

安全值守服务

白皮书

**文档版本：V2.0**

**发布日期：2024-01-10**

**保密级别：受控**

版权声明

本文中出现的任何文字描述、文字格式、插图、照片、方法等内容，除另有特别注明，版权均属杭州安恒信息技术股份有限公司（简称“安恒信息”）所有，受到有关产权及版权法保护。任何个人、机构未经安恒信息明确做出书面授权许可，不得为任何目的以任何方式或手段（包括电子、机械、复印、录音或其他形式）对本文档的任何部分进行复制、存储、引入检索系统或者传播。经授权使用本文中内容的单位或个人，应在授权范围内使用，并注明“来源：安恒信息”。违反上述声明者，安恒信息保留追究其法律责任的权利。除杭州安恒信息技术股份有限公司的商标外，本手册中出现的其他商标、产品标识及商品名称，由各自权利人拥有。

**文档信息**

|  |  |  |  |
| --- | --- | --- | --- |
| **服务名称** | 安全值守服务 | **保密级别** | 受控 |
| **作者** | WH4488 | **服务经理** |  |

**修订记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **修订版本** | **修订日期** | **修改记录** | **修改人** | **批准人** |
| V1.0 | 2020-10-28 | 初次发布 | 2422 | 2422 |
| V1.1 | 2021-02-23 | 修改文档格式 | AH7151 | 2422 |
| V1.2 | 2021-06-01 | 修改第五章内容 | AH7151 | 2422 |
| V1.3 | 2022-01-18 | 内容优化 | AH3818 | 2422 |
| V2.0 | 2024-1-10 | 内容优化 | WH4488 |  |

**目 录**

[1 概述 2](#_Toc32598)

[1.1 背景 2](#_Toc15691)

[1.2 基本概念 2](#_Toc23824)

[1.3 服务目的 2](#_Toc31681)

[1.4 服务优势 3](#_Toc17636)

[1.5 服务必要性 3](#_Toc23624)

[1.5.1 提升安全防护能力 4](#_Toc22114)

[1.5.2 提升安全运维能力 4](#_Toc7477)

[1.5.3 保障业务连续性 5](#_Toc1928)

[1.6 客户收益 5](#_Toc12703)

[1.6.1 专业级企业服务 5](#_Toc18392)

[1.6.2 弹性全天候安全值守 5](#_Toc6304)

[1.6.3 提升形象，提高知名度 6](#_Toc14625)

[2 服务说明 1](#_Toc30589)

[2.1 服务范围 1](#_Toc4991)

[2.2 服务特点 1](#_Toc22054)

[2.3 服务内容 2](#_Toc13915)

[2.3.1 重保前 2](#_Toc6323)

[2.3.2 重保中 7](#_Toc13939)

[2.3.3 重保后 9](#_Toc26056)

[2.4 服务流程 9](#_Toc31035)

[2.5 服务报告 9](#_Toc26879)

[3 服务实施标准和原则 11](#_Toc12299)

[3.1 政策文件或标准 11](#_Toc6607)

[3.2 服务实施原则 12](#_Toc23032)

[4 涉及工具与产品 14](#_Toc12941)

[5 为什么选择安恒信息 18](#_Toc26961)

[5.1 综合技术实力和服务经验 18](#_Toc8302)

[5.2 国内顶级安全服务资质 18](#_Toc21005)

[5.3 丰富的安全服务经验 19](#_Toc15549)

[5.4 专业的安全服务团队 22](#_Toc12469)

[5.5 安恒优势 22](#_Toc24739)

# 概述

## 背景

当前国际形势复杂，因种族、宗教、领土等问题引起的地区冲突此起彼伏，各种反动势力极有可能会在一些重大活动举办期间通过各种方式进行破坏和干扰大会的正常进行。其中就包括针对各级政务机构的业务系统和网站进行的各种网络攻击等行为，因此，在重大活动举办期间的信息安全保障工作比任何时候都显得尤为重要和急迫。

## 基本概念

安全值守服务是在重大活动举办前、举办中、举办后，根据客户需求和法律法规，提供举办前的安全自查、安全运维，举办中的日志分析、安全值守、应急响应等，以及举办后的复盘总结等，帮助客户从技术、管理和人员三个方面建立和完善信息安全保障体系，增强信息安全防护能力、隐患检测能力、应急响应能力、系统恢复能力，保障网络和信息系统安全、可靠、稳定运行，为客户提供安全、快速有效的安全服务，最大限度地降低客户重大会议及召开期间信息安全事故发生的可能性。

## 服务目的

全面保障重要时期，客户信息系统有效平稳运行，业务正常开展。

安全值守服务的范围：门户网站、信息系统、内外部网络、云计算中心、办公场所、客户需要防御的保障目标。

## 服务优势

安恒信息参与多年重大活动安保，具备丰富的对抗国际性攻击者经验，参与重大活动安保情况如下：

* 2016年G20等。
* 2017年一带一路、两会、国际刑警论坛、十九大等。
* 2018年两会、山东上合峰会、中非论坛等。
* 2019年建国70周年、篮球世界杯、两会、一带一路、亚洲文明对话、世界园艺博览会等。

