安恒信息
DAS-security 安全中国

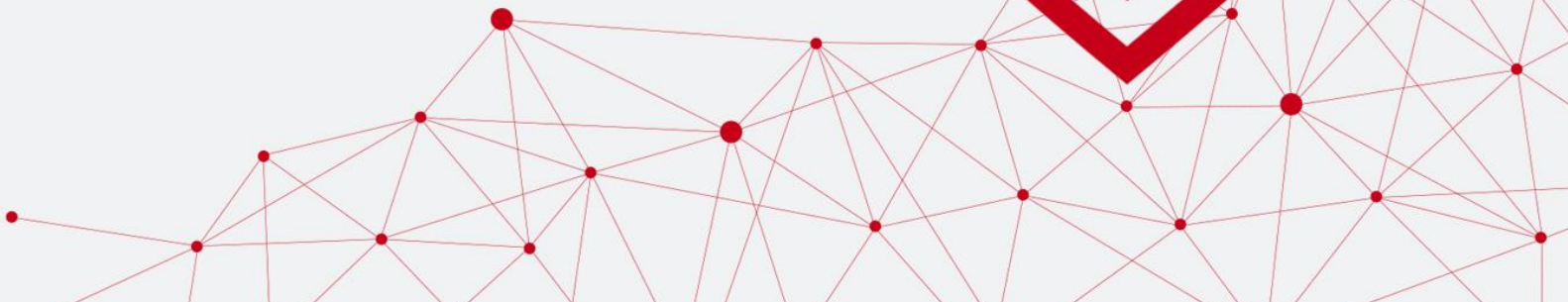
# 防数据勒索

# 解决方案

**文档版本：V1.0.1**

**发布日期：2021-04-14**

www.dbappsecurity.com.cn



## 版权声明



## 适用性声明

本报告仅适用于杭州安恒信息技术股份有限公司（以下简称“安恒信息”）在客户现场进行数据勒索防护项目时的状况。

# 目 录

# 1. 概述

## 1.1 背景

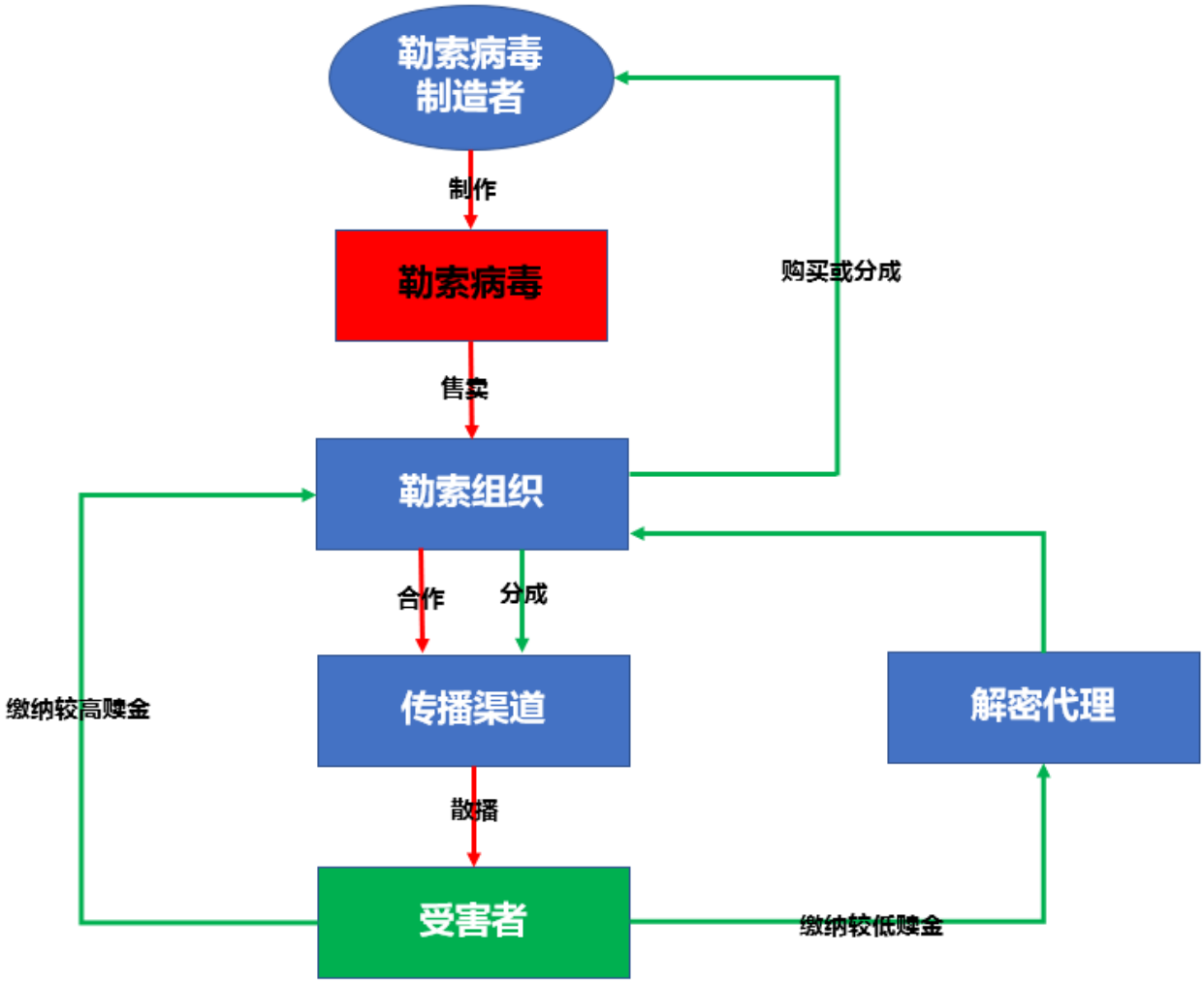
伴随着传统行业逐渐数字化、网络化、智能化、逐步拥抱产业互联网化的大浪潮中，暴露出一系列网络安全问题。勒索病毒也趁机发难，疯狂敛财，影响日渐扩大。全球范围内的交通、能源、医疗等社会基础服务设施，成为勒索病毒攻击的目标。2021 年 1 月，国内外新增勒索病毒 Vovalex、Babuk、YourData、Summon、HelpYou、Encrp、Judge、Epsilon、WormLocker、Namaste、 Povllsomware 等勒索病毒家族，其中 YourData、HelpYou、 Summon 已经在国内流行，Babuk 家族针对企业进行攻击并采用双重勒索模式——在加密受害者数据之前，会先窃取用户数据，若用户不支付赎金，黑客将会在暗网公布从受害者设备中窃取到的数据。

2020 年底，电子巨头富士康在在墨西哥的一家工厂遭遇数据勒索攻击，攻击者声称，加密了超过 1,000 台服务器，窃取了 100 GB 的未加密文件，并删除了 20-30 TB 的备份，勒索者还在数据泄露站点上发布部分数据。数据勒索者索要 1804.0955 BTC 赎金，约为 35,000,000 美元（约合 2 亿人民币），一度造成这家工厂停工减产。

## 1.2 数据勒索攻击链

通过追踪 Ryuk 勒索软件组织的比特币账户，截至 2021 年 1 月，Ryuk 勒索软件的受害者至少支付 1.5 亿美元的赎金，这还只是众多数据勒索组织中的一个。2013 年 CryptoLocker，CTBLocker 开启勒索病毒大量以蠕虫或病毒方式传播，到 2021 年，数据勒索发展成为从业人员数以万记，涉及金额达到百亿美金规模的黑色产业。深入分析数据勒索产业的分工情况和攻击路径，能帮助我们最大程度的降低数据勒索带来的损失。

数据勒索产业链一般可以分为五种角色，其分工如下：




- 勒索病毒制造者：负责勒索病毒编写制作，与安全软件免杀对抗。通过在“暗网”或其它地下平台贩卖病毒代码，接受病毒定制，或出售病毒生成器的方式，与勒索者进行合作拿取分成。
- 勒索组织：从病毒作者手中拿到定制版本勒索病毒或勒索病毒原程序，通过自定义病毒勒索信息后得到自己的专属病毒，与勒索病毒作者进行收入分成。

- 传播渠道:帮助勒索者传播勒索病毒,最为熟悉的则是僵尸网络,例 Necurs、Gamut,全球有 97%的钓鱼邮件由该两个僵尸网络发送。

- 解密代理:向受害者假称自己能够解密各勒索病毒加密的文件,并且是勒索者提出赎金的 50%甚至更低,但实际上与勒索者进行合作,在其间赚取差价,同事也解决部分勒索病毒失联无法解密问题。

再以富士康被勒索事件为例,勒索组织并不是仅仅将数据加密,而是渗透、窃取、泄露、破坏、加密相结合,由此可见,在实施企业数据勒索的过程中,勒索组织又有进一步的精细化分工。在对企业进行数据勒索时,勒索病毒反而成为最后实现勒索的工具,数据勒索过程与 APT 攻击有相似的攻击链,描述如下:

- 入侵内网:通过网站挂马、垃圾邮件、病毒、木马、社会工程等方式,甚至是 APT 攻击,勒索组织进入用户内网;

- 内网踩点:获取一部分资源的控制权限后,勒索组织会建立隐蔽通信通道进行远程控制,也为窃取数据建立数据传输通道;勒索组织会通过扫描探查、数据监听、记录分析等方式,了解用户内网的资源分布情况,到薄弱环节和有漏洞的系统,重点探查数据库服务器、备份服务器的数据较为集中的系统。

- 横向渗透:通过系统漏洞、口令攻击等方式获取更多系统的控制权,尤其是获取数据库权限,为窃取数据和实施勒索做准备;

- 窃取数据:将数据库中存储的数据复制或者外发到黑客控制的服务器,分析实施勒索的定价,勒索不成也可以卖到暗网上。

- 删除备份：数据备份是能否成功勒索的最大障碍，勒索者会找到数据备份系统，并删除备份数据，破坏备份机制，防止受害者因为可以利用备份恢复数据，不付赎金造成勒索失败；

- 加密数据：对数据进行加密，造成业务系统崩溃或者数据库宕机，一般选在晚上和周末，等用户发现系统异常时，已经来不及做响应；

- 实施勒索：从多个维度进行勒索，包括数据加密造成的生产停顿或者经营困难，威胁将下载的数据对媒体公开、出售给竞争对手、对企业高管进行人身攻击，逼迫受害人就范。如果勒索不成，被下载的数据会被在暗网出售，弥补勒索组织的损失。

即便支付了赎金还有可能由于技术原因数据恢复失败，泄露的数据也可能重新包装后进入暗网。

## 1.3 数据勒索危害

一旦企业被勒索组织成功入侵，可能造成的损害如下：

- 破坏生产：数据被加密，往往意味着业务系统崩溃、数据库宕机，如果被加密的数据包括生产控制系统、流程系统等，或者用户数据、订单数据等，则会造成企业生产的混乱，轻则减产，重则停工停产，销售停顿，会造成巨大的经济损失。

- 经营困难：如果被加密的数据涉及企业的经营数据，则可能造成经营决策的混乱，如无法进行政策的财务审计，无法进行市场分析、用户画像等经营决策，打乱企业发展步伐，造成长期的经济损失。

- 数据泄露：勒索组织在加密数据之前，会尝试窃取高价值的数据，这往往包含商业机密和客户信息，会使企业面临巨大的商业挑战和法律风险。
- 人身攻击：勒索组织往往根据窃取的企业高管个人信息，对高管甚至家人进行骚扰、造谣，胁迫企业交付赎金。
- 持续攻击：勒索病毒清楚不彻底，可能在信息系统中留有隐蔽通道，勒索组织会持续对企业进行攻击和袭扰，还有企业不胜其扰，定期向勒索组织缴纳赎金买平安，数据勒索从“拦路抢劫”模式，进入“收保护费”模式。
- 商誉损失：数据勒索会造成客户对企业的信任危机，企业的商业信誉会降低，面临的法律风险会升高，经营管理能力面临质疑，面临巨大的无形资产损失风险。

## 1.4 建设目标

通过对数据勒索产业和攻击方式的分析，我们发现，将数据勒索当成病毒进行防护的思路已经无法实现企业级的数据勒索防护，需要按照纵深防护思路，建立针对勒索攻击链的防护体系。

# 2. 防数据勒索方案框架说明

## 2.1 建设数据勒索的纵深防护链

针对企业的数据勒索按照：入侵内网→内网踩点→横向渗透→窃取数据→删除备份→加密数据→实施勒索的攻击链进行，安恒防数据勒索解决方案针对其攻击链的每个步骤，建立涵盖事前检测预防、事中监测防御、事后恢复溯源的纵深防御体系，将数据勒索风险降到最低。

