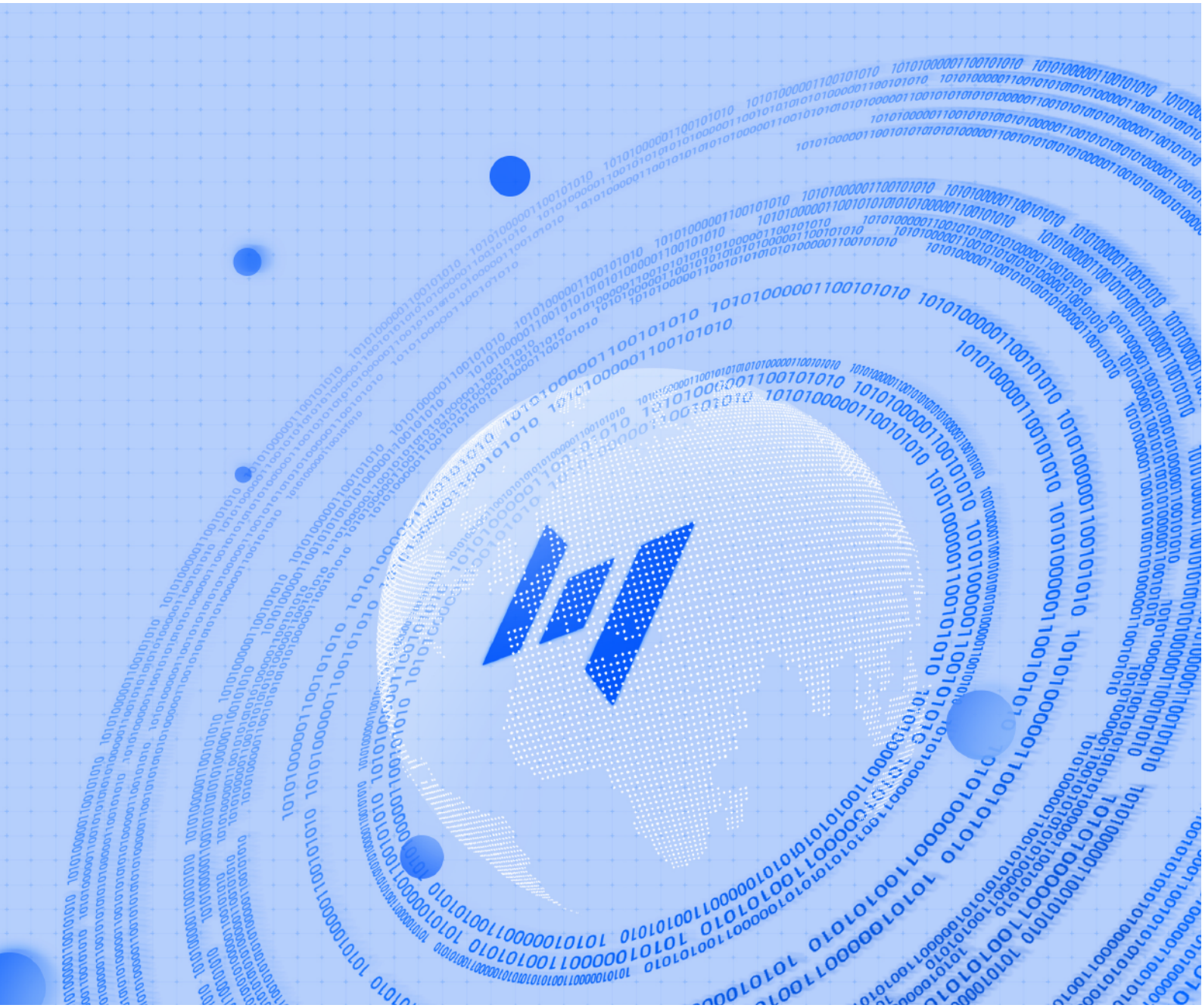
万径安全
MegaVector

CDSL-YAK
企业安全建设解决方案



四 维 创 智 （ 北 京 ） 科 技 发 展 有 限 公 司

近年来，随着互联网技术的快速发展和应用，互联网安全事件愈发频繁。从病毒勒索、网络钓鱼到数据泄漏，企业和用户都面临着严峻的网络安全威胁。中国政府高度重视网络安全问题，出台了一系列相关政策法规，包括《中华人民共和国个人信息保护法》、《中华人民共和国数据安全法》以及《网络安全法》等，为网络安全、数据安全和个人信息保护提出了方向性和基础性指引及监管要求。