同时，安恒信息自主研发多款安全产品，贯穿重要时期网络安保前、中、后阶段，产品名称如下：

* 明鉴Web应用弱点扫描器。
* 明鉴远程安全评估系统。
* 明御Web应用防火墙。
* 明御APT攻击预警平台。
* [玄武盾云防护](https://www.dbappsecurity.com.cn/show-58-16-1.html)。
* 明御主机安全及管理系统。
* 明鉴网络安全事件应急处置工具箱。
* …

## 服务必要性

政府和重要单位、媒体、重大活动的官方网站，不仅承载着向公众和国内外发布准确信息的重任，更是国家形象的一张名片。这些信息资产不仅代表着政府和组织的形象，也反映了相关单位的信息化水平和信息安全防护能力。

近年来，在重大活动举办期间，如奥运会、世界杯等，举办国和举办组织的官方网站等信息资产突发网络安全事件屡见不鲜，带来了不少的负面影响。这些事件不仅影响了官方网站的正常运行，还可能导致信息的泄露和篡改，进一步损害了公众的利益和国家的形象。

因此，在重要时期保证该类信息资产安全的重要性不言而喻。为了实现这一目标，我们需要采取一系列措施。首先，政府和组织需要加强对信息资产的监管和管理，建立完善的安全管理制度和体系，确保信息资产的安全性和可靠性。其次，我们需要加强技术防御，采用先进的加密技术和防火墙技术等手段，防止黑客入侵和恶意攻击。此外，我们还需要加强人员培训和教育，提高相关人员的安全意识和技能水平，避免因人为因素导致的安全问题。

政府和重要单位、媒体、重大活动的官方网站等信息资产是国家形象的重要代表，其安全问题直接关系到国家的形象和利益。因此，我们必须高度重视信息资产的安全问题，采取多种措施保障其安全运行，以更好地展示国家的信息化水平和信息安全防护能力。

### 提升安全防护能力

安恒信息安全专家可在重大活动举办前期开展安全检查工作，尽可能多的发现高风险、大问题，全面提升安全对抗能力，极大降低安全事件发现的几率。

### 提升安全运维能力

安恒信息拥有专业的安全运维团队，能够根据客户的需求提供7\*24小时的安全专家运维支撑服务。无论是在日常的运维过程中，还是在应对突发事件时，安恒信息的安全专家都能够迅速响应，确保客户网络的安全稳定运行。

在服务过程中，安恒信息的安全专家会密切关注客户网络的安全状况，及时发现并解决潜在的安全问题。针对后台大量的日志记录进行深入的分析和提炼，提取出安全预警、安全漏洞和攻击态势等信息。这些信息对于客户来说具有重要的参考价值，能够帮助他们及时了解网络的安全状况，采取相应的措施进行防范和应对。

通过深入的分析和提炼，为客户提供全面的网络安全保障，确保客户网络的安全稳定运行。

### 保障业务连续性

安恒信息安全专家基于前期的安全检查与协助加固，配合安恒信息全套安全防护设备，可对客户重要信息资产进行全方位的安全防护和安全监控，能有效保障重要信息资产的业务连续性，降低了基于各种攻击造成的安全事件导致的服务中断概率，有效提高重要信息资产可用性。

## 客户收益

### 专业级企业服务

安恒信息派遣具有丰富安全保障能力、攻防能力突出的专家支持；将遵循标准化流程、可控化操作、专业性处置提供服务。

### 弹性全天候安全值守

安恒信息可根据客户需求推出多种值守方案，包括7\*24值守、7\*8值守、5\*8值守、电话远程值守等

多模式的安全预警机制与应急响应机制，提供应急响应和运维支撑，对突发的安全事件快速发现，快速处置，全方位保障用户的重要信息资产。

### 提升形象，提高知名度

安恒信息具备多年国家级网络安全保障经验，在重保时期协助客户进行网络安全保障工作，确保客户重要信息资产在重保时期平稳运行。

# 服务说明

## 服务范围

* 资产梳理：本次重要时期保障核心资产为起始点，涉及相关的内外网资产。
* 脆弱性检查：基于本次重要时期保障的核心资产所在的网络结构、安全设备、服务器、应用系统。
* 渗透测试：前期进行资产梳理出的内外网资产（服务器、网络设备、安全设备、应用系统）。
* 安全整改方案：本次检测、测试中发现的所有安全问题，均提供整改方案。
* 应急预案：基于常见重要时期易发生的安全事件，制定应急预案。
* 应急演练：基于常见重要时期易发生的安全事件，开展应急演练工作。
* 安全培训：针对安全事件处置、发现、内部上报流程，开展的相关安全培训。
* 安全巡检安全值守：前期进行资产梳理的内外网资产（服务器、网络设备、安全设备、应用系统）及本次核心保障系统。
* 应急响应：针对所防护的核心系统及相关内外网资产，在出现安全事件后第一时间进行处置。

