horizon3.ai 则可利用 AI 提供更强的自主探索能力，以发现网络中的未知路径，提升验证的广度和深度。

8）云环境的验证

随着云计算的普及，国外 BAS 厂商将重点放在云环境下的安全评估，包括 IaaS、PaaS、SaaS 层的漏洞、错误配置，以及云原生组件（如容器、Kubernetes）的安全验证。许多厂商支持在云环境中部署验证代理或提供云原生集成，以评估云资源的暴露面和安全控制的有效性。例如，Google Cloud 受益于其云服务的原生优势，能够提供更深层次的云环境安全验证。

9）CTEM（持续性威胁管理）的实践

国外市场高度重视将 BAS 整合到 CTEM/AEV 这一更为宏观的安全管理框架中。CTEM 强调持续地发现、优先排序、验证、启动和测量安全暴露。BAS 在其中的核心价值是提供验证阶段所需的实战数据和经验，从而推动整个 CTEM/AEV 流程的有效运行。如 AttackIQ、Cymulate、Picus Security、SafeBreach、XM Cyber 等厂商都强调对 CTEM 的支持，帮助客户实现持续的暴露管理和风险优化，将 BAS 视为 CTEM 不可或缺的组成部分。

4.1.3 国外技术和应用的未来趋势

展望未来，BAS 技术及其应用正受到当前网络安全前沿趋势的深刻影响，并共同推动 BAS 从一个独立的测试工具，向企业安全感知建设的核心引擎演进。



国外 BAS 技术和应用的未来趋势

首先，AI 驱动的自动化将更深入地渗透 BAS 的各个部分，实现攻击模拟的深度演进。未来的 BAS 系统将不再单纯依赖 AI 辅助攻击生成，而是更广泛地利用人工智能进行自动化路径探索和优化。例如，系统能够基于对企业环境的理解，自主发现并模拟攻击者可能利用的最短攻击路径。同时，基于强化学习的自适应攻击决策将使 BAS 具备更高的自主性，能够根据实际防护反馈动态调整攻击策略，模拟出更复杂、更难以预测的攻击行为。此外，利用**大型语言模型（LLM）**进行复杂威胁情报的深入分析和攻击场景的智能编排，将有助于 BAS 实现对未知威胁的零日模拟能力，从而测试防护系统对未知威胁的响应能力，这一趋势将有助于企业实现更高级别的主动安全治理，将安全关口前移至 AI 驱动的风险预测和验证阶段。

其次，BAS 将加速形成与暴露管理平台（CTEM/TEV）的生态建设和深度融合。未来的 BAS 系统将不再孤立存在，而是与攻击面管理（ASM）、漏洞管理（VM）、安全配置管理（SCM）等暴露管理相关工具进行深度融合，共同构建统一的持续暴露管理（CTEM）或威胁暴露验证（TEV）平台。这些平台将为企业提供攻击面的全景视角，从发现潜在漏洞、评估风险、通过 BAS 进行实战验证，到对风险进行优先级排序并推动修复，形成完整的闭环管理。BAS 将作为 CTEM/TEV 平台的核心验证引擎，为暴露面提供持续的、实战化的验证数据，确保发现的漏洞和风险是真实可利用的，从而指导精准修复，提升企业整体安全。

再者，云原生安全与容器环境的深度支持将成为 BAS 的重要发展方向。随着云原生架构（如容器、Kubernetes、Serverless）在企业中的普及，BAS 的应用将更加聚焦于模拟和验证云原生环境中的特定攻击面和漏洞，以及云平台自身的安全配置和策略有效性。这包括对云 API 滥用、容器逃逸、云服务配置错误、微服务间通信安全等云原生威胁的精细化模拟，以确保云上资产的安全性和合规性。未来的 BAS 将发展出更加适应云环境动态特性和弹性伸缩的验证机制，能够实时响应云资源的动态变化，确保云上防护的持续有效性。

另外，BAS 的应用将向操作技术（OT）和工业控制系统（ICS）领域以及物联网（IoT）安全拓展。随

着工业互联网和智能制造的深入，IT 与 OT 网络的融合日益加剧，针对工控系统和物联网安全产品的网络攻击风险剧增。BAS 需要发展出针对特定 OT/ICS 协议的模拟能力，同时能够评估模拟攻击对物理世界可能造成的影响。未来的 BAS 将能够实现 IT/OT 融合环境下的攻击链验证，以保障关键基础设施的安全运行和生产连续性。

同时，BAS 的量化能力将持续提升，并与业务风险进行深度关联。BAS 将不再仅仅提供安全技术层面的指标（如攻击成功率、ATT&CK 覆盖率），而是更深入地探索如何将这些技术指标与业务层面的风险（如潜在财务损失、业务中断时间、品牌声誉损害）进行关联。这一趋势将使安全报告和决策支持增加业务说服力，帮助高层管理人员更清晰地理解安全投资的业务价值和风险影响，从而实现更高效、更精准的资源分配和安全战略制定，推动安全与业务的深度融合。

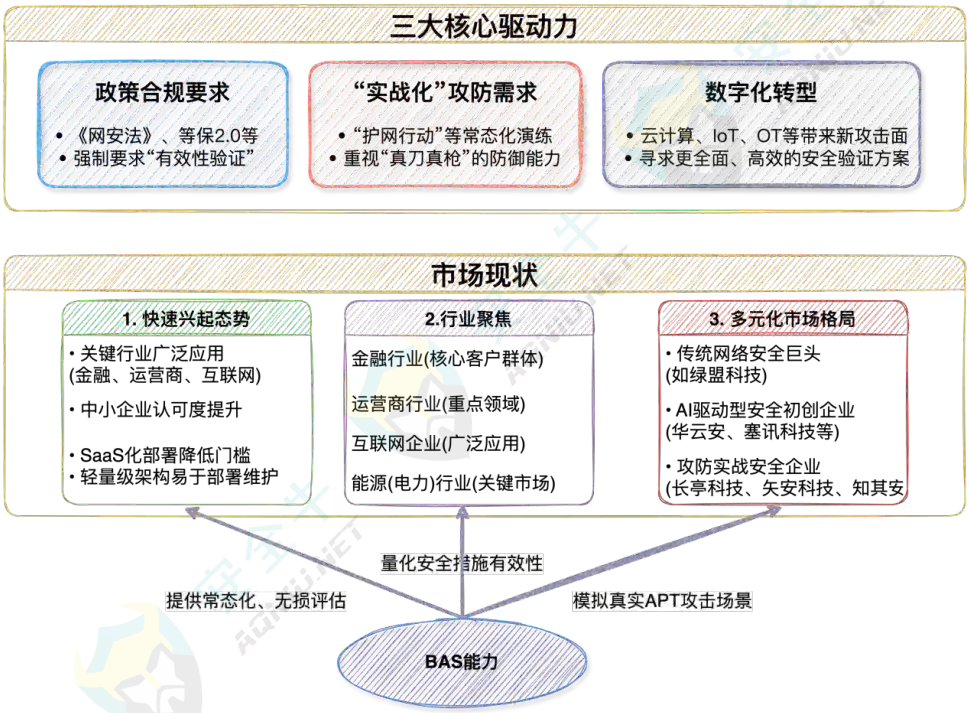
最后，AI 与人的协同演进将是 BAS 未来发展的重要模式。尽管 AI 在 BAS 中的作用日益增强，但安全专家的决策和专业能力依然强大且不可或缺。未来的趋势将是 AI 与安全专家的更加紧密配合，形成高效的人机协同安全运营模式。AI 将自动化繁琐的重复性验证任务，并提供定制的风险洞察和修复建议，从而赋能安全团队专注于增强威胁狩猎、高级分析和战略性决策。安全专家将利用 AI 驱动的 BAS 系统来提升自身能力，实现更高效、更智能的安全运营，确保在不断变化的网络威胁面前，企业始终保持领先的防护态势。

4.2 国内 BAS 市场和技术应用现状分析

国内 BAS 市场作为全球网络安全领域不容忽视的新兴力量，近年来发展态势迅猛，凸显出鲜明的中国特色与强劲的增长势头，市场格局也正逐步成型，众多具备强大竞争力的本土厂商如雨后春笋般涌现。国内 BAS 市场的核心特征包括以攻防经验构建的丰富攻击库、对无害化安全的高度重视，以及 AI 技术在攻击生成、量化评估和运营闭环中的深度融合。未来，市场将向着更智能的自动化、更广泛的场景覆盖、更统一的行业标准方向发展，真正实现以攻促防的战略价值。

4.2.1 国内 BAS 市场发展现状

国内 BAS 市场作为全球网络安全领域不容忽视的新兴力量，在政策与实战化关键因素的合力推动下，近年来发展态势迅猛，市场渗透率不断攀升，市场格局正逐步成型。



国内 BAS 市场发展现状

1）国内 BAS 市场呈现出显著的快速兴起态势

国内 BAS 市场在实战化需求的强劲驱动下，已快速演变为网络安全领域的重要增长因素，并呈现出显著的快速兴起态势。

一方面，BAS 技术在多个关键行业内已经被广泛接受与应用，尤其是在金融、运营商、互联网等对网络安全要求较高的关键行业中，已获得广泛认可并得到应用，成为提升实战化防御能力的重要工具。另一方面，中小型企业也逐渐认识到 BAS 的价值。厂商纷纷推出轻量级、易部署的 SaaS 服务，极大降低了企业投入成本。同时，厂商普遍强调产品架构轻量级、易部署、易连通、易运行、易维护，且对系统资源要求低，契合中小型企业的部署需求。让 BAS 不再是大型企业的专属，市场渗透率有望持续走高。

未来 BAS 不再是大型企业的专属，市场渗透率将持续提升。并且多家具备 SaaS 化部署能力的厂商通过提供轻量级、易部署、无需繁琐开发和维护的 SaaS 服务，极大地降低了企业的投入成本。并且厂商普遍强调其产品架构轻量级，易部署、易连通、易运行、易维护，对系统资源要求低，能够满足一般中小型企业的部署需求。

2）国内 BAS 市场在发展中展现出鲜明的中国特色和强劲的增长潜力。

国家网络安全政策与合规要求构成了核心驱动力。《网络安全法》《数据安全法》《个人信息保护法》以及等保 2.0、关键信息基础设施安全保护条例等法规的实施，使企业对实战化有效性验证的需求急剧增

长。BAS 能量化证明安全措施有效性，精准契合这些合规要求。

实战化攻防需求普遍化。国家常态化的网络安全攻防演练（如护网行动）促使企业重视真刀真枪的防御能力。国内用户期望 BAS 不仅能发现漏洞，更能模拟真实 APT 攻击场景，验证复杂攻防对抗下的防御能力，并提供常态化、无害化的评估手段。

同时数字化转型带来的复杂网络环境拓展了 BAS 应用需求。云计算、物联网、工业互联网等新兴技术的广泛应用带来新安全挑战与攻击面，推动企业寻求更全面、高效的安全验证方案，为 BAS 市场注入源源不断的增长动力。

3）国内 BAS 市场用户主要集中在金融、运营商、互联网企业。

国内厂商普遍将金融行业作为核心客户群体，借助 BAS 系统进行持续性防护验证，应对勒索病毒、APT 等高级网络威胁，以及攻防演练的挑战。头部金融行业对 BAS 应用成熟度高，甚至能基于 BAS 平台进行二次开发。运营商行业同样是厂商深耕的重点领域。厂商协助运营商应对海量数据告警、庞大网络基础设施与面临的复杂网络威胁。能源（电力）行业也被视为关键市场，利用 BAS 提升高强度攻防演练实战下的防御能力。此外，政府、互联网、工业制造、教育、医疗等行业也广泛运用 BAS 技术。

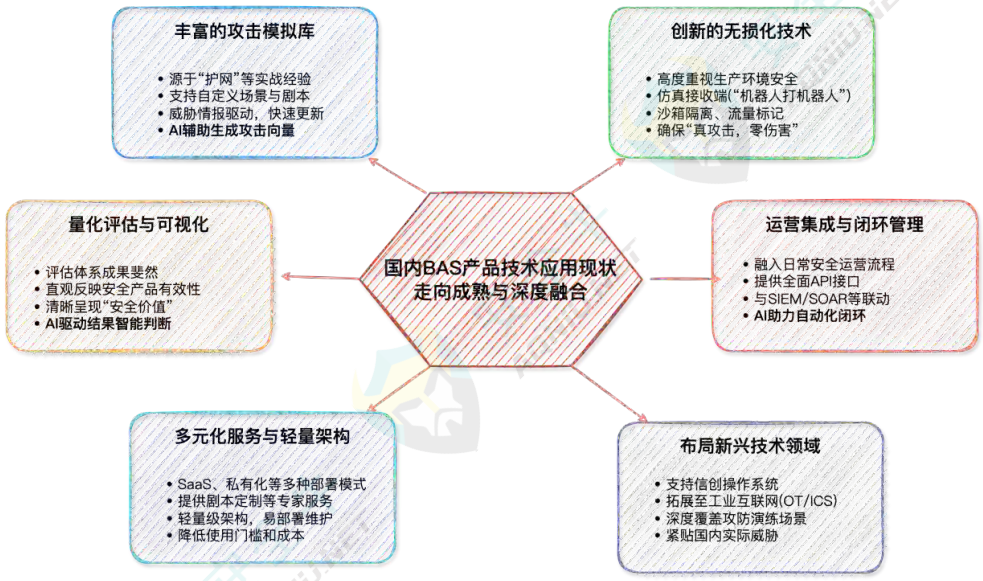
4）国内参与厂商的多元化市场格局

国内 BAS 市场格局逐步成型，竞争激烈，主要参与者包括传统网络安全巨头、新兴 AI 驱动型安全初创企业以及拥有强大攻防实验室背景的专业安全公司。

传统网络安全巨头，如绿盟科技，凭借深厚行业积累与广泛客户基础，将 BAS 纳入安全产品体系。新兴 AI 驱动型安全初创企业，如华云安、灰度安全、墨云科技、塞讯科技等，以 AI 技术创新为核心，在 BAS 领域探索智能化突破。拥有强大攻防实验室背景的专业安全公司，如长亭科技、赛宁网安、矢安科技、知其安等，依托实战攻防经验，强调攻击库的真实性与对抗性。

4.2.2 国内 BAS 产品技术应用现状

国内 BAS 产品技术已从概念认知迈向深度应用的成熟阶段。其核心特征表现为内外兼修：对内，以护网等实战经验沉淀出海量、高保真的攻击库，并以创新的无害化技术确保业务安全；对外，通过量化评估与可视化清晰呈现安全价值，并以开放的 API 融入企业安全运营生态。而 AI 技术的深度融合，正作为核心驱动力，全面提升着攻击模拟的智能化、评估分析的自动化和运营管理的闭环化水平。



国内 BAS 产品技术应用现状

1）基于威胁情报不断更新的攻击模拟库

国内厂商在多年攻防演练与护网、重保实践中积累了丰富的实战经验与攻击库资源。厂商通常将自身攻防实验室、APT 组织追踪能力以及攻防演练经验转化为产品攻击库，确保攻击模拟的真实性、全面性与有效性。厂商普遍支持自定义攻击场景与剧本编排，弥补内置攻击库不足，满足企业对特定业务场景和威胁定制化验证需求。同时引入 AI 能力辅助攻击向量生成与剧本编排，提升攻击模拟的灵活性、适应性与效率。并且提供基于威胁情报的攻击模拟库的更新，并针对突发的新型威胁快速提供专项的最新验证用例。

厂商案例 *（部分案例参考数据）*

- 长亭科技内置近万个漏洞，包括数百个 0day 漏洞，超危漏洞占比 16%，高危漏洞占比 63%。
- 华云安内置超过 6000 条安全验证用例，涵盖多种场景类型。
- 灰度安全利用全球蜜网系统监控和跟踪最新威胁，内置 40000+攻击向量。
- 绿盟科技攻击模式库与全球威胁情报、漏洞库和红队经验深度融合动态迭代。
- 墨云科技积累了 40000+攻击向量，能模拟多种 APT 攻击技术。
- 塞讯科技拥有 20000+模拟攻击，包括内置的 400+ APT 组织场景和 250+勒索团伙场景，并能够根据最新的威胁情报（如 30+海内外社区情报源）不断更新，确保了攻击模拟的真实性、全面性和有效性。
- 赛宁网安拥有 5200+模拟攻击用例，包含 100+勒索挖矿和 400+APT 组织情报。
- 矢安科技内置 20000+高质量攻击用例，覆盖了 2600+个 CVE/CNNVD 漏洞，并支持对 20+个 APT 攻击组织和 200+个勒索攻击组织进行模拟，能够在 24 小时内响应 0day 漏洞，并每周常态化更新规则库，确保攻击用例的及时性和有效性。

- 知其安科技通过敏捷用例高效发布，基于情报实现最快 4 小时上线最新用例。

请注意，该效果数据来源于部分案例或特定场景，实际效果受到多种因素的影响，数据仅供参考，并不代表所有企业都能取得类似的效果。

2）创新的无害化化技术

国内 BAS 产品高度重视安全性，并在无害化化技术创新方面取得显著成果，针对国内用户对生产环境稳定性高度重视的特点，厂商在无害化模拟技术上各显神通。部分厂商采用不依赖目标靶机的仿真接收端技术，通过自身仿真能力模拟业务环境；另一些厂商运用沙箱隔离、流量标记、权限降级等技术，确保攻击模拟无害化运行，即使在生产环境中也不会对业务造成任何负面影响。

厂商案例

- 长亭科技不依赖目标靶机的仿真接收端技术，规避传统靶机引入新风险的问题。
- 灰度安全采用数据包标记、流量控制等无害化测试技术，确保不影响系统的正常运行。
- 绿盟科技通过沙箱隔离、流量标记、权限降级等技术实现无害化运行。
- 塞讯科技采取机器人方式，被攻击目标是机器人，而非企业的业务系统和应用。并且设计了专为破坏性安全测试的沙盘，具有快照和回滚功能。拥有大量 PCAP 包，利用回放进行攻击模拟，无需目标操作系统安装、启用应用或服务，不引入新风险。
- 失安科技利用无害化、无害化失技术进行攻击验证时，对业务不入侵、无影响，并且模拟漏洞利用环境不引入靶场环境，避免了对企业可能造成的安全风险。

3）BAS 量化评估应用效果明显

国内 BAS 产品在量化评估体系建设上成果斐然，数据可视化效果显著。随着企业对安全产品的要求从有无向好不好转变，BAS 数据量化评估受到高度重视，厂商积极提供防御效率、整体安全态势、运营效率、风险与合规四大维度的量化指标体系，并引入多维度评估方法，使得验证量化指标数据的准确度得以提升，这些量化指标能够直观反映安全产品的有效性、攻击链的阻断情况以及整体防御体系的效能，帮助客户清晰地看到安全价值，推动市场从概念导入期走向价值验证期。

厂商案例 *（部分案例参考数据）*

- 长亭科技通过对 WAF、全流量、IPS 等产品的多次认证，实现 WAF 阻断率从 64%提高到 95%，检测率从 73%提高到 100%，全流量检测率从 85%提高到 100%。
- 华云安通过 BAS 验证发现 WAF 攻击防护能力失效率达 96%，主机/终端安全产品的防御有效率为 41%，并精准识别到了防护的弱点问题原因。
- 绿盟科技通过 BAS 持续验证和优化，实现 WAF 防护率从 40%提升至 90%，互联网暴露面防护覆盖度从部分路径缺失提升至 100%。
- 墨云科技通过持续测试验证，发现边界防护、主机安全、应用安全等多层面薄弱点，优化并推进防护成功率提升 40%。
- 塞讯科技通过安全验证大脑+验证机器人+沙盘的方案，持续验证，使自研安全产品检测率从 50%上升至 90%以上。
- 赛宁网安通过量化评估，实现 WAF 检出率从 0%提升到 90%。
- 矢安科技在某大型金融云案例中，通过验证整改提升闭环管理，使各个分子公司的单点防护安全产品防护覆盖率从低于 30%提升到 95%+。
- 知其安通过 BAS 验证和优化，使 WAF 安全产品拦截能力达到 99%，NTA、HIDS 检测能力达到 99%以上，并通过防御常态化验证，安全产品安全有效性提升总和达 83%。

请注意，该效果数据来源于部分案例或特定场景，实际效果受到多种因素的影响，数据仅供参考，并不代表所有企业都能取得类似的效果。

4）运营集成与闭环管理方面也迈向了新的成熟阶段

国内 BAS 厂商在运营集成与闭环管理方面日臻成熟，借助自动化、智能化手段，将安全验证深度融入企业日常安全运营，提升整体安全防御效能与响应速度。BAS 应用从评估工具进化为企业安全运营体系的核心组成部分，实现持续验证与优化闭环。厂商普遍提供全面 API 接口，促进 BAS 与企业现有资产测绘管理、SOAR、态势感知等系统对接，达成联动自动闭环。

厂商案例

- 灰度安全可对接外部态势感知、SOAR 等系统，实现风险度量集中可视化呈现、风险协同响应处置与统一作战指挥。
- 绿盟科技的防御突破模拟与评估系统 BAS 支持与漏洞管理、攻击面管理、态势感知等平台联动。
- 塞讯科技支持通过 API 接口与企业的 SOC（安全运营中心）和工单系统进行双向对接，实现任务执行、结果反馈和自动化响应（如封禁或隔离）的联动，从而帮助客户量化检测和响应时间，并将问题控制在最小范围内。
- 矢安科技支持与觅影 EASM（外部攻击面管理）联动，提供更贴合实际暴露场景的防护验证。在分子公司验证案例中，通过 API 调度，实现各分子公司的统一展示和安全风险的流程化闭环管理，确保发现的问题能够被有效驱动

并解决。

- 知其安支持与 SOC 平台双向联动，包括下发验证任务和接收告警日志，从而实现自动化验证结果闭环。

5）提供 SaaS 和专业服务和轻量级架构，满足不同客户需求

国内 BAS 厂商在服务形式和部署模式上呈现多元化，适应不同客户需求。厂商通过多样部署交付模式，结合专业的服务支持，并且采用轻量级架构，支持热加载、批量化部署与维护，降低部署运维难度与成本，满足不同客户的需求。

厂商案例

- 长亭科技提供多种 BAS 服务，旨在协助客户解决安全加固的“最后一公里”问题。
- 华云安提供验证用例更新及定制服务以及安全场景验证定制验证服务。
- 塞讯科技支持远程 SaaS 验证和本地化验证，并提供安全验证托管服务，协助客户解决安全验证各阶段难题特别是闭环阶段的困难。
- 矢安科技提供 SaaS 服务，支持用户按需、按服务周期订阅购买安全场景，旨在降低产品部署和日常运维成本，提供攻击路径分析、剧本定制服务和验证分析，以及闭环运营等多种服务，协助客户解决安全加固难题。
- 受访谈的所有厂商几乎都提供私有化部署和 SaaS 云服务模式，并重视 BAS 的轻量级和易部署易维护的特点。

6）积极布局新兴技术领域，并强调实战化与攻防演练场景的深度覆盖

国内厂商积极布局新兴技术领域，整合前沿技术与实战经验，提升安全验证精准度与时效性。国内厂商积极开发支持信创操作系统及其他信创环境的代理，并积极积累信创的攻击用例，以适应国内信创战略的推进。部分厂商将业务拓展至工业互联网（OT/ICS）安全领域，支持模拟工控协议、工控安全产品和工控系统的安全验证，这是国外上相对新兴但国内需求普遍存在的领域。在实战化方面，受国家级攻防演练常态化影响，国内厂商的产品普遍强调其攻击库来源于真实的红蓝对抗、APT 组织追踪和安全研究经验，能够快速收集、分析和转化本土最新的威胁信息，并融入其 BAS 攻击库和基线，实现攻击能力的快速更新和本地化模板，确保 BAS 模拟的攻击场景更贴近国内实际威胁，提升验证的精准度和时效性。

厂商案例

- 塞讯科技专注于打造基于 AI 能力的对抗式安全验证平台，利用真实的 APT 攻击场景、第一手的受害者威胁情报，结合 AI 情报派生技术。塞讯的 AI 助手能高精度解释攻击结果并生成可落地的缓解建议，准确率达 95%以上。

7）AI 深度融合成为提升产品智能化和自动化水平的核心驱动力

AI 技术成为 BAS 平台提升智能化、自动化水平的核心驱动力，在攻击模拟、结果分析、策略优化等环节发挥关键作用，显著增强了 BAS 的实战价值和应用效率。国内厂商积极将 AI 技术赋能于 BAS 的各个环节，使其在攻击模拟、结果分析、策略优化以及用户交互方面都实现了显著突破。

在攻击模拟与生成方面，厂商利用 AI 技术进行动态生成攻击 Payload，根据目标环境的特点，智能地生成多种攻击变体，甚至支持基于生成式 AI 的攻击向量编写架构，通过自然语言交互自动化生成可用的攻击向量和攻击剧本，这大幅提升了攻击模拟的隐蔽性、欺骗性和效率，并降低了复杂攻击编排的门槛。并利用 AI 实现基于强化学习的自适应攻击决策，使模拟攻击更加智能，能够自动决策攻击链并评估防御体系的鲁棒性。

在结果分析与策略优化方面，AI 的赋能使得 BAS 能够处理和理解海量、异构的安全日志数据。国内厂商的产品普遍具备全自动化智能日志闭环分析技术，通过独创的高效日志对接与分析引擎，支持多种安全产品日志格式的实时解析与关联分析，能够实现验证结果的全自动化智能判断，甚至无需人工干预。这种智能分析能力引入了动态阈值自适应算法，自动识别异常行为模式，能够显著降低误报率，并提供更精准的告警信息。在此基础上，AI 还能通过 AI 决策引擎自动生成修复建议**，并触发防护策略更新，将安全运营的闭环效率提升至新的高度，部分厂商声称可实现运维效率大幅提升。此外，AI 也被用于智能威胁预测和防御能力画像构建，通过大数据分析和学习，预测潜在攻击向量，并提供精准的防御建议，从而实现安全关口的进一步前移。

在应用场景与用户体验方面，AI 也发挥着日益重要的作用。结合大语言模型（LLM），BAS 产品能够快速生成钓鱼邮件模板和页面，大幅提升社会工程学攻击模拟的真实性，并降低了人工制作的成本。AI 还能辅助专家进行新攻击和漏洞的剧本编排，提供更强的自主探索能力，以发现网络中的未知攻击路径。国内厂商还通过 AI 来提升产品易用性，AI 助手能帮助用户理解平台功能、攻击脚本，并协助自动化配置，通过可视化度量模型，帮助用户更直观地理解安全态势和风险。

厂商案例

- 塞讯科技：通过 AI 助手编排各类攻击场景，解释攻击结果。AI 驱动平台与 AI 助手：塞讯科技专注于打造基于 AI 能力的对抗式安全验证平台，利用 AI 情报派生技术赋能安全防御体系。其 AI 助手能帮助用户理解平台功能、攻击脚本，并协助自动化配置，以提升易用性和运营效率。智能告警与分析：运用 AI 算法分析验证结果和历史数据，提供更精准的告警信息，并帮助用户快速定位和理解安全风险。智能威胁预测与缓解建议：具备基于机器学习的缓解建议生成能力，并通过 AI 的大数据分析和预测能力，提供智能威胁预测和精准防御建议。
- 矢安科技：利用 AI 生成高精度攻击用例。基于 AI 的主动安全与智能攻击模拟：利用 AI 技术，将风险及资产上下文关联，从传统事后扫描转变为事前体检，实现自动化智能体检并覆盖整个杀伤链的全面验证。AI 也能辅助生成高精度攻击用例，使 BAS 攻击模拟更智能，能自动决策攻击链并评估防御体系的鲁棒性。AI 生成钓鱼策略模板：结合大语言模型（LLM），能够快速生成钓鱼邮件模板及钓鱼页面。变种免疫性检测：通过 AS AI 模块，能够配

置各类用例变种并自动生成，提升对新型变种威胁的检测能力。

- 几乎所有国内厂商均正在开展引入 AI 的工作，并都将 AI 作为重要的未来规划内容。

4.2.3 国内 BAS 技术应用的不足

尽管国内 BAS 市场应用广泛，但仍面临诸多挑战，这些挑战也反映出市场正逐步走向成熟，企业在探索复杂应用场景时遇到的新问题促使厂商持续创新，拓展技术与应用边界。



国内 BAS 技术应用的不足

复杂攻击模拟能力不足。国内 BAS 产品在模拟 APT 攻击、精细化绕过技术，尤其是供应链攻击、零日漏洞利用等高级持续性威胁方面存在短板，深度模拟复杂隐蔽攻击手法是未来需要攻克的方向。

数据集成与归一化难题：BAS 系统与企业安全产品、日志平台对接时，跨厂商、跨产品数据集成与归一化难度大，AI 模型训练高质量数据获取困难，易形成数据孤岛，制约 BAS 效能发挥，影响其融入整体安全运营流程。

行业标准制定滞后：国内 BAS 行业标准制定处于起步阶段，量化指标缺失导致厂家验证结果差异大，评估结果客观性、权威性受质疑，厂商指标名称也未统一。

用户安全专业水平有限：BAS 产品自动化程度虽高，但结果解读、修复建议落地、安全运营流程优化依赖企业内部安全专业能力。部分企业缺乏专业人才，难以充分发挥 BAS 价值，需借助第三方专家服务。

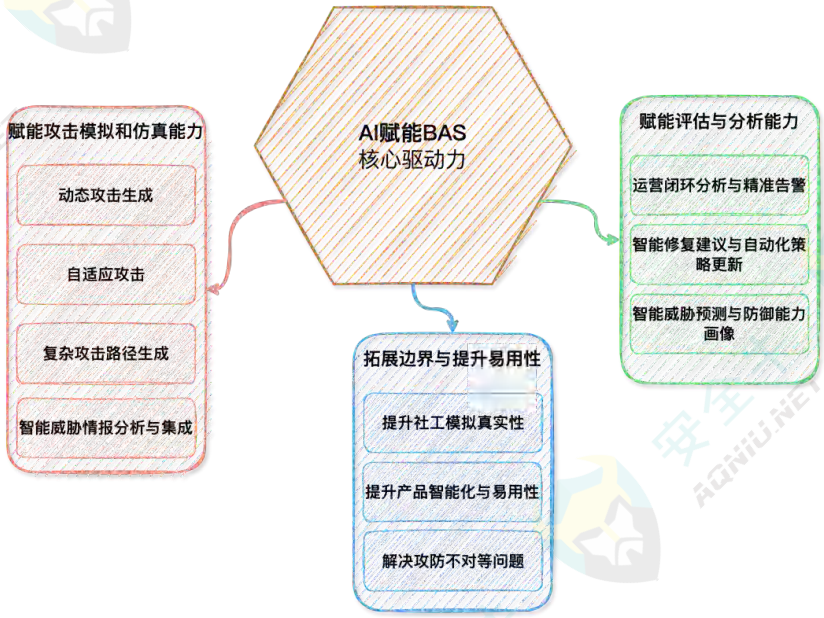
新兴场景验证能力待提升：针对大模型、工业互联网等新兴复杂领域，BAS 产品的通用化、标准化验证能力亟待提高，尽管部分厂商已布局，但仍需进一步验证与完善。

AI 利用能力需深化：AI 在 BAS 中虽已发挥重要作用，但在自动化与自适应攻击、智能日志解析和关联分析等方面仍有提升空间，需要厂商与用户共同努力，借助 AI 提升自动化、智能化水平，强化平台集成，打破数据孤岛，完善攻击库，应对最新威胁，实现更高级别智能安全运营。

第五章 AI 赋能 BAS 验证

在网络安全形势日益复杂、各类威胁不断涌现的当下，人工智能（AI）已然成为推动各行业数字化转型以及提升安全防御能力的关键力量。AI 正从根本上重塑 BAS，使其从传统的模拟验证工具进化为智能对抗中枢。其核心价值在于：通过赋能动态攻击生成、自适应路径探索、智能化结果分析与自动化策略闭环，将 BAS 的全生命周期智能化。这不仅极大地提升了验证的真实性与效率，更推动了安全防御从被动响应向主动预测与自主免疫的颠覆性变革，最终致力于解决攻防不对等的核心挑战。

国内众多厂商正积极投身于将 AI 技术广泛应用于 BAS 的各个层面，使其在攻击模拟、结果分析、策略优化以及用户交互等方面均取得了显著突破，成功开启了智能安全验证的新篇章。随着 AI 技术的不断发展进化，未来 BAS 将超越传统问题发现工具的范畴，真正成为企业构建主动防御体系、实现安全可量化、可视化的核心中枢，推动安全防御模式从被动响应向主动智能转变。



AI 赋能 BAS 验证智能化

5.1AI 赋能 BAS 验证应用现状

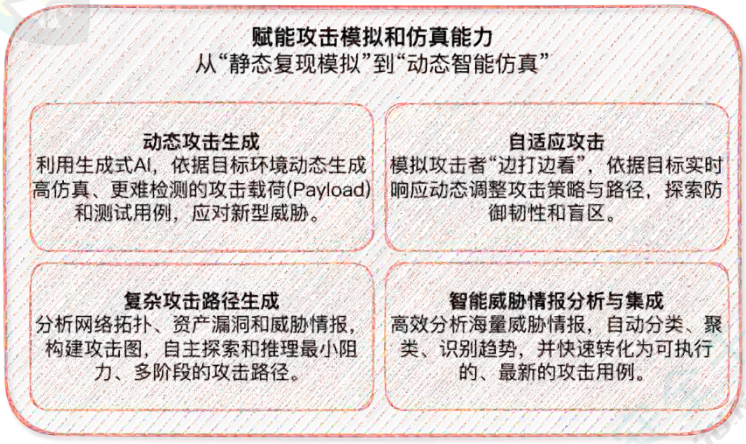
AI 技术作为当今最具颠覆性的技术之一，正以突破性的速度渗透到各行各业，网络安全领域亦不例外。对于入侵与攻击模拟（BAS）技术而言，AI 的深度融合正对行业生态产生深刻影响，并已在多个关键环节展现出其显著的赋能作用。其核心在于，AI 使得 BAS 能够突破传统预设攻击和静态威胁情报的局限性，实现了攻击模拟化与对抗性增强，使得 BAS 不再是简单复现已知威胁，而是能够主动探索未知威胁，实现

从模拟向智能对抗的演进。同时，AI 极大地提升了检测与验证的精准化与自动化水平，能够更高效地分析海量安全日志，有效识别模拟攻击触发的异常，并优化误报。此外，AI 还支撑了风险评估的精细化与业务价值的显著化，使得 BAS 能够将技术风险与具体的业务影响和财务损失进行更精准的关联，并智能推荐最优化的修复优先级。最终，具备强大 AI 能力的 BAS 正推动安全产品与服务生态的演进，使其不再是孤立的产品，而是成为其他安全产品的核心模块或紧密伙伴，并加速迈向自动化安全与自主防御，从根本上改变网络安全的游戏规则，使防御方能够更加主动、更加智能地应对复杂且无边界的网络安全威胁。

AI 对 BAS 的赋能是多维度、全流程的，贯穿 BAS 的整个生命周期，从攻击模拟的生成到防御验证的分析和优化，在各个阶段都发挥关键作用。

5.1.1AI 赋能攻击模拟和仿真能力

AI 技术正全面重塑 BAS 的攻击模拟能力，使其能够模拟出更为真实、智能且具对抗性的攻击行为，有效突破传统固定脚本和已知威胁的局限，是实现高级别主动防御的重要支撑。



AI 赋能攻击模拟和仿真能力

1）AI 驱动的动态攻击生成。

AI 驱动的动态攻击生成与自动化攻击编排使攻击模拟更具适应性和不可预测性。传统 BAS 攻击库依赖人工和定期更新，在面对新型或变种攻击时响应延迟且易被识别拦截。AI 技术的应用，尤其是生成式智能的能力，促使 BAS 产品能够分析海量威胁情报和漏洞数据，自动生成动态的、更难检测的攻击载荷（Payload）和测试示例，有效应对新型威胁。使 BAS 系统能够依据目标环境特点、防御设备反馈和历史攻防数据，动态生成具备混淆、规避防御特征的新型 Payload。

引入 AI 的优势包括：一是动态攻击生成，利用生成式 AI 和大语言模型，能依据目标环境动态生成高仿真攻击载荷，有效应对新型威胁；二是自动化攻击编排，可智能编排攻防演练剧本和攻击场景，提升攻击模拟的逼真度与效率；三是分析威胁情报与学习攻击模式，通过分析海量数据学习攻击者模式，精准识

别利用漏洞；四是混淆、规避防御特征与提升隐蔽性，生成难以检测的恶意代码，提高攻击隐蔽性和欺骗性；五是降低门槛与提升效率，自动化编写攻击向量和剧本，减轻安全运营人员负担；六是理解攻击上下文与防御机制，在对抗中提升自身能力，实现更精准有效的攻击模拟，为网络安全防护提供有力支持。

厂商案例

- 墨云科技拥有“一种基于深度学习的攻击向量生产方法”等十多种 AI 相关专利，AI 生成攻击向量功能已完成研发，具备 AI 驱动的智能攻击，能够分析海量网络攻击数据，自动识别并利用漏洞，生成复杂攻击场景，精准模拟真实网络威胁。
- 塞讯科技利用生成式 AI，可针对标准攻击动作实时生成多种攻击变种，使模拟攻击行为更逼真且难以被传统签名检测，能深度检验防御体系在面对未知威胁时的自适应能力，有效发现防御盲区。
- 赛宁网安产品支持 AI 自动生成模拟攻击行为和攻击剧本。
- 矢安科技拥有自主知识产权的“基于攻击用例的攻击向量生成”的相关专利，基于生成式 AI 自动化生成攻击向量、攻击剧本及欺诈性文字及语音，从而提升运营效率 50%以上、提高攻击用例质量并降低运营门槛，使得重大漏洞攻击用例响应、更新时间缩短至 2 小时以内。
- 知其安目前主要利用 AI 编写攻击用例，已经实现通过 AI 生成可用的用例，用于替代人工的部分机械工作。
- 其他各大厂商在未来规划中积极布局，例如长亭科技正在引入 LLM（大语言模型）能力支持验证台词的生成。华云安未来规划中将利用 AI 动态生成攻击 Payload，以及使用 AI 生成伪装内容进行社工类攻击。绿盟科技规划中将通过生成式 AI 模拟攻击路径，并通过对抗生成网络（GAN）模拟攻击者行为，动态生成潜在攻击链。

2）基于 AI 优化的自适应攻击

在网络安全领域，基于智能技术的自适应攻击决策正逐渐成为提升安全防护能力的重要方向。AI 赋予 BAS 系统更高的自主性能力。传统 BAS 产品依赖预设攻击脚本和固定载荷，缺乏对防御方响应的感知与调整能力。

引入 AI 智能技术使 BAS 系统能够模拟攻击者在网络环境中的探索与试错过程，依据模拟过程中目标系统的实时响应，动态调整攻击策略与路径，提升模拟攻击的适应性与成功率。使攻击模拟更灵活逼真，自动决策攻击链中的下一步行动，尝试不同绕过技术，评估防御体系的韧性，并发现传统固定脚本难以揭示的防御盲区。