在此背景下，企业更需要强大的网络安全能力来保障其业务的安全性。而一个企业要进行信息安全架构的体系建设，需要在网络的各个层次，针对不同的业务场景，进行安全能力部署。因此，对于网络安全产品的需求不仅要满足不同的业务场景，还要具有良好的兼容性和可扩展性。然而，当前的网络安全产品往往因为存在技术偏差、编程语言和规则的不统一，导致产品间存在割裂，无法很更好地进行集成和协同，从而无法最大化地发挥安全防护效果。这无疑为企业的信息安全构建建设增加了难度。

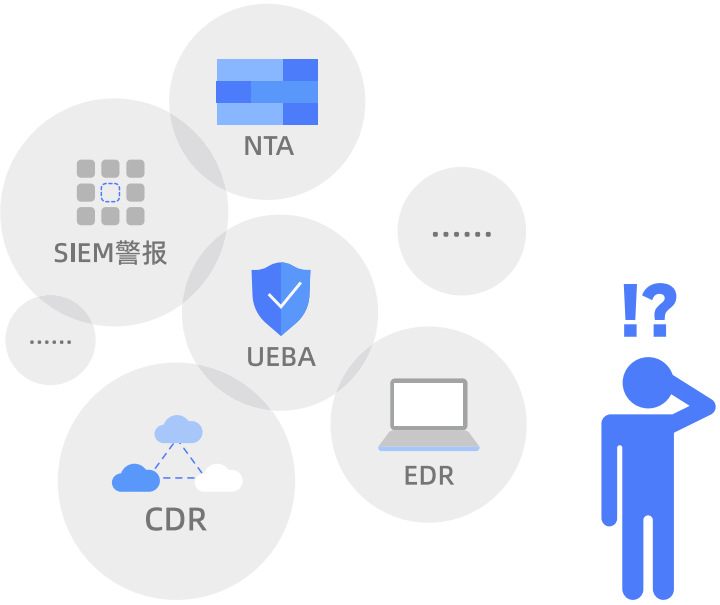
PART 01 痛点分析

低位安全能力的分散和不稳定

底层的网络安全能力，如端口探测、指纹、poc/exp等，我们可以将之称为低位底层安全能力，这是所有网络安全产品的基础。然而，在实际的安全环境中，这些原子化的安全能力常常是分散和不稳定的。大量的安全从业者使用不同的开发语言，开发出了大量功能相同或相似的安全能力。这不仅造成了巨大的人力物力浪费，也造成了这一层面的安全能力的割裂，导致低效和不稳定。这种现状严重阻碍了更高层次的安全产品的研发和优化。

安全产品的复杂性和能力割裂

在企业安全建设体系中，企业采购的各厂商之间的产品存在互不兼容的情景，这造成企业业务数据分散，安全能力冗余。目前在安全市场上还未出现攻防一体的安全产品，大多还是基于单一方向的目标来实现的中间层安全产品，例如：攻击侧的扫描器、态势感知等，防御侧的WAF、蜜罐等，而这些产品在服务厂商、研发语言上的不同使得产品功能异常冗杂和重复，这让产品在甲方进行业务场景测试时，尽管产品自身可能非常优秀，但往往无法通过测试。



