创宇云影内网主机安全监测系统（主机盾）

技术白皮书

2021-11-23

北京知道创宇信息技术股份有限公司

更好更安全的互联网

文档控制

文档名称	创宇云影内网主机安全监测系统（主机盾）技术白皮书
保密级别	内部公开
拟制	
审核	
标准化	

目 录

1. 产品简介

1.1 面临挑战

伴随着信息科技的发展，企事业单位面临的挑战越来越多，企事业单位的主机（PC 和服务器）是黑客进入其内部网络的主要途径，他们的目标通常是访问受限制的敏感数据。传统的反病毒系统不再有效的提供主机保护，因为它们只能通过与已知的病毒数据库或签名列表进行比较来检测威胁。然而，现在 0 day 攻击已经非常先进，这些新型的攻击手段不会出现在签名列表或者病毒数据库中，而且经常绕过传统的安全系统。主要体现在：

（一） 网络攻击肆虐蔓延

由于攻防不对称性的普遍存在，就技术、技能和工具的发展速度而言，网络攻击者已远超大部分的网络防御者。攻击框架的开源分享和漏洞利用工具的不慎泄露，使得网络犯罪的门槛越来越低。新兴的攻击手法肆虐破坏网络、应用和数据安全，甚至威胁到与每一位民众日常生活息息相关的国家基础设施行业的安危。

（二） 传统检测技术难以发现高级攻击

高级攻击刻意利用各种逃避检测的技术，传统的检测手段难以通过一次扫描判断正在处理的数据或者运行的程序是否含有恶意性。攻击者不留痕迹地多次攻陷系统，在系统中留下深度后门，潜伏和隐藏的时间越来越久。然而防御方只有在受到显性破坏性攻击（如乌克兰电力门事件、勒索事件等），或者在分析了大量日志数据之后，才能发现攻击行为，此时信息系统可能已经被长久控制，大量

敏感数据遭到泄露。

（三） 企事业单位需要应急响应支撑平台

全球爆发的 WannaCry 勒索事件充分表明，当猝不及防的威胁来临之时，依靠数量有限的安全运维人员手工操作处理，其响应能力是捉襟见肘的。互联网时代下，一套能够深入主机感知威胁、实现常态化的全面风险评估、以及面对重大威胁快速自动化响应的支撑平台，是政府和企业安全运维必不可少的。

（四） 新的 IT 业务模式需要新的安全解决方案

快速增长的云计算和大数据应用需求，打破了固定化的防御边界，传统安全方案从部署方式到事件响应速度都不足以提供必需的安全服务支持。新的安全解决方案必须满足部署便捷、适应规模变化、跨操作系统平台、易于更新使用的要求。

企事业单位近年虽在数据安全、主机安全采取了一些的管理措施，也取得了一定效果。但是仍存在不少薄弱环节，仍然一些高级持续攻击行为，这些行为无法通过传统防病毒系统进行有效防御，因为防病毒系统只能通过与已知的病毒数据库或签名列表进行比较来检测威胁。然而这些新型的攻击手段不会出现在签名列表或者病毒数据库中，而且经常绕过传统的安全防病毒系统。因此我们需要通过更为有效的技术手段进行管控，提升主机安全性。