## 2.2 防数据勒索框架


## 2.3 事前检测预防

勒索组织在散播勒索病毒过程中，一旦发现感染病毒的是企业终端时，会暂时隐藏下来，为进一步入侵内网进行准备。针对勒索病毒入侵和扩散的特点，进行事前检测预防，能够降

低数据勒索入侵和扩散的风险。事前检测预防包含的主要措施如下：

- 主机安全及管理（EDR）：在终端和服务器上部署 EDR，可以提供综合的勒索病毒和木马防护能力。EDR 通过多种杀毒引擎配合，能防止大部分已知的病毒、木马和勒索病毒侵入系统；一旦系统被侵入，EDR 也能够通过外联检测发现勒索病毒和木马建立的隐蔽通道，从而定位病毒和木马；通过诱饵引擎，诱使勒索病毒主动加密文件，从而隔离病毒；EDR 通过端口监控和漏洞管理，也能防止病毒横向扩散和蔓延。
- 防垃圾邮件：垃圾邮件是勒索病毒和木马传播的主要渠道之一，防垃圾邮件系统通过检查邮件源拦截常见僵尸网络发送的钓鱼邮件和垃圾邮件，防垃圾邮件系统通过对邮件主题、正文和附件的检查，可以拦截带毒邮件和钓鱼邮件。
- 关键数据识别：对于企业来讲，对数据的保护切忌“胡子眉毛一把抓”，应首先进行关键数据识别，关键数据应包括：对于有法律合规风险的数据，主要是个人信息；影响生产经营的数据，如：订单数据、财务数据、核心知识产权、生产控制数据等。对关键数据加强监控，可以更好的监控数据窃取和破坏行为，为关键数据的备份策略设置更高的 RPO 和 RTO，能更好的保证数据完整性。
- 安全评估检查：勒索组织会利用企业信息系统存在安全漏洞、弱口令、高危端口、安全基线缺失等安全问题进行网站挂马、入侵内网、横向攻击等操作，知道获取数据库控制权进行数据勒索。为了阻断勒索攻击链，需要通过弱口令检查、高危端口扫描、红队内网评估、数据库安全漏洞扫描、数据库基线检查等一些列安全评估检查尽可能的全面、快速、深入检测挖掘现有系统存在安全弱点，提出有效的安全整改建议，通过补短板来降低数据勒索风险。

- 安全意识：2020 年 RSA 大会上的主题是“ Human Element （人为因素)”，在面对日益增长、复杂多样的网络攻击下，“人”是最强大的防护武器；在全球数字化转型过程中，从数据开发、保护、治理到利用，“人”发挥着巨大创造力与安全能力。众所众知，“人”是整个安全链条中最薄弱的一环，人永远是数据安全的核心要素，勒索病毒传播很大程度上利用了人性的弱点。开展数据勒索专题安全意识培训，钓鱼邮件测试等，通过实际案例和安全事件、安全邮件意识测试，将数据勒索安全事件与员工自身利益、企业利益相结合，了解到数据勒索的危害，让员工重视数据安全，让员工保持警惕。通过详细讲解数据勒索的传播方式和技术手段，避免企业内部人员安全意识不足，实现企业的员工不再因为打开一封精心构造的带毒邮件或点击一个经过伪装的挂马页面，就让勒索病毒进入内网，让员工合规的行为准则成为解决数据防勒索的一环。员工重视数据安全，明白在防数据勒索中的责任，企业员工更新规范自己的日常办公行为，从源意识层面降低数据勒索的安全风险，能让防数据勒索工作事半功倍。从以人为本的角度出发，平衡 IT 框架、对风险管理策略进行汇总、降低新威胁带来的隐患、以及建立一个安全为中心的高效 IT 文化也是极为重要的。
- 应急演练：一旦数据勒索事件真的发生，做出正确响应的速度越快，遭受的损失越小，企业应制定针对数据勒索事件的应急响应流程作为预防措施，并开展模拟数据勒索的应急演练工作，既能检验应急响应流程的合理性，又能让各协同相关部门和人员熟悉面对数据勒索时的应对方法，还能更好的优化落实物质条件、人力和技术支撑等保障措施。避免真实事件发生时处理过程中出现混乱、无序状况，减少处理过程中错误的发生，从而避免不必要的损失。

## 2.4 事中监测防御

多年病毒与防病毒竞争中已经证明，现有的防病毒机制并不能对勒索病毒起到完全的防护作用，在勒索组织已经成功侵入内网后，为实现数据勒索的目标，会有建立隐秘通道、网络扫描、权限提升、数据探查、数据下载等一系列行为，针对这些行为进行监测，发现后阻断攻击链都能够成功阻止数据勒索。事中监测防御可以采取的安全措施包括：

- 数据访问审计：勒索组织会尝试连接数据库，尝试通过弱口令或者系统漏洞获取数据库的访问权限；一旦获取权限成功，勒索组织会尝试下载数据库里的数据，从中选取高价值数据发送至外网服务器，用于后续的勒索或者贩卖。数据访问审计通过分析数据库的访问流量，能够对数据库口令猜测、漏洞攻击和数据大量下载、高危操作的异常行为进行监控。并且，数据访问审计能够将数据访问行为发送给用户行为分析系统，由用户行为分析系统进行长周期分析，让勒索行为现出原形。

- 数据库蜜罐：针对数据勒索搭建的数据库蜜罐系统，将自身伪装成 CRM 数据库、HR 数据库、ERP 数据库等高价值目标，诱使勒索组织进行攻击。一方面，所有对数据库蜜罐系统的访问都是高危访问，这能够让我们快速准确的定位攻击来源，另一方面，数据库蜜罐系统还能分散勒索组织的精力，为及时做出响应争取更多时间。

- APT 攻击预警：勒索组织在内网踩点和横向渗透阶段，都会尝试进行网络扫描和服务扫描，会利用服务漏洞进行权限获取和提升，会通过建立隐秘通道与勒索组织服务器建立控制连接，并传输窃取到的数据，APT 攻击预警系统采用安全沙箱、DGA 等技术能够发现以上的行为异常，定位勒索渗透的主机，阻断勒索攻击链。

- 用户行为分析（UEBA）：基于大数据平台，运用 AI 技术和机器学习，对采集到的数据访问行为、告警信息，终端日志、应用日志、运维日志进行大数据分析，基于长周期访问行为建模，能够发现隐蔽更深的数据勒索，是将整个防勒索系统连接起来的智慧中枢。

- 数据分析处置：由于攻击者技术水平的不断提升，攻击手段已经由简单的口令拆解、窃听向着更为复杂的 0day 漏洞利用和 APT 攻击演变，越来越多黑客开始利用数据勒索病毒牟利，数据勒索的攻击手段与传统黑客攻击融合，会结合多种攻击手段发起攻击，攻击的方法也越来越隐蔽。企业迫切需要建立基于大数据的分析平台对海量数据进行高速、准确的提取和分析，从大量事件中发现攻击线索，再结合威胁情报和专家分析，对数据勒索和攻击行为进行长效监测。安全运维人员在对安全事件研判分析确认安全事件之后，流转至安全事件处置响应模块进行安全事件信息联动处置。对已经确认的攻击，可以通过人工的处置流程剧本编排，使响应流程尽量实现标准化、智能化，从而做到快速正确的响应和处置。

## 2.5 事后恢复溯源

如果之前所有的防御和监测措施都没有见效，那么数据备份与恢复是企业保护数据的最后一道防线，勒索组织也会千方百计的破坏企业的数据备份机制后，再实施加密勒索。所以，企业需要建立足够应对勒索组织攻击的完善的数据备份与恢复机制，另一方面，还需要具有溯源能力，发现勒索组织攻击链条，将整个系统恢复至安全状态，防止二次侵害发生。事后恢复溯源所采取的安全措施包括：

- 数据备份与恢复：大量的案例告诉我们，建立安全有效的数据备份与恢复机制，是对抗数据勒索，并将损失降到最低的有效措施。金融机构和大型企业很少被勒索成功，往往是因为在数据被加密后，成功对数据进行恢复，虽然，也会造成一定损失，却不需要支付赎金。

- 备份物理保护：勒索组织也意识到，破坏备份机制和备份数据，是勒索成功的必要条件，因此，再实施数据加密前，会想尽一切办法找到备份数据，然后将其破坏。对备份数据持续进行完整性检测，并通过物理隔离手段保证备份数据完整性，成为数据防勒索的最后一道防线。

- 应急响应：如果发现企业内部发生了勒索病毒事件，通过电话 365*24 小时咨询服务商安全专家，安全专家立刻进行应急响应，其目的是最快速恢复系统的保密性、完整性和可用性，阻止和降低数据勒索造成损失。在完成现场工作后，将对事件情况出具专业完整的应急响应报告，专业的应急响应报告不但需要对事件的描述和判断，也会针对此类勒索数据事件给出专业的安全加固建议以及应急处置办法，防止类似的事件再次发生。应急响应人员还会固化证据，从中分析数据勒索的攻击链条，然后将整个系统恢复至安全状态，防止二次侵害发生。

- 谈判专家：谈判专家团队是对数据勒索产业充分了解，并对勒索链条中各环节角色的心理进行过充分的分析。当勒索事件发生时，一方面，谈判专家能够与勒索组织沟通，得到勒索的更多线索，如：数据泄露情况、勒索者对企业的了解程度、数据恢复的可能性等，便于企业进行研判；另一方面，谈判专家与勒索组织谈判，能够为应急响应

和处置争取时间，防止勒索组织采用极端破坏行为；最后，谈判专家可以降低勒索组织对收益的预期，在恢复数据时，降低企业的损失。

- 网络保险：购买数据安全的专项保险是将风险转嫁的一种方式，可以进一步降低数据勒索造成的损失。

# 3. 防数据勒索体系详细设计

## 3.1 事前检测预防

### 3.1.1 主机安全及管理系统（EDR）

明御主机安全及管理系统是一款集成了丰富的系统加固与防护、网络加固与防护等功能的主机安全产品，是防数据勒索的核心装备。其中集成业界独有的高级威胁模块，专门应对攻防对抗场景；通过自主研发的专利级文件诱饵引擎，具有业界领先的勒索病毒专防专杀能力；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。目前产品广泛应用在服务器、桌面 PC、虚拟机、工控系统、国产操作系统、容器安全、攻防对抗等各个场景。系统核心功能包括：

#### 3.1.1.1 勒索病毒防护功能

明御主机安全及管理系统病毒查杀功能拥有丰富全面的平台支持：Windows + x86/x64、Linux + x86/x64、Linux + MIPS 32/64 + 大小字节序、Linux + ARM 32/64、Unix + PowerPC、国产操作系统（Linux 家族） + 国产 CPU（x86/MIPS）。

支持多种压缩包、自解压包、符合文档、媒体文件、加密脚本、电子邮件、邮箱文件、可提取文档中嵌入的其它资源，如：宏、脚本、可执行程序等。

丰富的脱壳能力，全面的模拟执行能力（反病毒虚拟机）。

可以通过开启勒索软件启动防护引擎，可以防御已知勒索病毒，在进程试图启动时进行阻断;并可以防御未知勒索病毒，在勒索进程试图加密时进行实时阻断;还可对未知勒索软件的大量文件操作行为进行监控。

#### 3.1.1.2 防止勒索病毒的 RDP 爆破

使用操作系统本身公开的安全登录插件机制实现此功能，相较于传统的读取系统日志判断的方法，插件防护不会遗漏掉任何登录数据，更加安全。

可对系统账户登录进行细粒度的精准访问控制，支持对访问来源（账户、地理位置、远程 IP 或域名、远程计算机名）、访问时间的配置，并能实时阻断非法登录。触发登录防护后，自动联动添加微隔离规则。

可周期性执行弱口令检测或立即执行一次检测，检测字典包括常见弱口令、同用户名的口令和空口令。

#### 3.1.1.3 防止勒索病毒进行端口扫描

在网络驱动中检查入站到本机的数据包，当某个 IP 在设置的时间周期内连接本地的不重复的端口数量达到一定次数时，将恶意探测 IP 锁定，防止其进一步获取终端敏感信息。可以查看并解除已临时锁定的 IP 清单。

