CSA GCR cloud security alliance GREATER CHINA REGION ®

网络基础安全之XDR扩展检测与响应平台

联盟简介

云安全联盟（Cloud Security Alliance,CSA）是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区（Cloud Security Alliance Greater China Region, CSA GCR）作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息

加入我们

CSA大中华区官网
(https://c-csa.cn)

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

《网络基础安全之 XDR 扩展检测响应平台》由 CSA 大中华区 XDR(扩展检测与响应系统)项目组专家撰写，感谢以下专家的贡献：

项目组组长:

吴湘宁　　顾立明

主要贡献者：

谢琴	计东	马权	严冬	毛备	曾永红
崔鉴	罗川	邢海韬	赵锐	岳炳词	张睿

参与贡献者:

车洵	陈昊闻	程碧淳	丁俊贤	董天宇	顾伟
何维兵	胡钢伟	刘斌	刘国强	刘涛	欧建军
潘海洋	舒庆	孙亚东	谢泳	余滔	郑亚东
周海生					

研究协调员：

蔺鹏飞

贡献单位:

北京天融信网络安全技术有限公司	中移(苏州)软件技术有限公司
杭州安恒信息技术股份有限公司	杭州极盾数字科技有限公司
奇安信网神信息技术(北京)股份有限公司	上海物盾信息科技有限公司
深信服科技股份有限公司	沈阳东软系统集成工程有限公司
腾讯云计算（北京）有限责任公司	网宿科技股份有限公司
新华三技术有限公司	亚信安全科技股份有限公司
中国电信股份有限公司研究院	中兴通讯股份有限公司

(以上排名不分先后)

关于研究工作组的更多介绍，请在 CSA 大中华区官网（https://c- csa.cn/research/）上查看。

在此感谢以上专家及单位。如此文有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正！联系邮箱 research@c-csa.cn；国际云安全联盟 CSA 公众号

序言

当前全球正在快速踏入数字化世界，无论是国家、政府、企业还是个人，都身处数字化的洪流之中。数字化手段正在有力地提升国家与政府的施政效率，并持续推动科技和企业的快速更新。

正如光影的两面性，数字化也蕴含着利弊并存的风险。不断涌现的网络安全挑战启示我们，网络威胁的严重程度日益加剧。随着黑灰产业服务化、武器化、组织化的兴起，以及 AI 技术的突破，网络攻击的门槛将大幅降低，黑客的攻击能力也将得到大幅度提升。而数字化程度的提高，使得网络资产的价值不断攀升，同时也加大了网络的风险暴露面，从而导致网络攻击的数量呈现增长趋势。如何应对日益猖獗的网络攻击，XDR（扩展检测响应）平台无疑成为当前不可多得的选择之一。

XDR 平台内建各类关键的网络安全检测功能，并将终端、网络、云/容器、网关、邮件、Web、蜜罐、沙箱等产品的核心能力标准化。平台通过开放的标准，构建了一个即插即用，灵活拓展的检测响应平台。全方位的攻击面风险洞察、高清的遥感数据与平台威胁感知模型相结合，使智能辅助、自动化运营成为现实，有效降低安全管理难度，提高日常运营效率。相较于传统的产品加平台集成方案，XDR 方案避免了平台与产品之间的能力断层，以及后期集成维护的困难。但 XDR 方案并非完美无瑕，在超大规模解决方案中，XDR 可以作为统一集成单元，降低整体集成与维护成本。

期望《网络基础安全之 XDR 扩展检测响应平台》能为大家提供参考，亦能启迪相关领域的发展。

李雨航 Yale Li

CSA 大中华区主席兼研究院长

目录

第一章概述

1.1 安全行业发展背景

20 世纪 80 年代中后期，计算机病毒和网络蠕虫的出现，催生了网络安全行业，最早的商业化网络安全产品如反病毒软件、防火墙、入侵检测系统等陆续面世。将近 40 年的时间内，计算机网络所面临的安全威胁已经从感染或入侵单机发展成有组织地发动大规模网络攻击（如分布式拒绝服务攻击、钓鱼、勒索、挖矿等），从单一的漏洞利用发展成采用多种组合式攻击手段进行高级定向攻击（如国家级和商业级的 APT 等）。而与之对应的，网络安全防御的理念和技术也在不断演进，从静态、被动的传统安全架构，逐渐向动态、主动的综合防御能力体系发展。

20 世纪 90 年代，国际著名安全公司 ISS 提出了防护、检测和响应的安全闭环模型（PDR 模型），这是最早体现动态防御思想的一种网络安全模型。该模型强调在了解和评估网络系统安全状态的基础上，通过实施安全加固和调整安全策略等手段形成快速抵御威胁的能力。

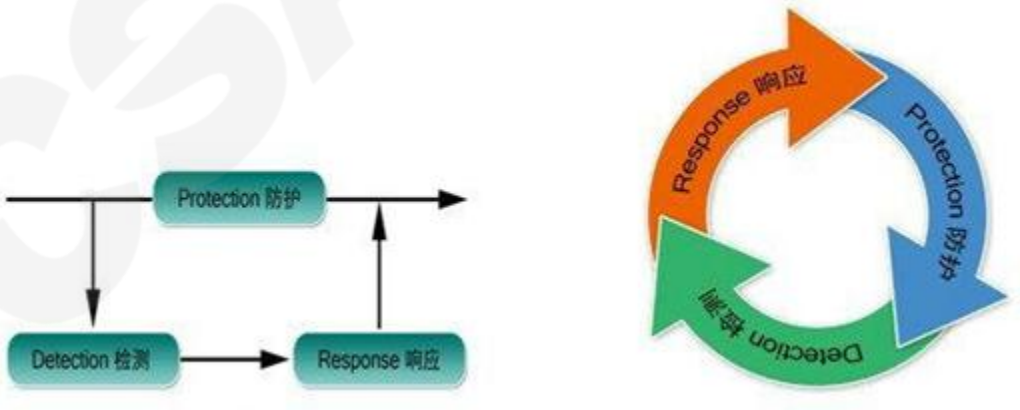


图 1-1 PDR 模型

然而在 PDR 模型中，“检测”受限于当时的技术发展水平，更多强调基于特征的已知攻击检测和基于统计的异常行为检测，威胁类型覆盖面窄，未知威胁

发现能力不足，而且基于“应急响应”式的安全防护框架，已经不再适用于充斥着各类高隐蔽性、高复杂度的新型威胁的环境。

2014 年，各大国际知名安全机构纷纷发布新的安全理念模型，旨在帮助安全行业更积极地应对新型威胁的挑战。SANS 提出的网络安全滑动标尺模型着重强调基于态势感知的动态防御和基于威胁情报的主动防御能力构建。NIST 发布的企业安全能力框架（IPDRR）则延续了 PDR 模型的概念，扩展了保护、检测和响应环节的内容，并增加了识别和恢复两个环节，形成了更全面的动态风险控制闭环。Gartner 提出了集防御、检测、响应、预测于一体的自适应安全框架（ASA），以持续监控和分析为核心，形成一个可持续自我完善的闭环，让安全防御体系能够适应环境的变化而自动进行安全保护功能的提升，以有效应对未来更加隐秘、专业的高级攻击。

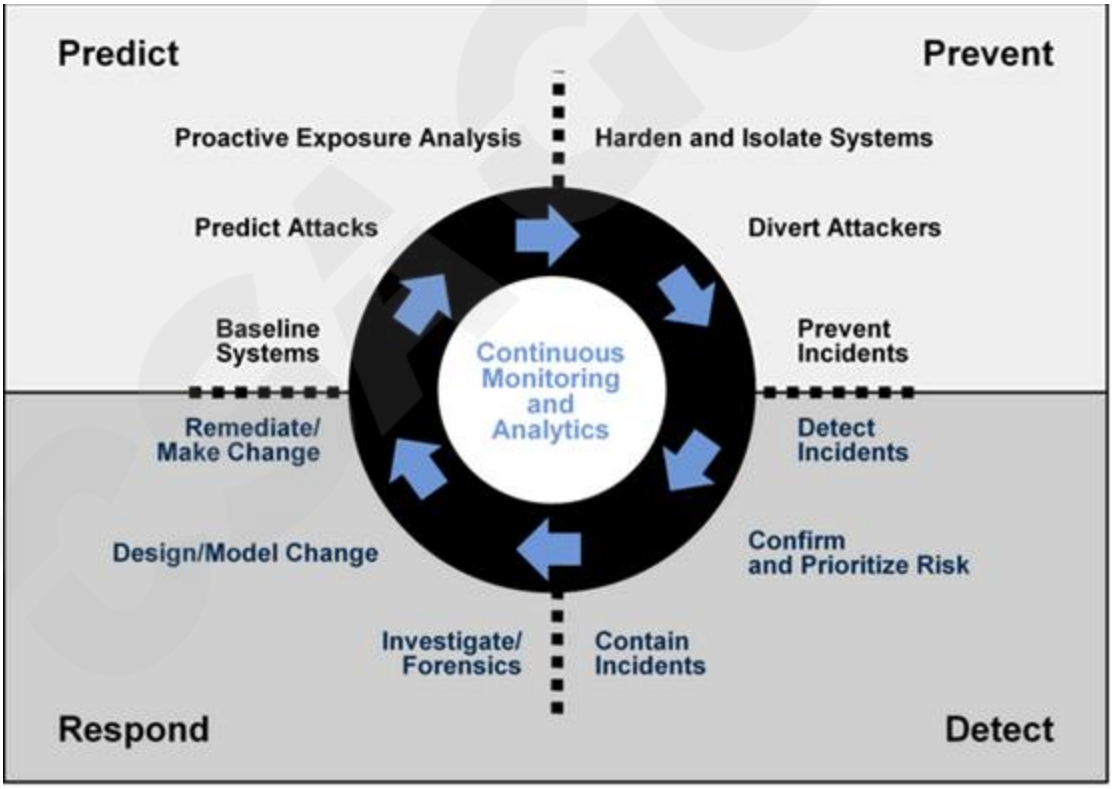


图 1-2 自适应安全框架（ASA）

经过两次迭代，自适应安全框架已经进化到了 3.0 版本，即持续自适应风险与信任评估（CARTA）。随着该框架理念的不断完善，越来越多的安全功能被加

入到其中，但其所追求的目标始终未变，即构建一个整合不同安全功能、共同分享信息并更具适应性的智能安全防护体系。该框架对整个网络安全行业所带来的影响极其深远，也推动了诸多安全产品和相关技术的发展演进。

以下一代防火墙的技术发展为例，早期的下一代防火墙中虽然集成了各种2-7层的检测能力，但都是基于已知的特征和事先配置好的规则进行检测和过滤，无法根据最新的安全隐患或网络威胁进行实时更新，只能通过与其他检测类产品联动来阻断新发现的威胁，反应比较滞后。而机器学习、威胁情报等技术的成熟改变了这种被动防御的局面，通过在防火墙中集成AI引擎和未知威胁检测引擎，并与后端的漏洞库、威胁情报库进行同步，可准确发现各种新型威胁和异常行为并实时阻断，真正在网络边界形成了安全防御和检测的动态闭环。

过去10年间，许多新的安全产品不断涌现，例如安全态势感知（SA）、终端检测与响应（EDR）、网络检测与响应（NDR）、安全编排自动化与响应（SOAR）等；一些传统安全产品的功能也发生了巨大变化，如网络流量分析（NTA）、安全信息和事件管理（SIEM）等；这些新的产品或新的功能都在不断丰富和增强现有的安全防护体系。然而，在企业安全运营和网络攻防实战过程中，人们发现“检测”和“响应”之间却仍然存在着巨大的能力鸿沟，对高级威胁的发现和防御效果并未达到预期。在这样的背景下，XDR应运而生。

1.2 XDR的概念与构成

根据Gartner对XDR的定义，XDR是一种基于SaaS的、特定于供应商的安全威胁检测和事件响应工具，将多个安全产品集成到统一所有许可安全组件的内聚安全操作系统中。XDR包含了前端感应处理能力和后端分析决策能力。其中前端包含了终端检测与响应、云工作负载防护平台、网络威胁检测与响应、Web安全网关、邮件安全网关、身份识别与访问管理、蜜罐与沙箱等，后端包含了威胁情报、数据湖、AI引擎分析、高级威胁分析引擎、事件分析算法、无代码自动化编排剧本、API注册与编排、持续集成和持续部署(CICD)等。

1.3 XDR 的核心能力

作为一类技术路径，XDR 所包含的技术点众多且关系复杂。在 Gartner 的报告《Innovation Insight for Extended Detection and Response》中，曾经列举了 XDR 可能包括的安全组件就有近 10 种，更勿论每个组件往往会包含多种技术。从环境讲，XDR 需要考虑终端、网络、数据中心、云等不同的环境；从安全运营过程讲，XDR 需要覆盖数据采采集、检测、分析、遏制、清除、加固等多个阶段，以及情报的生产和共享。

但 XDR 的定位出发，可以认为有 3 种技术的重要性最为突出：

1.3.1 全面的遥测数据采集

XDR 要让安全运营人员在一个工作界面中，完成检测、分析、响应的绝大部分工作，以显著提升工作效率，需要保证工作需要的所有数据可以在这个平台上方便地获得，减少在不同设备间切换的成本；除此之外，完备、详尽的数据采集，也是威胁关联分析、精准响应与处置不可或缺的基础。

1.3.2 高级威胁狩猎

XDR 需要发现各种具备高度绕过、逃避技巧的攻击，需要发现针对性极强的定向攻击，这就意味着 XDR 必须提供基于攻击技战术的行为检测能力——威胁狩猎；进一步考虑到狩猎专家的稀缺性，XDR 不可能依赖以人为主的狩猎，而更多需要基于 AI 或者机器学习的方式，以多维检测形成合力，方能应对各种复杂场景下的攻击威胁。

1.3.3 自动化响应

对于已经渗透到内部的攻击，需要尽快停止攻击的发展；同时识别出关键风险，进行完整的危害清除，并对被利用的薄弱点加固处理。整个过程非常注重时效性，需要抢先在攻击者之前完成，因此必须依赖自动化的机制，才可能有效的提升 MTTR。

1.4 XDR 的发展历程及趋势

XDR 发展至今，主要经过了以下四个阶段。

阶段一，关注终端安全。在互联网早期，网络安全关注在端点安全上，而杀毒软件类产品是主要的应对产品。在 2014 年 EDR 入选 Gartner 十大技术，区别于传统的被动式防御，EDR 在技术上通过记录分析终端行为与事件形成“主动防御”。EDR 作为终端安全产品，相对轻量、便捷。

阶段二，从终端覆盖到网络。网络安全检测与响应以往依靠 IDS 产品等产品，其通过签名指纹匹配的检测方式，主要针对当前已知的网络攻击进行检测，同时为了平衡威胁检出率和威胁检测效率，IDS 特征库往往会根据业务和资产情况进行不同程度的裁剪，这就意味着 IDS 产品的检测技术不仅无法检测新型变种威胁，对于一些已知威胁也可能存在漏检。NDR 技术不依赖于特征库，也不基于某个特定业务或资产对象，它主要通过使用机器学习技术，基于规则的检测和高级分析来检测企业网络中的可疑活动，极大的提高了安全运维效率。

阶段三，安全运营的转变和对网络的流量追踪溯源。随着信息化的发展，企业所面临的安全风险逐步和自身所具备的安全资源和能力发展不足形成了巨大的落差。Gartner 在 2016 年提出 MDR（可管理的威胁检测与响应），MDR 为安全工作提升了自身威胁检测、事件响应和持续监测的能力，同时又无需依靠企业自身的能力和资源。MDR 通过安全运营，联动网络中其他服务供应商提供的不同层面的攻击检测设备的威胁数据进行分析，通过机器学习模型发现以往不易发现的威胁，结合其他网络威胁检测技术使得问题定位和溯源得到了提高，进而提高了响应速度。

阶段四，更高效的运营和更精准的检测。2018 年 Gartner 十大安全项目中，EPP 与 EDR 以组合形式出现，这种基于端点而获得高级威胁检测、调查和响应的能力与 UEBA（用户行为分析）并列统称为“检测和响应项目”。这一趋势预示着更多的新兴技术将应用到威胁和检测中。在 2020 年 XDR 入选 Gartner 九大安全趋势，根据 Gartner 的定义，XDR 是指特定供应商提供的威胁检测和事件响应

工具，这种工具统一将多个安全产品整合在一个安全操作系统里。因此，XDR 将是整合性的产品组合和并具有更精准的检测能力。

未来 XDR 将持续发展，我们预计有以下趋势：

其一、扩大安全监测和响应的范围。XDR 所覆盖的范围将不仅包括云、网、边、端的流量和日志，也将涵盖威胁情报等更为全面的安全大数据。同时也可以通过 XDR 项目来推动不同安全产品、安全厂家之间存在的互相联动等问题。

其二、分析能力和安全效率的提升。通过工人智能、中台、自动化编排、及安全分析等技术，能缓解安全样本数据不充分、安全人员数量和能力不足，难以快速应对安全风险等问题，同时更好的发掘未知风险，提高安全防护能力和效率。

安全技术近年来不断推陈出新，XDR 将融合广泛的安全能力和新型的信息化技术，通过对安全能力的全面协同，形成一个上下联动、前后协作的整体。同时，XDR 刚刚起步，要成为普适性产品还行进一步探索和发展，XDR 的未来需要各个安全厂家和机构的共同参与和努力。

第二章 前端感应器能力

2. 1 终端检测与响应

2.1.1 EDR 的概念

随着威胁攻击的专业化，APT 等定向高级别攻击案例也越来越多，APT 攻击具有针对性强、组织严密、持续时间长、隐蔽性高、采用技术手段先进等多种特征，检测相关的攻击给安全行业带来很大的挑战。对于攻击者而言，内网终端和主机既可以作为被攻击目标，也可以作为攻击的跳板。勒索病毒和 APT 结合的攻击方式也开始逐渐显现，同时针对我国关键基础设施的 APT 攻击也开始愈演愈烈。

传统的终端安全解决方案 EPP 是基于已知风险产出的文件特征库和规则库，无法用于检测未知风险。不同于传统的签名检测或启发式技术，EDR 通过观察攻

击行为将检测技术提升到新的层次，能真正解决终端安全所面临的 APT、0day 和勒索病毒等各类高级威胁，做到事前预防、事中检测和事后修复，是面向未来的终端安全解决方案。

EDR 主要通过在终端上提供安全事件的完整可视来检测和防范未知风险。通常，攻击者潜入到企业网络内部后会持续很长一段时间，其攻击手法比较隐蔽，企业一般很难直接检测到其攻击行为，更难形成有效的攻击告警机制。为了更好地解决这种问题，EDR 采用了记录攻击者行为和系统事件地方式，所有终端行为信息都会被完整地记录下来，整个安全事件从发生了什么、如何发生、到如何修复等所有环节信息都会被完整地记录并以图形化方式展示出来。

EDR 能力成熟度模型，一般包括初级、中级、高级、SaaS 化和智能化四个等级。初级只有 EPP，对于企业用户来说，面对高级威胁是非常脆弱的，无法防护，也无法检测到高级威胁攻击；中级拥有有限的 EDR 场景，终端能够将收集到的攻击行为数据，以及系统级事件上传到云端，但云端大数据的处理和安全能力分析都比较缺乏；高级为标准级 EDR，能够实时检测到安全攻击事件，限制终端漏洞利用，同时基于云端的数据和安全能力分析，给终端提供快速的响应，以及修复指导建议；SaaS 化和智能化 EDR 在云端通过 SaaS 服务的模式提供安全大数据的存储、处理及分析能力，利用云端海量大数据、实时威胁情报以及机器学习能力，安全专家可以精准威胁狩猎，快速进行安全事件响应。

2.1.2 EDR 核心价值

在传统的终端安全解决方案的保护下，仍有大量的安全事件起源于端点。对于企业而言，部署并成功实施 EDR 的核心价值在于：

1、快速侦测与自动化响应

对于终端威胁的快速发现并采取自动化响应是 EDR 的基础。对于安全运营而言，时间是一个非常关键的要素。威胁在环境中存在的越久，就有可能带来越大的破坏。因此，尽早的发现威胁并进行响应是 EDR 带来的最核心的价值。而

自动化响应能力则会进一步加快针对威胁的处置的速度，降低安全隐患。

2、主动检测未知威胁

传统意义上的终端防护是通过将攻击模式与已知威胁的特征库进行比对从而发现安全威胁；因此几乎不具备对于未知威胁和潜在的 APT 攻击的抵御能力。EDR 对于终端进行了更全面的数据采集，进一步加强了可见性。通过对这些数据的的关联分析，EDR 具备了一定的预判能力，从而能够主动发现未知的安全威胁甚至应对 APT 攻击。因此市场上的 EDR 解决方案通常也都具有威胁情报、机器学习以及更高级的文件分析能力。云化的 EDR 则拥有了更广阔的视野和更强大的头脑，对未知威胁的侦测能力也就更加强大。

3、简化管理

普遍认为传统的 EDR 方案中，R 的能力稍有不足。这实际上是在指在自动化响应策略（编排剧本）层面由于缺少足够的信息支撑而在实践中有所不足。EDR 本身具备对终端完整的控制能力。通过集中化的管理平台，安全人员能够远程的进行针对终端的威胁处置，溯源取证，灾害恢复等工作。为企业 IT 运维和安全管理都提供了便利。

由于 XDR 具有更为全面的视野和更强大的后端能力，在 XDR 解决方案中，EDR 专注于终端层面的数据采集和操作的执行。EDR 是 XDR 方案中检测与响应能力在终端层面的重要组成，为 XDR 在终端层面提供了可见性与可控性。作为 XDR 在终端层面的感应器与执行器，EDR 能够协助 XDR 方案进行终端资产理清，攻击面梳理，以及风险管理。

2.1.3 EDR 核心能力

1、数据采集

EDR 需具有全面的终端数据采集能力，涵盖系统层、应用层行为数据，包括系统操作、进程、文件、网络、注册表等多个类别数据，为攻击全面分析提供丰

富数据源，提升威胁研判的精准度，减少误报，也为未知威胁的检测和发现提供数据基础。对于 SaaSEDR 来说，这些数据存储在中央数据库或数据湖中，通常托管在云端。

EDR 的数据能力体现在数据采集和分析能力上。只有采集足够完整的数据，才能实现对未知威胁的检测，以及对安全事件的溯源等，否则就无法进行有效的分析。因此，EDR 必然需要强大的数据采集能力，能采集到端点上的各类关键数据。不同厂商会对采集数据有不同的分类方式，在采集数据的种类上也会有一定区别。

EDR 数据采集的价值在于分析，能否有效地关联各个端点采集到的数据，并且分析后检测出威胁非常重要。在数据采集过程中，即使数据采集得足够多，在分析阶段一旦无法被合理使用，也是没有价值的。因此，EDR 的数据采集不是采集所有数据，而是围绕终端威胁检测和分析所需要的数据尽可能完整的采集。基于 ATT&CK 矩阵的技战术是数据采集标准的重要参考。

EDR 的数据采集能力对 XDR 来说，一方面通过网络数据、云上数据等其他数据，与终端数据进行关联分析，发现真实的攻击事件，还原完整的攻击路径，另一方面为终端攻击溯源提供数据支持。XDR 解决方案下要求数据格式“统一”，但现状是各家产品接口均不一致，也给 XDR 整体解决方案提出了挑战。企业在选择 EDR 厂商的时候，对于单点能力突出的厂商，还需要考虑其数据输出能力。这需要 EDR 产品能够和多个不同安全厂商进行数据对接，同时输出的数据也应该尽可能是更为有效、有价值、经过处理的数据，而不是将大量的原始数据直接进行输出。

不同部署形态对数据采集能力上也略有差异。本地化部署的 XDR 平台相对 SaaS-EDR 来说，前者对数据传输带宽小，传输安全性相对较低，后者则相反。

2、入侵检测

EDR 的入侵检测能力，旨在根据动态行为进行异常登录检测、口令暴力破解、

恶意行为检测等入侵检测行为。业内一般根据 ATT&CK 矩阵实现对各类入侵、攻击及新型未知攻击的持续检测。

众所周知 ATT&CK（全称 Adversarial Tactics, Techniques, and Common Knowledge ）是一个攻防战术框架，反映攻击者攻击生命周期中各个阶段的攻击行为模型和知识库，主要应用于评估攻防能力覆盖、APT 情报分析、威胁狩猎、日常监测与检测、攻击模拟及分析与缓解与防御差距评估等场景和领域，站在攻击者的视角来描述攻击过程中用到的战术技术的模型。站在攻击者视角，通过不断地攻防演练测试和评估，学习攻击者的技术和方法，就可以提升安全检测与分析系统的检测能力，不断扩大技术覆盖范围，丰富技术知识库，不断缩小与攻击者的技术和知识差距，其目标是以攻促防，以防验攻。正如《孙子兵法.谋攻篇》书中所述“知己知彼,百战不殆”,在网络作战中也是同样道理,只有更了解攻击者，才能更好地发现自身薄弱环节，从而弥补自身缺陷和优化防御方式，保护企业网络安全。ATT&CK 已成为安全业界通用语言，其框架已成为安全业界标准。

图 1

如图 1 所示，ATT&CK 改变了我们对 IP、域名、哈希和静态特征码等低级威胁指标(IOC，Indicator of Compromise)的认知，让安全业界从行为视角来看待攻击者和防御措施，即攻击指标(IOA，Indicator of Attack)，旨在描述攻击者所使用的攻击战术、技术和过程(TTP，Tactics, Techniques and Procedures)的方法。企业 ATT&CK(v10)将安全事件划分为 14 个阶段，即 14 种战术指导思想(从 v9 开始增加了 PRE-ATT&CK：侦查、资源开发)，在同一次实战攻击场景中不太会同时覆盖全

部的战术，以减少被发现的机率，但其顺序和方向是固定的，理论上通过攻击者的 TTP 分析，攻击者行为方向和目标是可以预测的。高级可持续性威胁的手段和方法越来越贴近用户日常操作，如信息收集、分析工具使用等，具有潜伏性、隐蔽性、持续性、针对性及多样化等特点，攻击力量分散和无明显攻击特征，这也给传统检测方法带来了挑战，威胁分析检测已不能通过常规的单一风险告警和攻击活动来判定，通过 ATT&CK 模型可提升网络攻击感知能力，增加未知威胁检测能力，同时防御方也可以通过该矩阵继续细化未覆盖技术检测点。

