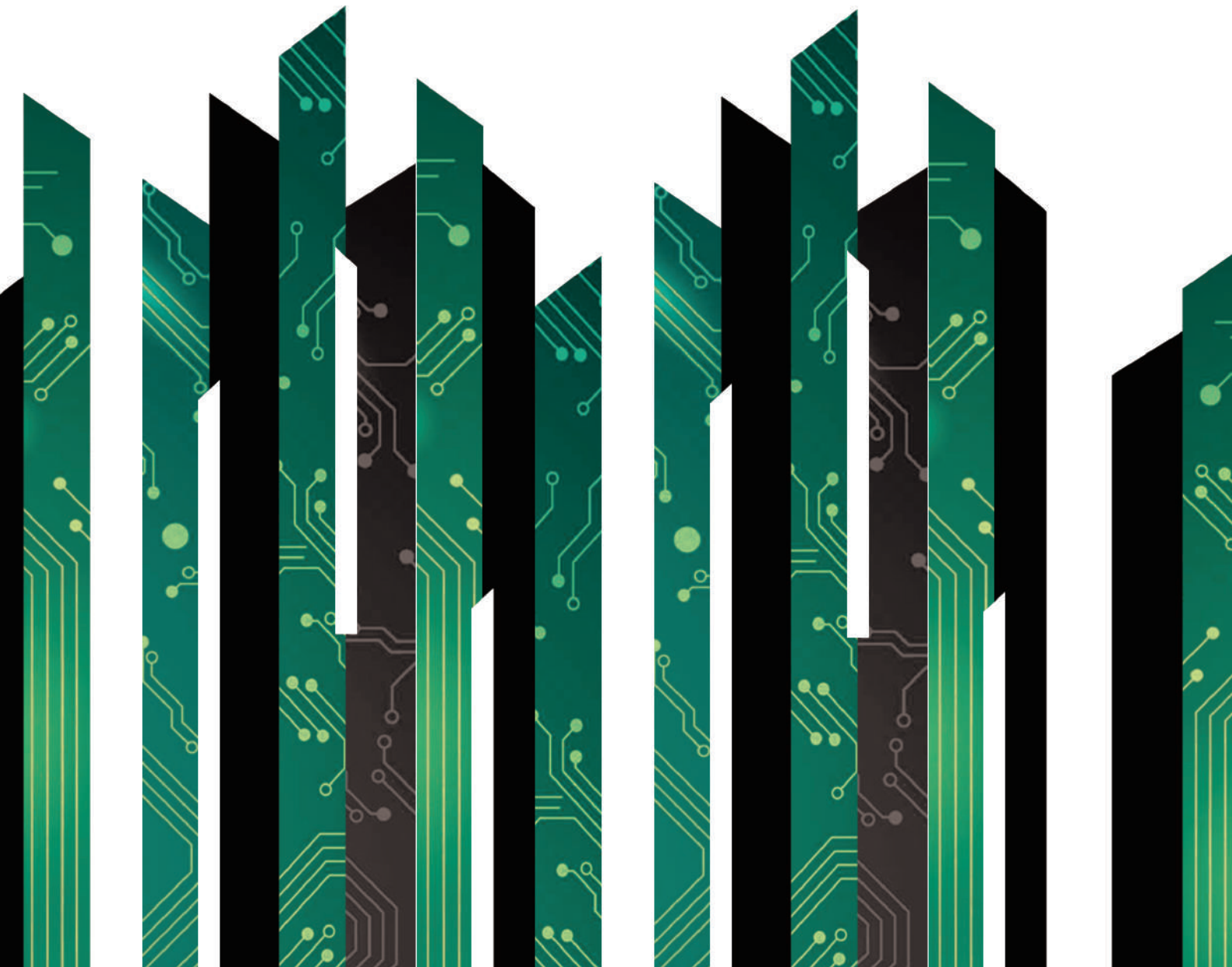
长亭科技
CHAITIN

长亭安全服务白皮书

北京长亭科技有限公司



长亭安全服务白皮书

目录
CONTENTS

网络安全服务：什么时候、如何、关注什么？

在开始之前，我们先看几组数据：

• 收到一封钓鱼邮件，23%的员工会打开，11%会点击邮件中的恶意链接。

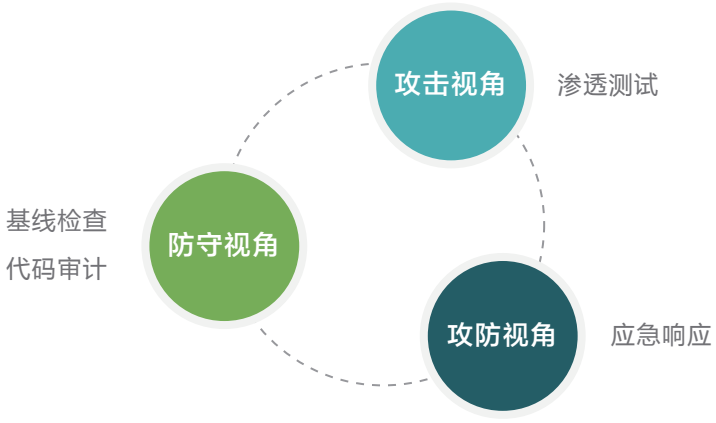
• 60%的攻击案例中，黑客只需要几分钟就可以危害到一家企业。

• 99%的CVE漏洞，被公布1年之后仍可被利用。

• 恶意代码事件每5秒发生一起，缺乏漏洞管理，不仅要担心攻击者进来，还要担心信息出去。

攻击防不胜防，网站漏洞、配置不当、员工安全意识匮乏……都成为企业中招的原因。而大多数时候，企业从大量安全咨询报告中拿到的，只是一长串存在问题的列表。关于如何分辨哪些漏洞会产生重大危害，如何修复这些问题，以及从哪儿开始，却内容寥寥。同时，除了防守之外，企业如何避免成为自身漏洞的生产者，不给攻击者留下可乘之机？一旦遭遇攻击，什么才是有效的应对？