#### 3.1.1.4 漏洞检测与补丁安装

采用漏洞库的方式进行检测，可精确快速根据不同的操作系统定位到未安装的补丁，依靠管理平台的推送功能，可将漏洞库文件推送到终端上安装最新补丁，免受黑客攻击。

即使终端无法连接互联网，也可依赖管理平台的离线补丁下载器，将补丁文件导入到管理平台，后续终端上即可正常下载安装补丁。

软件对操作系统进行全面漏洞扫描，并对漏洞补丁进行一键修复或单个修复。根据中心和端主机是否可访问互联网的不同情况，漏洞补丁的获取有以下几种情况：

只有中心可访问互联网：通过 admin 账户登录，中心去收集补丁后推送给端主机修复；

只有端可访问互联网：中心已下载过的补丁由中心推送给端主机修复，中心未下载过的由端主机下载进行修复；

中心和端都不可访问互联网：通过 admin 账户登录，离线上传补丁后，中心推送给端主机修复；

中心和端都可访问互联网：中心已下载过的补丁由中心推送给端主机修复，中心未下载过的由端主机下载进行修复，或选择(1)中的修复方式。

#### 3.1.1.5 系统进程守护

使用内核驱动技术，每当有进程启动时从操作系统内核中可以得到通知，获取到包括进程路径等一系列上下文信息后，可以根据用户设置的白名单直接拒绝或放行。支持仅记录模式、记录并阻断模式。

#### 3.1.1.6 防止黑客利用外网 web 应用漏洞进行攻击

使用 Web 容器的第三方安全插件机制实现，可在 Web 后台程序处理请求之前获取到所有的请求上下文信息提前过虑，对恶意请求及时拦截。

支持容器类型丰富：IIS6.0～IIS10.0、Apache2.2～Apache2.4、以及任何支持 Servlet 过滤模型的 java 类容器（Tomcat、Weblogic、Jboos、Jetty 等）。IIS 系列可支持插件的动态安装及卸载，不需要重启 Web 容器。

针对常见的 SQL 注入、XSS 跨站攻击进行防护；

可检测到各种主流扫描器行为，根据设置屏蔽对本站的扫描；

可防护低版本 Web 容器的文件名解析漏洞、畸形文件漏洞等；

针对集中爆发的 Web 应用程序漏洞（Struts 系列漏洞等）可及时更新策略达到免疫效果，自定义的网站漏洞防护，可对页面请求的所有字段进行过滤，并能支持对自定义的请求字段进行过滤（用户业务自定义字段）。

### 3.1.2 防垃圾邮件防火墙

垃圾邮件和钓鱼邮件是目前勒索软件传播的主要方式之一，攻击者以广撒网的方式大量传播垃圾邮件、钓鱼邮件，一旦收件人打开邮件附件或者点击邮件中的链接地址，勒索软件会以用户看不见的形式在后台静默安装，实施勒索。

防垃圾邮件网关提供强大、丰富的垃圾邮件及病毒防护功能，通过来源分析、关键词过滤、规则过滤等技术，有效拦截钓鱼邮件和垃圾邮件，从而保障邮件服务器不收垃圾邮件侵扰，可有效地抵御垃圾邮件及病毒袭击风险。

- 来源分析：防垃圾邮件网关主要通过对邮件的 IP 来源进行分析，来判断垃圾邮件的可能性。一般 IP 来源无法伪装，可根据垃圾邮件发送者 IP 的地理位置或者黑白名单分析来源是否真实，如果真实则通过，否则可能为可疑邮件。

- 关键词过滤：创建一些简单或复杂的与垃圾邮件关联的单词表来识别和处理垃圾邮件。比如某些关键词大量在垃圾邮件中出现，如一些病毒的邮件标题。这种方式比较

类似反病毒软件利用的病毒特征一样。是一种简单的内容过滤方式来处理垃圾邮件，基于一个庞大的过滤关键词列表来实现。

- 规则过滤：根据某些特征（比如单词、词组、位置、大小、附件等）来形成规则，通过这些规则来描述垃圾邮件，为了使得过滤器有效，需要对庞大的规则库进行日常维护。

- 病毒防护：采用防毒引擎进行严格病毒防护。不但可以防止各种病毒，还能够识别网络钓鱼邮件及部分间谍软件。同时也可以对压缩文件进行病毒检查。

### 3.1.3 关键数据识别

AiSort 数据安全分级与风险评估系统是一款集成数据资产发现、敏感数据识别、数据分类分级、数据资产管理等功能的数据安全专用产品。在关键数据识别中，AiSort 能完成如下工作：

- 数据资产自动发现：数据资产自动发现基于网络嗅探技术进行周期性探测，在指定 IP 地址范围内，通过端口扫描自动化发现网络环境中存在的数据库系统。通过扫描的方式可获取到数据库基本信息包括：数据源类型、主机 IP、端口、库名/实例名、版本号等信息。通过技术手段自动发现数据资产，动态形成数据资产地图，防止出现安全管理盲区。

- 敏感信息识别：在数据资产中精准区分敏感数据与非敏感数据，通过内置 AI 机器学习算法规则和内置行业法规标准，基于深度学习+条件随机场的命名实体识别模型，可以更准确、高效的识别，并可以进一步进行数据进行分类、分级。支持的敏感信息

包括个人信息,如：姓名、手机号、邮箱、地址、证件号等；支持的敏感数据包括业务信息，如：企业名称、纳税识别号、统一社会信用代码、银行账号、卡号等。通过识别敏感信息，对其进行重点监控和防护，防止勒索组织窃取数据用于售卖或以泄露数据威胁企业。通过敏感信息识别，确定需要重点防护的数据，对这些数据首先要制定数据备份与恢复策略，并实施数据备份，保证数据的完整性、可用性和机密性，同时，进行重点监控，能够尽早发现数据的窃取和破坏行为。

- 数据库账号梳理：支持对数据库账号状态及权限进行梳理评估，并且可对账号新增、权限变更及删除等变更情况进行分类展示，有效防止账号的违规授权和恶意提权。
- 数据资产目录：支持数据源，敏感数据，和所选定的分级标准多维度进行展示。支持分级概览，表列分布，级别分布等情况图标展示及详情展示，方便数据拥有者了解数据资产的分布情况。数据资产目录可与其他安全系统进行对接，如数据的细粒度访问控制，数据脱敏等，为数据安全建设提供进一步的支撑。

### 3.1.4 安全评估检查

在网络安全领域最长提到的说就是“木桶原理”，信息系统的安全状况，往往是由短板决定的。在事前防御阶段，安恒信息将以下技术手段进行全面安全评估检查，尽可能的全面、快速、深入检测挖掘现有信息系统存在安全脆弱点，分析面临的威胁，评价整体安全风险，提出有效的安全整改建议，自从而补齐安全中的短板，降低数据勒索风险。

#### 3.1.4.1 弱口令检查

安全服务人员将对企业的操作系统、网络设备、安全设备、业务系统等帐号进行弱口令

排查。弱口令通常有以下几种情况：用户名和密码是系统默认、空口令、口令长度过短、口令选择与本身特征相关等。系统、应用程序、数据库存在弱口令可以导致入侵者直接得到系统权限、修改盗取数据库中敏感数据、任意篡改页面等。为排查弱口令风险，安恒信息通过自动扫描+人工验证+调研三步走法，来为企业进行弱口令检查服务。

**■ 评估工具**

弱口令自动化检查主要使用安恒自主研发的“明鉴远程安全评估系统”，对操作系统、数据库、应用、中间件进行检查。设备通过旁路方式接入网络，无须改变网络架构，通过 IP 网络扫描的方式，实现对目标系统的安全漏洞和安全基线检查。

编制网络安全弱口令自查清单，针对操作系统、网络设备、安全设备、业务系统等帐号口令开展安全自查，检查是否存在弱口令、默认口令、常用短语等及时发现风险并处置。

### 3.1.4.2 高危端口扫描

针对企业信息系统资产 IP，安恒信息服务人员使用自主研发的扫描工具进行资产探测，结合客户提供的资产清单，尽可能发现完整的内网资产清单，并通过专业的端口扫描工具，对 IP 地址进行高端口扫描，统计出每个 IP 地址开放的端口、对应的服务，汇总成表格，然后与客户相关人员进行逐一确认，明确核心资产和边缘资产以及高危端口开放情况，据互联网资产探测结果，关闭不必要对互联网开放的服务和端口，如：文件打印共享服务（tcp:135/139/445），远程管理类（tcp:3389,22），数据库（tcp：3306/1433/1521）等，按“最小原则”，仅开放必要的服务和端口。

### 3.1.4.3 内网红队评估

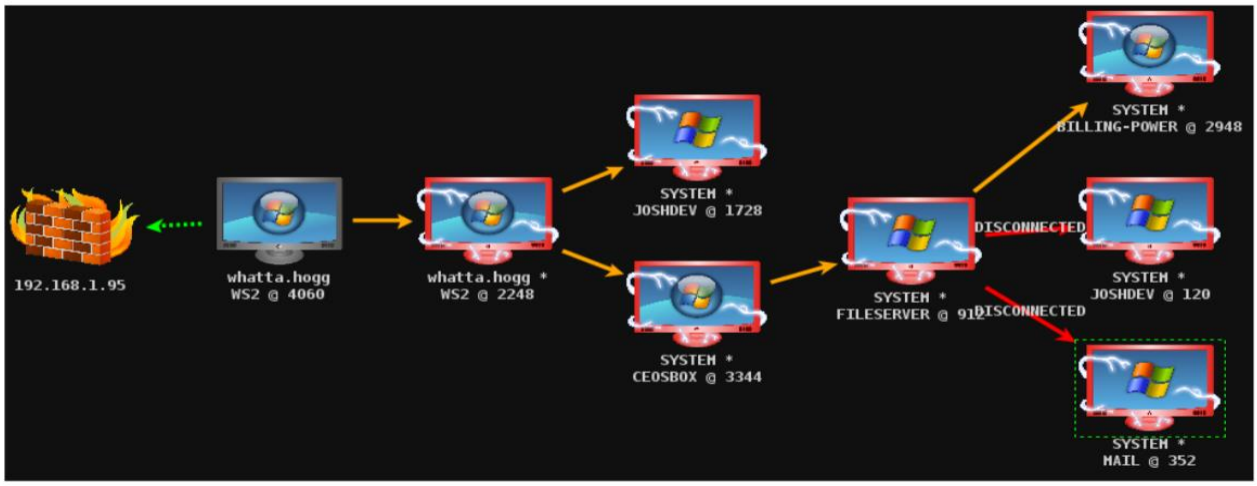
安恒信息内网红队评估针对企业的内网网络设备设置的访问控制策略、流量分析设备、终端 EDR（Endpoint Detection and Response：终端检测与响应）、内部系统漏洞进行测试，评估内网整体网络安全是否存在隐患。

在评估内网访问控制安全的环节中，红队人员会对内网跳板机进行权限提升、权限维持、凭证窃取、网络拓扑分析、内网横向，例如：操作系统账户密码、数据库账户密码、域环境下操作系统进程中的访问令牌等，后续进行内网的横向工作。

◆权限提升

获得操作系统一定权限后，红队将分析操作系统补丁情况、服务配置、寻找 DLL 劫持漏洞、利用系统特性等，使用提权载荷进行权限提升。

◆权限维持




获得高权限后，红队将使用 Cobaltstrike、Metasploit Framework、Empire 等开源渗透测试框架进行持久控制，期间对于控制程序的免杀环境而会采用 Shellcode 混淆、反射 DLL 注入、DLL 劫持、白利用