EDR 使用高级分析和机器学习算法，在已知威胁或可疑活动发生之前实时识别指示这些活动的模式。

一般来讲，EDR 会查找两种类型的迹象：感染迹象 (IOC)（即与潜在攻击或违规行为一致的操作或事件）以及攻击迹象 (IOA)（即与已知网络威胁或网络犯罪分子相关的行动或事件）。

为了识别这些迹象，EDR 会将自己的终端数据与来自威胁情报服务的数据实时关联，而威胁情报服务会提供关于最新网络威胁的持续更新信息 - 它们使用的策略、它们利用的终端或 IT 基础架构漏洞等等。 威胁情报服务可以是专有服务（由 EDR 提供商运营）、第三方服务或基于社区的服务。 此外，许多 EDR 解决方案还将数据映射到 Mitre ATT&CK。

EDR 分析和算法还可以自行执行侦查，将实时数据与历史数据和已建立的基线进行比较，确定出可疑的活动、异常的最终用户活动以及任何可能指示网络安全事件或威胁的内容。 这些算法还可以将"信号"或合法威胁与误报的"噪音"区分开来，以便安全分析师可以专注于重要的事件。

EDR 对于 XDR 来说，提供终端威胁检测能力，补齐 XDR 在终端上的威胁检测能力不全问题，为后续的事件分析、溯源取证提供分析线头等。

3、脆弱性检测

在信息安全技术《信息安全风险评估规范 GB/T 20984-2018 标准》中对于脆

弱性的解释是“可能被威胁所利用的资产或若干资产的薄弱环节”。 脆弱性一旦被威胁成功利用就可能对资产造成损害。脆弱性依附在资产上，资产具有的脆弱性越多则其风险越大，脆弱性是未被满足的安全需求，威胁者可利用脆弱性从而危害资产。EDR 需要具备对资产脆弱性检测能力，资产脆弱性包含漏洞、弱口令、配置风险等。EDR 检测终端的全部漏洞及未修复漏洞，避免因漏洞利用被攻击。EDR 脆弱性检测为 XDR 资产风险管理提供数据支持。

4、威胁响应

端点检测与响应，除了检测，自然需要响应能力。EDR 能力需要提供一系列响应能力，包括查杀、隔离、告警。从当前的情况来看，隔离能力最为重要，EDR 更需要能尽可能将威胁控制在受攻击端点。微隔离技术能够和 EDR 结合，更好地实现威胁控制。因为对于企业而言，最需要保护的资产是主机；因此，防止威胁在网络中扩散到主机最为关键。

当安全事故发生的时候，需要将威胁因素限制在相关端点之中，避免其扩散到其他端点，甚至主机，将危害限制到最低。另一方面，将威胁限制在少数有限的端点上，也更利于企业在事后进行追踪溯源。

响应策略是否可以做到自动化？在理想状态下，我们会期望响应行为能够自动化进行。但是在实际环境中，会遇到各种问题，包括异常行为难以判定是否属于攻击行为、某些响应行为是否会影响业务等情况。因此，现在的响应机制依然需要靠自动化与人工协同，通过安全策略设置，将大部分安全事件自动化处理，将一些难以区分或者处理的事件交由安全专家手动处理。但是，安全策略的设置对 EDR 的分析能力与策略配置能力也提出了一定的要求。

EDR 通过自动化技术引入"响应"机制（实际上是"快速响应"）。 根据安全团队设置的预定义规则（或机器学习算法随时间推移"学习"的规则），EDR 解决方案可以自动

提醒安全分析人员注意特定威胁或可疑活动

根据严重性对警报进行分类或划分优先级

生成"追溯"报告，以跟踪事件或威胁在网络上的完整轨迹，一直追溯到其根本原因

断开终端设备的连接，或从网络注销最终用户

停止系统或终端进程

阻止端点执行恶意/可疑文件或电子邮件附件

触发防病毒软件或反恶意软件，以扫描网络上的其他终端来查找相同的威胁

EDR 可以与 SOAR（安全编排与自动化响应）系统集成在一起，以自动执行涉及其他安全工具的安全响应运行剧本。这整个自动化流程有助于安全团队更快地响应事件和威胁，最大限度地减小它们对网络造成的损害。

EDR 的响应能力对于 XDR 来说非常重要，XDR 通过调用 EDR 提供的响应能力实现快速的进程查杀、文件隔离、IP 封禁等处置动作。

5、威胁狩猎

威胁狩猎是一项主动式安全活动，安全分析师可通过这种活动在网络中搜索未知威胁或者组织自动网络安全工具尚未检测或修复的已知威胁。高级威胁可能会在被检测到之前潜伏数个月，收集系统信息和用户凭证，为大规模入侵做准备。有效且及时的威胁狩猎可以缩短检测和修复这些威胁所需的时间，并减小或防止攻击造成的损害。

威胁狩猎者可以使用各种策略和方法，其中大多数策略和方法都依赖于 EDR 在威胁检测、响应和调查时使用的相同数据源、分析和自动化功能。 例如，威胁狩猎分析人员可能希望根据取证分析来搜索特定文件、配置更改或其他工件，或者搜索用于描述特定攻击者方法的 MITRE ATT&CK 数据。

为了支持威胁狩猎，EDR 可通过 UI 驱动的方法或编程方式向安全分析人员提供这些功能，以便他们可以执行临时搜索数据查询、与威胁情报进行关联以及进行其他调查。 专用于威胁狩猎的 EDR 工具包括从简单脚本语言（用于自动执行常见任务）到自然语言查询工具的所有工具。

EDR 的威胁狩猎是 XDR 威胁狩猎能力的基础，为 XDR 的威胁狩猎提供数据支持和能力支持。

2.1.4 EDR 应用场景

1、 安全风险态势管理场景

通过对网络空间的有计算能力的终端、服务器等部署 EDR，对终端资源进行风险检测，将检测的数据上送到态势感知模块，实现对网络空间中的计算资源进行风险评估和风险趋势分析。

2、 零信任防护方案场景

在零信任防护方案中，需要感知零信任终端的风险，根据风险动态调整用户的权限。EDR 是其中不可或缺的重要组件。EDR 具备连续和实时数据采集能力，为应对高级威胁提供了更强的可见性；对终端持续评估能力，满足了零信任的环境感知要求，通过对终端的全量信息采集，为判定终端安全状况和安全可信任程度提供更准确的数据。

3、 虚拟化、云场景下的安全防护场景

随着智慧服务的不断建设，云端运行业务成为常态化，虚拟机则成为安全的重灾区。EDR 可以对虚拟化终端、云场景下的终端进行风险检测，不受复杂的虚拟化环境限制，同时通过响应策络控制具备微隔离功能，能够解决云端特有的东西流量访问控制问题。EDR 可以对云主机连入、连出数据的进行采集、分析和展示，可以实现云主机流量的可视化，阻断非法访问、隔离失陷云主机。

4、 工业互联网安全防护场景

在工业互联网安全场景下，通过为智能工业设备、智能工业终端部署 EDR，对智能工业设备进行安全检测，风险评估，在产生风险告警同时可以根据风险事件或风险级别，对智能设备下发动态工业控制指令，保证工业生产安全。

5、 车联网安全防护场景

通过在车联网终端上部署 EDR，可以对车联网终端进行安全风险检测、安全风险预警及安全风险的及时响应，实现对车联网终端的安全管控。

2.2 云工作负载防护平台

2.2.1 CWPP 定义

云工作负载保护平台（Cloud Workload Protection Platform）简称 CWPP，其概念由 Gartner 在 2016 年首次提出，CWPP 是以工作负载为中心的安全产品，保护私有云、公有云，及混合、多云数据中心环境中的服务器工作负载，为物理机、虚拟机（VM）、容器以及无服务工作负载提供统一的可视化和管理能力。CWPP 通常会结合系统完整性保护、网络控制、应用控制、行为监控、入侵防御和运行时恶意软件检测等能力，保护工作负载安全。

2.2.2 部署与架构

部署模式

CWPP 产品一般采用“轻量级探针+统一安全中心+Web 控制台”的架构，为用户提供事前风险发现、事中入侵检测、事后追踪溯源的能力。

探针：一般安装在主机或容器上，能自动适配物理机、虚拟机以及云环境，在威胁检测方面，其功能主要是收集主机操作系统、进程、端口、账号、应用等信息；

统一安全中心：即服务端，其通过收集、分析探针采集的信息和行为，来发现主机侧的漏洞、弱口令等风险，以及 Webshell，反弹 shell，异常进程以及病毒木马等入侵行为；

Web 控制台：以可视化的管理界面和用户进行交互，通过数据分析以及图形化展示等方式为用户提供实时的风险态势以及集中管理的能力。

适用场景

CWPP 为用户提供资产清点、风险识别、入侵检测、实时防护、安全处置以及攻击溯源等能力，覆盖私有云、公有云、混合云、多云统一管理的场景，为用户提供针对服务侧各种工作负载全生命周期的防护以及安全管理能力。

CWPP 与 XDR 的对接

XDR 通过统一的交互框架、数据标准数据存储方式，进行安全数据采集、安全威胁集中分析、安全事件处置及响应编排能力。因此，CWPP 与 XDR 的对接，需要从数据采集、检测与响应方面保持一致性，主要包含如下三个方面。

采集：CWPP 采集工作负载侧的主机信息、日志以及威胁等信息，上报到 XDR 平台的统一安全分析中心。

检测：XDR 后端平台组件进行内部（资产、漏洞等）、外部（流量、日志）等多源安全告警进行关联分析、规则分析以及情报分析，发现潜在的威胁。

响应：XDR 控制台通过可视化剧本编排，对接联动 CWPP，在安全事件发生时下发通知告警，并在必要时自动下发阻断策略，及时完成安全闭环。

2.2.3 风险感知能力

CWPP 能够感知服务器工作负载上的多种安全风险包括资产、威胁、脆弱性和合规基线。资产一般包括组织在工作负载上的主机、应用、数据资产；威胁包含对资产造成损害的某种安全事件发生的潜在原因；脆弱性包括系统或应用弱密

码和漏洞；合规基线包含系统、应用和用户在最小安全需求下的配置和策略。从 Gartner 提供的 CWPP 能力金字塔（如图 2-X 所示）来看，从最基础的加固、配置与漏洞管理，以及高阶的漏洞利用预防，都离不开 CWPP 的风险感知能力。

图 2-2 CWPP 能力金字塔

加固、配置与漏洞管理是安全运营的重要工作，系统加固是指关闭非必要功能、端口和服务，及时进行系统补丁更新维护，和对已验证的漏洞进行补丁修复或升级。CWPP 能够通过资产发现和探测，收集工作负载的基本系统信息，从而在平台侧进行监测和管理。配置即为服务器的配置优化，针对应用和业务系统进行配置，保障系统以及应用的安全，避免因为错配和漏配导致产生安全问题，以提升安全防护能力。漏洞管理是针对操作系统漏洞和应用程序漏洞的生命周期管理，包括但不限于漏洞发现、验证、处置、闭环等跟踪过程。在网络安全事件中，基于漏洞的攻击数量一直居高不下，而最常见的最严重的漏洞就是系统漏洞和 Web 应用漏洞。因为 Web 应用一般对外提供服务，所以必须暴露于互联网之中，因此安全要求极为重要。基于上述的能力要求，CWPP 需要支持基于资产扫描和脆弱性发现，操作系统漏洞管理和应用漏洞管理，能提供标准化、同时支持制定自定义的漏洞防护策略。

在第一层的“加固、配置和漏洞管理”阶段，漏洞修复主要是针对 NDay 漏

洞，但除此之外，漏洞防护还应包含对 0Day 漏洞的防护。0Day 漏洞从利用方式可以分为两类：系统漏洞、应用漏洞。针对系统漏洞，CWPP 可以通过内存防护进行检测，内存防护是内存运行时自我保护技术，因为在工作负载上执行的数据都需要经过内存进行储，所以通过对内存行为的监控可以识别无文件攻击、内存型 Webshell 等基于文件监测无法识别的新型攻击手段。对抗应用漏洞的思路是应用运行时自我保护技术（RASP）。RASP 是从应用内部对关键函数操作的数据进行分析，即使原始请求经过加密和混淆，但是它在应用内传播到最终的底层函数时将会以明文方式被 RASP 截获，因此相比应用防火墙 WAF 能减少大量的误报和漏报问题。基于此特性，RASP 还能为安全人员和开发人员提供更为详尽的攻击链路，包括攻击原始 Payload、代码调用堆栈等信息，方便他们进行漏洞定位、复现以及修复，可以有效发现和阻断 0Day 漏洞的利用。

CWPP 能够通过主动资产扫描对主机上资产、脆弱性进行持续扫描和评估，包括漏洞、弱口令、合规基线等等，从而发现实时威胁以及隐藏的未知安全隐患，化被动为主动，提前预防和防御安全问题的出现，将风险消除在最前沿，从而提高攻击门槛，降低入侵风险。

2.2.4 威胁检测能力

CWPP 是 XDR 关键的部分之一，针对服务端的裸金属服务器、虚拟机、容器及应用，CWPP 既可以在本地完成威胁检测与响应，也可以与 XDR 配合，通过 XDR 来进行大数据分析，然后在 CWPP 本地做出响应。

服务端资产为用户业务的核心资产，拥有高价值的敏感数据，黑客攻击的最终目标就是用户服务端的业务与数据，一旦被攻击成功，核心资料被窃取，带来的影响不可估量。近年来针对服务端的攻击层出不穷，既有传统病毒、基于漏洞的攻击、暴力破解、反弹 shell、恶意提权等已知攻击，也有勒索、APT 等未知攻击，还有利用拿下正常权限账号而发起的恶意业务攻击或拖库行为等。这导致服务端威胁检测变得越来越重要且充满挑战。

为了应对这些安全挑战，作为与 XDR 配合的 CWPP 在威胁检测方面需要具

备以下关键能力。

第一，信息采集能力。任何针对服务端主机的攻击都会留下踪迹，通过完整的信息采集，记录行为信息和攻击事件的上下文，为深度的持续监控、威胁分析、调查取证、追踪溯源打下基础。需要采集的信息有：账号行为、进程行为、网络行为、文件操作、内存访问行为、容器运行行为等，尤其是要把有异常的行为、事件和信息完整地监控并记录下来。

第二，已知威胁检测能力。纵然未知威胁越来越多，但已知威胁的检测能力依然是基础，如果已知威胁检测都做不好，就谈不上难度更大的未知威胁了。在已知威胁检测上，要具备常见病毒检测、恶意文件检测、异常登录、暴力破解、恶意提权、反弹 shell、应用后门、内存安全等检测等，同样这些检测要能覆盖物理机、虚机、容器等各种工作负载。

第三，未知威胁与 APT 检测能力。技术的不断演进，导致攻防双方都受益，攻击者采用新技术，制造新型恶意软件越来越多，如 0Day 及这几年泛滥的各种勒索病毒，针对未知威胁与 APT 攻击，单靠人工进行恶意样本分析并提取新规则或特征码后再进行防御，一方面其难度越来越大，另一方面其时效性越来越难以满足用户的安全需求，新技术的出现，以及 XDR 的发展正是需要解决这个问题，帮助用户从被动防御转化为主动防御。

此外，在威胁检测上，还可以通过 ATT&CK 模型框架中的攻击阶段与攻击技术进行比较和验证，进一步提升威胁检测的准确率，降低误报率。

2.2.5 事件响应能力

事件响应的目标是消除其产生的影响。这依赖于将威胁检测阶段生成的结果转换成可执行的行动方案，并将行动方案拆解成可供响应设备执行的命令准确下达到安全组织中。事件响应在组织安全运营中往往体现为系统性的流程，包括"准备 - 识别 - 遏制 - 根除 - 恢复 - 重建"等过程。

图 2-3 事件响应流程

➢ **事件全流程处理**

威胁告警通过人工或者自动方式可以快速生成事件，按照模板流程，将其提交到不同处置人处理，同时通过内置状态机进行事件维护，保证事件状态的一致性，告警事件的节点状态同时被存储，以支持后期事件回溯。

➢ **安全剧本编排**

安全编排，是指将客户不同系统或者一个系统内部不同组件的安全能力通过可编程接口（API）和人工检查点，按照一定的逻辑关系组合到一起，用以完成某个特定安全操作的过程。不论是自动化编排，还是人工编排，都可以通过剧本（Playbook）来进行表述，为了方便管理人员维护剧本， XDR 平台还提供一套可视化的剧本编辑器，大多数 XDR 平台支持拖放操作，有些还支持直接编写代码来实现复杂流程编排，剧本面向编排管理员，让其聚焦于编排安全操作的逻辑本身，而隐藏了具体的编程接口及其指令实现。

➢ **联动响应**

这种方式通过与 CWPP 联动，对应不同告警事件调用不同的预置处置流程，给 CWPP 下发处理动作完成对告警事件的处置，提升业务系统的安全系数，及响应处置的速度与准确性。

XDR 平台基于多源数据分析技术，能够极大降低检测误报率，平台持续进行检测分析，基于平台分析结果，将告警与 CWPP 进行联动，针对发现的威胁时间进行响应，这些响应方式包括：隔离主机或容器、删除恶意文件、隔离恶意文件、阻断恶意进程、封堵攻击源 IP 等。通过 CWPP 与 XDR 在事件响应上的配合，实现服务端威胁检测与响应的闭环。

2.3 网络威胁检测与响应

2.3.1 NDR 的概念

NDR（Network Detection and Response）网络威胁检测与响应，是一种基于流量的网络侧安全解决方案，其集多种检测技术与一体，不仅能够实现基于签名指纹匹配的传统网络威胁检测技术，而且能对原始网络流量进行学习、训练和优化，形成相对准确且能动态调整的网络流量行为模型，以行为模型作为网络风险和异常判定的标准基线，配合其他网络威胁检测模块（如：动态沙箱、静态 AV、人工智能、威胁情报等）关联分析，进行精细化溯源定位。不仅仅是检测威胁，还可以通过本地控制实时响应威胁，或者支持与其他网络安全工具或解决方案（如安全编排、自动化和响应 (SOAR)）的广泛集成。

NDR 与 EDR 的不同之处在于它不使用代理来深入了解恶意活动，而是依赖网络或虚拟分路器来分析本地和云工作负载之间的流量。

2.3.2 NDR 的价值体现

NDR 是 XDR 体系中针对网络流量采集监控、应急处置的前端执行单元，负责持续监控流经关键网络设备的原始网络流量数据，其核心价值是向 XDR 后端平台提供完整的、全局视角的、真实可靠的网络通信元数据。主要体现在以下几点：

1)南北向、东西向的全方向流量采集、监控

2)集中式、基于硬件的高性能采集

3)隐式的旁路监控，攻击者无法感知是否被监控，痕迹真实性有保障

NDR 通过观察网络上的所有通信流量（包括流入、流出网络边界，以及内部横向流量），在 XDR 后端强大的平台能力支撑下，能够在流量进入网络的第一时间检测到可疑的用户行为、内部传播、未经授权的终端访问等潜在的威胁及异

常事件，并在 XDR 后端平台的协同下，通过手动或自动的方式进行及时有效的威胁处置。

2.3.3 NDR 核心能力

2.3.3.1 流量检测

XDR 是具备多方面安全检测与响应技术的可扩展安全能力，网络威胁检测与响应能力在 XDR 的能力体系中扮演着网络安全维度上的一个重要角色。网络威胁检测与响应系统（NDR）的核心能力之一是流量检测能力。网络型的入侵检测技术通过监视和分析在网络上传输的信息，能截取利用不同传输介质及不同协议进行传输的数据包。然而，随着网络攻击的日益复杂化，网络威胁检测的难度增大，要想快速检测和响应威胁事件，亟需推进下一代入侵检测技术的发展。

为应对新的网络安全环境，下一代入侵检测技术需在数据采集、存储检索、检测分析等方面有更大的进步。网络数据采集更加全面，探测和收集所有重要网段的数据，包括内外网通信和内部通信的双向流量，以通用的格式进行采集，针对流量类型进行更加高效的预处理，形成涵盖历史到当前时间的全流量数据集。在存储检索方面，应用分布式大数据组件，实现高可用、负载均衡、弹性扩展的存储方案；提供原始流量数据、威胁检测结果的快速检索接口，打通海量数据存储和分析利用的对接；使用分布式计算引擎处理和分析数据，实现高吞吐量的、实时或准实时的威胁检测功能。检测分析模块应覆盖更多更全的攻击类型，通过双向流量在“请求-响应”的层面更准确地发现攻击行为以及攻击成败的情况，发现高级威胁，形成对攻击源的画像、资产的安全态势的准确描述，并基于分析出的原子事件，进一步完成降噪、聚合、高风险攻击源挖掘、攻击链分析、溯源取证等高级功能。

在网络流量的检测技术中，异常行为检测是能够检测出已知和未知威胁的检测技术，是当前网络威胁检测研究的热门方向之一。异常行为检测是一个对待检测行为进行二分类的过程。异常行为检测对网络行为有一个正常状态下的期望，通过实际发生的行为与正常期望之间的偏差大小来判断是否异常。若行为偏离正

常情况过多，则有很大几率属于异常行为。

统计的方法是异常行为检测的常用方法。基于特征的方法需要由有经验的安全人员选择出对识别异常行为有帮助的数据特征，进行频率、速率或大小等方面的统计计算，然后与异常阈值相比较来判断是否属于异常行为。此种方式依赖领域知识，计算简单且识别出来的结果准确。基于传统统计学习方法的技术同样需要依靠人工进行特征选择，然后使用统计学习模型针对数据进行拟合学习，能够得到一个解释性较高的统计模型来对新的数据进行判别。基于深度学习的方法对人工介入的依赖最低，能够通过学习得到特征并用于训练模型，模型准确度与数据量和数据质量密切相关，缺点是可解释性差。但深度学习和人工智能是当今的热点，其在网络异常行为检测上的应用研究也吸引了人们的目光。

基于对网络流量监控、检测、分析，网络威胁检测与响应技术具备了实时、准确的网络威胁分析检测能力，能够积极响应安全事件，增强企业内网的安全性。因此，NDR 也成为了 XDR 中举足轻重的组成部分，为 XDR 系统在现网的网络流量分析应用提供了坚实的基础。

2.3.3.2 文件检测

文件检测通常有静态文件检测、动态文件检测、基于威胁情报的检测和基于人工智能技术的检测四类，各检测方式描述如下：

静态文件检测指在不运行程序的情况下，对样本文件进行静态特征检测。支持内置多个反病毒引擎，多个反病毒引擎交叉检测，可检测包括 Shellcode、Webshell、后门程序、挖矿木马、间谍软件、蠕虫病毒、恶意软件、远程木马等，对已知威胁进行基于特征的静态检测和多检测模块交叉验证，最终给出检测结果。

动态沙箱检测是一种通过文件的动态执行行为来识别恶意文件的检测技术，其利用虚拟化技术仿真出组织常用的操作系统和应用环境，然后利用虚拟执行手段使文件运行并捕获其对系统产生的影响，如释放文件、加密文档、增加启动项、API 调用等，并对这些影响进行评估，识别对系统产生破坏的恶意文件；动态沙

箱支持行为签名检测，根据主机或网络行为判断其是否为恶意文件，可支持多种沙箱运行模式,包括 Windows、Android 和 Linux 等类型沙箱，支持对沙箱内样本的流量进行检测、支持反虚拟机和反调试行为检测、支持恶意代码及变种检测，最大限度发现 APT 等未知网络攻击。

通过海量情报数据的采集、分析、验证及生命周期管理后生成威胁情报并内嵌于 NDR 系统或单独部署，形成情报中心，并将从流量中提取出的域名、IP、URL 等与情报系统进行关联比对，进一步确认网络威胁，支持 JA3、JA3S 和 SSL 恶意加密指纹检测，辅助各行业安全运营人员进行运营决策。

基于人工智能检测技术，结合机器学习/深度学习、图像分析技术，将恶意代码映射为灰度图像，通过恶意代码家族灰度图像集合训练卷积神经元网络（CNN）深度学习模型，建立检测模型，利用检测模型对恶意代码及其变种进行家族检测。基于灰度图像映射的方法可以有效的避免反追踪、反逆向逻辑以及其他常用的代码混淆策略。而且，该方法能够有效地检测使用特定封装工具打包（加壳）的恶意代码。在一定程度上解决了特征检测的人工提取困难、行为检测的时间开销大且误报高等问题。对于恶意代码变种和加壳文件具有优异的检测能力，且具有快速、准确率高、误报率低、跨平台检测等特点。

2.3.3.3 关联分析

在 XDR 系统中，来自流量分析的安全事件与日俱增，网络攻击事件的迅猛增加使得安全运维人员疲惫不堪，系统产生的误报事件也增大了安全人员发现真正攻击、分析网络安全状况的难度。若要使得 XDR 在企业应用中能够精准捕获真正的威胁，并且提高安全运维的效率，加快对安全事件的响应速度，就需要对数量众多的网络事件进行关联分析。在大量的原子事件之中，实现对事件的自动化整合、关联，形成攻击链，从更高层面上对攻击过程有整体把握，对攻击场景了如指掌，才能更好地明白攻击意图，为快速有效地响应和切断攻击行为提供基础。主要的关联分析技术有如下几类。

1、基于相似性关联

多个网络事件之间的相似性较高可能意味着它们存在关联。基于相似性的技术旨在依据相似性度量方法衡量多个安全事件的属性值之间的相似程度，对相似性超过预设阈值安全事件进行聚合。因此，此类方式关键在于选择有效的事件属性，提出合理的相似性度量策略来刻画事件之间的相似性距离，从而对相似的事件集进行整合和归并。

网络事件属性如源 IP、目的 IP、事件类型等可作为度量所使用的属性，基于一定时间窗口范围内对网络事件进行聚合。相似性度量策略同样决定了关联分析效果的好坏，事件之间相似性距离的度量方式可以有多种选择，例如欧式距离、夹角余弦等。此类方法需要专家知识对属性和度量策略进行选择。

2、基于因果性关联

网络攻击事件并非孤立存在，攻击者会进行一系列有先后顺序的攻击手段，来达到逐步入侵的目的。在实施前一阶段的攻击成功之后，发起下一阶段的更深入的攻击。因此，基于因果性的关联技术试图找到同属一个攻击链的子攻击事件之间的逻辑顺序关系，恢复出整个攻击的概貌，形成攻击链或攻击图。

首先，为每一类事件定义其前置条件和后续结果，明确哪些事件类型可以导出后续类型事件的发生；然后，针对不同的攻击情形定义出攻击的超类，它包含了一系列具有前后顺序关系的子事件类型，结合一定时间范围，将符合条件的子事件实例按攻击顺序整合到一起，形成超类事件。