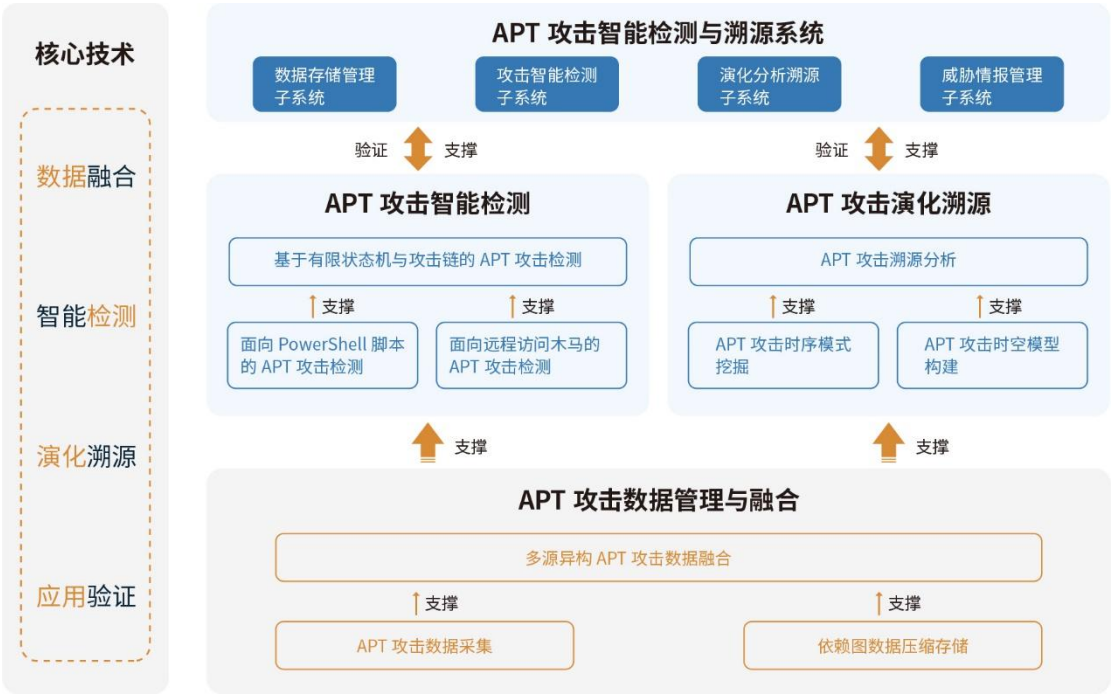
1.2 解决方案

知道创宇是一家国内技术领先安全产品提供商，我们开发了一种先进的安全解决方案，它使用行为分析来检测和应对传统主机系统未检测到的威胁。知道创

宇并没有使用签名来检查文件和过程，而是使用行为分析算法来检查从整个网络的端点收集的事件，识别恶意行为，并提醒安全团队，帮助他们对攻击作出反应，或者进一步调查。

2. 核心技术及功能

2.1 核心技术



- **机器学习技术**

机器学习：是一门多学科交叉知识，是人工智能领域的核心，专门研究计算机如何模拟实现人类的学习行为，通过获取新的技能知识重组已有的知识体系，并不断完善自身性能。在大规模数掘处理中，可以自动分析获得规律，然后利用这些规律预测未知的数据。

机器学习算法的分类应用步骤：分类器训练和模型检测。首先利用训练集

文件的向量模型及其类别标记生成分类器，其次利用分类模型对待检测数掘进行分类检测，通过将检测结果来与真实样本数掘进行比对，评估分类器的效果，最后根据结果进一步完善分类器。

EDR 中的机器学习：在 EDR 中，机器学习主要应用于端点用户和软件的正常行为和异常行为的提取，通过捕获大量的端点静态和动态的用户和软件行为特征向量，采用机器学习的思想进行端点用户和软件行为的训练建模和分类检测，得出该使用场景下用户和软件的正常和异常行为知识库，从而利用知识库可以更加高效地检测出端点的异常行为。

- **大数据关联分析**

用途：在 EDR 中，端点采集的各类安全运行数据是终端安全工作中防御、检测和响应的重要依据。对海量终端安全数据进行自动智能化的关联分析，追溯其攻击过程，寻找漏洞源和攻击源，是有效防御和确保终端安全的重要途径和方法。

主要目标：大数据关联分析的主要目标是不丢失终端安全相关的重要信息，并通过分析原始终端安全数据而形成全局、缜密、连贯的攻击视图。

针对 APT：为应对 APT 攻击的极强持续性和阶段性，关联分析过程中应尽量收集各层面、各阶段的全方位信息，同时适量将时间窗口拉大，通过宽时间域数据分析提取具有内在关联的若干属性，识别出攻击发生的时间、地点、攻击类型和强度等信息。

- **攻击场景溯源技术**

定义：通过对攻击者一次完整的攻击行为所采用的攻击步骤进行关联分析，

根据检测到攻击发生的时间序列，将该次完整的攻击的每一步攻击步骤以图形的形式重新表示出来，称为攻击场景的溯源。

在 EDR 中，攻击场景溯源通过对关联规则及知识的形式化表述，将庞杂，无序的安全数据流转换为结构化、易于理解的攻击场景，将反映攻击过程和意图的场景图呈现出来，发现攻击者的攻击策略和目的，甚至推测漏报的告警和预测下一步可能的攻击行为，以协助管理人员获取更有价值的网络安全信息。

2.2核心功能

- **海量数据收集，持续检测分析**

为了提供有效的检测，云影-内网主机安全监测系统不断记录来自主机端点的行为。这些行为包括：进程的加载、重要配置变更、文件访问和枚举、用户操作指令等等。这些行为数据收集可以覆盖整个网络，并发送到云影-内网主机安全监测系统管控中心，通过行为分析算法识别并显示相关攻击事件。基于行为分析的算法可以区分恶意行为和良性行为，并能适应客户的环境，从而达到非常有效的检测效果。

云影-内网主机安全监测系统通过行为数据分析可以提供了如下功能，使其成为一个最佳的主机安全管理平台:

- **行为建模和检测算法**

云影-内网主机安全监测系统使用一种主机安全行为的数据模型，它将细颗粒度且标准通用的主机事件解释成可理解的行为。这种行为包括对进程自我复制、钓鱼行为、文档勒索、特权升级或横向移动。云影-内网主机安

全监测系统分析解决方案提供了智能数据处理引擎，相关算法能够从大量的主机端点行为数据有效识别恶意行为。

- **有效的智能分析**

信息安全必须面临的一个关键挑战是如何减少误报。云影-内网主机安全监测系统应用行为分析算法，不断适应客户业务活动，以区分正常和恶意行为。这种方法可以提供更高的检出率，并极大地减少误报。行为智能分析算法对数据流进行了优化，并采用分层式分析结构。

- **基于高效数据检索的场景取证和攻击回溯**

今天的安全响应人员职责是积极地搜寻和寻找威胁，他们必须花费大量的时间在搜索和研究数据上。当发生攻击时，他们需要调查数据以快速了解根本原因并对抗攻击。云影-内网主机安全监测系统存储关于每个主机端点的详细信息，包括但不限于进程运行、命令行操作、文件访问、网络链接、配置变更等。这可以使安全响应人员能够对大量数据执行复杂的查询，并在易于理解的界面中呈现结果。云影-内网主机安全监测系统的高效搜索能力支持各种查询方式，这对安全响应工作来说是至关重要的。