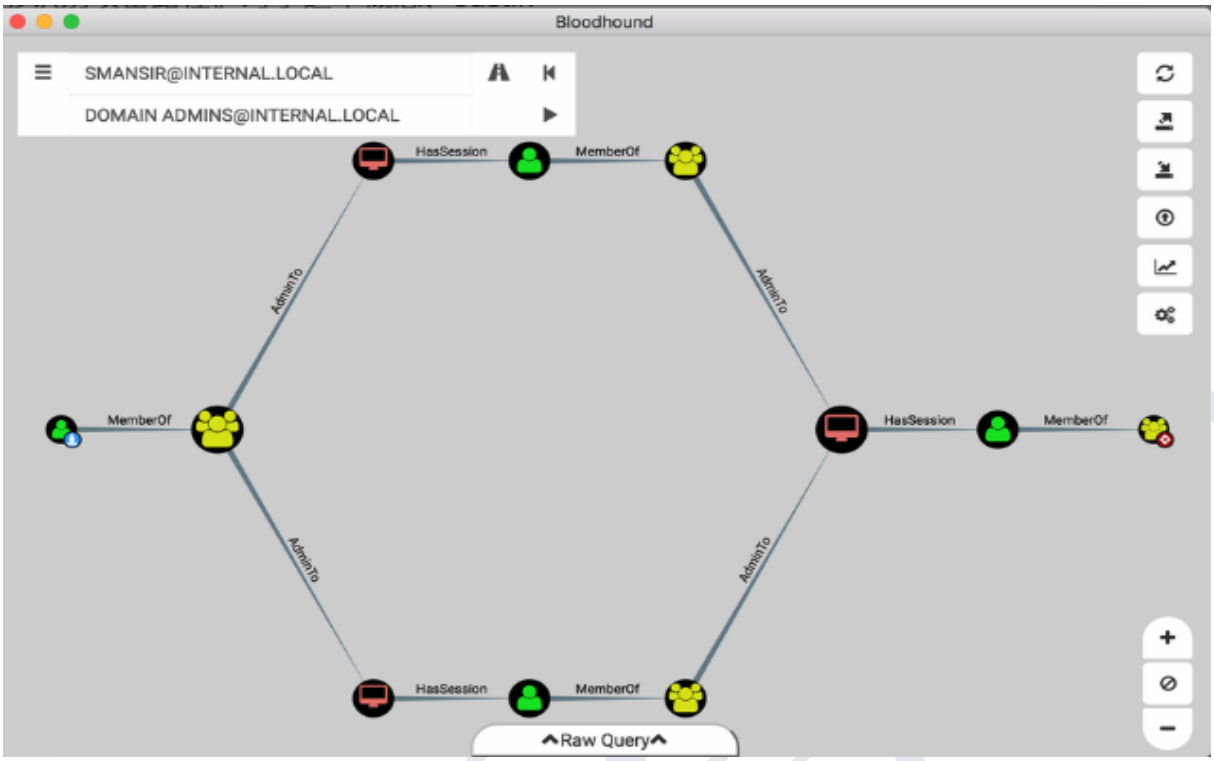
等 APT 常用技术建立 C2(Command And Control)尝试逃逸终端 EDR、反病毒软件、网络流量监控设备。

◆凭证窃取

- 凭证窃取的窃取对象主要为主机凭证、网络凭证、活动凭证、其他应用凭证：
- 主机凭证是针对操作系统的账户密码，红队将使用开源工具 Mimikatz 或导出注册表的方式提取 NT Hash、明文密码。
- 网络凭证主要是针对域环境下获取高权限后，使用已有的域账户伪造白银票据（Silver Tickets）、黄金票据（Golden Tickets）。
- 活动凭证主要是针对域环境下域用户登录服务器后创建了进程，红队在获取操作系统高权限的情况下，能够复制该进程的访问令牌，相应的也获得了域用户的权限。
- 其他应用凭证主要是针对系统上安装的服务软件的配置文件中保留的密码，如有：FtpServer、网站数据库配置文件、应用客户端配置文件等。

◆网络拓扑分析

网络拓扑分析主要工作是信息搜集，针对工作组、域环境下使用 Nmap 进行主机发现扫描、使用 Bloodhound 进行域环境拓扑分析，测绘出可到达目标的网络路径。




◆内网横向

红队使用后渗透框架将搜集到的口令与主机进行凭证枚举、Pass-The-Hash，同时根据内部应用开放的情况，尝试利用一些命令执行漏洞如：Struts2 反序列化、FastJson 反序列化、ms17-010 等漏洞，进行进一步的主机控制。

通过红队的内网安全评估，发现企业内网的脆弱性，并协助企业复盘整改，提升企业内网的安全行，加强内网数据安全的安全性，从而减少数据勒索事件的发生的可能性。

### 3.1.4.4 数据库安全漏洞扫描

安恒信息主要使用安恒自主研发的“明鉴远程安全评估系统”，从而得出数据库存在的安全漏洞及安全隐患。数据库系统安全检查主要包括：信息获取、版本识别、弱口令、缓冲区溢出、补丁安装、存储过程分析、数据库入侵痕迹扫描等；通过提前发现数据库安全漏洞并协助整改，降低数据库安全风险。

#### 3.1.4.5 数据库基线检查

安全服务人员将对业务系统涉及的数据库，如 MySql、Oracle、DB2、sql 等数据库系统进行安全配置缺陷的检查与评估。检测内容包括（但不限于）：身份认证方式、帐号安全设置、管理权限和角色设置、多余帐号和缺省口令检查、数据库目录和文件系统安全、监听器管理设置、日志及监控审计、数据库版本和补丁管理、数据库备份策略、硬件冗余情况等安全情况进行脆弱发现，并协助企业进行安全整改。

### 3.1.5 安全意识

#### 3.1.5.1 安全意识培训

开展安全意识培训是为了解决数据勒索人员被利用的问题，培训过程中通过大量典型的安全事件导入，反映当前安全形势的极端恶化，从感性认识层面对安全威胁给予直观、形象的描述，并形成一定的安全现象/知识冲击结果，分析、强调漠视信息安全的严重后果，以及安全威胁的发展趋势：速度更快、范围更广、影响更深刻。实际案例和安全事件，表述信息安全对于个人生活、工作、学习无处不在的事实，同时阐明安全问题并非孤立、遥远的技术，在此基础上按照一般的安全技术的划分深入浅出地描述信息安全所包含的各个领域，以及这些领域和日常工作、生活的密切联系，从而员工知道个人行为准则对数据安全的重要性。

课程还可以根据企业员工在信息化中的不同角色进行配置，下列是推荐的课程内容及其介绍。

| 课程编号 | 课程主题 | 课程内容 |
| --- | --- | --- |

| | | |
|---|---|---|
| DBS-C-010 | 安全意识培训 | 包含课程：<br>DBS-A-010（《信息安全事件和安全威胁》）<br>DBS-A-020（《日常安全和必备安全习惯》）<br>DBS-A-030（《信息安全基础》） |
| DBS-C-020 | 安全工程师培训 | 包含课程：<br>DBS-A-030（《信息安全基础》）<br>DBS-T-020（《常见操作系统安全》）<br>DBS-T-030（《系统检查和加固》）<br>DBS-T-040（《应急响应和入侵调查》）<br>DBS-T-050（《网络安全设备》）<br>DBS-T-080（《攻击目标信息采集与识别》）<br>DBS-T-090（《入侵防护技术》） |
| DBS-A-010 | 《信息安全事件和安全威胁》 | 通过大量典型的安全事件导入，反映当前安全形势的极端恶化，从感性认识层面对安全威胁给予直观、形象的描述，并形成一定的安全现象/知识冲击结果，分析、强调漠视信息安全的严重后果，以及安全威胁的发展趋势：速度更快、范围更广、影响更深刻。 |

| | | |
|---|---|---|
| DBS-A-020 | 《日常安全和必备安全习惯》 | 通过实际案例和安全事件，表述信息安全对于个人生活、工作、学习无处不在的事实，同时阐明安全问题并非孤立、遥远的技术，在此基础上按照一般的安全技术的划分深入浅出地描述信息安全所包含的各个领域，以及这些领域和日常工作、生活的密切联系，对常见客户端应用工具/系统的安全问题进行分析，采用实证方式阐明 OE、IE、Foxmail、MSN/QQ、P2P 工具等的安全设置，对 Windows 操作系统存在的安全问题进行叙述和演示。同时，就日益猖獗的病毒、木马等威胁进行必要的描述，并阐明具体的防范措施，最终协助建立起适合个人、企业的用户行为基准。 |
| DBS-A-030 | 《信息安全基础》 | 从 ISO 7498-2 模型出发，结合 CBK 领域、BS 7799 领域划分，对信息安全中涉及到的标准、协议、技术手段、工具/产品、过程方法等，通过对安全领域和知识的清晰划分和描述，最终能够形成一张信息安全的知识结构图。 |
| DBS-T-010 | 《常见操作系统安全》 | 从 Windows 以及 Unix 的安全结构入手，对 windows 安全子系统中的重要组件如 SAM、LSA、GINA 等进行详细分析，分别阐明帐户安全、文件系统安全、注册表安全，对于 Windows 的常见应用（如 IIS、Netbios、Terminal Server 等）的安全性加以分析。针对 Unix 系统，则对帐号安全、文件 |

| | | |
|---|---|---|
| | | 系统安全、常见应用安全的讨论，强调 Unix 系统本身安全配置的同时，还将重点描述 Unix 主要应用服务（Mail、HTTP 等）的安全问题。 |
| DBS-T-020 | 《系统检查和加固》 | 本讲通过对系统安全加固的流程进行介绍，说明安全加固工作的主要工作任务。完全参照实际的工作过程，通过大量的现场模拟环境的加固实践，针对不同操作系统（Windows、Linux、HP UX、IBM AIX、BSD、Cisco IOS 等）和相应应用系统（Web、Mail 等）描述其检查流程、入侵调查、加固方案和相应的 checklist。 |
| DBS-T-030 | 《应急响应和入侵调查》 | 本讲从将结合应急响应演练，通过多个应急响应经典案例，对应急响应预案等核心步骤进行清晰的分析和描述，并且对在多个系统上对入侵痕迹的调查，易消失证据的获取进行详解介绍和演示 |
| DBS-T-040 | 《攻击目标信息采集与识别》 | 在分析目标端网络数据采集方法的基础上，简明扼要地说明一些典型的工具应用，通过掌握目标端信息辨别的方法和原理，能够有效地进行 Footprinting 资料搜集、挖掘和准确的人工判断。 |

| | | |
|---|---|---|
| DBS-T-050 | 《入侵防护技术》 | 介绍一般的黑客攻击途径，着重描述当前流行的攻击技术和防御手段，从踩点扫描着手，重点分析网络嗅探、病毒与木马攻击、拒绝服务攻击、SQL Injection 原理、XSS 跨站脚本攻击等，并阐明相应的防御措施，通过一次完整、完美的黑客攻击过程的实践展示，首先对黑客攻击的一般步骤进行分析，阐明黑客攻防的基本思路，并按照步骤顺序对其中涉及到的工具、平台、弱点、手法进行叙述，对黑客的惯常思维方式进行归纳总结。 |

### 3.1.5.2 钓鱼邮件测试

为了更好提升企业员工个人安全意识、从源头降低数据勒索事件的发生概率，检验个人终端安全防护能力，强化个人数据以及内部数据的安全性，可以通过沟通全公司员工共同参与钓鱼邮件测试、共同提高个人安全意识能力认知。

安恒鱼叉钓鱼测试服务一般通过电子邮件进行，和传统撒网式钓鱼不同，鱼叉钓鱼针对公司内部的个人。

内容包括但不限于:

1.收集目标公司邮箱、组织架构等信息。

2. 收集个人信息，并精心构造准备好的文件或恶意链接发送给目标人员，一旦受害者打开文件或打开链接，

用户信息就可能被窃取，如果受害者计算机不幸被控制，公司重要资产将受到严重威胁。

钓鱼邮件测试: 基于钓鱼测试服务，通过定期发送钓鱼邮件的方式，提升员工识别钓鱼邮件能力;通过嵌入 式学习方式，推动企业强制性合规教育、防范商业邮件欺诈与勒索软件。 测试内容: 钓鱼测试-系统调试、模板定制、支持 SPF(发件人策略框架)检测、支持获取客户端外网 IP 地址、支持获 取客户端浏览器信息、木马远程控制。

最后输出钓鱼报告、行为矫正-强化钓鱼邮件网络安全、社会工程学等知识学习。 工作人员是业务开展的重要载体，人员数量众多，地点不集中。可以通过钓鱼测试一方面提升全体员工的安全意识水平，保障个人信息安全。另一方面构筑信息安全“人力防火墙”是具有重要意义的一项工作，需要倾注更为专业、有经验 的人力规划与开展钓鱼工作，将个人安全意识安全宣传工作落在实处，尽可能的扩大宣传范围，深化宣传效果， 最终构建信息安全管理文化，强化数据安全管理能力，提升信息安全保障水平。

### 3.1.6 应急演练

我公司安全咨询顾问将协助企业进行相应的数据勒索模拟演练，一方面使相关方熟悉应急响应流程，提高对安全事件的响应能力；另一方面验证预案正确性和适用性，进行总结分析，根据需要对应急预案进行修订。使得用户信息系统相关人员了解应急流程和自己的责任，在安全事件发生时，能够有条不紊地开展应急工作，最大程度降低安全事件带来的负面影响和损失。

开展应急演练是应急管理工作的重要内容，是检验应急预案实用性、应急机制科学性、应急体制合理性、应急程序的适用性的必要途径。我公司通过了解统计信息系统的服务质量和业务要求，确定应急恢复计划的范围与目标，指导企业设计完成应急演练计划，定期组织实施应急响应演练，以确定应急预案是否满足需要和达到设定的恢复目标。