## 服务特点

* 任务重：重要时期保障涉及网络安全多个方便，且时间跨度长。
* 要求高：网络无边界化的挑战，网络安全工作万无一失的要求，响应及时要求。
* 影响大：大型活动影响大，安全事件在重要时期保障中会尤为放大。
* 专业强：重要时期保障技术要求高，专业要求精。

## 服务内容

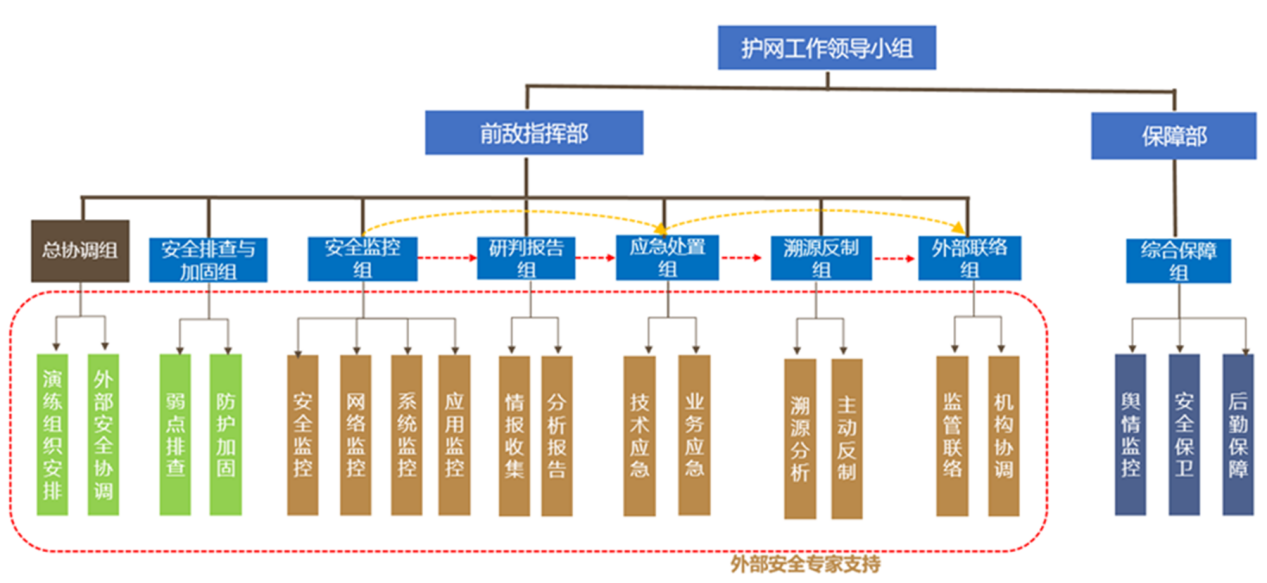
### 重保前

#### 重保团队建设

在重保活动开始前，安恒信息将根据客户的实际情况，量身定制专业的重保安全团队组建方案。该方案将覆盖团队建设的各个方面，确保团队具备高效、专业的安全保障能力。我们还将提供全面的培训计划，以提高团队成员的技能水平，并建立清晰的责任划分和沟通机制，确保团队的高效运行。通过这些努力，我们将为客户的安全保障提供强有力的支持。

在团队建设方面，我们将根据客户的业务需求和安全风险，精心挑选具备不同技能和经验的成员。团队成员不仅需要具备扎实的网络安全知识和技能，还需要具备良好的沟通协作能力，以便更好地与客户合作，共同应对各种安全挑战。

为了确保团队的高效运行，我们将制定清晰的责任划分和沟通机制。团队成员将明确各自的职责范围和工作重点，并建立有效的信息共享和协作机制。



图：重保团队组织架构示例

#### 资产梳理

对服务范围内信息系统的物理资产、系统资产、数据资产以及网络结构等进行了解并分析，并输出《重要时期保障业务系统和资产列表》。具体内容如下：

* 物理资产：了解客户信息系统中各种设备（包括路由器、交换机、服务器以及相关的安全设备等）的名称、型号、编号、管理地址、IP配置情况、物理位置、接线情况以及策略配置等信息。
* 系统资产：了解客户信息系统中的各种操作系统、数据库系统、办公自动化系统的名称、版本号、系统结构、存储格式、系统更新情况、系统防护情况以及系统支持的应用情况等。
* 数据资产：梳理客户信息系统中的重要信息，了解重要信息传输、存储的方式以及其他对重要信息的防护措施等。
* 网络结构：了解客户信息系统的网络结构，安全域的划分情况、划分依据以及边界的控制情况，网络接入方式、网络用户数量等。
* 应用系统：了解在客户信息系统中运行的各种应用系统的名称、版本号、功能以及与其他应用的关联情况和应用可支持的系统、数据库、中间件等情况。