长亭科技根据多年真实攻防经验，梳理安全服务核心环节，提供相应服务如下：



我们同时提供观点帮助洞察漏洞背后的逻辑：

1) 在一连串复杂、序列的攻击行为中，呈现完整的攻击线路图；

2) 从攻击者的视角解读，当前网络环境中风险评级的最佳实践；

3) 何种类型的安全管理对企业是有效的。

长亭安全服务概览

渗透测试

Web应用安全检测

Web服务安全检测

外网安全检测

内网安全检测

安全意识检测

移动端安全检测

IoT设备安全检测

红蓝对抗

代码审计

C／C++审计

Java审计

PHP审计

Python审计

Android审计

Objective-C审计

ASP审计

基线检查

基础安全检查项

通用安全提升检查项

安全能力提升项

应急响应

网络攻击

Web攻击

恶意程序

业务安全

先攻击者一步：渗透测试服务

长亭科技研究和服务项目的数据显示，约半数企业机构存在丢失系统最高权限的风险，超过70%存在信息泄露漏洞，超过50%存在越权漏洞，约30%存在越权以外的业务逻辑漏洞……

企业线上业务的基础架构与网络环境已经变得越来越复杂，安全漏洞经常出现在缺乏关注的角落；随着资产数据的价值升高，由恶意攻击导致的信息泄露、业务宕机，甚至系统权限丢失，正在让企业付出日趋高昂的代价。保障线上业务安全，需要先于攻击者找到并解决问题。

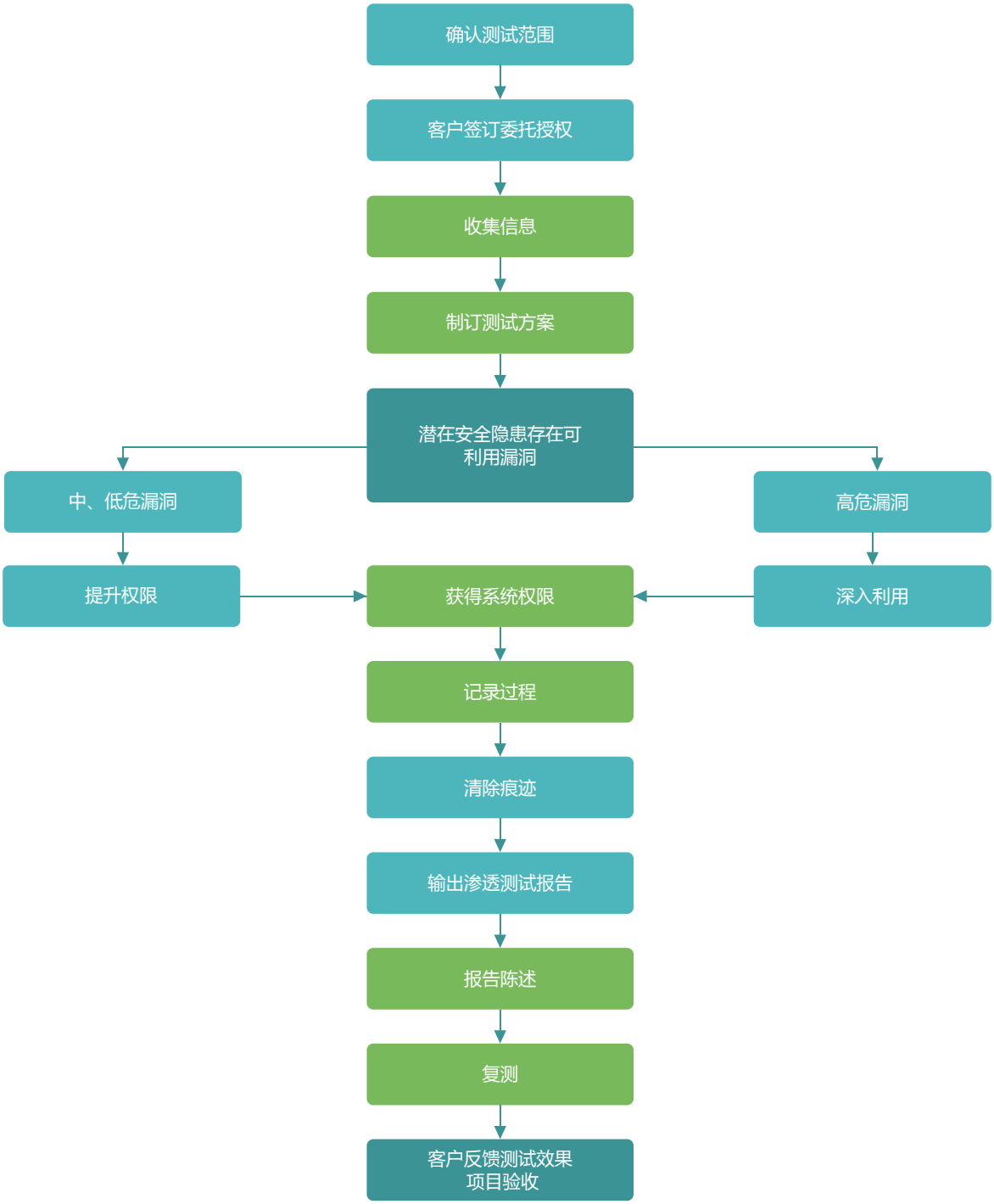
渗透测试是一种以攻击者视角，通过模拟入侵识别IT基础架构中不安全因素的评估方法，能够验证目标系统的技术安全性，快速发现当前最亟待解决的关键问题。通过修复漏洞，以领先攻击者的方式，帮助企业实现业务安全。