基于因果性关联技术是一种时序上的分析方法，寻找事件之间在时间先后和攻击逻辑上符合经验道理的关系。在概率统计方面，可使用马尔可夫链来描绘这个攻击链，以状态转移矩阵表示两个原子攻击事件之间的演变概率。若对于事件的因果性分析只需要考虑前后一步的攻击行为，则此攻击链模型具有马尔可夫性，符合 1 阶马尔可夫链。

3、基于场景化关联

基于场景化关联分析主要是先根据领域知识定义好一些特定的攻击场景，然

后从原子事件中找到符合场景化定义的事件集合，整合成一个大的场景事件。这种技术要求较丰富的安全领域经验。

根据攻击行为的可能发生情况，从一个或一类锚点事件出发，确定其前后存在的各种事件类型，往往选择较为重要的类型作为判据事件类型。所述的锚点事件即是在这个场景当中安全人员最关注的事件，例如隐蔽信道，目的是找到这个事件发生的更强有力的证据。利用场景化分析的过程中，根据锚点事件实例的属性，如源 IP、目的 IP、协议类型、载荷的某些特征等，在时间线上往前、往后检索符合定义条件的事件集合。若找到这样的事件集合作为判据，则锚点事件与判据事件整合成一个更高层次的场景化事件。

4、基于多源数据关联

单一来源的安全数据可能存在某些攻击行为检测不到、攻击信息覆盖不全等不足之处，整合多源数据的关联技术则可以让不同来源、不同类型的数据“互通有无”，得到更完整的安全面貌。

基于多源数据需要对数据进行规范化处理，形成一致的数据形式。由于数据来源多元化，必然存在冗余事件，需要进行去重和降噪。在此基础上，结合其他分析技术，完成基于多源数据的关联分析任务，得到更为全面的分析结果。

2.3.3.4 溯源取证

威胁检测与响应的一个重要应用成果就是溯源取证，XDR 系统提供了事件发生过程的完整的证据链，让受关注的威胁事件从事件结果到原始流量、从攻击产生到意图实现的过程都有迹可循。溯源取证是利用威胁检测及响应结果进行事实反推的环节，针对已检测到的安全事件回溯原始流量数据，寻找出具有说服力的证据来辅助事件调查和司法鉴定。因此，不管是在日常安全运维中，还是在应急响应排查中，溯源取证过程都将起到一个“信而有征”的作用，在后续的应对措施中提供强有力的帮助。

在网络威胁检测与响应系统中，探针镜像到系统的原始流量数据应当被完整

地保存下来，可使用 pcap 包的形式。威胁检测模块对流量数据进行各类网络事件的分析，得到异常事件结果。基于此，进行异常事件的溯源取证工作。

从一个异常事件出发，选择合适的网络事件属性，例如五元组，包括源 IP、目的 IP、源端口、目的端口、协议类型，到原始网络流量 pcap 包中匹配出相应数据，同时利用时间戳定位到具体的流量位置，将检索到的流量数据保存下来，则可以获得异常事件的回溯信息。回溯流量数据记录了攻击者确切的攻击行为、攻击行为网络数据包的原始信息，成为证明异常事件发生的重要证据。

将溯源取证功能集成到 NDR/XDR 中，实现一定程度上的自动化溯源取证能力，能够进一步解放运维和证据收集的人力投入，大大提高威胁响应和司法鉴定的效率，强化了网络威胁检测与响应系统的优势，辅助维护网络空间安全的司法公正。这也将是 XDR 在社会与司法上的一个重要贡献。

2.3.4 NDR 的应用场景

现网中，NDR 通常应用于云上及云下两种场景。

2.3.4.1 公有云环境

云上部署分为两种方式：一是通过在被监控服务器上安装 Agent 插件引流的方式，将进出服务器网络流量复制一份到虚拟 NDR 探针上，以达到网络威胁的检测与响应；二是通过云上服务器网卡流量复制的方式将进出服务器的流量复制到虚拟 NDR 探针上，进行威胁检测与响应。

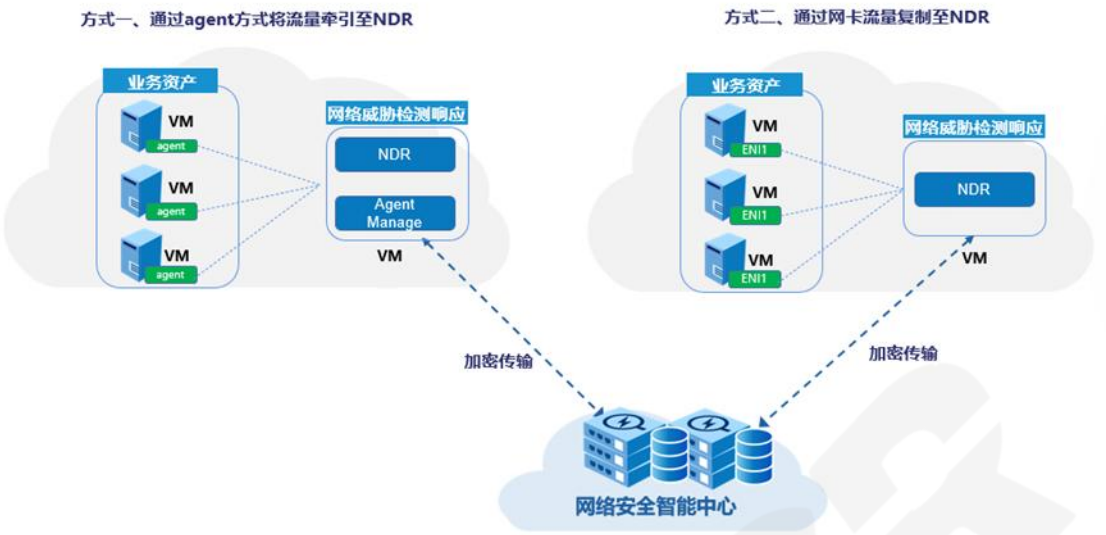


图 2-4 云环境部署示意图

2.3.4.2 本地数据中心

本地数据中心部署为通用部署方式，方式是通过镜像、分光或分流的方式，将南北向进出口流量或东西向横向流量复制给 NDR 探针，以对网络流量里存在的威胁提供检测及应急响应服务。

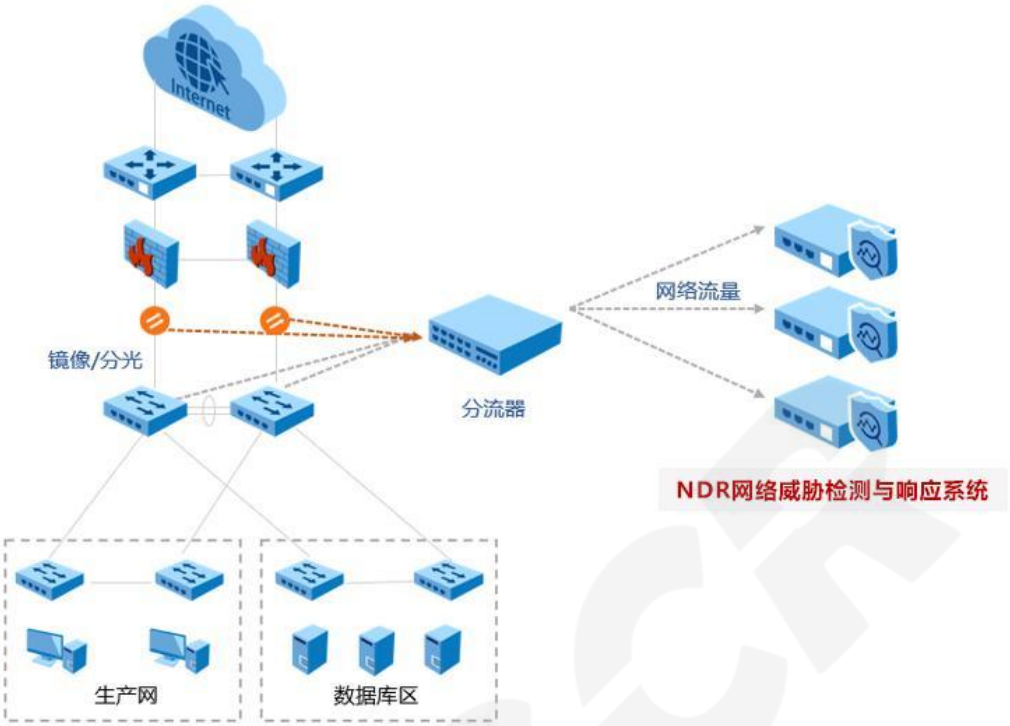


图 2-5 本地环境部署示意图

2.4 Web 安全网关

2.4.1 Web 安全网关的定义

Web 安全网关（SWG）是用来阻止用户访问互联网和云中可能感染其设备的威胁，它特指设备用来防止网络和数据受到损害，并确保企业员工访问符合安全基线与组织、行业数据安全监管的合规性遵从。

Web 安全网关（SWG）采用基于大数据和机器学习的动态分类技术，提供了可扩展的、快速的 URL 分类查询功能，包含了本地基本分类、本地高速缓存分类、云端实时分类查询技术，同时采用了 Web 信誉评分技术，用于根据指定的敏感度级别来识别风险，以及确定是否允许 URL 访问。

2.4.2 Web 安全网关的核心价值

互联网访问过滤，避免外部风险和法律风险；

阻止通过互联网外发机密数据造成企业的损失；

提高内网性能，降低网络拥塞带来的业务质量低下，保证业务连续性并节省 IT 投资。

2.4.3 Web 安全网关的关键能力

一、防病毒能力

Web 安全网关防病毒主要针对 HTTP/HTTPS、FTP、SMTP、POP3 等协议流量进行双向的过滤扫描，防止外部的攻击导致内网被病毒感染并防止内网已感染病毒的客户端和服务器对外扩散病毒。Web 安全网关作为内外网之间的唯一数据通道，可以扫描网络流量中是否存在恶意软件，并查看其是否与已知恶意软件中的代码匹配。一些网关还使用沙箱测试恶意软件，它们在受控环境中执行潜在的恶意代码，以查看其行为。如果检测到恶意软件，则网关将阻止它。

二、Internet 应用控制和带宽管理处理能力

Internet 应用控制和带宽管理，通常是通过对应用数据包进行分析，通过识别匹配协议或应用特征进行的 4-7 层的应用管控。Internet 上的许多网络流量都使用 HTTPS 加密。许多安全的 Web 网关可以解密 HTTPS 流量，以便扫描流量中是否存在恶意软件。检查之后，网关将重新加密流量，并将其转发给用户或 Web 服务器。因此 Internet 应用控制和带宽管理可以保证业务流量的优先级以及阻止不恰当的应用占用大量带宽。

三、URL 过滤处理能力

URL 过滤的实现机制是将客户端请求的 URL 与网关中的 URL 过滤策略进行匹配，从而达到过滤控制的目的。Web 安全网关仅仅需要对 http header 中的 URL 进行扫描处理，不需要对 http 请求的内容进行扫描。内容过滤可以阻止恶意信息进入公司网络。而公司的 IT 管理员通常可以自定义其安全 Web 网关的内容过滤策略。URL 过滤也可以起到一定的数据防泄露的功能。

2. 5 邮件安全网关

2.5.1 邮件安全网关的定义

当前网络空间形式下，社交网络日益发达，电子邮件发展至今已有几十年历史，但仍是最重要的现代互联网应用之一。从个人生活到工作场景的使用，邮件都在现阶段人们的生活中扮演着不可或缺的角色。近年来邮件攻击引发的网络安全事件频频发生，邮件系统作为现代企业关键信息基础设施，已成为攻击的重灾区。对 APT(高级持续性攻击)组织来说，邮件攻击是其最为常用的攻击手段。

邮件安全网管是邮件服务说使用的网关，是邮件服务以及网络安全的第一道防线，它应具备反恶意攻击、反垃圾邮件、病毒检测、敏感信息监测等功能，可有效检测 APT、社工钓鱼、商业欺诈、垃圾邮件、帐号受控、弱口令、帐号爆破、病毒、木马、蠕虫、URL 钓鱼等邮件攻击，为邮件服务提供全方位的安全保障。

2.5.2 邮件安全网关的核心价值

随着邮件业务规模的不断增长，对电子邮件系统的安全防护需求日益迫切。如何有效的防堵各类垃圾邮件，保护用户免受病毒木马及钓鱼邮件的戕害，是很多客户目前最需要迫切解决的问题。当遭遇垃圾邮件、病毒邮件、钓鱼邮件、或 DDos 时，做不到及时防御，可能会导致邮件服务不堪重负而崩溃，严重的话会对整个公司的业务发展造成毁灭性打击。

通过部署邮件安全网关，可以帮助用户解决如下问题：

可以有效避免遭受垃圾邮件或者黑客的拒绝复位攻击，有效减轻邮件服务器的负担；

可以斩断病毒的邮件入侵渠道，反勒索，反钓鱼，保障内外安全；

可以避免邮件账户被盗用，用来发送垃圾邮件和恶意邮件，危害用户信誉；

可以最大限度的减少垃圾邮件的干扰，提高邮件服务满意度；

可以避免重要信息通过邮件违规外泄，避免潜在的合规风险；

可以提高邮件应用效率，提高邮件传递速度。

2.5.3 邮件安全网关的关键能力

2.5.3.1 垃圾和广告邮件检测

邮件系统作为企业最为广泛使用的通讯系统，由于其开发性和易用性，不可避免的成为各种垃圾和广告的目标。各种反垃圾邮件技术也应运而生。这些年来，垃圾邮件的发送渠道又成为了网络攻击的首要突破口。垃圾邮件的泛滥已经成为企业安全不可忽略的巨大威胁，员工生存率下降、商务信息泄漏等问题已经造成了不少企业的经济效益损失，不断变换的邮件发送和编写方式，更让垃圾邮件防不胜防。

作为现在主流的邮件安全解决方案，邮件安全网管可以利用实时地址黑名单（RBL）、域名黑名单（DBL）、DNS 黑名单（DNSBL）、URI 黑名单（URIBL）、发件人策略过滤（SPF）、域名密钥识别邮件标准（DKIM）、关键字过滤和发送限制等手段，结合利用图像识别、语义分析等技术，识别并拦截垃圾邮件，保护邮件服务安全。

2.5.3.2 弱口令、帐号爆破等针对邮件帐号的攻击检测

获取可信的邮件帐号是邮件攻击黑色产业链的重要环节，同时也是 APT 对抗过程中的重要手段。近年来，针对邮件帐号的攻击持续发展，分布式帐号爆破、帐号撞裤、帐密钓鱼等新型攻击手段层出不穷。对攻击者来说，使用受控的可信帐号可大大增加邮件钓鱼的命中率。而对企业用户来说，对外发送大量营销、钓鱼邮件，会导致关键信息泄漏和商誉损毁。

邮件安全网关可对邮件登录会话和内容信息进行分析，实现对相关帐号的登

录频次、地点、收件频次、发件频次、口令强度等的监控，同时以个体历史登录行为基线或者同权人员登录行为基线进行比较，侦测弱口令、帐号爆破、异常登录和异地登录等行为。

2.5.3.3 识别精心伪装的鱼叉式钓鱼邮件

攻击者可能利用社会工程学广泛收集特定目标的相关信息，并在周密筹划后定向发送精心伪装的针对性邮件。为了达到精准钓鱼目的，攻击者会对邮件头、邮件正文、链接、附件等威胁载体进行选择结合、精致化伪装，鱼叉式钓鱼邮件攻击具有高隐蔽性。

邮件安全网关可以结合情报、攻击手法等知识库，结合语义智能分析综合建模对隐蔽的鱼叉式钓鱼邮件进行识别，满足用户对电子邮件系统更高的安全需求。

2.5.3.4 识别通过邮件的敏感数据泄漏

敏感信息在通过邮件流转的时候，泄漏的风险极高。可能财务部门把含有敏感财务内容的邮件发给了行政部门人员。员工在离职前，可能会把公司电脑上的文档发到个人邮件，但是企业却对其中发送的内容一无所知。上述敏感数据泄漏防不胜防，更糟糕的是损失无法追回。要防止通过邮件的泄密行为，需要通过邮件安全网关来实现。邮件安全解决方案在对于邮件内容进行内容检查时，包括邮件正文、附件、图片、收件人、发件人等内容，之后再根据企业的相关安全策略，采取审计、隔离、加密外发、审批流程等防护动作，实现对于邮件的合规化检查和审计。相关的审计记录直接记录在后台管理平台中，随时进行追溯审计；也可以将所有的邮件内容都保存到指定的外置存储中，在出现风险事件时对于存储下来的邮件内容进行快速的反查和检索和定位。能很容易的知道哪些用户在什么时候，接收了或者外发了敏感数据邮件，发送给谁。

2.6 身份识别与访问管理

2.6.1 什么是身份识别与访问管理

身份是安全基础架构的根本要素。随着企业以及政府单位信息化水平的快速提升，各领域向数字化智能化的加速发展，组织的信息环境越来越复杂，业务场景也更加丰富。人员、设备、应用、API 等实体都需要建立对应的身份，以支持设备与设备、人员与设备、组件与组件、服务与服务以及人员与人员等各种实体间的安全交互。然而，在信息系统的实际建设过程中，各系统的身份管理、认证、授权等机制的常常独立建设，不仅带来重复建设、成本提高，而且很容易造成信息孤岛，对身份的管理和运维带来极大的挑战。在现实世界中，孤儿账户、僵尸账户以及大量的弱口令和默认口令账户都成为黑客攻击的首选目标。

访问控制是解决安全问题的基础。通过访问控制，所有未授权的访问企图将被阻断，而经过授权的访问则被允许操作。访问控制的本质是控制何人（主体，Subject）对何物（客体，Object）执行何种操作（访问操作，Action）的一种方法。其中主体、客体和操作构成了访问控制的最基本要素。访问控制规则或策略表述了这些要素间的关系。访问控制模型用以评估访问请求是否符合访问控制策略并做出授权决策。访问控制方法则是模型与策略的实施指导。现代的访问控制技术应具备最小权限原则（The Principle of Least Privilege）和完全仲裁原则（Complete Mediation）。最小权限原则是安全的基本原则之一，其核心思想是仅为访问主体分配完成其对客体访问操作所需的最少权限；而完全仲裁原则要求每一个访问请求都必须经过一个正当有效的授权过程，即该授权控制点不可被绕过。

IAM 在 Gartner 中的定义为：Identity and access management (IAM) is the discipline that enables the right individuals to access the right resources at the right times for the right reason。即 IAM 是一个可有效控制人或物等不同类型用户访问行为和权限的管理系统，能够有效控制什么人或物体在什么时间有权限访问哪些资源。随着越来越多的组织开启零信任实践，对具备统一的身份识别和访问管理

的能力要求原来越高。IAM 通过统一的身份管理、认证和授权能力，有效的连接了组织的各类信息系统，相对于传统解决方案更加的安全与高效。

IAM 带来的信息系统的高效连接、访问安全性和有效性，使得 XDR 技术有能力以身份为核心进行关联分析，攻击溯源等工作，为 XDR 向组织提供更精准的检测和更及时的响应能力提供了重要支撑。

2.6.2 权访问管理

特权账户是对关键信息资源的访问身份凭据。顾名思义，特权账户通常都具有完整的数据可见性和信息系统的完全控制权。因此，攻击者一旦掌握了特权账户，便有可能发起最终的攻击并造成难以挽回的损失。

特权账户是如此的关键，在相当多的组织中，许多特权账户仍然没有受到保护，弱口令、默认口令等风险仍然存在。在实际使用中，特权账户口令经常会由于出于“运维需要”被普通员工和第三方人员获取。

特权访问管理 Privileged Access Management (PAM) 是通过监视、检测和防范对关键资源的未经授权的特权访问，帮助组织免受网络威胁。PAM 使得特权账户的使用与所执行的操作变得可见。在早期阶段，特权访问管理 (PAM) 只涉及保护用于特权账户的口令，并逐步发展为堡垒机的形态（如具备使用跳板机或独立终端软件进行会话录制的能力）。如今，PAM 的能力更加丰富，具备了包括多因素身份验证(MFA)、会话监控、代理和用户行为分析(UBA)等其他安全能力。

PAM 同样要求具备实现最小权限原则和完全仲裁原则的能力。通过会话监控、代理和用户行为分析能够根据用户职责限制其对系统的能力，实现用户仅具有其所需的最低访问权限；而完整的特权账户台账、自动化的扫描与检测关键资产及特权账户，异常访问请求的侦测与拦截，以及严格的口令轮换则是对完全仲裁的保证。

特权访问的滥用是一种网络安全威胁，可能会对组织造成严重的大范围损害。扩展检测和响应(XDR)技术与 PAM 的结合是相辅相成的。XDR 通过使用关键数据

和遥测来扩展所有关键资产的可见性，增强了完全仲裁的能力。而 PAM 通过对关键资源即时的最小访问授权，以及对特权会话的监视与特权账户事件的捕获，进一步丰富了 XDR 的遥测能力。

2.6.3 身份威胁事件检测与响应

随组织的信息环境日益复杂，安全边界愈加模糊。以身份为核心构建安全边界的思想成为主流安全解决方案关注的重点。相应的，针对身份的攻击也已经非常普遍。身份威胁检测和响应（Identity Threat Detection and Response, ITDR）技术变得重要。Gartner 对 ITDR 技术的正式定义为：身份威胁检测和响应（ITDR）包括保护身份基础架构免受恶意攻击的工具和流程。他们可以发现和检测威胁、评估策略、响应威胁、调查潜在攻击并根据需要恢复正常操作。IAM 为组织统一的身份识别和访问管理能力，在简化了管理难度的同时，也为攻击者提供了更大的潜在收益。越来越多的攻击者将目标对准身份基础设施本身。ITDR 技术将为身份和访问管理（IAM）部署增加额外的安全层。

与很多安全技术相似，身份优先安全也不是个全新概念。随着攻击者开始瞄准身份和访问管理功能并长期潜伏，身份优先安全变得更加紧迫。ITDR 技术通过对身份威胁的检测和响应为组织的信息系统增加防御层，如：防止端点上的凭据被盗、特权升级，避免 Active Directory 身份泄露等。混合办公和向云应用程序的迁移巩固了身份作为安全边界的趋势。ITDR 也成为 XDR 的关键组成部分。通过与 XDR 解决方案提供的额外情报相结合，组织的防御者增强了对可疑行为（特别是攻击早期的可以行为）快速识别和响应的能力，从而有效的避免了对手渗透组织网络。

2.7 蜜罐与沙箱

对于未知威胁，依赖传统的被动式防御无法有效应对，因为未知威胁的特征或行为是不确定的。那么，被动式防御主导下的攻防对抗往往演变为亡羊补牢式的疲于应对。只有基于未知威胁的攻击已经发生，甚至已造成破坏，才能分析其行为，进而给出应对方案，为了更好地抵御未知威胁，近年来研究人员逐渐转向

不依赖先验知识的主动防御技术，提出了各种新型的防御检测思想和技术，例如蜜罐/蜜网，安全沙箱等，引起了业界高度关注。

2.7.1 蜜罐

关于蜜罐，到目前为止还没有一个完整明确的定义。根据“蜜网项目组”的创始人 Lance Spitzner 给出了一个比较权威的定义：蜜罐是一种安全资源，其价值在于被扫描、攻击和攻陷。这个定义表明蜜罐并没有其他的实际作用，所有流入和流出蜜罐的网络流量都可能预示着扫描、攻击和攻陷。

九十年代初蜜罐概念的提出直到 1998 年左右，“蜜罐”仅仅限于一种安全思想，通常由网络管理人员应用各种技术手段，通过欺骗黑客达到追踪的目的。这一阶段的蜜罐实质上是一些真正被黑客所攻击的主机和系统。

从 1998 年开始，蜜罐技术引起安全研究人员的注意，并开发出一些专门用于欺骗黑客的开源工具，如 Fred Cohen 所开发的 DTK、Niels Provos 开发的 Honeyd 等，同时也出现了像 KFSensor、Specter 等一些商业蜜罐产品。这一阶段的蜜罐可以称为是虚拟蜜罐，即开发的这些蜜罐工具能够模拟成虚拟的操作系统和网络服务，并对黑客的攻击行为做出回应，从而欺骗黑客。

从 2000 年之后，安全研究人员更倾向于使用真实的主机、操作系统和应用程序搭建蜜罐，但与之前不同的是，融入了更强大的数据捕获、数据分析和数据控制的工具，并且将蜜罐纳入到一个完整的蜜网体系中，使得研究人员能够更方便地追踪侵入到蜜网中的黑客并对他们的攻击行为进行分析。

蜜罐的核心价值就在于对这些攻击活动进行监视、检测和分析。实际上，蜜罐中只有一些虚假的敏感数据，不用于对外的正常服务。所以，它可以是一个网络、一台主机、一项服务，也可以是数据库中的某些无用的数据或者伪装的用户名及其弱口令等，因此任何与它交互的行为都可以被认为是攻击行为，这样就简化了检测过程，它可以部署在各个内部子网或关键主机上，检测来自网络系统外部和内部的各种攻击，用一种以检测、监视和捕获攻击行为和保护真实主机为目

标的诱骗技术。

蜜罐 Honeypot 以及蜜罐延伸技术，当前十分流行，它已不是一种新的技术，可以说是一大进步的安全策略。它使我们知道正在被攻击和攻击者，以使“黑客”们有所收敛而不敢肆无忌惮。蜜罐的引入，类似于为网络构建了一道防火沟，使攻击者掉入沟中，装入蜜罐以至于失去攻击力，然后再来个瓮中捉鳖。

目前蜜罐技术方案主要有两种：商品型和研究型。商品型主要就是通过使黑客攻击蜜罐从而减轻网络的危险。 研究型主要就是通过蜜罐来获得攻击者的信息，加以研究。实现知己知彼，既了解黑客们的动机，又发现我们所面临的危险，从而更好地加以防范。无论是商品型还是研究型蜜罐，他们的主要目的是被用来探测、攻击和潜在的开发利用。

蜜罐系统是一个陷阱系统，它通过设置一个具有很多漏洞的系统吸引黑客入侵，收集入侵者信息，为其他安全技术提供更多的知识。蜜罐采用监视器和事件日志两个工具对访问蜜罐系统的行为进行监控。由于蜜罐是一个很具有诱惑力的系统，能够分散黑客的注意力和精力，所以对真正的网络资源起到保护作用。

蜜罐系统主要涉及网络欺骗技术、数据捕获技术、数据控制技术、攻击分析与特征提取等主要技术:

网络欺骗技术：是蜜罐的核心技术，利用各种欺骗手段和安全弱点和系统漏洞，引诱黑客的攻击。

数据捕获技术：主要目的是尽可能多的捕获攻击信息，而不被黑客发现，包括输入、输出及键盘和屏幕的捕获。

数据控制技术：主要目的是防止黑客将蜜罐作为跳板去攻击其他系统或危害别的主机，因此必须控制进出系统的数据流量而不被黑客怀疑。

攻击分析与特征提取：蜜罐系统设置一个数据分析模块，在同一控制台对收集到的所有信息进行分析、综合和关联，完成对蜜罐攻击信息的分析。

蜜罐技术在攻击检测、分析、特征提取、追踪、取证和预警防御等方面已经取得了比较显著的成果，展现了广泛的应用前景，可以作为现有安全机制的有力补充。

2.7.2 沙箱

沙箱也叫沙盒，英文 sandbox，在计算机领域指一种虚拟执行技术。沙箱技术源于软件错误隔离技术（ software - based fault isolation , SFI)。 SFI 是一种利用软件手段限制不可信模块对软件造成危害的技术，其主要思想是隔离，即通过将不可信模块与软件系统隔离来保证软件的鲁棒性。

在网络安全领域，沙箱是指一种隔离的运行环境，用以测试不受信任的文件或应用程序等行为的工具，它负责接管病毒调用接口或函数的行为，并会在确认病毒行为后实行回滚机制，让系统复原。不同于传统的基于静态分析和动态分析的恶意代码防御思路，它可以通过采用诸如虚拟化等技术构造一个隔离的运行环境，并且为其中运行的程序实体提供基本的计算资源抽象，通过对目标程序进行监测分析，准确发现程序中潜藏的非法代码、病毒攻击等，进而达到保护系统安全的目的。由于沙箱可以将恶意程序的所有操作都限制在一个完全封闭的计算环境中，并同时记录可疑程序运行过程的所有操作，所以沙箱的防护性能广受安全企业和安全专家的青睐。

经过几十年的发展，当前沙箱技术有很多分支，从计算机体系结构的角度出发，沙箱的实现架构分为三种：应用层沙箱、内核层沙箱和混合型沙箱。应用层沙箱主要部署于操作系统的应用层，内核层沙箱位于操作系统的内核层，混合型沙箱介于操作系统的应用层和内核层之间。

应用层沙箱系统运行在操作系统的用户层，该类沙箱可以分成应用程序沙箱和语言类沙箱。其中应用程序沙箱主要通过重定向系统服务来实现沙箱的基本隔离功能。最早的应用程序沙箱用于保证二进制代码的安全。

内核层沙箱驻留在内核的地址空间中，可以方便地借助硬件级别的保护机制

来实现安全隔离。

混合型沙箱是结合了应用层和内核层沙箱技术的沙箱系统。在该类沙箱中，内核层提供了操作系统的隔离支持及相关的执行机制，系统的剩余部分都在应用层实现。

沙箱技术由来已久，但真正产品化也不过是近几年的事情。网络沙箱一般都被以 APT 产品或威胁溯源分析类产品出现，并且融合了多种检测技术，通过旁路监听现网流量，并对流量做协议分析和文件还原，进而采用多种检测引擎来进行综合分析。在日常网络安全监测过程中，所有可疑的软件或文档一般都应将其在沙箱中运行一遍，如果发现恶意行为，则可以禁止程序在其常环境中的进一步运行。

沙箱的关键技术主要包含三方面：虚拟化技术、恶意行为检测技术和重定向技术。其中基于虚拟机的沙箱主要采用虚拟化技术和恶意行为检测技术；基于规则的沙箱主要采用重定向技术和恶意行为检测技术。

虚拟化技术是一种资源管理技术，可以将计算机的各种实体资源予以抽象、转换后呈现，打破了实体结构不可切割的障碍，进行更好组合。基于虚拟机的沙箱基于虚拟化技术构建一种隔离环境，运用记录机制把相关操作记录下来，当用户需要恢复到相应的时间点时，沙箱能够将所有这些操作撤销，回溯到该时间点。基于虚拟机完成目标操作。

恶意行为检测技术是沙箱的重要组成部分，其分析过程可分为行为分析和恶意检测两个步骤。其中行为分析包含行为捕获和对程序行为建模两个步骤。对恶意软件检测其主要是利用特征信息进行匹配判定，主要使用特征检测法和行为监测法。

重定向技术是一种可以将各种访问请求以及请求中的参数重新定位转移到其他请求或参数的技术，例如，网页的重定向、域名的重定向以及路由选择的重定向都是重定向技术的典型应用，重定向可以帮助程序实现自己期望的功能。在

基于规则的沙箱系统中，系统可以使用相关的重定向技术把对文件的不可靠操作重定向到系统的某一特殊文件内，即相当于限制了程序的操作，以此保护系统文件数据的安全。例如 Hook 技术就是一种典型的重定向技术，其本质就是劫持函数调用，它可以用于网络攻击和网络防御。

沙箱技术可以建立一个操作受限的应用程序执行环境，将不受信任的程序放到沙箱中运行来限制其对系统可能造成的破坏。但伴随着网络攻击技术的快速发展，沙箱技术本身还有很多地方需要改进。

目前网络中的恶意软件更新速度非常快，人工对沙箱规则库进行更新难以有效应对沙箱的现实需求，其规则集很可能滞后。未来如何在沙箱的架构中加入智能学习系统，自动化地更新规则集合能够改进现有沙箱系统性能。

针对沙箱防护，攻击者也在研究相应的逃逸技术。如果恶意软件的隐蔽性和针对性比较强，如 APT 攻击，仅从监控到的系统调用信息中获得的程序行为信息难以完全推理得到恶意程序的真正目的。因此，研究多维度的程序行为监控技术，从不同维度的程序执行信息中获得程序可能的行为，是改进沙箱防御能力的重要方向。

第三章 后端能力

3.1 威胁情报

3.1.1 威胁情报的定义及来源

根据 Gartner 的定义，威胁情报是关于 IT、信息资产面临现有或酝酿中的威胁的证据性知识，包括：可实施上下文、机制、标示、含义和能够执行的建议。这些知识可以为威胁的响应、处理决策提供技术支持。威胁情报包括攻击源信息、攻击所利用的漏洞、受害者信息，以及战术、技术和过程等。这些要素为网络安全态势感知提供有力的依据。

威胁情报，可以分为内部威胁情报和外部威胁情报。其中，内部威胁情报是在企业日常安全运营过程中，由内部安全专家不断分析、研判、识别出新的威胁情报指标，日积月累而得。内部威胁情报，是由企业信息架构内生的威胁情报指标数据，最为切合业务本身，在体现企业自身业务脆弱性和潜在威胁方面，具有得天独厚的优势。内部威胁情报的原始数据来源于企业部署的安全运营生态体系，包括 EDR、NDR、沙箱、蜜罐、SIEM 等设备和系统。外部威胁情报是指由企业采购的威胁情报产品厂商、在线威胁情报平台运营商，或开源威胁情报数据源生产的威胁情报数据，一般由文件哈希、域名、IP 和端口、恶意 URL 等几个常规维度的指标数据构成。此外，外部威胁情报还包括漏洞情报、技战术情报、重大事件威胁预警信息、APT 组织画像情报、攻击者画像情报等成熟度系数更高的威胁情报。

3.1.2 威胁情报增强网络安全态势感知

基于威胁情报的安全态势感知主要包括三个应用场景：威胁感知、攻击溯源和态势评估。

在威胁感知场景中，XDR 从终端、流量、沙箱、蜜罐等异构的数据源中采集汇聚多元化安全要素，通过恶意代码专杀引擎、人工智能引擎、资产画像分析引擎等全方位多维度的引擎能力，提取高价值高密度的特征要素数据。安全分析专家基于行业深耕累计的威胁建模及研判分析经验，在以 MITRE ATT&CK 矩阵为代表的攻击场景模型的指导下，辅以自动化攻击模拟工具，面向不同威胁场景的具体安全业务需求，设计告警合并规则，对海量特征要素数据进行狩猎建模分析，以“终端”行为打点数据为基点，辅以“流量”威胁特征为佐证，生成高置信度的平台威胁告警，充分发挥平台“面”的优势，弥补“端”类安全产品在“看见”全局，感知全景方面的不足。

攻击溯源场景基于安全专家对攻击者、攻击者组织及热点安全事件的持续观察与研究，总结各类有效攻击的意图、影响，推断每一次安全事件幕后的背景、机制、指标、攻击行为的时序关系，提炼总结安全事件模型，并针对不同的模型，分阶段分步骤规划安全防御点和破解方法，通过“纵深防御体系”构建层层壁垒，

逐一瓦解高级别攻击者因国家背景和巨额财力支撑而拥有的绝对优势。同时，在常态运营和攻防博弈的过程中，不断积累最具成效的处置措施，归纳形成处置预案知识库，通过最佳实战经验统筹规划指挥调度，合理优化安全布防。XDR 平台进一步探索威胁情报与检测分析能力的深层次融合，精心设计全面的情报指标检测点和新生情报数据采集点，打造企业“内生情报循环体系”，结合云端“大网情报知识库”的全力赋能，利用威胁图谱技术原生自带的“相关性”链式递传效应，真正实现跨系统、跨平台、跨数据中心、跨地域的攻击溯源能力。

态势评估场景在威胁感知阶段的自动化检测分析结果和攻击溯源阶段的研判溯源取证结论的基础上，面向企业信息架构的顶层安全战略要求，统计细粒度的安全资产台账，综合考量资产的安全敏感级别、各个维度的安全数据、数据来源的置信度，触发告警的威胁情报指标的成熟度系数以及资产和安全数据的关联关系，规划全局风险统计指标体系，设计合理的数学建模分析模型，有理有据地判断企业业务体系的综合安全风险分值，实现安全态势的量化评估，支撑态势信息的可视化呈现。

3.1.3 威胁情报赋能高级威胁识别

威胁情报数据源长期持续性地从企业内外部采集威胁特征指标数据，具备长周期多维度的特征，能够有效提高 APT 等安全事件分析的效率和攻击检测率。另一方面，威胁情报具有很强的独立更新能力，当安全事件的数量增加时，威胁情报也会相应进行更新，为安全管理者提供更新的安全事件信息。通过对威胁情报进行共享，可以在同一组织的领域中获得针对性的威胁信息，使企业了解行业环境、攻击者是什么、攻击者利用技术等信息的策略和防御策略，帮助客户了解企业本身将遭受的威胁，从而提高安全响应能力。威胁情报在提高处理网络安全威胁、漏洞管理和风险控制，了解威胁环境以及指定决策效率方面具有极高的应用价值。

3.1.4 威胁情报加速安全事件应急响应

在安全事件应急响应的过程中，综合利用全网威胁情报结合威胁图谱可加快

事件响应速度。首先，通过情报对碰，基于原始告警生成高置信度的有效告警；然后，基于大数据湖、关联分析和威胁图谱技术，基于有效告警，生成安全事件的时间线，同时，将调查任务、调查对象、告警、原始作证数据和处置建议以可视化的方式全方面多维度整合在一起，在多源单点设备统一联动处置的基础上，最大程度提升系统的自动化响应能力，解放人力，加快安全事件的应急响应速度，从安全基础设施和处理能力的根本层面，实现降本增效。

3.2 数据湖

根据 XDR 的定义：XDR 打破信息孤岛效应，将安全产品整合成一个统一的安全事件检测与响应平台。进行全面的遥测数据采集、检测、智能分析、威胁狩猎和自动化响应。因此 XDR 产品在后端，需要强大的安全大数据平台支撑海量安全数据采集、存储、分析、检索和可视。

3.2.1 数据湖的概念

信息技术领域内，数据分析与处理平台经过多年的发展，大致经历过四个阶段：

第一代：以数据库为代表的技术。数据库技术诞生于 20 世纪六七十年代，典型的是关系型数据库。如：Mysql、Oracle、SQL Server、PostgresSQL 等。仅能够在单机模式下，提供小规模数据（如 GB 级）下的实时查询分析。

第二代：以 Hadoop 为代表的大规模分布式计算和存储系统。进入二十一世纪之后，随着互联网的崛起，数据量爆发式增长。传统的数据库方案无力应对大规模数据的存储和分析，软硬件成本也指数级增长，再也无法支撑海量的数据统一查询和分析的需要。2004 年前后，Google 先后发表了 3 篇论文：GFS 分布式文件系统、MapReduce 并行计算框架、BigTable，奠定了大规模分布式计算和存储系统的框架，开创了大数据时代。随后开源社区开发 Apache Hadoop 开源大数据方案，风靡全球。

第三代：以 Spark/Flink/Storm 为代表的实时流式计算系统。2010 年之后，以 Hadoop 为代表的大规模分布式计算和存储系统的弱点暴露的越来越多，比如离线批处理的实效性问题、代价高昂且开发效率低的手写 MapReduce 作业问题。为了解决这些问题，出现了各种实时计算引擎、以 SQL 为表达式的引擎。如 Spark、Flink、Storm 等。

第四代：以数据湖/湖仓一体化为代表的新技术。随着云原生技术的发展，以数据湖为代表的新技术出现，可以对任意类型数据（结构化和非结构化），任意规模数据（GB、TB、PB、EB 等）进行集中存储。可以事先处理，也可以原样存储。支持数据采集、处理、实时分析、ML/AI、挖掘、和数据可视。

3.2.2 数据仓库与数据湖

1988 年，为解决企业的数据集成问题，IBM 的两位研究员创造性地提出了一个新的术语：数据仓库（Data Warehouse）。1992 年，“数据仓库之父”比尔.恩门，给出了传统数据仓库的定义：数据仓库是一个面向主题的、集成的、相对稳定的、反映历史变化的数据集合，用于支持管理决策。数据仓库用于支持决策，面向分析型数据处理，它不同于企业现有的操作型数据库，操作型数据库是为了支撑各种业务而建立的，而数据仓库是对多个异构的数据源有效集成，集成后按照主题进行了重组，并包含历史数据，而且存放在数据仓库中的数据一般不再修改。数据仓库主要处理历史的、结构化的数据，这些数据必须与数仓事先定义的模型吻合，将它们或者转化为多维数据，或转换为报表，满足高级报表及数据分析需求。数据仓库通常用于存储和维护长期数据，可以按需访问。新型数据仓库是基于大数据平台的存储引擎、存储格式（Hive、Delta Lake 等），基于维度建模方法建设的结构化数据集合，目的是为所有类型的数据支持提供数据环境。典型的数据仓库架构：

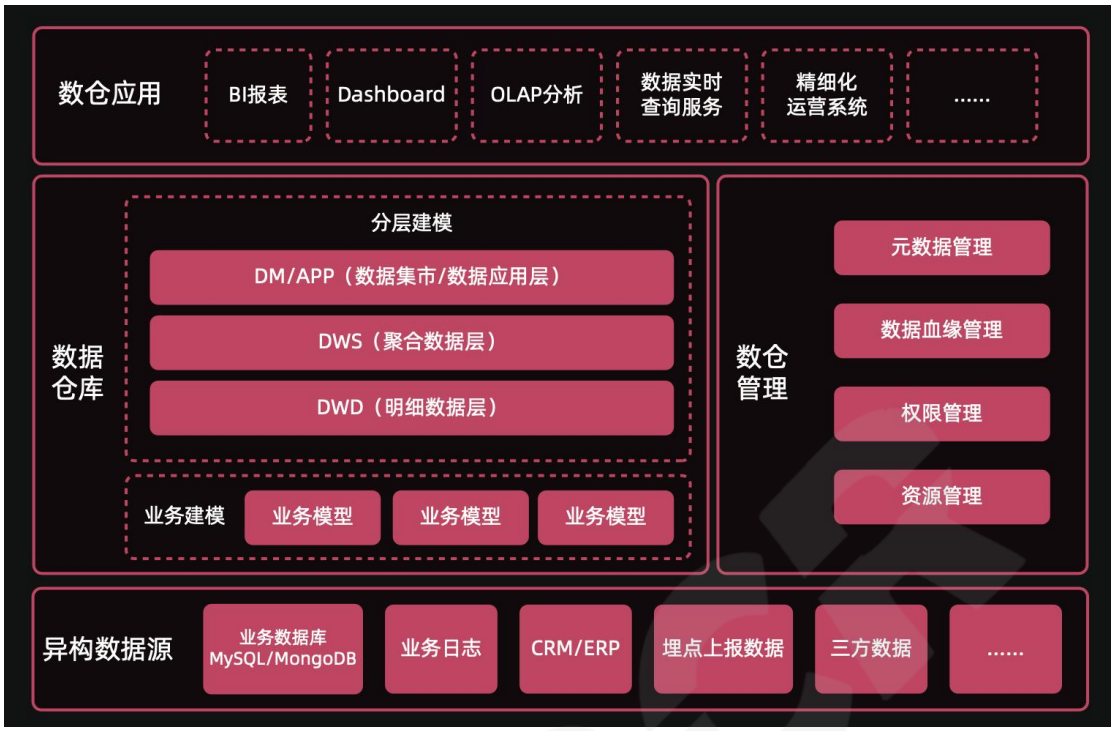


图 3-1 典型的数据仓库架构图

Pentaho 首席技术官 James Dixon 创造了“数据湖”一词。它把数据集市描述成一瓶水（清洗过的，包装过的和结构化易于使用的）。而数据湖更像是在自然状态下的水，数据流从源系统流向这个湖。

维基百科对数据湖的定义：是一个存储企业的各种各样原始数据的大型仓库，其中的数据可供存取、处理、分析及传输。数据湖是以其自然格式存储的数据的系统或存储库，通常是对象 blob 或文件。数据湖通常是企业所有数据的单一存储，包括源系统数据的原始副本，以及用于报告、可视化、分析和机器学习等任务的转换数据。

亚马逊公司对数据湖的定义：数据湖是一个集中式存储库，允许您以任意规模存储所有结构化和非结构化数据。您可以按原样存储数据（无需先对数据进行结构化处理），并运行不同类型的分析 – 从控制面板和可视化到大数据处理、实时分析和机器学习，以指导做出更好的决策。

数据湖可以支持任意类型的数据，包括:

- 来自关系数据库（行和列）的结构化数据
- 半结构化数据（CSV，日志，XML，JSON）
- 非结构化数据（电子邮件，文档，PDF）
- 二进制数据（图像，音频，视频）。

数据湖需要提供足够用的数据存储能力，这个存储保存了一个企业/组织中的所有数据。数据湖可以存储海量的任意类型的数据 包括结构化、半结构化和非结构化数据。数据湖中的数据是原始数据，是业务数据的完整副本。数据湖中的数据保持了他们在业务系统中原来的样子。数据湖需要具备完善的数据管理能力（完善的元数据） 可以管理各类数据相关的要素，包括数据源、数据格式、连接信息、数据 schema、权限管理等。数据湖需要具备多样化的分析能力 包括但不限于批处理、流式计算、交互式分析以及机器学习；同时，还需要提供一定的任务调度和管理能力。数据湖需要具备完善的数据生命周期管理能力。不光需要存储原始数据，还需要能够保存各类分析处理的中间结果，并完整的记录数据的分析处理过程，能帮助用户完整详细追溯任意一条数据的产生过程。

3.2.3 湖仓一体化在安全领域的应用

数据湖因为能处理所有类型的数据，如结构化数据、非结构化数据，半结构化数据等，数据的类型依赖于数据源系统的原始数据格式。可以想象仓库和湖泊的区别：仓库存储着来自特定来源的货物，而湖泊的水来自河流、溪流和其他来源，并且是原始数据。

从数据采集范围或完整性角度看，数据湖的数据更轻松采集，具有可追溯性。从数据来源类型上看，诸如 Web 服务器日志，传感器数据，社交网络活动，文本和图像等非传统数据源，也入湖管理，数据内容更全面，而且数据湖通常是在存储数据之后定义架构，数据湖存储所有最原始的数据，最细节的数据，使用较少的初始工作并提供更大的灵活性，也消除了数据孤岛问题。

湖仓一体是一种新型开放式架构，充分利用数据湖和数据仓库的优势，并实现优势互补。其构建在数据湖低成本的数据存储架构之上，又继承了数据仓库的数据处理和管理功能，打通数据湖和数据仓库两套体系，让数据和计算在湖和仓之间自由流动。作为新一代大数据技术架构，将逐渐取代单一数据湖和数据仓库架构。

湖仓一体化是一种不断演进中、可扩展的大数据存储、处理、分析的基础设施；以数据为导向，实现任意来源、任意速度、任意规模、任意类型数据的全量获取、全量存储、多模式处理与全生命周期管理；并通过与各类外部异构数据源的交互集成，支持企业级数据安全应用，典型的湖仓一体化架构如下：

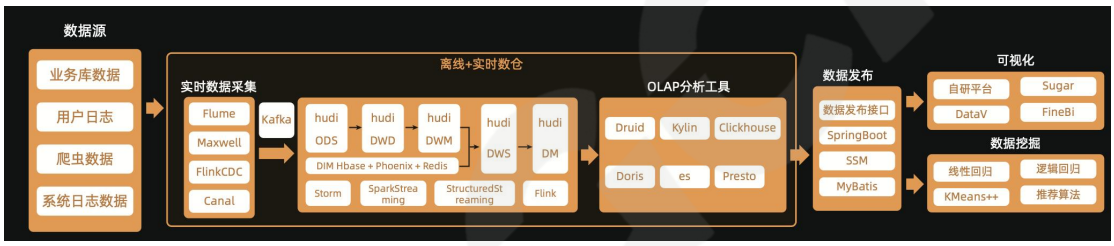


图 3-2 典型的湖仓一体化架构图

湖仓一体化大数据平台是更加全面、高效、可靠和智能的大数据处理架构。它支持更多的数据类型和计算任务，提供更高效的数据存储和查询能力。主要特性包括：

- 任意数据类型的支持：
  - 来自关系数据库（行和列）的结构化数据
  - 半结构化数据（CSV，日志，XML，JSON）
  - 非结构化数据（电子邮件，文档，PDF）
  - 二进制数据（图像，音频，视频）。
- 任意数据规模：从 KB、MB、GB、TB、PB、甚至 EB 级数据规模。

- 混合数据存储：支持同时支持行存储和列存储，以适应数据处理和分析任务的多样性。

- 多场景支持：公有云、私有云、IDC 等环境，计算资源支持硬件服务器、虚拟机、容器。存储支持本地磁盘、对象存储等。

- 高性能：可以实现大规模数据存储和计算的分布式处理，满足不同应用场景的高并发、高扩展性等需求。

- 低成本：能够实现高数据压缩比，能够利用廉价的硬件，实现低成本。

- 实时分析：支持即时查询能力，支持对大数据集的快速交互式查询和分析。

- 弹性扩展：具备弹性扩展的能力，可以根据业务需求自动扩展计算和存储资源。

- 智能分析：除了支持关联分析、聚合统计、特征匹配外，还提供机器学习/AI 平台支持智能分析计算和数据挖掘。

- 安全可靠：提供更细粒度的数据访问控制和保护机制，以确保数据的安全性和可靠性。

3.3 AI 引擎分析

3.3.1 网络安全检测现状

在新一代网络安全威胁面前，传统基于特征、签名检测技术的统一威胁管理（UTM）、下一代防火墙（NGFW）、入侵检测/防御系统（IDS/IPS）、防病毒（AV）等安全产品并不能使组织安全得到充分保护，传统的防毒墙、防火墙、IPS 等安全设备已无法完全满足企业的安全防护要求。

基于特征检测和行为检测的传统威胁检测手段已经越来越难以应对新型的安全攻击手法，难以识别安全攻击事件。且近年来随着人工智能技术的发展，攻击方在使用扫描、利用、破坏等攻击工具中对人工智能技术的应用，进一步加剧了对目标系统的破坏、缩短了攻击进程、隐藏了攻击特征，对新技术背景下的安全威胁检测手段提出了更大挑战。

3.3.2 AI 在网络安全中的作用

AI 概述

人工智能（Artificial Intelligence，AI），它是研究、开发用于模拟、延伸和扩展的智能的理论、方法、技术及应用系统的一门新的技术科学。

机器学习是人工智能的一个子集，其使用算法自动学习和改进经验，而无需明确编程。其主要用于网络安全，有两个目的：

异常检测: 机器学习可用于自动检测异常，例如异常的用户行为或意外的网络活动，这些异常可能表明存在安全威胁。

AI 的作用

传统的基于特征的检测手段，如 IDS 或杀毒软件无法及时有效的应对新产生或手段高明的网络攻击，而人工智能所擅长的图像识别、模式识别、自然语音处理等技术，可以落地到网络安全检测领域当中，具备对全新威胁的适应及预测能力，可以更加智能、精准的发现 APT 等未知威胁。

通过内置人工智能模型到 NDR 系统，分别对恶意文件变种、恶意加密流量、暗网流量、翻墙代理、VPN、DNS/ICMP/HTTP 隐蔽隧道、WEB 攻击等进行检测，有效弥补了传统检测手段的不足，结合多种检测技术及威胁情报实现对网络威胁的交叉检测和交叉验证、关联分析、溯源取证等。行为分析和 ML/AI 直接对攻击者行为进行建模，并以手术般的精度检测高级和持续性攻击。它们避免了大量低保真和无趣的警报，因为它们不检测异常，而是检测主动攻击。它们为攻击生

命周期的多个阶段提供检测范围，包括持久性、特权升级、防御规避、凭证访问、发现、横向移动、数据收集、C2 和渗漏。有效的 AI 驱动的网络检测和响应平台通过收集和存储正确的元数据，并使用 AI 衍生的检测模型安全洞察力去丰富它。人工智能的有效使用可以推动实时检测攻击者并执行决定性的事件调查，提高整个安全运营的可见性和生产力。

AI 的优势

自动化：AI 可以通过持续监控和分析网络流量来帮助自动执行信息安全的各个方面。

减少人为错误：AI 可以通过每次都遵循相同流程的自动化功能和算法来消除数据处理、分析和其他任务中的人为错误。

消除重复任务：AI 可用于执行重复任务，从而让人力资源能够空出手来解决影响较大的问题。

快速准确：与人类相比，AI 可以更快地处理更多信息，从而查找模式并发现人类可能错过的数据关系。

无限可用性：AI 不受时段、休息需求或其他人类负担的限制。在云端运行时，AI 和机器学习可以“始终开启”，从而持续处理分配的任务。

更快的研发速度：快速分析大量数据的能力可以加快获得研发突破的速度。

3.3.3 AI 在网络安全领域中的应用

3.3.3.1 文件基因图谱检测

基于人工智能检测技术，结合机器学习/深度学习、图像分析技术，将恶意代码映射为灰度图像，通过恶意代码家族灰度图像集合训练卷积神经元网络（CNN）深度学习模型，建立检测模型，利用检测模型对恶意代码及其变种进行家族检测。基于灰度图像映射的方法可以有效的避免反追踪、反逆向逻辑以及其