安全产品的复杂性和能力割裂

在企业安全建设体系中，企业采购的各厂商之间的产品存在互不兼容的情景，这造成企业业务数据分散，安全能力冗余。目前在安全市场上还未出现攻防一体的安全产品，大多还是基于单一方向的目标来实现的中间层安全产品，例如：攻击侧的扫描器、态势感知等，防御侧的WAF、蜜罐等，而这些产品在服务厂商、研发语言上的不同使得产品功能异常冗杂和重复，这让产品在甲方进行业务场景测试时，尽管产品自身可能非常优秀，但往往无法通过测试。

PART 02 方案说明

当前企业的网络安全体系依然以单一的安全产品为主，已经无法应对日益复杂和不断演化的网络环境。建立一个工程化、系统化、统一化的安全平台就显得尤为重要。一个完整的安全平台能够更灵活、更全面地响应各种安全挑战，也能确保关键组件的相互协调和整合，更能根据业务需求和业务场景有针对性地完善安全制度、安全策略、安全方针等具体安全管理要求。

以YAK语言为核心，以衍生产品为配套的CDSL-YAK企业安全建设解决方案应运而生。其目的在于解决网络安全底层能力的分散与不足，安全产品之间的割裂和冗余等问题。借助YAK语言的特性，将安全能力融合在底层基座，实现低位安全产品的高效集成，增强安全产品之间的协同性和通用性。同时，依托衍生产品，通过构建底层安全能力基座，协助企业进行网络安全体系建设，推动企业安全运营与安全管理的改革，提高企业高位安全能力。

PART 03 方案详述

当前企业的网络安全体系依然以单一的安全产品为主，已经无法应对日益复杂和不断演化的网络环境。建立一个工程化、系统化、统一化的安全平台就显得尤为重要。一个完整的安全平台能够更灵活、更全面地响应各种安全挑战，也能确保关键组件的相互协调和整合，更能根据业务需求和业务场景有针对性地完善安全制度、安全策略、安全方针等具体安全管理要求。

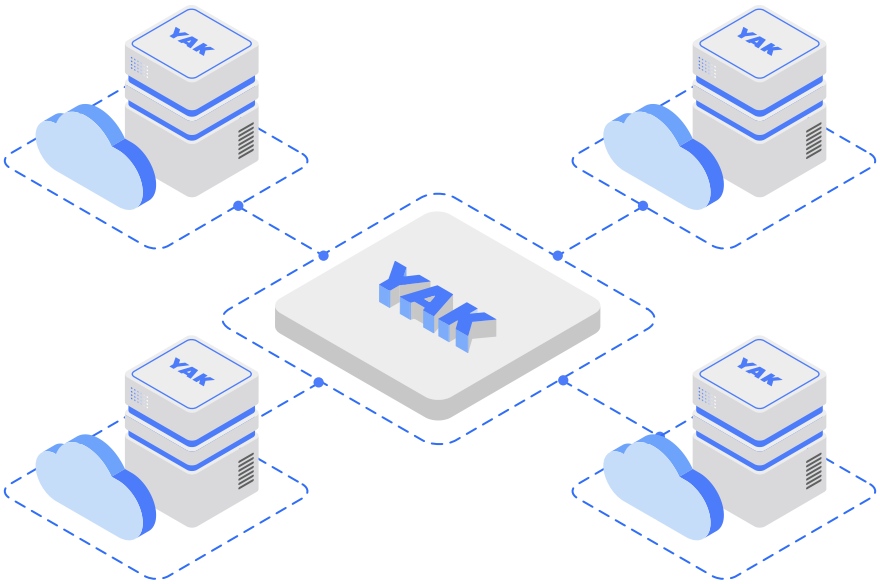
以YAK语言为核心，以衍生产品为配套的CDSL-YAK企业安全建设解决方案应运而生。其目的在于解决网络安全底层能力的分散与不足，安全产品之间的割裂和冗余等问题。借助YAK语言的特性，将安全能力融合在底层基座，实现低位安全产品的高效集成，增强安全产品之间的协同性和通用性。同时，依托衍生产品，通过构建底层安全能力基座，协助企业进行网络安全体系建设，推动企业安全运营与安全管理的改革，提高企业高位安全能力。