长亭渗透测试服务

长亭渗透测试服务，由在国内外黑客比赛中屡摘桂冠，又服务过大量知名企业的专业团队实施，以全面、贴合业务的视角深入检测，挖掘漏洞并最大程度模拟其可能造成的危害，使企业先于攻击者发现问题，防患于未然。

过程中，长亭安全团队严格遵守授权许可范围，并通过风险规避和过程控制保证渗透测试不妨碍正常业务运转。

服务流程



图：长亭渗透测试服务流程

- 确认测试范围并委托授权

  根据企业需求确认测试范围与测试深度，双方签订委托授权书。

• 收集信息

信息收集分析是模拟入侵攻击的基础，很大程度上影响着测试的贴合程度与测试结果的评估作用。方法包括主机网络扫描、操作系统类型识别、应用判别、账号扫描、配置判别等。

• 制订测试方案

在充分沟通测试目标、测试内容的基础上，针对客户业务逻辑、网络环境、系统架构定制测试计划与实施规划，包括但不限于时间安排、流程控制、参与人员、工具使用等。

• 报备测试IP

提前沟通测试IP，避免因突然出现的大量未知攻击干扰企业运维工作，也可选择让攻击流量经过代理服务器并监控记录攻击日志，方便复盘。

• 测试执行

经过信息收集和数据分析，渗透测试通过对漏洞的路径式利用达到模拟入侵的效果。具体执行存在两种可能性：

1）目标系统存在重大弱点，测试人员可直接控制目标系统，调查弱点分布；

2）目标系统没有重大弱点，但可以获得远程普通权限。测试人员通过已有权限进一步收集目标系统信息，提升权限，最终获取系统最高权限。

• 记录过程与痕迹清除

模拟渗透过程中，测试人员会详细记录操作步骤，以呈现完整的攻击路径，并为之后的痕迹清除做准备。

测试完成后，测试人员将清理过程中产生的操作痕迹，恢复系统日志、配置等至原始状态。

• 渗透测试报告输出

串联安全弱点形成攻击路径，评定漏洞级别并提出落地可行的修复建议，帮助企业优先解决阻碍业务发展的关键威胁。

• 报告陈述

由安全工程师上门复盘测试过程并讲解报告内容，涵盖漏洞成因、危害程度、修复建议，以及为防止同类问题再次发生而应采取的流程规范等。

• 复测

当修复完成后，企业可选择复测服务以确认漏洞的修复状态。

服务内容

基于丰富的渗透经验和精湛的攻防技术，长亭安全服务团队提供高度定制化的高质量服务，主要包括：

• Web应用安全检测

对被测系统业务功能进行安全检测，对象包括OWASP Top10在内的常规漏洞，如SQL注入、代码注入、XSS、CSRF、SSRF、XXE、越权、逻辑漏洞、文件包含、文件上传、任意文件读取、验证码安全等。

• Web服务安全检测

对支持Web业务稳定运行的服务进行安全检测，对象包括常见系统服务、常见容器组件、业务框架、业务相关支撑系统。

• 外网安全检测

模拟真实的黑客攻击，通过互联网（外网）对被测系统进行安全检测，检测范围包含应用层安全、系统安全、运维安全等。

• 内网安全检测

以外部获取内网主机权限，或直接接入企业内网的方式，对内网进行横向深度安全检测，发现内网中的安全问题，如业务系统未授权访问、系统弱口令、核心敏感信息泄露等。

• 安全意识检测

从非技术层面提供定制化的模拟钓鱼攻击、撞库攻击等，测试企业安全制度和员工安全意识。

• 移动端安全检测

通过逆向分析对客户端自身安全性进行测试，包括客户端本地存储安全、加密算法安全、加密协议安全、接口安全性等。

• IoT设备安全检测

针对物联网设备进行安全检测，测试对象包括执行器、网关、传感器、云托管平台、移动设备、通信协议等。

• 红蓝对抗

由长亭顶尖安全研究员组成蓝军，与企业安全团队（红军）进行针对性模拟对抗。蓝军使用非常规性渗透思路，以不限于物理渗透、Wi-Fi渗透等方式，对目标实施可控的真实网络攻击，以检测并提高企业的入侵发现、事件处置等能力。

服务交付

• 渗透测试报告

长亭渗透测试报告客观记录漏洞的挖掘与利用过程，方便漏洞复现；同时提供清晰可落地的修复建议，帮助快速修复隐患，总结抵御攻击的最佳实践。

此外，报告还涵盖尽量详细的项目信息与测试细节，为企业管理人员提供可查找、可核对的实施记录，也可作为参考案例用于后续测试与培训。

长亭渗透测试服务优势

了解攻击思维，攻防技术领先

只有匹敌、甚至领先攻击者技术水平的测试团队，才能真正帮助企业领先黑客一步。

长亭安全服务团队在连续两年的时间里，获得10多个信息安全大赛冠军，多次包揽国内外赛事的前三名，即使和一群真实的黑客同台竞技也表现出极大的技术优势，他们不仅仅是安全专家，更是一群有黑客思维、了解“坏事情”的人。

深谙客户需求，降低沟通成本

真正理解客户需求的测试团队，才能直击痛点，准确解决问题。企业间的网络环境、系统架构、业务逻辑千差万别，需求侧重各有不同。行业深耕让长亭安全服务团队了解不同场景下的安全诉求，通过定制化渗透方案，发现日常业务流程中未知的安全缺陷，较传统渗透测试更注重帮助业务发展，常被客户评价服务效果远超预期。