- **可信任的企业级海量数据分析处理技术**

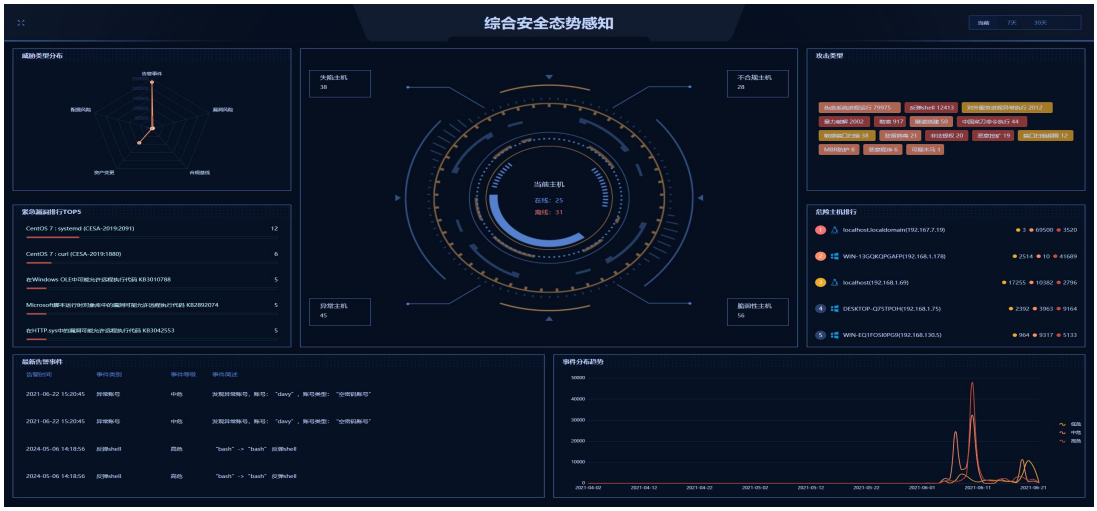
云影-内网主机安全监测系统通常被高安全需求的大中型规模客户使用。因此，云影-内网主机安全监测系统采用了可靠的、健壮的、可扩展的海量数据处理技术，这些数据技术将受到客户的信任，包括政府、金融、运营商、军队、制造业、设计单位和媒体。云影-内网主机安全监测系统的健壮性可以支持大规模的主机端点部署。

3. 主要功能

3.1 主机态势感知

主机态势感知采用先进的大数据架构，通过采集系统的行为数据，自主开发 AI 分析引擎对所有安全数据进行统一处理分析，实现对 APT 攻击以及入侵攻击等威胁事件的实时发现和告警；同时从资产异常变更、合规基线、漏洞风险、配置风险等多维度展示主机安全态势。通过态势感知大屏展示并营造安全可监控、威胁可感知、事件可控制的安全能力。

- 实时推送攻击以及威胁事件
- 攻击类型分布
- 威胁类型分布
- 威胁事件趋势
- 主机脆弱性



3.2资产清点

随着企业信息化的全面发展，运维以及开发环境的多样化，业务规模的不断扩大以及配套设施的随时变化，资产的边界已经越来越模糊，传统的软硬件资产管理已经无法满足信息化企业安全建设需求。如何能将本地环境、虚拟环境以及云环境中的基础资产以及业务资产进行有效梳理，是企业在信息化高速发展过程中首要解决的问题。

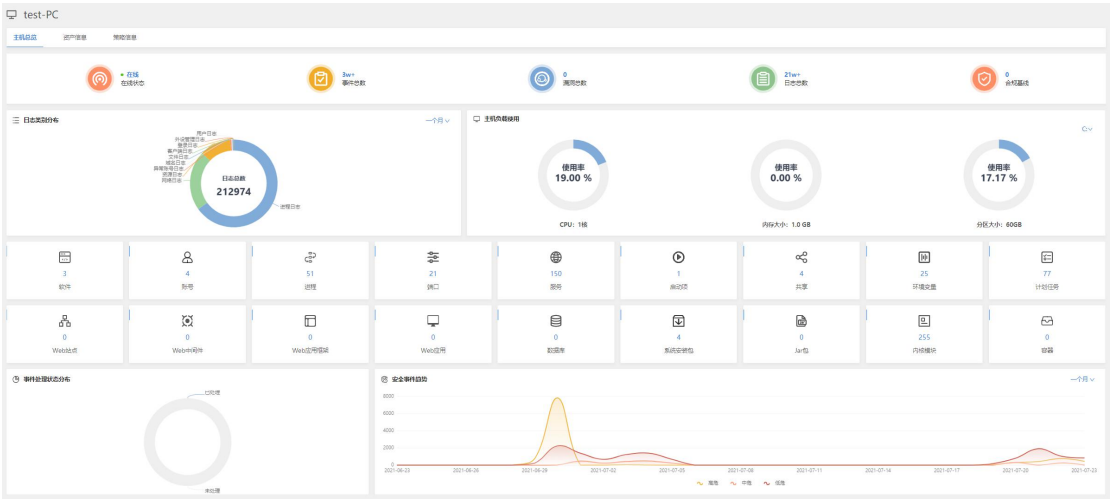
云影资产清点，从传统的基础资产信息到混合数据中心架构中的业务资产进行全面梳理，支持对资产动态的精准识别，可监测资产的动态，对资产的非法变更进行实时告警。