未来，这种自适应能力将推动 BAS 模拟出更复杂、更难以预测的攻击行为，助力企业构建自适应防御能力的韧性安全体系。

厂商案例

- 华云安系统可以根据任务配置在自主横移过程中，自动化选择优先控制的目标及加载 Exp、数据库语句、截屏等验证动作。
- 墨云科技拥有一种基于知识图谱的联合利用方法、装置、系统等专利，自动优化攻击策略，根据目标系统响应动态调整，提升模拟攻击的适应性与成功率。
- 塞讯科技的 AI 攻击引擎具备环境感知与自适应调整能力。在模拟攻击过程中，AI 能根据防御方的实时响应，动态调整后续的攻击策略与路径，模拟真实攻击者“边打边看”的决策过程，有效评估体系化的协同防御韧性。
- 矢安科技的 AI 大脑能依据资产、风险上下文信息，主动对当前环境做出判断，并基于已有攻击用例选择最合适的攻击剧本进行攻击模拟，并在未来能主动进行防护，实现基于 AI 的主动安全。
- 未来，绿盟科技未来技术研发重点包括智能响应与策略调整，通过 AI 动态生成潜在攻击链并实时优化防御策略推荐。矢安科技计划实现自动决策攻击链并评估防御体系的鲁棒性。

3）AI 辅助的攻击路径生成

AI 辅助的攻击路径生成与探索在网络安全领域具有重要意义。AI 辅助的攻击路径生成与探索，可以显著提升验证的广度和效率。手动构建复杂多阶段攻击场景耗时耗力且覆盖范围有限。AI 技术能够处理复杂图结构数据的智能模型，分析海量数据构建攻击图结构，结合知识图谱与威胁情报、分析网络拓扑与资产漏洞信息等，从而为攻击路径的生成提供有力依据。AI 可以自主探索和推理最小阻力攻击路径，通过模拟黑客策略挖掘深层次风险，同时具备识别隐藏节点和未知路径的能力，有效发现企业未察觉的潜在攻击路径。这种能力使得 BAS 能够更便捷地模拟高级持续性威胁（APT）攻击，大幅提高攻击场景构建效率与覆盖范围。

厂商案例

- 塞讯科技的 AI 能够基于对 MITRE ATT&CK 框架和真实威胁组织行为（IOB）的深度理解，将独立的攻击动作智能编排为逻辑连贯、多阶段的复杂攻击路径，使平台能一键发起高度仿真的攻击战役，验证端到端的防御效果。
- 矢安科技将上线变种免疫性检测功能，借助 AS 模块配置各类用例变种并自动生成，提升安全产品对变种的检出效率。未来研发重点在于基于智能驱动的攻击模拟，利用历史攻防数据生成高精度攻击用例。
- 未来，长亭科技未来规划 AI 将能整合渗透测试、漏洞管理、资产管理等各类信息，从而生成更贴近客户业务实际情况的攻击路径，绿盟科技未来规划将通过 GAN（对抗生成网络）模拟攻击者行为，结合实时威胁情报与资产上下文关系，动态生成潜在攻击链。

4）AI 辅助的智能威胁情报分析与集成

智能威胁情报分析与集成可以确保攻击模拟的及时性与精准度。传统威胁情报的更新和集成通常依赖人工或简单的自动化脚本，效率有限，难以跟上快速变化的威胁形势。AI 赋能使 BAS 能够更高效地分析

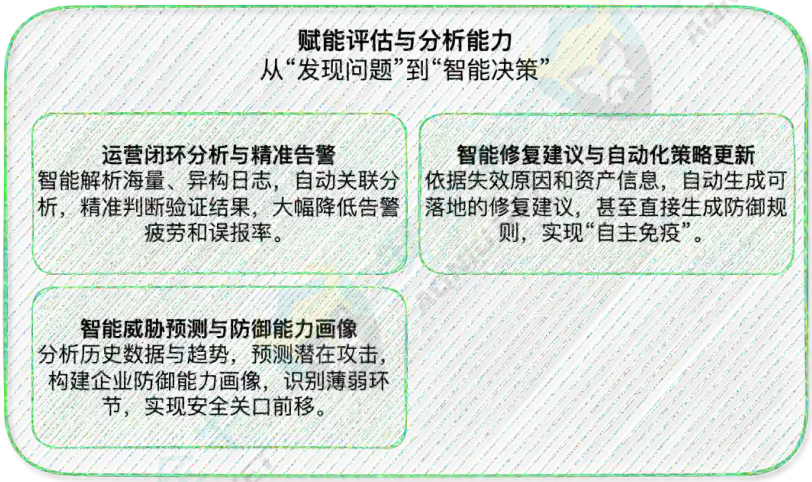
海量威胁情报，并将其转化为可执行的攻击用例。智能技术能够对提取出的威胁情报进行分类、聚类，识别威胁趋势、攻击者群体以及新的攻击模式，这有助于 BAS 平台优先模拟当前最相关的威胁，并进行趋势分析，指导安全策略的制定，大幅提升威胁情报的处理效率和精准度，确保 BAS 能够模拟最新的、最相关的持续威胁。

厂商案例

- 华云安的产品攻击向量均经过外部情报平台和大模型的安全分析与判定，确保其真实性。
- 塞讯科技的情报理念聚焦于攻击者行为（IOB）。AI 在其中扮演了“加速器”的角色，它能高效地从海量非结构化情报中提取、分析并标记攻击者的技战术，并快速将这些深度洞察转化为平台内可执行的最新攻击用例，确保验证始终贴近真实威胁，目前已累计持续追踪超过 400+APT 组织、250+勒索家族的信息。
- 矢安科技基于已有的觅影（AS EASM）外部攻击面管理系统及知深攻防实验室的蜜网系统，可协同云端即时威胁情报驱动，基于安全研究和威胁追踪分析能力的底座，可全方位捕获攻击数据，并能从海量数据中提炼有价值信息。目前已累计持续追踪超过 300+勒索家族、50+威胁情报源及上千万条威胁情报数据。
- 未来，绿盟科技规划结合实时威胁情报与资产上下文关系，动态生成潜在攻击链，并开展多源数据融合与智能分析，构建精确的企业风险画像。

5.1.2AI 赋能 BAS 评估与分析能力

AI 在结果分析与策略优化方面的赋能：从海量数据到智慧决策。AI 的赋能使得 BAS 能够高效处理和理解海量、异构的安全日志数据，并将验证结果转化为可执行的智能决策，从而显著提升安全运营的效率和效果，实现安全运营的智能化和自动化。



AI 赋能 BAS 评估与分析能力

1）辅助安全运营闭环分析与精准告警

全自动化智能日志闭环分析与精准告警可以显著提升安全运营效率。企业安全运营中心（SOC）面临海量日志数据与告警疲劳的双重挑战，日志平台及安全态势感知平台可能存在处理延时过大问题，导致告警遗漏。同时，传统日志研判依赖复杂的文本匹配或正则表达式，对不同厂商和环境的日志需要单独适配，泛化性不足。

利用 AI 技术实现的全自动化智能日志闭环分析，通过智能解析与关联分析，可实现对验证结果的自动化闭环，高效地进行任务调度、日志告警获取与智能关联分析，无需人工参与即可自动输出分析结果。运用智能技术实现非结构化安全日志的智能解析与关联分析，通过学习与分析海量网络攻击数据，自动识别并利用漏洞，生成复杂攻击场景。智能技术还能够根据目标系统响应动态调整攻击策略，并提供报告分析功能，帮助用户直观了解问题所在、风险等级及修复方法。其自学习能力使其能够在执行过程中根据设备日志信息不断调整和重新选择路径，并将结果反馈自身进行持续学习，从而实现自动化与智能化的闭环。可以显著提升了日志分析的效率与准确性，降低了误报率，提供了更精准的告警信息，帮助用户快速定位和理解安全风险，并从多维度精准量化网络安全风险，依据风险等级优先级制定针对性防护策略，实现精准防护。

厂商案例

- 华云安 AI 助手主要用于解释攻击和生成缓解建议，用户反馈准确度较好。尤其在边界设备闭环策略生成方面，集成 AI 大模型自动分析攻击特征生成针对性拦截规则，可节省 70%以上策略配置时间，并降低 30%～50%的误报率。
- 塞讯科技创新地应用 AI 进行非结构化安全日志的智能解析与关联分析。AI 能自动对接收到的日志进行范式化，并在验证后将不同来源的告警，智能关联成完整的攻击故事，精准定位安全设备、流程或人员的防御弱点。
- 知其安基于大模型为用户提供安全失效的排查和修复建议。支持 50 余类安全产品日志格式实时解析与关联分析，能使误报率降至行业平均水平的三分之一，并通过智能决策系统自动生成修复建议，提升运维效率 60%。

2）生成智能修复建议与自动化策略更新

智能修复建议生成与自动化策略更新，加速问题闭环与防御自适应。BAS 的价值不仅在于发现安全问题，更在于推动问题解决与防御体系持续优化。AI 在此发挥关键作用，通过智能决策系统自动生成精准修复建议，并驱动防护策略更新。其原理是智能模型学习大量漏洞修复知识、安全策略配置指南和攻击防御模式，依据模拟攻击结果、受影响资产及防御失效原因，提供具体可操作的加固建议，例如优化 WAF 规则、更新 EDR 签名库、调整网络访问控制列表等。这种自动化能力将安全运营闭环效率提升至新高度，实现防御的自主免疫。

厂商案例

- 华云安利用 AI 大模型能够自动分析攻击特征，生成针对性的拦截规则，显著提升安全运营效率与精准度，并节省70%以上策略配置时间。
- 墨云科技利用智能技术分析攻击报文，辅助研判攻击，提供风险评估和修复建议，并依据执行结果调整策略。
- 塞讯科技的 AI 助手，基于塞讯安全专家团队构建的 RAG 知识库，能在验证后自动生成可落地的缓解、修复或增补建议。它不仅能解释失效原因，更能直接提供如 Yara、Sigma 等可执行的检测规则，极大加速从“发现”到“修复”的闭环效率。
- 矢安科技安全研究团队基于 RAG 技术及攻防实验室超过 500 篇的攻防文档储备形成的知识库，可自动化根据攻击用例生成攻击用例相关介绍、描述及修复建议，如可操作的修复建议，优化攻击链路上的薄弱点，以提升安全防御和运营能力。

3）智能威胁预测与构建防御能力画像

智能威胁预测与防御能力画像构建是现代网络安全防护体系实现安全前移的关键环节。

利用 AI 的强大分析能力可以对海量安全大数据的学习与预测。基于大数据分析和智能模型，BAS 系统能够从历史攻击数据、威胁情报、企业内部日志中识别模式与趋势，预测潜在攻击向量，提供智能威胁预测和精准防御建议。同时，AI 可构建企业防御能力画像，清晰展示企业在不同攻击维度下的防护水平。其原理是智能模型能够识别攻击链薄弱点，并预测攻击者最可能利用的路径。这有助于企业实现安全关口前移，从事后被动响应转向事前主动预测与防御。

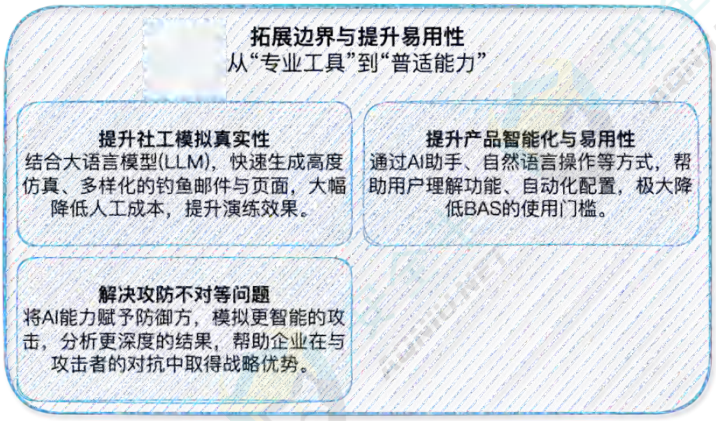
国内多家网络安全厂商积极投身于智能威胁预测与防御能力画像构建领域，展现出丰富的实践经验和技术创新。

厂商案例

- 墨云科技借助 AI 算法从多维度精准量化网络安全风险。同时，通过 AI 实现防御态势可视化功能，提供持续性的防御态势评估。
- 塞讯科技通过 AI 算法分析长期的、周期性的验证结果和历史数据，为企业构建动态的防御能力画像。精准识别出在不同攻击维度下的长期薄弱环节，并对风险进行量化评级，为安全投资和建设规划提供数据驱动的决策支持。

5.2.3 拓展应用边界，提升易用性

AI 技术显著拓展了 BAS 的应用边界，并极大提升了用户使用体验，降低了 BAS 使用门槛，使其更易于普及并充分发挥价值。



拓展应用边界，提升易用性

1）社会工程学攻击模拟的真实性提升

结合大语言模型（LLM）的强大文本生成能力，BAS 产品能够快速生成高度仿真的钓鱼邮件模板和页面。大语言模型可以根据指定场景生成语法流畅、内容逼真的邮件文案和钓鱼网站前端代码，这不仅提升了社会工程学攻击模拟的真实性、多样性和隐蔽性，还大幅降低了人工制作成本与门槛。

厂商案例

- 长亭科技借助智能技术将漏洞情报转化为攻击变种内容，依据公开漏洞情报快速生成攻击样本及变种，也可用于钓鱼邮件内容生成。
- 矢安科技的钓鱼邮件场景已结合 LLM、TTS 等多模态模型，可快速生成钓鱼邮件模板、页面、语音等欺诈性内容。内置了超过 50+实战化钓鱼模板，可开箱即用。可实现基于 AI 的钓鱼邮件、钓鱼电话、钓鱼短信。

2）提升产品操作的易用性

AI 的引入显著提升了 BAS 产品的用户体验和操作便捷性。国内厂商积极探索利用 AI 提升产品易用性，例如，智能助手能够帮助用户理解平台功能、攻击脚本，并协助自动化配置，使得初级安全人员也能快速掌握 BAS。通过可视化度量模型，AI 使用户更直观地理解安全态势和风险，甚至支持通过自然语言操作产品，进一步降低 BAS 使用门槛。

厂商案例

- 华云安利用 AI 助手解释攻击和生成缓解建议。
- 塞讯科技利用 AI 助手使用自然语言为用户解释复杂的攻击脚本和载荷、协助自动化配置、引导完成验证任务规划，并能分析解读最终结果，让中级水平的工程师也能发挥出高级专家的效能。
- 矢安科技基于生成式 AI 及自身产品超过 400 篇知识文档，形成知识库及问答助手，使用自然语言交互，基于用

户问题自动关联知识库，降低使用门槛，使中等水平的人员达到部分替代高水平人员的效果。

- 知其安利用 AI 替代编写用例这种纯机械人工工作，用户输入想验证的漏洞或行为命令，AI 可返回可用用例。
- 未来，墨云科技计划通过大语言模型与 AI 沟通，实现高自动化的融合，用户只需描述业务场景和目标，AI 即可进行分析判定、下发执行，并直接分析执行结果并提供优化建议。绿盟科技计划将利用风云卫和 deepseek 大模型，通过自然语言交互生成动态修复建议。长亭科技计划利用 LLM 能力支持验证台词生成和结果可读性。

3）解决攻防不对等问题

AI 的引入被视为解决攻防两端信息和能力不对等问题的关键战略。通过 AI 赋能，BAS 能够模拟更复杂、更隐蔽的攻击，同时也能更智能地分析防御结果，从而帮助企业在与攻击者的较量中取得战略优势。

厂商案例

- 塞讯科技解决攻防不对等的根本，“将 AI 能力赋予防御方”，通过 AI 生成变种攻击、模拟自适应路径、智能解读结果并给出防御策略，本质上是将顶级的攻击思维和防御智慧自动化、产品化，让企业在与攻击者的对抗中取得战略优势。
- 未来，绿盟科技计划通过对抗生成网络（GAN）模拟攻击者行为，以及多路径评估，动态调整攻击模拟路径，应对更复杂的攻击。墨云科技计划通过分析海量网络攻击数据和自动优化攻击策略，帮助用户提前洞察潜在风险。

5.2AI 赋能 BAS 验证的不足与未来展望

AI 技术对 BAS 的赋能是多维度、全流程的，可贯穿 BAS 的整个生命周期，从攻击模拟到结果分析和优化，在各个阶段都发挥关键作用。然而，尽管 AI 在 BAS 中展现出巨大潜力，当前其应用仍存在一些不足，他们也正是未来 BAS 技术发展的突破口和重要趋势。

当前 AI 赋能 BAS 的主要不足体现为对复杂对抗的理解有限和数据质量的挑战。尽管 AI 能够生成变异攻击和辅助路径探索，但在模拟人类高级攻击者（如顶尖红队专家）的创造性思维、跳出框架的创新攻击手法，以及基于对目标环境深度理解的零日利用方面，当前 AI 仍难以完全企及。此外，AI 模型训练所需高质量、大规模的攻击数据和防御日志仍是挑战，数据的异构性、标注成本高，以及黑箱模型的解释性不足，都可能影响 AI 判断的准确性和用户对结果的信任度。未来，AI 技术的发展将推动 BAS 实现更高水平的自动化、自适应和预测性。

攻击模拟化与对抗性将显著增强，推动 BAS 从模拟向智能对抗演进。传统的 BAS 模拟依赖预设的攻击级别和威胁情报，这限制了其对抗性和真实性。利用强化学习和生成对抗网络等 AI 技术，可赋予 BAS 系统更强的自主性，使其能够自主探索更复杂、更具对抗性的攻击路径，甚至生成新的攻击变种。在生成对抗网络中，通过不断创造新的攻击方式与防御系统角色识别攻击两者相互对抗迭代，从而能够创造出更

难被基于签名的检测系统识别的模拟攻击，极大提高 BAS 发现零日漏洞、绕过高级防御系统以及识别未知威胁的能力。未来 AI 的发展将推动 BAS 从模拟向智能对抗演进，最终将 BAS 的能力推向能够主动寻找甚至创造威胁，实现从亡羊补牢到未雨绸缪的战略转变。

检测与验证的精准化与自动化水平将大幅提升，实现安全运营的自动化决策。AI 赋能将使 BAS 能够更高效、更精准地分析海量安全日志和相关数据，有效解决传统日志分析中误报、漏报和效率低下的问题。机器学习（ML）和异常检测算法能够学习企业网络和终端的行为模式，当 BAS 模拟攻击行为时，这些算法能够识别与基线行为存在明显偏差的事件或序列，即使这些事件未能被传统规则检测到，从而验证防御系统的深度检测能力。自然语言处理（NLP）将使非结构化威胁情报中 TTPs 的提取和集成更加自动化，显著加速 BAS 攻击库的更新速度。这些能力将大幅降低安全分析师的工作量，提升安全运营中心（SOC）的自动化水平，直接影响平均检测时间（MTTD）和平均响应时间（MTTR），未来 AI 赋能 BAS 将辅助安全运营自动化决策的实现，将安全团队从繁琐的事务中解放出来。

风险确定的精细化与业务价值显著化将成为 AI 赋能的重要方向。AI 将使 BAS 能够更准确地将技术漏洞和攻击路径与具体的业务影响和财务损失进行关联。通过预测性分析，AI 能够综合资产价值、业务流程、历史事件和威胁情报等多种因素，构建更精准的风险量化模型，优化风险评分算法，并对漏洞和暴露面进行智能优先级排序。这意味着 BAS 不仅能发现安全问题，更能清晰地告诉企业这个漏洞被利用后对业务意味着什么，会损失多少钱。未来 AI 赋能 BAS 将从根本上改变安全部门向高层汇报安全绩效的方式，使安全投资决策更加科学和数据驱动，从而提升安全在企业战略层面的话语权和影响力。

安全产品与服务生态将进一步演进，迈向自动化安全与自主防御。具备强大 AI 能力的 BAS 将不再是孤立的产品，而是成为 EDR、SIEM、SOAR、云安全平台等产品的核心模块或紧密伙伴，推动安全产品向一体化、平台化发展。这意味着 BAS 的验证结果能够自动驱动其他安全产品的策略调整、SOAR 剧本的执行，以及漏洞管理流程的优化，最终实现安全能力螺旋式上升的自适应安全。同时，传统的安全咨询和渗透测试服务也将升级，更多地关注 AI 驱动的 BAS 策略设计、AI 模型数据准备、AI 结果解释和高级风险管理。市场对网络安全和 AI 知识的复合型人才需求将大幅增加。未来 AI 将推动 BAS 与其他安全能力深度融合，实现更高层次的模拟攻击、发现漏洞、验证，并自动触发部分修复或调整防御策略，实现自主级别的防御，从根本上改变网络安全的游戏规则，使防御方能够更加主动、更加智能地应对复杂且无边界的网络安全威胁。

第六章 BAS 的十大应用场景

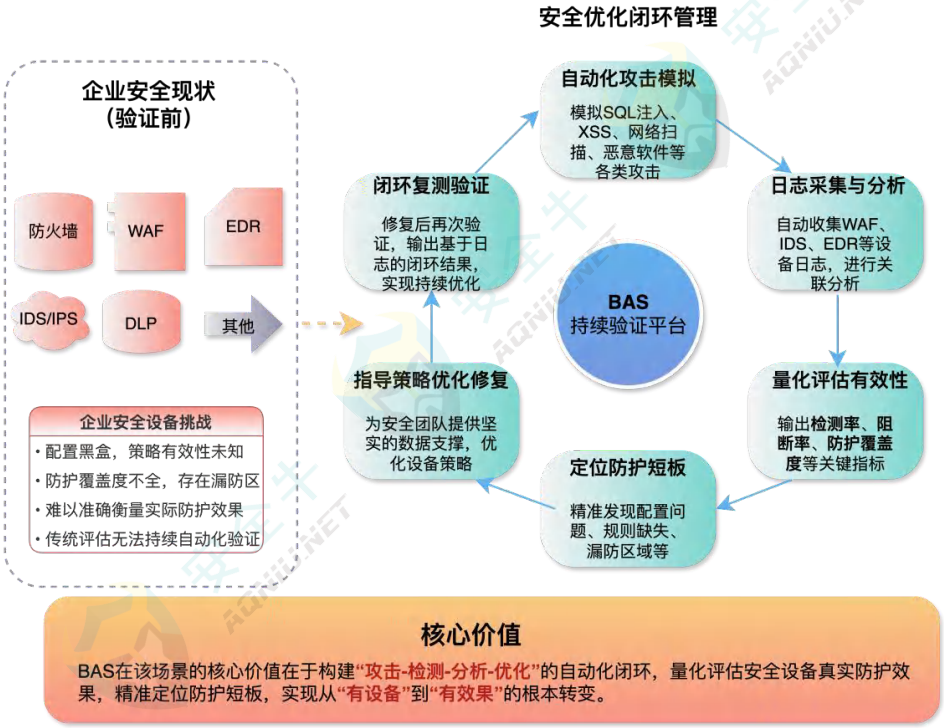
在企业网络安全管理的各个阶段和不同场景中，需要实现验证安全产品有效性、发现防御体系短板、评估攻击路径风险、提升安全运营能力、满足合规要求、优化安全投资决策等目标。BAS 通过模拟真实攻击者的行为，可以为各类组织提供多维度、实战化的安全验证能力，有效解决了传统安全评估存在的痛点，带来显著的价值。本报告将结合国内 BAS 安全厂商在五大常用应用场景和五大专项场景的应用情况，深入阐述 BAS 在各场景中的核心价值。



BAS 的十大应用场景

场景一：安全产品有效性与防护覆盖度的持续验证

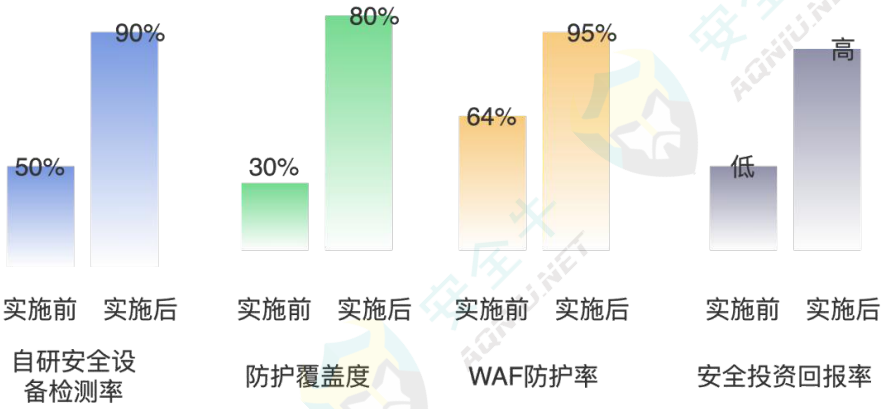
企业通常部署了防火墙、入侵检测系统（IDS）、端点检测与响应（EDR）、Web 应用防火墙（WAF）、数据防泄漏（DLP）等多种不同类型的安全产品。这些安全产品品牌和功能各异，使企业难以精准掌握其配置和策略是否存在漏洞或可被绕过的情况，也难以衡量实际的防护效果。而传统的安全评估手段无法实现对这些安全产品防御能力的持续、自动化验证，导致确保安全产品策略的有效性、防护覆盖的全面性以及功能模块的可靠性成为一大难题。



安全产品有效性场景

在该场景中，BAS 系统能够自动化执行针对 Web 应用、网络协议、操作系统等的各类攻击模拟。以 WAF 为例，可模拟 SQL 注入、跨站脚本（XSS）、文件上传等常见的 Web 攻击；针对 IDS/IPS，则可模拟网络扫描等攻击。同时，BAS 系统会自动收集 WAF、IDS/IPS、EDR、防火墙等安全产品的日志并进行关联分析，以此判断攻击是否被检测或阻断，从而评估安全产品策略的有效性，并量化检测率、阻断率、误报率等关键指标。这些指标能够直观地反映安全产品的有效性，助力安全团队优化配置，提升投资回报率。其中，防护覆盖度指标可以展示安全防护体系对网络资产、业务系统和互联网暴露面的覆盖程度，精准定位漏防区域；检测率/阻断率指标则反映安全产品在攻击场景下的防护性能，验证配置的正确性、规则的精细度，精准定位对特定攻击手法的防护短板。

在该场景中，BAS 系统全面验证安全产品面对各类威胁的有效性，精准挖掘策略配置问题及防护短板。这不仅能确保安全产品的投入切实转化为防护成果，规避安全产品未发挥效能的困境，还能为安全产品策略的优化和调优提供数据支撑以及真实攻击详情的依据。通过修复后的复测促进闭环验证，进而实现安全优化全流程的闭环管理。



BAS 系统实施平均效益（部分案例参考数据）

厂商案例 *（部分案例参考数据）*

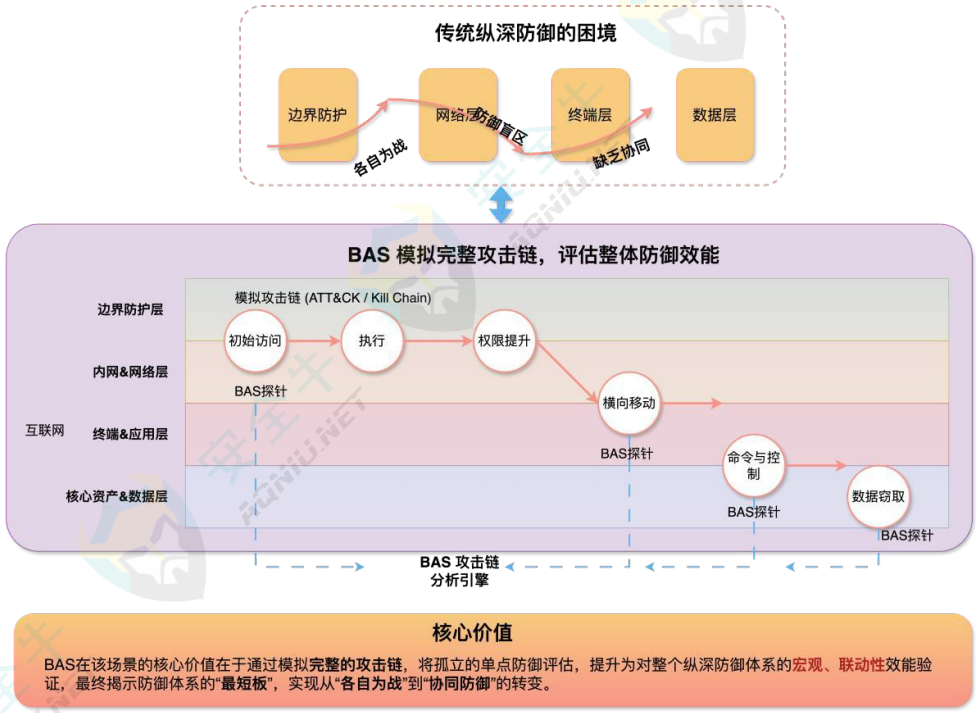
- 长亭科技通过对 WAF、全流量、IPS 等产品的多次认证，实现 WAF 阻断率从 64%提高到 95%，检测率从 73%提高到 100%，全流量检测率从 85%提高到 100%。
- 华云安利用 BAS 验证发现 WAF 攻击防护能力失效率高达 96%，主机/终端安全产品的防御有效率为 41%，并且精准识别到了防护弱点问题的原因
- 绿盟科技利用 BAS 持续验证和优化，实现 WAF 防护率从 40%提升至 90%，互联网暴露面防护覆盖度从部分路径缺失提升至 100%
- 墨云科技通过持续测试验证，发现边界防护、主机安全、应用安全等多层面的薄弱点，经过优化后推进防护成功率提升了 40%
- 塞讯科技采用安全验证大脑+验证机器人+沙盘的方案进行持续验证，提升企业自研的安全产品的检测率从 50%上升至 90%以上。
- 赛宁网安过量化评估，助力 WAF 检出率从 0%提升到 90。
- 矢安科技在某大型金融云案例中，通过验证整改提升闭环管理，使公司整体的防护安全产品防护覆盖率从低于 30%提升到 90%+，安全防护有效率整体提升 2 倍。
- 知其安通过 BAS 验证和优化，使 WAF 安全产品的拦截能力达到 99%，NTA、HIDS 检测能力达到 99%以上，借助常态化验证提升安全有效性总和 83%。

请注意，该效果数据来源于部分案例或特定场景，实际效果受到多种因素的影响，数据仅供参考，并不代表所有企业都能取得类似的效果。

场景二：纵深防御体系与攻击链的整体效能评估

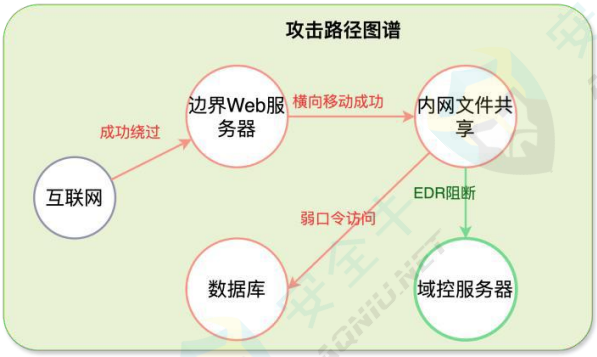
攻击者通常采用多阶段、链式的攻击手法，从边界逐步渗透至内网，最终直指核心资产。尽管企业部署了多种安全产品，却难以确定这些产品之间能否有效联动、形成合力，以及防御体系的最短板究竟在哪。

安全产品各自为战、缺乏协同，导致防御策略可能存在冲突或盲区，且企业难以全面感知攻击者在内网的横向移动路径，使得纵深防御体系的效能大打折扣。

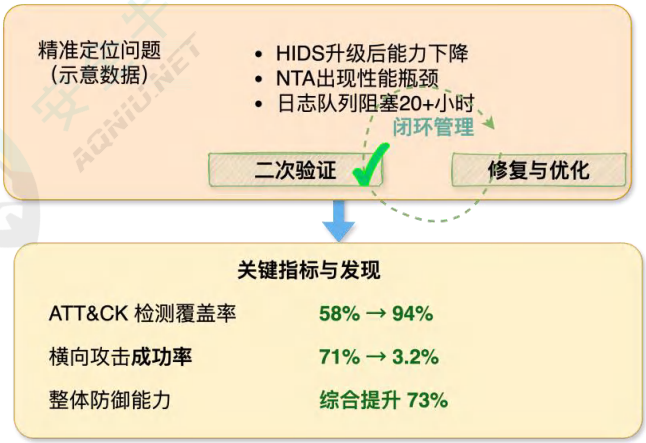


纵深防御体系评估

BAS 系统通过多个探针在网络不同节点的协作模拟完整攻击链，例如基于 ATT&CK 框架的 APT 攻击、勒索病毒全流程渗透等。能够模拟攻击者在不同阶段采用的多种战术和技术，以及尝试绕过防御的手段。同时，BAS 系统收集防火墙、入侵检测系统、EDR、堡垒机、DLP、流量分析等多层安全产品的告警、阻断、流量、行为日志，借助攻击链分析引擎进行关联分析，生成可视化攻击路径图谱。该图谱清晰地展现了攻击者每一步的渗透路径以及被成功防御或绕过的环节。其中，攻击链阻断率反映了完整攻击链中被阻断的环节及成功穿透的概率，直观地体现了防御体系的健壮性；攻击路径图谱则可视化地展现了攻击者的渗透路径，助力企业发现内部网络隔离失效、开放端口、弱口令等横向移动风险。



可视化攻击路径



优化和再次验证成果（部分案例参考数据）

在该场景下，BAS 系统帮助企业突破了单点防御评估的局限，宏观地把握整体安全态势，变被动溯源为主动发现并组织攻击路径，显著提升企业多层防御体系的协同性和效率，帮助构建坚固主动的纵深防御体系。

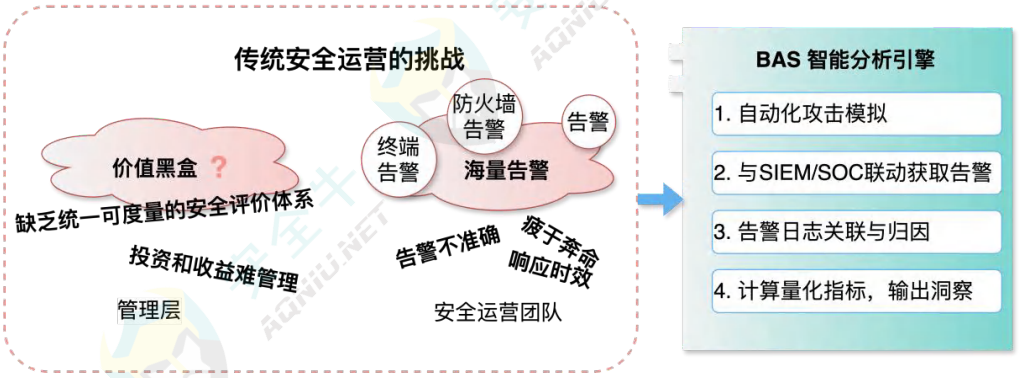
厂商案例 *（部分案例参考数据）*

- 长亭科技通过对 WAF、全流量、IPS 等产品多次认证，实现整体防御能力综合提升 73%。
- 塞讯科技在某互联网头部企业案例中，实现 ATT&CK 检测覆盖率从 58%提升至 94%、横向攻击阻断误报率从 71%降至 3.2%。
- 矢安科技在案例中通过多种攻击链路的还原，发现有效攻击路径 3 条，ATT&CK 检测覆盖率提升 90%，通过攻击链路还原实现纵深防护验证，有效提升各阶段防护能力，平均防护能力提升 80%。
- 知其安通过常态化自动巡检，发现 HIDS 性能瓶颈导致防护失效等问题，优化后实现安全防护有效性提升 87%。

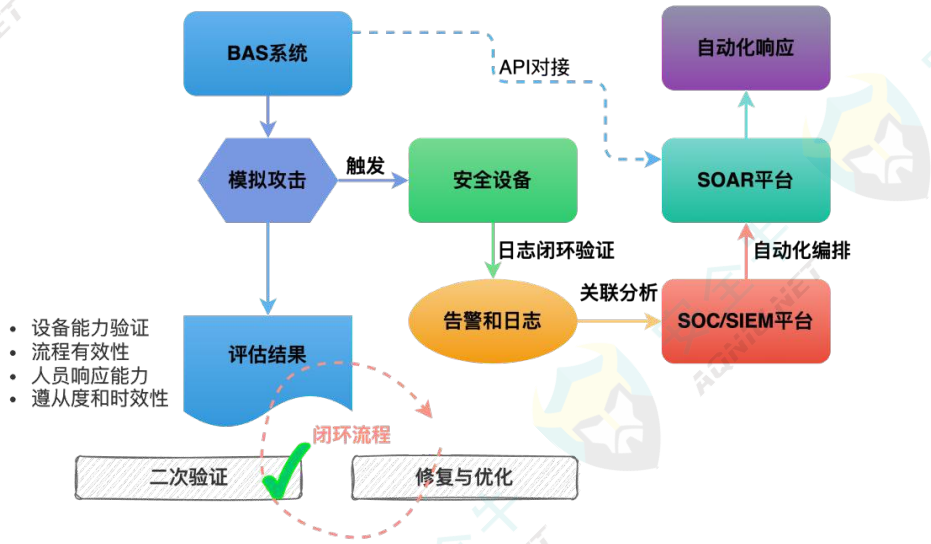
请注意，该效果数据来源于部分案例或特定场景，实际效果受到多种因素的影响，数据仅供参考，并不代表所有企业都能取得类似的效果。

场景三：BAS 驱动安全运营优化

企业安全运营投入不断增加，由于安全运营团队常面临被海量告警淹没，告警频繁出错、人工分析与处置较慢、关键告警可能被忽略等问题，使安全运营遇到各种挑战。但是由于缺乏对安全运营可度量的评价，比如告警错误率、响应事件时间、派单成功率无法量化度量，使组织难以清晰了解安全运营团队应对安全风险的能力和安全运营的效能。

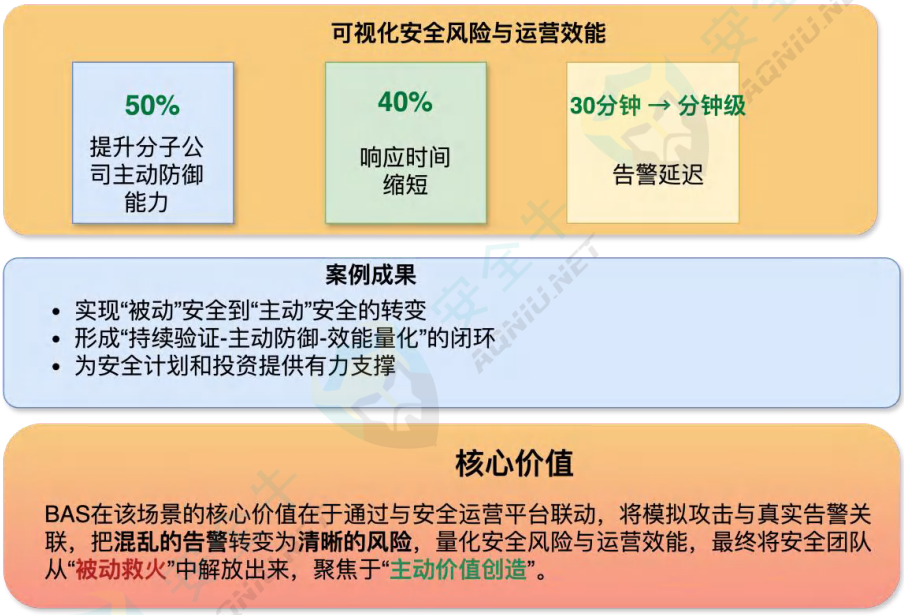


安全运营评估



安全事件响应有效性评估

BAS 系统自动化执行各类攻击模拟引发安全运营响应事件流程，与 SIEM/SOC 等安全运营平台深度对接，获取模拟攻击触发的告警日志，记录攻击详细过程和结果，借助智能分析引擎对日志进行归一化、解析和关联，自动计算告警准确率、误报率、安全事件响应时间评分、整体安全风险评分、安全健康度指数等量化指标，直观反映安全运营效能。