标准化测试流程，高质量全覆盖

多年总结的标准化流程是长亭渗透测试服务高质量、低风险、全面覆盖的保证，有效避免了诸如系统宕机、漏洞类型漏测等问题。此外，除了更落地的安全整改建议与漏洞修复指导，长亭渗透测试团队还可提供针对性培训，帮助客户提升安全能力水平。

四大规避措施，降低测试风险

为了最大程度减轻影响，避免由于模拟攻击造成的目标服务器故障，或网络和主机的业务中断，长亭安全服务团队从以下四个方面采取措施：

- 参数收集

在信息搜集和整理环节，优先考虑受测网站或程序的基本参数，以便尽可能减少其在测试过程中受到的压力，保证稳定运转。

- 时间选择

了解受测网站或程序的负荷分布，测试时间避开业务高峰时段。

- 密切沟通

建立高效沟通机制，测试前充分了解系统信息，测试中随时沟通已发现的高危问题，当可能产生不可控后果时，与企业再次协商测试方案。

- 信息控制

分层进行信息控制并严格保密系统数据与测试结果，保证敏感信息不外泄。

解决业务隐患：代码审计服务

- 渗透测试更擅长解决“点”的漏洞，那么“面”的问题如何应对？
- 系统迭代频繁，新版本如何在上线之前消除隐患？
- 有些问题重复出现，如何彻底解决？

当企业安全建设面临如下情境：某些业务接口隐蔽性较高，需要依赖传递正确参数后才能正常访问；或是某些业务逻辑前置的交互步骤中缺失漏洞触发的要素，需要较多前置条件；甚至如二次注入、无外网访问的服务端请求伪造，以及无回显命令注入等漏洞成因本身就需要对业务逻辑特别清晰才能发现时，代码审计就成为了更为妥当的解决方案。

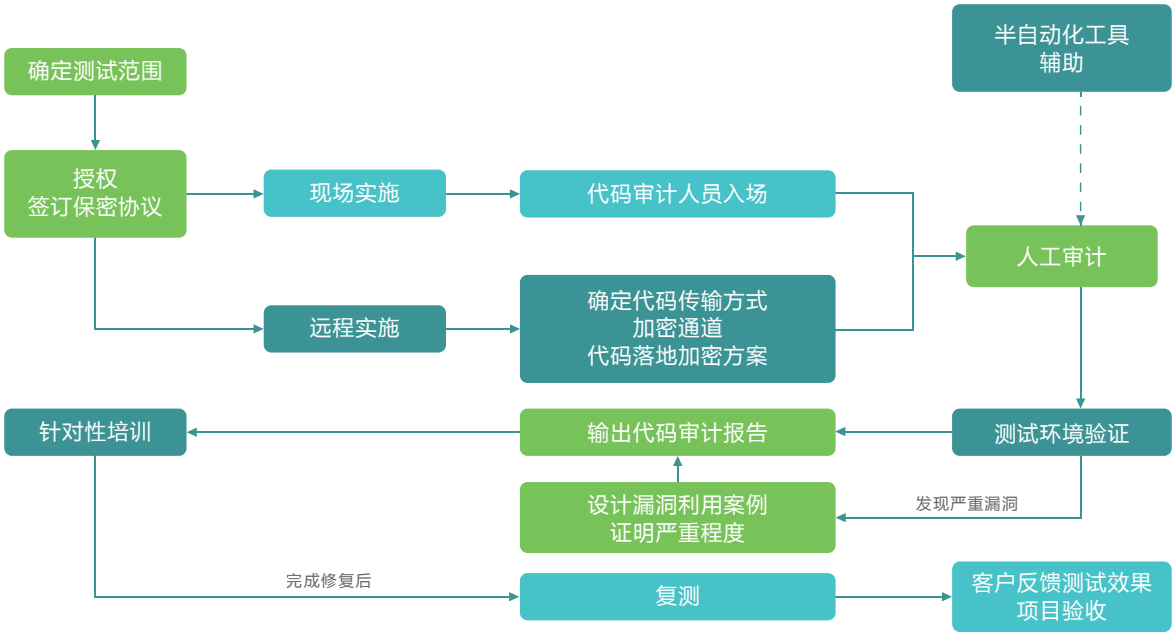
代码审计是一种以发现程序错误、安全漏洞和违反程序规范为目标的源代码分析。它是防御性编程范式的一部分，旨在检测代码中存在的安全缺陷，针对存在的缺陷提供解决方案，降低程序使用时的安全风险。在软件发布前进行代码审计，可将不安全因素扼杀在萌芽状态，极大缩减了后期修复所花费的成本。

代码审计能更深层地发现代码中的隐患，为测试人员开启“上帝视角”。测试过程不会对线上业务造成影响，不会导致诸如系统宕机、服务卡死、数据库阻塞、业务数据丢失等风险。但由于代码审计需要深入理解代码逻辑和业务结构，因此对审计人员的能力素质要求较高，需要花费的精力也更多。

长亭代码审计服务

长亭安全团队提供的代码审计服务，通过人工观察、模拟执行或半自动化工具扫描的方式，全面深入挖掘代码中的通用Web漏洞、业务逻辑漏洞、应用程序漏洞以及应用程序配置文件中的不安全因素等，不仅解决现存隐患，更能通过针对性培训帮助企业整体提升编程安全水平。