他常用的代码混淆策略。而且，该方法能够有效地检测使用特定封装工具打包（加壳）的恶意代码。在一定程度上解决了特征检测的人工提取困难、行为检测的时间开销大且误报高等问题。对于恶意代码变种和加壳文件具有优异的检测能力，且具有快速、准确率高、误报率低、跨平台检测等特点。

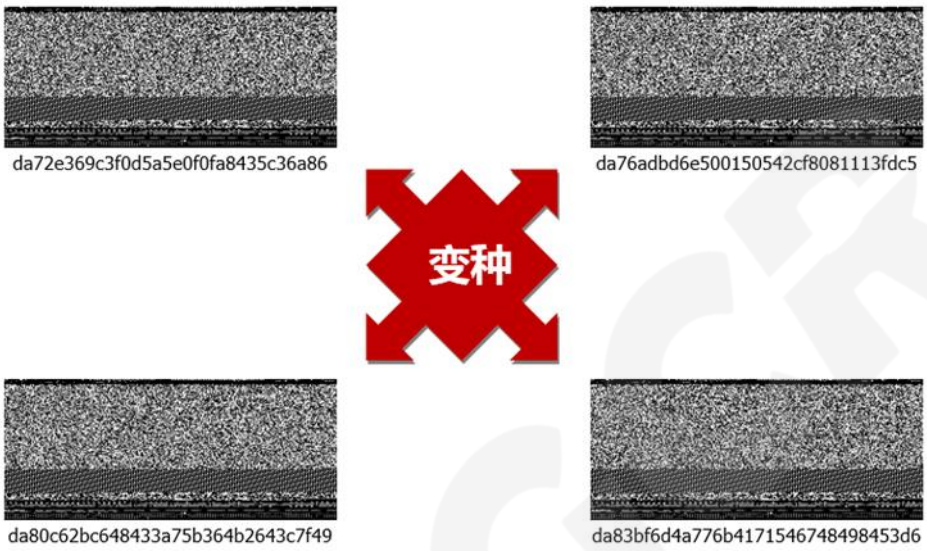


图 3-3 恶意代码变种

如图 1 所示，上述图片都是某个恶意软件的多个变种，但各自的 MD5 值都不一样，现有的基于特征的检测技术如果未曾更新到最新特征库，就无法检测和识别。

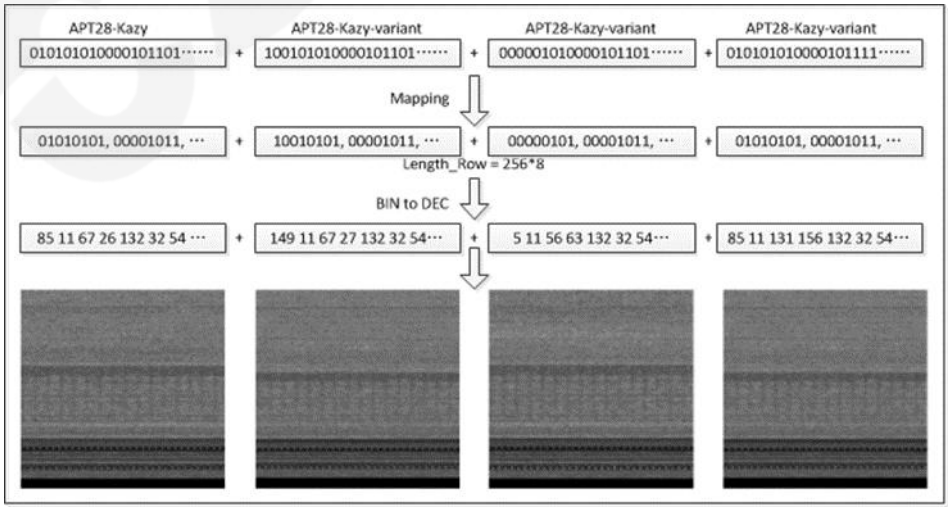


图 3-4 基因图谱检测

如图 2 所示，采用基因检测技术，可以利用恶意代码在变种过程中的遗传学特征，即基因在遗传过程中的复制特性及部分基因突变特性，对恶意代码及其变种进行检测。

3.3.3.2 恶意加密流量检测

从大量恶意软件监测分析的情况来看，越来越多的恶意软件采用了 TLS/SSL 加密方法进行通信。在网络流量使用 TLS 加密后，使得威胁检测变得更加困难，传统的检测方式不能很有效的检出加密数据是否为恶意流量。

人工智能用于加密流量安全检测将是一种新技术手段，一种基于集成学习的恶意加密流量类型识别方法。

数据收集过程，首先针对恶意加密收集难的问题，综合应用网络资源下载、沙箱虚拟执行、自有威胁情报收集、商业合作真实流量采集和处理等多种手段收集的恶意加密通信样本数据，对采集的数据采取多 AV 标记、威胁情报标记和进一步使用聚类算法将相似行为的恶意软件家族聚合的家族簇作为新的类型，从而避免恶意软件家族数量多且变种更新快导致类型识别不准确的问题。

训练数据收集，首先需要下载黑样本。下载的样本来源包括但不限于：stratosphereips 黑白样本、lastline、CICIDS 样本、ADFA-NB15-Datasets 样本、netresec 样本、VT 等。整体数据收集过程如图 1。

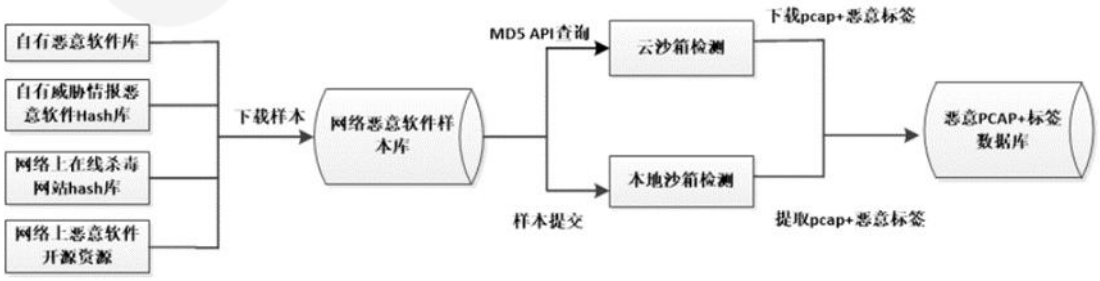


图 3-5 恶意加密流量采集流程

AI 模型特征提取涉及的大类特征包括流元数据特征、分组长度和时间序列特征、字节分布特征、未加密的 TLS 头信息特征、关联的 DNS 数据特征等。

模型训练过程，用机器学习中的集成学习算法先训练一个二分类模型识别加密流量是否为恶意，再训练一个多分类模型识别产生恶意加密通信的恶意软件类型，并对识别的结果进行威胁情报、JA3/JA3S 被动指纹、证书指纹和一千余条恶意加密证书检测规则交叉验证，根据验证结果进行告警自适应参数调优降误报，最后进一步的 JARM 指纹主动取证，获得比单一分类模型更好的泛化能力同时提升恶意软件类型识别的准确性，经过 AI 算法建立检测模型，实现对同类恶意加密流量在不解密情况下进行有效的识别与检测。

模型应用于现网流量检测过程中，针对检测结果持续从准确性和误报率上进行优化。通过域名、JA3/JA3S 指纹、Mercury 指纹等白名单方式过滤，通过 IP 访问行为、周期内告警数量、证书过期日期、域名和 IP 关联关系等行为分析方法进行白流量过滤，通过行为分析和 AI 模型检测相结合提升整体检测效果。

3.3.3.3 隐蔽隧道检测

DNS 隐蔽隧道

DNS Tunneling，是隐蔽信道的一种，通过将其他协议或数据封装在 DNS 协议中传输建立通信。DNS 隧道木马带来的威胁很大,而且 DNS 隧道木马难以得到有效的监控.一方面是因为 DNS 报文具有天然的穿透防火墙的能力;另一方面,目前的杀毒软件、IDS 等安全策略很少对 DNS 报文进行有效的监控管理. 除了上面已经提到的 DNS 协议使用示例之外，还存在许多 DNS 工具，它们可以使攻击者通过 DNS 协议创建隐蔽通道，传统的技术检测手段很难发现 DNS 的隐蔽隧道通信行为。

通过渗透环境搭建收集黑数据和白数据，生成用于分类 DNS 隧道和正常 DNS 数据的样本集合，基于机器学习技术的 DNS 隐蔽隧道检测方法，从 DNS 会话的视角对比分析 DNS 隐蔽隧道通信行为与正常 DNS 解析行为的差异性，提取 DNS

隐蔽隧道识别特征向量（DNS 隧道空间、回应包的长度、qname 中数字字符占比等），建立 DNS 隐蔽隧道检测模型构建 DNS 隐蔽隧道检测模型。在现网中使用 DNS 隐蔽隧道检测模型对网络流量进行 DNS 隐蔽隧道检测。

ICMP 隐蔽隧道

隐蔽通道利用了网络协议的特点来秘密进行数据的传输,严重威胁信息安全.大多数 ICMP 流量可以躲避防火墙等网络设备的检测，通常 ICMP 隧道技术采用 ICMP 的 ICMP_ECHO 和 ICMP_ECHOREPLY 两种报文，把数据隐藏在 ICMP 报文的数据部分，利用 ping 命令建立隐蔽通道。由于防火墙对 ICMP 协议开放，恶意攻击者常会利用 ICMP 协议进行非法通信。

ICMP 隐蔽隧道人工智能检测技术，通过搭建 ICMP 隧道流量捕获环境，使用 ICMP 隧道工具集合进行 ICMP 隧道数据传输，基于窗口的 ICMP 隐蔽隧道特征向量（pktlenMax、payload_n-gram-213、pktlenEnt 等）进行训练建立 ICMP 隐蔽隧道检测模型，在现网中，获取 ICMP 隐蔽隧道特征向量，使用 AI 检测模型对网络流量进行 ICMP 隐蔽隧道通讯检测。

HTTP 隐蔽隧道

HTTP 隧道多用于在受限网络连接的条件下在两台计算机之间创建网络链接，用于绕过 IDS、Firewall 一类的安全设备限制，实现基于 HTTP 协议的通信，常常用于内网里面的端口转发与流量代理，HTTP 通信流量往往与正常流量差异性不大，一般通过特征识别不容易被检测出来，HTTP 隧道多用于建立远程桌面和 ssh 连接，负载内容基本没有可读性，传统的特征检测技术很难对 HTTP 隧道通讯进行检测。

基于 AI 的 HTTP 隐蔽隧道检测技术通过提取原始流量 HTTP 流量特征，规则引擎用来打标和清洗过滤 HTTP 流量，经标注的正常流量和 HTTP 隧道流量分别经过自动化特征提取引擎，提取出重要特征向量，根据特征向量建立 HTTP 隐蔽隧道流量识别模型，在现网中，获取 HTTP 隐蔽隧道特征，建立动态自学习 AI

检测模型，通过集成机器学习技术实现高准确性和高召回率的隧道检测模型可对HTTP 隧道进行有效检测与分析。

3.4 高级威胁分析引擎

数字中国战略不断深化演进，加速 IT 行业推进业务创新和产业链变革。国家政府、金融、能源等重点企事业单位和关键基础设施全面联网，城市信息化程度创下历史新高。随着网络空间信息价值密度持续高涨，国家级对抗力量开始入场，高级威胁和未知攻击时刻危及着国计民生。网络空间安全成为我国数字化转型的关键要素，已然上升到国家战略层面。高级持续威胁和复杂未知攻击的检测能力，是现代安全运营体系的核心评价指标之一。

3.4.1 高级威胁的特征及挑战

高级威胁针对攻击目标的业务架构特点，从资产、身份、权限等多维安全切面侦察目标系统的脆弱点，综合利用社工、零日漏洞、钓鱼、后门等多元攻击向量，有规划、有目的地设计每一个入侵、渗透步骤，分阶段逐一规避目标系统的安全防御控制点，最终达成窃数、破坏和长期潜伏的目的。不同于传统网络攻击，高级威胁具有针对性强、组织严密、持续时间长、高隐蔽性和间接攻击的显著特征，攻击链路每一环所采取的步态行为往往与常规的网管和安管操作行为极其相似，辅以各类“毁踪灭迹”的技术手段，成功隐形于信息化系统的日常运营流程。

安全产品孤岛之间的视野裂隙，是高级威胁主体“穿透”防御体系的首要着力点。各家安全产品采用异构的技术栈，对安全要素的定义和规约也不统一，最终形成的安全体系防御能力呈现片段化、不连续的点状散列模式，为高级威胁主体设计规避方案提供了可趁之机。

3.4.2 失陷指标与攻击指标

防守的要点，是巧妙地为对手设置屏障，以拖延时间周期的方式降低攻击效力。识别威胁的指标体系，是防御能力的重要保障。整合全球威胁情报、资产、

漏洞、暴露面信息等多元威胁数据和持续更新的全网 APT 技战法，从终端、网络、云端、移动端、邮件、资产、浏览器、蜜罐等多个维度，深度挖掘情报大数据，提取全面且高度可识别的静态和动态威胁特征指标，有助于在信息化系统内部构建可靠的安全防护滤网。

早期，业界广泛普及应用的失陷指标（Indicator of Compromise，IoC），只是简单提取恶意样本文件哈希值、威胁情报 IP 地址和域名，很容易被威胁主体绕过。随着技术不断演进，安全策略研究人员和计算机电子取证专家，开始致力于从攻击事件在主机侧或网络侧留下的痕迹中提取指标参数，利用多元参数的逻辑组合来定义威胁。受限于商业解决方案的问题域，这类增强的 IoC 也仅限于识别高级威胁攻击链路上某一环节的威胁特征，譬如：在失陷主机上落盘的恶意样本，或在 C2 通信中利用的某种隐蔽信道协议。拥有丰富资金和资源支持的高级威胁主体仍然可以在攻击时效内研究新的规避方法，绕过“孤岛式”安全防御控制点。

在传统失陷指标（IoC）的基础上，有效融合多源扩展安全数据，利用关联分析技术，对攻击从侦察到初始访问，再到数据渗漏或勒索加密的全过程进行安全事件画像建模；针对全网威胁情报中积累的每一个攻击技战术，基于以 MITRE ATT&CK 矩阵为代表的攻击模型，构建相应的攻击指标（IoA），能够从根本上解决当前以异构安全技术栈为基础构建的安全防御体系中原生固有存在着的安全视野不连续的核心缺陷。

3.4.3 高级威胁的检测与识别

纵深防御和安全视野，是高级威胁检测与识别的关键。打破“安全数据孤岛”，落地全局全域安全视野，对现有安全防御体系赋予“上帝视角”，通过增强大数据、关联分析、智能分析、异常行为分析、未知恶意样本深度沙箱分析、威胁图谱、全网威胁情报赋能等新兴技术，实现有效的高级威胁检测、响应和线性预测能力。同时，XDR 以终端检测与响应为基础，从用户网络中已部署的安全设备中获取富化的安全遥测数据，扩展安全视野和检测能力，提升安全事件应急响应速度，同时避免引入更多复杂性。

在技术实现层面，XDR 解决方案重点聚焦终端、流量，从内存、磁盘、流量数据包、代码、日志等多维数据源提取威胁指标数据和上下文证据，面向具体业务场景，择优选取基于异常或基于模式匹配的检测方法，利用监督学习或无监督学习等人工智能技术，建立目标系统的安全行为基线，高效识别高级威胁。

3.4.4 高级威胁的调查与响应

XDR 解决方案引入威胁图谱，全面增强系统的自动化能力，解放安全专家的人力投入。威胁图谱技术，综合应用图分析和机器学习算法，有效建立主机、用户、内外网 IP、域名、文件、进程等实体之间的关系和行为，提供客户业务环境所有端点、网络、用户、应用数据的完全实时可见性和洞察力。针对具体的调查实体对象，威胁图谱全维度可视化地展示其访问域名、访问 IP、访问用户、关联漏洞、关联样本、代码执行行为、访问行为等开展调查任务所需的多元上下文要素及要素间的时序关系。

没有威胁图谱之前，不同实体对象的信息是孤立的，通过威胁图谱所有实体信息及实体间的关系都呈现在一个统一视图和操作界面上，安全专家可以非常方便的基于实体的上下文、事件的关系来进行攻击溯源和研判，快速判定攻击源、优先级和影响面，从而进行响应处置。

3. 5 无代码自动化编排剧本

3.5.1 SOAR 技术简介

在 XDR 解决方案中，SOAR 是一个具备智能协作的安全运营系统，而这其中最核心的是安全编排与自动化，充分使用自动化技术，将人、技术和流程高度协同起来，在帮助企业和组织将繁杂的安全运行（尤其是安全响应）过程梳理为任务和剧本，并提供定制化的流程和控制，实现快速编排响应策略。解决安全运行响应人员匮乏、安全告警多、安全事件响应不及时、重复性运维、等难以度量的问题。

3.5.2 安全编排与自动化技术

安全编排与自动化是 SOAR 的核心能力和基本能力，核心是剧本库和应用库（动作库），这些库可以被安全分析、告警管理和案件管理等功能随时调用。通过该功能，能够真正实现 SOAR 将不同的系统协同联动起来的目标。

3.5.2.1 安全编排自动化

安全编排(Orchestration)的过程就是将团队、流程、技术和工具等各种要素以流程为纲整合到一起以服务于安全运营的过程，即将不同设备或组件能力通过可编程接口（API）和人工检查点，按照业务诉求编排成有序的执行逻辑块，创建手动或自动化执行的工作流步骤，让机器按照编排好的流程执行相应的工作任务。另外，安全编排也适用于识别、防护、检测、响应、恢复等各个环节，通过减少人的参与来降低人为错误因素，以提升编排的工作效率。

无论是自动化的编排，还是人工的编排，都可以通过剧本(playbook)来进行表述，而支撑剧本执行的引擎通常是工作流引擎，通过将预防、调查、缓解、补救等步骤形成一个或多个行动方针剧本，自动或手动协同操作工作流，将重复的、常规的、确定的部分交给机器完成，将新的、复杂的、不确定的交给人工研判处置，并分解运营流程中的任务，抽象成不同类型的自动或手动触发的剧本。

例如针对恶意文件处置可编排如下剧本：当检测到某恶意样本，触发创建的剧本后，搜集主机资产范围搜索相似样本文件，并上传，将分析统计结果传送安全运营团队，供其审核。运营团队研判之后，调用“删除文件”剧本，自动化地下发操作指令，清除恶意文件，在检测引擎剧本的识别下，生成安全事件，随着工作流的推进，其剧本动作也将有序执行。

系统通常内置通用的漏洞或攻击事件响应、钓鱼邮件处置、主机异常登录场景、病毒告警事件、WebShell 检测告警、DNS 异常日志、重大安全事件告警、复盘会议等通用剧本模板，为了方便管理人员维护剧本，内置可视化剧本编辑器，通过傻瓜式拖拽方式进行选择的可扩展安全能力编排，实现动作的选择、特定动

作参数的设置，安全能力的编排的同时支持网络设备、安全设备的配置与运维等任务，方便管理人员维护剧本，降低安全配置工作。

3.5.2.2 安全流程自动化

安全自动化 (Automation)特指自动化的编排过程，也就是一种特殊的编排。安全过程自动化不等于安全编排，编排本身不是自动化，如果编排的过程完全都是依赖各个相关系统的 API 实现的，那么它就可以称为是可以自动化执行的，其核心目标就是为了加速安全流程的标准化、自动化、智能化。因此，要想发挥 SOAR 的核心作用，必先梳理出组织自身的标准安全操作流程和规程。常见的安全业务流程自动化框架如图 1 所示：

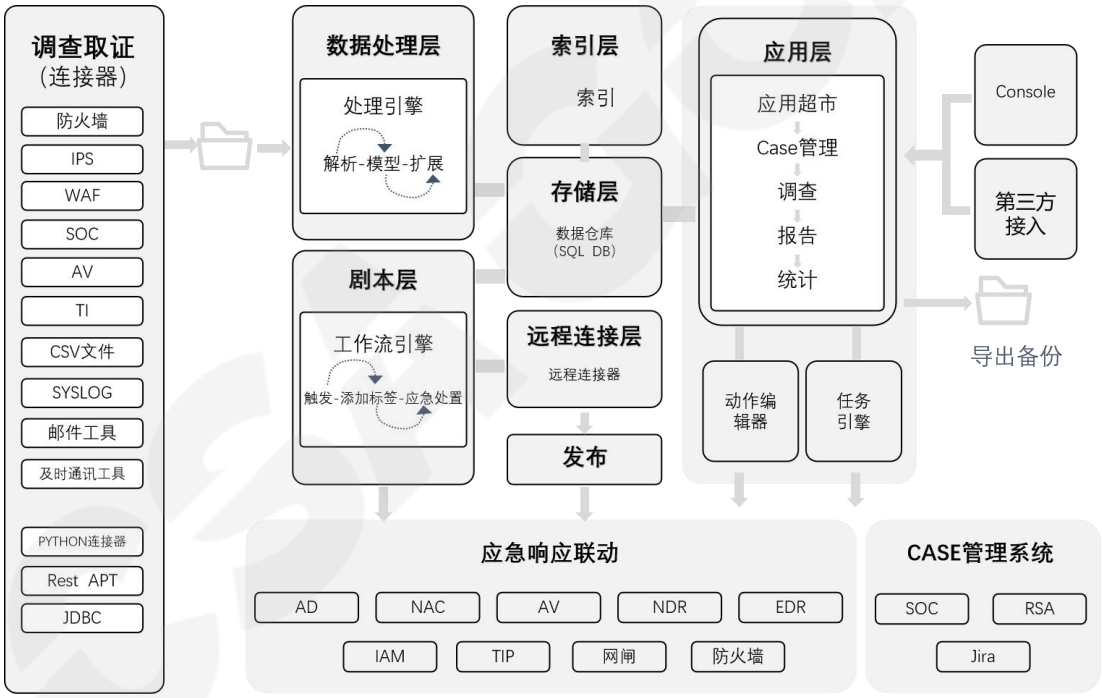


图 3-6 安全业务流程自动化

基于自动化技术的安全运营，将重复的信息安全工作自动化运转起来，通过 SOAR 实现不同的系统协同联动起来，利用技术去监测数据资产以及信息资产中存在的安全风险，再利用标准化流程分析信息输入层、数据处理层、处置响应层的安全风险，持续优化整个过程，达到人、技术、流程一体化。并具备统计、展示与工作流编排、响应过程相关数据的能力，能够生成相关数据报表，维度包括：

工作流、用户、事件、情报等。剧本的编辑维护，应用和动作的管理，可以被安全分析、告警管理和案件管理等功能随时调用。

3.5.3“挂图作战”核心策略

“挂图作战”是一种在网络安全领域中应用的防御策略和战术思想，其核心思想是将攻击者的攻击路径和影响范围以图形化方式展现，采用“行为力导图”“攻击路径图”“对抗指导图”等图形化方式作为核心策略。帮助防守方更直观、全面地理解攻击者的行为以及对组织资产的影响，从而更有效地进行威胁检测、分析、响应等动作。

3.5.3.1 关联案例

网络安全攻击是由一系列攻击技术组成的，因此需要将所有相关联的攻击路径上的安全事件合并，才能更全面清晰地分析和处置。通过自定义归并规则，将安全事件合并形成案例，还原整个攻击路径，并抽出关注的实体，直观地并完整地共享至所有的安全团队。如果攻击路径不完整，可以通过手动搜索缺失的日志，并补全到案例中。

3.5.3.2 生成攻击溯源图

用易于理解的方式表示通过系统实现安全目标的所有路径，生成攻击溯源图，确定事件从哪里开始、经过哪些节点，最终导致问题的产生。 每个实体都将展示详细分析页面，如文件路径、恶意软件类型、危险等级、处置结果等，建立时间线，将事件按照发生顺序排列，以便安全团队追踪事件的发展过程。“对抗指导图”结合实体、人员、要求、阶段等信息，为安全作战团队，提供安全进程指导，帮助团队更快的完成调研、分析、研判、处置、总结的全流程分析过程。

3.5.3.3 识别异常

通过攻击溯源图标识的可疑或失陷资产，查看预分析的情报信息，如识别威胁情报提供的已知攻击者和威胁源、EDR 提供的终端恶意软件感染或异常进程调用、NDR 提供的网络流量揭示异常的连接和异常数据传输。如果预分析的情报信息还不足以做出研判，可以选中关键资产，通过机器学习、预置的剧本或手动分析数据流中的异常情况。通过“挂图作战”策略的应用，团队可以更加高效、直观地处理网络攻击风险，更好的保护其重要资产。

3.5.3.4 安全能力集成

安全设施接口化是 SOAR 得以落地的重要前提条件，SOAR 往往通过应用(App) 和动作(Action)来实现可编排能力和接口调用能力。因此，对要处理的任务，事件，创建各种类型的 APP，是安全能力集成的基础，是编排化安全剧本的基本元素。应用的集成过程通常包括开发、调试、打包、导入四个阶段。

开发：包括应用配置定义、应用编码实现、和应用动作结果渲染；

调试：在测试环境中对开发好的应用进行调试；

打包：按照应用集成框架的开发要求，对开发调试完毕应用进行打包；

导入：将应用导入系统，并纳入系统的应用库进行统一管理。

借助 SOAR 内置的应用管理功能，可以将所有与外部安全设施和运营相关的各种系统和功能映射为内部可识别的应用，友好便捷地集成各类安全工具和产品。应用支持相关开箱即用的应用，支持自定义开发及上传，提供框架便于用户自开发，应用容量不设上限，且在维保期间可根据用户需求定制化开发新应用。

XDR 通过安全编排与自动化能力，支持基于应用工作流来拉通各种安全过程与规程，从而为安全运营人员提供机器协助的解决方案。这些过程和规程可以通过剧本来编排（通过与其它技术的集成）并自动执行以达成预期结果，可实现对突发网络安全事件、特定网络攻击等进行应急预案的制定，实现对突发事件的快

速响应处置。随着高等级的安全应急响应活动越来越频繁，专业化、系统化、自动化等能力越来越关键，SOAR 技术也将会成为 XDR 网络安全应急响应解决方案的一个新常态。