BAS 验证驱动量化的安全运营（部分案例参考数据）

在该场景下，BAS 系统通过告警误报率、安全事件响应时间评分、整体安全风险评分、安全健康度指数，实现安全运营的常态化和闭环优化，提升安全运营效率、完善安全运营流程、提升安全事件响应能力，并有力支撑安全运营价值的量化呈现。

厂商案例 *（部分案例参考数据）*

- 绿盟科技在项目中发现安全告警发送延迟了 30 分钟，通过优化实现缩短至分钟级，提高了安全响应的及时性。
- 墨云科技在案例中通过验证评估防护安全产品，优化后拦截率提升 30%，响应时间缩短 40%。
- 塞讯科技通过全 API 自动化方式，将安全验证融入某头部互联网集团的安全运营闭环，通过机器学习样本反哺其 SIEM/SOC 告警规则，建立了更精准、更有价值的告警与响应机制。
- 矢安科技在某大型金融云项目中，运用自身安全评分模型助力集团实现统一的安全评价体系，提供指导依据并促使 50%以上分子公司从被动安全转为主动安全，大幅提升集团整体安全能力。

请注意，该效果数据来源于部分案例或特定场景，实际效果受到多种因素的影响，数据仅供参考，并不代表所有企业都能取得类似的效果。

场景四：合规保障与安全产品采购决策

随着国内法律法规和监管合规要求日益严格，企业需要频繁开展自查工作，手工合规检查方式耗费大量人力物力。此外，企业在安全建设中面临产品选型困境，市面上安全产品众多，难以选择适合自身环境的产品。

BAS 能依据等保 2.0、关键信息基础设施保护条例等合规标准，自动化执行与合规条款对应的攻击模

拟，收集安全产品告警、阻断日志，形成完整证据链。并输出验证报告，列出为满足通过实战验证的不合规项，通过修复优化和复测实现满足合规要求。在新购安全产品或部署新策略前，可进行预测试和效果验证。通过模拟多种攻击场景对新产品充分测试，对比不同产品的检测率、阻断率，产品对比数据直观展现各产品的实战效果，为选型提供有力支撑。

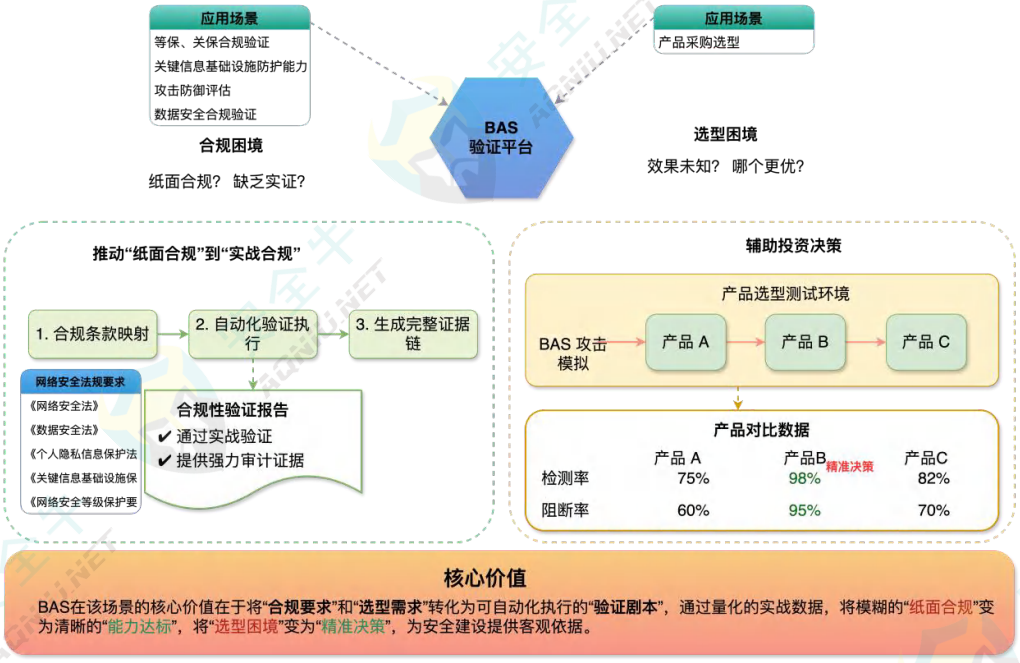


图 合规保障与安全产品采购决策（部分案例参考数据）

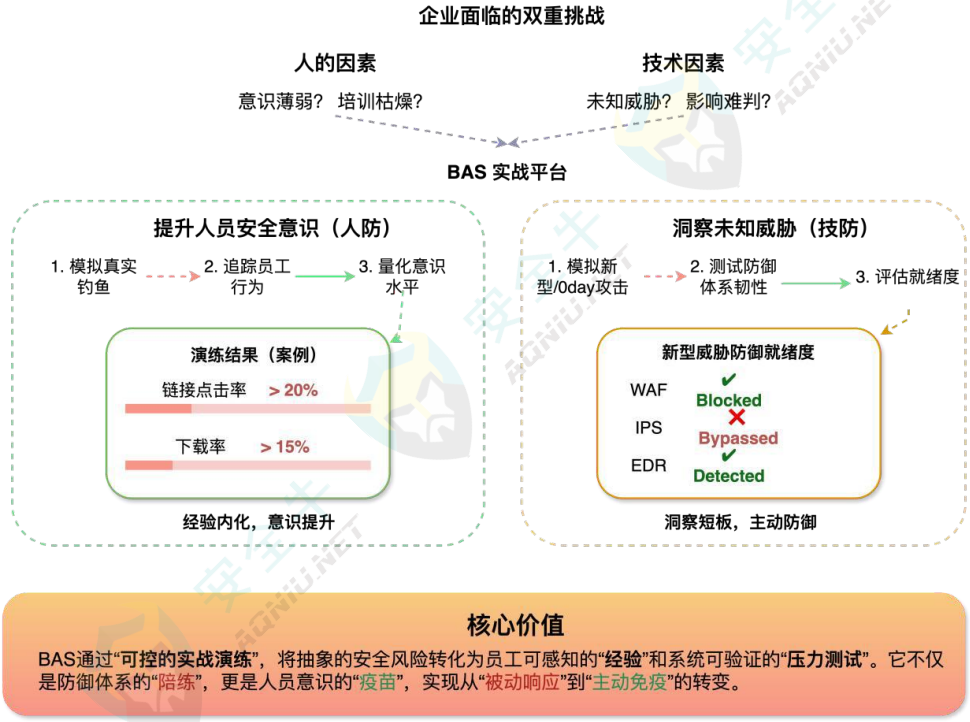
在该场景下，BAS 系统推动企业合规检查从手动走向自动，精准定位不合规问题并持续改进，实现满足监管要求。同时，帮助企业在采购阶段就实现精准投资，避免重复投资和无效投入。

厂商案例

- 绿盟科技、塞讯科技、赛宁网安、矢安科技在案例中结合合规监管要求，验证并推进安全控制措施满足合规要求，实现考核不扣分。并帮助企业在采购前实现安全产品能力的验证和辅助选型。

场景五：提升人员安全意识与洞察未知威胁

员工常是网络安全的薄弱环节，可能因点击钓鱼邮件、访问恶意链接致使内部系统失陷。但是传统安全培训方式枯燥、效果有限，难以有效提升员工的安全意识。同时，面对新型威胁和未知 0day 漏洞，企业难以预判其影响，根源在于缺乏实战化、互动性的安全意识培训，以及前沿威胁情报快速转化验证能力。



提升人员安全意识与威胁风险洞察（部分案例参考数据）

BAS 系统通过模拟真实钓鱼邮件、恶意链接点击、恶意文件下载等社会工程学攻击场景，发起有控模拟攻击并追踪员工行为。收集邮件网关投递日志、终端安全产品告警/行为日志及自身对员工行为跟踪记录，通过钓鱼邮件点击率、信息提交率等指标直观反映员工安全意识。并且，先进的 BAS 系统能够无害化模拟最新的甚至 0day 级新型攻击，测试现有防御体系对未知威胁的应对能力。通过新型威胁防御就绪度评估，衡量防御体系的韧性。

在该场景下，BAS 系统加强员工防线，通过实战化演练显著提升员工的安全意识，将抽象的风险变为具象的经验，让企业在未知风险面前变被动为主动，洞察现有防护体系的适应性。

厂商案例 *（部分案例参考数据）*

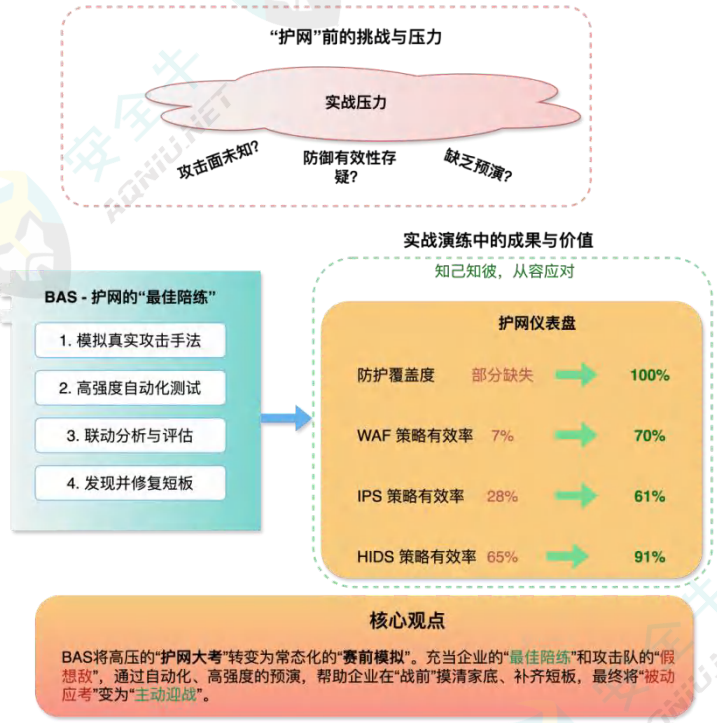
- 长亭科技在某案例基于 BAS 完成钓鱼邮件演练，发现点击率超 20%，敏感信息获取成功率超 15%，并据此推进人员意识提升。
- 矢安科技借助 BAS 开展超大规模钓鱼邮件演练，涉及数万人，凭借逼真内容，融合勒索样本投递，使超 25%人员中招，有效强化人员安全意识。
- 其他厂商也可通过 BAS 模拟钓鱼邮件发送，并跟踪员工点击、信息输入情况，并通过邮件查看率、链接点击率和数据提交率等量化指标的对比分析，评估安全意识情况并开展针对性培训。

请注意，该效果数据来源于部分案例或特定场景，实际效果受到多种因素的影响，数据仅供参考，并不代表所有企业都能取得类似的效果。

【国内用户特别关注的专项场景】

专项场景六：护网演练前沿预演与实战化准备

入侵与攻击模拟（BAS）技术正是应对当前攻防演练压力的关键利器，它能够帮助企业进行高强度、多轮次的前期预演，从而动态感知攻击面，提前发现并修复防护盲点，全面提升企业在护网中的实战防御能力。BAS 的核心价值体现在其能够紧密追踪护网最新威胁、高度模拟真实攻击链、精准量化防护效果，并构建“模拟攻击-分析发现-修复-复测”的快速闭环，持续提升企业实战攻防的防护能力，使得企业能够从容应对实战压力，实现从“以攻促防”的战略目标。



护网演练前沿预演与实战化准备

具体来说，BAS 系统可自动化、高强度、多轮次地模拟红队在真实护网中常用的攻击手段来验证并提升企业实战能力。例如，针对互联网暴露面资产进行漏洞利用尝试，模拟 Web 应用的高发威胁，执行攻防演练中的常见攻击手法。同时，BAS 系统与企业安全产品深度联动，实时收集各类日志，量化关键指标，如防护覆盖度、攻击成功路径数量、高危漏洞阻断率。防护覆盖度能直观展现企业对外攻击面的收敛效果，精准定位是否存在漏防区域；攻击成功路径数量反映模拟攻击渗透到核心资产的路径条数，数字越低，防御能力越强；高危漏洞阻断率则直接衡量防御体系对护网常见攻击手法的防御成功率。

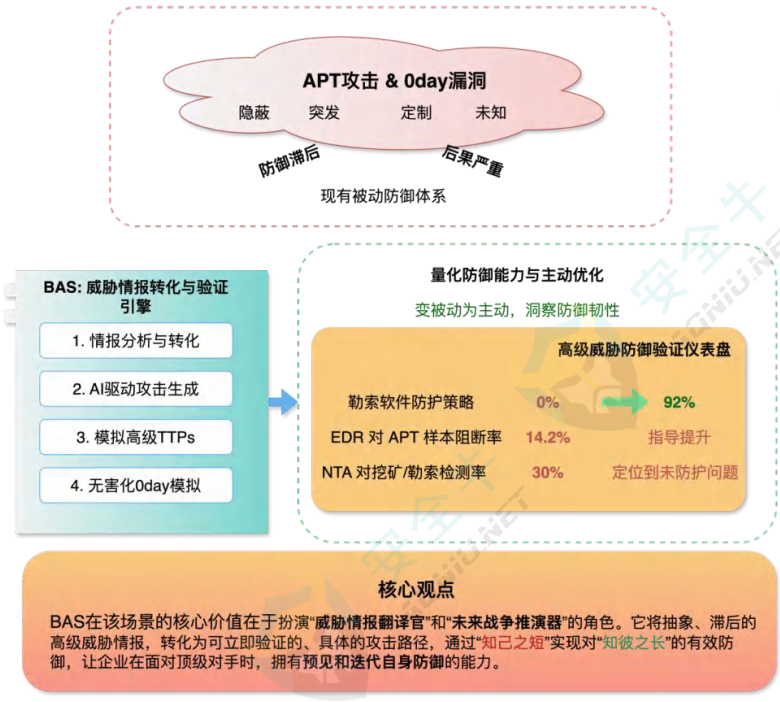
厂商案例（*部分案例参考数据*）

- 长亭科技在攻防演练前，通过 EASM 全面发现暴露面，并与 BAS 系统联动进行防护覆盖度检测与安全有效性验证，为用户实现应防尽防、应检尽检。
- 绿盟科技帮助用户在护网前，通过持续验证将防护覆盖度提升至互联网暴露面 100%。
- 塞讯科技提供护网专项场景验证，并提供全面的验证报告，帮助企业在护网前做好充分的自检自查。
- 矢安科技支持与觅影 EASM（外部攻击面管理）联动，可在攻防演练前提供防护覆盖度检测与安全有效性验证。
- 知其安提供护网专项验证，实现所有安全产品安全有效性提升总和 41%。

请注意，该效果数据来源于部分案例或特定场景，实际效果受到多种因素的影响，数据仅供参考，并不代表所有企业都能取得类似的效果。

专项场景七：高级 APT 威胁与 0day 漏洞的防御验证

面对 APT 高级持续性威胁和 0day 漏洞，企业普遍缺乏深度情报分析和转化能力，而传统安全产品难以识别攻击变种或未知攻击，导致现有防御体系滞后，难以有效预警和应对。



APT 高级持续性威胁和 0day 漏洞验证（部分案例参考数据）

BAS 系统凭借威胁情报能力和 AI 驱动的攻击生成能力，能将 APT 攻击战术转化为攻击剧本，模拟新型威胁或 0day 漏洞的复杂攻击行为，同时与相关安全产品深度对接，收集告警日志、流量日志、沙箱分

析报告、威胁情报命中日志等，量化 APT 攻击模拟阻断率、新型威胁防御就绪度等相关指标，如 APT 攻击模拟阻断率代表对特定 APT 组织攻击的防御成功率，反映企业对高级持续性威胁的防御水平；新型威胁防御就绪度则评估企业防御体系应对未知威胁的韧性。

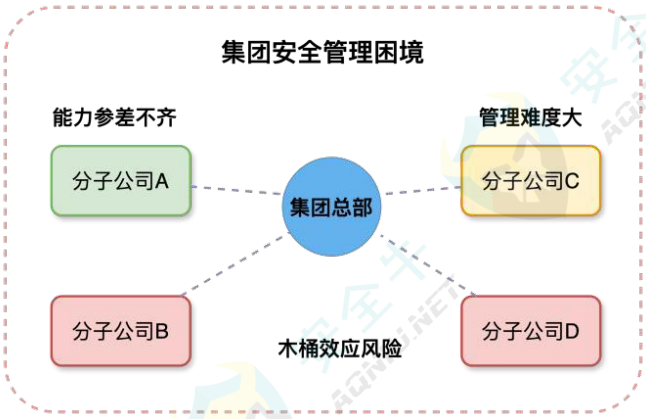
厂商案例 *（部分案例参考数据）*

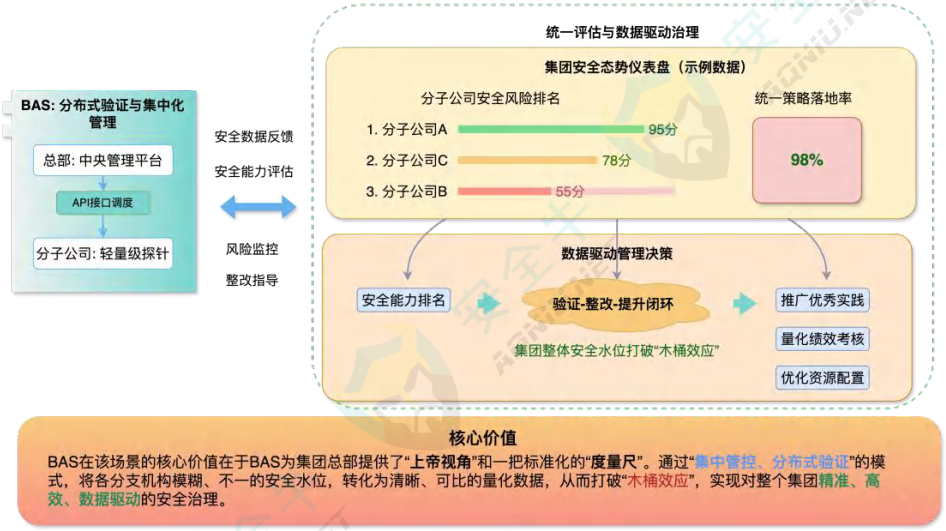
- 墨云科技在案例中发现 EDR 防护对 APT 样本的阻断率仅为 14.2%，为企业提供了明确的提升方向。
- 塞讯科技拥有十几年 APT 组织追踪研究经验，将第一手受害者威胁情报转化为可执行攻击模拟规则，提供内置的 400+APT 组织场景和 250+勒索团伙场景供选择使用。并提供 AI 分析攻击载荷、生成检测规则的能力，正向更多 AI 功能演进。
- 赛宁网安通过开展勒索挖矿等验证，发现整体防护检测率仅有 59%，精准定位到部分产品未采取防护措施，NTA 检测率仅为 30%等问题。
- 矢安科技借助 BAS 的漏洞验证能力，为某集团在重保期间，24 小时内完成了 0DAY 漏洞的可利用与防护验证，提升了集团整体防护能力。
- 知其安通过勒索验证，使勒索软件防护策略有效率从 0%提升到 92%。

请注意，该效果数据来源于部分案例或特定场景，实际效果受到多种因素的影响，数据仅供参考，并不代表所有企业都能取得类似的效果。

专项场景八：分子公司/上下级单位的安全能力验证

大型集团企业或拥有众多分子公司、上下级单位的机构，常面临各分支机构安全能力参差不齐、管理难度大等问题，集团总部难以统一管理和评估，安全政策落地难，可能存在安全短板，导致木桶效应风险。





分子公司验证场景（部分案例参考数据）

BAS 系统支持分布式部署和集中化管理，集团总部可在中央部署管理平台，在各分子公司部署轻量级探针或虚拟节点，进行远程、常态化、标准化的安全验证和评估。可模拟针对各分子公司特定业务系统、网络边界和内网环境的攻击（如针对分支机构 VPN 入口的弱口令爆破、办公网终端的恶意文件投放），并收集各分支机构安全产品的告警日志、阻断日志、审计日志。量化分子公司安全风险排名/评分和统一策略落地率。分子公司安全风险排名/评分能直观展现各分支机构的安全短板和优秀实践，便于集团进行资源倾斜和经验推广；统一策略落地率体现了集团安全治理能力的体现，确保集团安全政策能够有效渗透到每一个分支机构。

BAS 系统支持分布式部署和集中化管理，可在集团总部部署中央管理平台，在各分子公司部署轻量级探针或虚拟节点，进行远程、常态化、标准化的安全验证和评估。针对各分子公司特定业务系统、网络边界和内网环境的攻击（如针对分支机构 VPN 入口的弱口令爆破、办公网终端的恶意文件投放）进行模拟攻击，并收集各分支机构安全产品的告警日志、阻断日志、审计日志。并通过对分子公司安全风险排名/评分和统一策略落地率等量化指标，直观展现各分支机构的安全短板和优秀实践，便于集团进行资源倾斜和经验推广；或通过统一策略落地率体现集团安全治理能力，确保集团安全政策能够有效渗透到每一个分支机构。在该场景下，BAS 系统助力集团总部把握整体安全态势，优化资源配置，提升全集团安全水位。

厂商案例

- 塞讯科技通过在某全球连锁餐饮企业的多个 IDC、办公区和云上部署验证机器人，实现了对跨区域、分布式机构的统一安全能力评估，为集团摸清了整体安全水位，持续助力防御水平。
- 矢安科技在某大型金融云项目中，运用自身安全评分模型助力集团实现统一的安全评价体系，为集团安全运营提供指导依据，促使半数以上分子公司从被动安全转为主动安全，大幅提升集团整体安全能力。

专项场景九：云环境与复杂异构网络安全验证

随着业务上云和数字化转型，企业面临混合云、多云、容器化、微服务等复杂网络架构的新型安全挑战，云上安全配置错误或 API 暴露风险高，一旦出现问题，影响范围广。但是云环境的动态性、弹性以及云原生技术的复杂性，增加了安全防护和验证的难度，同时，传统安全工具难以深入验证云环境的防护效果。



云环境与复杂异构网络安全验证（部分案例参考数据）

通过 BAS 模拟针对云主机、云服务（如对象存储、数据库服务）、容器、Serverless 等各种云原生组件的攻击，并与云平台 API 集成，可自动发现云上资产并部署探针，验证云防火墙、云 WAF、云安全组、VPC 等云原生安全产品的有效性，识别云上配置缺陷，收集云安全平台日志、云资源配置日志、容器运行时日志、云原生安全产品的告警和阻断日志，形成关键量化指标，并通过云资产防护覆盖率可评估云上关键资产被防护的比例，帮助企业发现云上未受保护的资产；通过云安全策略有效率可验证云安全组、VPC 等配置的有效性，避免云环境因配置错误导致的安全事件；通过容器逃逸/微服务攻击阻断率可评估企业对

容器、微服务等新兴云原生威胁的防御能力。在该场景下，BAS 系统助力企业在复杂云环境中实现安全可控，应对新风险，保障数字化转型顺利进行。

厂商案例（*部分案例参考数据*）

- 塞讯科技在对横跨多 IDC、混合云的复杂环境，开展验证并推动了相关策略的优化。
- 矢安科技在某案例中，为用户完成从云上环境、到 IDC 网络、到办公网、再到隔离内网的安全能力验证，贯穿式的验证方式最大程度还原了攻击者可用的攻击路径与攻击方法，实现综合防护能力提升 60%。
- 知其安在某案例中，对一朵云中横跨多网域的复杂云环境进行验证，实现所有安全产品安全防护有效性提升总和 87%，包括 WAF 策略有效率从 75%提升至 94%。

请注意，该效果数据来源于部分案例或特定场景，实际效果受到多种因素的影响，数据仅供参考，并不代表所有企业都能取得类似的效果。

专项场景十：数据安全防护能力验证

国内法律法规和监管要求日益严格，数据泄露、勒索攻击等安全事件频发。但企业缺乏对敏感数据的全面识别、分类和流转监控，数据防泄漏（DLP）可能存在策略配置不当等问题，导致企业不清楚敏感数据传输和存储过程中的安全防护是否有效，无法验证数据安全防护的有效性。

BAS 系统能够模拟数据窃取、数据篡改等各种攻击场景，包括数据库审计、数据库安全、API 安全、开发安全等多元化场景的攻击，如模拟攻击者定位敏感数据（如通过扫描、弱口令爆破），然后尝试外传数据或进行加密。BAS 与数据防泄漏（DLP）、加密系统、数据备份系统等联动，验证这些系统是否能及时发现并阻止数据异常行为以及数据恢复的有效性，收集 DLP 告警日志、数据库审计日志、文件访问日志、异常行为日志。通过敏感数据泄露风险可评估数据外渗的成功率，帮助发现 DLP 策略盲区；通过数据勒索恢复就绪度可评估企业应对勒索攻击和数据恢复的准备程度；通过数据访问控制有效性则能发现特权账户滥用、权限过大等风险。在该场景下，BAS 系统直接验证数据防护措施有效性，助力企业满足合规要求，保护核心数据资产，降低数据风险。

厂商案例

- 灰度安全，不仅提供数据泄漏场景，并将范围延伸至数据库审计、数据库安全、API 安全、开发安全等多元化场景，实现对数据安全中各关键环节的安全验证需求。
- 其他大部分厂商都提供对数据 DLP 产品的数据安全场景的有效性验证。

第七章 BAS 实施部署与建议

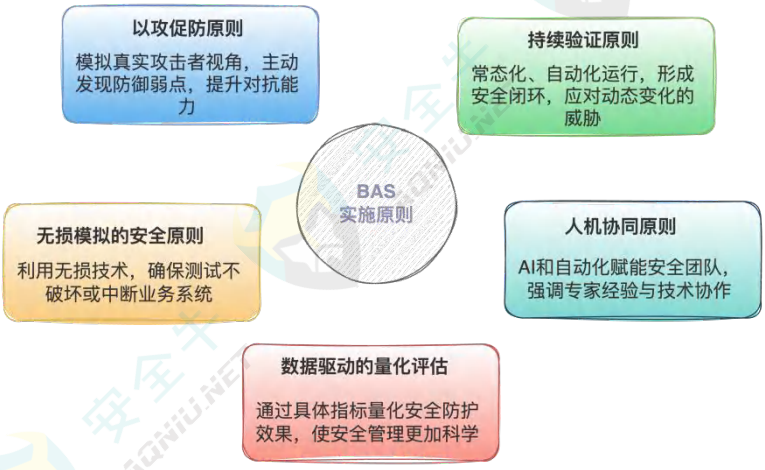
入侵与攻击模拟（BAS）产品的有效落地，不仅需要依赖于先进的技术产品，还应使用科学的部署方法、安全的实施以及对运营流程模式的深刻理解。应按照分阶段实施、从简单到复杂、重视安全与合规、持续改进与优化和结合业务需求的思路开展。



BAS 实施部署

7.1BAS 实施原则

BAS 的部署是一个系统性的过程需要充分的规划、准备和精细地实施管理。在 BAS 产品的部署和应用过程中，遵循以下核心原则以确保其成功最大化并规避潜在风险，



BAS 实施原则

以攻促防原则：应将 BAS 视为主动发现防护弱点、提升对抗能力的工具，而非简单的合规检查手段。其核心是通过模拟真实的攻击者视角和技术，对现有安全防护体系进行实战化评估，推动防护体系的持续优化和提升。

持续验证原则：BAS 的价值在于其持续性。部署后应常态化、自动化运行，形成发现－修复－验证－改进－持续监控的闭环，确保安全防护能力在动态变化的 IT 环境中持续有效，并应对不断演变的安全威胁。这与传统人工渗透测试难以常态化形成了本质区别。

无害化模拟的安全原则：应积极利用无害化/无害化模拟技术，如流量回放、沙箱隔离、仿真接收端等，并应具备熔断机制应对异常情况，确保业务系统不造成任何实际破坏或中断。

数据驱动的量化评估：将安全防护效果进行量化评估，通过具体的指标（如攻击成功率、检测告警率、阻断成功率、误报率、响应时间等）来助力安全价值能力的提升和安全投入的证明，使安全管理有数据依据，更加科学，并辅助风险优先级的确定和决策。可视化呈现是重要手段。

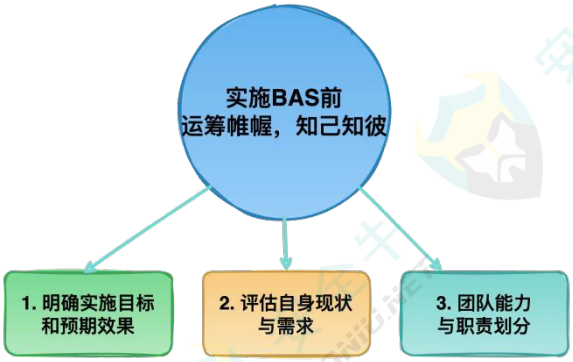
人机协同原则：AI 和自动化虽然能极大地提升效率和精准性，但安全专家的专业知识、实战经验和决策能力仍然至关重要。BAS 是赋能安全团队的工具，辅助进行攻击场景编排、数据分析、生成建议等，而不是完全替代人工。应强调安全专家、开发团队与运维团队之间的高效协作是确保 BAS 落地并发挥作用的关键。

7.2BAS 实施路线图

入侵与攻击模拟（BAS，Breachand Attack Simulation）技术作为提升企业网络安全防御能力的关键工具，近年来在行业内备受瞩目。然而，众多企业在实际推进 BAS 落地时，没有计划，无法切实实施，或缺乏有效方法使其持续运转，最终沦为摆设。安全牛通过为企业打造一套切实可行的 BAS 实施路线图，涵盖规划、选型、部署、运营以及深化应用等全流程环节，指导企业高效开展 BAS 应用，充分释放其价值潜能，助力企业安全运营实现从理论有效到实战有效的跨越。

7.2.1 实施 BAS 前：运筹帷幄，知己知彼

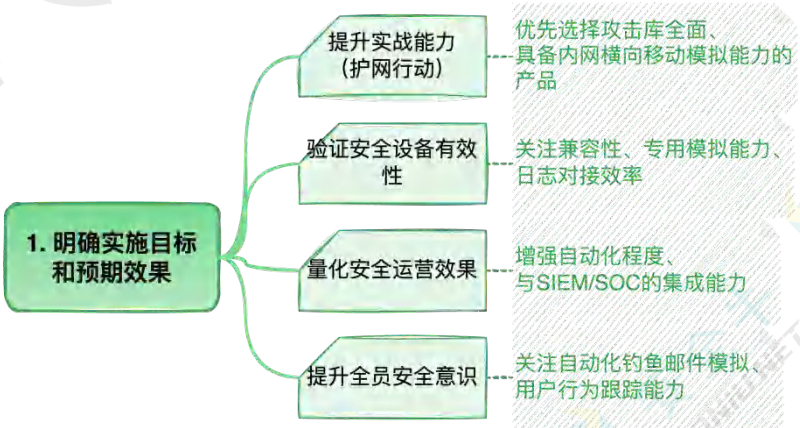
在正式引入 BAS 技术之前，企业应必开展全面且深入的内部规划与自我评估工作，这是确保 BAS 项目顺利落地、达成预期效果的坚固基石。



实施 BAS 前的规划

1）应明确实施目标和预期效果：

企业首要任务是明确实施 BAS 的核心目标，不同的实施目标将影响 BAS 的选型、部署以及运营等各环节的策略制定，清晰的目标能够使 BAS 实施更加聚焦，有效规避资源无端浪费，并且为后续的价值评估提供明确且可靠的衡量基准。



实施 BAS 应明确实施目标和预期效果

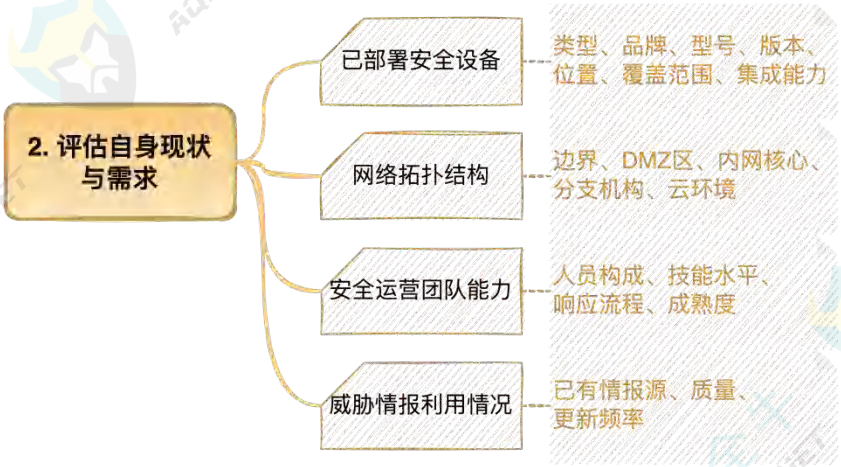
例如：

- 以提升护网行动实战能力为目标：企业应将选型重点聚焦于全面覆盖护网常见的高频攻击手法以及 APT 攻击，并且具备内网横向移动模拟能力的产品。在部署环节，要着重针对互联网边界以及内网核心业务区进行布局，并且在护网行动前，组织应开展高强度、多轮次的模拟演练，加强检验和优化安全防护策略，提升实战能力。
- 以验证安全产品有效性为目标：企业选型应关注 BAS 产品与特定安全类型的兼容性、专用模拟能力以及日志对接的及时性。部署时应紧密围绕待验证的安全产品展开，并且在安全产品正式上线前，开展针对性的功能验证工作，确保其安全效能稳定可靠。

- 以量化安全运营效果与提升效率为目标：企业应着力强化 BAS 的自动化水平、日志智能分析功能以及与 SIEM/SOC 等安全产品平台的集成效能。运营重心应在于常态化、周期性的验证任务执行，持续追踪诸如安全风险评分等关键指标，实现对安全运营状况的精准量化与高效掌控。
- 以提升安全意识为目标：企业应着重考量 BAS 产品是否配备自动化钓鱼邮件模拟能力，能否对用户行为实现精准跟踪以及生成详细的员工报告。后续应紧扣定期面向全员或特定群体开展钓鱼邮件演练这一关键举措，逐步筑牢企业安全意识防线。

2）评估自身安全现状与需求：

在目标明确之后，企业应对自身的安全家底进行全方位、深层次的排查与评估。通过细致评估工作，精准确定应要 BAS 解决的安全痛点，同时为后续的 BAS 选型与部署提供参考信息，这是 BAS 实施迈向成功的关键前提。



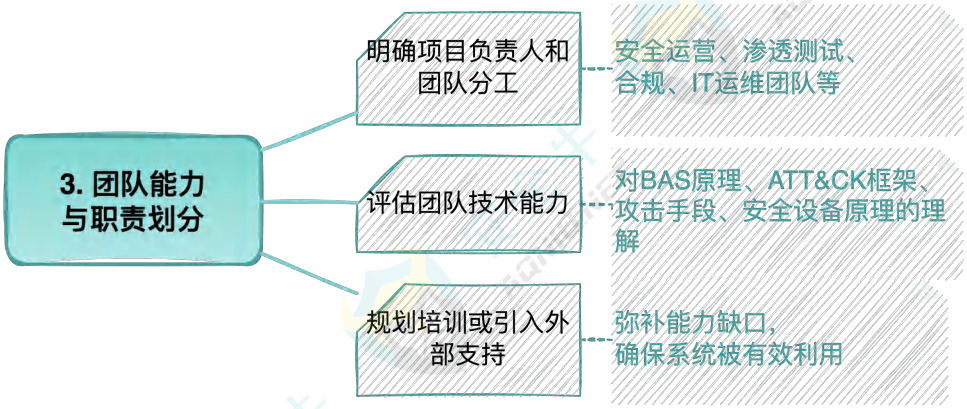
实施 BAS 应评估自身安全现状与需求

评估工作应全面涵盖企业已部署的安全产品信息，包括但不限于类型、品牌、型号、版本、部署位置以及覆盖范围等关键要素，并且深入了解安全产品的集成能力与日志输出格式。除此之外，企业还应精准识别网络拓扑结构，详细梳理边界、DMZ 区、内网核心区域、分支网络以及云环境（公有云、企业云、混合云）等不同区域的构成与关联，并明确各自的关键特性与安全应求。并对当前安全运营团队的人员构成、技能水平、安全事件响应流程以及威胁情报利用等多方面的成熟度进行全面审视，及时察觉如响应滞后、告警疲劳等安全痛点。并且企业还应了解威胁情报的订阅或收集情况，以及这些情报的质量品控与更新频率等关键指标。

3）团队能力与职责划分：

BAS 的有效实施需要多部门的紧密协同作战，因此明确 BAS 项目的负责主体以及各部门的职责分工，

是保障项目稳步推进、系统持续稳健运行的关键环节。



实施 BAS 应团队能力与职责划分

企业要明确参与的各部门（例如安全运营团队、渗透测试团队、合规团队以及 IT 运维团队等）和分工职责（如采购、部署以及日常运营）。与此同时，深入评估团队成员对 BAS 技术原理、攻击影响链模型（如 ATT&CK 框架）、常见攻击手段。若团队缺乏相关经验，则应提前规划专业培训，亦可以考虑使用厂商的专业服务，以弥补能力缺口。明确的职责划分和充分能力的准备，能够确保 BAS 系统能够被有效利用，并持续为企业创造安全价值

7.2.2 BAS 产品选型：找到最适合你的实战伴侣

在当今市场上，BAS 产品种类繁多、功能各异，众多企业常常难以抉择出真正适合企业自身应求的产品，精准地选出合适的 BAS 产品是 BAS 成功实施的关键所在。



BAS 产品选择

1）攻击库的真实性与覆盖度

攻击库作为 BAS 产品开展攻击模拟的根基，其质量直接决定模拟的全面性、真实性和有效性。企业在选型阶段，应着重考察厂商的攻击库能否全方位映射 MITREATT&CK 框架中的各类攻击策略与技术，以保障攻击模拟的完整性。鉴于国内网络安全环境的复杂性，还应评估攻击库是否涵盖针对国内企业的高发威胁，像勒索病毒变种、Web 通用漏洞利用等情况，以及 APT 组织的最新攻击手段（TTPs）。此外，厂商的持续更新攻击库的能力，能否及时纳入最新的零日漏洞验证（无害化）、新型威胁和攻击演练中涌现的新手法，对确保 BAS 产品有效应对不断演变的威胁至关重要。

例如，部分先进厂商依托其安全实验室对全球黑客组织活动的持续追踪与情报积累，将第一手的受害者威胁情报转化为验证实验素材，其攻击库也源于多年的国家级实网攻防演练经验，从而确保攻击库与主流攻击技术相契合，为企业提供高真实度、强对抗性的模拟能力。