1）主机发现

- 采用 Nmap 扫描、Ping 扫描等多种探查方法，对网内未安装主机探针设备进行自动发现，并针对未安装探针主机一键推送主机探针。

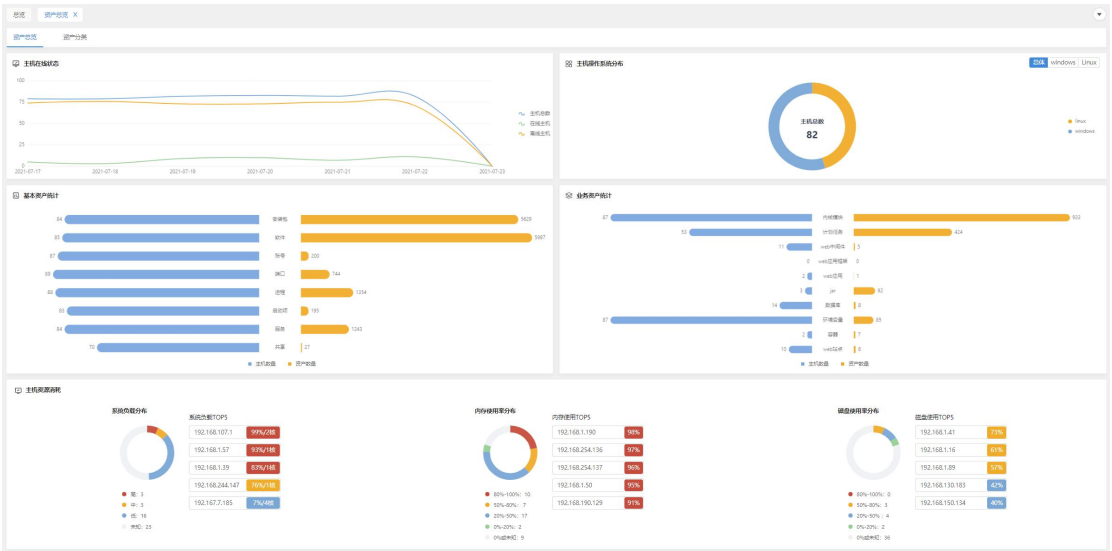
2）资产清点

- 针对主机基础的信息，如硬件信息、软件信息、账号信息、进程信息、端口信息、服务信息、启动项、计划任务等进行自动化清点；
- 针对安全业务资产，如 Web 应用、Web 中间件、Web 应用框架、Web 站点、环境变量、内核、数据库、容器、Jar 包等二十余类资产进行自动化清点，并可支持资产报表导出。



3）资产展示

- 全图形化展示，以图形化多个角度展示主机资产分布以及现状，包括不限于主机在线状态、操作系统分布、基础资产统计、业务资产统计以及主机资源消耗等。
- 双维度资产展示，分为“主机维度”及“资产维度”，主机维度可查看特定主机的所有资产以及图形化展示资产状况；资产维度可针对每类资产进行详细统计，并可从多个角度进行快速检索。



3.3 APT 攻击溯源

据《全球高级持续性威胁(APT)2020 年度报告》显示，中国首次超过美国、韩国、中东等国家和地区，成为全球 APT 攻击的首要地区性目标。

APT 攻击具有针对性强、组织严密、持续时间长、隐蔽性高、破坏性大等特点。并且使用的攻击技术相对先进，政企机构即使网络层部署防火墙、WAF 等，主机层即使部署防病毒等系统，APT 攻击也能绕过，甚至利用防火墙和服务器漏洞获取访问企业网络凭证。此外，通过社交工程侵入内部的 APT 攻击成为了最主要的方式，并且防不胜防。

对于 APT 这种具有未知性攻击，很难提前预知以及提前预防，更多的是事中发现和防御以及事后的溯源。云影产品核心功能即针对主机端 APT 攻击检测以及溯源。

- APT 攻击场景示例：

攻击者在开始执行 APT 攻击时，通常会给攻击目标发送一个具有诱导性的钓鱼文件，作为 APT 攻击的前置侦测动作，被攻击人员一旦打开文件，之后该文件会自动调用系统的 powershell 程序从远端服务器下载远控木马并自动运行，攻击者从而获取靶机的控制权限。

1）被攻击人员打开文件（此时后台自动调用 powershell 下载远控木马，被攻击人员无感知）

2） 攻击者的电脑上靶机上线，并可对靶机进行控制。此时上传了勒索软件和 ghost 木马；

3） 攻击者执行命令运行 ghost 木马，之后可对靶机进行远程桌面控制、键

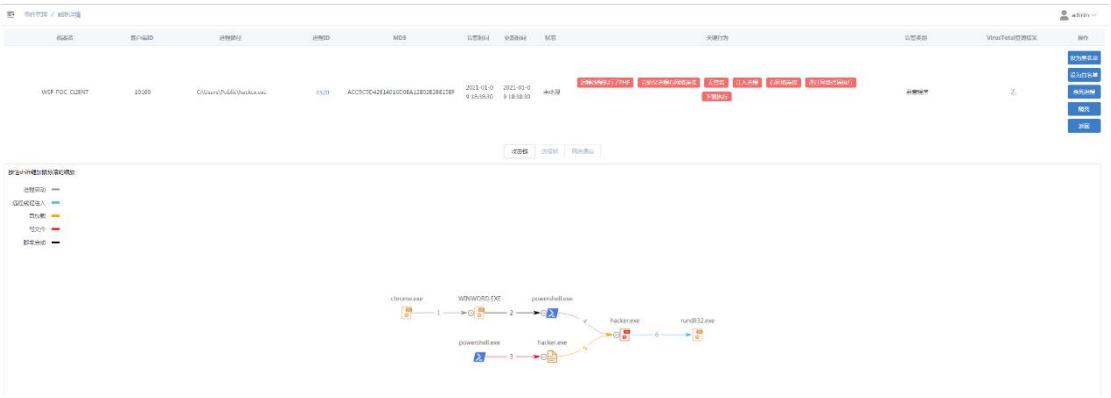
盘记录等操作。

4) 攻击机执行命令运行勒索软件；

5) 勒索软件被阻断；

6) 查看管控中心日志，会实时产生钓鱼攻击、远程执行、勒索软件防护等告警事件；

7）攻击溯源图：



- APT 攻击：

1) 钓鱼攻击：所谓“姜太公钓鱼，愿者上钩”，钓鱼攻击即攻击者伪造成一个可信组织散发诱骗邮件等进行诱骗，这种电子邮件一般会包含一个恶意链接或恶意文件等，只要用户点开就会进入黑客的陷阱。云影-内网主机安全监测系统可通过恶意行为标签，检测到钓鱼攻击，并可通过 APT 攻击溯源进行事后分析，并可将一系列相关的攻击行为通过综合分析关联起来追因溯果。