服务流程



图：长亭代码审计服务流程

支持编程语言

C / C++、Java、PHP、Python、Android、Objective-C、ASP

审计方式

• 纯人工观察

代码审计实施人员通过阅读代码理解业务逻辑，从而发现通用的Web安全漏洞、业务逻辑漏洞以及配置缺陷。

• 模拟执行，跟踪调试

代码审计人员在测试环境模拟执行代码或利用编译器编译部分代码执行，通过跟踪调试快速定位问题。

• 半自动化工具扫描

根据客户需求，可选择半自动化工具对人工审计后的代码进行扫描，提升结果的准确性。

可发现漏洞类型

- 通用Web安全漏洞及业务逻辑漏洞

SQL注入	XSS
SSRF	CSRF
JSON Hijacking	远程命令执行（Remote Command Execution）
远程代码执行（Remote Code Execution）	任意文件上传
任意文件读取	文件包含
信息泄露	逻辑漏洞 （遍历、越权、任意账号重置、验证码校验机制漏洞）

- 应用程序漏洞

二次释放（Double Free）	竞争条件
缓冲区溢出	整数溢出
命令注入	格式化字符串
数组越界访问	内存泄露
未检查返回值	空指针引用
未初始化变量	资源未释放
释放后再使用	

- 应用程序配置缺陷

密码明文存储	加密通讯的密钥可被破解
选用不安全的加密方式	web.xml配置缺陷

执行规范

1） OWASP安全开发指南

2）《软件安全开发标准》（ISO/IEC 27034）

3）《信息安全技术 应用软件系统安全等级保护通用技术指南》（GAT 711-2007）

4）《信息安全技术 信息系统安全等级保护测评要求》（GBT 28448-2012）

服务交付

• 代码审计报告

从数量庞大的源代码中准确找到不安全因素，通过长亭代码审计报告详细呈现审计过程与结果，同时提供简洁易懂的问题定位与整改方案。企业可参考问题的重要性与严重程度，有序地解决安全隐患，也可以报告为蓝本，制订安全编码规范。

• 严重漏洞的Demo展示

对可能造成严重后果的重要漏洞进行可视化展示，帮助了解漏洞的潜在危害，也可作为培训案例，提升企业相关人员的安全意识。

长亭代码审计服务优势

跟踪顶尖技术，保持前沿水平

长亭安全团队运营PWNHUB社区和代码审计知识星球两大平台用于经验分享与技术交流，能够时刻掌握行业最新技术，并取长补短保证服务质量业内领先。

• PWNHUB社区

PWNHUB是国内活跃用户最多的代码审计在线攻防竞赛社区，云集国内外众多高校与知名厂商的一线选手，借助此平台可以充分吸收安全圈最新的代码安全攻防思路，保持世界顶尖水平。

• 代码审计知识星球

代码审计知识星球是由长亭团队核心成员主导的在线代码安全分享圈子，目前已吸引千余名活跃在攻防一线的代码审计高手，通过互动分享经验，不断提高代码审计人员的眼界和技巧。

深耕金融行业，高效审计思路

长亭安全团队曾服务大量金融客户，已形成一套针对Java网银特有的代码审计思路，能够快速并彻底地解决问题。

总结编码习惯，杜绝重蹈覆辙

安全问题归根结底是人的问题，长亭代码审计服务总结程序开发人员的编码习惯，在编码规律中挖掘开发者的安全盲区，通过定向培训从根本上解决由于安全基础参差不齐导致的代码隐患。

补齐安全短板：基线检查服务

基线检查，又称为基础安全配置核查，旨在针对不同版本服务器系统、第三方应用软件、第三方网络硬件设备、接入控制、恶意软件对抗等进行基础安全配置检查。基线检查的目标在于补齐安全最短板，提升企业的安全系数。

在日常安全建设工作中，基线检查可以有效解决以下实际问题：

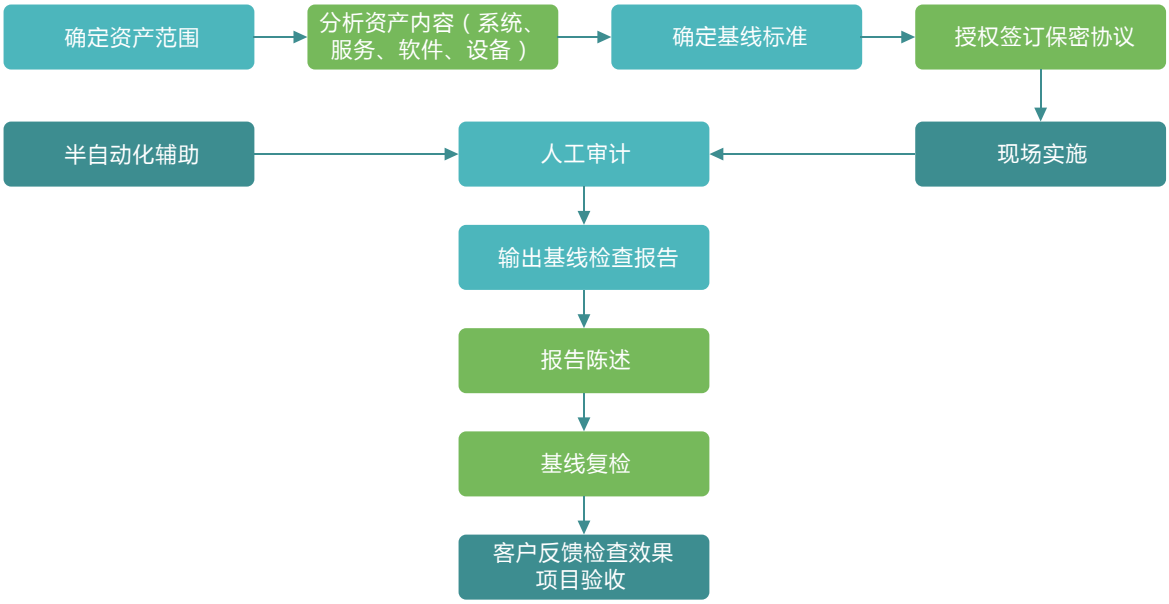
- 是否使用正确配置来持续管理企业系统？
- 是否有攻击者已经进入企业的系统或网络？
- 是否明确现行系统和网络上运行着（或试图运行）哪些软件？
- 是否妥善记录安全设置的更改行为，并对试图绕过安全设置的恶意操作加以限制？