2）无害化安全部署机制

BAS 产品在运行过程中，应重点考量模拟攻击无害化能力，确保不会对企业的业务系统造成任何负面影响。企业应深入了解产品具体的无害化攻击技术实现路径，诸如基于流量重放却不实际利用漏洞，以此规避引入真实漏洞对目标系统造成破坏；模拟文件读写操作却不真正篡改数据，避免数据被篡改风险；或在隔离的受控沙箱环境中执行高风险不良样本，并进行环境回滚，确保样本不漏洞。

同时，BAS 产品的轻量化设计及其自身安全性不容小觑，应保证系统资源占用极少，或借助攻击模块介入加载等技术，仅在任务执行时加载相关模块，降低自身被攻击或引入新漏洞的风险。而且应协同厂商

共同制定应急预案和熔断机制，以便在意外发生时，BAS 系统能够自动终止攻击任务并迅速回滚环境，将风险压缩至最低限度。

目前，部分厂商在无害化领域已掌握专利技术，强调其系统在测试过程中无需依赖真实靶机，凭借对业务的仿真能力来规避风险，有力地保障了其在生产环境中的安全运行。

3）AI 能力与智能化程度

AI 技术与 BAS 的深度融合，可显著提升自动化水平，大幅削减运营成本，从基础的自动化工具跃升为智能安全助手。企业应着重考量 BAS 产品在 AI 赋能方面的效能。具体而言，应考量 BAS 是否具备用户辅助攻击场景智能编排与生成能力，能否借助自然语言交互或智能推荐，根据验证测试的目标，自动化生成复杂多变的攻击分析和测试用例，进而提升效率，降低对专业攻防知识的依赖。配备 AI 驱动的日志智能分析能力可以对海量、多源异构的安全日志实施自动化解析、归一化以及深度关联分析，自动识别攻击行为并评判防御效果，实现验证结果的自动化判定，甚至达到减少人工干预的程度，降低日志分析的复杂度，使安全团队能够有更多时间聚焦风险研判与策略优化工作。

当前，国内前沿的 BAS 产品还可运用 AI 智能生成精准且具可操作性的修复建议，甚至自动触发策略更新，进一步推动安全运营的自动化进程。

4）集成与自动化闭环能力：构建高效安全运营

BAS 的价值不仅局限于发现问题，更应驱动问题解决，并构建自动化闭环。因此企业应关注 BAS 是否能够与现有的安全运营平台（例如态势感知、SIEM/SOC、XDR）、安全编排自动化与响应（SOAR）、漏洞管理系统、工单系统以及资产管理系统等实现深度且实时的 API 或 Syslog 日志对接。这种集成能力能够保障 BAS 发现的安全缺陷自动通过安全运营平台，由 SOAR 平台自动编排响应流程，譬如隔离受感染主机，或自动向工单系统分发修复任务，同步更新资产管理系统中的风险状态。

目前，先进的 BAS 产品能够支持 50 多类安全产品日志格式的实时解析与关联分析，这在很大程度上增强了其兼容性，为自动化闭环的构建筑牢根基。借助这种无缝集成，企业得以实现从发现问题到解决问题的自动化闭环管理，大幅提升安全运营效率，促使安全运营从被动响应迈向主动防御新阶段。

7.2.3 初步的基础单点验证

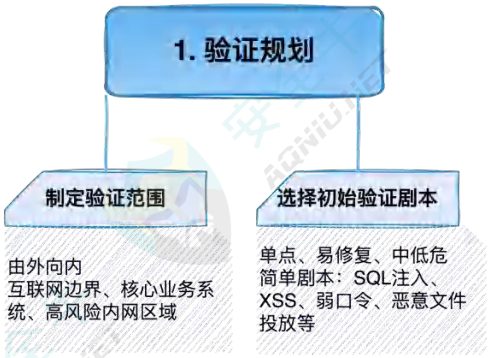
完成前期准备与产品选型环节后，企业便可进入 BAS 实施的初期的单点验证进行试点测试，步骤包括验证技术、部署对接以及执行验证，初步阶段的核心目标是筑牢根基，保障 BAS 系统的安全稳定运行。



初步实施 BAS

1）单点安全产品简单级别的验证计划

在 BAS 正式部署前，应制定验证计划并挑选攻击剧本，这一环节将直接关乎后续验证的有效性与准确性。



单点安全产品简单级别的验证

首先要明确验证的范围。建议根据验证目标，按照从外到内的顺序划定 BAS 验证的重点区域。例如，互联网边界区域、承载核心业务的特定业务系统，或是存在已知高风险的内网区域，可以迅速收获初期成效。

其次挑选初始验证剧本。建议结合企业现状及主要痛点，优先选择 BAS 内置的、基础的、易修复的中低级模板，或者常见高频攻击场景作为首次验证剧本。例如，针对 Web 应用的 SQL 注入、XSS 等常见漏洞，系统弱口令问题，以及模拟恶意文件投放等场景。这些基础剧本能够高效验证 BAS 的无害化能力与检测效果。

2）部署并与安全产品对接

BAS 系统与现有安全生态实现无缝连接是有效发挥作用的基础前提。企业应综合考量自身 IT 基础设施状况、数据安全要求以及运维能力等多方面因素，选择最适合部署方式并进行部署安装。



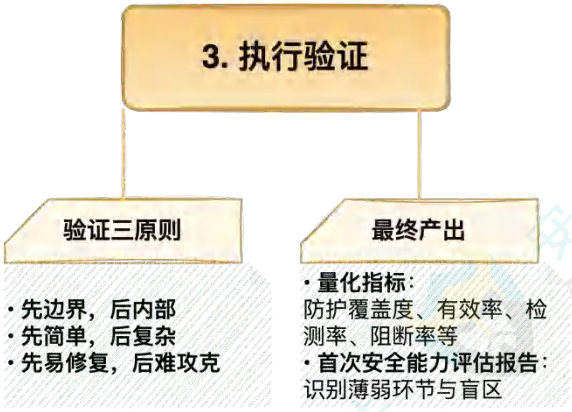
部署 BAS 并与安全产品对接

- 本地化部署：此种方式适用于大型企业以及对数据不出域有严格要求的场景，能够实现对数据安全的完全掌控，但是需要企业自身具备一定的人员团队资源与专业技术能力。
- SaaS 化部署：此种方式比较适合中小型企业或是分子公司，优势是运维成本较低，无需投入大量硬件资源，日常的系统维护以及攻击库更新等工作则由厂商负责。
- 混合部署：这种部署模式兼顾了前两者的优点，比如管理平台可选择本地部署，探针则以 SaaS 化方式连接。

部署代理是确保攻击模拟覆盖度与真实性的关键所在。企业应依据自身需求，在核心业务系统服务器、关键终端资产以及不同安全区域（诸如互联网边界 DMZ 区、内网核心区、开发测试区等）部署代理，重点关注其无害化能力，避免对生产环境造成不良影响。与此同时，还应关注 BAS 与企业现有的安全产品（如 WAF、IPS、EDR、防火墙、DLP 等）以及日志平台（如 SIEM/SOC）的 API 或 Syslog 接口对接工作，打通数据通路。保障 BAS 在模拟攻击过程中能够实时获取安全产品产生的日志，包括阻断日志、流量日志等，为后续的精准分析提供可靠的数据支撑。

3）单点与批量验证

初级阶段，验证任务目的是摸清当前安全防护现状的薄弱环节并推进修复优化。



单点与批量验证

验证顺序应遵循先边界、后内部的原则。建议从企业最直接的攻击面－互联网边界安全产品（如 WAF、边界防火墙、互联网 IPS）开始外部进行验证，因为这是抵御攻击的第一道防线，其效果直接了于企业是否会高频的尝试，在初步验证边界防护稳定后，再深入到企业内部网络、验证内网安全产品和内部资产的防护效能。

攻击模板选择顺序应遵循先简单，后复杂的原则。建议从 BAS 内置的简单、高频攻击模板起步，之后逐步引入涉及多步骤、多协议的复杂攻击链编排。例如，优先针对 Web 应用的 SQL 注入、XSS、简单弱

口令爆破以及常见的恶意软件投放进行模拟验证。这些模板操作简便，有助于快速检验 BAS 系统的基本功能与无害化能力。待确认基础功能稳定且结果精准后，再循序渐进地引入复杂的攻击链编排。

风险点选择顺序应遵循先易于修复，后难攻克的原则。建议优先聚焦那些易于修复的风险点。例如，因配置错误、规则未开启或仅应简单策略调整即可修复的问题。有助于迅速取得成效，并为后续处理更复杂、更难攻克的问题积累宝贵经验。

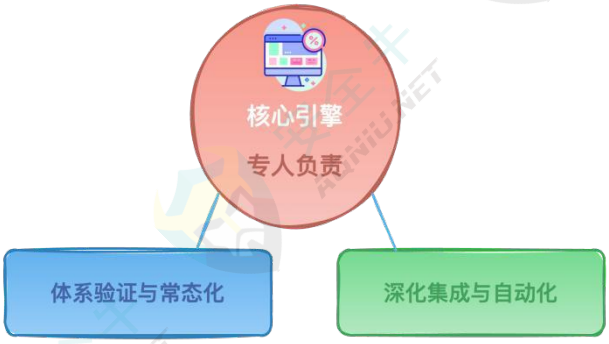
通过单点与批量验证，企业能够获取诸如防护覆盖度安全产品有效率检测率阻断率等量化指标，并形成首份安全能力评估报告。这份报告将如实呈现企业当前安全防护体系的薄弱之处，比如哪些安全产品配置有误、哪些防护区域存在盲区，为后续的优化调整指明方向，帮助企业从想象中的安全迈向实战安全的关键步骤。

本阶段的难点与重点：

- 产品无害化验证：尽管 BAS 强调无害化攻击模拟，但在首次运行时，还是应谨慎运行任务，确保不会对企业的业务系统造成任何负面影响
- 日志对接与分析准确性：应确保 BAS 能够精准、全面地获取并解析各类安全产品的日志，规避误报或漏报现象。
- 安全能力基线建立：首次验证所形成的报告将作为后续持续优化的起点，其基线数据对于平稳引入 BAS 具有关键价值，因此应建立清晰且可量化的安全能力基线。

7.2.4 BAS 持续深化应用：整体协同与常态化运营

完成了 BAS 的初期部署和基础验证后，企业便进入了 BAS 应用的核心阶段－持续深化和常态化运营。此阶段的目标是突破单点验证的局限，评估多层防御体系的协同效果，并实现此类评估的日常自动化，真正将 BAS 融入企业的安全运营生命周期。



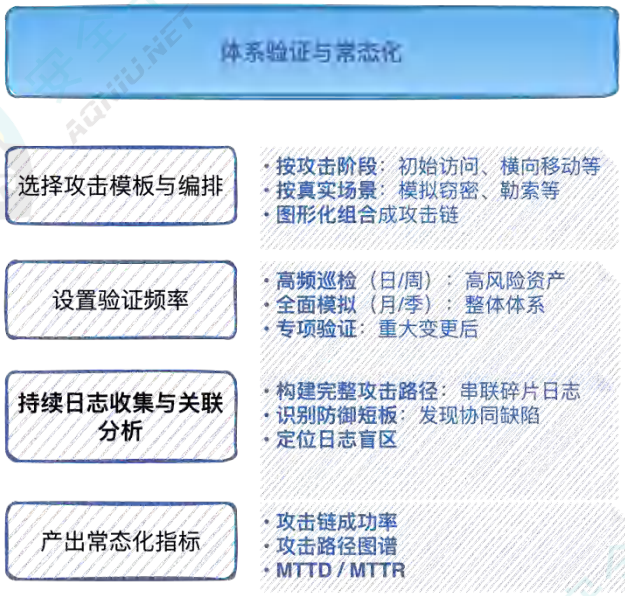
BAS 持续深化应用

注：为确保 BAS 的持续有效运营，企业应指定专人负责，职责包括：BAS 系统的日常维护与健康度监控；依据企业安全目标及最新威胁动态，精心规划、编排并适时调整验证任务；深度分析 BAS 产出的各类报告，精准解读量化指标；推动内部安全团队与 IT 运维团队对所发现问题进行修复；确保发现－修复－复测的闭环流程运行等，这是 BAS 从测试工具升级为企业赋能安全运营的核心平台的关键，

1）整体防御体系验证与常态化

真实的网络攻击往往呈现出链式、多阶段的特征，涉及多层防御安全产品的协同应对。

因此应对整个纵深防御体系的整体效能进行评估，并实现常态化持续进行，这是 BAS 确保安全防护能力能够动态适应业务发展及应对威胁快速变化的关键。



整体防御体系验证与常态化

选择多个攻击模板与编排：企业应依据自身网络架构特点、业务核心资产的重要性以及实际面临的真实威胁场景，精心挑选多个复杂的攻击模板并加以编排。可按照攻击阶段，如初始访问、持久化、权限提升、防御、安全产品访问、发现、横向移动、数据渗漏等进行攻击复杂链剧本的编排，以贴近企业可能遭遇的真实攻击场景。例如，为评估内部横向移动，可选择模拟使用窃取工具、PsExec 进行远程执行，或利用 SMB/RDP 等协议进行文件共享访问的模板；或选择模拟多种绕过 WAF 的 SQL 注入变体、XSS 攻击以验证 Web 防护，并借助图形化编排将多个攻击模板整合为完整的攻击链场景，模拟更复杂的攻击情境。

持续验证的频率设置：验证频率应根据风险等级、业务重要性、合规要求以及资源投入等进行调整。例如对于互联网暴露面、核心业务系统、敏感数据存储区域等高风险资产，建议采用每周甚至每日的短周期、自动化巡检方式进行验证，以便迅速发现因策略或配置变更而产生的风险。对于整体纵深防御体系或

为应对年度合规审计（如等保、关基），可设定每月或每季度开展一次全面的攻击链模拟，确保宏观防护能力符合标准。此外，每当网络架构调整、新的安全产品上线、核心业务系统更新或重大安全策略变更后，应执行专项验证，以确认变更未引入新的安全风险。

日志持续收集与分析（重点增强）：BAS 系统将与企业所有相关的安全产品（如防火墙、IPS、WAF、EDR、DLP、堡垒机等）和 SIEM/SOC 平台持续进行日志对接。在每次自动化验证运行后，BAS 会实时收集这些安全产品产生的行为日志、阻断日志、流量日志等，并借助智能分析引擎开展深度关联分析。这种深度关联分析能力至关重要，能够将不同来源、不同时段的碎片化日志信息串联整合，构建完整的攻击路径，精准识别出在整个攻击链中未被有效检测、阻断或遗漏的关键日志点。例如，通过关联分析，BAS 可发现边界 WAF 虽遭攻击，但后续内网中的横向移动行为却未被 EDR 或内网 IDS 及时察觉，进而精准定位多层防御系统间的薄弱点与日志盲区。

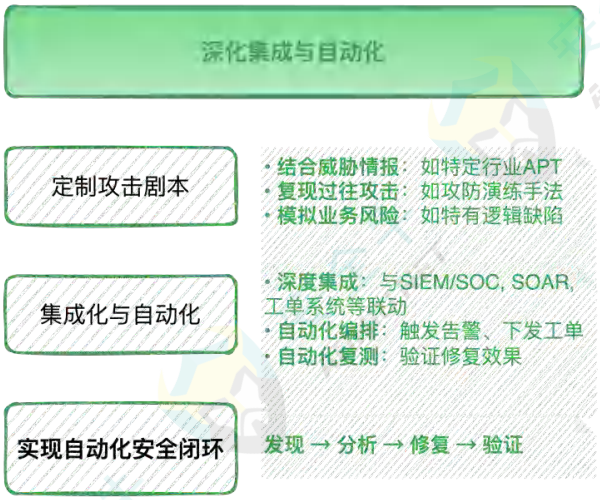
持续掌握整体防御能力和实现验证优化常态化。借助一系列关键指标，能帮助企业持续洞察整体防御能力，并推动安全优化的常态化。关键指标包括攻击链爆发率（反映整个防御体系的健壮性）、攻击路径图谱（可视化呈现攻击者渗透路径）、平均检测时间（MTTD）与平均响应时间（MTTR）（体现安全运营团队效率）等。

本阶段的难点与重点：

- 复杂攻击链的编排：设计出贴近实际且涵盖多阶段的攻击链要求较高的攻防知识。企业初期可借助厂商提供的模板，随着经验积累逐步尝试自定义编排。
- 跨安全产品日志的准确关联：确保来自不同厂商、不同类型的安全产品日志，能够被 BAS 准确关联到对应的攻击行为，这是保障分析结果准确性的基础条件。

2）集成和自动化

实现常态化验证后，企业应进一步深挖 BAS 的应用潜力，从两个方面提升其应用深度：其一，通过定制化攻击模拟，对高级复杂攻击的模拟，并增强 BAS 模拟的真实性、精准性，以验证应对高级持续性威胁能力，并使其紧密贴合企业实际面临的威胁，从而确保防护体系具备应对能力；其二，借助集成化自动化，提升安全运营效率，降低人工干预，最终构建发现－分析－修复－验证的自动化循环，推动安全运营从被动响应向主动防御转变，使 BAS 从独立的测试工具华丽转身，无缝融入安全运营流程，成为驱动安全能力持续提升的核心引擎。



BAS 的集成和自动化

定制攻击剧本：利用 BAS 产品提供的灵活图形化编排功能，结合企业实际面临的最新威胁情报（例如特定行业 APT 攻击）、过往攻防演练中被利用的攻击手法、内部安全检测发现的特定业务漏洞以及企业特有的逻辑缺陷，量身定制高仿真、高隐蔽的攻击管理和脚本。比如，依据最新勒索病毒变种的特征，定制模拟其文件加密行为及勒索信息弹窗的攻击剧本；或者针对供应链合作方可能存在的特定漏洞，定制从合作方系统渗透至内部网络的攻击路径模拟剧本。

集成化与自动化：实现攻击验证－分析－修复－验证闭环的关键，在于 BAS 与其他安全系统的无缝集成与自动化联动。一方面，应将 BAS 系统与 SIEM/SOC、SOAR、工单系统、资产管理系统等深度集成。例如，当 BAS 发现安全缺陷后，能够自动触发 SIEM，并通过同步操作，将详细的攻击路径、资产信息、建议修复措施等内容同步至 SIEM 的事件记录中。另一方面，借助 SOAR 平台或 API 调用，自动编排响应流程。在问题修复完成后，BAS 能够自动化开展复测，验证修复措施的有效性，从而完成自动化安全优化。

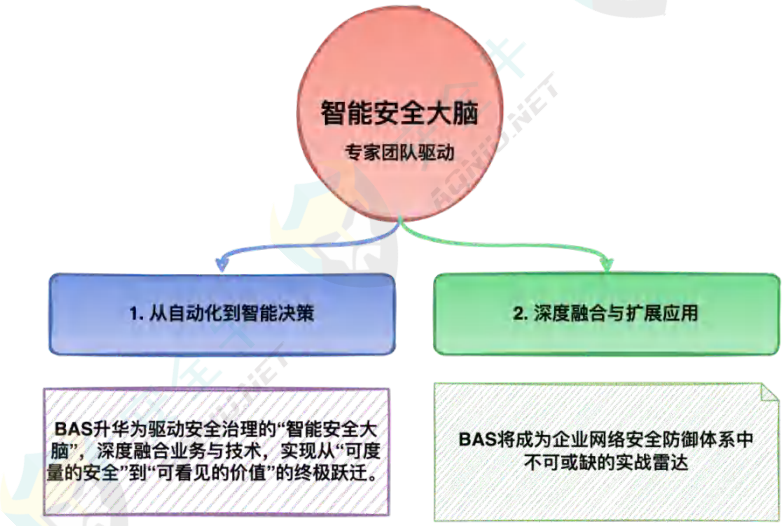
当前，领先的 BAS 产品已支持多种安全产品日志格式的实时解析与关联分析，这为其与各类安全平台的集成提供了坚实基础，并可通过 AI 决策引擎自动生成修复建议，触发防护策略更新，大幅提升运维效率。

7.2.5BAS 成熟进阶：智能化驱动与持续优化

当企业将 BAS 应用推进至常态化运营，并实现与现有安全流程的初步自动化闭环后，应借助其赋能构建面向实战、具备前瞻性的防御体系；通过量化指标客观评估安全团队和安全建设的绩效；辅助安全投资决策，实现精准采购，真正达成让安全价值看得见的目标。该阶段的主要目标是将 BAS 从自动化工具升级为智能安全大脑，使其成为企业安全治理体系中不可或缺的一部分，驱动持续优化。

专人负责的职责深度变化：在 BAS 的成熟进阶阶段，负责 BAS 的专人或专家团队将扮演更加关键的

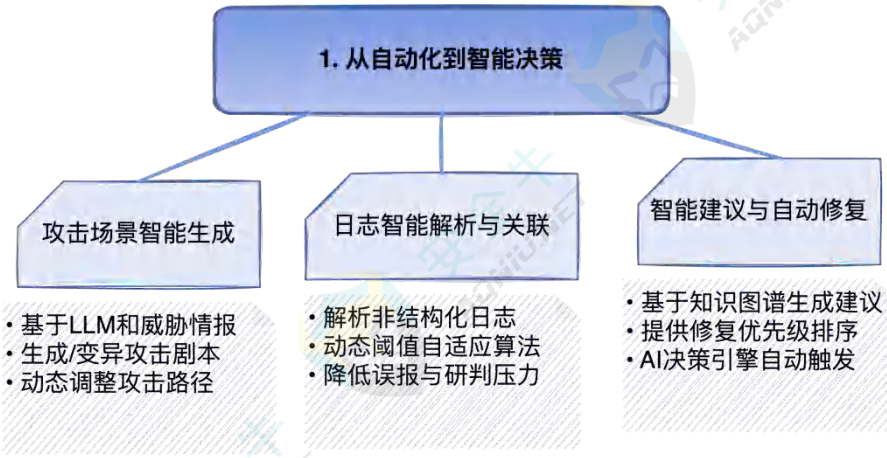
角色，不仅要保障 BAS 系统的日常健康运行和报告质量，更要深入参与企业的安全策略制定、风险决策以及安全建设规划中，将 BAS 的验证结果与业务风险、合规要求进行深度关联，推动安全体系的持续改进和创新。



BAS 成熟进阶

1）从自动化到智能决策

智能化是 BAS 未来发展的核心趋势，也是企业应对复杂威胁、提升运营效率的必由之路。建议企业应充分利用 BAS 产品的智能化能力，实现对新型威胁和 0day 漏洞的快速响应与防御验证，大幅提升威胁防御就绪度，同时减少人工分析和决策成本，进一步提升安全运营效率。利用人工智能（AI）技术，将 BAS 从简单的自动化测试工具升级为具备自主学习、智能决策能力的智能安全大脑。



从自动化到智能决策

攻击场景智能生成与优化：成熟的 BAS 产品能够突破固定模板的依赖限制，通过 AI 技术实现攻击场

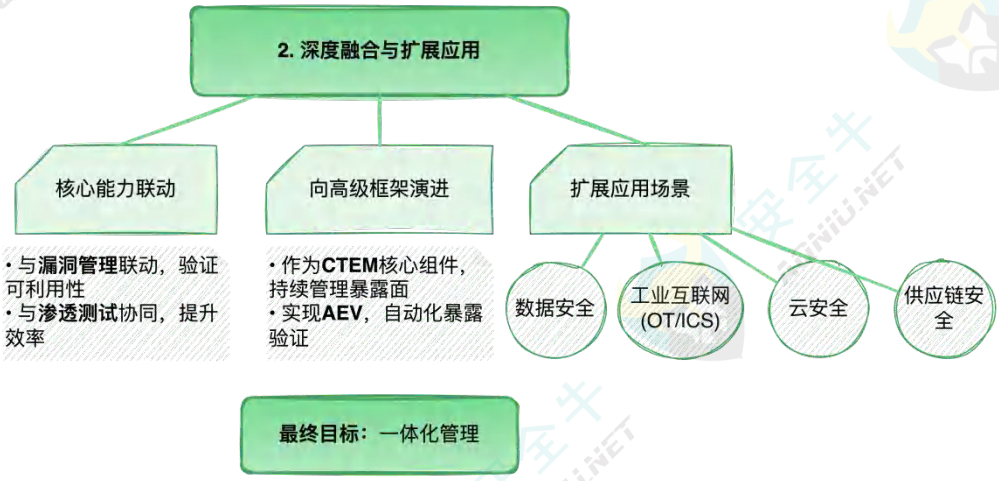
景的智能生成与优化。例如，基于大型语言模型（LLM）和最新的威胁情报，BAS 可智能地生成或变异出新的、分布式和对抗性的攻击样本，甚至能够根据当前网络环境的实时状态，动态调整攻击路径和方法，较大程度地提升模拟攻击的真实性和有效性，降低安全运营人员手动编排复杂攻击场景的工作量。

非结构化日志智能解析与关联：传统日志分析常面临海量、复杂的日志挑战，需要消耗大量人工进行规则匹配和解析。先进的 BAS 产品能够利用 AI 技术对非结构化安全日志进行智能解析、归一化和深度关联分析，自动识别并标记关键日志信息，支持多种安全产品日志格式的实时解析与关联。通过引入动态阈值自适应算法，自动识别异常模式和行为，有效降低误报率，大幅减轻安全运营团队的日志研判压力。

智能修复建议生成与自动修复：AI 在 BAS 中的应用进一步延伸至修复建议的生成。成熟的 BAS 产品能够基于验证结果和内置的知识图谱，智能地生成精准、可操作的修复建议，并提供优先级排序，甚至能够通过 AI 决策引擎自动触发安全产品策略更新或工单下发。这种自动化能力有效提升运维效率，加速问题的闭环管理，将安全运营从发现问题到解决问题的周期大幅缩短。

2）深度融合与扩展应用使价值最大化

在成熟阶段，BAS 不再是一个独立的测试工具，而是深度融合到企业安全治理的方方面面，成为实现持续威胁暴露管理（CTEM）和自动化暴露验证（AEV）的核心驱动力。建议企业积极推动 BAS 与其他安全能力的深度融合以及应用场景的扩展。



深度融合与扩展应用

联动漏洞管理与渗透测试：企业应将 BAS 与漏洞管理平台深度联动，实现漏洞的攻防验证。BAS 不仅能发现资产中的已知漏洞，更能验证 WAF、IPS 等防御安全产品对这些漏洞利用的实际防护效果，从而帮助企业优先修复那些虽然已知但可被利用的漏洞。同时，BAS 的自动化和常态化能力可作为人工渗透测试的预检工具或回归测试工具，帮助渗透测试团队快速定位高风险区域，提升人工渗透测试的效率和精准性，并通过自动化复测验证渗透测试后修复的有效性。

BAS 向 CTEM 和 AEV 框架演进：BAS 是实现 CTEM 和 AEV 框架的核心组件。CTEM 强调持续识别、评估和缓解企业面临的威胁暴露面，而 AEV 关注自动化验证攻击面的可利用性。BAS 通过持续自动化模拟攻击，验证攻击面的可利用性，并驱动暴露风险的修复，实现对威胁的持续管理。这种演进使安全管理从静态的漏洞列表转向动态的风险视图，更有效地降低安全风险。

扩展应用场景与融合一体化管理：随着企业业务的拓展，BAS 的应用场景也应随之完善和扩展。建议企业将 BAS 的应用范围延伸至以下领域：

数据安全验证：扩展数据安全验证场景的深度和广度，验证 DLP、加密系统、API、数据备份恢复等数据安全措施的有效性，实现对核心数据资产的持续保护。

工业互联网环境验证：针对工业控制系统的特殊协议和脆弱性，扩展工业互联网环境安全验证场景，模拟针对工控网络的攻击（如 PLC 篡改、SCADA 系统入侵等），验证工控防火墙、入侵检测系统和隔离措施的有效性，保障工业生产安全。

云安全环境验证：针对混合云、多云、容器、微服务等复杂云原生环境，扩展云环境安全验证场景，模拟云上攻击（如容器逃逸、云 API 漏洞等），验证云安全策略和产品的有效性，实现云环境下的风险量化和统一管理。

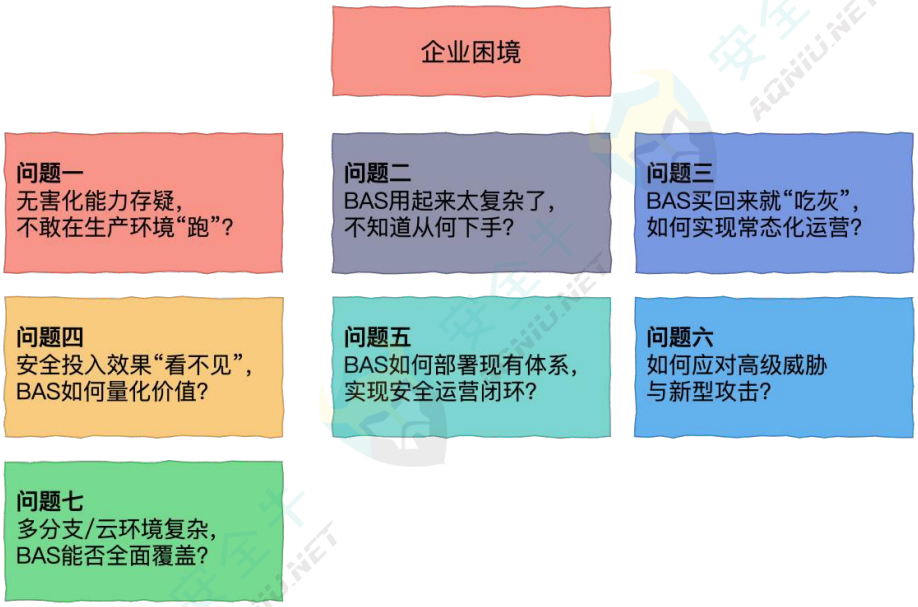
供应链安全：评估代码开发安全产品、第三方供应商、合作伙伴或外部接口带来的风险，模拟从供应链底层渗透到内部网络的攻击，验证企业对第三方风险的管控能力。

一体化管理：最终应将 BAS 验证结果整合至统一的安全管理平台，实现对所有安全能力（包括漏洞管理、威胁情报、安全运营、合规审计、安全建设）的集成化管理和部署，构建真正的安全大脑。

7.3BAS 实施：常见挑战和策略

在数字化浪潮下，企业对网络安全投入不断增加，入侵与攻击模拟（BAS）作为以攻促防的利器，日益受到青睐。然而，企业用户在从采购到实际应用 BAS 的过程中，却陷入了买了用不好的困境：系统部署后被闲置，不敢在生产环境运行，不知如何持续运营，更难以将验证结果转化为警示价值。

在数字化转型加速推进的当下，企业对网络安全的重视程度与日俱增，不断加大相关投入。入侵与攻击模拟（BAS）作为一种有效的以攻促防手段，凭借其独特优势，正逐渐受到企业青睐。然而，在企业从采购到实际应用 BAS 的过程中，却普遍遭遇诸多难题，陷入买了用不好的困境：系统部署后被闲置，不敢在生产环境运行，不知如何持续运营，更难以将验证结果转化为实际价值。安全牛对企业在 BAS 应用中的七大核心困惑进行逐一剖析和建议。



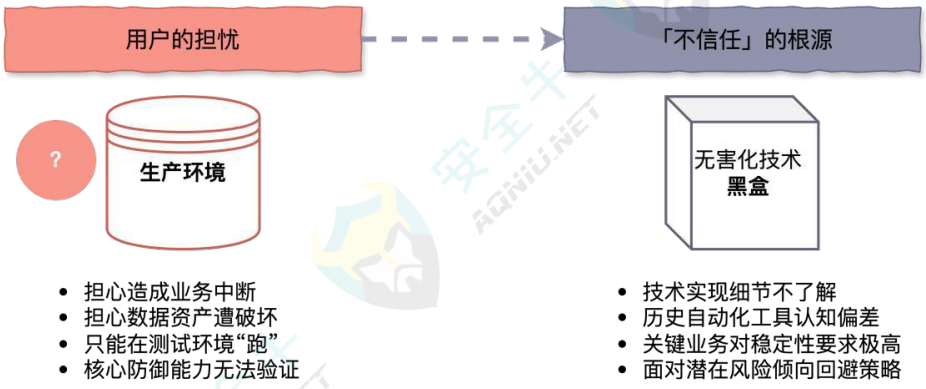
BAS 实施中常见的挑战

问题一：BAS 无害化能力存疑，不敢在生产环境跑?

企业在考虑或部署 BAS 时，最为关注的焦点在于其生产环境中的无害化能力。许多管理者担心 BAS 系统模拟攻击会像真正黑客一样，对核心业务系统造成威胁、数据破坏或留下隐患，这种担忧致使 BAS 系统往往只能在测试环境或小范围非核心区域运行，无法有效验证核心防护能力，难以发挥其最大价值。

安全牛分析

企业难以辨别 BAS 产品在无害化攻击技术上的具体差异，且担心在复杂生产环境中，即使有无害化设计，也可能出现不可预见的影响。同时，关键业务系统对稳定运行的要求极高，任何潜在风险都难以被接受，促使企业倾向回避策略。



BAS 无害化能力存疑，不敢在生产环境跑

安全牛建议

企业在选型和实施 BAS 时，应将无害化技术作为核心考量因素，采取以下安全策略保障 BAS 的安全运行：

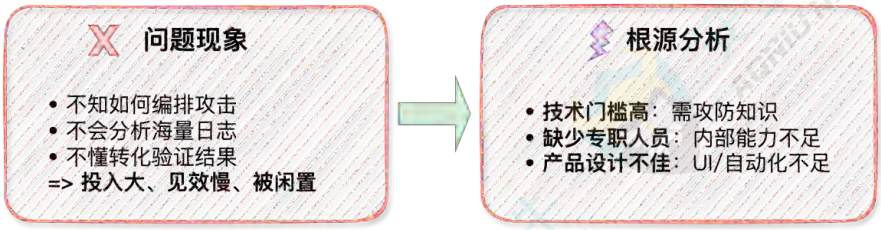
- 全面理解无害化攻击的实现原理：建议企业详细了解产品无害化攻击技术的具体实现，如通常包括基于流量重放但不实际利用漏洞，以避免引入真实漏洞并对目标系统造成破坏；通过 Agent/漏洞模拟文件读写但不修改实际数据，以避免数据丢失；在隔离的受控沙箱环境中执行高风险恶意样本后快速回滚环境，以确保样本不扩散；以及代理/探针本身仅行为模拟攻击而不实际执行恶意负载等机制。这些机制共同保障了 BAS 在高度仿真攻击的同时，未造成真实伤害。
- 关注轻量级 Agent 的设计：BAS 通常部署轻量级 Agent 聚焦于目标主机或网络。企业需关注其对系统资源的占用是否微乎其微，确保不影响业务运行。同时，接口本身需经过严格的安全设计，并能通过攻击模块实现安全验证任务加载等技术，仅在执行安全验证任务时才加载相关模块，降低 Agent 本身成为攻击目标或引入新漏洞的风险。
- 审慎评估厂商的市场应用案例：建议企业了解 BAS 厂商在其他关键行业客户（如金融、运营商）的实际应用案例，观察其如何成功保证无害化，通过行业应用实践增强对 BAS 在核心生产环境应用的信心。
- 构建完善的应急预案与熔断机制：即使 BAS 具备无害化能力，也应保持警惕。企业需在部署前与厂商共同制定应急预案，涵盖极端情况下如何快速暂停或终止验证任务、如何快速回滚等。BAS 系统本身也具备自动熔断功能，能在检测到异常行为或潜在风险时自动中止攻击任务，将风险降至最低。实施时，建议从非核心系统开始试运行，逐步扩大验证范围。

问题二：BAS 用起来太复杂了，不知道从何下手？

许多企业在采购 BAS 系统后，常面临操作困惑，如不知如何高效进行攻击编排、准确分析海量日志，以及如何将验证结果转化为具体改进措施。这种操作复杂性导致 BAS 系统投入大却难以快速见效，使用率不高，最终被闲置，难以融入日常安全运营流程。

安全牛分析

该困惑根源在于 BAS 技术专业性要求高，用户须具备网络攻防知识并熟悉复杂攻击链和日志分析方法。同时，企业内部可能缺乏相关专职人员，若 BAS 产品用户界面和操作流程设计不佳、自动化程度不足，会进一步增加上手难度。



BAS 用起来太复杂了，不知道从何下手？

安全牛建议

破解 BAS 使用复杂性的核心，在于转变一步到位的观念，采取产品+服务+流程三位一体的渐进式路径。首先，应选择具备高度自动化和 AI 赋能的易用产品，以技术手段降低操作门槛；其次，从标准化场景入手，逐步建立信心与能力；最后，借助厂商专家服务，将外部经验内化为组织能力，最终实现 BAS 从被闲置的工具到深度融入日常安全运营的价值回归。

具体建议如下：

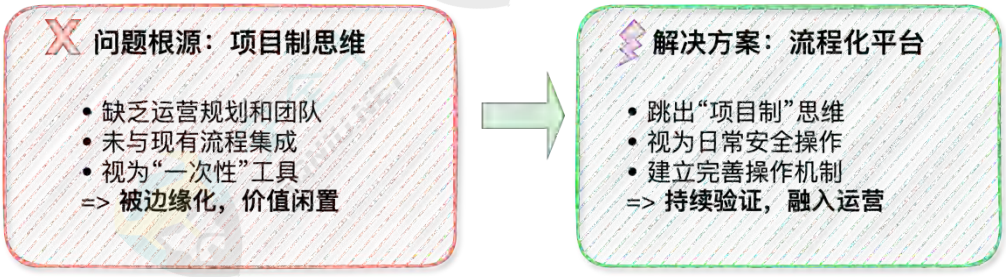
- 从标准化模板和基础场景循序渐进：企业初用 BAS 时，可先选择内置的标准化攻击模板和基础验证场景，如验证 Web 应用防火墙（WAF）对常见 SQL 注入、跨站点脚本（XSS）的拦截效果，或验证 EDR 对已知恶意文件的检测能力等。这些模板操作简单，能验证 BAS 系统功能和无害化能力，可以帮助企业快速得到验证结果，并了解产品。
- 充分利用 AI 辅助攻击编排与日志分析：BAS 产品正深度融合 AI 技术以降低使用难度。选型时，企业应重点考量产品 AI 赋能能力，如具备 AI 辅助攻击场景智能编排与生成功能，能通过自然语言交互或智能推荐，自动生成复杂攻击预警和测试指标；具备 AI 驱动的日志智能分析能力，可自动化解析、归一化海量日志，并深度关联判断，自动识别攻击行为，判断防护效果，实现验证结果自动化判断，减少人工干预，简化日志分析。
- 重视产品的可视化与可读性：易读的用户界面和直观的可视化报告是降低理解成本的关键。企业应选择提供整体防护态势可视化功能的 BAS 产品，如能以沙盘或业务拓扑图形式，直观展现攻击路径、被突破防护节点及与业务系统关联的风险点，帮助非专业背景管理者和初级安全人员更好理解安全风险和验证结果。
- 利用厂商的专家服务和持续培训：初级安全人员使用 BAS 时易遇知识和经验不足问题。企业可充分利用厂商提供的专家服务和持续培训资源，领先 BAS 厂商凭借攻防背景和安全实验室，能提供全方位指导，助力团队掌握实操技能，解决实施中的具体问题。

问题三：BAS 买回来就吃灰，如何实现常态化运营？

不少企业在采购 BAS 系统后，仅进行几次测试获取报告，随后系统便被闲置，无法融入日常安全运营流程，成为间歇性投入。这种吃灰现象使 BAS 的持续性价值难以体现，安全投入无法持续实践，最终沦为摆设。

安全牛分析

该问题根源在于企业缺乏明确的 BAS 运营规划、专业运营团队，且未能将 BAS 与现有安全流程和管理体系集成。企业将 BAS 视为项目制工具而非流程化平台，未深刻理解其持续性和自动化特点，缺乏专人负责日常管理和运营，也无年度、月度、周验证计划，导致 BAS 在安全运营中被边缘化。



BAS 买回来就吃灰，如何实现常态化运营？

安全牛建议：

要让 BAS 摆脱吃灰的宿命，核心在于思维模式的根本转变：从一次性项目采购转向持续性能力运营。这需要建立一个以人为本、以规划为纲、以流程为体的运营体系。通过明确责任、融入日常、闭环优化，将 BAS 从孤立的测试工具，打造成为驱动企业安全水位持续提升、量化安全投入价值的核心引擎。

- 设立专人负责并制定详细运营规划：BAS 需明确责任人进行日常管理和运营。企业可设专职人员或指定现有安全运营团队核心成员负责 BAS 系统维护，依据企业安全目标和威胁动态，规划、编排、调整验证任务，并制定年度、月度、周验证运营计划，将 BAS 任务纳入日常安全运营考核指标，确保持续运行和效果。
- 将 BAS 融入日常安全运营流程：企业应将 BAS 验证任务纳入现有安全运营流程，如针对高危资产和关键安全产品设定周期性、自动化巡检验证任务，实现实时感知安全策略威胁变化、产品状态异常或新风险。同时，将 BAS 验证作为 IT 或业务变更管理流程关键环节，重大变更后进行专项验证，确认未引入新安全风险。
- 强调并实现持续验证的长期价值：网络环境和攻击手段动态变化，安全防护能力易衰减。BAS 的价值不仅在于发现已知问题，更在于发现因配置、策略老化、新业务上线或外部环境变化带来的潜在风险。

自动化验证可弥补传统安全评估盲区，确保企业安全防护体系的长期稳定。持续运行模拟攻击，能持续提升防护体系强度，实现安全保障的长期成效。

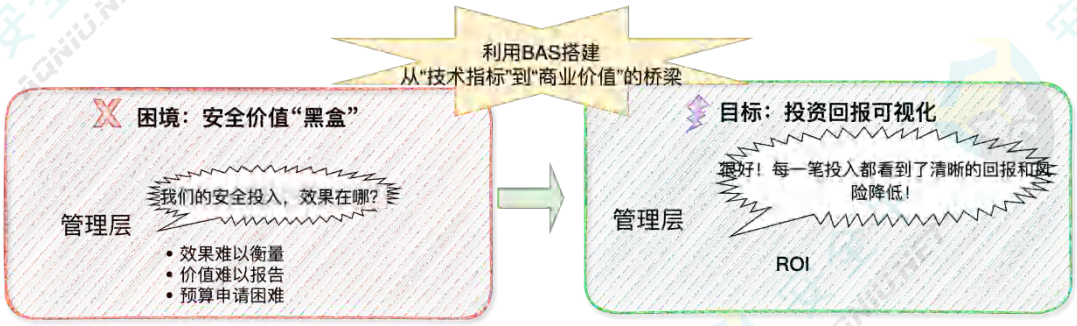
- 构建发现－分析－修复－复测的闭环机制：BAS 的常态化运营需与闭环优化结合。企业要明确问题解决迭代过程，利用 BAS 复测验证。安全缺陷修复后，立即通过 BAS 复测，自动验证修复效果，判断问题是否解决，实现自动化风险闭环管理，将安全操作从被动响应转向主动防护。

问题四：安全投入效果看不见，BAS 如何量化价值?