#### 互联网暴露面检测

通过用户调研和信息收集的方式确定用户资产范围，结合人员丰富经验、标准化流程、强大自主研发工具，采用网络扫描、网络空间雷达、搜索引擎等多种探测技术，对用户暴露在互联网上的网站、信息系统、主机/服务器、安全设备、网络设备等信息资产进行主动发现。

#### 脆弱性检查

根据《重要时期保障业务系统和资产列表》，对用户信息系统相关的网络结构、设备配置和主机配置等进行检查。涉及网络结构、安全设备、服务器、应用系统脆弱性检查。

#### 渗透测试

在客户的授权与监督下，由专业安全工程师模拟黑客使用的漏洞发现技术和攻击手段，对重要的网络、应用系统、主机等安全性进行深入探测，发现其脆弱性。帮助客户更直接的了解所面临的安全问题，并及时进行修复。

#### 安全架构梳理与差距分析

网络架构分析是通过对用户评估范围内信息系统的网络拓扑及网络层面细节架构的评估，主要从以下几个方面进行分析：

* 网络建设的规范性：网络安全规划、设备命名规范性、网络架构安全性；
* 网络的可靠性：网络设备和链路冗余、设备选型及可扩展性；
* 网络边界安全：网络设备的ACL、防火墙、隔离网闸、物理隔离、VLAN（二层ACL）等；
* 网络协议分析：路由、交换、组播 、IGMP、CGMP、IPv4、IPv6等协议；
* 网络流量分析：带宽流量分析、异常流量分析、QOS配置分析、抗拒绝服务能力；
* 网络通信安全：通信监控、通信加密、VPN分析等；
* 设备自身安全：SNMP、口令、设备版本、系统漏洞、服务、端口等；
* 网络安全管理：网管系统、客户端远程登陆协议、日志审计、设备身份验证等。

#### 制定安全整改方案

根据脆弱性检查和渗透测试结果，针对其中较严重的安全隐患，结合重大活动的信息安全保障目标，为用户制定有针对性的安全整改方案，以消除或减少脆弱性，降低安全风险，安全整改方案主要包括以下内容：

1. 安全加固：对重大活动期间要重点保障的业务系统相关的网络设备、安全设备、操作系统、数据库以及中间件等对象的安全策略进行调整，方案中将针对不同加固对象设计不同的加固策略和方法，提高被加固对象自身的安全防护能力。

2. 安全集成：对于部分安全问题采用部署安全产品的方式进行解决，方案中将针对技术措施、产品选型和部署进行详细设计。

#### 制定应急预案

应急预案是针对可能发生的安全事件，为应急准备、事件报告、事件处理、灾难恢复的各个方面，预先制定的科学有效的行动规范和工作流程。在发生信息安全事件时，能够及时开展有序和有效的应急响应工作。

应急预案内容将包含制定相应应急响应组织、预防预警机制、事件定义分类、应急响应程序、事件上报处理机制、后期处理机制等内容。具体将分为综合预案、专题预案以及特定预案。

* 综合预案是面向整体的、针对信息安全事件的综合性应急预案。这种应急预案着重阐述基本原则、应急组织结构、部门职责、应急行动的总体思路、应急救援活动的组织协调等。综合预案是该预案管辖范围内所有专题预案、特定系统预案的指导性文件。
* 专题预案是针对某种具体的、特定类型的安全事件的应急响应而制定的，例如黑客攻击，蠕虫爆发等。专题预案是在参考综合预案的基础上，充分考虑特定威胁的特点，对应急的形势、组织机构、应急流程等进行更具体的阐述，具有较强的针对性。专题预案应与综合预案的精神保持一致。
* 特定系统预案是以某个需要保护的特定系统、特定设施为具体目标而制定和实施的应急预案。特定系统应急预案是在参考综合预案的基础上，针对某一具体系统的特殊威胁及周边环境进行详细分析，对应急响应中的各个方面做出具体、周密而细致的安排，因而特定系统预案具有更强的针对性和对现场救援活动的指导性。特定系统预案应与综合预案的精神保持一致。

#### 组织应急演练

安恒信息将协助客户制定应急预案演练工作方案，并模拟在本单位网络及重要设备出现故障等紧急情况下，依据前期制定的应急预案进行处理，其中包括事件的发现、上报、处理等环节。通过演练，使相关方熟悉应急处理流程，提高对安全事件的响应能力；同时验证预案的正确性和适用性，进行总结分析，并根据需要对应急预案进行修订。

#### 专题安全培训

针对用户在重大活动期间的信息安全组织结构、岗位职责、安全事件发现和上报机制以及处理流程等内容，为客户量身定制符合客户特点的安全培训内容。

### 重保中

#### 现场安全值守

通过现场值守人员对网络、主机、应用、数据库及其他设备运行状况进行监测，随时监控系统“健康”状态，如果发现问题及时与用户进行沟通，并提出解决方案，得到用户确认后对出现的问题进行解决，做到及时、准确保证无差错。