3.1 安全能力融合

YAK语言是一门专门为网络安全设计的领域编程语言（DSL）。它能够实现与通用编程语言（GPL）的无缝对接，通过嵌入式计算系统将DSL的能力与GPL的能力深度融合，定制的语法和专业的虚拟机让DSL在专业领域的表现力远超越GPL。同时，YAK强大的协调和整合能力，能将现有的各种安全产品无缝融合，且提供多种安全能力，有效地补齐了现有网络安全市场的短板。

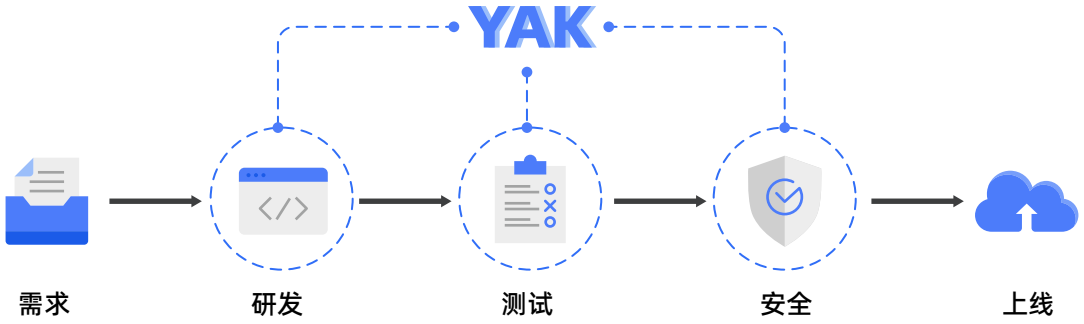
3.2 安全能力下放

YAK语言衍生的配套产品，均封装了YAK语言强大的安全能力。无论用户是否具备专业的安全知识，都能够有效地应对企业现有的安全危机。特有的远程协助功能也能让总部帮助分中心进行远程的能力支持。这种能力对于分散式的企业架构，例如一地多中心或总部+分部的架构具有非常显著的优势。



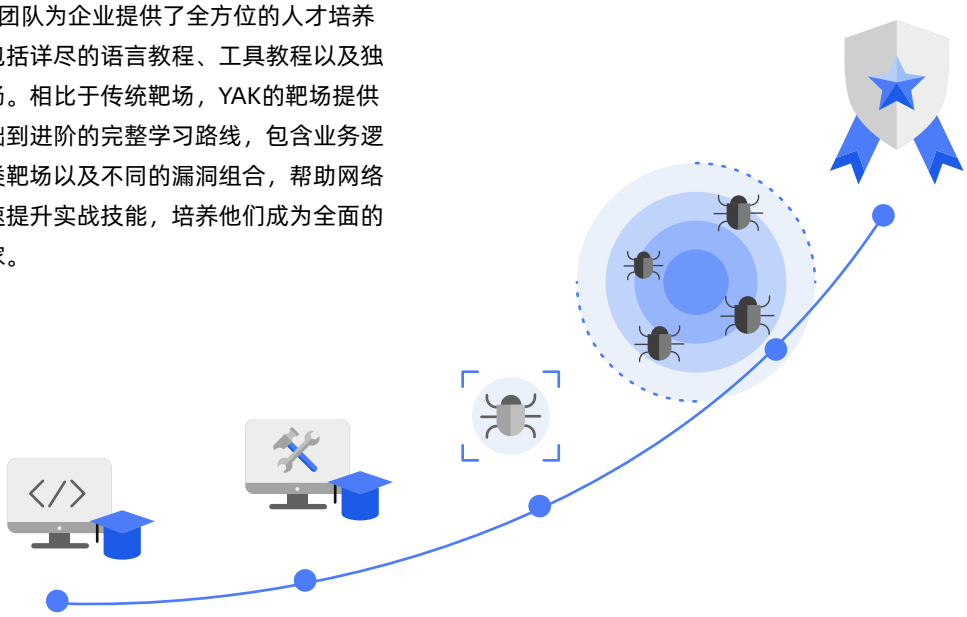
3.3 安全能力左移

YAK语言的“安全能力左移”理念颠覆了传统模式，将安全能力主动赋予给开发和测试人员。在业务研发测试阶段，除了通过Yakit产品本身的检测能力进行自动测试外，有编程基础的他们，只需要通过YAK封装的现有库函数，就能够快速编写针对业务场景的漏洞检测脚本。“安全能力左移”有效地针对了业务场景的检测，使得安全测试变得更加高效。