许多企业安全负责人面临安全投入巨大，但安全效果难以衡量的困境，难以在管理层报告时体现安全业务的工作价值和投资回报，导致计划和预算审批困难。传统安全评估结果多为抽象漏洞列表或定性报告，缺乏与业务风险关联的量化指标，使安全部门难以论证安全工作对业务的实际贡献。

安全牛分析

该困惑根源在于传统安全评估手段难以提供量化的安全效果数据，导致安全业务的工作价值难以精确地积累和呈现。此外，安全团队可能缺乏将技术指标与业务价值关联的沟通能力，使安全工作的实际价值被低估。



安全投入效果看不见，BAS 如何量化价值?

安全牛建议

BAS 通过将抽象的攻防对抗过程，转化为可量化、可追溯、可对比的指标（如覆盖度、拦截率、MTTD），破解了安全投入效果看不见的困境。使得安全部门不仅能证明自身工作的价值，更能以数据驱动的方式指导产品选型与预算决策，最终实现安全投入的精细化管理和最大化投资回报（ROI）。

- 企业应将 BAS 视为实现安全价值可视化的核心工具，利用其量化评估能力，将抽象安全风险转化为易懂指标，洞察安全投入价值，驱动安全建设与运营优化：
- 明确量化目标与指标：目标可包括提升关键安全产品拦截率、降低整体攻击链平均检测时间（MTTD）、

降低预估损失率等。BAS 系统能将攻击链模型、ATT&CK 模型和威胁知识图谱融入攻击模拟，可视化防护效果，让安全价值和风险清晰可见。

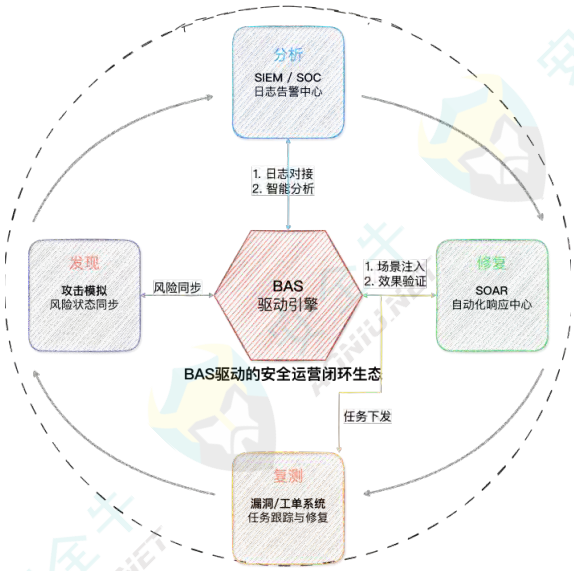
- 深入解读关键指标的业务含义：企业不仅要获取数据，更要理解数据背后的业务内涵。例如，防护覆盖度可展示安全防护体系对网络资产、业务系统和互联网暴露面的实际覆盖程度，帮助企业发现漏防区域；检测率/拦截率直接反映安全产品遭受特定攻击的成功率，通过 BAS 验证，若安全产品在 Web 攻击拦截能力上显著提升，可直接证明其部署后的实际成效。
- 利用 BAS 驱动数据安全投资决策：BAS 提供的量化数据是安全产品选型和能力投入的科学依据。企业可利用 BAS 对不同产品进行开箱即用测试和对比，评估漏报率、检出率，选择运维成本低、最适合自身需求的产品，避免采购和重复投资。BAS 能提供实战能力评价，助力企业基于实战效果进行更明智的投资。

问题五：BAS 如何实现安全运营闭环？

不少企业在采购 BAS 后，发现其与现有安全运营中心（SOC）、安全信息与事件管理（SIEM）、安全编排自动化与响应（SOAR）平台、漏洞管理系统或工单系统等安全工具和解决流程难以有效集成。这导致 BAS 验证结果成为信息孤岛，无法自动触发后续分析、响应和修复流程，安全运营效率难题依旧存在，无法实现发现问题－解决问题的自动化闭环。

安全牛分析

该问题根源在于企业安全产品体系间日志格式、API 标准接口不统一，安全操作流程自动化程度不足，依赖人工干预过多。同时，缺乏将 BAS 验证结果与现有安全事件管理、漏洞管理、工单系统有效关联的机制，致使 BAS 发现的问题难以及时转化为修复行动并有效跟踪。



BAS 驱动的安全运营闭环生态

安全牛建议

要实现安全运营闭环，BAS 的角色必须从孤立的风险发现器转变为联动的运营驱动引擎。其核心在于通过开放的 API 和智能日志分析，将自身深度嵌入到 SIEM、SOAR、漏洞管理和工单流程中。BAS 不仅是问题的发起者（触发自动化响应），更是修复效果的验证者（通过复测确认闭环）。这种深度集成将彻底打破信息孤岛，实现从发现到解决的自动化流程，将安全运营提升至智能、高效的新高度。

要实现安全运营闭环，BAS 的角色应从孤立的验证工具转变为联动的运营驱动引擎。其核心在于通过开放的 API 和智能日志分析，将自身深度嵌入到 SIEM、SOAR、漏洞管理和工单流程中。BAS 不仅是问题的发起者，更应是修复效果的验证者。这种深度集成将彻底打破信息孤岛，实现从发现到解决的自动化流程，将安全运营提升至智能、高效的新高度。

- 实现日志与其他系统的自动化对接与智能分析：企业应确保 BAS 能与 SIEM/SOC 平台进行 API 或 Syslog 的深度、实时对接，将模拟攻击触发的事件信息自动化上报至统一安全运营平台。同时，BAS 须具备多源日志的归一化处理和智能分析能力，精准解析海量日志，实现验证结果全自动化判断，简化安全团队工作量，提升准确率，为自动化响应提供高质量数据输入。
- 利用 BAS 驱动自动化响应与任务下发：BAS 应成为 SOAR 平台的验证场景输入和验证工具。企业可将 BAS 验证发现的安全缺陷，通过 SOAR 平台自动编排响应流程，如自动隔离受感染主机、自动封禁不良 IP，或自动向工单系统下发修复任务，同步更新资产管理系统中的风险状态，实现安全缺陷从发现到解决的高度自动化，缩短问题解决周期。
- 构建发现－分析－修复－复测的闭环流程：明确问题解决过程，利用 BAS 复测验证。安全缺陷修复完

成后，立即通过 BAS 复测，自动验证修复效果，判断问题是否解决，形成自动化风险闭环管理实践，提升安全操作效率，减少重复性工作。

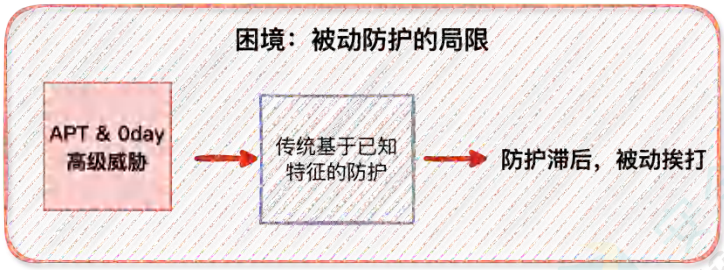
- 关注厂商的闭环能力规划与生态融合：选型时，企业应深入研究 BAS 厂商在自动化闭环方面的技术路线和生态合作策略，包括其与主流安全运营平台的联动能力，以及在自动下发工单、自动修复方面的规划，使 BAS 成为企业安全运营体系的驱动力，实现自动化安全治理。

问题六：如何应对高级持续性威胁与新型攻击，增强防护实战能力？

高级持续性威胁攻击（APT）具有定制化、定位性强、难以发现的特点，突发新型威胁和零日漏洞（0day）也使企业防不胜防。传统安全产品多基于已知特征检测，难以识别未知攻击，导致防护体系滞后，无法有效预警和应对，一旦被突破后果严重。企业缺乏对高级持续性威胁的深度情报分析和应对突发未知攻击的响应机制。

安全牛分析

高级持续性威胁的复杂性在于其多级、链式攻击过程和不断进化的入侵、隐匿技术。传统基于签名的防护难以识别变种和无文件攻击。企业虽有外部威胁情报，但缺乏将其转化为自身可验证工具和场景的能力。0day 漏洞的突发性使企业防护体系难以第一时间防护，无法预判影响，致使未知攻击时防护被动。



如何应对高级持续性威胁与新型攻击，增强防护实战能力？

安全牛建议

应对高级持续性威胁的核心，是实现从基于已知特征的被动拦截到面向未知威胁的主动免疫的战略升级。BAS 在此过程中扮演了高级持续性威胁陪练与防御体系教练的双重角色。通过将外部威胁情报转化为可执行的攻击，利用 AI 模拟未知威胁，最终以量化数据指导防御策略的精准优化。这个情报－模拟－优化的持续闭环，是企业在与高级持续性威胁的持续对抗中，构建动态、自适应安全韧性的关键。

- 将威胁情报转化为可执行的防护验证：企业应选择能将威胁情报（特别是 APT 组织的 TTP）转化为可执行攻击场景的 BAS 产品。此类产品拥有专业实验室和威胁情报研究团队，可追踪全球黑客组织，利用 BAS 在 APT 攻击来临前，用真实手段检验自身防护体系对各类攻击的检测和阻断能力，提升防护

接入能力。

- 利用 AI 新型模拟与变异能力攻击，提升防护泛化：面对不断演变的新型威胁和 0day 漏洞，企业需关注 BAS 产品中 AI 技术的深度应用，能根据环境或威胁情报，自动生成或变异出新的、具有对抗性和不可预测性的攻击。AI 驱动的攻击生成能力可模拟传统签名无法识别的变种攻击和无文件攻击，有效测试防护体系的泛化检测能力和对未知威胁的应对能力。一些领先 BAS 产品已具备高级 APT 模拟能力，能帮助企业验证其应对前沿威胁的能力。
- 增强防护能力，指导优化：BAS 不仅要能模拟，更要能量化防护效果，为企业提供改进方向。企业可利用 BAS 指标，如 APT 攻击模拟爆发率 ATT&CK 检测覆盖率横向攻击包围率，评估防护体系对高级持续性威胁的防护能力。若发现短板，企业应立即优化策略或考虑产品升级，并通过快速调整安全策略、升级安全产品版本、引入精准威胁情报源，推动闭环优化与情报反哺，持续提升防护体系对高级持续性威胁的感知、判断和应对能力。

问题七：多分支/云环境复杂，是否可以全面覆盖这些复杂环境？

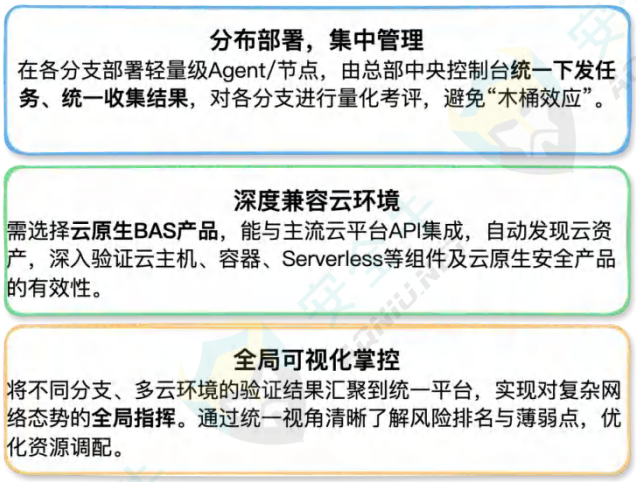
对于拥有众多分子公司、上下级部门或采用混合云、多云架构的大型集团企业，网络环境复杂，分子公司安全能力参差不齐，地域分散导致管理风险大；云环境动态多变，传统工具难以深入验证云上防护效果。这使集团总部难以实现对整体安全态势的统一管理、评估，出现木桶效应，单个薄弱环节风险可能蔓延至整个集团。

安全牛分析

传统安全管理工具和评估手段对复杂环境能力不足。物理分散的外部分子公司难以统一安全管理平台和标准化评估，导致安全水位难以统一。云环境的弹性、动态性和复杂性使安全边界模糊，传统部署模式难以覆盖，云上配置错误或 API 暴露风险高，增加防护和验证盲区。各分区系统间的数据孤岛也阻碍了集团内部的整体安全建设。

安全牛建议

面对多分支、多云的复杂环境，BAS 的核心价值在于扮演安全度量衡与统一指挥塔的角色。通过分布式部署，集中式管理的架构，将分散的安全验证能力汇聚，破解了传统工具难以覆盖、难以统一评估的难题。这不仅能有效识别集团整体的木桶短板，更能以全局可视化的量化数据，驱动总部分支协同治理与资源优化，最终实现复杂环境下整体安全水位的持续提升。

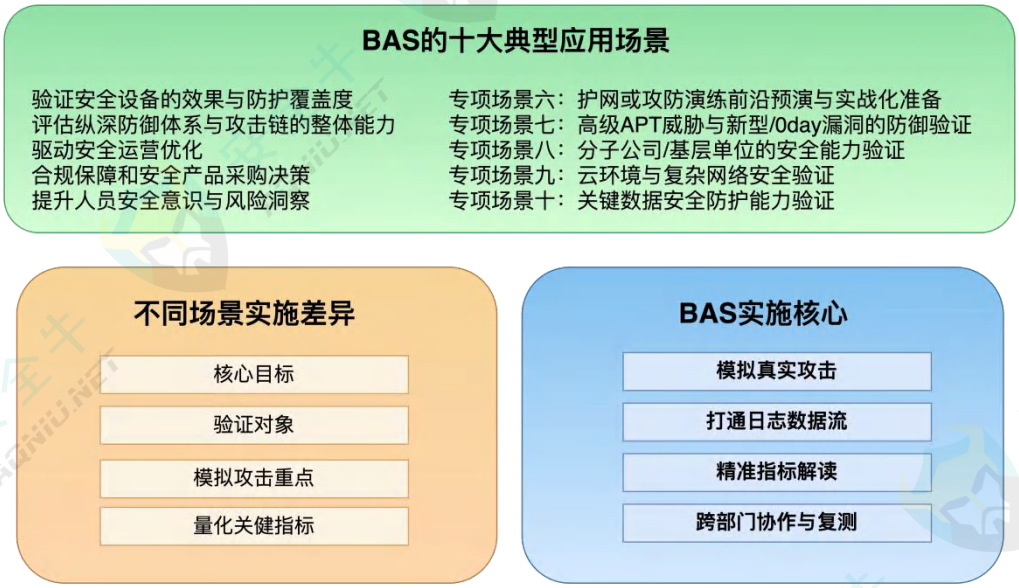


覆盖多分支/云环境

- 利用 BAS 的分布部署与集中管理实现统一管控：对于集团企业，建议选择支持在各分支部署轻量级 Agent 或虚拟节点的 BAS 产品，实现安全验证和评估。集团总部通过中央控制台统一下发任务，接收量化评估结果，对各分支安全风险进行量化多维考评，指导区域管理考核、预算分配和建设规划，避免木桶效应。
- 确定 BAS 对复杂云环境的深度兼容与验证：业务上云后，企业需验证云上安全防护有效性。建议选择能深入云环境内部，模拟针对云主机、云服务、容器、Serverless 等云攻击组件的 BAS 产品。此类产品与主流云平台 API 深度集成，自动发现云资产，验证云防火墙、云 WAF 等云原生安全产品有效性，识别云配置缺陷，模拟新兴威胁，有效降低混合云架构风险。
- 追求一体化管理与可视化，实现全局掌控：BAS 应能将不同分支、云环境的验证结果汇聚到统一平台进行可视化展示，实现对复杂生态网络安全态势的全局指挥。通过统一视角，企业清晰了解各分支安全风险排名和混合云架构下的风险点，进而开展统一优化和调配。

第八章 BAS 场景应用实战指南

BAS 的十大典型应用场景涵盖了安全管理从局部到宏观（点、线、面）、从技术到管理的渗透，以及对复杂环境的适配，充分体现了 BAS 验证能力的全面覆盖性。通过对 BAS 的十个常用 BAS 场景的落地实战，可以帮助企业构建从点到面、由内而外、从技术到管理的全面安全能力评估体系，帮助企业的安全从黑盒子，迈向可视化价值，实现主动性、实战化、数据驱动的安全治理，从而有效应对不断演进的复杂威胁。



应用场景实施的不同

BAS 的不同的应用场景，其目标不同，并导致验证对象、模拟攻击重点和量化指标。具体对比详见下表：

表 1:BAS 不同应用场景的对比

主要场景						
场景名称	核心目标	主要验证对象	攻击模拟重点	关键指标与关注点	难点与挑战	预期价值与拓扑
验证安全产品效果与防护覆盖度	掌握单点安全产品效益与资产防护覆盖度	防火墙、IDS/IPS、EDR、WAF、DLP	基础、高频攻击模板（SQL注入、XSS、端口扫描）	防护覆盖度、检测率/有效率、阻断率、误报率	日志对接品牌兼容性、代理部署无害化	对安全心中有数，安全产品配置与策略优化
评估纵深防御体系与攻击链的整体能	评估多安全产品联动合	多安全域安全产品（边界、	多阶段、多协议攻击链（钓	攻击链检测率、攻击路径图谱	攻击链复杂性、日志关联	攻击路径可视化，整体防

力	力，发现攻击链短板	DMZ、内网）、SIEM/SOC	鱼-横向－窃取复杂度）		全面性	御健壮性提升
量化安全风险与驱动安全运营优化	实现安全风险可量化评估，驱动运营流程优化	SIEM/SOC 平台、同时处理流程、SOAR 平台	有关验证、效率提升场景（Web 攻击、恶意文件投放）	安全风险评分/健康度、同样准确率/误报率、运维效率提升比例	SIEM/SOC 日志全面性、初始指标设定、模拟真实性	安全价值可视化，运营效率提升，疲劳缓解
合规和安全产品采购决策	为合规性提供实战证明，辅助安全产品选型	待采购/已部署安全产品、合规条款	产品性能对比测试、合规条款攻击验证	产品性能对比数据、合规性验证报告	合规条款转化、产品测试公平性	数据驱动采购决策，顺利通过合规审计
提升人员安全意识与风险洞察	提升员工安全意识，应对新型威胁	企业员工、邮件网关、终端安全产品、沙箱	仿真钓鱼邮件、新型威胁/0day 模拟行为	钓鱼邮件点击率/信息提交率、新型威胁防御可靠性	钓鱼邮件真实性与无害性平衡、0day 模拟的泛化目标	员工肌肉提升，应对未知威胁能力增强
专项 1-护网或攻防演练前预演与实战化准备	提前修复发现防护盲点，全面提升实战防御能力	所有可能成为攻击目标的安全产品和资产	护网高频攻击、全流程复杂攻击链（高强度、多轮次）	护网得分覆盖率、攻击成功路径数量减少率、高危面修复率	攻击模板时效性、大规模模拟无害化、攻击行为一致性	护网实战能力大幅提升，攻防知识库积累
专项 2－高级 APT 威胁与新型/0day 漏洞的防御验证	深度模拟高级持续性威胁，验证未知威胁防御能力	APT 防御安全产品、沙箱、NDR、EDR、SIEM/SOC	定制化 APT 攻击（TTPs）、AI 生成类型/0dayAPI	APT 攻击模拟告警/阻断率、新型威胁防御耐受度、ATT&CK 检测覆盖率	威胁情报获取与转化、0day 模拟的超高无害化技术	对未知威胁，核心资产安全
专项 3－分子公司/基层单位的安全能力验证	统一评估分散机构安全能力，确保集团整体安全	各郊区边界/本地安全产品、集团统一平台	从外部环形枢纽、环形内网外围集团资源	风险各漩涡多维考评、排名/评分、统一策略落地率	跨区域网络关联性、日志上报统一性、统一与差异平衡	集团安全治理水平提升，避免木桶效应
专项 4-云环境与复杂网络安全验证	评估云环境安全风险，确保云环境安全有效性	云原生安全服务、第三方云安全产品、云上传统安全产品	集装箱逃逸、云 API 补漏、对象仓库数据泄露	云资产防护覆盖率、云安全策略效率、集装箱逃逸/微服务攻击告警/阻断率	云环境动态性与复杂性、云平台 API 集成深度、云环境无害化	云新建安全防护有效，降低云上配置风险
专项 5－数据安全防护能力验证	验证敏感数据全生命周期防护，满足合规要求	DLP、数据库审计、加密、备份、访问控制、堡垒机	数据窃取（SQL 注入、WebShell 外传）、窃改	敏感数据风险泄露、数据勒索恢复可靠性、数据访问控制效果	数据识别准确性敏感、数据流转复杂度、无害化操作	数据合规保障，数据泄露/勒索风险降低

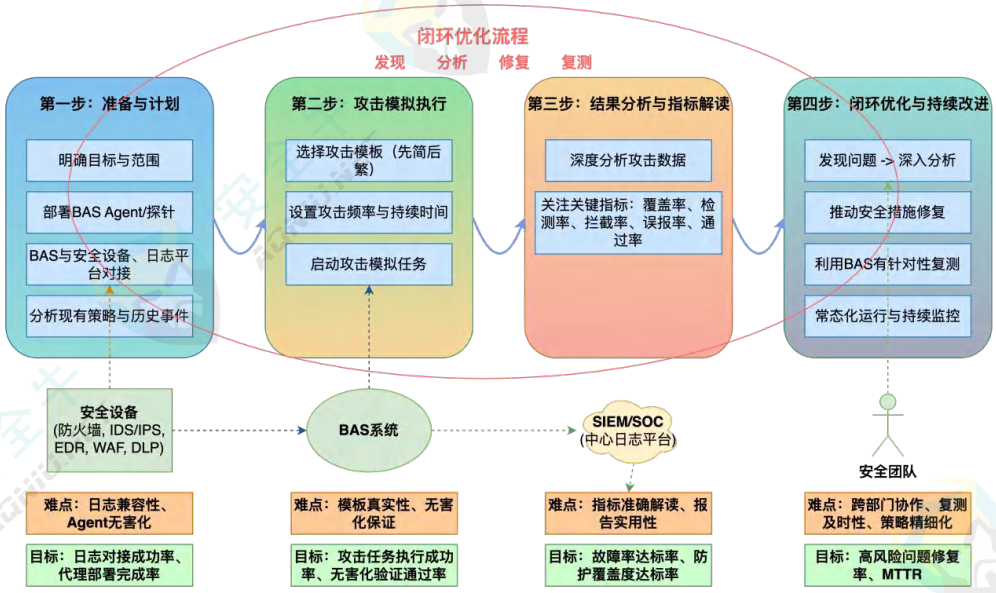
BAS 应用场景实施的差异对比

接下来，我们将针对这十大应用场景，详细阐述如何一步步运用 BAS 实现安全能力的实战验证与持续优化。

8.1 场景一：安全产品防护能力验证场景

企业内部部署多种安全产品（如防火墙、IDS/IPS、EDR、WAF、DLP 等），品牌与功能各异，企业往往难以精准掌握实际配置和策略是否存在漏洞或绕过风险。

本场景旨在通过 BAS 的自动化验证，确保企业部署的防火墙、入侵检测系统（IDS）、端点检测与响应（EDR）、Web 应用防火墙（WAF）和数据防漏（DLP）等各类安全产品功能模块以及策略是否持续有效，以及对资产防护的全面覆盖，从而消除企业安全顾虑。



场景一：安全产品防护能力验证场景

第一步：准备与计划

首先。企业应设定明确的目标和范围。从互联网边界安全产品（如 WAF、边界防火墙、互联网 IPS）着手，因为这些安全产品是抵御外部攻击的第一道防线，其有效直接决定了企业的入侵风险；待边界防护稳定后，再逐步深入内部网络，验证内网 IDS、EDR、堡垒机等安全产品。

其次。企业应在目标安全产品防护区域内部署 BAS 的 Agent。在验证目标安全产品所防护的区域内部（如 WAF 防护的 Web 服务器、EDR 部署的终端、IDS/IPS 监控的网络队列），部署 BAS 的 Agent，同时应确保 BAS 系统与目标安全产品及中心日志平台（如 SIEM/SOC）实现 API 或 Syslog 对接，精准筛选与安全产品阻断相关的核心日志，保障日志实时性和准确性；分析目标安全产品当前策略、配置缺陷及历史安全事件，为后续选择威胁攻击模板提供依据。

难点与关键点：

- 日志对接品牌兼容性：由于企业安全产品种类繁多，应确保 BAS 兼容并准确解析所有安全产品日志格

式至关重要。

- Agent 部署的无害化：确保 Agent 部署与运行不影响生产业务。

具体目标：

- 目标安全产品日志成功接入 BAS 平台。
- 代理成功部署上线并运行。

第二步：模拟攻击的设计编排和执行

企业在选择攻击模板时，应遵循先简单后复杂原则，先选取针对目标安全产品的基础、高频攻击模板。例如，验证 WAF 可选 SQL 注入、XSS 等常见 Web 攻击模板；验证 EDR 可模拟恶意软件投放等行为；验证 IPS/防火墙可选网络扫描等模板。BAS 产品通常配备图形化界面，方便用户进行攻击编排，如选择 Web 攻击模块指定目标 URL，选 SQL 注入模板及 Payload 类型。

攻击频率和持续时间的设置应依据风险等级与安全产品重要性。如对边界 WAF 等关键安全产品，建议每天自动化快速巡检，每周全面验证；内部安全产品可设为每周或每月一次。环境准备就绪后，在 BAS 平台启动攻击模拟任务，自动化执行高仿真攻击行为，触发目标安全产品响应。

难点与关键点：

- 攻击模板的真实性与多样性：确保模板能模拟真实黑客手段，避免仅限于 PoCC。
- 无害化保证：确保攻击的运行对生产业务的无害化。

具体目标：

- BAS 系统成功执行模拟攻击任务。
- 模拟攻击未对业务系统造成任何不良影响。

第三步：结果分析与指标解读

攻击模拟完成后，需深度分析数据并转化为可操作洞察。企业应重点关注防护覆盖度、检测率、阻断率、误报率等关键指标，可参考同类场内行业内同类企业场景中实现的提升效果作为优化参照。

防护覆盖率能洞察安全防护对网络资产等实际覆盖程度，揭示漏防区域；

检测率/有效率/阻断率/误报率反映安全产品在模拟攻击场景下的防护表现，验证配置与规则是否精细。企业可依业务风险设定及格分数，如 WAF 对 SQL 注入阻断率不低于 95%，EDR 对恶意软件检测率不低于 90%等，并参考同类企业场景中提升效果优化。

难点与关键点：

- 指标的准确解读：避免片面追求高分，要结合业务风险和实际威胁来理解指标。例如，提高检测率，如果关键攻击仍能成功，则防御仍然存在问题。
- 报告的实用性：BAS 生成的报告应有具体的修复建议和优先级排序。

具体目标：

- WAF、EDR 等核心安全产品对关键故障故障率达标。
- 核心资产防护覆盖度达基线标准。

第四步：闭环优化与持续改进

发现问题不等于提升安全水平，需将短板转化为改进措施并验证效果，这是 BAS 核心价值闭环所在。其闭环管理是攻击－发现－修复－复测的迭代过程。当 BAS 验证报告指出防护缺陷（如某 WAF 规则被绕过，某 EDR 策略未生效等），应由专人负责团队深入分析，定位问题根源，判断是策略配置、软件版本还是安全能力缺失所致。接着，与 IT 运维等相关部门协同，依报告修复建议，实施安全措施，如优化 WAF 规则等。修复后，利用 BAS 系统针对性复测，并将优化后验证场景常态化运行，持续监控指标变化，发现新风险点则重启闭环流程，实现企业安全能力持续提升。

难点与关键点

- 跨部门协作与推动力：修复安全问题涉多部门，需专人团队具备强协调和推动能力，建立明确责任制。
- 复测的及时性与精准性：修复后立即复测，快速确认效果，复测应聚焦修复点。
- 策略的精细化调优：修复策略时避免引入新业务影响或错误报告。

具体目标：

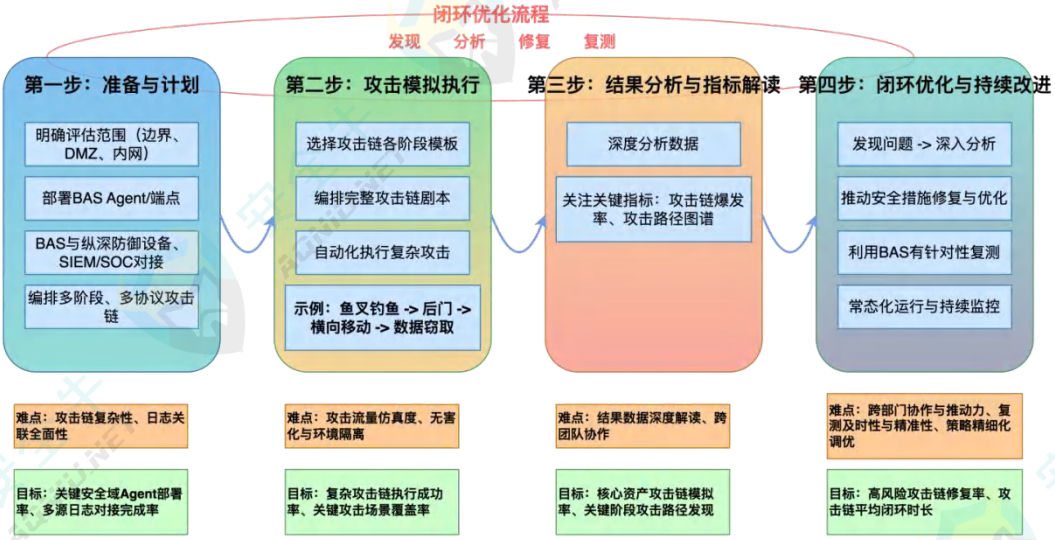
- BAS 发现的高/中危风险问题在规定期限内修复。
- 从 BAS 发现问题到修复验证通过的平均时间（MTTR）可控。

8.2 场景二：纵深防御体系防护能力验证场景

攻击者通常从边界到内网，再到核心资产，通常采用多层次、链式的攻击手法。企业虽部署了多个安全产品，但是这些安全产品各自为战、缺乏协调，防御策略间可能存在差异冲突或盲区，且难以全面捕获攻击者的横向移动路径，这些都易导致纵深防御失效。而是否能有效联动形成合力，整个防御体系的最短

板在哪里，往往是难以回答的问题。

评估纵深防御体系的关键在于突破单点安全产品验证的局限，从攻击者视角出发，模拟多层次、链式的攻击手法，验证安全产品间的联动效果以及整个防御体系的最短板。通过 BAS 实现攻击路径可视化，确保防御体系的完整性和有效性。本场景的目标是突破单点安全产品验证的局限，从攻击者视角评估整个纵深防御体系的效果，发现攻击链中的关键短板，并实现对攻击路径的清晰可视化，以确保整个防御体系的有效性。



场景二：纵深防御体系防护能力验证场景

第一步：准备与计划

纵深防御体系评估应设定全面、深入的验证范围。企业要明确本次纵深防御评估的范围，通常应涵盖互联网边界、DMZ 区、内网核心业务区、办公网等多个安全域，并识别各安全域内的关键资产、业务系统及其访问关系。在关键安全区域内（如内网服务器、办公终端、DMZ 区中的跳板机）部署 BAS 的 Agent/端点，确保这些 Agent 能模拟攻击者在不同阶段的行为，进行跨区域、跨安全产品的模拟攻击。同时，确保 BAS 能与所有相关纵深防御安全产品（防火墙、IDS/IPS、EDR、DLP）、堡垒机、流量分析系统、SIEM/SOC 平台进行日志对接，筛选出与攻击各链阶段行为（预警、横向移动、权限提升、数据外传）相关的日志。最后，结合企业自身网络架构、业务特点和威胁情报，选择或编排模拟多阶段、多协议的攻击链。

难点与关键点：

- 攻击链的复杂性：真实攻击链涉及多种攻击技术和安全产品，编排难度高。
- 日志关联的全面性：需收集攻击链中所有阶段、所有安全产品的日志，并被 BAS 平台准确关联。

具体目标：

- 确保 BASAgent 在核心安全域内关键资产上完成部署。
- BAS 平台成功对接并解析多层安全产品日志。

第二步：模拟攻击的设计编排和执行

企业应通过自动化方式执行复杂、多阶段的攻击行为。编排攻击链各阶段的攻击模板并将其形成完整攻击链。例如，初级访问阶段模拟鱼叉式钓鱼邮件或 Web 应用漏洞利用；执行与持久化阶段模拟脚本执行、后门植入；横向移动阶段模拟使用远程执行工具或利用 SMB/RDP 等协议进行网络移动；数据窃取阶段模拟敏感文件查找、打包并外传至外部服务器。BAS 产品通常提供图形化编排界面，用户可拖拽攻击模块，设置攻击参数，定义攻击顺序和条件依赖，定制复杂攻击路径，甚至可设置某一步攻击成功则自动触发后续攻击模块的逻辑。

攻击频率依业务关键性和合规要求而定，核心业务系统可设定每周或每月一次全面攻击链模拟，对护网或重要保障时期，应前期进行高强度、多轮次集中模拟。

难点与关键点：

- 攻击流量的仿真度：确保模拟攻击流量特征和行为与真实黑客高度相似，避免被安全产品轻易识别为测试流量。
- 无害化与环境隔离：模拟跨区域、多阶段攻击时要确保无害化，如数据窃取仅模拟生产环境，不真实窃取数据。

具体目标：

- BAS 系统成功执行多阶段攻击链的比例。
- 全面模拟关键业务场景下的攻击链。

第三步：结果分析与指标解读

深度分析数据并转化为可操作洞察，指导防御体系优化。企业应重点关注攻击链检测率和攻击路径图谱等关键指标。

攻击链检测率表示模拟攻击链在整个渗透过程中被防御体系成功阻断或告警的部分，是衡量企业整体防御健壮性、各安全产品间协同能力以及企业对复杂、多阶段攻击的整体抵抗力的核心指标，能洞察各安全产品间协同能力和企业对复杂、多阶段攻击的整体抵抗力。高攻击链检测率意味着企业安全防御体系在攻击过程中能有效阻断或检测攻击的多个阶段，从而降低攻击成功的可能性。若告警/阻断率低，则表明防

御链存在薄弱阶段，企业需深入分析攻击链在哪个阶段、被哪个安全产品未能有效告警/阻断，并优化策略和安全产品。如核心业务的攻击链目标达到 90%。

攻击路径图谱通过可视化方式展示攻击者渗透路径，包括攻击初始跳板、利用的漏洞和被绕过的安全产品，能帮助企业发现内部网络隔离连接、开放端口、弱口令等可能导致横向移动的风险。同时，企业要重点关注攻击路径图谱中的未检测点和热点危机点，深入分析原因，如策略配置错误、安全产品规则或日志未上报，并检查各安全产品在攻击链不同阶段是否产生预防动作，能否反映攻击真实进展。