应急演练将通过培训以及现场支持的方式采用桌面推演和实操演练相结合的方式展开，演练过程重点考察的方面主要包括：

- 信息系统的应急计划是否覆盖了保护对象的全部；
- 应急计划是否满足信息系统的保密性、可靠性和可用性的要求；
- 预防策略是否满足当灾难发生后信息系统的恢复响应速度要求和灾难恢复后数据的完整性要求；
- 预案的可实现性；
- 安全事件的响应方案的可操作性；
- 各类型各级别应急事件的响应操作规程、详细说明、操作步骤或方法等的指导意义及描述的准确程度；
- 事件的发现、上报、处理等环节。

## 3.2 事中监测防御

### 3.2.1 数据库审计

安恒明御数据库审计与风险控制系统是一款基于对数据库传输协议深度解析的基础上进行风险识别和告警通知的系统。只要将数据库访问的网络流量复制给数据库审计系统，就能分析出数据访问行为，所以，数据库审计是分析数据库勒索行为提供很好的分析工具和数据来源。

明御数据库审计与风险控制系统支持近 400 条内置风险识别的安全规则，安全规则分成

SQL 注入规则、漏洞攻击规则、账号安全规则、数据泄露规则和违规操作规则。系统具有对数据库访问行为进行实时审计、对数据库的恶意攻击、数据库违规访问等行为识别的能力。

系统核心功能包括：

#### 3.2.1.1 强大的审计能力

系统通过数据库协议解析的方式将访问数据库 报文中的信息格式化解析出来，针对不同的数据库需要使用不同的方式进行解析。系统支持审计目前主流的数据库系统，包括传统的数据库系统、大数据系统和 Web 系统等

#### 3.2.1.2 安全规则

安全规则库用来保存已发现了的不安全 SQL 的特征信息，明御数据库审计与风险控制系统支持通过对审计的 SQL 语句和安全规则进行匹配，判断 SQL 语句中是否包含可疑行为。根据不安全 SQL 的特征信息，将安全规则分成 SQL 注入攻击、漏洞攻击、账号安全、数据泄露和违规操作。

#### 3.2.1.3 告警日志

明御数据库审计与风险控制系统根据安全规则捕捉到异常访问时，会根据匹配的安全规则产生对应级别的告警信息，系统支持在页面查看告警日志的所有 SQL 语句的信息和告警等级，并可以根据时间、告警等级、规则名称等字段进行筛选。

#### 3.2.1.4 智能分析

明御数据库审计与风险控制系统的行为模型是通过 UEBA(用户实体行为分析)的理念分析数据库访问行为中可能存在的可疑行为。行为模型通过学习数据库服务器历史被访问轨迹，

来判断新访问行是否存在可能的风险。行为模型是通过配置学习维度，在对不在学习范围内的审计记录进行陌生告警。行为模型配置为可以分为应用 IP，学习维度，学习截止时间。其中学习维度可以分为客户端 IP、客户端主机名、数据库用户名、操作系统用户名、客户端工具名、数据库名、操作类型、资产 IP。

### 3.2.2 数据库蜜罐

明鉴迷网系统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，通过蜜罐、蜜饵构建沉浸式诱捕蜜网，混淆攻击视听，增加攻击代价，达到延缓攻击进程，进而保护用户资产的目的。

针对数据勒索迷网的核心能力主要体现在三个方面：

1)通过极低的硬件代价构建多个数据库蜜罐系统，将自身伪装成 CRM 数据库、HR 数据库、ERP 数据库等高价值目标，掩盖保护真实用户业务与数据，增大攻击的成本。

2)在部署数据库蜜罐系统的基础上，对仿真数据库蜜罐系统进行监控，任何对数据库蜜罐系统的访问都是高危访问，通过监控捕获攻击者的攻击行为、采集攻击者指纹、并分析其动作以感知其攻击意图，为反制、追溯提供数据支撑。

3)通过构建数据库蜜罐系统，混淆攻击者的攻击对象，有效防止攻击者快速找到目标对象，从而拖延其攻击节奏，为及时做出响应争取更多时间。

为进一步监控数据勒索和数据泄露行为，数据库蜜罐系统还可以在系统中构造多张诱饵表用于监控黑客对数据库渗透和攻击的情况，这些诱饵表正常的业务系统不会去使用。根据实际业务情况在诱饵表中灌入少量历史数据或者专门添加一些具有数据特征的伪数据，这些

数据正常情况下不会被当前的业务系统使用。一旦这些诱饵表被访问时，说明可能存在外部黑客渗透甚至恶意攻击的风险。对于诱饵对象的监控与告警，可以通过数据库审计设置场景化规则，并关联到需要被监控的诱饵对象，一旦发生对诱饵对象有任何操作时，如：select、update、delete 或者导出等时，数据库将产生高风险的告警。同时告警可设定邮件、短信、企业微信等实时告警方式，一旦触发相关诱饵表的操作行为，将及时对此告警行为进行风险告知，溯源到攻击者的账号信息，排查风险问题。

### 3.2.3 APT 攻击预警平台

安恒 APT 产品可以提供一套整体的覆盖多种区域的 APT 深度威胁分析方案，基于关键区域入口的旁路镜像流量分析，可以实现 WEB、邮件、文件三个维度多个层次的 APT 攻击检测，主要包含：WEB 层面的 APT 攻击检测（包含各种已知 WEB 攻击特征检测、WEBSHELL 检测、WEB 行为分析、异常访问、C&C IP/URL 检测等），邮件层面的 APT 攻击检测（包含 WEBMAIL 漏洞利用攻击检测、恶意邮件附件攻击检测、邮件头欺骗、发件人欺骗、邮件钓鱼、恶意链接等邮件社工行为检测等），文件层面的 APT 攻击检测（多引擎检测已知特征攻击、静态无签名 shellcode 检测、动态沙箱行为分析等），木马回连行为分析（包含 C&C IP/URL 自动学习提取、非法回连行为检测、恶意数据盗取检测等）。

APT 系统能够解析除了数据库访问协议外的几乎所有协议，能够为勒索组织进行内网踩点和横向渗透的过程中，发现建立的隐秘通道和渗透行为，并且，其分析出的访问内容，是对内外网攻击进行关联分析的重要数据来源，是应对数据勒索组织与黑客结合的有效措施。

系统核心功能包括：

### 3.2.3.1 深度协议解析

明御 APT 攻击预警平台可以对双向全流量进行深度解析，为发现流量中的恶意攻击提供了全面的检测和预警的能力。

明御 APT 攻击预警平台能够在网络中出现攻击时主动发现攻击，并进行预警。利用各种检测手段发现其中的恶意攻击及 0day 攻击。 目前支持解析的协议包括 HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、Mysql、MSSQL、DB2、Oracle 等，在拥有私钥证书的情况下，也支持对加密协议 HTTPS、SMTPS、POP3S、IMAPS 进行解析。

明御 APT 攻击预警平台能检测和预警一系列的攻击，无论是已知的或未知的，如：基于 web 的恶意攻击、基于文件的恶意攻击、基于特征的恶意攻击，并且能发现和定位僵尸主机、受控主机。

### 3.2.3.2 Web 攻击检测

WEB 经常使用一个大型网络的入口，而 WEB 应用种类非常多，存在大量的安全漏洞。所以通过 WEB 应用入侵到内网再进行渗透攻击在 APT 攻击中非常常见。

明御 APT 攻击预警平台通过对 Web 流量和应用进行深度检测，提供了全面的入侵防御能力。

其主要检测方式体现如下：

1) 常规检测

明御 APT 攻击预警平台通过解码所有进入的请求，检查请求是否合法或合乎规定。仅允许通过正确的格式或 RFC 遵从的请求，已知的恶意请求将被阻断。(例如：跨站点脚本攻击、

缓冲区溢出攻击、恶意浏览、SQL 注入攻击等。）解码所有进入的请求，检查请求是否合法或合乎规定。仅允许通过正确的格式或 RFC 遵从的请求。已知的恶意请求将被阻断。（例如：跨站点脚本攻击、缓冲区溢出攻击、恶意浏览、SQL 注入攻击等。）

2) 行为检测

对于普通的 WEB 攻击检测设备只是基于攻击特征的黑名单方式或白名单方式判断攻击，而大量的常规告警和随处可见的云联网扫描使真正的攻击淹没在海量的日志中，安全管理人员根本无法确定哪些才是真正的攻击告警。明御 APT 攻击预警平台特有的高级行为检测功能，可以识别用户的行为特点，区别机器行为和人工渗透行为。能够分析出普通的扫描器扫描、大量数据获取（拖库行为）、手工渗透等大量的基于行为特征分析。

3) 文件检测

明御 APT 攻击预警平台会对通过 WEB 上传和下载的文件进行检测，检测的内容包括：WEBSHELL 检测、 可执行文件检测、非执行文件检测（office、pdf、flash 等大量可能被利用直接攻击客户端的文件）。

#### 3.2.3.3 邮件攻击检测

在 APT 攻击中，使用邮件发起针对个人的攻击是最常见的手段之一。攻击者通常使用对个人发起攻击方法包括：

1)利用钓鱼邮件诱骗账户密码等信息；

2)发送挂马页面诱骗点击后控制主机；

3)发送恶意的可执行程序诱骗点击；

4)发送恶意的非可执行漏洞程序诱骗点击（主要途径）。

明御 APT 攻击预警平台对邮件协议进行深度分析，通过对已知、未知攻击漏洞的扫描和动态分析的方式检测邮件内容及附件是否含有 APT 安全威胁。通过分析邮件中的内容可分析出欺骗链接、挂马页面、伪造发件人等各种常见攻击手段。分离邮件中的附件，使用深度的检测手段找到邮件附件中可执行文件攻击和非可执行文件攻击。主要防护内容包括：

1)伪造发件人攻击检测；

2)欺骗挂马检测；

3)伪造欺骗链接检测；

4)恶意文件检测；

5)webmail 攻击检测。

#### 3.2.3.4 病毒木马攻击预警

当 APT 攻击已经进入内网后，黑客将会利用所获得的权限对一些如 FTP 上的文件进行挂马操作，通过外网下载各种恶意后门，发送带溢出的攻击文件。

明御 APT 攻击预警平台通过对内部网络流量进行抓包分析，捕获 APT 攻击行为，实现 APT 预警。在检测过程中会分离流量中的各种协议的文件，对文件进行检测。发现文件中的恶意代码，并及时进行预警。

- 病毒木马特征检测

通过对分离出的文件进行快速扫描，内部集成全面的多引擎特征库，及时检测其中存在

的各种病毒木马文件，并对文件的来源、目的、详细信息进行分析，便于进一步的进行理。

- Shellcode 静态行为分析

静态二进制文件安全分析技术可发现常见格式文件的异常特征，如：pdf、doc、exe、xls 等。并根据其异常格式、文件异常特征、异常代码等判断文件的可疑特征。并进行进一步的分析。

- 沙箱动态行为分析

系统中内置了动态沙箱系统，可针对文件进行动态行为分析，通过分析恶意文件的运行时行为来确定文件是否存在问题。

沙箱采用业界领先的多沙箱和单沙箱多进程并发设计，极大的提升了沙箱检测性能，通过建立恶意代码行为模型，深度分析和判断可疑文件的行为特定，并确定文件是否存在恶意代码。

#### 3.2.3.5 0day 攻击识别

安恒通过长期的研究，总结并提取各类 0day 攻击的特点。在网络流量中分析关心的文件。通过快速检测算法，对目标文件进行检测，识别攻击样本。

通过检测目标文件中的 shellcode 以及脚本类文件中的攻击特征，并结合动态分析技术可以有效识别 0day 攻击行为。

#### 3.2.3.6 异常行为识别

APT 通常会结合人工渗透攻击，在人工渗透攻击中经常含有扫描或病毒扩散的过程。这

些过程中，通常会产生大量的恶意流量。我们通过沙盒行为分析技术分析这些恶意流量特征，建立了基于时间、IP、端口、协议等多维度有效检测方式发现攻击行为。

- 对内网向外请求异常行为进行分析，包括非法请求外连、恶意盗取数据和敏感数据回传等行为；
- 基于恶意行为的模型化分析，提取真正的恶意回连行为。
- 通过一段时间对访问频度进行统计，发现其访问频度的异常行为，如：暴力破解操作、sql 注入数据获取（短时间大量请求相同页面 ）， 扫描（长时间遍历网站文件）等
- 基于 url 异常访问行为的统计
- 通过一段时间的请求分析，对请求 url 进行统计分析，发现其中的异常，如：没有带 referrer 的 url 进行逆序排列。频繁访问特定页面，并且时间非常集中