网络安全环境不断变化，许多组织面临着新技术与新问题层出不穷的网络威胁困局。大部分企业安全人员对于复杂、变化的安全威胁无计可施，面对不清晰的规则与复杂的要求无所适从，要求快速寻找有效的市场解决方案。

长亭基线检查服务

长亭安全服务团队推出了有效、全面的基线检查安全服务，帮助保护企业和数据免受已知的网络攻击，是提高安全短板的最佳选择。

服务流程



图：长亭基线检查服务流程

- 确定范围与信息收集

确定资产范围，针对需要加固的信息系统（包括主机、网络设备、数据库和中间件等）完成信息收集，并评估工作耗时。

- 基线检查

制订基线检查方案，对加固范围内的资产进行安全评估，确认安全现状。

- 输出基线检查报告

全面记录检查项目与评估结果，并就需要改进的地方提出针对性加固方案，输出基线检查报告。

• 报告陈述

与企业管理人员交流整体检查结果，推演可能面临的安全风险，同时讨论加固方案以形成落地可执行的操作规范。

• 加固与复检

实施安全加固方案，并通过基线复检测试加固效果。

服务标准

一些调查报告显示，实施CIS前五个控制项（硬件资产的清单和控制，软件资产的清单和控制，持续漏洞管理，控制权限使用，移动设备、笔记本电脑、工作站和服务器上的硬件和软件的安全配置）即能有效防御大约85%的攻击。相比于传统的基线检查，CIS标准可以修复更多的不安全配置，阻止常见网络威胁造成危害。

长亭安全服务团队一直参考国际CIS（Center for Internet Security）标准执行基线检查服务。

• CIS标准主要构成：

一、基础（Basic CIS Controls）

1. 硬件资产的清单和控制
2. 软件资产的清单和控制
3. 持续漏洞管理
4. 控制权限使用
5. 移动设备、笔记本电脑、工作站和服务器上的硬件和软件的安全配置
6. 审计日志的维护、监视和分析

二、整合（Foundational CIS Controls）

1. 电子邮件和Web浏览器保护
2. 恶意软件防御
3. 网络端口、协议和服务的限制和控制
4. 数据恢复能力
5. 网络设备的安全配置，例如防火墙、路由器和交换机

6. 边界防御
7. 数据保护
8. 基于需求控制权限
9. 无线访问控制
10. 账户监管和控制

三、组织（Organizational CIS Controls）

1. 实施安全意识提升和安全技能培训计划
2. 应用软件安全
3. 事件响应和管理
4. 渗透测试和红蓝对抗练习

服务内容

长亭基线检查服务对以下项目进行检查：

硬件资产的清单和控制

管理企业网络上的所有硬件设备，确保只有授权的设备才能访问，发现并阻止未授权和未管理的设备访问。

软件资产的清单和控制

管理企业网络上的所有软件，保证只有获得安装授权的软件执行，发现并阻止未经授权软件的安装或执行。

持续漏洞管理

持续获取、评估最新安全事件和漏洞，对其采取合理措施以最大限度地减少攻击者可利用的机会。

控制权限使用

应用合理的流程和恰当的工具跟踪控制计算机、网络和应用程序管理权限的使用、分配和配置，防止权限滥用、错用。

移动设备、笔记本电脑、工作站和服务器上的硬件和软件的安全配置

采用严格的配置管理和变更控制流程，主动管理（跟踪、报告和纠正）笔记本电脑、服务器和工作站的安全配置。

审计日志的维护、监视和分析

收集、管理和分析日志，发现攻击者的痕迹。

电子邮件和Web浏览器保护

防止攻击者通过Web浏览器和电子邮件系统进行钓鱼和挂马攻击，尽量减少攻击面。

恶意软件防御

控制恶意软件的安装、传播与执行，同时优化自动化工具的使用，以快速更新防御策略，及时纠正异常行为。

网络端口、协议和服务的限制和控制

管理（跟踪、控制、更正）联网设备上端口、协议和服务的正常运行情况，最大限度地减少攻击者可用的入口。

数据恢复能力

应用成熟的数据恢复流程和工具，对关键信息适当备份以便及时恢复。

网络设备的安全配置，例如防火墙、路由器和交换机

采用严格的配置管理和变更控制流程，建立、实施和主动管理（跟踪、报告和纠正）网络基础设施设备的安全配置。

边界防御

检测不同信任级别的信息传输，防止、纠正异常行为。

数据保护

采纳防止数据泄露的流程和工具，确保敏感信息的隐私性和完整性。一旦发生泄漏，有应急预案用于减轻泄露数据的影响。

基于需求控制权限

依据人员、计算机和应用程序的需求和权限，运用恰当的流程和工具追踪、控制、防止、纠正其对关键资产（例如信息、资源、系统）的访问。

无线访问控制

跟踪、控制、防止、纠正无线局域网（LANS）、接入点和无线客户端系统的使用状况，保证安全访问。

账户监管和控制

主动管理系统和应用程序账户的生命周期，覆盖它们的创建、使用、休眠、下线过程，避免给攻击者留下可乘之机。

实施安全意识提升和安全技能培训计划

了解组织中所有职能角色（特别是对业务发展有重要影响的岗位）需要具备的安全知识、技能和能力；制订并执行综合计划以评估水平，有效改进。

应用软件安全

管理所有应用软件（来源包括内部开发与外部采购）的安全生命周期，检测并消除不安全因素。

事件响应和管理

具备事件响应流程机制和快速发现攻击、有效控制损失的安全能力，避免由于服务器、应用软件配置不当引发的记录日志缺失或错误，最终导致排查难、取证难、溯源难。

服务交付

- 基线检查报告

长亭基线检查报告致力于呈现全局化的安全评估结果，帮助企业管理人员形成对安全现状的整体认知。同时报告提供清晰的安全加固方案与操作管理建议，企业可据此制订更加完善的流程和规范，最大化检查效果，找到与自身特点契合的最佳安全实践。