难点与关键点：

- 结果数据的深度解读：BAS 报告数据量大，需专人团队深入分析，找出问题根因。
- 跨团队协作：纵深防御优化涉多个安全产品和业务部门，需加强沟通和推动。

具体目标：

- 针对核心资产的完整攻击链攻击模拟比例。
- BAS 发现的关键攻击阶段（如横向移动、权限提升）的攻击路径。

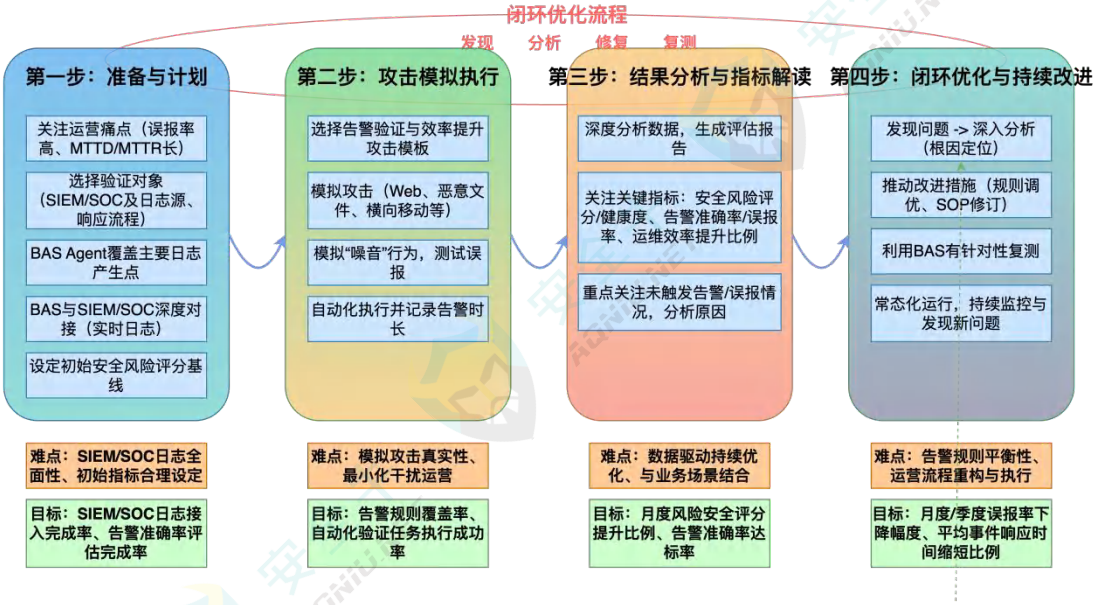
第四步：闭环优化与持续改进

（同场景一的第四部分）

8.3 场景三：安全运营验证场景

企业安全投入不断增加，但安全效果难以计量。同时，安全运营团队每天面对海量告警，误报多，易忽视关键威胁，疲于奔命。根源在于缺乏统一、可量化的安全评估体系和自动化验证机制。

本场景旨在通过 BAS 的自动化验证，实现安全风险的可量化评估，并通过攻击－发现－修复－复测闭环管理，持续优化安全运营流程与效率，将安全投入转化为清晰可见的业务价值。



场景三：安全运营验证场景

第一步：准备与计划

企业应持续关注安全运营痛点，如误报率高、MTTD（平均检测时间）/MTTR（平均响应时间）过长，规划 BAS 验证任务，如每日短周期巡视。选择验证的安全运营平台，核心是 SIEM/SOC 平台及其日志接入源，以及安全事件响应流程、SOAR 平台。确保 BAS 覆盖主要日志点和安全产品，全面模拟各种威胁行为。同时，确保 BAS 系统与 SIEM/SOC 平台深度对接，实时、完整收集模拟攻击产生的日志、事件。最后，了解当前 SIEM/SOC 的规则数量、误报率、人工处理平均时长，设定初步的安全风险评分基线或目标准确率。

难点与关键点：

- SIEM/SOC 日志的全面性：确保 BAS 能获取 SIEM 上报的所有安全产品日志，避免数据盲区。
- 初始指标的设定：合理设定初始安全风险评分，以便后续对比优化。

具体目标：

- BAS 成功关联 SIEM/SOC 中日志的比例。
- 完成第一次模拟攻击后，对 SIEM/SOC 准确率的评估。

第二步：模拟攻击的设计编排和执行

企业应通过自动化方式测试安全一致性机制和运营流程，模拟常见 Web 攻击、恶意文件投放、横向

移动等，触发 SIEM/SOC 告警，观察其准确性和及时性；也可设计噪音行为模拟，测试 SIEM 误报情况，并自动化执行这些场景，如运行 Web 攻击脚本后，BAS 自动发送攻击流量，等待 SIEM/SOC 平台产生告警，记录从攻击到告警产生时长。

攻击频率依据业务量和运营需求设置，核心安全产品的一致性验证可每天运行短周期验证，优化规则效果可在规则更新后立即复测。

难点与关键点：

- 模拟攻击的真实性：确保模拟攻击能触发 SIEM/SOC 的告警规则，而非被简单过滤。
- 对现有运营流程的最小干扰：自动化验证不影响日常安全运营。

具体目标：

- 模拟攻击预期产生告警的攻击场景与实际产生告警的比例。
- 自动化验证任务按计划执行的比例。

第三步：结果分析与指标解读

攻击模拟完成后，BAS 平台生成安全运营评估报告。此阶段关键是深度分析数据并转化为可操作洞察，优化安全运营流程和效率。企业应重点关注关键指标：

安全风险评分/健康度指数，是整体安全分数的量化指标，反映企业网络安全防护水平，分数越高风险越低。企业依据风险承受能力和合规要求设定及格分数，如目标风险评分不低于 90。

告警事件准确率/误报率揭示告警有效性及不一致性，帮助企业优化规则，减少告警疲劳，准确率目标达 85%以上，误报率低于 10%。

运维效率提升比例确定 BAS 自动化验证和分析减少安全运营团队在告警处理、问题排查上消耗的精力或时间，如通过 AI 决策引擎自动生成修复建议和触发防护更新策略，可大幅提升运维效率，甚至达 60%。

同时，企业应重点关注模拟攻击未触发告警的情况，以及模拟非攻击却触发告警的情况，深入分析原因。

难点与关键点：

- 驱动的持续优化：以量化指标变化趋势驱动运营流程和策略优化，避免为验证而验证。
- 与业务场景结合：将运营指标与业务风险结合，优先解决对业务影响最大的安全风险。

具体目标：

- 提升度安全风险评分。
- 季度准确率达到预设标准。

第四步：闭环优化与持续改进

（同场景一的第四部分）

难点与关键点

- 相关规则的平衡性：优化规则时，在精准与全面间找平衡，避免因追求低误报致漏报。
- 运营流程的重构：确保优化后的运营流程能被团队有效执行和重构，并定期复盘。

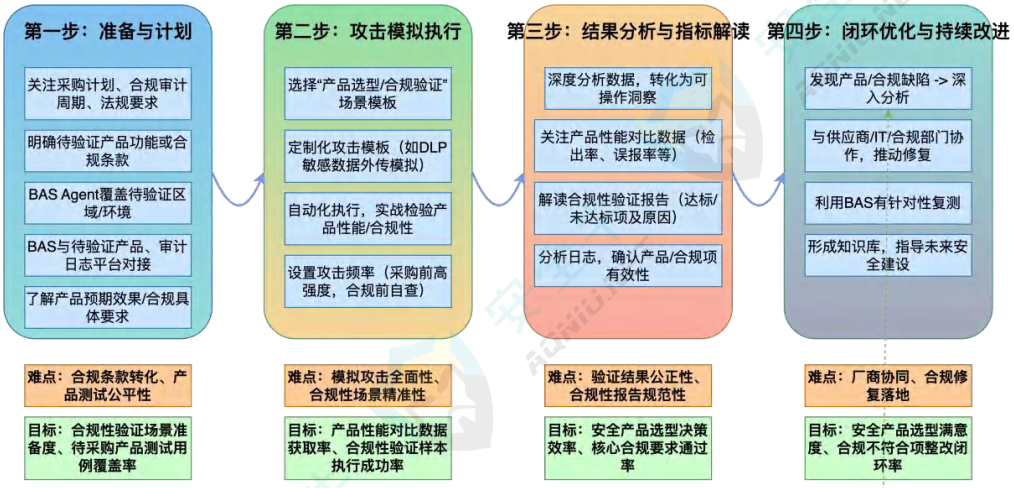
具体目标

- 月度/季度误报率下降。
- 平均事件响应时间（MTTR）总量减少。

8.4 场景四：合规保障验证和安全产品采购场景

等保、关基和行业监管等安全合规要求日益严格，企业需要开展频繁的自查工作，手工检查将耗费大量人力物力。同时，企业在安全建设中普遍面临安全产品选型困境，市面产品众多，难以确定哪个更适合自身环境，易盲目采购。

本场景核心是利用 BAS 的数据驱动验证能力，将抽象合规要求转化为可实战检验场景，并对多款产品公平基准对比。通过 BAS 量化结果，企业能满足安全合规要求，并做出明智安全建设决策，实现安全投入透明化与价值最大化。



场景四：合规保障验证和安全产品采购场景

第一步：准备与计划

企业应根据年度合规审计周期及重要法规政策落地要求、新产品采购计划，规划 BAS 验证任务，如选择验证产品或合规条款，针对待采购或已部署安全产品（如新一代防火墙、DLP 系统、漏洞扫描仪），明确其主要功能和预期效果，或明确合规审计涉及的关键信息安全控制措施（如入侵防护恶意代码防御访问控制等要求），或在新产品围测阶段验证或合规审核前自查自验，确保 BAS 代理覆盖模拟合规场景网络环境或待验证产品防护区域。同时，确保 BAS 系统能与合规审计日志平台和待验证产品对接，筛选出与产品功能验证和合规相关条款的日志。最后，企业要了解熟悉合规条款具体要求和待验证产品技术规格和预期效果。

难点与关键点：

- 合规条款的转化：将抽象合规要求转化为具体的 BAS 验证场景。
- 产品测试的公平性：确保对不同厂商产品测试在相同基准下进行。

具体目标：

- 与合规审计相关的合规性验证场景准备数量。
- BAS 测试用例覆盖待采购安全产品核心功能。

第二步：模拟攻击的设计编排和执行

企业应设计编排产品选型测试的攻击。例如，验证合规时，可编排模拟勒索攻击，测试有害代码防护系统是否识别和告警/阻断；测试 DLP 时，模拟多种敏感数据外传路径；验证入侵防护要求时，模拟高危漏洞利用；验证访问控制时，模拟非授权用户访问敏感系统。BAS 产品通常支持自动化执行这些场景，如

对比不同 WAF 性能，可编排相同 Web 攻击发送至各 WAF 防护测试环境对比响应。

攻击频率建议采购决策前集中高强度、多轮次测试，合规审计前集中自查自验，之后依需要周期性验证，确保合规持续达标。

难点与关键点：

- 合规性场景的精准性：确保模拟攻击行为与合规条款验证点精确匹配。
- 模拟攻击的监测性：确保模拟攻击能准确、全面反映产品真实能力，避免偏颇。

具体目标：

- 成功执行所有合规性验证样本。
- 成功获取待选产品关键性能对比数据。

第三步：结果分析与指标解读

企业应深度分析数据并转化为可操作的洞察，指导安全建设决策和合规改进。企业应重点关注合规性验证报告不合规项和产品性能对比数据等关键指标。

合规性验证报告不合规项是合规性验证报告中详细描述通过 BAS 实战验证的不合规项，并指出未达标项及原因，尤其在关键信息基础设施领域。企业需重点检查同一攻击下不同产品日志差异、级别、消除事件，包括日志能否说明安全控制措施有效，以及未通过验证合规项的日志中是否有详细攻击路径和失败原因。

产品性能对比数据观察不同安全产品在相同 BAS 模拟下的检出率、阻断率、误报率等对比数据，帮助企业选择适配自身环境和需求的产品，避免盲目采购。在评估时，依据业务安全容忍度设定标准，并关注产品在关键攻击场景下的表现。

难点与关键点：

- 合规性报告的规范性：确保 BAS 生成的合规性报告格式规范，便于提交审计机构。
- 证结果的公正性：确保 BAS 验证过程侦查性和公正性。

具体目标：

- 通过核心合规中技术控制措施要求率：关键信息基础设施和等保障要求，经 BAS 验证的比例。
- 从启动测试到完成采购决策的平均时间。
- 基于 BAS 测试结果选型的新产品，在实际运营中的满意度。

第四步：闭环优化与持续改进

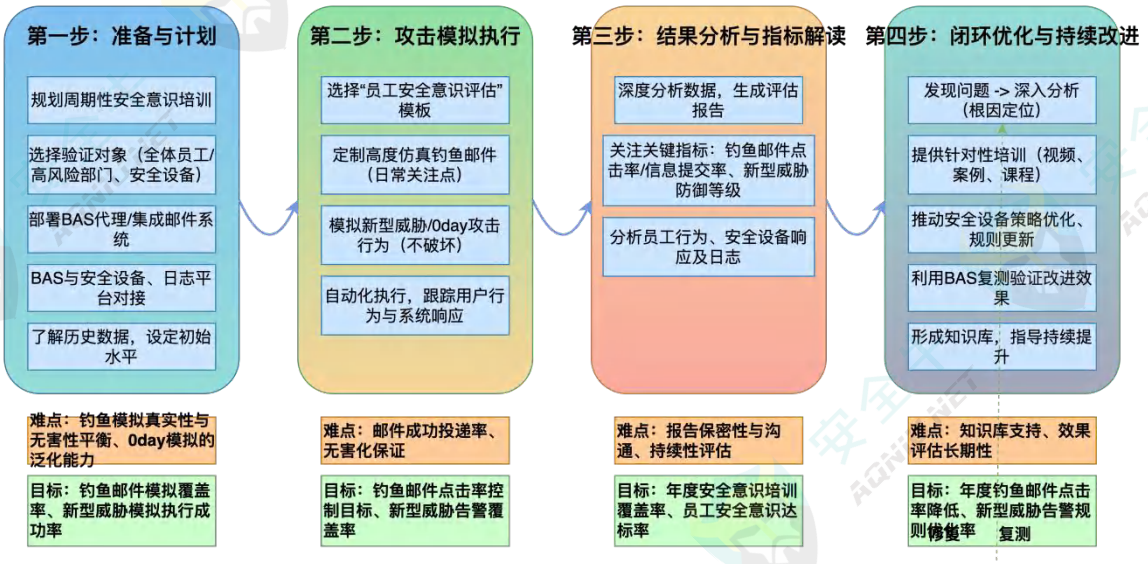
（同场景一的第四部分）

具体目标：

- BAS 发现的合规不符合项，在规定期限内完成整改并通过复测的比例。

8.5 场景五：钓鱼演练与风险洞察验证场景

人员是网络安全中最薄弱的环节，可能因无意点击钓鱼邮件、访问恶意链接导致内部系统失守。面对新型威胁和未知 0day 漏洞，企业难以预判其影响。本场景旨在通过 BAS 的实战化模拟，将安全意识教育转变为风险体验，提升员工免疫力和风险洞察能力，构建主动、动态、有针对性的人员安全防线，强化企业整体安全防御能力。



场景五：钓鱼演练与风险洞察验证场景

第一步：准备与计划

企业为安全意识提升和风险洞察活动做好准备。规划周期性安全意识培训活动，如每季度全员钓鱼邮件模拟或新型威胁的模拟。选择验证对象，包括全体员工或特定高风险部门（财务、IT、研发），以及邮件网关、终端安全产品、沙箱等安全产品。部署 BAS 代理以覆盖人员节点，或配置 BAS 与企业邮件系统集成。同时，确保 BAS 系统能与邮件网关、终端安全产品、行为日志平台对接，筛选出邮件投递、用户点击、恶意程序执行、网络连接等日志。最后，企业要了解安全意识培训情况、历史钓鱼邮件点击率，并设定初步水平。

难点与关键点：

- 模拟真实性与无害性平衡：钓鱼邮件要足够有效，但又不能真正造成伤害。
- 0day 模拟的削弱：0day 模拟的目的是泛化防御能力，而非验证特定漏洞。

具体目标：

- 钓鱼邮件成功投递到目标员工邮箱。
- BAS 成功模拟新型威胁行为。

第二步：模拟攻击的设计编排和执行

企业应设计编排员工安全意识评估的攻击，如自定义制作高度仿真的钓鱼邮件模板，内容可围绕工资调整、会议通知、快递异常、税务申报等员工日常关注点，并嵌入恶意链接或附件。例如，设置邮件发送时间、目标员工列表，并跟踪用户点击。针对风险洞察，利用 BAS 的威胁情报库和 AI 能力，生成针对最新的，甚至 0day 级别的新型攻击，例如对于新型威胁，设定其在事件的执行路径和行为特征。

攻击频率建议钓鱼邮件每季度进行一次，每次间隔调整模拟内容；新型威胁分析每月或每季度一次，有新高危威胁情报时及时专项验证。

难点与关键点：

- 邮件成功投递率：避免被邮件网关阻断，确保模拟效果。
- 无害化保证：严格控制模拟攻击范围和影响，防止对业务系统或员工造成真实伤害。
- 具体目标

具体目标：

- 逐步降低模拟钓鱼邮件点击率。
- BAS 模拟的新型威胁被安全产品成功阻断。

第三步：结果分析与指标解读

企业深度分析数据并转化为可操作洞察，指导安全意识培训和防御体系优化。重点关注：

钓鱼邮件点击率/信息提交率反映员工安全意识水平，数字越低越好，能帮助企业发现薄弱环节，为培训提供依据，优秀企业通常将点击率控制在 5%以下。

新型威胁防御度评估企业防御体系对未知威胁的应对程度，助力企业发现防护盲区，指导防御体系升

级。企业需关注哪些员工点击链接/附件，是否提交敏感信息，以及终端安全产品或 APT 防御产品是否对模拟威胁产生预防内容，是否准确。

难点与关键点：

- 报告的保密性与沟通：钓鱼邮件模拟结果涉员工隐私，报告需妥善处理，并以教育为目的沟通。
- 持续性：安全意识提升是长期过程，需持续模拟和培训。

具体目标：

- 所有员工参与 BAS 安全意识模拟。
- 结合点击率和后续培训效果，员工安全意识的整体达标率提升。

第四步：闭环优化与持续改进

（同场景一的第四部分）

难点与关键点：

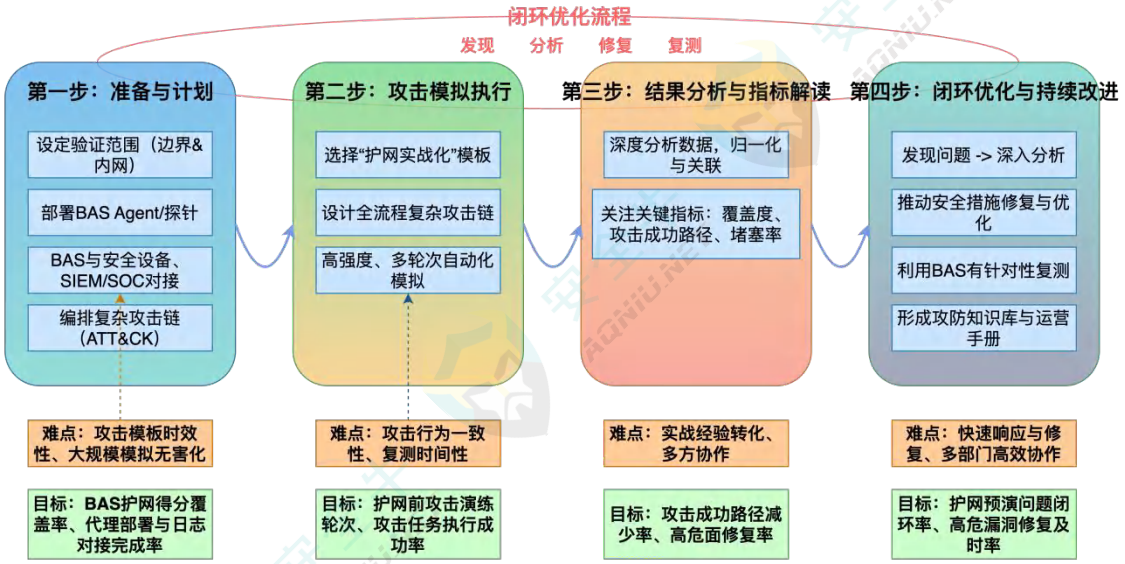
- 知识库支持：安全意识培训需知识库持续支持和资源投入。
- 效果评估的长期性：安全意识提升是渐进过程，需长期评估。

具体目标：

- 相比上一年度，钓鱼邮件模拟点击率降低。
- 根据 BAS 模拟结果，新增或优化新型威胁规则的比例。

8.6 专项场景六：攻防演练前验证场景

国内护网行动和攻防演练频繁且强度高、范围广，给企业带来巨大实战压力。企业普遍缺乏对自身攻击面的持续性、动态感知，对演练中常见攻击手段缺乏常态化预演，担心暴露面资产未收敛、无法有效防御真实攻击，导致在演练中被攻破。本场景目标是利用 BAS 进行高强度、多轮次前期预演，动态感知攻击面，提前发现并修复防护盲点，全面提升企业在护网中的实战防御能力。核心能力是紧跟护网最新威胁、模拟真实攻击链、精准量化防护效果，并构建发现－分析－修复－复测快速闭环，最终形成可持续提升的攻防知识库，从容应对实战压力。



场景六：攻防演练前验证场景

第一步：准备与计划

为护网预演设定明确的验证范围并准备全面的攻击剧本。建议企业在演练前至少一个月开始 BAS 验证任务，并在整个准备阶段持续验证，同时，应深入关注历年护网中高频出现的攻击类型、漏洞利用手段以及红队惯用的渗透路径，以便构建更具针对性的防御体系。企业需全面确定应验证的安全产品范围，覆盖所有可能成为攻击目标的边界安全产品（如防火墙、WAF、IPS）、内网安全产品（如 IDS、EDR、准入控制、堡垒机）以及核心业务系统和重要资产。

在关键节点，如互联网暴露面服务器、内网核心业务主机和高价值终端等重要区域部署 BAS 的 Agent/探针，并确保其与 BAS 管理平台网络调用正常。同时，确保 BAS 系统能够与所有相关安全产品和 SIEM/SOC 平台进行日志对接，筛选出与护网高频攻击、横向移动、权限提升等相关的告警、阻断、审计日志。最后，借鉴历史护网经验、最新威胁情报和 ATT&CK 框架，选择或编排覆盖护网常见攻击手段和渗透路径的复杂攻击链脚本，如利用 0day 漏洞渗透核心数据库。

难点与关键点：

- 攻击模板的时效性：护网攻击手段更新迅速，要求 BAS 攻击库能够及时更新并保持高度真实性。
- 大规模模拟的无害化：大规模模拟的无害化在生产环境中进行高强度模拟时，要严格控制，避免对业务造成影响。

具体目标：

- 确保模拟覆盖所有历年护网得分或高频攻击手段。
- 所有关键演练区域的代理部署完成且日志对接成功。

第二步：模拟攻击的设计编排和执行

通过自动化方式执行护网场景下的真实对抗行为。企业应利用 BAS 产品的攻击编排能力，设计编排涵盖护网全流程的复杂攻击链攻击，例如模拟护网高频 Web 漏洞利用、常见服务弱口令爆破、内网横向移动获取数据的完整攻击链。在执行过程中，应确保 BAS 系统攻击流量高度仿真，模拟行为设计精巧，既能有效触发安全产品响应，又能避免对生产业务造成影响。

攻击频率建议在护网前 1-2 个月，设定每周 2-3 次高强度、多轮次自动化模拟，以进行充分的预热和问题发现；临近护网时，可增加到每天 1-2 次的快速验证，确保关键修复及时生效。

难点与关键点：

精确模拟攻击者的行为，使其能够有效绕过或隐藏自身，从而突破安全产品的检测；

- 复测的及时性至关重要，每次修复后，必须立即通过 BAS 进行复测，以验证修复效果。

具体目标：

- 完成多轮 BAS 模拟攻击演练。
- 保证模拟攻击的真实性，确保 BAS 系统能够成功执行所有模拟攻击任务

第三步：结果分析与指标解读

BAS 系统自动化完成日志的归一化和关联，并生成详细的护网前沿预演报告。企业应深度分析这些数据，并将其转化为可操作的洞察，以指导防御体系的精准优化。应重点关注以下量化指标：

“防护覆盖度”反映企业安全防护对网络资产、业务系统和互联网暴露面的实际覆盖程度，能够精准定位和消除“漏防”区域，例如，通过 BAS 验证，防护覆盖度可从部分路径提升至 100%；

“攻击成功路径数量”反映模拟攻击渗透到核心资产的路径条数，该数字越低，防御能力越强，表明防御体系对实战攻击的有效阻断能力；

“高危漏洞利用阻断率”则直接衡量防御体系对护网常见攻击手法的防御成功率。企业可依据自身业务特性和合规要求设定“及格分数”，例如，防护覆盖度目标达 100%，攻击成功路径数量趋近于零，高危漏洞利用阻断率目标在 95%以上。

重点关注 BAS 模拟报告中“异常”或“未生效”的攻击路径，深入分析安全产品未能识别或阻止的原因，检查告警内容与攻击的匹配度，以及日志上报的时效性。

难点与关键点：

- 将实战经验有效地转化为 BAS 攻击库，确保其攻击模板的真实性和有效性；
- 多方协作至关重要，护网准备涉及多个部门，安全部门需与 IT 运维、业务等多方高效协作，共同推动问题解决。

具体目标：

- 对比之前的模拟结果，显著减少攻击成功路径数量。
- 将 BAS 发现的互联网高危风险在护网前修复并复测通过。

第四步：闭环优化与持续改进

发现问题不等于提升安全水平，将短板转化为改进措施并验证效果才是 BAS 发挥核心价值，实现防御体系螺旋式上升的关键。BAS 的闭环管理是一个“攻击-发现分析-修复优化-复测”的迭代过程。

应由专人负责团队深入分析 BAS 指出的防护缺陷，例如某 WAF 规则被绕过，或某 EDR 策略未生效等，并定位问题根源，判断是策略配置、软件版本还是安全能力缺失所致。接着，与 IT 运维等相关部门协同，依据报告修复建议，实施安全措施，如优化 WAF 规则、升级补丁、加固网络隔离等。修复后，应利用 BAS 系统针对性“复测”，验证优化效果，并将优化后验证场景常态化运行，持续监控指标变化，发现新风险点则重启闭环流程，最终实现企业安全能力的持续提升。

难点与关键点

- 快速响应与修复，护网时间紧迫，要求发现问题后能够迅速响应和修复，缩短问题闭环周期；
- 多部门高效协作是关键，需确保安全团队、IT 运维、开发团队间沟通顺畅，形成高效协作机制。

具体目标

- 护网前对 BAS 发现的问题完成修复，并实现高闭环率，
- BAS 发现的弱点应在指定期限内完成修复。

8.7 专项场景七：高级 APT 威胁安全防护验证场景

企业缺乏对高级持续性威胁的深度情报分析和转化能力，面对 APT 的定制化、聚焦性强的特点，以及突发新型威胁、零日漏洞（0day），企业常担心难以预警和响应。

本场景目标是利用 BAS 的强威胁情报能力和 AI 技术，深度模拟高级持续性威胁，切实验证企业防御

未知威胁，确保核心资产安全。核心是利用 BAS 的威胁情报和 AI 技术，实现高级持续性威胁深度模拟与实战验证，通过将情报转化为动作脚本、模拟高级迂回技术、快速防御效果并驱动持续闭环优化，帮助企业构建针对未知威胁的防御，确保核心资产在严重攻击前绝对安全。



场景七：高级 APT 威胁安全防护验证场景

第一步：准备与计划

企业应为高级持续性威胁和 0day 漏洞验证活动充分准备。持续关注权威威胁情报平台、安全厂商发布的 APT 活动报告、新型漏洞预警和 0day 披露，规划 BAS 验证任务，如收到高优先级 APT 威胁情报后第一时间模拟验证。应在关键业务系统、高价值数据资产区域及潜在受攻击终端部署 BAS 代理，确保模拟高级持续性威胁复杂行为。同时，确保 BAS 系统能与 APT 防御产品、沙箱、EDR、NTA、SIEM/SOC 平台深度对接，实时收集同类日志。深入分析 APT 组织的攻击策略、技术和过程（TTPs），理解新型漏洞利用原理，选择或编排能复现高级持续性威胁行为的攻击脚本。

难点与关键点：

- 威胁情报的获取与转化：及时获取高质量 APT 威胁情报并转化为 BAS 脚本，需专业能力。
- 0day 模拟的无害化：模拟 0day 攻击需超高无害化技术，避免破坏生产环境。

具体目标：

- BAS 成功获取 APT 威胁情报并转化为新的可执行模拟用例。
- BAS 攻击库中新增的 0day 模拟攻击样本数量。

第二步：模拟攻击的设计编排和执行

企业应设计编排高级 APT 威胁验证的攻击模拟。例如，模拟横向移动获取权限等。并利用 AI 能力生成针对最新甚至 0day 级别的新型攻击描述符，如模拟未知无文件攻击，测试 EDR 泛化检测能力。并可将 APT 攻击各环节联合起来，模拟完整渗透路径。

攻击频率建议对高价值资产核心每月进行一次全面的 APT 攻击模拟；对新出现的 0day，应在收到预警后立即进行模拟验证。

难点与关键点：

- 高级绕过技术的模拟：确保 BAS 能模拟 APT 攻击中的防御绕过技术，如反沙箱、反虚拟化、Rootkit 等。
- 攻击与防御的对抗升级：每次模拟触发防御升级，下次模拟需适应新策略。

具体目标：

- BAS 成功执行复杂 APT 模拟攻击。
- 生成新型威胁模拟，并成功触发安全产品告警/阻断。

第三步：结果分析与指标解读

企业应深度分析数据并转化为可操作的洞察，优化防御体系。重点关注：

- APT 攻击模拟告警/阻断率代表对 APT 组织攻击的防御成功率，反映企业对国家级高级持续性威胁的防御水平，发现薄弱阶段。
- 新型威胁防御度评估企业防御体系应对未知威胁的能力，
- ATT&CK 检测覆盖率反映对各种攻击 TTP 的识别能力，确保覆盖关键行为特征，通过 BAS 验证可将覆盖率提升至 90%以上。
- 重点关注日志中是否明确识别出模拟 APT 攻击的 TTP、是否有隐蔽通信、沙箱绕过行为，以及安全产品是否对模拟 0day 攻击产生响应。

难点与关键点：

- 结果的深度解读：APT 攻击模拟结果复杂，需高级持续性威胁分析经验的专人深度解读，找出精细防御逻辑缺陷。
- AI 辅助分析：利用 BAS 的 AI 能力辅助日志分析和攻击路径推理，减轻人工负担。

具体目标：

- 相比上次评估，提升核心 APT 攻击场景的检测率。
- 安全产品成功响应 BAS 模拟的关键 0day 攻击。

第四步：闭环优化与持续改进

（同场景一的第四部分）

难点与关键点：

- 修复的复杂度：应对高级持续性威胁的修复涉及多层次、多维度的系统性改造。
- 对抗持续性：APT 攻击者不断进化，防御需持续迭代。

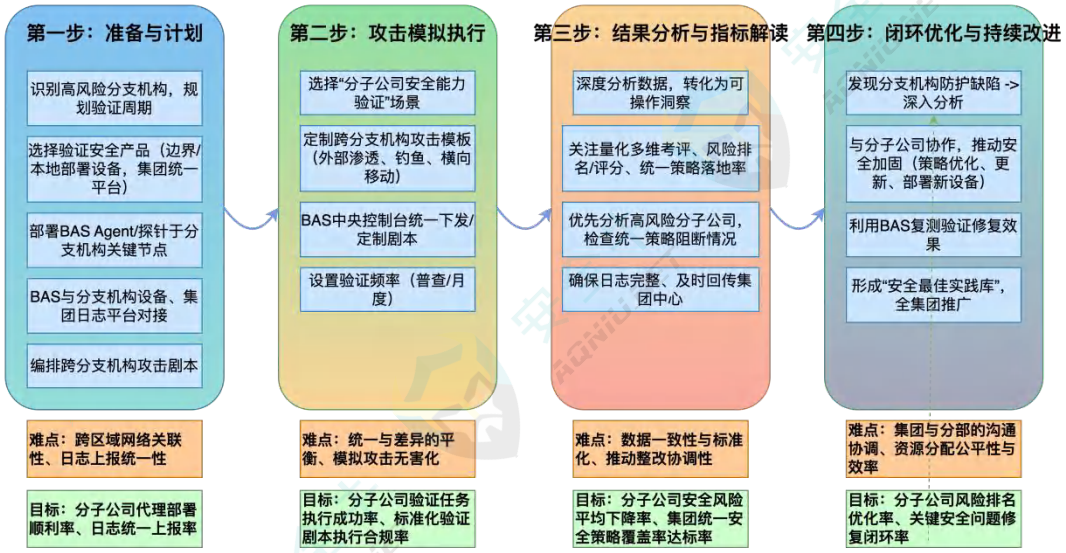
具体目标：

- BAS 发现的 APT 威胁防御缺陷在规定修复。
- 将高价值威胁情报转化为 BAS 模拟用例。

8.8 专项场景八：分子公司安全防护能力验证场景

大型集团企业及其众多分子公司、上下级单位的安全能力往往参差不齐。地域分散导致管理难度大，各分子公司安全投入与人员能力不一，使得集团总部难以进行统一、高效的安全管理和风险评估，集团安全政策难以落地。一旦某个分支机构被攻破，就可能影响整个集团，形成木桶效应。

本场景的目标是对分散机构的安全能力进行统一、量化。通过集中式管理、标准化验证、跨区域模拟攻击、量化考评排名与高效闭环整改，确保集团安全政策有效落地，并促进各分子公司安全能力的协调提升，构建大规模的集团整体安全防线。



场景八：分子公司安全防护能力验证场景

第一步：准备与计划

企业应识别集团内各分子公司的安全管理成熟度差异以及高风险分支机构，例如业务独立性强、对外暴露面多或历史安全事件频发的分公司。规划验证周期，如按季度或半年对所有分支机构进行普查，对高风险分支机构则进行月度验证。其次，需选择应验证的安全产品，范围涵盖各分支机构的边界防火墙、本地部署的 IDS/IPS、EDR 以及任何本地部署的安全产品和策略，同时关注集团统一管控的安全平台在分支机构的落地情况。再者，在各分子公司的网络关键节点部署 BAS 的 Agent/探针，并确保 Agent 与集团中央 BAS 管理平台之间的网络连通性，能够实现跨区域的模拟攻击。同时，确保 BAS 系统能够与各分支机构本地的安全产品以及集团统一的日志平台进行对接，筛选出与分支机构边界防护、内网横向移动、合规性配置相关的告警、阻断、审计日志，并统一上报至集团中心。最后，依据集团统一的安全政策和各分支机构的实际业务特点，选择或编排能够模拟多分支机构场景下的攻击剧本，例如模拟从分支机构的开放服务尝试进入集团内网，或模拟对分支机构内部资产的合规性配置检查。

难点与关键点：

- 跨区域网络关联性：确保集团 BAS 平台能够稳定、安全地连接到各分子公司的代理。
- 日志上报的统一性：确保各分支机构安全产品产生的日志能够以统一格式上报到集团平台，并利用 BAS 平台进行有效解析。

具体目标：

- 分子公司代理成功上线并运行。

- 各分子公司安全产品日志成功上报至集团中心日志平台。

第二步：模拟攻击的设计编排和执行

企业应设计编排多分支机构环境的攻击，如从外部尝试渗透分支机构边界、模拟针对分支机构员工终端的钓鱼攻击，以及模拟从分支机构内部网络尝试访问集团核心资源的横向渗透。集团安全团队通过 BAS 中央控制台，统一下发标准化攻击剧本到各分子公司，确保验证范围和方法的一致性，也可根据各分支机构的业务特点和 IT 环境差异进行定制化编排。

攻击频率建议集团总部设定每月或每季度对所有分子公司进行一次全面的安全能力普查验证，对高风险分支机构，可增加验证频率至每周一次。

难点与关键点：

- 统一与差异的平衡：集团层面需统一验证标准，同时考虑各分子公司的实际业务和技术差异，进行灵活调整。
- 模拟攻击的无害化：确保在各分支机构生产环境中进行模拟时，不对本地业务造成任何影响。

具体目标：

- 分子公司成功执行 BAS 系统模拟攻击任务。
- 统一执行集团下发的标准化攻击剧本。

第三步：结果分析与指标解读

企业应深度分析数据并转化为可操作的洞察，以指导集团层面的安全治理。重点关注：

各分支机构的量化多维考评分数能帮助集团基于量化数据统计实现对各分支机构的考核，指导对区域管理人员的考核、安全预算的合理分配以及安全建设规划。集团可设定统一的安全及格线，并对比各分支机构的攻击阻断率、安全漏洞数量、告警响应时间等，形成直观的对比排名。

分子公司安全风险排名直观展现各分支机构的安全短板和优秀实践，便于集团进行资源倾斜和经验推广。

统一策略落地率代表集团安全策略在各分子公司的执行效果，目标应力争达到 100%落地。企业应重点关注风险排名靠前的分子公司，优先深入分析这些分支机构的详细报告，找出具体问题；检查是否存在多个分子公司反复出现的、未能阻断集团统一策略的攻击；以及确保各分子公司（特别是偏远分支）的日志能够完整、及时地回传至集团中心。

难点与关键点：

- 数据一致性与标准化：确保各分子公司上报的日志和验证结果数据标准统一，以便在集团层面进行聚合分析。
- 推动整改协调性：集团总部需与各分子公司建立高效的沟通协调机制，共同推进安全问题整改。

具体目标：

- 季度/年度分子公司安全风险平均下降。
- 集团统一安全策略覆盖各分子公司。

第四步：闭环优化与持续改进

（同场景一的第四部分）

难点与关键点：

- 集团与总部的沟通协调：确保集团总部与各分子公司在安全管理上的目标一致，并建立沟通协调机制。
- 资源分配的公平性与效率：集团根据 BAS 的量化评估结果，合理分配安全配置和资源，优先投入风险最高的公司。

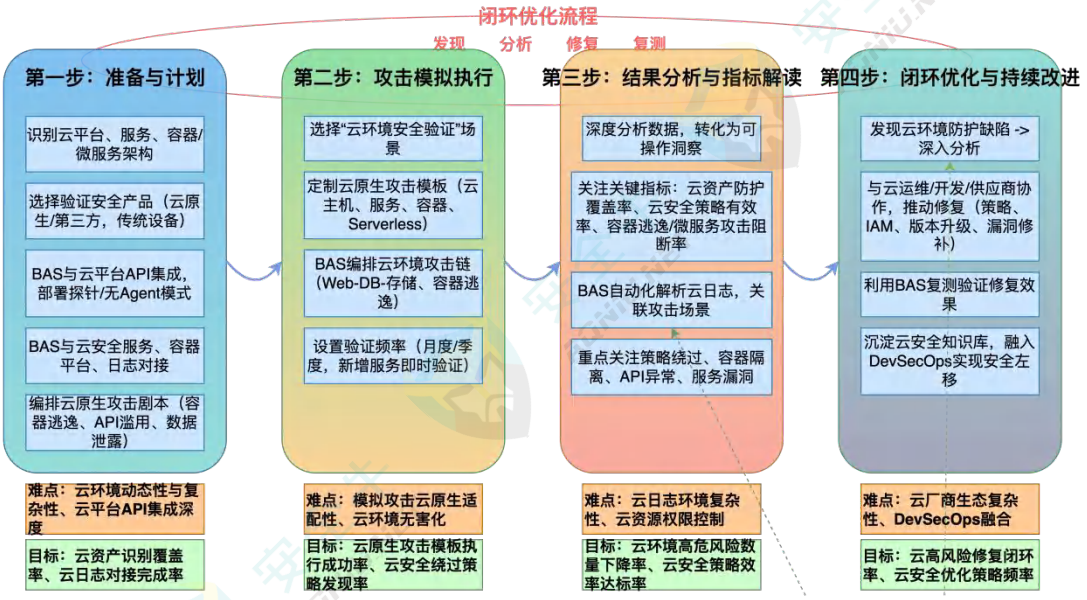
具体目标：

- 年度安全风险排名靠后的分子公司排名提升。
- 分子公司高危安全问题，在规定期限内修复并验证通过。

8.9 专项场景九：云环境安全防护能力验证场景

随着业务上云和数字化转型，企业面临混合云、多云、容器化、微服务等复杂网络架构带来的新型安全挑战。云环境的动态性、弹性以及云原生技术的复杂性增加了安全防护和验证的难度。传统安全工具难以深入验证云环境的防护效果，云上安全配置错误或 API 暴露风险高，一旦出现问题，影响范围广。