3.5.3.5 威胁情报关联分析

威胁情报关键能力是基于大数据关联分析系统异常状态，以及控制依赖、数据依赖图等多源数据关联方法，对异常流量和攻击行为进行全面检测定位及追踪，追踪溯源技术融合了安全威胁并发追踪溯源技术，通过获取攻击源的信息、设备信息、各层数据流信息，对捕获的数据进行清洗、挖掘与存储，识别相关业务，形成高质量的自有威胁情报库、知识库，并结合外部情报，提供快速查询与获取威胁情报能力。形成的威胁情报中心如图 3 所示：

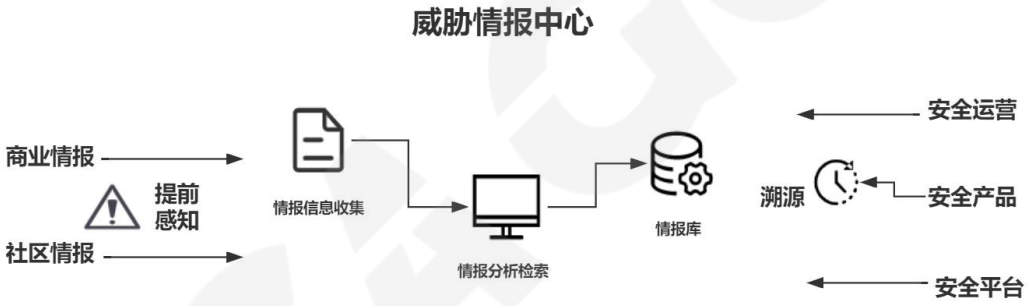


图 3-7 威胁情报中心

通过提前预防已发生在其他地点的攻击威胁，为组织和企业的安全管理提供纵深防御能力。由于威胁是不断变化的，通过动态的手段来对抗攻击者，平台进行线索研判，攻击定性和关联分析追溯威胁源头，有效预测威胁的发生并及时预警。解决因高级威胁或未知威胁导致漏洞利用、主机失陷、病毒感染、钱财勒索等威胁定位问题，以威胁情报为驱动，赋能安全运营、安全产品、安全平台，建立具备威胁溯源、关联分析、攻击画像、事件通告、共享赋能等情报管理能力的情报中心。

3.5.3.6 基于大数据攻击溯源分析管理

攻击溯源本质上是在大量的正常数据中寻找出攻击者在攻击过程中留下的痕迹，并通过这部分痕迹回溯攻击者，即为了应对外部高级可持续威胁（Advanced Persistent Threat，APT）攻击者和内部利益驱动的员工威胁而提出的一种解决方案。由于 APT 攻击往往会长时间潜伏，而少量攻击数据则是伴随海量的业务数据共同产生的，例如每秒几千兆字节数据的业务流量场景，真实的攻击行为数据只有不到几千字节的数据，在这种情况下，利用大数据技术为快速完成攻击溯源带来了新的可能。

网络攻击溯源一般分为三个部分，首先，需要通过安全设备告警、日志和流量分析、服务资源异常等对网络攻击进行捕获，发现攻击；其次，利用已有的 IP 定位、恶意样本分析、ID 追踪等技术溯源反制收集攻击者信息；最后，通过对攻击路径的绘制和攻击者身份信息的归类形成攻击者画像，完成整个网络攻击的溯源。

大数据技术可以收集大量的异构数据，并对这些数据进行清洗，提炼出有价值的攻击痕迹，再通过数据分析和模型关联将这些信息串联起来形成攻击路径，通过攻击路径的反溯找到攻击入口、还原攻击过程。基于大数据攻击溯源总体框架如图 4 所示：

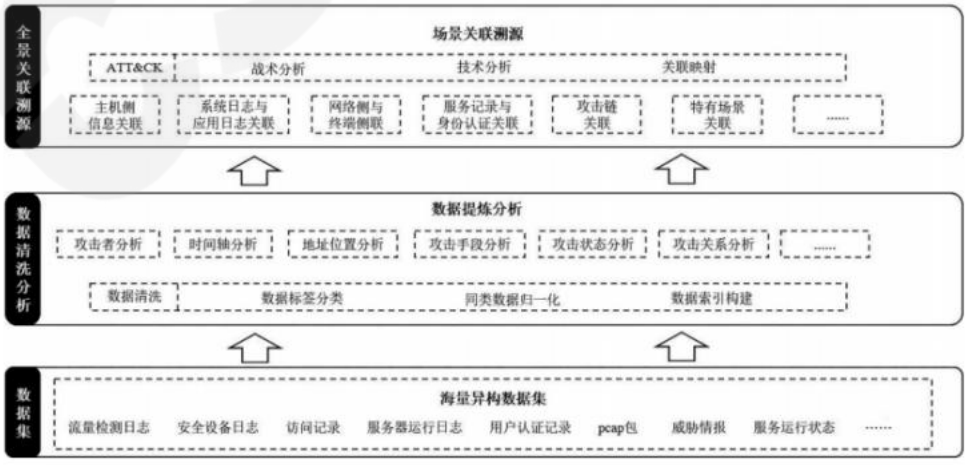


图 3-8 攻击溯源总体框架

数据集层

数据是攻击溯源的基础，整个 APT 攻击过程可能覆盖系统漏洞发现，包括恶意代码植入、远程控制、数据泄露等过程，攻击手段繁杂，收集数据的丰富程度决定了溯源能力的高低，如利用系统漏洞攻击时，系统日志、应用日志、网络入侵检测设备均可监控到部分攻击线索，可完整地绘制一条攻击链。如果主机执行恶意程序等信息则会留下恶意程序执行后的痕迹。利用不同类别的数据集构建一个大的异构数据集，实现大范围地涵盖攻击溯源所需的数据，包括以下数据集：

①网络侧数据集：包含威胁监测设备的攻击日志、入侵防御系统、应用防火墙等网络安全设备日志。

②主机侧数据集：包含业务访问记录、系统日志、系统进程监控数据等。

③辅助佐证数据集：收集威胁情报作为辅助佐证数据集。

数据清洗分析层

分析层的核心目标是完成有价值的数据的初步提炼，为后续的数据分析提供结构化的数据。对数据进行分类、归并和标签化处理，提炼有价值的数据，获取的数据主要涉及结构化、半结构化和非结构化。以防火墙记录的连接关系日志和服务端记录的业务访问记录为例，两种数据都是访问记录，针对此类记录需要提取公共信息和必要的附加信息，并针对冗余数据进行去重，避免冗余信息干扰。使不同来源的同类数据在同一框架规范下进行异构数据清理、去重、归一、索引建设等步骤，形成高质量、有价值的归纳数据。

全景关联溯源层

溯源模型的构建是自动化溯源的基础，围绕着溯源模型进行分析处理，形成自动化溯源调度工作流，在数据清洗分析层基础上进行单场景溯源、全场景关联。完成单场景溯源模型的准备后，再通过 ATT&CK 模型进行全场景关联溯源，ATT&CK 模型由 MITRE 公司提出，它是一个站在攻击者视角来描述攻击中各阶段

用到的技术模型，将攻击划分为战术和技术两部分，该模型涵盖了网络侧数据的映射和主机侧数据的映射，按照攻击者的思路即可梳理出一个完整的攻击过程全景图。

3.5.4 报告管理

报告管理提供了报告模板和事件、任务关联生成自定义报告的能力，旨在进一步简化过程，通常内置报告编辑器，提供编辑报告的素材，包括事件或任务基本信息。报告的模板化与智能化不仅使工作变得更简单，还消除了对手工生成的度量的需要。

3.5.5.1 报告模板

例如事件或任务处置过程中的调用的剧本、应用和处置模型等处置信息，以及证据和结论等痕迹信息，方便用户进行报告的在线编写。根据报告汇报对象，可导入报告模板进行编辑，报告编写完成后，支持报告提交和审核操作，同时报告的审批路径支持自定义配置审核流程和审核人，审核时，可以驳回到任意一级，审核通过的报告支持分享给多人和导出操作。也可通过报告列表中查看各报告的发生时间、提交时间、审核时间、报告概述、报告附件、审核状态、报告结果等信息。

3.5.5.2 事件和任务关联报告

对于等级较高或新型的告警事件，可升级到团队运营进行协同处置，可实时沟通和处置任务。事件和任务响应中的各方以聊天的方式进行实时沟通与处置，支持添加、移除成员，以及设置成员在各任务运营群中的角色。系统自动记录协作处理中剧本、应用和任务的执行结果，以及整个任务处置过程的聊天记录、证据、结论和星标信息，便于实时查看和复盘。处置完成的事件和任务，能在线编辑报告，系统提供编辑报告的素材，如事件和任务处置过程中的调用的剧本/应用，证据和结论等。

3.6 API 中心

3.6.1 背景介绍

在当代安全建设框架中，客户环境往往使用了多个厂商、不同类型的安全设备来完成日常运维任务。在当前企业环境中，这项任务往往通过人工完成，完成整个任务耗时耗力。部分客户可能已经部署过了 SOAR 系统，但是由于各个厂商产品上的差异，集成的工作往往比较繁重，效率较低，而且面对各版本的变化不能很好地进行响应，存在大量重复开发工作。

在此，在已经来临的 XDR 时代，任何安全产品，都需要对外提供 API 来输出自己的业务能力。一个没有 API 的产品是一个停留在上一个时代的产品。

在目前已有的安全运维场景中，常规的 API 需求往往有以下类型：

联动响应类

这一类型的 API 接口是在 XDR 发展初期比较常见的。比如通过入侵检测设备发现外部攻击 IP 联动防火墙进行封堵拦截，将已失陷主机从内网中隔离，向被感染了木马的主机部署专杀工具进行清理，向杀软下发新发现恶意软件的哈希值等。

样本分析类

在安全运维过程中，往往会有机会获得一些文件或者网络包样本。用户往往想知道这些样本是否有问题，或者现有的安全设备是否能够检测。如果用户有配置沙箱或者网络分析设备，会使用这些设备进行分析。同时，很多安全产品也会有一些自动化的分析需求。

这些分析设备很多情况下都是异构的，由于这部分目前是没有业界都认可的标准的，不同厂商的产品之间的接口必定是不兼容的。

溯源取证类

在分析过程中，用户很多情况下会使用全流量，EDR 等工具对攻击的过程进行分析溯源，提取样本，分析进程行为，调查 DNS 请求记录等。

信息上报类

如主机及个人电脑杀毒软件安装情况，全网软件资产列表等。此类数据需要与 EPP 管理系统或者桌管类产品的接口打通后获取。

除了以上类型的 API 之外，一定还存在着我们目前想象不到的 API 类型。

在实际使用过程中，之前的实践往往是产品和产品直接集成，平台和产品直接集成，或者是用户手动直接操作相关安全产品等。这样的做法，周期长，效率低，版本依赖程度高。

基于上述问题，我们提出 API 注册与发布系统，作为一个中间层来适配安全能力的提供者与使用者，提升联动效率，降低研发成本。

3.6.2 API 注册与发布

通过 API 注册与发布，将一个第三方 API 转变为平台内可用服务，实现平台能力的有序扩展。

如何将一个外部 API，转变为内外部可用的 API 需要做以下事情：

指定服务入口点

服务入口点指的是业务调用方来使用该服务时使用的 URL，该 URL 具备以下形式：

${SCHEME}://${DOMAIN-NAME}/${URI}

SCHEME: 在一般的业务系统中，往往采用 http/https 的方式来使用 API.

DOMAIN-NAME: 在较大型企业内部，会通过内部 DNS 的方式来部署业务，但是大部分企业还是会直接使用 IP 来指定服务的访问地址。

URI: 用来在系统内唯一标识 API 资源。

入口点位置：需要注意的是，入口点需要区分集群内与集群外。所谓集群内，我们的定义是一组一起工作的工作负载实例，通过独立的内部网络互相连接，内部之间可以直接访问，但是如果要从集群外部访问内部服务，需要通过 NAT 或者反向代理等方式将内部访问暴露到集群外部。同一个 API 服务的内部入口点和外部入口点是不同的。

内部和外部接口的另一个不同之处在于，如果一个 API 仅仅从集群内部访问，在集群存在内部 DNS 的情况下，可以任意设置内部 DNS。但是如果是对外暴露的服务，其域名或者被访问的 IP 是不能任意指定的。因此引来的一个问题是同一个服务入口是不能够同时服务内部和外部的。

除此之外，我们还需要指定：

API 名称：以字面可理解的形式给该 API 一个名称。

method：请求方法，一般指 HTTP 的 GET 或者 POST。

请求类型：指定请求体的数据格式。

响应类型：指定响应体的数据格式。

请求类型与响应类型需要根据实际情况进行定义，比较常见的数据类型有 json，xml。有一些特殊情况如上传样本，可选择设置类型为二进制。

指定认证方式与授权

任何 API 资源的访问需要经过认证后才能实施。一般来说，API 服务可能需要支持业界常见的一种或者多种标准认证方式。如：HTTP 基本认证，基于 Session

的认证，基于 Token 的认证，OAuth 等。具体使用哪一种，取决于业务使用方的现状，系统安全性要求及成本等方面的平衡。如果采用类似 HTTP 基本认证这种固定式认证数据的方式，建议强制采用 https 方式来承载 API 业务调用请求。

基于安全性考虑以及一些合规性要求，很多场景下会对业务调用方进行限制的需求。

如集群内部访问，会限制调用方的地址来着某子网或者业务逻辑上的命名空间。

在提供对外访问服务时，有可能会需要限定访问客户端的 IP 地址。

指定后端服务

API 服务提供方可能会提供多个后台实例来提供服务。基于提供的服务类型不同，有的 API 提供的是无状态的服务，即在 API 后台实例中不保存状态，整个业务都通过请求的响应来完成。比较典型的是通过 http 提供病毒扫描的服务，只需要告知业务调用端相应文件是否是病毒，至于是哪一个扫描服务执行的，业务调用端并不关心。反之，如果具体的业务与具体执行 API 的实例强相关。比如要调查一个终端上面的进程行为，而相关 API 的提供方是对应 EDR 管理端，那边只有请求被发送到托管相关终端的 EDR 服务端，请求才会有结果。当然，这种情况很多厂商会在自己提供的 API 内部做好处理。

每个服务后端，在正常情况下会就有自己的认证方式，每个服务后端的认证方式需要可以单独进行设置。

数据适配

在业务应用和后端服务之间，数据传输的格式，编码方式，参数名等可能是不匹配的，作为中间层的 API 平台需要有这样的能力，对业务侧与后端服务之间的请求和响应做格式方法的调整。以适配两端让调用能够正常进行下去。可能需要进行以下一些调整：

格式转换，比如 JSON 转 XML

在请求头，请求行等请求部位中增加参数

向请求体的结构化数据中增加参数

对参数进行重命名

对数据的修改可以有很多方式，除了平台可以提供的一些标准化操作外。针对一些特殊的接口，可以开放一些服务注册到平台或者开放一个插件进行定制化处理。

测试 API

在创建好 API 后，平台提供相关页面对已创建好的 API 服务进行测试。以验证服务构建的正确性。

API 发布与下线

在完成我们的 API 的配置与测试后，我们需要正式将该 API 发布至网关从而使得内部或者外部的调用者可以正常使用该 API。

当 API 需要重新发布或者停止服务时，需要将 API 从网关上下线。停止提供服务。

3.6.3 集成与应用

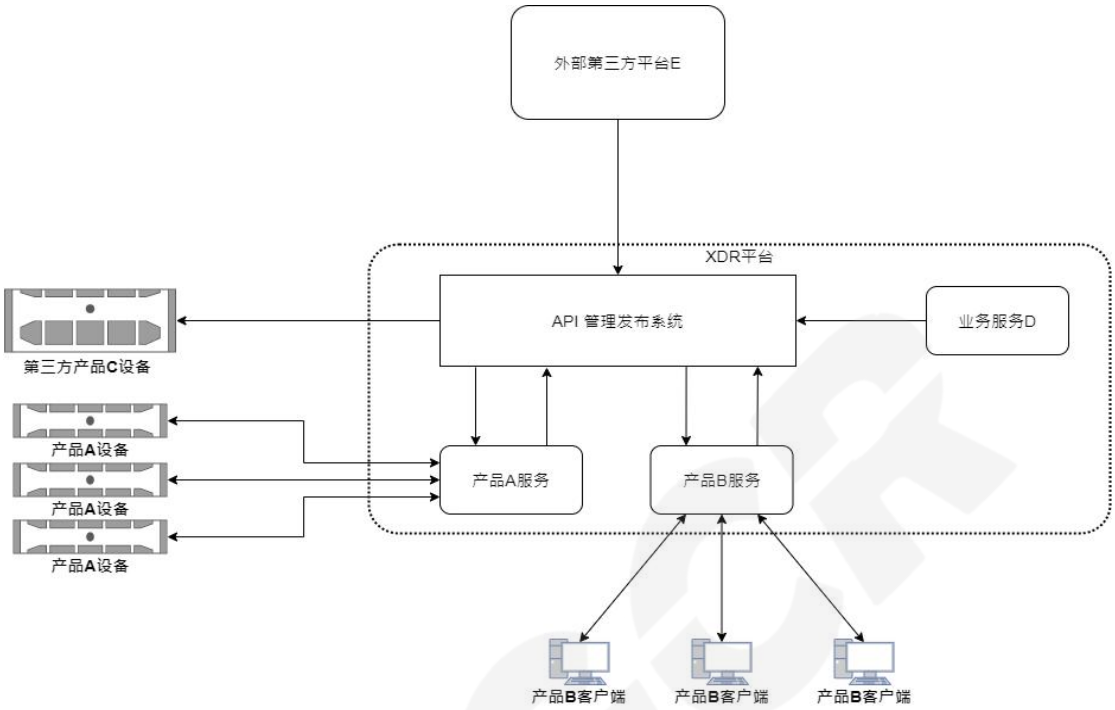


图 9

如图 9 所示，首先，在 API 的集成与应用场景中，我们认为有如下几个角色：

API 服务提供者

API 服务使用方

API 管理发布平台

同时，这里还有内部外部的概念区分，一般来说，一个平台内的多个服务会部署在同一个虚拟子网或者 VPC 中，相互直接从网络层面是可以互通的。我们称这种情况为内部。平台往往会通过一个或者多个网络地址/网关对外提供服务，通过平台对外提供服务进行访问的调用者或者服务提供者，我们成为外部。

在这个层面来讲，API 管理服务既是整合多个厂商能力的支点，同时也是向外输出厂商能力的门户。在大量异构的安全运营场景中，这样的能力是非常关键和重要的。

抛开平台以外，在常规业务场景中，API 服务的提供者和使用者往往有以下情况：

同时是服务提供者和使用者的平台内部服务

这种情况往往是和平台同厂商的标准化产品，如上图中的设备型产品 A 和终端型产品 B。相关产品团队通过在平台内部开发相关产品的服务来向 API 管理系统注册发布 API。

在这种情况下，设备或者客户端与平台之间的通讯和调用由相关产品服务来负责，这部分内容，对于平台来说是不需要考虑的。上一节中提到的路由，负载均衡等工作全部由相关产品的服务来提供，可以有多种方式，包括直接使用。

同时，同一厂商的产品之间往往有联动的需求。在这个时候，部署在平台内的产品服务直接调用其他产品在 API 平台发布的接口即可实现联动需求。

平台内部使用者

很多情况下，XDR 平台会内置一个轻量级的 SOAR 或者类似的系统，甚至很多产品经理有可能会设计出各种功能。当需要各种 API 能力时，该服务可以直接使用 API 平台发布的各类 API。图中的业务服务 D 即是此种。

提供 API 能力的外部设备/系统

不论是外部的第三方设备，还是厂商自己的产品，都存在一种情况，那就是存在一个独立于平台的系统需要将能力输出到平台。同时，其产品团队没有意愿或者能力在平台上开发一个服务来维持外部系统和平台之间的通信与交互。如果该系统提供了供第三方调用的 API。平台方或者项目的运营方可以利用 API 管理服务的能力，将该能力集成到平台里。

外部使用者

很多中大型用户的安全运营往往会采用异构方式进行，通过购买不同厂商的

产品来规避因为某厂商的问题导致整个企业出现风险。API 管理系统作为各类安全能力集中的平台，天然具备向第三方输出安全能力的功能。

3.6.4 小结

API 中心作为 XDR 平台的基础能力部分，对内，使实现平台自身能力的编排与扩展成为可能；对外，南北向接口能力，使自身平台的建设成为可能；API 中心能力将成为客户选择 XDR 平台的关键指标。

3.7 CICD

3.7.1 基础安全

CI（Continuous Integration）是在软件开发期间自动化和集成来自许多团队成员的代码更改和更新的过程。在 CI 中，自动化工具在集成之前确认软件代码是有效且无错误的，这有助于检测错误并加快新版本的发布。

CD（Continuous Deployment）是指不断将新软件投入生产的能力，从而自动化向基础设施环境交付应用程序。CD 是 DevOps 的一部分，它有助于缩短软件开发生命周期。

在基础安全方面，至少要保障人、技术、流程方面的安全:

人：要建立安全管理组织，建设组织级的安全文化，开发人员、测试人员、运营人员都要对各自阶段的安全负责，在 CICD 过程中的对需求开发、安全交付、安全运维进行安全风险控制。

技术：对基础资源、操作系统、数据库、中间件等使用有效开展安全风险控制的基础设施，在需求开发、安全交付、安全运营的各阶段使用安全工具，并将安全工具嵌入到 CICD 过程中，实现自动化的安全风险控制。

流程：CICD 的过程要可以重复，需要将需求开发、安全交付、安全运营流

水线中的安全工作固化，无论由谁负责都能实现相同的安全风险控制能力和水平，可以通过撰写发布制度、规则，实现流程化的安全风险控制。

3.7.2 需求开发

按 CICD 的过程，在需求开发阶段包括需求、设计、开发三个阶段。

需求：通过获取客户或业务的建设系统或更新系统的需求，将安全工作左移到应用生命周期的源头，在应用的需求阶段进行安全风险控制，定义安全需求并采取安全风险控制措施，从而控制开发过程的安全。

设计：根据业务架构确定系统架构、网络架构以及设计，并在过程中开展安全风险控制。通过了解相关的法律、法规、标准，分析攻击面、开展威胁建模，参考业界最佳实践，来识别应用可能面对的安全风险和威胁，制定风险控制措施，确保应用系统的安全。

开发：根据安全需求和安全设计，在编码过程中的进行安全风险控制。使用安全编码规范、代码检测、漏洞扫描、渗透测试等多种方面控制开发阶段的安全风险。

3.7.3 安全交付

安全交付是从代码提交到应用交付给用户过程中实现安全，确保交付给用户最安全的应用。在些过程中要实现资产安全治理、安全构建、安全测试、安全部署。

资产安全治理，在安全交付过程中，与应用相关的资产和关联关系都被有效定义、记录，交付内容完整、一致并且可以被追溯。包括：源代码、脚本、依赖关系、发布制品、配置等安全内容。

安全测试，这是一个验证安全需求、安全设计的过程，尽量发现并减少应用的安全风险，提升应用的安全质量。

安全部署，通过系统配置、发布、安装等一系列变更操作，向最终用户交付应用，并保障此过程中的安全。同时，为安全运营准备相关的所有交付材料。

3.7.4 安全运营

安全运营，在应用发布以后，在运营过程中使用监控、运营、响应等手段实现安全运营。

安全监控，在应用运营过程中，对基础设施和应用的运行状态进行监控，识别内部和外部的安全事件和风险。

安全运营，对于安全监管发现的安全问题和风险，进行安全分析、安全检测、安全风险识别，并通过调整配置、生产变更等手段进行安全处置，减少安全风险对生产运营的影响。

安全响应，基于应用的业务架构、系统架构、网络架构建立安全应急预案，并开展安全应急演练，以确保可以及时控制安全风险，减少安全风险，保障业务连续性。

3.7.5 CICD 与 XDR

随着软件规模和复杂性的增加，安全防御也变得愈发重要。传统的安全防御手段往往只关注边界防御，忽视了内部网络和终端设备的安全。而 XDR 则强调全面的安全事件检测和响应能力，涵盖了终端、网络、云环境等多个维度。它通过整合和分析各种安全数据源，并借助人工智能和机器学习等技术，实现了精准的威胁检测和快速的事件响应。

CICD 和 XDR 在软件开发和安全防御中有着千丝万缕的联系。

首先，CICD 为 XDR 提供了数据源。由于 CICD 的持续集成和持续交付特性，软件开发团队可以实时获取到各种开发和部署活动的数据，包括代码变更、部署日志、运行指标等。这些数据对于 XDR 来说是宝贵的，可以用于检测异常行为、

分析攻击路径等，帮助安全团队制定有效的安全策略。

其次，XDR 为 CICD 提供了安全保障。安全漏洞和恶意攻击往往会导致生产环境的故障和不稳定，严重影响软件的交付周期和用户体验。通过 XDR 的威胁检测和响应能力，可以及时发现并应对安全事件，保障软件交付的稳定性和质量。

此外，CICD 和 XDR 还可以通过自动化和标准化的方式实现更高效的软件开发和安全防御。CICD 可以通过自动化测试和部署，提高开发团队的工作效率；而 XDR 可以通过自动化事件响应和威胁狩猎，降低安全团队的工作负担。同时，通过标准化的工具链和流程，可以提高开发和安全人员之间的协作效率，减少误解和沟通成本。

第四章 生态现状洞察

4.1 数字化评价指标与可视化

4.1.1 XDR 管理性指标和评价

XDR 是以威胁检测和响应为中心的整合安全平台解决方案，通过前端 XDR 组件遥测进行高级安全分析，通过数据预处理和关联分析来减少误报，交付误报数量较少且高质量的告警。

XDR 目标在于降低运营成本并提供更好的威胁检测能力，XDR 后端服务一般为统一分析平台，集中式数据分析，对所有安全组件统一策略管理；不同安全组件之间通过 API 注册管理来实现更好的响应用例，XDR 可以从终端、云、网络等多个点检测 IOC，也能从一个通道检测其他通道进行响应。

建立 XDR 指标体系需要结合组织业务安全目标，明确关键性能指标，并确定如何度量这些指标。此外需建立量化指标评价体系，以便实时可量化的观测 XDR 性能并作出及时调整，还需要考虑数据来源、数据质量、数据分析和数据可

视化等方面问题。

XDR 指标体系整体可以分成管理指标和技术指标。其中管理指标是通用的威胁检测和响应能力指标，是对可管理的威胁进行处置的安全能力的衡量。技术指标针对不同的安全组件有不同的检测和响应的技术指标，文中会分具体的不同的安全组件来分别进行阐述。