2) 远控木马攻击：远控木马可被设计用于远程操作用户的计算机，黑客可通过远控木马得到计算机的使用权，从而窃取个人信息、键盘记录甚至可以将其变为僵尸网络的一部分。云影-内网主机安全监测系统可通过恶意行为标签，检测到远控木马攻击，并可通过 APT 攻击溯源进行事后分析，并可将一系列相关的

攻击行为通过综合分析关联起来追因溯果。

3) 漏洞攻击：漏洞攻击可谓是当前最为火热的攻击手段，大部分攻击行为都是通过各种漏洞实现，当目标主机存在漏洞时，攻击者可以通过漏洞直接执行恶意命令攻击主机或留存后门等，从而获取到主机的控制权及各种敏感信息等。比如众所周知的爆发于 2017 年的永恒之蓝即是一种利用 Windows 系统的 SMB 协议漏洞来获取系统的最高权限，以此来控制被入侵的计算机。云影-内网主机安全监测系统可通过一系列的恶意行为标签，检测到漏洞攻击，并可通过 APT 攻击溯源进行事后分析，并可将一系列相关的攻击行为通过综合分析关联起来追因溯果。

4) 无文件攻击：“无文件攻击”这个名词伴随“APT 攻击”的慢慢火热逐渐进入了人们的视野。APT 的特点是不易被安全检测引擎所发现，当中的功劳很大程度都是归“无文件攻击”所有。比如用户打开了一个恶意 office 文档，这个文档通过漏洞直接执行了 powershell 脚本进行木马植入，最后通过写入注册表实现持久化潜伏。由于无文件攻击无需落地到目标的磁盘，因此病毒引擎一般很难检测到，而云影-内网主机安全监测系统通过识别恶意行为特征标签，包括但不限于漏洞利用、网络连接、内存攻击、注入进程等，检测到无文件攻击，并可通过 APT 攻击溯源进行事后分析，并可将一系列相关的攻击行为通过综合分析关联起来追因溯果。

5) 勒索病毒攻击：勒索病毒通过加密文件的方式向受害者勒索收费，自 2016 年开始勒索病毒出现到 2017 年 wannacry 肆意传播，再到 2020 年 WannaRen 通过各大下载资源站传播，此种攻击手段越演越烈。云影-内网主机安全监测系

统通过文件过滤驱动在随机位置创建诱捕文件，当检测到有程序对诱捕文件进行加密时，会立即结束该程序，阻止其进一步运行，并上报安全事件，可对其进行处理，包括隔离/放行等操作。

3.4综合性分析

云影-内网主机安全监测系统基于全量数据采集支持内网横向溯源。为了帮助用户全面了解攻击者进行的攻击，我们提供综合性分析功能，可对多个主机的疑似相关威胁进行关联分析，通过关键元素将攻击事件自动关联起来，把多个相关联的事件合并成一个事件组，通过综合性分析可在一定程度上还原攻击者的攻击路径与攻击手法，

3.5入侵检测

此前入侵检测大部分都是通过对已知攻击的检测，但近年来，由于攻击手段的千变万化，未知的攻击和威胁难以防范。因此对于未知威胁及未知攻击手段的

检测成为了所有安全团队的燃眉之急。云影-内网主机安全监测系统通过实时监控和持续分析，能够实时、准确地检测到入侵事件，感知到攻击行为的细小变化，并提供多种响应手段，比如自动封停、黑/白名单和手动隔离威胁文件等。

- 反弹 shell

  实时监控主机上利用 shell 反向连接的行为。当检测到反弹 shell 时会通过主动防御机制，实时阻断反弹 shell，并上报事件，用户可查看和处理。

- 系统提权

  实时监控进程行为，云影-内网主机安全监测系统可检测到进程提权行为，并通过主动防御机制，实时阻断非法提权行为，并上报事件。用户可以查看并处理。

- 恶意挖矿

  挖矿病毒会大量消耗系统运行资源非法挖矿，云影-内网主机安全监测系统通过实时监控进程行为可检测到恶意挖矿行为，并通过主动防御机制，实时阻断挖矿病毒的运行，并上报事件，用户可查看和处理。

- 恶意扫描

  实时监控端口扫描行为，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，自动将恶意探测 IP 锁定，防止其进一步获取终端敏感信息，并上报事件，用户可以查看并处理。

- 暴力密码破解

  实时发现暴力破解行为，覆盖主流操作系统，根据自定义检测规则可检测到暴力密码破解行为，并通过主动防御机制，可实时检测，并上报事件，用户

可查看和处理。

- 访问恶意域名

  实时监控域名访问行为，当检测到访问恶意域名，通过主动防御机制，可实时阻断，并上报事件，用户可查看和处理，同时支持用户自定义恶意域名库，满足用户实际业务需求。

- 异常登录

  实时监控主机登录行为，包括对于异常地点、异常事件、异常用户及 IP 等异常登录行为进行检测，当检测到异常登录行为时，通过主动防御机制，可实时阻断登录行为，并上报事件，用户可查看和处理。