#### 定期安全巡检

根据用户在重大活动需要重点保护的资产规模及其面临的风险程度，安恒信息指派1-2人定期前往用户现场进行安全巡检，及时发现信息系统中存在的安全隐患并进行改进。

安全巡检主要内容如下：

* 服务器巡检：对服务器的CPU使用率、内存使用率、硬盘使用率等情况，以及运行进程、后台服务、日志、中间件和数据库运行的安全状态等进行检查；并重点对操作系统、数据库的安全策略进行检查，及时发现存在的安全隐患或问题，并进行上报和处理；
* 网络设备巡检：对网络设备的CPU使用率、内存使用率、硬盘使用率、接口和连接情况进行检查；并重点对安全策略进行检查，及时发现存在的安全隐患或问题，并进行上报和处理；
* 安全设备巡检：对安全设备的CPU使用率、内存使用率、硬盘使用率、接口情况和连接情况等进行检查，重点针对安全策略进行检查，及时发现存在的隐患或问题，并进行上报和处理；
* 病毒查杀：对防病毒服务器在防范区域、查杀病毒的准确性/实效性、防病毒代码更新频率、防病毒预警响应方面进行检查。

#### 网站实时监控

通过网站远程监控平台和人工分析相结合的方式，实时监测客户网站安全状况，主动发现网站存在的漏洞，在发现问题后及时采取修补措施，最大程度降低影响和减少损失。

通过网站实时监控服务，对目标站点进行不间断的页面爬取、分析、匹配，为政务机构门户网站提供远程安全监测、安全检查和实时告警服务，保证政务机构门户网站在重大活动期间的运行安全性和内容完整性。

网站实时监控服务主要内容如下：

1. 多维度、高频率、全方位洞察站点群的各项风险隐患，可对目标站点进行高频率的风险监测，一旦发生高危安全事件，及时告警，第一时间帮助客户降低风险；

2. 远程透明监测，无需改变现有网站结构，只要对系统简单配置，就可对用户网站远程监测，无需部署任何代理设备。

#### 快速应急响应

为帮助客户进一步提升应对突发信息安全事件的能力，安恒信息在提供现场安全值守服务的基础上，还建立了一支组织严密、技术过硬、响应及时的应急安全专家队伍，同时还与国家和北京市信息安全机构建立紧密联动机制，具有强大的安全专家资源队伍，能在出现紧急情况、发生安全事件时，及时到达现场，进行有效的应急处理，最大限度地减少损失和降低影响。

#### 威胁情报赋能

为进一步让安全设备应对最新安全威胁，重保期间安恒信息云端威胁情报中心对全球重要产品、软件、系统的安全威胁资讯实时跟踪，收集、验证、转化为最新安全威胁情报，赋能给客户部署的安全设备，帮助客户掌握最新安全态势与热点技术，提前布置针对性措施。

### 重保后

#### 重保复盘总结

在重保时期保障结束后，安恒信息将整合服务过程中的现场保障数据、云端防护数据、安全事件数据等，结合客户实际需求，梳理出工作过程亮点及重大成就，并输出总结报告。

同时，根据重保期间的防护数据和安全事件处理等内容，对防护体系、处理流程和应急预案进行优化。

## 服务流程

安恒信息针对本次客户现场及核心保障系统进行内外网资产梳理，针对所梳理出来的结果进行脆弱性检查与渗透测试工作，并在测试完毕后根据实际情况提供安全整改建议。在本次服务期间可以协商应急预案、应急演练、安全培训的时间并开展。

在重要时期开始之时定期开展安全巡检与实时监控工作，确保信息系统平稳运行。出现问题时第一时间开展应急响应处置工作，降低风险。

## 服务报告

* 《现场安全值守日报/巡检/监控报告》
* 《重要时期保障总结报告》
* 《应急响应处置报告》

# 服务实施标准和原则

## 政策文件或标准

* 《中华人民共和国网络安全法》
* 《网络安全等级保护2.0》
* 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）
* 《信息安全技术 网络安全等级保护安全设计要求》（GB/T 25070-2019）
* 《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）
* 《中华人民共和国密码法》
* 《中华人民共和国突发事件应对法》
* 《国家网络安全事件应急预案》
* 《国家突发公共事件总体应急预案》
* 《计算机病毒防治管理办法》
* 《信息技术 安全技术 信息与通信技术灾难恢复服务指南》（ISO/IEC 24762:2008）
* 《信息系统灾难恢复规范》（GB/T 20988-2007）
* 《信息技术 安全技术 信息安全管理体系要求》（GB/T 22080- 2016）
* 《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2019）
* 《信息安全技术 信息安全应急响应计划规范》（GB/T 24363-2009）
* 《信息安全技术 网络安全事件分类分级指南》（GB/Z 20986- 2023）