建立 XDR 指标体系一般需要考虑到以下方面：

确定业务安全目标：首先需要明确组织业务安全目标，这有助于明确运营目标和度量。例如，如果组织业务安全目标是保护客户数据，那么 XDR 目标应该是检测和阻止数据泄露相关威胁，如果是保护业务连续性，那么首要目标应该是组织控制破坏或者勒索相关威胁。

确定关键技术指标：例如检测率、误报率、平均响应时间等。这些指标应该与业务目标相关，能够标准化衡量 XDR 是否达成目标性能参数。

确定指标度量方法：为了确保指标的可测量性，需要明确如何度量这些指标。例如，检测率可以通过确定检测到的安全事件与所有安全事件的比率来度量。误报率可以通过确定被确定为安全事件但实际上是误报的事件与所有检测到的安全事件的比率来度量。

确定度量频率：需要确定指标的度量频率。这有助于确保数据的准确性和实时性。例如，某些指标可能需要每小时度量一次，而其他指标可能只需要每天度量一次。

建立指标报表：需要建立指标报表系统，以确保团队成员和管理层都能够及时获得相关指标的量化数据信息。指标报告应该易于理解，可以清楚地显示指标的趋势和表现。

XDR 作为整合安全平台，首先建立管理类的评估指标体系，综合评价 XDR 的检测和响应能力，这样可以帮助安全团队更好地了解各种安全组件的性能和效

果，并选择最适合的安全组件：

1.威胁检出率：指 XDR 组件能够检测到网络威胁的能力，如网络攻击、漏洞利用、恶意软件、蠕虫病毒、勒索攻击等。较高的威胁检测率通常意味着组件能够更好地识别和防御攻击，从而减少潜在的风险和损失。

2.异常行为识别率：指 XDR 组件能够识别异常行为的能力，如异常网络流量，隐蔽隧道，异常进程行为，异常登录、异常访问等。一般通过正常行为基线学习来判定异常，异常检测往往误报率较高，如果能够相对精准的异常告警，甚至可以发现未知威胁；更高的识别率表明 NDR 解决方案可以更好地检测和应对威胁，从而降低潜在损失。

3.安全可视化能力：指 XDR 组件可视化分析视图的质量和深度。如果组件能够提供直观的聚合视图和可视化工具，那么它就能够帮助安全团队更好地理解威胁和采取行动。

4.安全整合程度：指 XDR 组件的统一运维管理和运营分析管理便利性，支持统一安全策略管理和告警优先级管理，支持统一的安全运营分析，支持一站式的多安全组件的统一平台管理，通用管理工作流体验。

5.安全数据关联深度：指 XDR 的安全数据关联分析的质量和深度。安全数据的维度是否足够丰富，安全数据的字段是否统一，自动化关联和确认告警来减少漏报，多个安全组件的弱告警组合升级成强告警信息，对告警快速分级；此外还包括安全组件间实时共享威胁情报的能力。

6.自动化编排能力：指 XDR 为重复性工作和任务提供自动化编排功能的能力，包括低代码水平和可编程能力，好的编排能力能够让分析师可视化的进行运营流程的编排，覆盖更多的安全应急预案；支持 XDR 平台提供与工作流平台集成接口，提供集成响应选项，来自所有安全组件的上下文信息并支持快速处置。

7.数据平台可维护性：XDR 平台一般具备大数据分析平台，数据分析平台的稳定性和数据检索性能也是 XDR 重要的衡量指标，一般需要支持可靠的数据存

储功能，支持低成本存储选项或混合存储来降低长期存储成本。

4.1.2 EDR 指标和可视化

端点检测与响应（Endpoint Detection & Response，EDR）是一种新型的、智能化和快速迅捷的主动防御技术，遵循自适应安全架构，从预测、防护、检测和响应四个维度，实现持续性安全防护，贯穿安全威胁事件的整个生命周期。EDR 实时监测端点上发生的各类行为，采集端点运行状态，在后端通过大数据安全分析、机器学习、沙箱分析、行为分析等技术，提供深度持续监控、威胁检测、高级威胁分析、调查取证、事件响应处置、追踪溯源等功能，及时检测并发现恶意活动，包括已知和未知威胁，并快速智能地做出响应，全面赋予端点主动、积极的安全防御能力。

EDR 的使用指标

根据行业、公司、以及安全管理人员的不同偏好，EDR 可用在不同的地方，也会产生对应的指标。以下阐述常见的使用指标

部署率、覆盖率

部署率、覆盖率指的是 EDR 产品在企业所管理的设备终端的安装率、部署率等。这是最常见的指标之一。

部署率、覆盖率有时也会延展到更深的层次，比如

EDR 产品客户端的版本合规率，用来确保 EDR 产品本身升级到企业所要求的版本，来解决兼容性、功能性等问题。

EDR 客户端的最后一次连接时间，用来确保 EDR 的信息能被后台及时接收到，从而可以快速响应

资产收集相关

EDR 中一个重要功能是收集终端中的相关资产，比如软硬件信息、软件名称、版本号；有部分 EDR 产品也会收集账号资产信息、中间件信息、数据库信息等。

由此而展开的指标包含，非标操作系统比率、非标软件比率、账号资产盘点清单、账号变更等衍生指标

系统加固类

EDR 通过对终端进行定期安全检查，来发现其中的问题，并被动建议或主动要求进行加固。其中的安全问题包含，风险账号（弱密码、重复密码等）、漏洞（操作系统、应用程序漏洞等）、基线（操作系统基线、中间件基线、数据库基线等）、补丁修复（虚拟补丁、或修复建议等）。

而加固手段有黑白名单（进程、网络、行为等）、虚拟补丁等。

由此而展开的使用指标有：

风险账号的数量、漏洞数量、危险级别等、基线不合规律、补丁修复完成率等

威胁检测类

能对内外部的攻击行为进行主动检测，其中包含各种漏洞攻击、跨站脚本、提权等异常行为。

其中展开的指标有：

高危事件事项、已处理事件数量、误报率、策略调整次数等

响应取证类

针对全网的安全威胁进行可视化展示，能够针对安全威胁自动化地进行隔离、修复和补救，自动完成安全威胁的调查、分析和取证工作，降低事件响应和取证

分析的技术门槛，不需要依赖于外部专家即可完成快速响应和取证分析。

扩展的相关指标：自动化修复率

4.1.3 NDR 指标和可视化

NDR 作为 XDR 核心组件，通过全流量检测分析和响应处置的，对威胁进行高效的检测和响应。NDR 使用机器学习、高级分析和特征分析来检测企业网络上的可疑行为。NDR 不断地分析原始流量，以构建反映正常网络行为的模型，当检测到异常的流量模式时会发出异常警报。

NDR 融合了传统的基于规则的检测技术，以及机器学习和其他高级分析技术，用以检测网络中可疑行为，尤其是失陷后的痕迹。NDR 通过 DFI 和 DPI 技术来分析网络流量，通常部署在关键的网络区域对东西向和南北向的流量进行分析，一旦发现异常后进行可管理响应，包括专家人工专家分析和自动化编排。

中大型组织一般都会对多个关键网络节点的镜像流量数据进行威胁检测，因此在这种情况下，使用分布式探针和整合平台架构是非常合理的。在探针侧进行数据采集、在平台侧进行数据汇总及管理，后期也便于和其他产品联动。平台侧需要强大计算能力，因此平台侧选择大数据架构比较合适，大数据架构提供的信息存储能力、信息检索能力、信息计算能力，可以有效提升我们的异常分析和数据检索能力。NDR 可以整合威胁检测沙箱，通过流量数据还原网络传输的样本数据投递到沙箱进行威胁判定，能够相对精准的判断网络传输或下载的威胁情况。

NDR 技术指标可以从安全和流量解析能力两方面来进行评价，可分成安全能力指标和流量分析能力指标：

安全能力指标包括：

1.检出率：指被检测到的威胁数量与总威胁数量的比率。高检测率表示 NDR 能够检测到更多的威胁。

这里可以具体细分到不同场景威胁检测率：

入侵检出率：指被检测到的网络入侵攻击事件和实际统计的总入侵事件数量的比率。高检测率表示 NDR 能够检测到更多的网络入侵攻击事件。

恶意样本检测率：指被流量还原后检测到的恶意样本数量与总恶意样本数量的比率。高检测率表示 NDR 能够检测到更多的恶意样板。

完整性检测率：指被检测到的未经授权的数据访问事件的数量与总未经授权的数据访问事件的比率。高完整性检测率表示 NDR 能够检测到更多的未经授权的数据访问事件。

数据泄露检测率：指被检测到的数据泄露事件数量与总数据泄露事件数量的比率。高数据泄露检测率表示 NDR 能够检测到更多的数据泄露事件

2.误报率：指被误报为威胁的事件数量与总事件数量的比率。低误报率表示 NDR 的报警更加准确。

3.平均检测时间（MTTD）：指从威胁发生到被 NDR 检测到的平均时间。较短的平均检测时间意味着 NDR 更加及时地检测到威胁。

4.平均响应时间（MTTR）：指从 NDR 检测到威胁到响应该威胁所需的平均时间。较短的平均响应时间表示 NDR 能够更快地响应威胁。

5.威胁场景覆盖率：一般 NDR 需要能覆盖到主要的威胁场景，包括漏洞攻击、蠕虫、木马后门，APT，钓鱼攻击，挖矿等等。

流量分析能力指标包括：

1.网络协议解析覆盖类型（Supported Network Protocols and Traffic Types）：指 NDR 组件支持的网络协议和流量类型范围和覆盖率。如果组件能够支持多种网络协议和流量类型，那么它就具有较强的可扩展性和适应性。

2.网络协议解析能力：协议解析是后续异常流量分析的根基，应从 ISO 七层模型和应用领域两个维度支持尽可能全的通讯协议。NDR 产品将协议解析作能力视为核心技术，除了链路层、传输层，网络层等基础协议外，应用层可解析还原的协议的数量和能力是

3.网络协议还原深度：指 NDR 组件支持网络协议解析的协议栈深度，是否能够支持到应用层核心协议字段，包括数据包的头部信息和 Payload 信息。能够将流量数据以不同的统计维度进行透视分析，将 HTTP、DNS、SMTP、POP3、邮件等等数据还原溯源路径。

4.网络流量分析精度：指 NTA 组件检测到威胁的准确性和完整性。较高的网络流量分析精度通常意味着组件能够更好地识别和防御攻击，从而减少潜在的风险。

5.其他网络性能指标：丢包率、流还原率、网络吞吐量、解码率等等。

4.1.4 IAM 指标和可视化

IAM（Identity and Access Management，身份识别与访问管理）是一种安全技术和管理工具，IAM 作为 XDR 的核心组件，它可以帮助企业实现身份验证、授权和控制以及审计。IAM 具有身份认证、访问控制、身份管理、安全管理、审计等功能；IAM 可以帮助企业实现访问控制，确保只有授权的用户才能访问网络资源；实现安全审计，记录用户的访问行为，以便及时发现安全威胁；实现安全管理，确保企业的数据安全。

同时，IAM 可以与 XDR 的其他组件联动，以保护企业的数据安全。IAM 可以与 EDR 组件联动，以发现和响应内部网络的攻击行为；IAM 可以与 DLP 组件联动，以防止敏感数据的泄露；IAM 可以与 SIEM 组件联动，以收集和分析安全日志，发现潜在的安全威胁；IAM 可以与 NDR 组件联动，以确保只有授权的用户才能访问网络资源。

IAM 在使用过程中，主要的评价指标分为：认证、授权与访问控制、身份管

理、安全管理和审计等几个方面，依据使用的侧重点不同，对常用的指标简述如下：

认证相关

认证相关的二级指标，主要包括：身份验证、认证策略、认证机制、认证管理、认证安全性等。其中，

身份验证是指确认用户身份的过程，可以采用多种方式，如密码、数字证书、生物特征等；认证机制应支持目前常见的认证因子应包含口令、数字证书、手机短信认证、证书认证、人脸识别、声纹识别、指纹识别、虹膜识别等；

认证策略是指认证的规则和流程，可以指定认证的方式、认证的频率、认证的级别等；

认证机制是指认证的技术和方法，可以采用多种技术，如加密、数字签名等；多个认证因素可以灵活地进行组合认证，形成多种认证方式。

认证管理是指认证的管理和控制，可以指定认证的管理者、认证的审核者等；

认证安全性是指认证的安全性和可靠性，可以采用多种技术，如双因素认证、多因素认证等，以确保认证的安全性和可靠性。

授权与访问控制相关

授权与访问控制相关的二级指标，访问控制是指对用户访问资源的控制，主要指标包括：访问控制要素、访问控制策略、访问控制机制、访问控制管理、访问控制安全性等。其中，

访问控制策略是指访问控制的规则和流程，可以指定访问控制的方式、访问控制的频率、访问控制的级别等；

访问控制机制是指访问控制的技术和方法，可以采用多种技术，如加密、数

字签名等；

访问控制管理是指访问控制的管理和控制，可以指定访问控制的管理者、访问控制的审核者等；

访问控制安全性是指访问控制的安全性和可靠性，可以采用多种技术，如双因素认证、多因素认证等，以确保访问控制的安全性和可靠性。

身份管理相关

身份管理相关的二级指标，主要包括：身份管理策略、身份管理机制、身份管理的管控、身份管理安全性等。其中，

身份管理策略是指身份管理的规则和流程，可以指定身份管理的方式、身份管理的频率、身份管理的级别等；

身份管理机制是指身份管理的技术和方法，可以采用多种技术，如加密、数字签名等；

身份管理的管控是指身份管理的管理和控制，可以指定身份管理的管理者、身份管理的审核者等；

身份管理安全性是指身份管理的安全性和可靠性，可以采用多种技术，如双因素认证、多因素认证等，以确保身份管理的安全性和可靠性。

安全管理相关

安全管理相关的二级指标，主要包括：安全策略、安全机制、安全管理的管控、安全审计等。其中，

安全策略是指安全的规则和流程，主要包括安全管理的方式、安全管理的频率、安全管理的级别等；

安全机制是指安全的技术和方法，可以采用多种技术，如加密、数字签名等；

安全管理的管控是指安全的管理和控制，可以指定安全的管理者、安全的审核者等；

安全审计是指安全的审计和监控，可以采用多种技术，如日志审计、安全扫描等，以确保安全的审计和监控。

审计相关

审计相关的二级指标，主要包括：审计策略、审计机制、审计管理、审计安全性等。其中，

审计策略是指审计的规则和流程，可以指定审计的方式、审计的频率、审计的级别等；

审计机制是指审计的技术和方法，可以采用多种技术，如日志审计、安全扫描等；

审计管理是指审计的管理和控制，可以指定审计的管理者、审计的审核者等；

审计安全性是指审计的安全性和可靠性，可以采用多种技术，如数据加密、数据完整性等，以确保审计的安全性和可靠性。

4.2 XDR 与态势感知平台的关系

4.2.1 态势感知平台概念

态势感知平台是由数据本原驱动，通过威胁情报、AI、机器学习等新兴技术，帮助用户构建一套从被动防御向主动安全转型的安全能力体系，其对可能引起网络态势变化的各种安全要素进行收集并处理，利于大数据平台进行智能化分析理解，最终实现对网络安全态势的全面感知。

态势感知平台定位为客户的安全大脑，是一个检测、预警、响应处置的大数据安全分析平台。其以全流量分析为核心，结合威胁情报、行为分析建模、UEBA、失陷主机检测、图关联分析、机器学习、大数据关联分析、可视化等技术，对全网流量实现全网业务可视化、威胁可视化、攻击与可疑流量可视化等，帮助客户在高级威胁入侵之后，损失发生之前及时发现威胁。

4.2.2 态势感知平台行业实践情况

安全信息全面、实时的获取和分析是实现态势感知的关键。当前国内主要态势感知解决方案厂商已通过日志审计、SIEM 等技术手段实现了网络设备信息、安全设备信息以及网络流量威胁分析数据的采集获取。

但是态势感知平台与其他安全产品的对接仍然缺乏统一接口。虽然目前业内正在努力通过“能力中台化”、开放式应用程序编程接口（API）等方式提升自身态势感知平台与第三方产品对接的标准化水平，但短期内安全厂商的产品和平台缺乏相对统一接口的问题仍将普遍存在，因此，中大型客户的态势感知平台建设项目的定制化开发依旧难以避免。

持续增强“网络安全采集、分析、响应”能力依旧是态势感知解决方案的发展核心。安全厂商不断加大在先进技术领域的人员和资金投入，大数据分析、机器学习等技术已经广泛应用到态势感知解决方案的众多功能组件中，并有效提升了日志泛化、威胁检测、关联分析、溯源取证等能力。

此外，威胁情报将在威胁判定和溯源方面发挥越来越重要的作用，甚至能够帮助企业提前感知同行业相关威胁，实现恶意威胁的主动防御。通过优质的威胁情报信息融入到态势感知平台进行威胁事件关联分析和溯源，对提升平台威胁判定的准确性以及对新型威胁的及时感知能力效果明显。

国内主要态势感知解决方案已经解决了“网络安全采集、分析、响应”功能的基础满足，但通过功能所展现出来的技术实力和经验积累仍然存在差异。除了威胁检测这一核心能力，对威胁事件的编排与响应成为态势感知重点发展的能力。

随着企业规模的快速发展和 IT 资产的不断增加，态势感知平台获取和管理的数据量与日俱增，企业安全运营人员需要面对繁多的告警信息和安全事件。自动化 / 半自动化的分析和处置能力能够将安全运营人员从简单重复的工作流程中解放出来，腾出更多精力处置突发和复杂的安全事件，降低重复性低效工作，提升工作价值同时，态势感知的编排与响应能力不应仅仅局限于设备一键阻断、添加黑白名单等简单操作，而是更多的与企业真实业务结合，制定规范化、流程化、协作化的高价值安全能力。

作为主动网络安全防护体系的“智慧大脑”，态势感知平台根据不同行业客户的具体业务场景进行适配，尤其是针对中大型客户的安全需求和业务特点提供策略调整和定制化开发。例如政府和行业监管部门关注的监管态势感知平台、广大企业关注的运营态势感知平台、工业企业关注的工业互联网态势感知平台等，均具备自身独特的需求和关注功能点，从而使态势感知平台发挥更精准的安全防护作用。

4.2.3 XDR 与态势感知平台的差异

态势感知（Situation Awareness）从 NDR 演进而来的态势感知，更关注通过大数据、特征检测、机器学习算法等技术对全流量进行过滤，加深对于安全趋势的预测，侧重点在安全告警的聚合、安全态势的建模。而且由于态势感知的数据大多都来自于 NDR 设备，优点在于可以快速镜像出流量进行旁路检测，不会对网络链路造成影响，从而快速的在网络侧进行大面积的安全视野覆盖，但伴随而来但是只有网络侧的数据输入形成聚合分析，容易造成海量告警难以处置的困境，同时态势感知往往不具备拦截功能，在实战攻防对抗场景，XDR 的响应处置、联动封锁的功能，可以使安全事件的影响面最小化，尽可能的保障用户的资产和信息系统安全。

态势感知由于缺乏端点上的监测数据，不可避免的难以发现攻击者在端点上的具体行为，更多的是展示攻击者攻击路径、攻击入口，并且网络侧能够覆盖的 ATT&CK 技战术较少，在对抗不同攻防场景的情况下显得乏力。其对接能力也相对固定，与其他设备的对接一般是联动处置，或者将其他设备分析过后的告警接

入平台，是一个依托网络流量为基础构建的威胁检测和安全态势平台。

XDR 通过对接网络侧和终端侧的不同安全组件，首先定义遥测数据的标准，所有对接的组件都以该标准进行一手数据上报，其次将所有不同来源的异构数据放在一起分析，编织出大的数据网络，能够包含整个攻击发生的情景、上下文，包括攻击入口、端点上的操作、攻击范围扩散等等，能够感知的安全态势更细致更全面，其检出的结果不同于传统的单个设备的告警，而是一个完整的、包含攻击全过程的安全事件，仅端侧检测项就可以覆盖 ATT&CK 技战术超过 80%种，是态势感知在网络侧收集数据所不能比拟的。通过遥测数据的深度采集，能够发现端点上的各种危险行为和操作，可以有效对抗高级攻击手法和隐蔽威胁。与 XDR 对接的设备除了联动处置的动作下发，还要按标准提供一手数据，或者将已经分析过的二手告警上报作为 XDR 数据编织过程中的富化信息。是一个依托遥测数据为基础、可以广泛对接各种安全组件的威胁深度检测和统一安全平台。

4.2.4 XDR 优势分析

XDR 是安全产业未来发展的重点业务方向。深入理解 XDR 的架构规划、架构设计、系统设计、关键重点场景，基于业务流落地各层各级管理规定，有助于解决现在面临的众多安全设备协调的问题。

4.3 XDR 与 SIEM 平台的关系

尽管EDR可以收集和关联多个终端的活动，但却局限在终端内部，无法打通网络、其他终端、以及SIEM等平台。XDR有效的解决了这个问题，将检测范围扩大到终端之外，并提供跨终端、网络、服务器、SIEM等的检测、分析和响应。

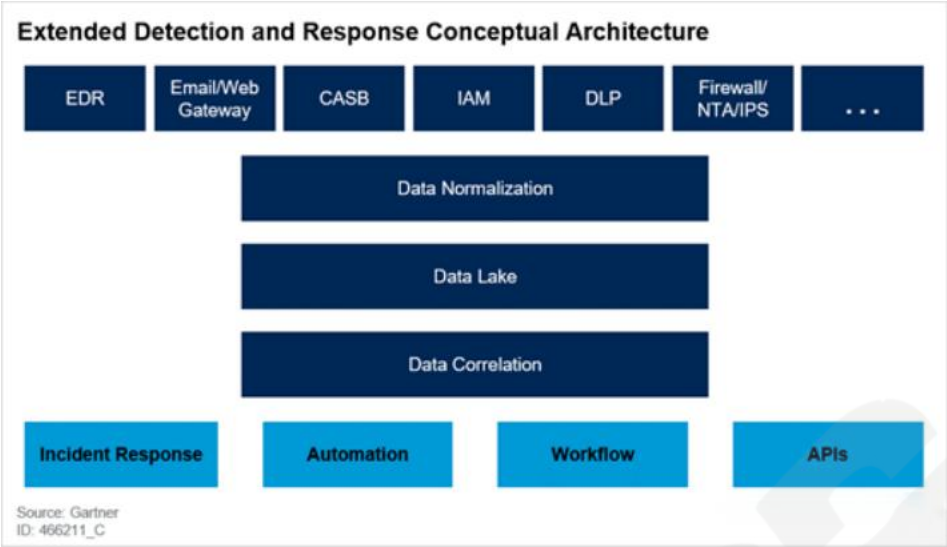


图 1

同时 XDR 可以提供一个跨多个工具和平台的统一的管理视图，管理视图中包括了这些攻击的详细信息，可以帮助分类、调查和快速修复工作。XDR 可以自动收集和关联多个安全向量的数据，促进更快和更复杂攻击场景下的攻击检测，以便安全人员可以在攻击进一步扩大之前快速做出响应。XDR 还可以实现跨多个不同产品和平台的检测机制，可以大大有助于提高生产力、攻击检测和取证的进程。简而言之，XDR 扩展到终端之外，可以根据来自更多产品的数据做出决策，并且可以通过对电子邮件、网络、身份等采取行动，进而在整个堆栈中采取防御。

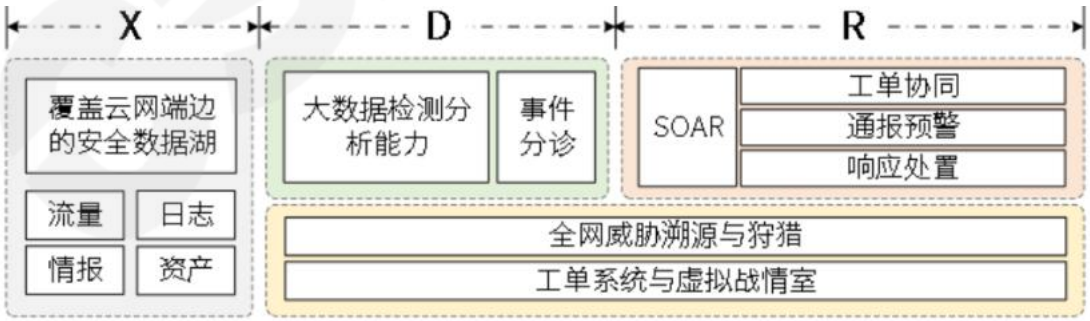


图 2

说起 SIEM 的发展，离不开态势感知产品的发展，之前看到的都是单个安全设备告警，比如防火墙告警、WAF 告警、漏扫告警等等，安全运维需要一个一

个设备的看告警。于是自然而然想到了融合所有的告警在一张屏幕上，这就是SIEM 的雏型。早期的 SIEM 功能比较简单，主要实现了告警转换，将设备上的告警一比一的转换到 SIEM，最终实现多台设备的告警汇聚到 SIEM 中，因此早期 SIEM 告警数量太多，为了进一步优化，聪明的安全运维人员发现，如果防火墙上有一个告警，漏扫上有一个对应的漏洞，而且还是同一个主机，那么就可以认为黑客在利用这个漏洞在入侵网站，这就是关联分析，自从有了关联分析，SIEM 便有了超越了任何单个设备的安全发现能力了。关联分析让 SIEM 的告警从以前的单个安全设备告警，变成了多个安全设备的组合告警，虽然提高了告警质量，但是随着而来的是告警数量再次暴涨，安全运维人员苦不堪言。

因此 Gartner 定义 SIEM 或安全信息和事件管理，作为“通过收集和分析（近实时和历史）安全事件以及各种其他事件和上下文数据来支持威胁检测、合规性和安全事件管理的技术”。SIME 安全信息事件管理是整个信息收集、聚合、分析和存储大量的日志数据，SIEM 可以从终端、网络、系统等整个企业的几乎任何来源收集可用的日志和事件数据，SIEM 可以支持同时为多个用例进行存储。其中包括治理和合规性、基于规则的模式匹配、启发式/行为攻击检测（如 UEBA），以及跨遥测源寻找 IOC 或攻击指标。