该场景的目标是利用 BAS 实现对云环境和复杂异构网络的安全风险量化评估，确保云原生安全防护的有效性。核心能力是通过深入集成云平台 API、自动化部署演示、模拟云环境的攻击，实现混合云、多云通过持续验证和攻击模拟－分析发现－修复－复测的闭环，确保云原生安全防护的有效性，降低云上安全配置错误与 API 暴露的风险，保障业务上云的安全张力。



场景九：云环境安全防护能力验证场景

第一步：准备与计划

企业应识别企业正在使用的云平台类型（公有云、私有云、混合云）、云服务（IaaS、PaaS、SaaS）、容器化应用数量和微服务架构的复杂性。规划验证频率，如对云上关键业务应用进行月度或季度验证。其次，需选择应验证的安全产品，包括云厂商提供的原生安全服务（如云防火墙、云 WAF、云安全组、IAM 策略）、第三方云安全产品（如云 WAF、容器安全平台），以及云上部署的传统安全产品。再者，利用 BAS 与主流云平台 API 集成，自动发现云上资产并部署探针（如在云主机或容器内部署 Agent），或按厂商文档配置无 Agent 模式，确保 BAS 能够模拟云原生攻击，并连接到云环境中的关键网络区域。同时，确保 BAS 系统能够与云厂商提供的安全日志服务、云安全平台、容器安全平台，以及云上部署的传统安全产品进行对接，筛选出云安全组日志、云防火墙日志、云 WAF 日志、云原生安全告警、容器运行时日志、云平台操作审计日志等。最后，依据云环境特性和面临的威胁，选择或编排能够模拟云上攻击的剧本，例如模拟容器逃逸、云 API 滥用、对象存储桶配置错误导致的数据泄露等。

难点与关键点：

- 云环境的动态性与复杂性：云环境变化快，资产弹性伸缩，给 Agent 部署和攻击模拟带来挑战。
- 云平台 API 集成深度：确保 BAS 能集成云平台 API，进行资产发现和配置验证。

具体目标：

- 成功识别云上资产。

- BAS 成功对接云平台和云安全产品日志。

第二步：模拟攻击的设计编排和执行

企业应设计编排适合云环境的攻击，涵盖模拟针对云主机、云服务（如对象存储、数据库服务）、容器、Serverless 功能等各种云原生组件的攻击。并将攻击链延伸到云环境，例如模拟从云上 Web 服务到云数据库的攻击，再到云存储的数据窃取；或模拟从一个被攻破的容器逃逸到宿主机，测试容器隔离是否有效。

攻击频率建议每月或每季度进行一次全面的云环境安全验证，对于新增的云服务或重大云环境配置变更，应立即进行专项验证。

难点与关键点：

- 模拟攻击的云原生适配性：确保模拟攻击适用于云原生环境，理解其特性。
- 云环境无害化：确保模拟攻击对云资源和业务无害化，避免意外的云费用或业务中断。

具体目标：

- BAS 成功执行云原生模拟攻击。
- BAS 成功发现云安全策略（如安全组、VPC）的绕过漏洞。

第三步：结果分析与指标解读

企业应深度分析数据并转化为可操作的洞察，以指导云安全策略的优化。重点关注：

- 云资产防护覆盖率评估云上关键资产被防护的比例，核心云资产防护覆盖率应力争达到 100%。
- 云安全策略有效率验证云安全组、VPC 等配置的有效性，目标应力争达到 90%以上。
- 容器逃逸/微服务攻击阻断率评估企业对新兴云原生威胁的防御韧性，针对高危容器逃逸场景，阻断率应力争达到 90%以上。
- 关注云安全策略绕过、容器隔离是否有效、云服务 API 调用是否异常、云服务漏洞等日志中反映的问题。

难点与关键点：

- 云日志环境的复杂性：云平台日志种类繁多，格式各异，对 BAS 的日志解析能力要求高。
- 云资源权限控制：BAS 在云上的操作权限需严格控制，遵循最小权限原则。

具体目标：

- 季度/年度云环境高危风险数量下降。
- 云安全策略效率达到预设标准。

第四步：闭环优化与持续改进

（同场景一的第四部分）

难点与关键点：

- 云厂商生态的复杂性：修复可能涉及与云厂商的紧密协作，或调整云厂商原有的服务配置。
- DevSecOps 的融合：将云安全验证融入 DevSecOps 流程，实现安全左移。

具体目标：

- 在规定期限内修复 BAS 发现的云环境高危风险，并验证通过。
- 进行月/季度的云安全策略优化。

8.10 专项场景十：数据安全防护能力验证场景

随着国内法律法规和监管要求日益严格，数据泄露、勒索攻击事件频发，给企业造成巨大的经济和系统损失。然而，企业缺乏对敏感数据的全面识别、分类和流转监控，尤其是数据防泄漏（DLP）可能存在策略配置不当，导致企业无法明确敏感数据传输和存储过程中的安全防护是否有效，无法保证数据安全防护的效果。

该场景的目标是利用 BAS 实战化模拟数据攻击，验证企业对敏感数据的发现、分类、保护、监控和响应能力，确保满足合规要求和核心数据资产的安全。核心能力在于利用 BAS 的实战模拟能力，全面验证企业对敏感数据的发现、分类、保护、监控和响应能力，通过无害化模拟数据攻击、量化防护效果并驱动持续闭环优化，确保关键数据资产全生命周期的安全。

第一步：准备与计划

企业应法律法规要求和监管要求，规划验证频率，如每季度对核心敏感数据进行一次全面的安全防护评估。其次，需选择应验证的安全产品，包括数据防泄漏（DLP）系统、数据库审计系统、数据加密、数据备份与恢复系统、访问控制系统、终端数据保护产品，API、代码开发安全以及堡垒机。在存储或处理敏感数据的服务器、数据库服务器、文件、终端等关键节点部署 BAS 的 Agent，确保 Agent 能够模拟数据窃取、篡改、勒索等行为。同时，确保 BAS 系统能够与 DLP、数据库审计系统、员工服务器、安全网

关、SIEM/SOC 等进行对接，筛选出 DLP 日志、数据库审计日志、文件访问日志、异常行为日志、网络流量日志（特别是外发流量）。最后，需要识别企业内部最敏感的数据类型、存储位置和流转路径，选择或编排能够模拟数据窃取、篡改、勒索的攻击剧本，例如模拟攻击者利用 SQL 注入窃取数据库敏感信息，或模拟勒索病毒加密文件。

难点与关键点：

- 敏感数据识别的准确性：确保 BAS 能够准确识别并定位企业内部的敏感数据。
- 数据流转的复杂度：敏感数据可能涉及多系统、多网络流转，攻击路径复杂。

具体目标：

- 识别企业敏感数据资产。
- 对接 DLP、数据库审计等数据安全产品并获取完整日志。

第二步：模拟攻击的设计编排和执行

企业应设计编排数据安全防护的攻击，实现数据窃取、数据篡改、数据勒索等场景。企业可以利用 BAS 的编排功能，模拟攻击者发现敏感数据、尝试访问、复制、删除或加密敏感数据的完整行为路径。

攻击频率建议每月或每季度进行一次数据安全防护评估。对于涉及重大敏感数据处理的系统立即上线或策略变更，应进行专项验证。

难点与关键点：

- 无害化操作：模拟数据窃取时，只模拟传输行为，不真实窃取数据。模拟勒索加密时，只在受控环境中进行，并确保能完全回滚。
- 与业务流程结合：数据安全验证应与企业实际数据流转过程相结合。

具体目标：

- 成功执行数据安全攻击。
- 未造成任何业务影响。

第三步：结果分析与指标解读

企业应深度分析数据并转化为可操作的洞察，以指导数据安全策略的优化。重点关注：

- 敏感数据泄露风险评估模拟数据外泄的成功率，应尽可能为 0%。

- 数据勒索恢复就绪度评估企业应对勒索攻击和数据恢复的准备程度，验证备份系统、应急响应流程是否有效。
- 数据访问控制有效性评估授权访问敏感数据的成功率，发现特许账户收费、权限过高等风险。
- 关注 DLP 是否准确响应、数据库审计中是否存在异常查询、敏感文件是否被异常访问、是否有异常数据外发流量。

难点与关键点：

- 敏感数据识别的准确性：确保 DLP 策略能够准确识别企业所有敏感数据，避免误报和漏报。
- 业务流程与数据流：将数据安全验证与企业实际业务流程和数据流转相结合，确保覆盖关键场景。

具体目标：

- 降低敏感数据泄露风险。
- 满足数据安全合规要求。

第四步：闭环优化与持续改进

（同场景一的第四部分）

难点与关键点：

- 数据安全法规的理解与落地：将法律法规要求准确转化为可验证的技术措施。
- 业务与数据的关联性：确保数据安全防护能够与业务流程和数据流转紧密结合。

具体目标：

- 控制敏感数据泄露事件发生数量。
- 通过每年数据安全合规审计。

通过对 BAS 的十个常用 BAS 场景的落地实战，可以帮助企业构建从点到面、由内而外、从技术到管理的全面安全能力评估体系。通过 BAS 的持续验证、闭环优化，帮助企业的安全从黑盒子，迈向可视化价值，实现主动性、实战化、数据驱动的安全治理，从而有效应对不断演进的复杂威胁。

第九章 BAS 优秀案例研究

（按厂商简称首字母排序）

9.1 优秀案例一 电力行业安全有效性验证案例（塞讯科技提供）

用户背景

该电力集团是国内领先的大型能源类上市企业，拥有千亿级资产和数百亿市值，主营业务覆盖电力生产、输配与销售，业务范围广泛，涵盖多个省份，旗下设有数十家分/子公司，员工逾万人。企业 IT 环境复杂，涵盖办公内网、工业控制系统（ICS）、数据中心（IDC）以及云平台，已经历二十余年的信息化与数字化建设。

在网络安全方面，该集团早期即启动了纵深防御体系建设，陆续部署了防火墙、WAF、入侵检测系统（IDS/IPS）、终端安全、安全运营中心平台等多种安全产品。近年还积极响应监管要求，参与公安部等单位组织的攻防演练，具备较为完善的网络安全制度与技术体系。

然而，随着业务复杂度和攻击技术的同步提升，如何验证已建设防御体系的真实有效性，成为集团亟须解决的关键问题。

用户痛点和需求

作为关键基础设施行业，为了确保电力系统的安全与稳定运行，电力集团重视并持续投入安全防御体系建设，形成了日益复杂的安全防御体系架构，也增加了安全运营的难度。集团对于安全防御体系真实的效果缺乏全面、量化的认知，存在多种安全运营困境：

- 尚无充分验证现有安全防御的有效性的手段

主要表现为对 APT 攻击检测滞后且时间长；缺少对不断出现的 0Day 漏洞的缓解措施的效果验证；所采用的渗透测试、攻防演练等手段不具备长期验证能力，且只针对点而不是面，易受人员因素影响，单位成本也很高。

- 事中和事后的关联分析困难
- 当安全工具没能直接发现或阻断攻击时，安全运营中心平台需要基于各维度上下文的行为关联分析来判断；而攻击未发生时，安全运营中心平台难以创建相关攻击关联分析 Use Case；已创建的 Use Case 则需要攻击模拟来进行准确性的验证。
- 缺乏基于攻击者视角的攻击验证

- 当前安全建设仅基于防守角度，自有安全团队缺少基于攻杀链以及 ATT&CK 框架分析和溯源攻击行为的能力。

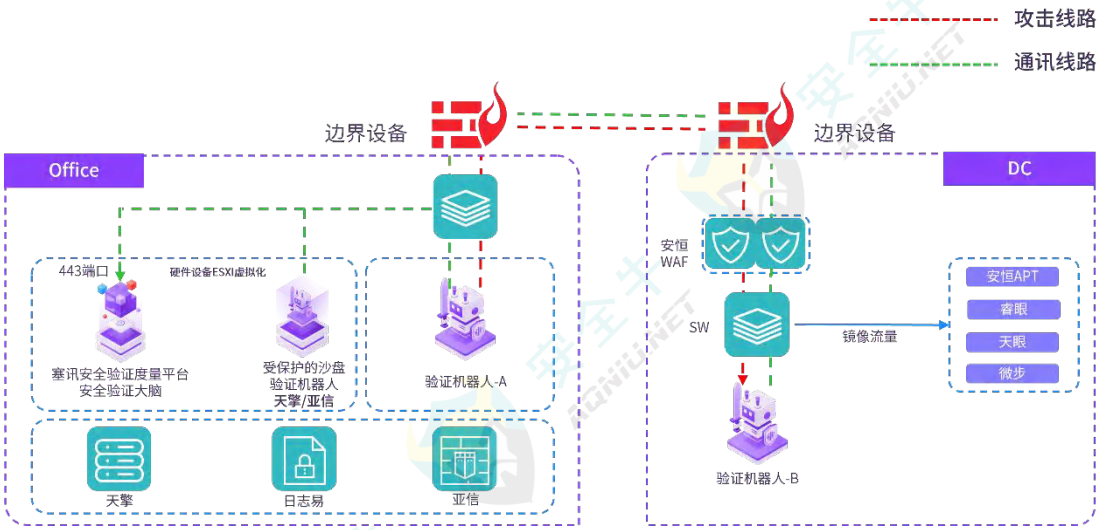
此外，安全团队在被攻击之后所进行的整改，效果也并没有得到明确验证。经过分析与沟通，塞讯验证建议集团从三个方面进行验证：

1. 验证现有安全防御体系有效性的情况：包括安全防御体系的多个控制手段防御有效性验证和安全运营中心平台的威胁检测与狩猎有效性的验证。
2. 验证对于威胁组织的监测与防御能力的有效性：通过模拟多种常见威胁组织的各种攻击手法和技战术来验证当前安全防御体系对其的监测与防御的有效性。
3. 验证安全运营能力：对安全运营中心平台的关联分析场景进行确认或增补，并验证响应流程。

解决方案

对于以上三方面安全防御能力的验证，具体落实为几大场景的模拟攻击验证：

- 基于 ATT&CK 框架的几种战术场景
- TOP3 勒索软件场景
- 常见威胁组织场景
- 隐蔽隧道泄露数据场景
- 历年重大漏洞和热点安全事件场景
- WAF 等其他安全产品场景

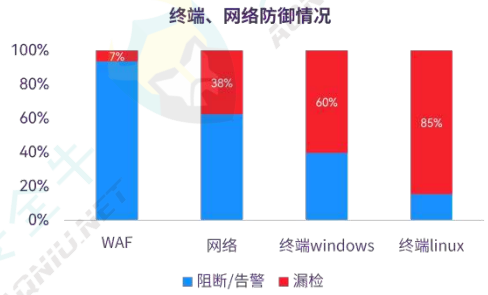


塞讯科技解决方案

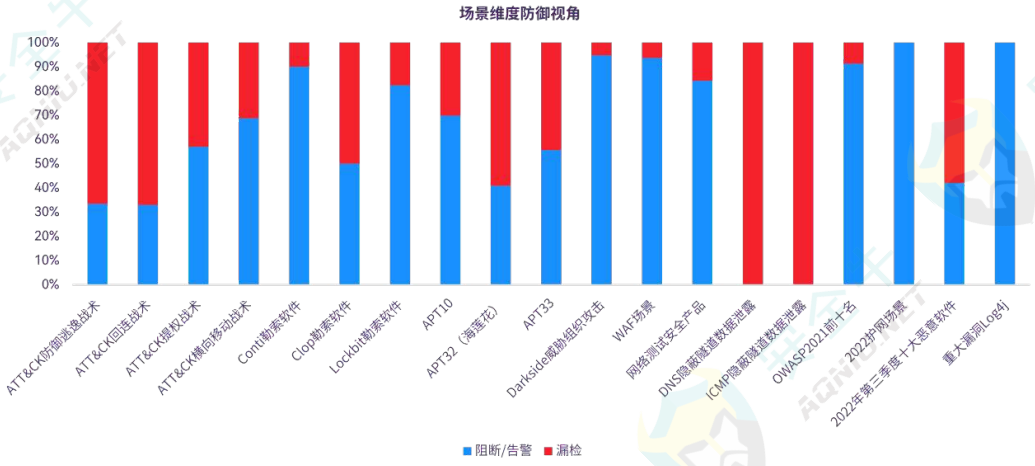
建设效果和客户价值

首次验证共进行了 987 个攻击手法的模拟验证，其中 559 个攻击手法成功被阻断或告警，其余 428 个攻击手段则被漏检，漏检率高达 43%。

验证结果从各个维度展示了集团的安全防御情况，可以看到终端 windows 和 linux 的漏检率分别高达 60%和 85%。从场景维度来看，通过隐蔽隧道数据泄露的漏检率则达到了 100%。



验证结果 1



验证结果 2

根据塞讯验证的分析结果，发现集团安全防御和运营主要存在以下问题：

- 安全产品某些配置不正确
- 日志中包含的告警时间不准确
- 安全产品漏报或误报，告警不上报
- 日志类别不明确
- 现有威胁情报未与安全产品对接
- 缺少对隐蔽隧道方式进行数据防泄漏的检测技术

- 缺少安全运营中心平台的关联分析来弥补单点安全产品不认为有问题的行为的检测

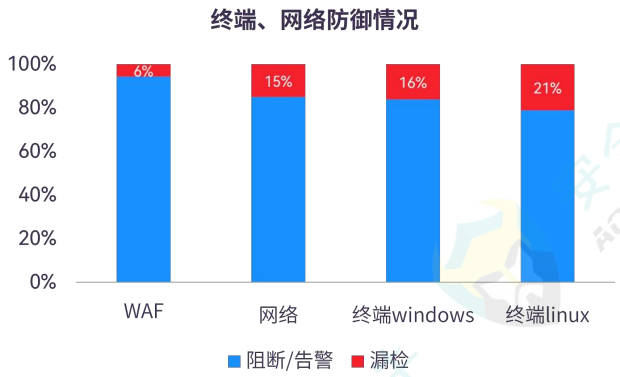
提供解决方案和缓解建议

在首次验证后，塞讯验证分析验证结果数据，该电力集团在 WAF、勒索软件、历年重大漏洞和热点安全事件等方面在首次验证中表现良好；在 ATT&CK 框架和威胁组织等攻击手法的防御上仍有很大提升空间；需要着重关注隐蔽隧道数据泄露场景以避免信息泄露风险。

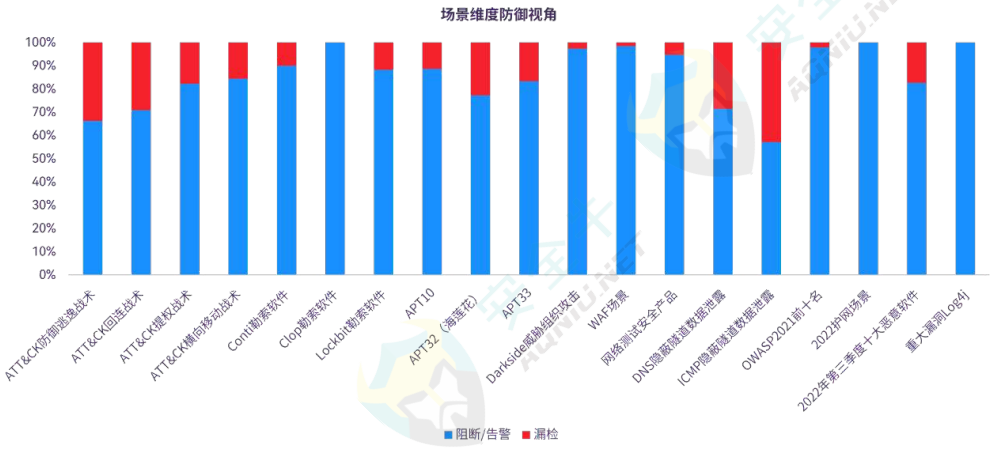
塞讯验证为集团提出的优化整改建议包括以下几点：

- 增加威胁检测与防御手段部署在办公区与 IDC 之间；
- 建议以天/周/月为周期持续验证，确保防御效果；
- 对于已发生的安全事件，在溯源后通过自定义功能进行验证；
- 通过多次验证训练响应团队的能力和熟练度；
- 对关键业务资产进行系统级审计，同时进行日志分析优化和安全产品策略优化。
- 增加安全运营中心平台上的关联分析 Use Case

该集团历经数月的持续验证和优化（安全产品本地化策略优化+安全运营中心平台的关联分析）之后，各维度的安全防御能力和运营水平已经明显提升。最近一次验证结果显示，其终端 windows 和 linux 漏检率已分别降至 16%和 21%。在数据泄露场景也采取了相应的措施，其数据泄露场景漏检率也降低至 36%。



验证结果 3



验证结果 4

安全牛评价：

电力行业这样的关键基础设施领域，虽然普遍已构建了多层次、复杂的安全防御体系，但往往缺乏对现有防御体系真实有效性的全面、量化认知。包括对高级持续威胁（APT）和零日漏洞（0-Day）的检测滞后，传统渗透测试和攻防演练成本高昂且无法持续验证“面”上的防御能力。另外，在攻击发生时，事中和事后的关联分析困难，难以将孤立的安全告警串联成完整的攻击链条，导致响应效率低下；同时，安全团队普遍缺乏基于攻击者视角的攻击验证能力，无法从攻击杀伤链和 MITREATT&CK 框架出发审视自身弱点，使得投入大量资源进行的安全建设和整改，其效果也无法得到明确验证。这种投入巨大，效果不明的困境，严重制约了电力系统在日益严峻的网络威胁面前的韧性。

塞讯科技提供的解决方案构建了一个持续、量化且具备攻击者视角的安全有效性验证体系，通过模拟基于 ATT&CK 框架的战术场景、勒索软件、常见威胁组织以及隐蔽隧道数据泄露等多种高威胁场景，对客户的防御体系进行多维度、全方位的实战化检验。这种主动、持续的验证模式，能够精准发现安全产品配置不当、日志告警不准确、威胁情报未对接、缺乏关键检测技术（如隐蔽隧道检测）以及 SOC 平台关联分析不足等深层问题。通过提供详细的分析结果和优化建议，并辅以以天/周/月为周期的持续验证，形成了“发现问题-分析根源-优化整改-再验证”的闭环，不仅显著提升了客户的防御能力，还通过多次验证训练和提升了响应团队的实战能力和熟练度，实现了从被动防御向主动验证与持续优化的先进转变。

塞讯科技的解决方案方案以持续自动化攻防验证为核心，推动安全验证常态化、数据化。亮点是仿真攻击场景模拟威胁组织手段，深度覆盖 ATT&CK 框架编排攻击链，并量化分析攻防结果提供解决方案，实现动态攻防验证与自动化风险管理，提升电力集团防御和安全运营能力。该案例为众多关键信息基础设施运营者提供了极具价值的示范作用，尤其对于金融、电信、能源等网络安全要求极高的行业而言，具有广泛的借鉴意义。

9.2 优秀案例二 某大型金融机构有效性验证案例（矢安科技提供）

案例背景

某大型金融机构是国内领先的金融机构，业务覆盖零售、对公、跨境金融等领域。构建了网络安全纵深防护体系，部署了下一代防火墙（NGFW）实现网络边界隔离与攻击面控制，集成 WAF 与 IPS 实时拦截应用层威胁并采用动态防御技术提升防护强度；通过内网分区、VLAN 隔离结合零信任架构和强制多因素认证（MFA）实施最小权限访问控制，并构建覆盖主机入侵检测、防病毒及行为监控的终端安全体系以阻断横向渗透；依托安全运营中心（SOC）平台整合全流量分析、威胁情报与 APT 防御系统，实现自动化攻击溯源阻断。

随着数字化转型加速，该机构业务规模扩大，暴露面激增。同时，高级持续性威胁（APT）和潜在的勒索攻击频发，安全运营面临了一系列新的挑战。

安全管理的需求

作为大型金融机构又属于关基单位，当面对复杂的网络环境以及安全态势时，机构考虑需要严格审视自身的安全能力，以实战化角度出发去衡量当前各项安全运营指标。这意味着客户从网络安全管控由面向合规为主的安全，转变为面向真实网络安全攻防的综合安全保障。

如何以 ATT&CK 以及能力成熟度（CMM）等标准模型为基础，结合红军发展建设对防守方的具体要求，抽象出与攻防演练密切相关的能力维度，梳理形成适用落地、易执行的网络安全综合防御能力评估标准，成为核心诉求。

解决方案

面对客户的诉求，矢安科技经过沟通与深入分析，为客户提供了以下解决方案：

基于 MITRE ATT&CK 框架，将攻击行为拆解为初始访问（钓鱼邮件、漏洞利用）、横向移动（利用域内信任关系提权）、命令与控制（C2 通信隐蔽化）、目标达成（数据渗出、持久化后门）等战术阶段。结合历史攻防演练与 APT 攻击事件中实际突破的路径，构建更接近真实的高威胁攻击方案。通过记录攻击链各阶段成功率（如钓鱼邮件成功率、漏洞利用成功率、横向移动突破率等），生成攻击路径热力图，定位防御薄弱环节（如终端防护缺失、网络分段失效）。



失安科技解决方案

通过上述方式重点评估以下五项能力：

（1）攻击防御能力：包括入侵防御、应用攻击防御、恶意软件防御、流量防御等能力。

（2）关联分析能力：包括策略中心、情报中心的信息共享及分析能力。

（3）事件检测能力：包括入侵检测、应用攻击检测、恶意软件检测、流量检测等能力。

（4）事件响应能力：包括入侵处理、应用攻击处理、恶意软件处理、流量拦截等能力。

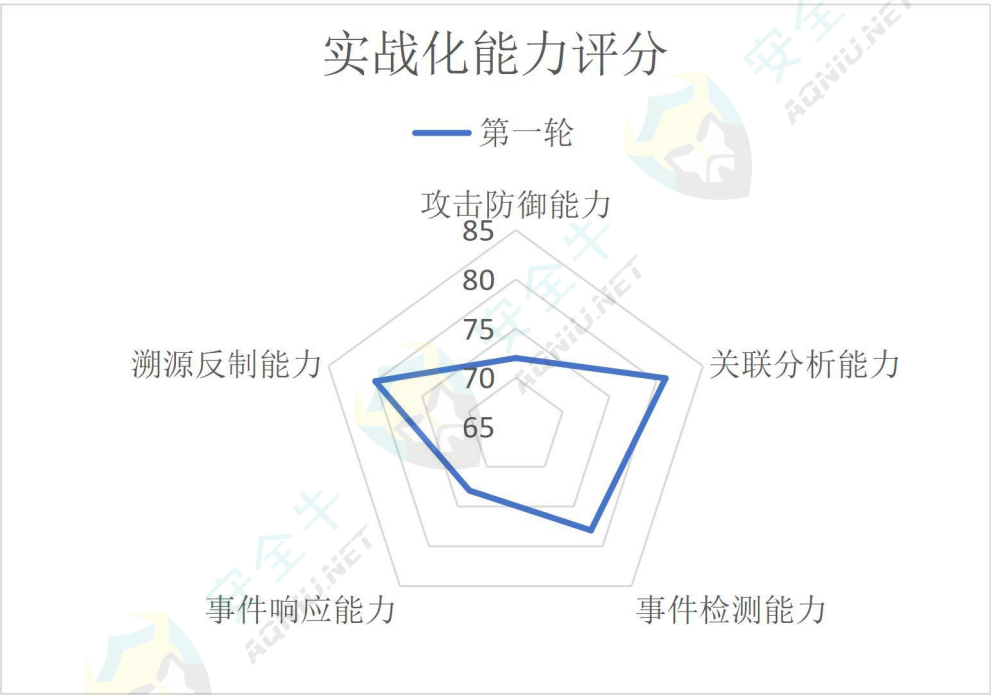
（5）溯源反制能力：包括攻击诱捕、攻击溯源及攻击反制等能力。

并根据失安攻鉴产品内置的评价模型进行分值标注，科学、客观、公正的反应出实战化能力的真是水平。

效果与收益

失安科技为客户梳理并提供了十数条攻击路径，每条攻击路径均基于 MITRE ATT&CK 框架，包含了各个战术阶段。

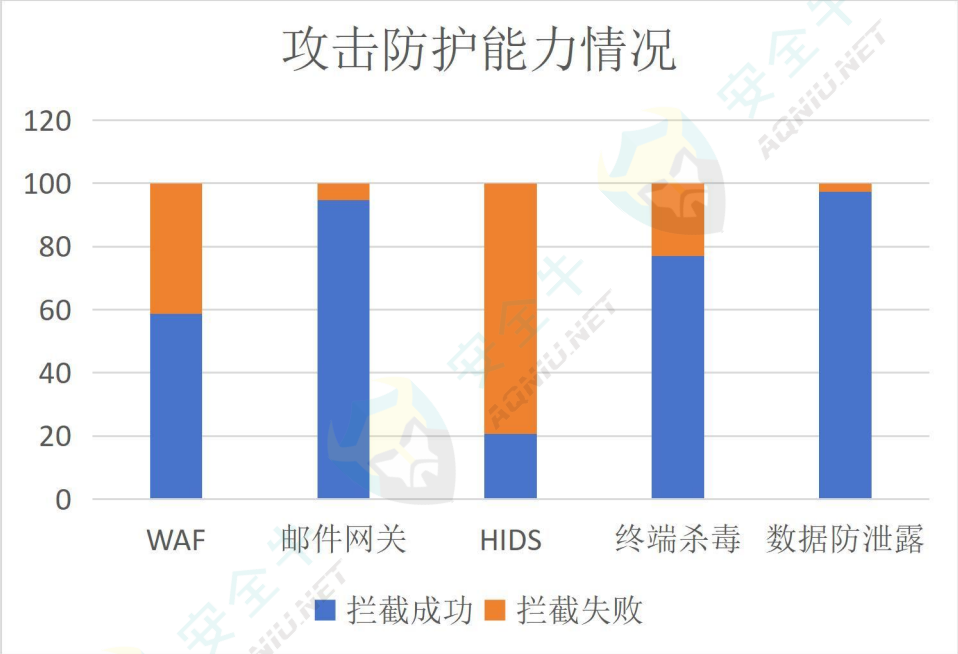
首轮实战化能力综合评分为 76.8 分。



验证结果 1

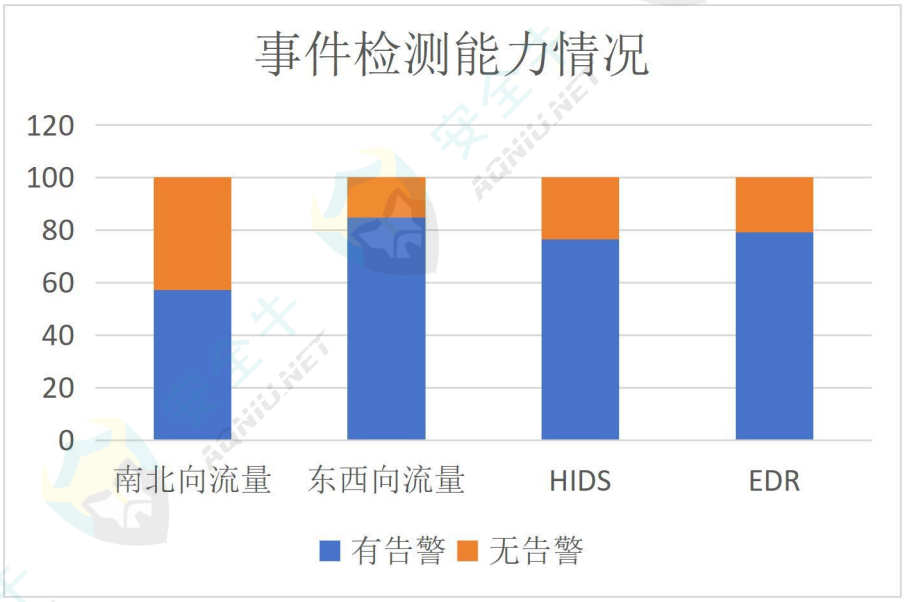
通过首轮检验发现主要的问题有：

- 攻击防御能力整体偏低，尤其在 WAF 和终端防护能力上问题较为突出。下图列出了部分攻击防御能力的验证情况。



验证结果 2

- 事件检测能力不足，主要反应在南北向流量上，事件检测率低于 60%。下图列出了部分事件检测能力的验证情况。



验证结果 3

- 事件响应与关联分析存在不足，难以保障在预定时间内对事件做出响应动作，以及对攻击的上下文关联工作进行分析时，有较大几率出现分析偏差。

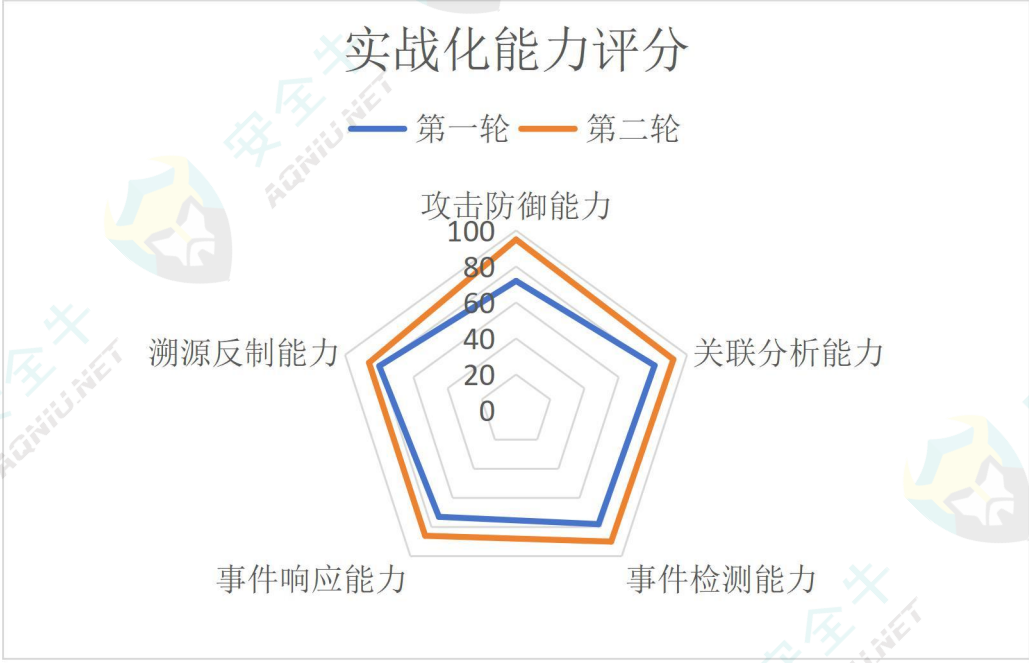
根据结果进行深入分析，矢安科技发现导致这一结果的主要原因是：

- 安全策略配置不正确，过期的策略配置、错误的策略开关、不正确的白名单策略等情况导致了应检未检，应拦未拦的现象出现。
- 告警日志时钟未同步，这严重影响了安全团队对事件的响应时效，以及做关联分析时无法准确对应；同时部分时钟不同步也影响到了告警检测率，使得应有的检测率偏低。
- 安全产品自身能力缺陷，某些安全产品在能力设计时，便无法应对一些攻击情况，如攻击者采用动态编码、加密、隐蔽通道等措施绕过安全产品的检测。

为杜绝同类问题的再次发生，矢安科技又为客户提出相关安全建议：

- 针对各个安全设备以天为单位采取常态化的验证措施，验证安全策略基线的防护有效性
- 基于时钟同步，并整合安全运营平台进行日志关联分析，将验证用例的执行时间与平台告警时间进行对比，判断告警是否存在延迟（最大容忍 5 分钟的延迟）
- 对于当前安全产品无法有效防护的攻击手法，增加监控告警策略，对特定的攻击手法持续监控；同时采取联动策略，将无法有效防护的攻击用例联动至下一环节，验证后续攻击行为是否能够防护

客户根据矢安科技分析的原因及建议采取相关整改措施，待整改完成后一个月开启第二轮验证。与第一轮验证相比，第二轮各项能力均有大幅提升。



验证结果 4

经过后续与客户的沟通了解发现，在整改的过程中，客户仅针对了安全产品相关的事项做整改，并没有涉及安全人员能力的培训。但从验证结果来看，事件响应能力和溯源反制能力均有提升。这一现象说明，想让安全运营人员正确的、高效的处理攻击事件，保障安全设备/产品能正确发挥其应用的作用是至关重要的。

安全牛评价：

当前金融机构等关键信息基础设施单位在数字化转型加速的背景下，正面临着严峻的网络安全挑战。尽管这些机构普遍构建了纵深防御体系，并部署了下一代防火墙、WAF、IPS、终端安全、安全运营中心（SOC）等多种安全产品，但传统上以合规为主导的安全建设模式，难以有效应对日益复杂且实战化的高级持续威胁（APT）和勒索攻击。机构普遍存在难以准确评估现有安全投入的实际效果，不清楚在真实攻击场景下自身防御体系的脆弱点何在。这种“盲人摸象”式的安全运营，导致安全策略配置不正确、或部

分安全产品自身能力存在缺陷等问题，严重制约了安全运营的效率和威胁响应的及时性与准确性，使企业难以将安全能力从被动合规真正转向主动的实战攻防。

矢安科技的解决方案以 MITRE ATT&CK 框架为核心，展现了显著的优势与创新性。矢安科技的解决方案通过模拟真实历史攻击路径，构建了更贴近实战的高威胁攻击方案，不仅能够量化评估机构在攻击防御、关联分析、事件检测、事件响应和溯源反制等关键能力上的表现，更能通过记录攻击链各阶段的成功率，生成攻击路径热力图，直观且量化地揭示防御体系的薄弱环节（如 WAF 和终端防护能力的不足、南北向流量检测率低下等），并建立了从发现问题、深入分析根源（例如策略配置错误、时钟不同步、产品能力缺陷）到提出具体整改建议（如常态化策略验证、日志关联分析、联动策略）的闭环优化机制。显著提升了企业事件响应和溯源反制能力，提升整体安全效能，也为安全运营团队的发展指明了方向。

矢安科技的解决方案提供了从“面向合规”向“面向实战攻防”转型的清晰路径，帮助准确识别并解决高级威胁面前的防御短板，从而有效提升网络安全韧性。该案例对金融、能源、交通等关键信息基础设施运营者具有深刻的借鉴意义。

第十章厂商推荐（按厂商简称首字母排序）

10.1 厂商选型建议

安全牛从攻击模拟能力、无害化技术、集成能力、部署架构能力、服务与支持和 AI 能力等方面给出了 BAS 产品选择的通用要求，企业在选择时，应从自身安全场景出发，挑选符合场景特点的 BAS 产品。