## 服务实施原则

安全值守服务实施将满足以下原则：

* 符合性原则

符合中办发[2003]27号文指出的积极防御、综合防范的方针和等级保护的原则；

* 标准性原则

服务方案的设计与实施应依据国内或国际的相关标准进行；

* 规范性原则

服务厂商工作中的过程和文档，具有很好的规范性，便于项目的跟踪和控制；

* 整体性原则

服务方案的范围和内容应当整体全面，包括安全涉及的各个层面（应用、系统、网络、管理制度、人员等），避免由于遗漏造成未来的安全隐患；

* 可控性原则

实施方法和过程需要在双方认同（认可）的范围之内，项目进度要严格按照项目工作计划执行，保证客户对于评估工作的可控性；

* 最小影响原则

安全评估、渗透测试和安全整改工作应尽可能小的影响系统和网络的正常运行，不能对现有网络的运行和业务的正常运行产生明显影响；

* 保密原则

对项目实施中产生的数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害客户的行为，否则追究乙方的责任。

# 涉及工具与产品

* 明鉴Web应用弱点扫描器

明鉴Web应用漏洞扫描系统（简称“MatriXay”）是杭州安恒信息技术股份有限公司在深入分析研究B/S典型应用架构中常见安全漏洞以及流行的攻击技术基础上，研制开发的一款Web应用安全专用评估工具。它能够对Web应用的资产进行识别分类以及对Web应用进行深度弱点探测。通过漏洞产生的原理和渗透测试的方法，快速分析出被测目标所开放的端口服务和对应的协议信息，发现资产暴露面。漏洞库覆盖国内外常见CMS、中间件、操作系统等严重漏洞，帮助用户全面分析Web应用网络环境中存在的安全弱点。

* 明鉴远程安全评估系统

明鉴远程安全评估系统严格按照计算机信息系统安全的国家标准、相关行业标准设计、编写、制造。明鉴远程安全评估系统可以对不同操作系统下的计算机(在可扫描IP范围内)进行漏洞检测。主要用于分析和指出有关网络的安全漏洞及被测系统的薄弱环节,给出详细的检测报告,并针对检测到的网络安全隐患给出相应的修补措施和安全建议。

* 明御Web应用防火墙；

明御®Web应用防火墙是一款专注为网站、APP等Web应用提供安全防护的专业应用安全防护产品。能够对网站及APP业务流量进行多维度、深层次的安全检测和防护。系统内置五大安全引擎（包括语义分析引擎、机器学习引擎、威胁情报引擎、行为分析引擎、基础特征引擎），可通过主动防护与被动安全相结合的方式识别可疑、已知、未知安全威胁，有效保障网站及APP业务安全、可靠运行。

* 明御APT攻击预警平台；

明御APT攻击预警平台基于丰富的特征库、全面的检测策略、精准的深度分析模型、高效的沙箱动态分析，结合智能机器学习和云端威胁情报协同，能实时发现用户网络中的各种已知威胁和未知威胁，检测能力可完整覆盖APT攻击链，支持包含各类恶意代码攻击、远程控制、WEB攻击、邮件攻击、漏洞利用、隧道通信等在内的二十余种攻击类型检测，帮助用户发现APT武器库指纹、异常加密流量、无文件攻击、防溯源C&C攻击、0day攻击等高级威胁，并基于可视化技术态势呈现网内威胁，提供完整的数据包存储和回溯分析取证能力，帮助用户实时预警网络攻击事件，提升网络攻击感知能力，助力高级威胁溯源分析，满足等保合规建设，为用户提供更全面的安全保障。

* 玄武盾云监测

玄武盾云监测服务依托于云端分布式的监测引擎和专业的安全运营团队，通过SaaS化的方式为用户提供即开即用的网站安全监测服务，为用户实时准确的监测网站漏洞、安全事件、敏感内容、可用性等多个维度的信息，并提供相应的安全告警，辅助用户发展网站和业务系统存在的安全风险。

* 玄武盾云防护

玄武盾基于云和威胁情报能力，提供零部署零运维云防护服务，分钟级接入，完成防通报、防黑、防泄露、防CC等安全防护。玄武盾遍布全国50个防护节点，确保不断网不变慢，是国内首家符合等保三级要求的云防护平台，自发布以来先后为G20、世界互联网大会、一带一路、上合峰会等大会官网提供安全保障，并为多个部委级用户提供了安全防护服务，政府行业市场占有率第一。

* 明御终端安全及防病毒系统

明御终端安全及防病毒系统（以下简称EDR）是一款集成了丰富的系统防护与加固、网络防护与加固等功能的主机安全产品。EDR具备业界独有的高级入侵威胁模块，专门应对攻防对抗场景，通过自主研发的文件诱饵引擎，有着业界领先的勒索专防专杀能力；通过内核级东西向流量隔离技术，实现网络隔离与防护；拥有补丁修复、外设管控、文件审计、违规外联检 测与阻断等主机安全能力。