3.4 安全人才培养

YAK安全团队为企业提供了全方位的人才培养解决方案，包括详尽的语言教程、工具教程以及独具特色的靶场。相比于传统靶场，YAK的靶场提供了一条从基础到进阶的完整学习路线，包含业务逻辑漏洞、各类靶场以及不同的漏洞组合，帮助网络安全人才快速提升实战技能，培养他们成为全面的网络安全专家。



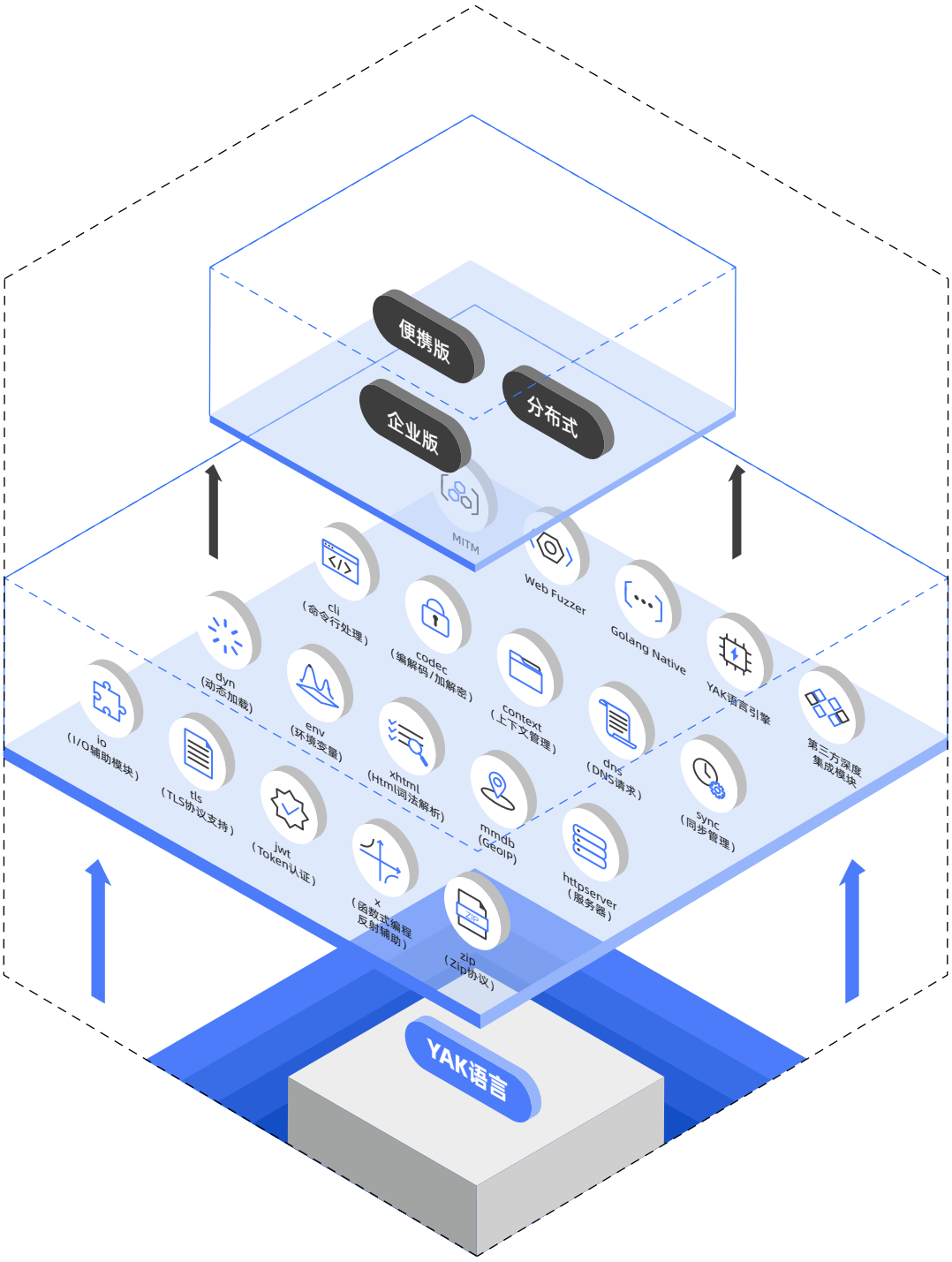
3.5 安全测试流程管控

部分行业对安全测试的风险控制的要求极高。针对渗透测试的人员、工具、目标范围、数据、行为等环节进行集中授权和管理，是部分行业对渗透测试的明确需求明文要求。所以，对于渗透测试过程中的风险控制就显得尤为重要。Yakit的分布式测试，实现了对测试流程的集中管理：

- 对测试人员进行认证授权，获得授权的人员才能接入渗透测试系统开展渗透测试任务
- 对工具的使用进行授权，不同的渗透测试人员，仅能使用获得授权的工具使用权

- 对测试范围和时间进行授权，渗透测试人员只能够在规定的时间内，对授权的目标范围进行渗透测试
- 对渗透测试过程中产生的数据进行自动的集中存贮，包括渗透测试过程数据、结果数据、影响业务的干扰数据、漏洞验证和利用数据等等
- 能够记录渗透测试的行为，能够记录并自动上传每个测试人员的操作日志
- 能够对每一个渗透测试任务以多个维度进行审计，包括按任务、按人员、按时间、按目标（测试范围）等

PART 04 方案技术架构



PART 05 方案核心优势

知识沉淀，解放企业安全团队生产力

YAK最核心的思路不仅仅是解决企业的安全问题，更重要的是注重安全行业人才的培养与建设。通过学习YAK语言Yaklang，安全从业人员能力可以得到有效提升质的飞跃。企业安全团队也能在整个安全建设中，不断筛选、不断调整，降低整个安全团队的用人成本。