长亭基线检查服务优势

增加攻击成本，不只是合规

以升高攻击成本，降低入侵事件成功率为目标，长亭基线检查服务依据国际公认的CIS（Center for Internet Security）标准执行，并在此标准上持续提升——根据最新事件实时增加防御规则，并通过定制自动化检查实现高效监控管理。

相较于传统同类服务，长亭基线检查服务能够在满足合规要求的基础上，修复更多的不安全配置，真正提升企业的安全系数。

应对安全事件：应急响应服务

攻防对抗的过程中，企业的防护水平不断增强，但攻击技术和思路也在不断变化演进。虽然很多信息安全事件可以通过技术的、管理的、操作的方法予以消减，但没有任何一种信息安全策略或防护措施能够提供绝对的保护，确保安全事件一定不会发生。

有一个广为流传的观点：世界上有两类公司，一类是已经被黑客入侵的公司，另一类是被黑了却还不自知的公司。“怎么知道被黑了”和“被黑了怎么办”两个任务，既是妥善应对安全事件的必答题，也是应急响应的覆盖范围。

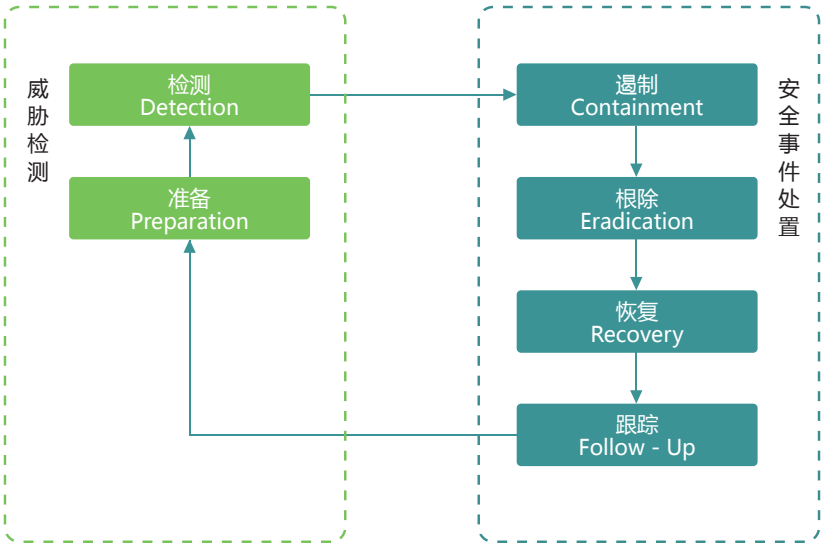
应急响应是指组织为应对突发、重大的信息安全事件发生所做的准备，以及在事件发生后所采取的措施，其目标是帮助企业机构合理应对安全事件，最小化负面影响。

长亭应急响应服务

针对“怎么知道被黑了”以及“被黑了怎么办”两个问题，长亭安全团队提供定制化的应急响应服务，分别从事件发生前的威胁检测与攻击发生时的应急处置入手，帮助企业提升信息安全事件的发现能力和应对能力，并在根除攻击症状之后，针对问题根源提供加固建议，以避免同类事件再次发生。

应急响应生命周期

根据国际广泛采用的PDCERF方法，应急响应生命周期分为6个阶段：准备、检测、遏制、根除、恢复、跟踪。



图： 应急响应生命周期

以上步骤可根据攻击是否发生，划分为两类任务：

- 威胁检测

对应准备和检测阶段，需要第一时间发现异常，并为事件响应做好准备。

- 安全事件处置

对应遏制、根除、恢复、跟踪阶段，需要快速、高效地从攻击事件中恢复，并彻底根除隐患。

服务内容

长亭安全团队围绕上述任务分别提供相应服务。

- 威胁检测能力提升解决方案

1. 威胁情报中心

构建威胁情报中心，及时获取威胁情报，缩短攻击发现时间。

威胁情报主要包含：

漏洞情报	通用软件爆发0day漏洞时，推送漏洞披露过程、漏洞详情和修复方案。
恶意软件情报	僵木蠕爆发时，推送感染状况、样本行为分析和预防与清理方案。
威胁事件情报	发生具有重大影响的安全事件时，推送事件过程和进展情况分析。