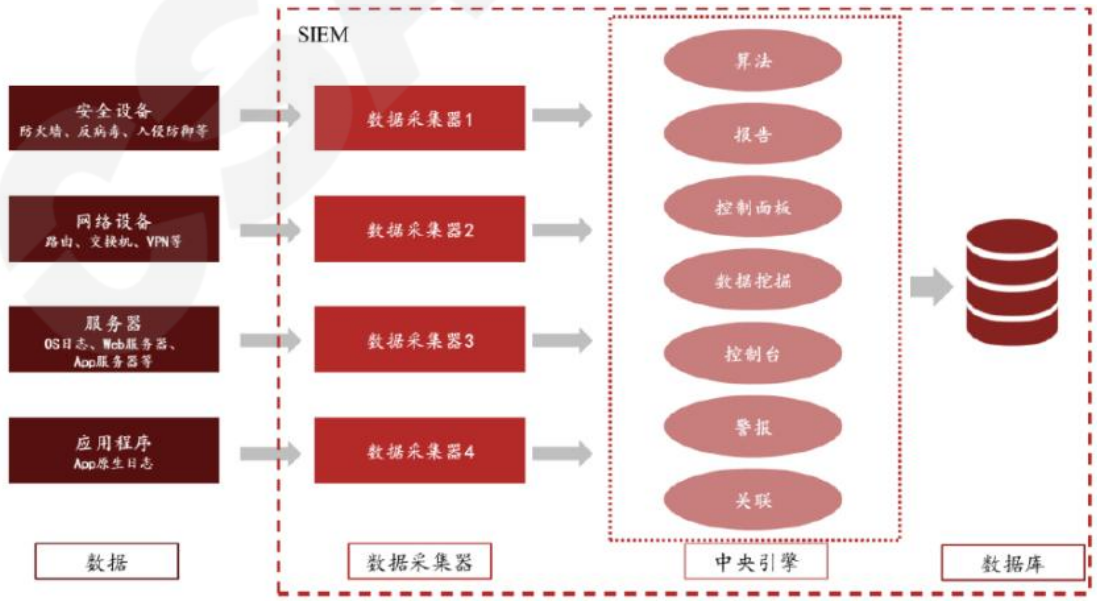


图 3

IEM 解决方案就像飞行员和空中交通管制员使用的雷达系统。如果没有该数据安全管理解决方案，企业 IT 无异于处于“盲飞”状态。虽然安全设备和系统软件擅长捕捉和记录孤立的攻击与会产生威胁的异常行为，但是当今最严重的威胁是分布式的，跨多个系统协同工作，并使用先进的逃避技术来避免进行威胁情报检测。如果没有 SIEM 安全信息事件管理，攻击就会发生并发展成为灾难性事件。SIEM 工具需要大量的微调和努力才能实现。安全团队也可能被来自 SIEM 的大量警报淹没，导致 SOC 忽略关键警报。此外，即使 SIEM 从数十个来源和传感器捕获数据，它仍然是一种发出警报的被动分析工具。

尽管 XDR 与 SIEM 在功能上存在相似性，比如都有数据采集、范化、关联，而且通常都会采用大数据分析技术，还可能都有 SOAR 剧本编排与自动化响应技术，但在目标定位和技术路线上存在差异。在目标定位上，XDR 仅关注威胁检测与响应，而 SIEM 除了关注威胁检测与响应，还要覆盖日志存储及合规审计等其它场景。在技术路线上，XDR 强调对单一厂商的安全产品集成，并且在出厂前就将这些产品打包在一起，提供了更易于部署和使用的操作过程。相比之下，SIEM 必须具备跨厂商产品集成能力。正是因为在设计上的这些简化，XDR 规避了 SIEM 当前存在的几个问题，比如架构开放性和扩展性问题、产品集成问题、部署和实施复杂性问题、知识管理问题，使得 XDR 的部署和实施复杂度相较于 SIEM 要简化不少。简言之，就是在相同条件下，以威胁检测为目标，XDR 出效果比 SIEM/SOAR 更快。

因此 XDR 是一个整理的解决方案，而 SIEM 是 XDR 的重要组成部分。现代 SIEM 的核心组成部分：威胁检测、响应。SIEM 是当今的核心 SOC 平台，最具有价值的功能包括告警检测、安全操作、集成、可视化等，其中 XDR 可以改进威胁检测和响应，使 SIEM 实现流程的现代化、集成和自动化。XDR 可以有效协助 SIEM 提升威胁检测和响应效率。尤其是在改进高级威胁检测、自动化任务以及威胁平均响应时间方面。同时，XDR 的核心价值是检测复杂攻击，可以跨端点、网络、服务器和云阻止攻击非常重要，尤其是 APT 攻击在不同场景的检测，仅通过传统的检测方式很难有效将多个低风险事件关联分析，XDR 是检测、识别、理解整个杀伤链中的复杂攻击的有效方案。

4.4 XDR 生态

4.4.1 国外生态

4.4.1.1 相关标准

美国围绕漏洞、威胁信息等领域开展了网络安全信息相关标准的研制，主要包括通用漏洞披露（CVE）、结构化威胁信息表达（STIX）和可信自动情报信息交换（TAXII）等。

通用漏洞披露（Common Vulnerabilities & Exposures，CVE），对已发现的网络安全漏洞进行统一的命名和编号，并进行规范化的描述，可以在不同的漏洞数据库和漏洞评估工具中实现漏洞数据共享。

结构化威胁信息表达（Structured Threat Information Expression，STIX）是一种用于网络威胁情报的语言和序列化格式标准，用于定义、描述威胁信息内容和关联关系。STIX 规范了威胁因素、威胁活动、威胁属性等威胁情报特征，适用于威胁协同分析、自动化威胁情报交换、自动化威胁检测和响应等。

可信自动情报信息交换（Trusted Automated eXchange of Indicator Information，TAXII）在 STIX 基础上定义了网络威胁情报共享的协议、服务和格式等。TAXII 是网络威胁情报数据的共享和传输交换标准，主要用于实现跨产品、服务和组织边界来共享网络威胁信息。

4.4.1.2 相关接口

国外相关技术组织围绕网络安全信息交换功能接口实现等开展了相关标准的研制，主要包括开放命令和控制语言（OpenC2）、开放消息总线规范（OpenDXL）等。

开放命令和控制语言（Open Command and Control，OpenC2）通过提供一套互操作的指令规范，提升网络安全产品联动能力。OpenC2 包括语言描述类规范、

不同功能场景的配置文件规范及传输方式。其中，语言描述规范定义命令、控制内容和结构；传输规范定义不同协议、环境下的命令和控制传输规范；配置文件规范定义不同产品执行命令和控制信息的功能和配置信息。

开放消息总线规范（Open Data eXchange Layer，OpenDXL），定义了通信模型，用于将网络安全产品连接到消息总线，实现不同安全产品间的消息共享和集成。OpenDXL Ontology 是建立在 OpenDXL 消息总线上的一种开源模型描述，通过消息传递机制连接各类网络安全产品，旨在发生网络安全事件时及时响应处置。

4.4.2 国内生态

4.4.2.1 相关标准

在漏洞管理、威胁信息、网络安全事件和网络安全攻击等领域，我国已经开展了数据相关标准的研制。

在漏洞管理方面，GB/T 28458-2020《信息安全技术 网络安全漏洞标识与描述规范》规定了网络安全漏洞的标识和描述信息，明确了网络安全漏洞名称、发布时间、发布者、相关编号等描述项内容。GB/T 30279-2020《信息安全技术 网络安全漏洞分类分级指南》规定了网络安全漏洞的分类方式和分级指标，给出了分级方法建议。

在网络安全威胁信息格式方面，GB/T 36643-2018《信息安全技术 网络安全威胁信息格式规范》给出了网络安全威胁信息模型和威胁信息组件，以实现各组织间网络安全威胁信息的共享和利用，提升网络安全威胁的共享效率和互操作性。

在网络安全攻击方面，GB/T 37027-2018《信息安全技术 网络攻击定义及描述规范》规定了网络攻击的定义、属性特征和描述方法，并从攻击对象、攻击方式、漏洞利用、攻击后果、严重程度等多个维度描述网络攻击。

在网络安全事件方面，GB/T 28517-2012《网络安全事件描述和交换格式》规定了网络安全事件的通用数据格式，并提供了参考实现。

4.4.2.2 相关接口

目前，我国已正式发布 29 项网络安全产品相关标准，涉及防火墙、网络安全审计产品、入侵检测系统等网络安全产品。其中，仅 8 项标准对产品的功能接口实现进行了规范，未明确产品间互联互通的相关要求，如 GB/T 37931-2019《信息安全技术 Web 应用安全检测系统安全技术要求和测试评价方法》。其他 21 项网络安全产品国家标准均未对产品接口进行规范，如 GB/T 20281-2020《信息安全技术 防火墙安全技术要求和测试评价方法》。

4.5 XDR 与 MSS

安全托管服务（Managed Security Service,MSS）是近几年网络安全行业备受关注的领域 。Gartner对MSS（Managed Security Services）服务的定义是：

- 7*24 小时远程监控安全事件及相关安全数据源；
- 管理和控制安全相关的技术和产品；
- 交付的安全运营能力主要是远程的SOC服务，并不是通过驻场或者远程的一对一的安全服务。

图 4

MSS的核心服务内容是对安全事件的监控和安全事件的响应以及合规方面的报告。除此之外还可能包括以下方面的内容：

- 安全设备和技术的管理，包括防火墙、入侵检测系统（IPDS）、终端管理（EPP）、EDR、安全应用网关（SWG）、安全邮件网关（SEG）等；
- 事件响应服务（包括远程服务和现场服务）；
- 漏洞评估和漏洞管理服务；
- 威胁情报服务；
- MDR服务。

根据 Gartner 统计数据，通过前瞻产业研究院对国内外权威机构的汇总，IDC、Gartner、中国信通院的报告分别显示 2021 年全球网络安全市场规模为 1687.7 亿美元、1577.5 亿美元、1554.0 亿美元，较 2020 年增速分别为 27.8%、17.9%、13.7%。其中，截至 2023 年 3 月 31 日，IDC 披露了 2022 年全球网络安全规模为 1955.1 亿美元，同比增速达到 15.8%;Gartner 披露了 2022 年全球网络安全规模为 1691.6 亿美元，同比增速达到 7.2%。安全托管服务（又常译作“托管安全服务”），顾名思义即将网络安全运营等技术类工作委托给第三方代为管理，以服务化的形式帮助用户发现和解决各类安全问题。国际咨询机构 IDC 将安全托管服务（MSS）定义为安全服务提供商（MSSP）通过安全运营中心（SOCs）进行全天候监控和管理的 IT 安全服务。服务范围包括部署在本地、外部数据中心和云上的安全托管服务。国际分析机构 Frost & Sullivan 将 MSS 划分为安全资产监控/管理、托管威胁检测与响应（MTDR）和其他新兴 MSS 服务三类。由此可见，托管服务的形式与内容是相对多元的。

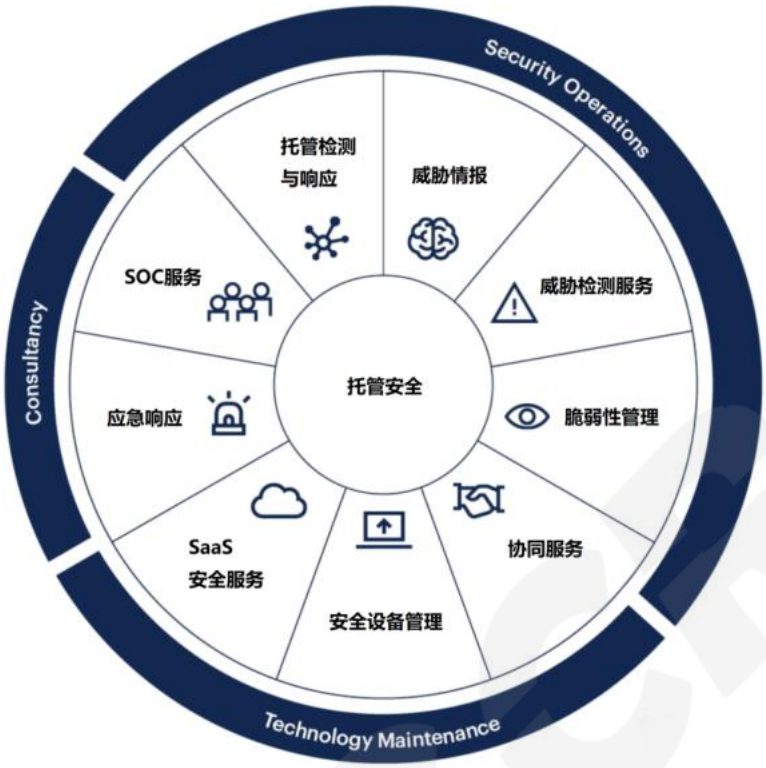


图 5

在国内，由于中国自身实际情况的特点，相对“远程服务”，国内更为青睐“驻场运维”模式。驻场托管也是 IDC 所定义的一种形式。目前，一些网络安全服务商均提供网络威胁检测、分析、响应、处置等多种能力，但主要为相应安全产品的增值性服务，以及提供威胁情报等。

相对于国外安全产品及一揽子外包服务，国内市场普遍更为倾向于本地驻场的安全运维模式，依靠本地的安全网络安全管理平台等产品和驻场运维人员，实现对本地网络设备、网络安全设备流量和日志等的采集处理、深度分析和事件处置。然而对于 MSSP(Managed Security Service Provider，安全托管服务提供商)来说，搭建一套有效且易于管理的安全技术架构来为客户提供可靠的安全服务也并非易事，其实现过程同样困难重重。XDR(扩展威胁检测和响应)技术的成熟让我们看到了希望，与 MSSP 目前采用的大多数传统安全架构相比，XDR 技术有望以更低的成本实现更高的安全级别。它可以帮助 MSSP 提升服务能力，并改善服务收益，特别是在面对中小企业客户时，效果更加明显。未来，MSSP 势必会因为 XDR 技术而改变服务策略，并从这项技术中获得运营收益。通常，XDR 为 MSSP

提供的基本功能包括：扩展威胁检测能力，以增强威胁可见性;关联安全数据，以提高准确性，并将警报整合到事件中;在企业整个网络环境中扩展、协调和自动化开展安全事件的响应。相比于购买和集成一套传统的安全技术，XDR 技术提供了更高的安全级别。由于 XDR 技术旨在改进威胁检测、调查和响应，并实现自动化，因此它理论上可以准确地预防更广泛的威胁。

除了安全能力方面的改进外，XDR 解决方案还可以为 MSSP 降低成本——有些 XDR 解决方案包括多个威胁情报来源和基础安全功能，可以让 MSSP 以较小成本替换现有技术，同时，还有一些 XDR 解决方案提供增强自动化，可以让 MSSP 大幅减少人工调查和响应时间和需求，减轻对专业安全人员的依赖，从而降低成本。因此，MSSP 从 XDR 平台获得益处在很大程度上取决于提供商的方法和其实际实施。

4.6 XDRaaS

XaaS 代表“一切皆服务”，因此示例数不胜数。现在，有很多种 IT 资源或服务都通过这种方式交付。比如云计算模式：软件即服务 (SaaS)、平台即服务 (PaaS) 和基础架构即服务 (IaaS)。除了这些类别之外，还有其他一些示例，例如灾难恢复即服务 (DRaaS)、通信即服务 (CaaS)、网络即服务 (NaaS)、数据库即服务 (DBaaS)、存储即服务 (STaaS)、桌面即服务 (DaaS) 和监控即服务 (MaaS)。

随着安全能力的逐步迭代升级，网络安全同样可以以服务的方式提供，XDRaaS(XDR As a Service)，以服务化的方式提供 XDR，是一切皆服务”(XaaS) 是与云计算和远程访问相关的一类的服务的升级。XaaS 认识到现在有大量的产品、工具和技术都通过互联网作为一种服务提供给用户。从本质上说，任何 IT 功能都可以转变为服务供企业使用。此服务采用灵活的消费模式收取费用，无需提前购买或提前许可。因此 XDR 作为与云计算和远程访问相结合比较深入的技术也可以通过订阅服务的方式进行提供。

XDRaaS 具有以下几个优势：改进支出模式，加快安全防护技术落地，将 IT 资源转移到价值更高的项目。

改进支出模式。借助 XDRaaS，企业可以通过订阅方式从提供商购买服务来降低成本。在使用 XDRaaS 和云服务之前，企业必须购买多个安全产品，在现场进行安装，然后将所有东西整合在一起以进行安全检测及安全防护。现在，借助 XDRaaS，企业只需购买自己所需，然后随需付费即可。以前的资本支出现在变成了运营支出。

第五章 实践案例分享

5.1 大型企业 XDR 实践案例分享

5.1.1 背景

随着组织信息化建设规模的扩大，安全架构日趋复杂，各种类型的安全设备、安全数据越来越多。某大型企业集团以网络安全设备互联互通技术为基础，构建 XDR 安全框架体系。网络安全态势感知平台和安全产品互联互通基于集成多个具备安全能力的产品，可以灵活调度各类安全产品的安全能力，简化安全流程，增强安全自动化以加速事件响应。图 5-1 给出了典型应用场景，具体如下：

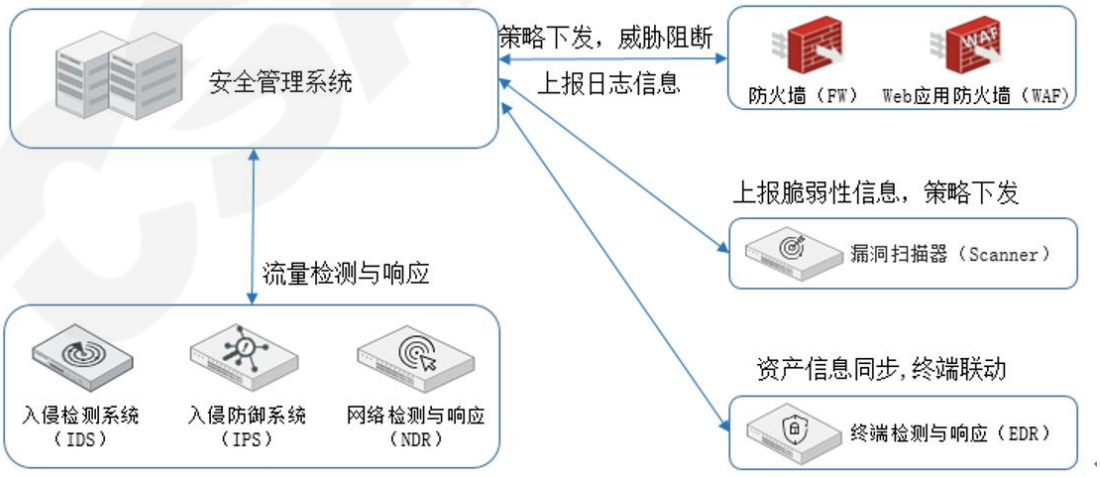


图 5-1 网络安全态势感知平台与安全产品互联互通

数据采集场景。网络安全态势感知平台与其它产品、系统和不同的前段数据

源通过数据接口进行数据采集，主要包括资产信息、脆弱性信息、日志信息、流量信息等。

1)资产信息：通过终端检测与响应系统（EDR）或 NDR 等流量数据检测系统或产品中获取网络中的资产信息，包括操作系统、版本、用户、IP 等；

2)日志信息：通过防火墙、漏洞扫描产品、终端检测与响应系统（EDR）以及 IDS、IPS、NDR 等流量数据检测系统获取网络设备、主机、应用、安全设备等记录的日志数据和告警信息；

3)威胁与脆弱性信息：通过漏洞扫描产品和其他安全监测产品获取威胁情报信息、脆弱性数据等；

4)流量信息：通过终端检测与响应系统（EDR）以及 IDS、IPS、NDR 等流量数据检测系统或产品获取异常流量数据和按规则匹配的网络流量数据。

5)联动处置场景。以网络安全态势感知平台为中心，通过联动处置接口，支持防火墙策略下发、威胁阻断等功能，支持终端检测与响应系统（EDR）和 IDS、IPS、NDR 等安全监测产品的威胁与攻击检测响应功能，支持通过接口进行防护策略的更新和下发等操作。

5.1.2 技术路线

XDR 安全框架体系是一项不断完善建设的工作，不可能一蹴而就。根据对国际和国内完技术分析，集团公司以网络信息安全基础平台战略为基础，逐步完成三个阶段目标。

1、数据标准化，基于通用协议的数据采集抽象形成一个数据字典，形成大数据资源池；

2、数据建模功能化：依据标准化的大数据资源池，根据安全功能建模，形成安全功能数据池；

3、服务能力接口化：面向应用场景提供标准的对外服务接口。

图 5-2 集团 XDR 安全技术框架

数据接口主要采用协议包括 HTTPS、SFTP、SYSLOG、Kafka 等协议采集数据，采集的主要类型包括资产数据、脆弱性数据、威胁信息、流量、威胁情报等。

控制接口主要基于 API 接口或其他方式（SSH）提供联动处置接口，支持通过接口进行防护策略的更新、扫描策略的下发等操作。

5.1.3 案例介绍

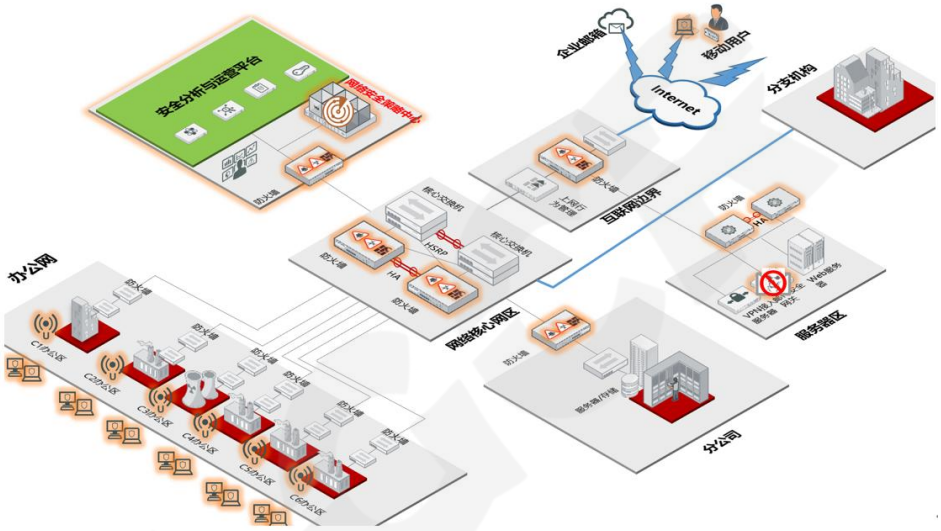
背景现状

在日常网络和安全运维工作中，由于业务需要，经常需要对相关的出口防火墙的规则进行配置以及对相关部门的防火墙下发阻断策略；主要存在以下问题：

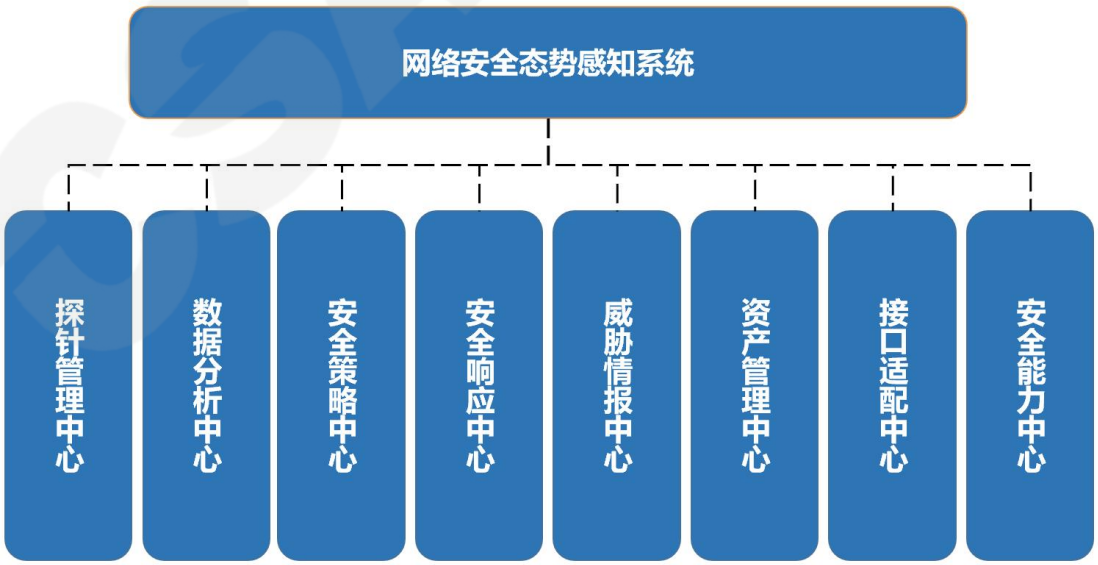
配置效率低。在大型集团企业中，不同的事业部都有自己的出口防火墙，集团信息中心需要手动定位目标防火墙并手动配置策略，同时请求流程繁复，实施周期长，影响开通业务的时效性。

客户除了部署多种品牌的防火墙，缺少防火墙的统一管理平台。针对恶意 IP 阻断，只能"一刀切"，不能基于事业部的方式进行精准阻断。

产品应用部署以网络安全态势感知平台为核心的整体方案，平台覆盖企业主园区、分园区、各大区核心和汇聚网络设备；累计共完成网络设备 267 台；公司级防火墙设备 30 台，共计 297 台；部署图如下：



集团网络安全态势感知平台组件如下：



通过平台的安全策略中心组件，实现以下能力：

1、集中配置。通过安全策略中心可以集中配置集团的多个品牌防火墙，既可以通过 API 接口的方式同步和下发配置，也可以通过 SSH 的方式同步和下发配置。

2、精准阻断。通过标签，把防火墙和事业部绑定，自动定位需要阻断恶意 IP 的目标防火墙，通过集中控制台自动下发策略。

3、运维规范化。策略中心和业务工单系统数据同步，请求开通工单直接实现防火墙权限变更，策略用途直接关联工单描述，直观显示。

客户收益

未部署 XDR 架构前，集团网络月均总工单量 420 单，其中防火墙规则设置月均 340 单，占比近 80%，防火墙规则设置日均投入时长为 2.7H；应用 XDR 方案并联动工单系统后，预计日均时间投入不超过 10Min，时间投入先后减少 94%，预计月减少 7.1 人/天的人员投入，年人员投入节约 4.1 人/月。

CSA GCR cloud security alliance GREATER CHINA REGION ®

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网：https://c-csa.cn 电话：0755-86548359
地址：上海市浦东新区东育路255弄5号3FB30（前滩国际经济组织集聚区）/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905