#### 3.2.3.7 云端高级分析

APT 的对抗是以时间对抗时间，云端是产品的重要补充，是对用户提供的一种更为高级的服务，可更为及时有效的利用大数据的能力提升 APT 检测的效果。

明御 APT 攻击预警平台云端可提供更为深层的威胁分析服务、安全预警服务和情报共享服务，依托于云端的海量数据、高级的机器学习和大数据分析能力，可及时共享最新的安全威胁情报，提供更为精准的威胁分析能力。

### 3.2.4 用户行为分析（UEBA）

安恒 AiThink 用户与实体行为分析系统（以下简称 AiThink）实现对用户整体 IT 环境的

威胁感知，包括用户管理、资产管理等核心能力，辅助梳理和识别企业的业务场景；通过数据治理能力，将原本零散分布于各类不用信息系统的数据进行标准化和规范化，辅助梳理和选择正确的数据；同时通过深度及关联的安全分析模型及算法，利用 AI 分析模型发现各系统存在的安全风险和异常的用户行为，在此基础上，实现统计特征学习、动态行为基线和时序前后关联等多种形式场景建模，最终为用户提供包含正常行为基线学习、风险评分、风险行为识别等功能的实体安全和应用安全分析能力，可作为企业 SIEM、SOC 或数据防泄漏（DLP）等技术和企业安全运营体系的升级，为企业提供内部安全威胁更精准的异常定位。系统核心功能包括：

#### 3.2.4.1 UEBA 分析要素梳理

UEBA 解决方案进行内部威胁分析的三大关键要素为用户、实体和关键数据，UEBA 属于高级安全技术应用的一种形式，是建立在基础安全防护建设之上，利用大数据、人工智能技术解决某类特定的安全风险场景，准备实施 UEBA 之前，需要对企业的安全业务或痛点进行梳理，进行针对性的开展后续各项工作。

#### 3.2.4.2 特征工程

特征工程是 AiThink 的全部特征管理、统计、分析以及特征自适应学习功能，从数据层面为用户提供全局的特征管理能力，特征列表支持创建特征与特征计算任务监控能力，从特征列表中可提供关键特征用于 UEBA 风险分析。

#### 3.2.4.3 风险分析与溯源排查

安恒 UEBA 通过机器学习对用户、实体进行分析，具备实时和离线的检测方式，得到一

个具备多维特征和威胁综合分析的风险评分指数，并通过风险评分指数的变化趋势，让运维人员实时感知风险的变化。通过风险评分，告知安全人员需重点关注的异常账户，并提供用户画像进行威胁研判，让安全人员能够快速响应异常和威胁。

风险评分指数包括个体总体风险综合评分和单视角风险评分两个维度，前者用于个体风险直观评判，后者用于个体威胁研判溯源。

### 3.2.5 数据分析处置

数据勒索攻击具有很高的隐蔽性，从大量的日常事件中，定位到勒索攻击，对于安全人员是很大的挑战，安恒 AiLPHA 智能安全平台在作为过内领先的安全大数据分析与处置平台，在数据勒索的监测和处置中，会成为企业的网络安全大脑，安全运维人员手中的神兵利器。其主要功能架构如下：

（一）数据采集

大数据智能分析平台以协议/接口采集为主，Agent 收集为辅，除了采集对象不支持通过协议或接口转发之外，采用安装 Agent 进行采集。

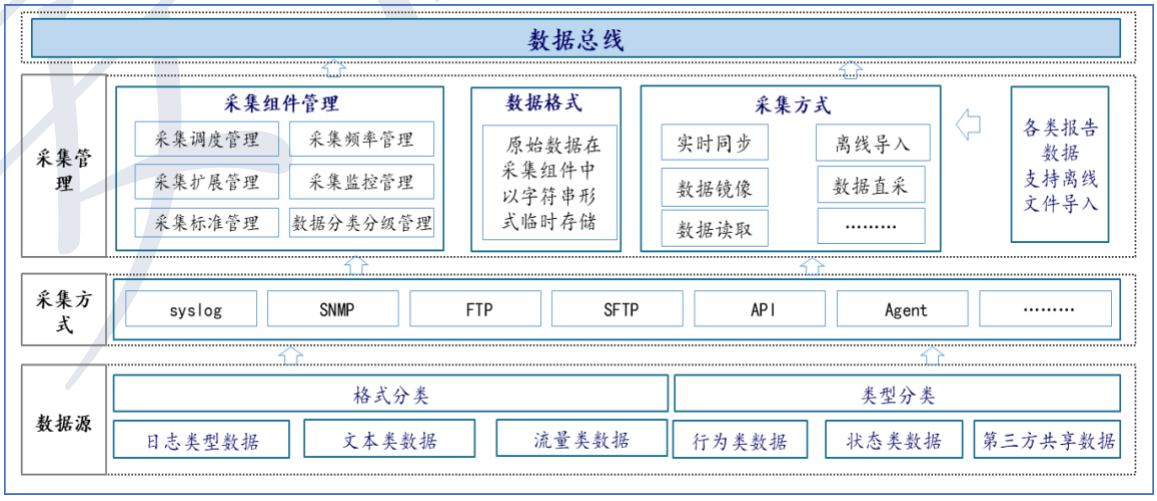


图 数据采集流程图

支持的数据采集方式如下：

◆协议/接口采集：支持采集节点通过 Syslog、Ftp/Sftp、webservice、SNMP、file、JDBC/ODBC 等协议或接口采集数据；

◆Agent 采集：Agent 支持 Windows、Linux、Unix 等系统的数据收集。

（1） 分布式部署

每个数据采集引擎支持配置不同的采集策略，保证每个数据采集引擎有针对性的采集数据，如动态配置采集周期，清洗过滤策略等。需满足如下采集部署要求。

- 支持分布式多节点部署；
- 支持多采集节点存活、健康状态监控，发现节点异常后，及时告警；
- 支持对采集节点性能监控，保证采集性能与数据量匹配，防止数据丢失。
- 采集策略管理。支持对设备的采集策略的管理，包括采集频率、采集协议、采集目标、过滤策略等。
- 支持流量数据镜像采集的方式。支持在多个机房的交换机上复制镜像，分布式部署分光器和 DPI 的方式采集，并将多余的接口关闭；
- 支持主机终端的数据采集，支持数据库审计分析的数据采集；
- 支持数据汇聚。综合考虑专网传输性能的基础上，需满足将多个机房采集到的数据传输汇聚。

（2） 采集协议

大数据智能分析平台为适配各种采集数据源，需要支持多种采集协议，以实现对各类数据的采集，包括不限于安全对象属性、运行状态、安全事件、评估与检测等数据。为实现对包括安全对象的属性、运行状态、安全事件、评估与检测等数据的采集，针对不同类型的数据以及对应的适配协议，采集频率建议如下：

表 适配协议

| 主要适配协议 | 主要采集数据 | 建议采集频率 |
| --- | --- | --- |
| Syslog | 采集 Linux、Unix 等服务器日志及各种支持 Syslog 协议的防火墙、WAF、防病毒和 IDS 等安全设备的日志； | 实时/准实时采集 |
| SNMP | 采集各种支持 Snmp 协议的路由器、交换机等系统或设备； | 每 15 分钟一次 |
| JDBC/ODBC | 采集存储在关系型数据库的数据，如资产数据、人员数据、工单数据等； | 每 4 小时一次 |
| FTP/SFTP | 采集开放 FTP/SFTP 下载服务的应用系统的日志文件，例如 Apache 的日志文件； | 每 15 分钟一次 |
| File | 支持基于文件的日志采集，如通过 SSH/Telnet 等登录到设备上获得数据文件； | 每 15 分钟一次 |

| | | |
|---|---|---|
| Webservice/ API | 支持 webService 方式监听，主要用于同步第三方应用系统的数据； | 按需调用 |
| 爬虫 | 支持爬虫的方式获取公网上的数据,包括但不限于威胁情报 | 按需调用 |

（3） 采集扩展

大数据智能分析平台支持线性扩展，从软件层面，支持采集脚本的热插拔和即插即用，能够灵活扩展采集脚本；硬件层面，支持采集服务器的直接入网，无需改变网络环境；

当新类型资产入网后，在不影响系统其它功能的前提下，能迅速将此资产数据纳入采集。

一、 数据汇聚和处理

大数据智能分析平台数据汇聚存储用于对采集上来的不同类型的数据进行分类存储，以满足数据分析的要求。

（1） 数据存储规则

定义数据存储中支持的数据类型、存储方式、存储要求、存储周期等。数据存储根据数据结构类型的不同，采用如下存储方式。

表　存储方式

| 数据源 | 数据量 | 处理实时性 | 数据类别 | 存储方式 |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 网络设备 | 大 | 低 | 路由器日志、交换机日志等 | 分布式文件存储<br>分布式全文检索 |
| 安全设备 | 大 | 低 | 防火墙日志、IDS/IPS 日志、DDOS 日志、VPN 日志、WAF 日志等 | 分布式文件存储<br>分布式全文检索 |
| 服务器 | 大 | 低 | 登录日志、运行日志、状态数据、访问日志、中间件日志等 | 分布式文件存储<br>分布式全文检索 |
| 应用系统 | 大 | 低 | 数据库审计系统、网马检测系统数据等 | 分布式文件存储<br>分布式全文检索 |
| 业务系统 | 中 | 低 | 基础类数据（如资产数据，用户数据、资产数据等）、场景分析结果数据、业务数据（如安全评估与检测平台的漏扫结果、管理合规结果）等 | 分布式文件存储<br>分布式全文检索 |
| 流量数据 | 大 | 高 | 原始数据包、Flow 数据等 | 分布式文件存储<br>分布式消息总线 |

（2） 数据存储备份

从不同种类数据源收集的安全事件信息通过大数据采集器的泛化和压缩处理，经过标准化的安全事件信息进入 Kafka 消息列队，消息列队中的安全事件信息通过安全事件分析调度任务引擎处理后保存到 ElasticSearch 和 HBASE 中。

支持主流的数据备份技术主要包括：冷备份和热备份技术、写前拷贝技术、快照技术、镜像技术、独立冗余磁盘阵列（Redundant Arrays of Inexpensive Disks，RAID）技术等。具备原始日志、范式化日志事件、告警等数据全量集群存储与备份。

（3） 数据字段管理

数据字典管理是整个系统对采集的数据信息的统一管理及发布平台。负责维护数据信息的录入、修改、删除。

支持数据字典中数据信息的维护，包括数据信息的录入、修改、删除。数据信息字段包括：数据信息唯一标识、数据来源、同步方式、数据的标准化字段格式说明、备注、目标存储平台等基础信息。

二、 分析引擎设计

大数据智能分析平台分析引擎包含实时流计算和离线计算两大引擎，技术框架包含 HDFS、Hive、Flink、Mapreduce 等。可通过模型中心配置业务关注的统计指标、规则模型、关联模型等，对数据中的任意字段进行统计、求和、均值、唯一值等算子的计算，对多源数据通过事件优先级和字段包含关系关联，实现业务指标高实时运算。

分析人员可以利用统一图形化接口，上传统计脚本和算法模型等。界面可配置脚本参数，可查看结果反馈。根据日志和输出结果调整模型，达到模型训练效果。

数据分析整体流程如下图：

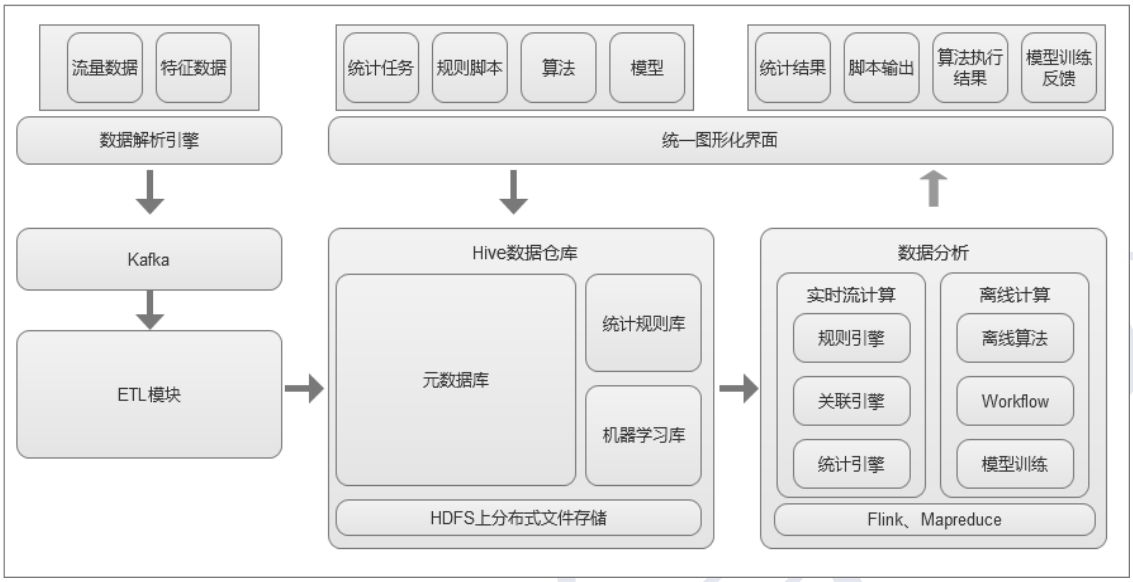



图　数据分析流程图

分析引擎实现如下辅助建模能力：

(1)数据仓库。数据库是基于 HDFS 实现的分布式 Hive 数仓，数据查询集成了 impala 工具，支持 SQL 查询。数仓包含所有元数据和分析人员上传的规则脚本，所有数据由数据仓库统一管理；