- 可疑命令

  记录主机上执行的命令，实时监控被事件规则定义为可疑操作的命令，根据规则定义触发事件，并生成事件，用户可查看即处理。

3.6 系统加固

云影-内网主机安全监测系统提供系统加固相关功能，可对系统资源、外设、文件、注册表等进行实时监控，并对违规进行记录日志并上报事件，供用户查看及处理。

- USB 文件监控

  实时监控 USB 设备中的文件操作，并上传操作日志至管控中心，用户可查看具体的操作信息；

- 注册表变更

系统内置关键注册表路径，并支持用户根据自身需要自定义注册表监控路径以及防御手段，根据配置策略实时监控记录日志并生成事件，用户可查看及处理。

- 文件防篡改

  用户可自定义要监控的文件路径及文件类型，以及允许对配置的路径及文件操作的进程，系统根据配置的规则进行实时监控，检测到违规操作可根据防御手段进行阻断，并记录日志以及上报事件，用户可查看即处理。

- 日志异常删除

  实时监控系统日志异常删除行为，检测到异常删除系统日志的行为，记录日志并上报事件，用户可查看及处理。

- 外设管理

  云影-内网主机安全监测系统可对于 USB 存储设备、其他设备（如蓝牙、光驱等)、打印机、刻录机进行实时监控，用户可自定义允许使用或者禁止使用、允许打印哪些文件等，根据规则设置检测到违规操作就会记录日志并生成事件，用户可查看即处理。

- 资源监控

  为了更方便的管理和维护主机，云影-内网主机安全监测系统对主机上的系统资源及进程资源进行监控，主要包括 CPU、内存、磁盘、网络 IO 的监控。可以对主机资源进行报警设置，当在一定时间内超过设定的阈值就会记录日志并生成事件，用户可查看即处理。

3.7策略模板

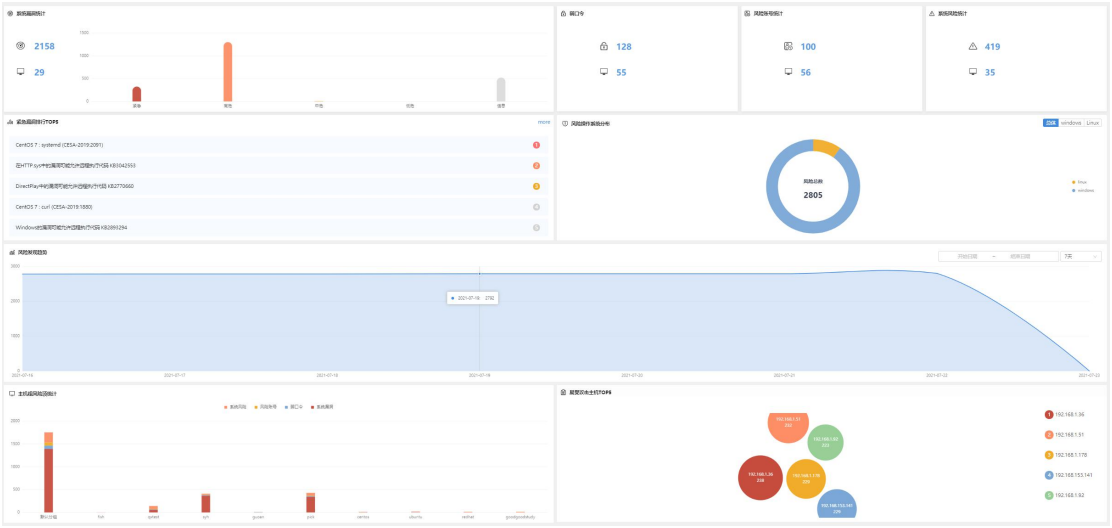
不同的企业对于安全防护有着不同的侧重点，以及不同的业务场景。云影-内网主机安全监测系统提供策略模板功能，提前预置适用于多种业务场景的策略模板，如个人终端防病毒、主机监控审计等，可直接使用，快速应用给资产。

3.8合规基线

如今所有企业单位网络安全建设都需要满足来自于国家或监管单位的安全标准，云影-内网主机安全监测系统提供合规基线功能，支持对国家等级保护的合规检查，并涵盖多个版本的主流操作系统，并可根据资产操作系统信息，自动筛选出适用的系统基线，同时支持自动周期检测，提供给用户检测结果及修复建议，并支持以报表形式导出合规基线检测结果，方便用户查看。

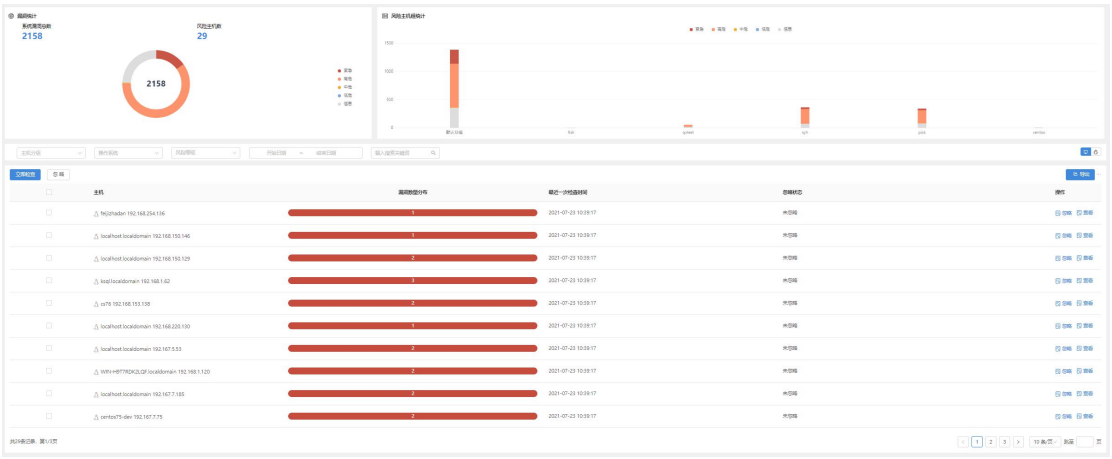
3.9风险发现

云影-内网主机安全监测系统提供风险发现功能，包括漏洞管理、系统配置风险、账号风险检测。知道创宇致力于帮助用户主动且精准的发现内部风险，帮助安全团队快速定位问题并有效解决安全风险，并提供详细的资产信息、风险信息以供分析和响应。