跨部门协作

安全能力的左移，使得不同部门间能够相互交流和分享知识，这促进了全员的安全意识和教育，有助于降低人为失误引发的安全风险。综合不同部门提供的信息，能够更好地评估整体风险状况。有助于组织制定更全面的风险管理策略，以便在业务发展中保持适当的安全性。

安全测试自主可控

测试工具的统一，使得安全测试有了最低保障，能够实现渗透测试任务的发布和共享，实现多人或者多个团队针对同一个任务的协同作战，实现优势互补、数据共享、分时联动的团队渗透测试模式，提升渗透测试的效率和紧急任务的响应能力。

全新思路，让安全更融合

CDSL-YAK以全新的网络安全领编程语言为基础，通过构建安全底层能力基座，让技术、运维、运营、管理完美融合，建立企业网络安全生态体系。

扩展性、灵活性、高可用性，保障企业安全

CDSL-YAK以全新的网络安全领编程语言为基础，通过构建安全底层能力基座，让技术、运维、运营、管理完美融合，建立企业网络安全生态体系。

贴心服务，保姆式一站教学

Yaklang.io 团队可为企业用户提供专属一对一保姆式教学服务，同时针对企业用户，还有专属的产品使用手册。“做难而正确的事”是我们对技术的态度，也是我们不变的初心。

万径安全
渗透测试质量提升方案

万径安全
MegaVector

万径安全
MegaVector

让 世 界 更 安 全　　让 安 全 更 简 单

YAK公众号

万径安全公众号

010-5945 6626（北京）
北京市海淀区 上地街道 金隅嘉华大厦 F座804
market@4dogs.cn
http://megavector.cn