(2)图形化界面。数据平台提供图形化界面，方便数据接入，方便任务、脚本以及算法和模型部署。分析人员可以提交离线、实时任务，可以编辑自定义 workflow，也可以提交自定义脚本。全流程可监管，可控制，分析结果即时反馈。

➢ 实时流计算

实时流计算引擎包含规则引擎、关联引擎和统计引擎三大模块，应用无边界流数据计算场景。分析人员可以对数据中的任意字段做统计、求和、均值、唯一值等计算，编写 SQL 提

交 Flink Job，实现业务指标高实时运算。

分析人员上传规则和关联脚本到数据平台，通过界面配置参数，提交任务到平台。规则和统计结果实时输出到图形化界面。

➢ 离线计算

离线计算引擎支持部署离线算法，模型训练和机器学习场景。分析人员可以利用离线分析引擎对数据进行深度提炼挖掘，算法输出结果即时反馈，提供模型训练能力。

分析人员编写算法脚本和机器学习模型，上传到平台后提交离线任务。任务执行结果及时反馈到界面，可以根据算法执行结果调整模型，形成模型训练和机器学习闭环。流程图如下：

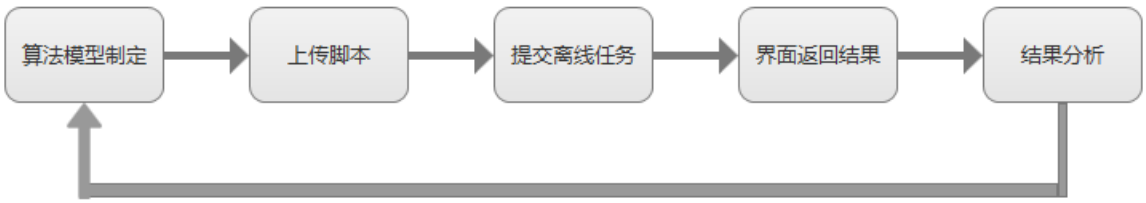



图　离线分析流程图

➢ 模型智能编排设计

可实现对模型的智能编排，支持用户不是常用的数据挖掘和集群学习基础算法。模型智能编排逻辑如下。

✧ 模型编排画布中，元素左侧代表输入，右侧代表输出；

✧ 使用有向连接线标书模型数据的流程，支持多个元素的链接；

✧ 支持已建立的模型复用（可直接调用已有模型作为下一个模型的输入）；

✧ 模型编排修改模型时，在完成界面显示模型指标的增删改情况。

✧ 模型实时输出。模型编排完成 ，可实时返回模型的计算结果。

✧ 支持使用 Python、Java 等语言开发数据分析程序。

三、 安全分析场景和模型设计

大数据智能分析平台基于模块化设计的思路来数据分析中多源异构数据的融合性分析的实现 。

（1） 网络安全分析

网络安全分析功能主要提供针对网络层信息设备的安全分析结果可视化和分析结果可视化以及审计服务功能。主要包含的设备为交互机、防火墙、IDS 等安全设备和网络设备等。实现网络层面的安全攻击、入侵分析要求，主要提供如下分析、审计功能：

- 攻击方向识别。通过日志数据和流量数据以及客户的实际网络环境关联分析，实现对攻击方向的识别，为用户提供区分外对内、内对内、内对外攻击视角。提供外部威胁感知、横向威胁感知和资产外联感知功能；
- 异常行为分析。能够通过深度及关联的安全分析模型及算法，利用 AI 分析模型发现各系统存在的安全风险和异常的用户行为，主要包括但不限于下列分析场景：账户异常行为分析、账户权限变更行为分析、资产被访问异常分析、账户监测异常、非法外

联外访、数据违法泄露、业务违规场景、APT 攻击场景、挖矿病毒类等异常场景；

- 网络安全分析报告。对网络安全分析结果提供报告。

（2） 主机安全分析

主机安全分析功能主要为对主机、服务器、中间件等访问、操作日志进行安全分析，提供安全分析结果可视化和审计结果可视化以及审计服务功能。主要提供如下分析、审计功能：

- 操作对象安全分析。提供对主机的操作对象进行安全分析，分析对象包括主机的登陆用户、访问用户等，对主机的恶意操作、删除日志、修改权限、病毒扩散等高风险操作行为进行安全分析和审计；
- 应用性能分析。提供对主机、服务器、中间件、数据库以及应用系统的可用性、性能参数进行监控的功能，保障主机承载的服务的连续性和可用性；
- 主机安全分析报告。对审计分析结果提供分析报告。

（3） 数据安全分析

提供针对的数据进行安全审计分析，本期主要分析关系型数据库。主要为了确保数据访问的授权性、检测可疑访问和越权访问等，保障数据不被非法窃取、删除、篡改等恶意操作。主要提供如下分析功能：

- 数据操作行为分析。对审计分析结果提供分析报告。提供对数据库的操作对象进行安全分析，分析对象包括对数据的访问用户包括远程应用访问用户等，对数据的恶意操作、删除、篡改等高风险操作行为进行安全分析和告警；

- 数据安全分析评估。自动完成对几百种不当的数据库配置、潜在弱点、数据库用户弱口令、数据库软件补丁等等的漏洞检测；
- 应用三层关联审计分析。将 web 审计记录与数据库审计记录进行关联，直接追溯到应用层的原始访问者及请求信息（如：操作发生的 URL、客户端的 IP 等信息），从而实现将威胁来源定位到最前端的终端用户的三层审计的效果。通过三层审计能更精确地定位事件发生前后所有层面的访问及操作请求；
- 数据安全分析报告。对审计分析结果提供分析报告。

（4） 应用系统安全分析

实现对核心应用系统的访问行为、连接行为、攻击行为以及应用系统性能进行审计分析，及时发现异常行为和应用系统应用性能监控，对异常行为和性能进行分析和预警，及时发现针对应用系统的安全攻击。主要实现如下分析、审计功能：

- 操作对象分析。提供对应用系统的操作对象进行安全分析，分析对象包括应用的登陆用户、访问用户等，对应用系统的访问频次、访问时间、访问地点等行为进行安全审计，及时发现异常的访问连接；
- 访问流量审计分析。提供对应对应用系统的来着互联网的访问流量进行审计分析，包括协议解析、应用会话行为、深度风险行为、合规行为等，支持全网双向流量、流向等行为的审计；
- 应用系统漏洞被利用行为审计分析。提供针对应用系统的漏洞被利用、尝试利用漏洞攻击等行为进行安全分析，及时发现漏洞的被利用情况，监控漏洞的修复进度，提供

漏洞数据进行安全审计功能；

- 应用性能监控。提供对应用程序的可用性、性能参数等进行监控功能，保障应用服务的连续性。
- 应用安全分析报告。对应用安全分析结果提供分析报告。

（5） 用户行为分析（UBA）

运用大数据的技术，汇总用户相关的历史、档案、行为得出个体和群体在一个长期时间范围内稳定的数据特征，从而描绘出用户的信息全貌。用户画像和异常行为分析系统根据用户的 Hadoop 历史使用行为习惯来画像和定义行为模式。用户行为模式通过机器学习算法生成，在用户当前实时行为模式与其对应的历史模型模式存在一定程度的差异时识别用户行为是否为异常。通过对数据进行分割、审查、交叉分析，周期性地为每个用户依次创建行为模型。系统能够近乎实时地识别出异常行为。

从个体特征维度、群体属性维度这两个方面对用户画像进行全面的分析。

✧ 个体特征画像

个体特征画像将用户的基础属性数据与行为数据进行统计分析，为不同的用户建立适应性动态行为画像特征库，用于描绘个体用户行为；

✧ 群体特征画像

群体特征维度画像是基于个体特征画像的基本属性数据和行为数据，所描述出相同特征的人群轮廓，分别定义出各类人群的标准属性和行为特点，可结合单位的组织划分进行群体描绘。

（6） 终端用户行为分析

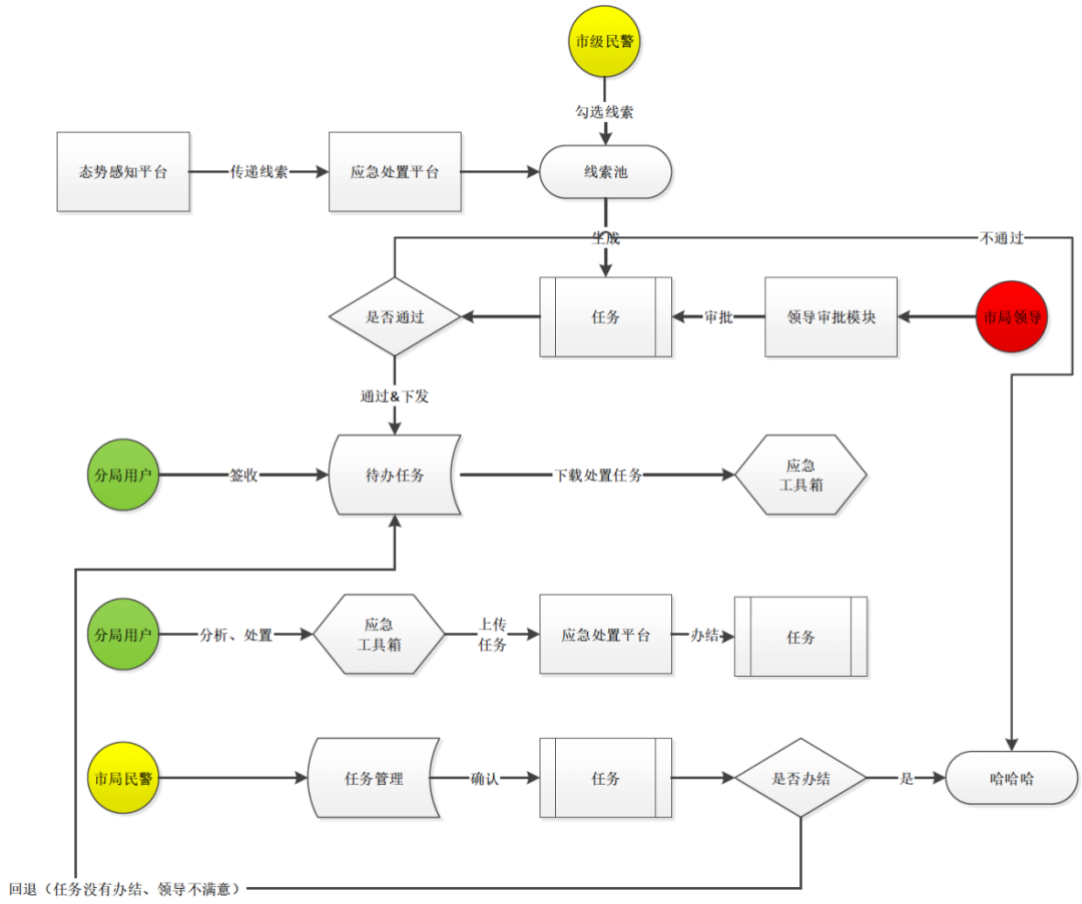
提供对终端用户的行为审计功能，主要包括终端的访问时间审计、访问地点审计、访问的应用系统审计、访问频率审计等。结合用户画像和资产画像，及时发现异常的终端行为。如利用安全事件溯源分析引擎，当发现应用系统受到的攻击来着终端用户，结合用户画像，定位到具体的终端责任人，提供如下终端用户行为审计报告和统计结果。主要提供如下功能：