- 漏洞管理

当前超过 90%的攻击事件都是利用未修复的漏洞，云影-内网主机安全监测系统提供漏洞管理功能，可根据用户需求对系统漏洞进行周期性、持续性的扫描，化被动为主动，并提供检测结果以及修复建议等。同时图形化展示扫描结果，动态展示漏洞发现趋势。



- 账号风险检测

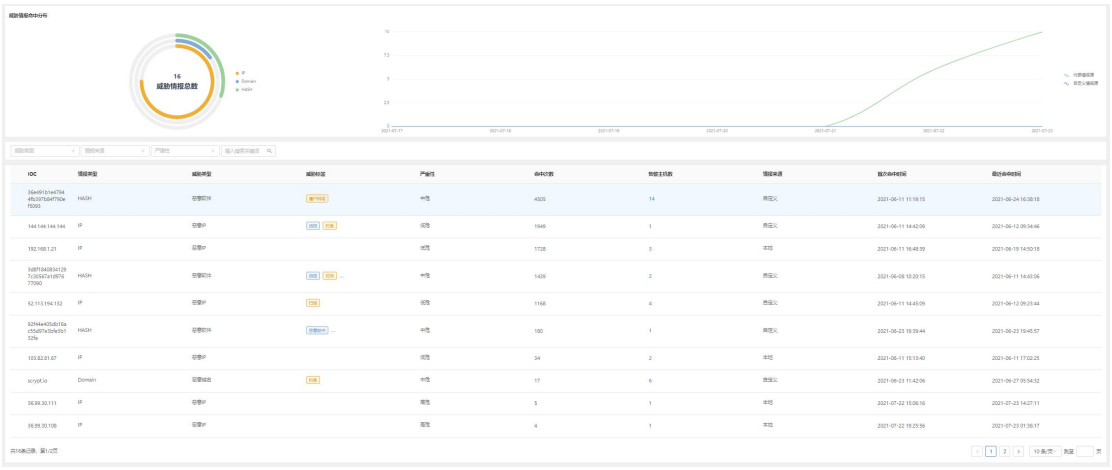
当资产存在风险账号或弱口令时，其被黑客攻陷的可能性可谓是直线上升。云影-内网主机安全监测系统支持对于系统风险账号、弱口令的精准检测，并提供检测结果及修复建议，能有效预防被黑客破解的风险。

- 配置风险

  当系统存在一些配置风险时，黑客很可能会通过这些配置成功攻入，比如未设置密码复杂度、存在失效未删除账号等，知道创宇系统可针对配置风险进行持续性检测，并提供检测结果及修复建议。

3.10 威胁情报

云影-内网主机安全监测系统提供内部情报源，并支持主流第三方情报源，可对恶意软件、恶意 IP、恶意域名等威胁进行检测，及时发现和响应告警事件，并可根据威胁事件历史进行溯源分析，快速定位威胁。

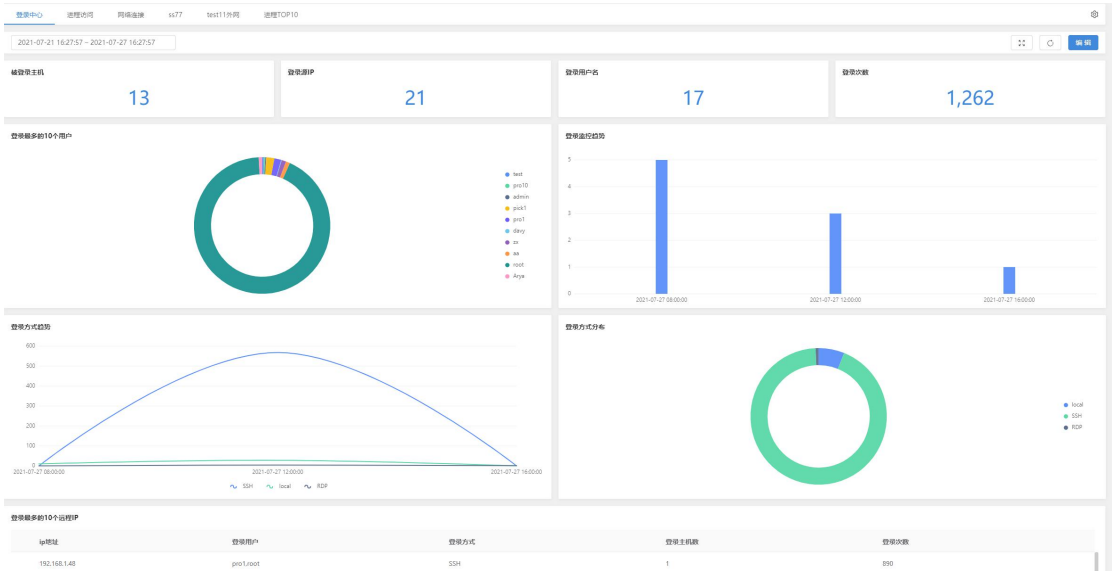


3.11 日志分析

无论是攻击溯源，还是研发安全技术对抗攻击，数据都是重中之重，有庞大的数据支撑，才可以在当发生攻击时，快速进行调查分析，确定攻击者的攻击手段以及被攻击的根本原因，并“对症下药”。