* 明鉴网络安全事件应急处置工具箱

应急工具箱主要面向政府、公安机关以及企事业单位。在重要门户网站、重要信息系统遭受攻击的情况下，应急工具箱利用技术手段帮助政府、公安机关以及企事业单位对网络攻击事件进行溯源、取证、后门清除并快速进行系统恢复。最大程度上维护单位的形象，最大程度上减少政府或企事业单位的损失。

* AiLPHA高级威胁检测与分析系统

AiLPHA高级威胁检测与分析系统是一种跨多个安全层收集并自动关联信息以实现快速威胁检测的方法。它可以监视企业网络中不同来源或位置的威胁。通过全面的整体检测和响应策略消除了安全孤岛。它收集信息并匹配许多安全层(包括为端点、服务器、电子邮件、云和工作负载配置的安全层)上的深度活动数据的关系。可以对各种数据进行自动分析，以更快地检测到威胁，并使安全分析人员有足够的时间进行彻底的调查。

* AiLPHA大数据智能安全平台

AiLPHA安全分析与管理平台采用业界领先的大数据分析技术架构，结合专业的安全经验，依托雄厚的研发实力，兼顾未来业务的发展，以“数据驱动安全分析，构建智能自适应安全运营中心”为产品理念，为企业用户提供全局安全态势感知能力，为业务不间断稳定运行提供安全保障，为用户提供信息系统安全决策支撑。

* 明鉴®迷网系统

明鉴®迷网系统（以下简称“迷网”）是安恒信息根据多年在安全领域的攻防经验，打造的一款应对攻防实战场景的安全产品。迷网基于网络欺骗和主动防御理论，通过在真实业务网络中部署各种高交互、高仿真蜜罐、蜜饵，形成沉浸式诱捕蜜网，混淆攻击视听，增加攻击代价，进行溯源反制，达到延缓攻击进程，保护用户资产的目的。

* ……

# 为什么选择安恒信息

## 综合技术实力和服务经验

安恒公司是国家级的核心网络安全保障单位，拥有一支超过数百人的国家级网络安全保障实战团队，具备一流的网络与信息安全技术能力和丰富安全攻防经验。安恒信息作为重要支撑单位，为北京“奥运会”、“国庆60周年”庆典、上海“世博会”、广州“亚运会”、深圳“大运会”、“十八大”会议、“亚信”峰会、“APEC”会议、“世界反法西斯胜利70周年”大阅兵、贵阳“数博会”、“G20”峰会、“B20”峰会、连续三届“世界互联网大会”、首届“丝绸之路”（敦煌）国际文化博览会、首届“世界物联网博览会”、“博鳌”亚洲论坛、2017年“两会”、厦门“金砖”、“一带一路”国际合作高峰论坛、香港回归20周年、第十三届“全运会”等重大活动提供全方位网络安全保障支持，并荣获多封感谢信。以先进的理念和专业的服务，15年重大活动和赛事的安保实践，并先后签约2020第六届亚沙滩运动会、2021年成都大运会，以先进的理念和专业的服务获得各盛事主办方和监管机构的一致好评。

安恒信息作为OWASP最佳技术支撑单位，核心项目成员为《OWASP测试指南》提供了重要的参考数据，并主导了该指南的审核、修订和推广、实践工作。安恒信息可以有效针对 Web 应用程序进行测试，更好地规避WEB应用风险。

## 国内顶级安全服务资质

* 中国信息安全测评中心认证通过的信息安全服务资质（安全工程类三级）——国内最高级。
* 中国网络安全审查技术与认证中心认证通过的信息¥安全服务资质(一级应急处理服务资质) ——国内最高级。
* 中国网络安全审查技术与认证中心认证通过的信息安全服务资质(一级风险评估服务资质) ——国内最高级。
* 中国通信企业协会认证通过的通信网络安全服务资质（二级风险评估）。
* 国家计算机网络应急技术处理协调中心省级网络安全应急服务支撑单位资质。
* 国家网络与信息安全信息通报中心技术支持单位。
* 国家信息安全漏洞库（CNNVD）一级技术支撑单位。
* 国家ISO9001认证资质。
* ISO27001认证资质。
* ISO20000认证资质。