- 异常登录行为分析。包括异常时间登录、异常地点登录、堡垒机绕过等异常行为分析；
- 终端安全事件溯源。结合用户画像分析，当终端发生安全事件时，可以定位到具体的责任人；
- 分析报告。提供安全分析报表。

安全运维人员根据安全监测发现的网络攻击、重大安全隐患等情况以及相关部门通报的情况，下达网络安全事件快速处置指令。指令接收部门按照处置要求和规范进行事件处置，及时消除影响和危害，开展现场勘察， 固定证据，快速恢复。对事件处置情况、现场勘察情况以及证据等方面情况及时建档、归档并入库。

快速处置系统在网络攻击事件发生后，对攻击事件做应急处置，建立快速处置任务。快速处置系统与应急处置工具箱联动使用，对攻击现场做事件取证、快速恢复等工作，包括全盘镜像、分区镜像、提取项目部署文件、提取边界设置文件、提取主机访问日志、提取应用程序日志等操作，为追踪溯源提供数据支撑。

- 快速处置流程




● 快速处置可视化展现

可视化展现全国及各个下属单位的事件总数、事件发生情况及处置情况。

直观展示全国及各个下属单位的线索数量，事件处置过程中待签收、处置中、已完结等各个状态的事件数，展示全国及各个下属单位事件等级数，包括高危事件、中危事件和低危事件，统计全国及各个地区每季度的事件总数，横向对比展现各个季度的事件趋势。

● 快速处置任务

事件发生后，快速处置系统可对对应事件建立处置任务。

可在平台新建快速处置任务，包含该次处置任务的单位信息、系统信息、事件信息、处

置策略等。平台可与应急处置工具箱联动使用，将处置任务下发到应急处置工具箱后，执法人员持应急处置工具箱前往事件现场进行处置，完成处置后将结果回传到平台，由平台用户审核该次事件，并对事件后续进行管理。

- 线索传递

快速处置系统在平台构建了一个统一的线索池，线索来源包括用户上传，管理员推送和其他来源。

可在平台上查看该条线索的详情，或者将该线索生成处置任务：填写任务信息、单位信息、系统信息、事件信息和处置策略即可完成。

- 处置策略

快速处置系统在平台构建了一个处置策略库，生成快速处置任务时需要从库里选择的处置策略。处置策略由用户事前新建，根据事件不同的情况，紧急程度、破坏程度等建立不同的策略，合理调用、分配资源。

在安全事件研判分析确认安全事件之后，流转至安全事件处置响应模进行安全事件信息联动处置。对已经确认的攻击，可以通过人工的处置流程剧本编排，通过不同威胁级别的安全事件，可以选择不同的处置方式，如邮件/短信通知、联动 EDR、防火墙等设备进行阻断隔离等。

## 3.3 事后恢复溯源

勒索病毒就像笼罩在企业头顶的一朵乌云，众多企业遭受了勒索病毒的入侵，造成了核

心业务系统全线停摆，企业为此蒙受了巨大的损失。勒索病毒的防范和事后补救最有效的方法就是备份与恢复。数据备份与灾难恢复是数据安全的最后一道防线。但是光有数据备份是不够的，健康的备份介质也可能感染勒索病毒，造成数据无法恢复，因此对于备份介质的保护也是至关重要的。

### 3.3.1 数据备份与恢复

建立一套数据备份与恢复机制至关重要，企业建立数据备份系统时，根据业务需求选择以下的备份机制：

- 完全备份：对某一个时间点上的所有数据进行的一个完整的备份。实际应用中就是对整个数据库系统进行完全备份，包括其中所有的数据对象。当发生数据丢失的灾难时，完全备份无需依赖其他信息即可实现 100%的数据恢复，其恢复时间最短且操作最方便。
- 差异备份：备份那些自从上次完全备份之后被修改过的文件。从差异备份中恢复数据的时间较短，因此只需要两份数据即最后一次完整备份和最后一次差异备份。
- 增量备份：在一次全备份或上一次增量备份后，以后每次的备份只需备份与前一次相比增加或者被修改的文件。这就意味着，第一次增量备份的对象是进行全备份后所产生的增加和修改的文件;第二次增量备份的对象是进行第一次增量备份后所产生的增加和修改的文件，如此类推。这种备份方式最显著的优点就是没有重复的备份数据，因此备份的数据量不大，备份所需的时间很短。

### 3.3.2 备份物理保护

勒索组织在加密数据之前，会采用删除备份数据、加密备份数据等方式，想方设法破坏企业的备份与恢复机制。Dell EMC 提供的 Cyber Recovery 解决方案，采用备份数据监控和物理安全环境相结合的一种数据备份保全机制，其主要功能如下：

- 备份文件加密存储：使用加密和公钥加密方法来保护备份文件，可有效保护备份文件免受勒索病毒感染。
- 备份文件多副本管理：为了防止备份数据意外损坏，产生多个备份副本是非常有必要的。产生数据副本的方法有两种：同步和异步。同步的方法是，在备份时，同时把备份数据写入到两个不同的介质中；异步则是，先把备份数据写入一个介质，然后再利用空闲时段，将备份数据复制到其他介质上。当然也可以通过网络将其复制到异地，达到数据容灾的目的。
- 备份文件完整性检测：通过准生产环境或者灾备环境定期做备份文件完整性校验，根据不通要求或数据量选择不同的备份或架构，可以在与正式生产环境隔绝的情况下不定期进行备份文件恢复演练，以确保备份文件的完整性、正确性。
- 备份文件存储区安全：存储区环境设置为单独的安全区，与生产环境在物理和逻辑上均进行隔离。让存储区拥有自己的网络交换基础架构。存储区间的通信不会路由到任何其他环境，隔离可进一步减少备份文件存储区的攻击面，有效保护备份文件的完整性。

### 3.3.3 应急响应

安恒信息客户服务中心提供 7*24 小时的电话支持安全服务，企业可以根据安全运维人员的初步判断认为发生了数据勒索事件，可以立即通过电话咨询安恒信息安全客户服务人员，服务人员会根据客户信息提供电话支持服务，在客户和安恒信息安全服务人员同时确认需要信息安全专家或安全服务队伍现场支持后，安全专家立即赶到现场。

安全专家抵达现场后，首先开始保护或恢复计算机、网络服务的正常工作，抑制（缩小事件的影响范围）、然后再对入侵者进行追查，解决问题、恢复以及后续跟踪等。

安全专家利用采用大数据平台等平台工具手段对安全事件进行追踪溯源，追踪溯源系统在发生网络攻击事件或有线索情况下，对攻击者及其使用的攻击手法、攻击途径、攻击资源、攻击位置、攻击后果等进行追踪溯源和拓展分析。

（1） 攻击溯源

攻击溯源联动分析是以攻击手法作为模型进行检测，这些攻击手法的模型源自于攻击者历史攻击的特征的累计识别。

该系统的攻击溯源，依靠多个云端引擎库和智能算法的结合、依托于互联网大数据深度挖掘分析技术、联动了互联网其他安全厂商共同组成了攻击溯源体系。

（2） 取证攻击过程

攻击溯源联动分析在确定攻击事件后会回溯所有攻击相关的网络数据包，对系统近期的所有行为进行串联，确定攻击事件的整个事件周期，展示整个攻击事件的所有攻击路径。以时间轴的方式将攻击者的所有攻击动作列举出来。通过安全设备的告警日志、系统设备日志

与资产画像对比分析，确定遭受攻击的服务器。通过分析这些被攻击的设备的系统日志，挖掘出攻击者的攻击入口。还原出攻击者在不同服务器之间的攻击路径。如图，模拟出某次攻击的攻击跳转路径，还原出如图所示的攻击路径。

### 3.3.4 谈判专家

安恒信息建立首支具备过硬专业技能的安全危机谈判专家团队并提供相应服务，通过与政法类高等院校合作培训，联合赋能培育防数据勒索的【安全谈判专家】，具备信息技术顾问、公关顾问、法律合规顾问以及危机谈判专家的能力，专项应对国际勒索团队，一起构建更稳健的网络安全商业生态环境。

### 3.3.5 网络保险

保险具有经济补偿、风险管理功能，能够发挥社会稳定器和经济助推器的作用。在发展数字经济过程当中，通过保险“兜底”，可以协助单位做好网络风险管理，实施创新发展。一是通过网络安全技术与保险相结合，由专业安全机构通过网络安全技术，帮助企业实时防控外部风险；二是在内部人员疏忽风险等技术无法触及的领域，使用保险来转移风险、补偿损失，通过科技与保险相互结合、相辅相成，形成全周期闭环的网络安全风险解决方案，可以有效提高企业的整体风险管理水平。安恒信息联合保险公司打造网络信息安全综合保险，通过技术与保险相互结合的方式，为企业信息系统正常运营和持续运营提供整体的网络安全风险管理方案。

# 4. 产品与服务清单

本方案所涉及的产品和服务清单如下：

| 防护领域 | 名称 | 类型 | 具备的安全能力 | 备注 |
| --- | --- | --- | --- | --- |
| **事前监测预防** | 主机安全及管理系统（EDR） | 产品 | 主机安全管控，防勒索病毒和木马入侵，集成安全沙箱、端口检测、补丁管理、进程防护等功能。 | 由管理中心和客户端组成 |
| | 防垃圾邮件防火墙 | 产品 | 通过对来自僵尸网络邮件来源进行过滤，对邮件题及附件进行检查，隔离和阻断不安全的邮件。 | 网关部署 |
| | AiSort 数据安全分级与风险评估系统 | 产品 | 集成数据资产发现、敏感数据识别、数据分类分级、数据资产管理等功能，识别关键数据，为数据备份与恢复和重点监测保护提供依据。 | |

| | | | | |
|---|---|---|---|---|
| | 安全评估检查 | 服务 | 采用专用工具为企业提供整体安全评估和检查，并提供协助进行整改。 | |
| | 安全意识培训 | 服务 | 对企业员工进行数据防勒索专项培训，提高员工的安全意识和责任心。 | |
| | 邮件钓鱼服务 | 服务 | 基于钓鱼测试服务，通过定期发送钓鱼邮件的方式，提升员工识别钓鱼邮件能力；通过嵌入式学习方式，推动企业强制性合规教育、防范商业邮件欺诈与勒索软件。 | |
| | 应急演练 | 服务 | 协助用户模拟数据勒索事件的应急处置，优化应急响应流程，提高配合度和响应速度。 | |
| **事中监测防御** | 明御®数据库审计与风险控制系统 | 产品 | 旁路分析数据库访问，可以监控攻击行为、高危操作和 | 解析网络协议，通常采用交换机 |

| | | | | |
|---|---|---|---|---|
| | | | 批量数据下载，可以外发数据用于安全分析。 | 端口镜像 |
| | 明鉴®迷网系统 | 产品 | 通过构造数据库蜜罐，诱使攻击者攻击，从而捕获攻击行为， | 包含管理中心和蜜罐终端。 |
| | 明御®APT 攻击预警平台 | 产品 | 分析网络流量，发现其中对持续性攻击，综合安全沙箱和威胁情报等技术，对木马、勒索病毒、Oday 攻击防护都具有明显效果。 | 解析网络协议，通常采用交换机端口镜像 |
| | AiThink 用户与实体行为分析系统 | 产品 | 运用大数据技术对用户和实体行为采用人工智能和机器学习方法进行建模分析，对主体威胁进行评价，发现潜藏的勒索组织或企业内部不怀好意人。 | |
| | AiLPHA 智能安全平台 | 产品 | 采用大数据技术作为企业海量安全数据的分析平台，对安全事件进行安全研判，并 | 大数据平台 |

| | | | | |
|---|---|---|---|---|
| | | | 集成安全处置功能。 | |
| **事后恢复溯源** | 数据备份与恢复 | 体系 | 企业应建立与业务需求一致的数据备份与恢复体系。 | |
| | 备份物理保护 | 产品 | 为防止勒索组织删除备份数据，需要采用更加严格和安全的方法，对备份数据进行防护 | 需要建立与生产系统隔离的备份安全区，并通过软件实现数据同步 |
| | 应急响应 | 服务 | 安恒的安全服务专业团队，能够为用户提供迅速、有效的应急响应服务，对数据勒索进行善后处理。 | |
| | 谈判专家 | 服务 | 安恒培养的谈判专家，能够帮助企业在面对勒索时进行心理建设，运用谈判技巧协助用户进行沟通，把损失降到最低。 | |
| | 网络保险 | 保险 | 安恒提供的网络安全综合保 | |

| | | | | |
|---|---|---|---|---|
| | | | 险，可以帮助企业转嫁网络安全风险，减少损失。 | |