- 云影存储关于每个主机端点的详细信息，包括但不限于进程运行、命令行操作、文件访问、网络链接、配置变更等，共计 70+种主机行为日志；

- 可自定义日志字段，并支持日志字段统计，对每个日志字段都可进行字段值、数量以及百分比统计，并可一键正选及反选；
- 支持关键字搜索、多个条件组合搜索等，即使用户不了解查询语法也可快速创建查询条件，从而使得安全响应人员能够对大量数据执行复杂的查询，并在易于理解的界面中呈现结果。
- 支持对搜索的日志结果自定义创建统计图表，当前支持多种统计图表，包括但不限于柱状图、饼图、面积图、折线图等。
- 系统内置仪表盘功能，同时支持用户自定义，实现用户无需看复杂的海量日志就可了解主机的运行状况



3.12 报表管理

云影-内网主机安全监测系统提供报表功能，报表系统帮助用户进行各类数据的报表导出；对报表文件进行管理。

- 可创建一次性报表或者周期性报表

- 可对报表内容进行自定义
- 支持：安全巡检报表、风险发现报表

4. 通用功能

4.1 告警通知

云影支持邮件告警、短信告警、企业微信告警等 4 种告警方式；可灵活选择接收的告警内容，包含威胁事件告警、系统告警；同时用户可自定义告警主题、紧急程度等。

4.2 权限管理

云影提供权限管理功能，包括用户管理、角色管理功能。其中用户可根据企业内部人员所属部门以及权限范围创建不同的角色和对应的用户账号。

4.3 操作审计

云影-内网主机安全监测系统提供操作审计功能，记录用户在系统上的操作，方便快速查看操作详情以及后续追溯失败操作或误操作的原因等。

4.4 Agent 运行保障

云影-内网主机安全监测系统由三部分构成，分别为 server、Agent、Web 控制台。

- Server

Server-服务器作为云影的中心枢纽，将所有 Agent 收集的信息集中管理；采用 B/S 架构，独立部署在服务器或者 linux PC 上，安装完成后，用户可以在任意与 Server 网络可达的计算机上访问 Server 的 Web 控制台页面，对终端进行集中策略下发及管理；

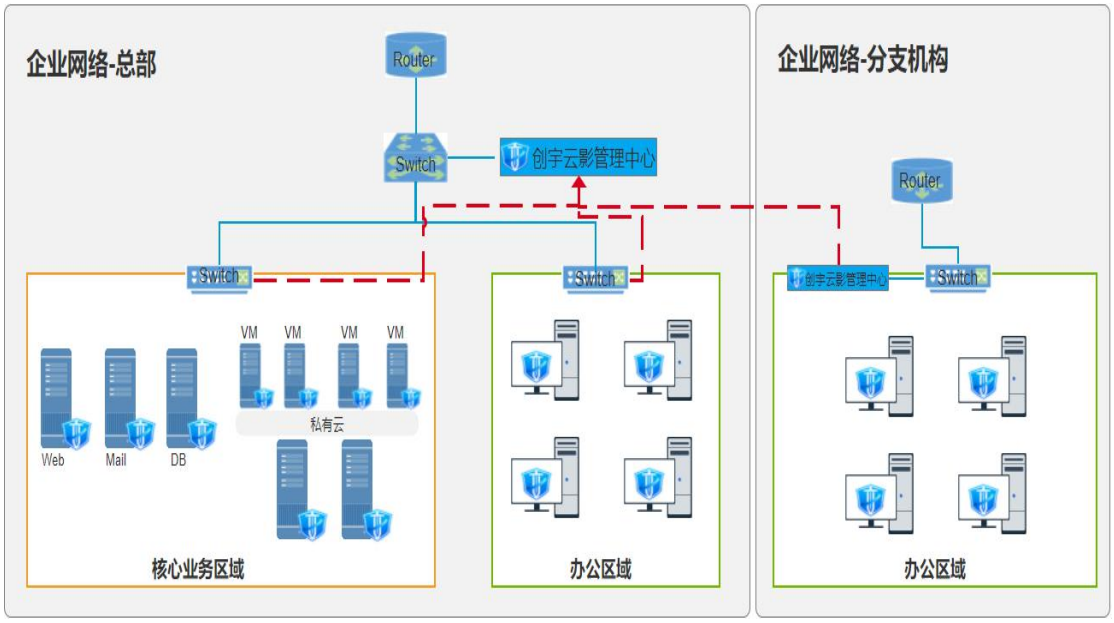
- Agent

Agent 安装在需要被管控的主机上，安装便捷，可通过命令直接安装成功，且覆盖主流的操作系统。

- Web 控制台

云影提供 Web 控制台，以 Web 控制台的形式和用户交互，可清晰展示各项资产统计情况、安全检测及分析结果等，方便用户处理安全告警事件，以及攻击溯源，综合分析等。

5. 产品部署



- 快速部署

  支持命令与脚本自动安装

- 稳定运行

  持续监控探针稳定性状态，最小化原则运行

- 超低负载

  低负载运行，最大程度保证探针 主机业务连续性，支持自定义负载阈值，CPU 占用不超 1%，内存占用不超 100MB

- 超轻量级

  服务端单台服务器即可运行，探针负责数据采集与状态监控，管理端负责安全分析与状态管理。