## 丰富的安全服务经验

* 在2008年北京奥运会期间，作为北京奥组委安全产品和服务提供商，安恒信息被奥组委授予“奥运信息安全保障杰出贡献奖”。
* 在建国60周年网站安全大检查中，安恒信息作为工信部唯一技术合作伙伴发挥了重大作用。
* 2009年安恒信息荣获浙江省网络与信息安全通报中心技术支持合作先进单位称号。
* 2009年，建国 60 周年全国网站安全大检查技术支撑单位。
* 2010年，安恒信息成为上海世博会安全产品和服务提供商，全力保障上海世博会期间政府信息系统安全。
* 2010年，广州亚运会安全产品和服务提供商。
* 2011年，安恒信息作为深圳大运会安全产品和服务的提供商，为深圳大运会信息安全保驾护航。
* 2012年，安恒信息作为“十八大”安全保障单位，为“十八大”顺利召开做好网络安全保卫工作。
* 2013年，安恒信息作为技术支持单位，为全国网站安全大检查提供技术保障。
* 2014年，安恒信息作为“两会”安全保障单位，为大会的顺利召开做好网络安全保卫工作。
* 2014年，安全信息作为“APEC”安全保障单位，为大会的顺利召开做好网络安全保卫工作。
* 2015年，安恒信息入围全球网络安全企业500强榜单，国际知名度不断提高。
* 2015年，安恒信息作为“第二届世界互联网大会”保障单位，为大会的顺利召开做好网络安全保卫工作。
* 2016年，安恒信息作为“杭州G20峰会”核心安保单位，为峰会的顺利召开做好网络安全保卫工作。
* 2016年，安恒信息作为“第三届世界互联网大会”主要网络安保单位，再次为大会的顺利召开做好网络安全保卫工作。
* 2016年，世界物联网博览会核心网络安保单位。
* 2017年，“一带一路”国际合作高峰论坛网络安全保障单位。
* 2017年，安恒信息作为“金砖五国会议”核心安保单位，为峰会的顺利召开做好网络安全保卫工作。
* 2018年，天网工程、平安城市、雪亮工程等信息化项目展开。
* 2018年，安恒信息作为“上合峰会”核心安保单位，为峰会的顺利召开做好网络安全保卫工作。
* 2019年，与厦门市人民政府签署战略合作协议。
* 2019年，安恒信息作为“武汉军运会”核心安保单位，为运动会的顺利召开做好网络安全保卫工作。
* 2020年，成为“2020年第六届亚洲沙滩运动会网络安全技术服务支持单位” 。
* 2020年，成为成都大运会网络信息安全类官方独家供应商。
* 2020年，安恒信息签约2022年杭州第19届亚运会，安恒信息成为2022年杭州亚运会官方网络安全服务合作伙伴，为2022年杭州亚运会网络安全保驾护航。
* 2022年，成为成都世界乒乓球团体锦标赛网络安全类官方供应商

## 专业的安全服务团队

* 公司创始人范渊先生为国际知名的信息安全专家，对信息安全技术研究极具创新能力。
* 国内最大最专业的安全服务队伍，90%以上为本科学历。
* 拥有多位国际注册信息系统安全认证专家（CISSP）、国际信息系统审计师（CISA）、信息安全注册工程师（CISP）、信息安全管理体系（ISO27001）主任审核员及高级项目经理（PMP）。

## 安恒优势

* 2016年成立“网络安保特勤部”专职负责网络安保(目前唯一)
* 自2015年以来，大型活动安保参与率近100%(国内唯一为境外提供安保服务)。
* 网络安保支撑类型全面，涵盖政治、经济、体育、主题类等。
* 业务熟练，依据经验能快速有效开展针对性工作。
* 网络安全规划全面，提供专业安保问题咨询及做法惯例咨询。
* 具备多部门协同的威胁情报猎取及处置能力。
* 专业网络技术队伍(运维、防御、取证、对抗等)。
* 成熟的网络安全技术方案，避免“走弯路”。
* 满足保密要求(支撑人员背审，核心人员政审均通过)。
* 产品线及服务全，能够随时提供必要的技术手段、工具。

杭州安恒信息技术股份有限公司

使用过程中如遇任何问题，请致电服务热线400-6059-110。

**联系信息**

地址：浙江省杭州市滨江区西兴街道联慧街188号安恒大厦

邮编：310052

电话：0571-88380999

传真：0571-28863666

官网：<http://www.dbappsecurity.com.cn>

邮箱：[400-doc@dbappsecurity.com.cn](mailto:400-doc@dbappsecurity.com.cn)

**商标声明**

是杭州安恒信息技术股份有限公司的商标，在本手册中出现的其他商标、产品名称、服务名称以及公司名称，由其各自的所有人拥有。

**免责声明**

本文中出现的任何文字描述、文字格式、插图、照片、方法等内容，除另有特别注明，版权均属杭州安恒信息技术股份有限公司所有，受到有关产权及版权法保护。任何个人、机构未经安恒信息明确做出书面授权许可，不得为任何目的以任何方式或手段（包括电子、机械、复印、录音或其他形式）对本文档的任何部分进行复制、存储、引入检索系统或者传播。

经授权使用本文中内容的单位或个人，应在授权范围内使用，并注明“来源：安恒信息”。违反上述声明者，安恒信息保留追究其法律责任的权利。

**版本所有©杭州安恒信息技术股份有限公司。保留一切所有权利。**

非经杭州安恒信息技术股份有限公司书面同意，任何单位和个人不得擅自摘抄、复制本手册内容的部分或全部，并不得以任何形式传播。