2. 流量日志审计方案设计

流量与日志是日常威胁检测，以及事后溯源分析、取证分析的重要依据。长亭安全团队为企业提供流量日志审计的最佳实践方案。

审计方案涵盖：

网络流量	系统日志
应用日志	终端日志

3. 实时威胁检测解决方案

深度整合行业尖端产品，基于业务特点，为企业量身定制系统化的威胁检测解决方案，实现更加快速、精准的攻击行为捕捉，构建实时检测体系，全面提升企业的威胁发现能力。

威胁检测解决方案中使用的系统主要包括：

入侵检测系统	内网威胁感知系统
Web攻击检测系统	主机安全检测系统

- 应急事件处置服务

长亭应急响应服务妥善处置影响企业业务发展的四大事件类型，并在输出应急事件处置报告后，安排安全工程师复盘讲解，分析事件成因并陈述应对过程。

1. 事件类型

1）网络攻击事件

网络扫描事件：黑客利用扫描器对操作系统或应用进行漏洞扫描，尝试发现漏洞。

漏洞攻击事件：操作系统或应用存在未知漏洞（0day）或已知但未修复的漏洞（1day），遭受黑客攻击。

暴力破解事件：业务系统遭到暴力破解攻击，黑客尝试获取后台管理员账号的密码。

拒绝服务攻击事件：服务器遭到拒绝服务攻击，例如大流量DDoS或者CC攻击，导致服务器无法提供正常服务。

2）Web攻击事件

WebShell：网站被上传了WebShell，黑客可借此控制主机。

网页篡改事件：网站页面被篡改，黑客植入炫耀标语。

网页挂马事件：网站页面被挂马，黑客在页面中植入病毒。

网页暗链事件：网站页面被植入暗链，指向网站类型包括博彩、色情、游戏等。

3）恶意程序事件

恶意病毒：终端被病毒感染，正常功能或数据遭到损坏。

僵尸网络程序：主机被控制，成为了黑客发起DDoS攻击的帮凶“肉鸡”。

挖矿程序：服务器变成了“矿机”，大量资源被消耗，业务系统无法正常工作。

勒索软件：数据文件被加密，黑客勒索高额赎金。

4）业务安全事件

薅羊毛事件：黑客利用业务逻辑缺陷进行欺诈，获取不正当利益。

数据泄露事件：隐私数据被非授权人员获取，包括用户账号、密码、银行卡信息、订单数据等。

权限泄露事件：业务相关权限失控，数据或系统配置被修改。

2. 处置手段

1）系统与应用日志审计

全面审计系统与应用中的日志，识别异常行为，为后续溯源与取证工作提供支撑。

2）恶意程序清理与分析

全面排查和清理系统中的病毒、木马、蠕虫、后门等恶意程序，以及Web站点中的WebShell、篡改页面、暗链、挂马等恶意页面。

3）系统异常恢复

第一时间恢复因受黑客攻击而无法正常运作的系统，最大限度地降低事件对业务产生的不良影响。

4）入侵原因分析

综合分析系统、应用中的各类事件线索，包括日志审计结果与漏洞存在情况等，找到黑客的入侵途径。

5）入侵证据收集

采集黑客攻击时留下的痕迹，为后续法律程序准备数字证据。

6）安全改进建议

针对入侵分析中发现的安全问题提供修复建议，配合用户需求完成整改和加固，降低业务安全风险。

服务交付

- 应急事件处置报告

长亭应急事件处置报告完整记录事件处置过程与具体应对操作，包括问题表现、深层原因、处置流程与手段、处置结果等，帮助评估事件影响，并对事件中暴露出的安全隐患提供针对性的修复建议，提高企业的事件应对能力。

长亭应急响应服务优势

快速响应，高效处理

基于一线积累的攻防经验和对企业网络环境的长期钻研，长亭应急响应服务保证20分钟内响应，100%有效处理结果，支持7X24小时现场或远程服务。

涵盖全周期，提升风险应对能力

从事前准备、检测、到事中处理、再到事后追踪与加固，长亭的解决方案涵盖了生命周期中的全部环节，让企业应急响应体系建设变得省心省力。

定制化方案，应对复杂事件

随着网络环境和业务形态日渐复杂，不同行业、不同类型的企业机构，甚至同一企业的不同业务系统都具备差异化的安全特征和需求。长亭安全服务团队凭借精湛的技术、认真谨慎的态度，为客户定制真正高效的解决方案，已妥善处置了系列复杂的安全事件。

- 成功案例

事件	某企业业务系统订单泄露，竞争对手获取后恶意争抢客户。
处置结果	• 根据日志溯源，分析得出泄露原因，同时发现了其它潜在的信息泄露点； • 修复安全漏洞，并给出了系统化的加固建议。

事件	某企业Linux主机感染远控木马，向外发送大量DDoS流量。
处置结果	• 清理木马，恢复业务； • 回溯入侵点，找到了未修复的漏洞； • 分析木马行为和攻击目的，区分批量扫描行为和APT行为。

事件	某企业高管遭到钓鱼攻击，高权限账号密码泄露。
处置结果	• 立即修改所有关联密码，阻止进一步恶意行为； • 分析钓鱼技术和攻击目的； • 评估事件影响。

附录：长亭安全服务团队比赛获奖

2017

07月
受邀在Black Hat发表演讲《一石三鸟击溃全线浏览器》

03月
Pwn2Own世界黑客大赛 全球第三名

2016

10月
GeekPwn安全极客嘉年华 中国第一：破解PS4（4.01系统）

08月
DEFCON CTF全球总决赛 第二名
XPwn智能硬件破解大赛 最高奖金团队
公安部网络攻防比武 冠军

07月
CFF网络安全攻防大赛 冠军

05月
GeekPwn澳门站 一等奖
中国网络安全技术对抗赛 一等奖

04月
第三届4.29首都网络安全日网络安全技术大赛 一等奖

2015

12月
第三届通信网络安全知识技能竞赛年度总决赛 一等奖

10月
GeekPwn安全极客嘉年华 一等奖

08月
受邀在Black Hat展示新型SQL注入防御技术

05月
中国网络安全技术对抗赛 二等奖
腾讯安全应急响应中心“最具价值安全问题”之一

04月
第二届4.29首都网络安全日网络安全技术大赛 一等奖

2014

12月
“湖湘杯”全国网络信息安全公开赛 三等奖

10月
首届阿里巴巴安全技术竞赛 第一名

08月
第二届360杯全国大学生信息安全技术大赛决赛
优秀团队奖、优秀个人

05月
第二届360杯全国大学生信息安全技术大赛 团体一等奖

03月
上海交通大学第一届信息安全技术挑战赛0CTF 一等奖


卡亭科技
CHAITIN