厂商选型建议

- 攻击模拟能力：需关注其真实性、全面性、更新频率，是否覆盖 ATT&CK 战术技术，是否包含国内特有威胁和攻防演练常见手段（如护网、重保高危高频漏洞和攻击手段），是否支持多样的攻击类型、协议和场景（如恶意软件、APT、勒索、钓鱼邮件、流量攻击、Web 攻击、工控协议等），以及是否支持模拟攻击过程中的混淆/逃逸技术。攻击库的质量直接决定了 BAS 模拟的实战化程度和对新威胁的覆盖能力，另外应支持自定义攻击场景和剧本编排，是对攻击库的有效补充。

- 无害化技术：BAS 的核心是无害化模拟，需关注厂商的专利技术及具体实现，确保在生产环境中运行不会对业务造成任何影响。通常通过沙箱隔离、流量标记、权限降级、模拟目标节点、不对漏洞直接利用、剔除有害代码、模拟器间攻击等方式实现，并可能需要熔断机制来应对意外情况。

- 集成性与闭环能力：能否与现有安全运营平台深度联动，如 SIEM/SOC、SOAR/XDR、EASM/CAASM、漏洞管理、工单系统等。需关注其提供的 API 接口和数据输出能力，以实现从发现问题（攻击模拟验证）到修复问题（生成建议、驱动流程）的自动化闭环。验证结果应能融入整体安全运营体系，支持告警分析、关联分析等。

- 部署架构能力：针对复杂异构网络，BAS 需要具备灵活且强大的部署能力。包括支持多种部署模式（如 SaaS、私有化部署、边界验证、内网验证、终端验证模式），并能够在不同网络区域（如边界 DMZ 区、内网办公区/生产区、子公司网络、不同的逻辑区域如指挥网/政务网/互联网等）部署攻击节点、目标节点（真实或模拟）、模拟器或探针/客户端。需关注其能否通过多节点协同实现对纵深防护体系和跨区域攻击链的完整模拟和验证。此外，部署架构应支持多级架构以满足大型企业需求，具备大规模并发执行能力，支持轻量化和快速部署，并能适应现有的网络拓扑，支持跨操作系统、跨硬件形态的节点部署。同时，需要关注攻击流量是否能按需穿透安全产品进行验证。
- 服务与支持：厂商的攻防背景、安全实验室实力、专家团队经验、本地化服务能力及持续运营支持同样重要。这些软实力能保证 BAS 的攻击能力持续更新、更贴近实战，并在项目实施和后期运营中提供专业的指导和问题解决。
- AI 能力：AI 是提升 BAS 智能化水平的关键。需关注 AI 是否能智能编排攻击场景和剧本、自动生成攻击向量/payload/剧本、自动化日志分析和风险评估、生成精准的修复建议或缓解措施、辅助发现攻击路径、预测潜在威胁以及驱动动态的防护策略调整和优化。这决定了 BAS 的智能化、自动化程度和应对未知/新型威胁的能力。

安全牛从攻击模拟能力、无害化技术、集成能力、部署架构能力、服务与支持和 AI 能力等方面对国内厂商进行识别并推荐。（按厂商简称首字母排序）

10.2 推荐厂商－长亭科技

1）厂商简介

长亭科技成立于 2014 年 7 月，秉持知攻善防，智能安全的理念，从攻击视角构建防御体系，以 AI 驱动重塑安全运营，通过新一代智能安全产品防护体系和专业的安全测试及咨询服务，打造了先进可靠的实战化、体系化、常态化的智能安全运营能力。主要客户涉及金融、通信、政府、能源、互联网等行业。

2）产品简介

长亭御衡（Alioth）安全技术验证平台是长亭秉承以攻量防，敏捷运营的思想，自主研发的一款针对安全运营体系有效性。御衡通过将实战攻防中用到的技术和方法，进行提炼总结，并使用自动化平台在企业内部网络中进行重放，验证安全运营三要素（人员能力、工具/技术有效性、流程）有效性，量化评价防御能力。

3）推荐理由

- 丰富的攻防经验：长亭科技团队具有丰富的攻防演练实战、渗透测试的经验，并将专业知识和自动化工具沉淀为 BAS 产品，实现高仿真攻击，能更精准地发现防御薄弱点。
- 高质量攻击样本：攻击剧本均来自其安全服务团队的真实攻防场景，并在高危漏洞出现后 24 小时内迅速更新验证能力，确保威胁知识库的时效性和高质量。
- 精准量化度量：自研评分引擎通过模糊评价算法等高级机制，提供定性与定量反馈，将验证结果可视化并明确给出加固优先级，帮助企业精准评估和优化安全防御。

10.3 推荐厂商－华云安

1）厂商简介

华云安成立于 2019 年，是国家级专精特新小巨人企业。公司致力于构建人工智能驱动的下一代网络安全防御体系，通过攻击面管理、防御体系验证、自动化防御的技术创新，打造云原生安全能力平台，提供面向未来的智能化防御解决方案。在智能安全领域取得了显著的成绩，技术创新和产品能力获得核心客户认可，广泛应用于监管、电力、能源、金融、教育等行业。

2）产品简介

华云安灵刃·智能渗透与攻击模拟系统（Ai.Bot，简称灵刃）是基于人工智能技术自主研发的企业级安全建设有效性验证系统。其沉淀攻防专家经验，对目标网络持续开展无害化的智能渗透和攻击模拟验证，

确保安全防护策略有效运行；并结合 ATT&CK 安全框架各战术及最新攻击技术，验证边界突破、内网横向移动等多种攻击场景下的安全防护体系的防御、响应能力，协助用户持续优化和补齐安全防护体系，持续推动企业安全防护实战化发展。

3）推荐理由

- AI 驱动的智能攻击与及时威胁情报：华云安融合 AI 技术，可自动生成和调整模拟攻击剧本，并持续更新最新威胁情报，确保模拟攻击高逼真度和及时性。
- 轻量化部署与精细化多设备验证：架构轻便，资源需求低、易于部署和维护，通过热加载避免引入安全隐患。精细化验证边界多设备场景，帮助用户识别防御短板。
- 可量化的防御能力度量与持续优化：提供实战化攻击模拟和高精度闭环验证，结合多维度评估准确量化网络薄弱点。提供风险缓解建议，指导企业持续优化安全防御体系。

10.4 推荐厂商—绿盟科技

1）厂商简介

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于 2000 年，总部位于北京。在国内设有 70 余个分支机构，为用户提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。绿盟远程安全评估系统（RSAS）、风云卫大模型等多款产品多次获得国外权威咨询机构推崇，具有一定的国外知名度，主要客户涉及政府、金融、运营商、能源、交通、科教文卫、企业等各大行业。

2）产品简介

绿盟防御突破模拟与评估系统 BAS，率先将攻击模拟技术应用在网络安全体系建设中，建立起从外到内的安全防御评估能力，覆盖安全设备、安全区域、安全体系、专项威胁等各类场景的防御评估，通过高度自动化、高安全性的攻击模拟，让用户以实际攻防对抗的方式验证、评估、并持续优化企业安全防御有效性，将安全防护由事中提至事前，从被动防守转移到主动防御，实现事前的精准防御评估，在动态威胁态势下持续保障客户全面的安全状态。核心功能主要包括全场景自动化攻击模拟覆盖、全时段自动化检测与持续优化、精准防御能力画像及分析、轻量部署与弹性扩展。

3）推荐理由

- 无害化与零侵入：绿盟科技的无害化攻击模拟技术确保不对真实资产造成任何损害，且零侵入设计简化了部署和验证过程，降低了安全验证的风险。
- 拥有全链路攻击场景模拟能力，能复现完整攻击行为，并支持多路径可视化评估，利用攻击图算法推

导潜在攻击路径及其成功概率。

- 广泛行业覆盖与标准参与，绿盟科技广泛服务于金融、运营商、能源等多个关键行业，并积极参与多项行业标准制定，确保产品紧密贴合最新合规与最佳实践。

10.5 推荐厂商－墨云科技

1）厂商简介

北京墨云科技有限公司成立于 2017 年，是一家网络攻防科技安全服务提供商，公司秉持着让网络攻防更智能的使命，不断创造突破性技术，专注人工智能在攻防安全领域的应用研究，打造智能化产品体系，为客户提供全方位的信息安全服务。目前，墨云科技已在北京、南京、上海、广州、深圳、成都、武汉、济南、西安等多地设有研发中心及分支机构,服务行业客户上百余家。

2）产品简介

墨云科技 VackBAS（深鉴）系统，以 AI 赋能网络安全。通过自动化、持续的攻击模拟，实战化验证安全策略、防护体系与运营流程，覆盖传统评估盲区且无害化。具备攻防场景全覆盖、攻击编排可视化、高自动化、多维可视化等优势，助力企业精准量化网络薄弱点，优化防御体系，提升网络安全效能。

3）推荐理由

- AI 驱动的智能模拟： 墨云科技拥有十余项 AI 技术专利，运用 AI 技术，能智能生成并动态调整攻击路径，高效模拟真实网络威胁，并提供智能威胁预测。
- 实战化的攻击用例： 拥有超 6 万条覆盖多维度的实战攻击用例，能完整模拟从渗透到数据窃取的全攻击链条，确保测试的深度与广度。
- 全方位安全验证： 系统可全面覆盖各类攻防场景，对企业的纵深防御体系进行评估，并采用无损测试技术，确保在模拟攻击时不影响实际业务系统的正常运行，为安全决策提供量化依据。

10.6 推荐厂商－塞讯科技

1）厂商简介

塞讯科技与 2021 年成立，专注于打造基于 AI 能力的对抗式安全验证平台。致力于利用真实的 APT 攻击场景、第一手的受害者威胁情报，结合 AI 情报派生技术，赋能组织现有的安全防御体系，实现有效的网络安全提前布防。塞讯科技在北京、上海、深圳、杭州均设有分支机构，服务可覆盖全国各个角落，

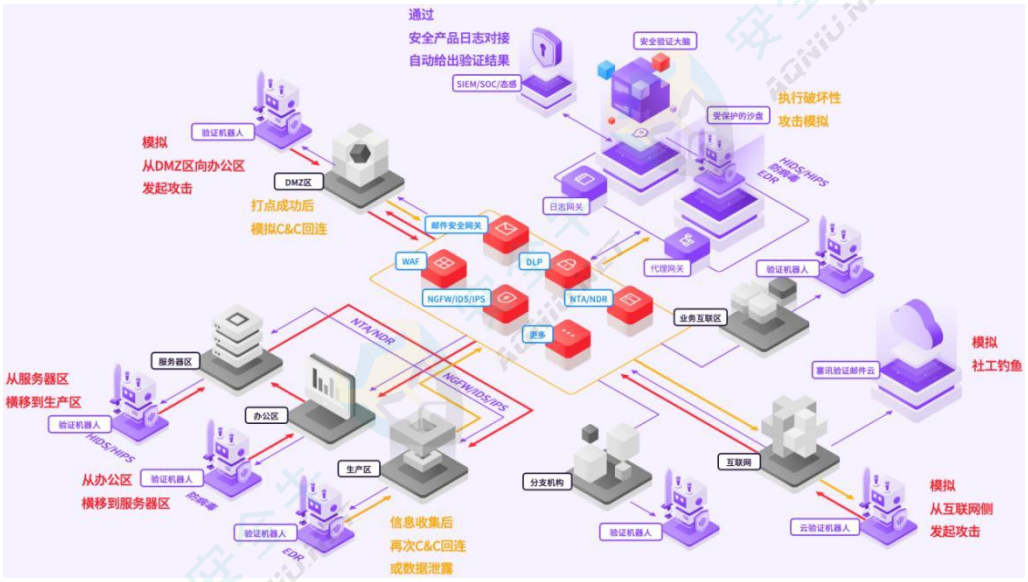
核心团队均来自全球知名网络安全公司和 APT 研究机构，拥有业界突出的安全研究与 APT 组织追踪能力。主要客户涉及电力、央国企、大型企业等行业。

2）产品简介

塞讯安全度量验证平台以攻击者视角出发，针对企业的安全防御体系，通过 AI 助手挑选或编排各类攻击场景，进行对抗式验证，发现防护短板。平台可分析完整攻击过程中所产生的结果、告警、审计等所有相关日志，发现安全防御短板，精准定位安全产品、流程和人员等各方面的弱点。基于实际数据，平台借助 AI 技术提供可落地的缓解、修复或增补建议，帮助客户构建主动防御能力。



安全验证场景



覆盖完整攻杀链

产品主要能力包括：

1.全面的攻击模拟与覆盖：

庞大攻击库：拥有超过 20,000 种攻击手法和 2,000 种攻击场景，覆盖 ATT&CK 框架和完整攻击链（侦察到目标执行）。

多维度验证：覆盖网络、端点/主机、邮件、AD、云、API、应用、数据、DNS、OT、IoT、移动安全等多个维度。

真实攻击模拟：基于真实攻击事件和 APT 组织 TTPs 进行模拟，还原真实威胁。

2.自动化与持续性：

全自动化运行：支持自定义范围、场景、剧本、周期，实现无人值守的持续验证。

持续监测环境变化：定期执行模拟攻击，主动发现因环境变更导致的防御能力下降，并告警。

3.灵活编排与定制：

攻击剧本编排：可灵活编排攻击步骤顺序，模拟已知威胁组织、特定恶意软件家族行为，或还原事件。

多维度筛选：方便地根据关键词、安全维度、ATT&CK、攻杀链查找所需攻击手法。

预定义场景：提供针对不同行业和特定威胁（勒索、挖矿、供应链、漏洞）的预设验证场景。

4.量化与可视化：

可视量化防御体系：通过仪表盘和报告，将安全防御能力、覆盖度、有效性等进行量化展示。

多角色视图：满足从高层、CISO 到运营中心不同人员对安全态势的了解需求。

关键指标衡量：帮助评估安全有效性、安全运营和覆盖度（防御手段、策略）。

5.快速响应新型威胁：

快速更新能力：依托塞讯安全实验室 7x24 威胁追踪，第一时间更新攻击库，使用户能快速验证对新型攻击的防御力。

6.安全保障与集成：

过程安全：通信加密、机器人隔离、沙盘保护，确保验证过程不泄露信息、不损害资产。

广泛集成：支持对接国内外主流安全产品（WAF,NGFW,EDR,SIEM/SOC 等），也可配置对接非原生支持的产品。

优化运营决策：发现并优化单点防御配置、改进响应流程，通过与 SIEM/SOC 联动填补场景空白，提升整体运营能力。

3）推荐理由

- 对黑客行为的深度研究与真实攻击库的极致还原：塞讯科技拥有数十年的 APT 组织追踪研究经验，对真实攻击进行的深刻洞察。并形成基于真实威胁情报构建的攻击库（400+APT 组织、250+勒索家族），确保了模拟攻击的真实性、全面性和性。
- 适应多层次成熟度需求，支持复杂规则与合规性验证：塞讯科技的产品能够根据不同安全成熟度阶段的需求提供相应的验证解决方案，如验证常规设备性能、提升基础运维效率，以及进行高级关联分析和响应效率评估。多设备串联场景可精细化验证，清楚知道每个设备的用例执行情况、防御和拦截结果。
- 上下文关联分析，揭示高级持续性威胁：塞讯科技强调深度关联分析，将正常行为的行为关联分析与攻击上下文进行关联，精准识别单点安全产品难以知晓的认知性攻击行为，帮助安全运营团队从海量中精准捕捉真实威胁，提升威胁狩猎效率。
- 高效安全的无靶机架构与沙盘技术：塞讯科技利用无靶机架构设计，避免了传统靶机模式引入新漏洞的风险，并实现了安全性、轻量化、易维护，并通过风险沙盘技术的应用，确保在运行违法样本或包含违法操作的验证动作时，能够在一个受保护的隔离环境中安全执行，并在完成后快速回滚，彻底消除对环境生产的任何潜在影响。
- AI 助手赋能用户体验，实现智能解释与建议：塞讯科技打造基于 AI 能力构建攻击脚本和配置攻击场景，智能解释攻击结果和防御失效的原因，提供可落地的修复、修复或增补建议，将安全操作的复杂性转化为分析的、高效实施的指导，赋能安全团队决策。
- 全面的 API 化与持续化服务能力，构建闭环安全运营：塞讯科技提供全面的 API 接口，能够与企业现有的资产测绘管理、SOAR、深度感知或 SOC、漏洞扫描管理、攻击面管理等进行深度对接，促进实现验证发现－分析－修复－复测的联动自动化完整闭环。

10.7 推荐厂商－矢安科技

1）厂商简介

上海矢安科技有限公司（以下简称矢安科技，英文名 ASants），成立于 2021 年 4 月，是一家创新型智能安全企业。矢代表攻击，安代表防御，公司提供基于攻防实战化的创新安全产品、服务及解决方案，运用 AI 及创新技术提升安全自动化、智能化程度，有效促进企业安全生产力。矢安科技致力于成为新一代智能安全的领跑者。

矢安科技是 AI 主动安全的倡导者，发布了安全体检智能体，以 AI 之盾应对 AI 之矛，基于技术创新和行业实践，帮助企业全面洞察数字化时代暴露面，从攻击者视角建立安全验证框架、推理最小阻力路径，构建面向数字资产、风险和威胁的“点-线-面”攻击图谱，主动预知风险，驱动安全风险有效治理。矢安科技高度重视安全创新与技术研究，公司拥有创新研究团队及攻防实验室。创新研究团队跟踪国内外安全趋势及前沿安全技术，攻防实验室致力于研究最新攻防对抗技术。在基础安全研究、创新技术探索、攻防实战化、行业最佳实践等各个层面，技术团队的深厚底蕴及不断积累为公司提升核心竞争力及持续创新发展注入活力。主要客户涉及金融、运营商、能源、政府及国资等。

2）产品简介



矢安科技产品方案

一、人员意识安全

社会工程学攻击是网络安全的重要威胁，尤其是钓鱼邮件攻击。为此，我们推出了针对性的解决方案。我们的产品具备模拟钓鱼邮件攻击的功能，通过向目标用户发送模拟攻击邮件，评估用户的安全意识水平。评估内容涵盖查看邮件、打开附件、点击链接、提交信息等多个行为维度，进而量化安全意识评分，直观展现安全培训的实际成效。产品内置多样化的钓鱼邮件模板，同时支持用户自定义模板，以适应不同场景需求。我们从攻击视角出发，整合多方资源，助力企业主动收集对外暴露邮箱信息，有效收敛攻击入口，提升主动防御水平，全方位守护企业网络安全防线。

二、网络安全

在国家级攻防演练及常态化安全对抗中，邮件系统因直接面向互联网、用户操作频繁，成为攻击者重点突破目标。攻击者常利用免杀技术或后门程序，绕过邮件安全设施，广泛投递恶意邮件寻找突破口。企业虽部署了邮件安全网关、邮件沙箱等防御设施，但针对邮件入口的防御体系仍需不断优化。我们的产品

通过在内网部署客户端，由指定发件服务器向目标企业邮箱发送包含恶意邮件的测试邮件，客户端拉取目标邮件服务器收件信息，对比评估邮件网关、邮件沙箱等安全产品防御有效性。攻击用例覆盖畸形邮件、恶意链接、恶意附件等类型，囊括勒索病毒、恶意软件、蠕虫、Payload、EXP、挖矿、C2、钓鱼链接等攻击形式，全面评估邮件系统安全防护水平，发现潜在漏洞并采取针对性防御措施，确保邮件系统有效保护机密信息与敏感数据。

网络威胁日益复杂多变，攻击手段防不胜防。我们产品所打造的威胁情报场景，能够模拟恶意程序的网络请求行为，全面覆盖多种协议与场景，精准评估威胁检测能力，让潜藏威胁无处遁形。我们的安全研究团队凭借深厚技术背景与丰富分析经验，持续跟踪全球网络威胁，确保威胁情报及时性与准确性，并将其赋能产品。通过模拟真实攻击行为，验证用户安全产品对威胁情报的响应能力，帮助企业及时发现威胁情报盲区，提升网络安全水平。

在 Web 安全领域，我们的产品提供丰富的攻击向量，全面覆盖各类常见漏洞，同时支持自定义规则编写，灵活应对不同安全需求。在常规攻击载荷基础上，创新支持多种 WAF 绕过方式评估，有效检验防护措施的完整性。通过外部投递方式，无需额外部署，周期性投递攻击向量，精准检测 WAF 策略有效性。重大漏洞发布或活动前，及时验证补丁规则，确保企业 Web 应用安全无忧。

面对复杂多样的流量安全威胁，我们的产品推出流量安全验证体系，精准模拟各类攻击场景，全面检验威胁检测与防御效能。采用两台客户端模拟完整攻击交互，持续评估网络安全产品的防御水平，为企业网络空间安全保驾护航。攻击模拟采用插件化脚本更新，能够即时更新重大漏洞利用脚本，快速验证企业安全防御体系的响应能力，及时发现并弥补情报威胁源的缺漏，有效降低潜在安全风险。

在终端安全方面，我们的产品是一道坚固的防线。通过自动部署与模拟攻击，精准执行各类攻击操作，持续监控主机行为。这一综合验证流程能够全面评估终端安全防御能力，助力企业及时发现并修复安全漏洞，有效抵御 0day 漏洞、内网横向移动等高级持续性威胁，守护企业核心资产。

三、数据安全

数据安全是企业发展的基石，不容有失。我们的产品从攻击者视角出发，精准验证网络 DLP、终端 DLP 等设备及策略的可靠性。利用先进算法规则生成敏感数据，模拟多途径外泄行为，全面覆盖常见数据类型与外泄通道。通过严谨的验证流程，为企业的数据安全提供坚实的保障。

四、云原生安全

云技术的蓬勃发展，使得容器安全成为企业上云过程中的关键考量。我们的产品全面支持对国内主流容器安全厂商的设备进行验证，能够模拟容器逃逸、漏洞利用等真实攻击类型。通过自动部署容器镜像及运行依赖，精准下发模拟攻击向量，持续检测容器镜像行为，结合日志闭环验证结果，全方位评估容器安全产品的检测能力，助力企业及时发现并弥补安全能力缺失，提升整体防护水平。

3）推荐理由

- 源于实战的攻防基因，确保验证的真实性与性：积累丰富的攻防实战经验，致力于研究最新的攻防技术，拥有十余项多项攻击检测方法的专利，并转化 BAS 产品高质量的攻击库和验证能力，确保模拟攻击的真实性和对抗性，有效验证企业实战的防护能力。
- 多维度攻击场景，覆盖新兴领域：矢安科技的 BAS 产品不仅覆盖了 Web 应用、终端、内网等传统核心攻防场景，更将多维度攻击场景的验证范围拓展至新兴领域。未来规划包括云原创、数据安全、物联网和工控安全等场景，对新兴技术带来的安全风险进行提前验证。
- 攻击面管理与实战验证的深度融合：矢安科技可以将攻击面管理与实战验证紧密结合，帮助企业实现从被动资产清点到主动风险消减的转变，使得安全投入能够精准聚焦于最容易被攻击者利用的风险点。
- AI 驱动的智能攻击生成与策略编排：矢安科技积极利用 AI 技术赋能攻击模拟，利用 AI 驱动实现基于历史攻防数据生成攻击实例，模拟更智能，自动决策攻击链并评估防御体系。使企业能够更加便捷地模拟复杂且不断变化的攻击手段，保证验证的深度和广度。
- 产品的开箱即用，实现高效部署与便捷操作：强调安全验证产品的易用性，开箱即用使得企业安全团队能够更有效地进行部署和日常运营，减少人工干预，从而保证 BAS 能够持续、稳定地运行，并快速实现有价值的验证结果。
- 量化评估与风险优先等级划分，驱动精准安全决策：提供多维度的量化防御指标，覆盖人员、技术、流程的综合指标，将抽象的安全效果转化为具体的量化分值和评估报告，帮助企业更清晰地理解安全业务的价值和风险影响，驱动安全风险的有效治理。

10.8 推荐厂商—知其安科技

1）厂商简介

北京知其安科技有限公司成立于 2021 年，是一家致力于技术和产品创新的新一代网络安全企业。知其安是国内较早提出并推广安全验证理念的公司，并自主创新大规模商业化落地的网络安全能力验证平台，已服务超百家金融、央企、运营商、能源、智能制造、互联网等客户。公司目前已通过国家高新技术企业、国家级科技型中小企业、北京市专精特新中小企业认证。

2）产品简介

离朱安全有效性验证平台专注于各行业网络安全防护成效评价领域，尤其针对复杂网络环境下入侵与攻击模拟场景，精准检测安全防护脆弱性，量化评估防护有效性，助力企业筑牢网络安全防线。在国内实

践基于自动化攻击还原模拟的安全防护验证技术体系，主动感知安全防护薄弱点，弥补安全防护系统攻击局限于被动发现技术缺陷；目前已经覆盖 450+类、30000+种具体攻击手段。

3）推荐理由

- 高质量用例并迭代更新：知其安科技拥有多项安全验证专利，积累了丰富的高质量攻击用例，判断准确率达 99%，误报率降低 40%以上。并每周常态化更新，对 0Day 漏洞 24 小时内上线验证用例，确保模拟攻击的广泛性、真实性和时效性。
- 技术创新：动态对抗学习的智能验证体系，通过融合图神经网络（GNN）与深度强化学习（DRL），构建攻击路径推理模型，实现对复杂网络环境中防护体系的全生命周期有效性验证。
- 丰富的项目经验积累：在金融、互联网等关键行业积累了丰富的用户实施经验，在实战化安全运营中的卓越可靠性。
- 集成性能和稳定性较好，可以与企业安全运营体系深度融合，帮助企业实现自动化攻击验证闭环。

10.9 其他特色厂商

安全牛也针对其他国内主流 BAS 厂商开展了调研和访谈，厂商依据自身优势各有侧重。

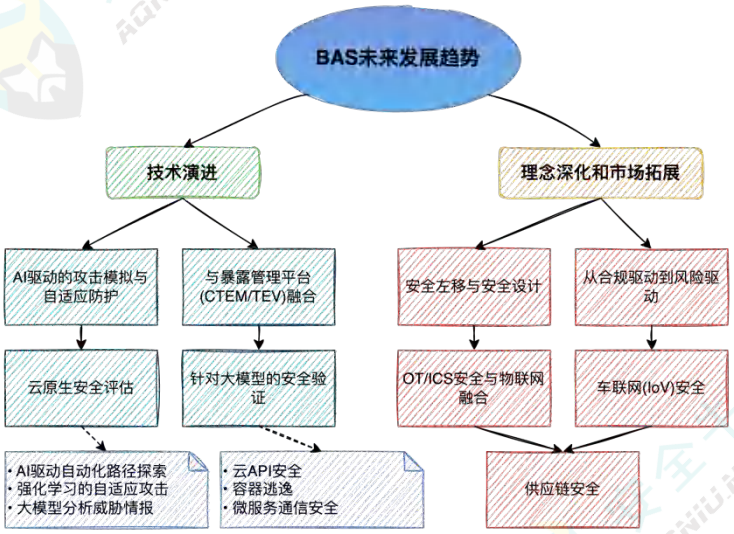
- 灰度安全成立于 2021 年，持续创新，可基于 ATT&CK 模型进行攻击场景编排和可视化呈现，融合漏洞优先级（VPT）和攻击面测绘技术。通过机器学习自动识别并利用漏洞，生成复杂攻击场景，以及生成式 AI 编写攻击向量。拥有全球蜜网进行实时监控并跟踪最新威胁。
- 赛宁网安依托攻防实战经验的经验积累，在攻击库的真实性和多样性上具有一定优势，提供无害化验证过程，支持跨操作系统和硬件形态部署，同时利用 AI 自动生成模拟攻击行为剧本，场景扩展了新兴工业互联网安全场景的布局和精细化模拟能力。

第十一章未来趋势与建议

网络安全领域的技术演进永无止境，入侵与攻击模拟（BAS）作为其中的关键一环，其未来发展同样充满机遇与机遇。本文提出 BAS 研究领域的未来趋势进行展望，以及用户和厂商提出建议，以期共同推动行业发展。

11.1 未来趋势

BAS 的未来发展将紧密结合前沿技术、深化安全理念，并不断拓展其应用边界，以适应日益复杂且动态变化的威胁环境。



BAS 的未来发展趋势

11.1.1 技术演进

1）AI 驱动的攻击模拟与自适应防护：

AI 和机器学习将不再局限于辅助攻击生成，而是更深入地贯穿于 BAS 的各个环节。将涵盖 AI 驱动的自动化路径选择与优化、基于强化学习的自适应攻击决策制定，以及借助大模型对复杂威胁情报进行深入分析和场景智能编排。

前景：未来的 BAS 系统将具备显著的自主性，能够模拟更为复杂、难以预测的攻击行为，甚至有望实现针对未知威胁和 0day 漏洞模拟能力，以此检验防护体系应对未知威胁的稳健性。这将助力企业实现更高级别的主动安全治理，将安全防线提前至人工智能驱动的风险预测与验证环节。同时，AI 的深度赋能将

推动 BAS 从单纯的攻击模拟向智能对抗转变，使防护方能够更积极、更智能地抵御复杂多变的网络安全威胁。

2）与其他管理平台（CTEM/TEV）的融合：

BAS 将加速与攻击面管理（ASM）、漏洞管理（VM）、安全配置管理（SCM）等暴露管理相关工具的深度融合，共同构建统一的持续暴露管理（CTEM）或威胁暴露验证（TEV）平台。

未来 BAS 将为企业呈现攻击面的全方位视图，实现从发现、评估、验证、优先级排序到修复的全流程闭环管理。BAS 作为 CTEM/TEV 平台的核心验证引擎，将为暴露面提供持续且实战化的验证数据，确保所发现的漏洞和风险具有真实可利用性，从而为精准修复提供可靠指导。

3）云原生安全评估的解析：

随着云原生架构（如容器、Kubernetes、Serverless）的广泛普及，BAS 将重点关注模拟和验证云环境中原生的特定攻击面、漏洞，以及云平台自身的安全配置与策略有效性。

未来 BAS 将涉及对云 API 漏洞、容器逃逸、配置错误、微服务间通信安全等云原生威胁的精细化模拟。BAS 将发展出适应云环境动态特性与弹性伸缩的验证机制，以保障云上资产的安全性与合规性。

4）针对大模型的安全验证：

随着大模型在国内各行业的广泛应用，构建完善的大模型安全验证体系已成为当务之急，亟须利用突破性攻击模拟（BAS）技术对大模型安全性进行全方位评估，重点关注模型算法安全、数据隐私保护机制、对抗样本防御能力等核心安全维度。

未来 BAS 技术将可模拟多种攻击场景，检验大模型在面对提示词注入、越权访问、数据投毒等威胁时的防御能力，为企业大模型安全部署提供可靠保障。同时，该技术还可助力企业满足国家网信办《生成式人工智能服务安全评估规定》等法规要求，降低合规风险，提升模型安全可信度，为大模型在金融、医疗、政务等敏感领域的安全落地奠定基础。

5）OT/ICS 安全与物联网（IoT）的融合：

在工业互联网与智能制造不断深化的背景下，BAS 的应用场景将拓展至操作技术（OT）和工业控制系统（ICS）领域，模拟对工控协议、SCADA 系统以及物联网安全产品的攻击行为。未来 BAS 产品发展出针对特定 OT/ICS 协议的模拟能力、对物理世界影响的评估能力，以及在 IT/OT 融合环境中进行攻击链验证的能力，以保障关键基础设施的稳定运行与生产连续性。

6）车联网（IoV）安全：

随着智能网联汽车的快速普及，车联网安全成为新的关注焦点。BAS 将需要模拟针对车辆系统、V2X

通信、自动驾驶系统等关键组件的攻击。未来将推动 BAS 在车辆网络、车载系统以及云端平台的安全验证技术方面取得发展，从而确保智能汽车的行车安全与数据隐私。

7）供应链安全：

鉴于供应链攻击日益频繁，企业对第三方供应商和合作伙伴的安全威胁管理需求愈发迫切。未来 BAS 将具备更强的供应链安全验证能力，能够模拟对供应商软件、硬件组件、服务以及人员的攻击，精准评估供应链中的薄弱环节，助力企业有效管控复杂的供应链风险。

11.1.2 理念深化

未来：安全理念将向安全左移与安全设计的更广泛应用，从合规驱动到风险驱动的全面转型。市场拓展向 OT/ICS 安全、车联网、供应链安全等新兴领域的应用。

1）安全左移理念的拓展应用：

网络安全理念将持续从产品部署后的打补丁模式，向开发早期（设计、开发阶段）的安全左移与安全设计模式转变。未来 BAS 在 DevSecOps 体系中的重要性将更为凸显，借助自动化安全测试（如 API 安全测试、IaC 安全测试）等手段，在代码编写、版本迭代阶段就能及时发现并修复安全缺陷。这将使安全真正根植于业务系统，从源头强化产品的内生安全属性，显著降低后期修复成本与风险。

2）从合规驱动到风险驱动的转型：

尽管合规仍是企业安全建设的基础，但重心将逐步转向基于风险实际状况和业务影响的风险驱动模式。未来 BAS 的量化能力将成为这一转型的关键支撑。通过精准量化攻击成功率、业务损失风险等指标，BAS 能够助力企业优先分配资源应对最具威胁的风险，而非仅仅聚焦于合规清单中的漏洞。这将促使安全投资决策更加科学、高效，推动企业迈向主动安全治理的新阶段。

11.2 建议

基于对 BAS 技术发展趋势的深入研判以及对第三季度市场现状的详细分析，现向用户和厂商提出如下建议，旨在共同推动 BAS 在网络安全领域实现价值最大化。

11.2.1 面向用户的建议

企业作为 BAS 技术落地与发挥实际效用的关键力量，应从以下几方面着手：

1）持续学习与能力提升：

建议深入学习 BAS 的核心概念、技术原理、主流产品功能及其应用场景，密切关注行业发展动态，尤

其是 AI、大模型在 BAS 领域的最新应用成果。具体而言，可通过阅读专业报告、行业经典书籍，积极参与行业研讨会以及线上课程等方式，不断提升自身对 BAS 平台的操作技能与结果分析能力。同时，加强对 MITREATT&CK 框架等攻防知识的学习，从而提高对攻击链和 TTPs 的认知水平，为有效利用 BAS 打下坚实基础。

2）将 BAS 融入日常安全运营：

转变安全运营思维模式，把 BAS 从间歇性测试工具转变为日常安全运营的常态化机制。为此，应设定周期性 BAS 验证任务，例如每日或每周针对核心系统开展攻击模拟；实现 BAS 结果与 SIEM/SOAR 平台的自动对接，以此触发相应的自动化响应流程；将 BAS 纳入漏洞管理流程中的修复验证环节；并借助 BAS 进行常态化攻防演练与团队训练，以此磨砺应急响应能力。

3）关注指标量化，实现量化安全：

深入理解并充分运用 BAS 提供的各项量化指标，如攻击成功率、检测率、MTTD/MTTR、ATT&CK 覆盖率等，将其作为优化安全投入与提升防护效果的关键依据。具体措施包括建立安全绩效基线，持续跟踪指标变化趋势；将技术性指标转化为业务人员能够理解的语言，以便向上级准确阐述安全价值与投资回报；依据量化结果，持续驱动安全策略的优化调整以及资源的合理分配。

4）推动安全文化建设，实现人机协同：

明确 BAS 是辅助人的工具，而非替代人。致力于在企业内部营造以攻防为导向的安全文化氛围，鼓励安全团队与 BAS 系统实现高效协同。为此，应倡导团队成员运用攻击者思维，借助 BAS 模拟攻击，从攻击者视角洞察防护体系的薄弱环节；强化红蓝团队协作，将 BAS 打造为蓝队提升检测能力的陪练工具；同时，突出安全分析师依据 BAS 结果开展深度分析与策略优化的重要价值，避免其仅停留在报表阅读层面。

5）与厂商积极沟通与协作：

主动加强与 BAS 厂商的沟通交流，及时反馈产品使用过程中的问题与需求，携手推动产品的持续优化与功能创新。具体做法涵盖积极参与厂商组织的用户社区活动和研讨会；针对企业特定业务场景以及本土威胁特点，踊跃提出定制化需求；深入了解厂商的库更新机制与威胁情报能力等关键信息。

11.2.2 面向厂商的建议

BAS 厂商作为技术创新与市场发展的核心驱动力量，肩负着重大的责任与使命，应重点关注以下几个方面：

1）加大人工智能研发投入，深化 AI 赋能：

将人工智能研发确立为企业的核心战略方向，着力攻克 AI 在 BAS 领域应用的核心技术难题。具体措

施包括大力开展强化学习、图神经网络、生成对抗网络等前沿人工智能技术在攻击生成、攻击路径探索、防御规避模拟等环节的应用研究；促进人工智能与威胁情报分析、风险量化评估、智能修复建议以及自动化响应等领域的深度融合；积极探索 AI 模型的可解释性，以增强用户对 AI 输出结果的信任度。

2）提升产品集成度，构建开放生态：

BAS 厂商应积极寻求与 SIEM、SOAR、EDR、云安全平台、ASM、漏洞管理平台等各类现有安全产品实现深度融合，协同构建以 AI 驱动的安全运营平台。为此，需积极推广开放 API 以及标准化数据接口，确保产品能够在多云、混合云环境下实现深度集成；加强与国内主流安全厂商的紧密合作，实现产品间的无缝对接与数据共享，有效突破工具孤岛的困境。

3）深耕行业定制化需求，提供精细化解决方案：

针对金融、能源、政府、工控、互联网等不同行业的独特业务特性与安全痛点问题，量身定制契合行业需求的 BAS 解决方案与攻击场景。具体而言，应组建行业专家团队，深入剖析行业监管要求与业务流程；开发具有行业特色的攻击评估模型与威胁模型；提供符合行业规范的合规性报告模板以及量化指标体系。

4）加强与用户合作，共同完善行业标准：

积极参与国家及行业标准的制定工作，助力推动 BAS 技术在国内实现标准化、规范化发展。为此，需与用户建立起紧密且高效的反馈机制，将用户在实际应用过程中的宝贵经验与需求作为产品改进以及标准制定的关键参考依据；在信通院、保联盟等行业权威平台积极贡献技术力量，全力推动 BAS 能力等相关标准的落地实施。

5）注重用户教育和服务，降低使用门槛：

尽管产品具备高度自动化特性，但仍需提供高质量的用户教育服务以及专业的技术支持服务，以降低用户使用 BAS 的难度与成本。具体措施方面，应精心编制详细的产品文档与在线教程；定期举办用户培训活动与技术交流会议；打造专业水准的服务团队，为用户提供更优质的攻击场景定制、结果分析指导、策略优化建议等增值服务。

参考文献：

【1】 网络安全法.[2017-06]

【2】 数据安全法.[2021-09]

【3】 个人信息保护法.[2021-11]

【4】 关键信息基础设施安全保护条例.[2021-09]

【5】 Forrester Choose Your Own MDR Adventure Amid EverExpanding Services，[2025 02].

【6】 Forrester Strengthen Proactive Security With Continuous Security Testing，[2025 01].

【7】 Forrester The Attack Surface Management Solutions Landscape Q2 2024,[2024 05].

【8】 Forrester The Four Steps For More Proactive Security,[2024 05].

【9】 Forrester The Three Principles Of Proactive Security,[2024 05].

【10】 Gartner How to Select the Right Penetration Testing Provider for Your Organization,[2023 11].

【11】 Gartner Innovation Insight Automated Security Control Assessment,[2024 08].

【12】 Gartner Market Guide for Adversarial Exposure Validation,[2025 05].

【13】 Gartner What should I know about Breach and Attack,[2025 04].