SANGFOR 深信服科技 | CAICT 中国信通院 | CCCoE 网络安全卓越验证示范中心

XDR技术及行业发展研究报告

www.sangfor.com.cn

CONTENTS

目录

XDR概述 01

XDR发展背景 01

XDR的概念 03

XDR与防御体系建设 05

XDR国内外发展现状 06

XDR关键技术 09

全面遥测数据采集 10

自动化威胁狩猎 11

自动化响应 12

XDR 核心价值 15

应对潜伏威胁 15

根除攻击影响 17

多维安全视野 19

攻击可视化 20

发展问题及建议 21

平衡效率与隐私，逐步接受SaaS 21

关注AI+安全，提升行业生产力 22

建立互通标准，推动生态建设 23

XDR概述

XDR OVERVIEW

XDR发展背景

网络安全监测、预警、响应、处置是网络安全防护工作的重点。近年来，国家高度重视网络安全工作，先后发布了多项网络安全战略政策。《国家网络空间安全战略》明确指出需要建立完善国家网络安全技术支撑体系，完善网络安全监测预警和网络安全重大事件应急处置机制。《网络安全法》则提出了“国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏”的要求。

加强网络安全信息统筹机制、手段、平台建设，是提升网络安全事件应急指挥能力的有效途径。当前全球网络空间威胁水平不断提升，网络攻防对抗技术快速发展，网络安全防御存在着技术落后，甚至是失效等风险。在这种趋势下，业界普遍认为，拥有全局化、体系化的安全视角，掌握复杂的安全态势，是应对各类复杂网络攻击一种有效思路。在这种的理念驱使下，采用统一平台化构建的、拥有多维聚合检测和响应处置一体化能力产品方案则成为了一种业务共识。这也为之后 XDR 理念的提出和发展，奠定了重要基础。

XDR（Extended Detection and Response）最早由网络安全公司 Palo Alto Networks 的首席技术官 NirZuk 在 2018 年提出，之后被业界广泛接受。在最新发布的《2022 Gartner 安全运营技术成熟度曲线（Hype Cycle）》报告中，XDR 登顶，被评为“安全运营体系中最炙手可热的技术之一”。各类的网络安全厂商都在考虑向XDR技术转型，包括绝大多数 EDR 厂商，主流的 SIEM、MSS、NDR 厂商等。

XDR 理念是网络安全行业在近十年的网络威胁事件应对中，通过不断反思和探索而逐渐形成的。XDR 能够得到爆发式发展，并不是因为 Palo Alto Networks 公司或者 NirZuk 个人的影响力，而是网络空间安全的威胁态势、防御技术发展水平、数字化转型需求三方面因素共同作用的结果。

01

重新定义检测：2012-2013 年，多起 APT 事件被披露，展现出对各种高等级防护目标突破的普遍可能性，使整个行业认识到既有的被动防御难以应对当前面临的挑战，大多数情况下企业要么已经被攻陷，要么在被攻陷的路上，这就需要在传统 IPS、AV 等特征检测防御的基础上，构建新的主动检测能力，以发现高级的、隐蔽的渗透攻击行为。

02

发现响应价值：2015 年美国知名百货公司 Target 数亿用户隐私被窃事件，多种检测机制均产生了警报，但事件却没有被及时处理，这件事引起了美国政府和安全企业的高度重视和深刻反思。由此认识到除了构建新的检测能力外，为及时控制、清除已经在内部建立立足点的攻击者，还需要进一步完善事件响应能力，以保障在攻击者完成最后的破坏、偷盗行为前进行有效地阻止。

03

构建统一平台：随着主动检测和事件响应相关技术和产品的发展，市场上出现了非常多种类的相关产品，如：NDR、EDR、SOAR、UEBA、SIR、NTA 等等，因为细分的产品太多，以致于在一个安全事件闭环运营过程中，可能会涉及 10 个以上的安全工具或产品，这种情况不但效率低下，也难以通过相互独立的产品看到攻击的全景。2021 年 2 月，CrowdStrike 的 CEO George Kurtz 就 SolarWinds 事件在美国参议院情报委员会作证，就强调 XDR 是跟上当今对手复杂性的关键创新："长期以来，行业参与者一直专注于狭隘的解决方案。网络上的任何盒子或单一用途的软件都无法覆盖全部范围。安全团队需要跨越整个环境的上下文和可见性，包括在云和临时环境中。XDR 旨在通过在企业内部任何地方获得可见性和可操作性，从而将混乱的安全工具阵列变得井然有序。正如本委员会所理解的那样，XDR 可能不仅仅是从信息过载中生成情报。"[1]

如果威胁对抗的过程造就了 XDR 的大趋势，那么检测、响应技术的发展则是 XDR 形成的现实基础。威胁狩猎从早期阶段高度依赖安全分析师，已经发展成为绝大部分工作都可以依赖 AI 智能完成；随着 SIR、TIP、SOAR 的逐步整合，自动化的事件分类 / 分级、自动化响应也逐步成熟起来；而 EDR 产品、MDR 服务在多个场景下的成功，也使得行业对如何完成平台的整合开发、交付和运营积累了足够的经验。这个时间点上 XDR 成了水到渠成的自然之选。

同时数字化转型形成的迫切性，进一步推进了 XDR 的加速发展。随着近年数字化转型日益深化，越来越多的企业网络中分布了大量的关键业务资产（数据、应用、服务、设备等），这些资产对企业的发展至关重要，也使得攻击者更觉得有利可图，因此定向攻击已经从之前相对狭窄的国家 APT 对抗发展到更广大的网络犯罪领域，而和数字化相关的企业都有可能成为受害者，其中最典型的就是勒索软件，这几年不但越来越多的勒索攻击具备了定向攻击的特点，同时也从单纯的以数据加密为勒索手段，转化为加密勒索、泄露数据勒索、向竞争对手或投资者暴露攻击机密等多重勒索的方式。同时对工业网络和 IoT 网络的攻击时有发生，这种攻击可能对整个社会的正常生产、生活造成巨大影响，市场迫切需要可以及时发现各种高水平攻击并实时响应、遏制的产品，因此 XDR 的解决方案受到广泛关注。

[1] https://www.intelligence.senate.gov/sites/default/files/documents/os-gkurtz-022321.pdf

XDR的概念

不同的安全厂商，往往存在对 XDR 的不同理解，即使是权威的咨询机构，对 XDR 的定义也有很大的不同：

Gartner 的定义：“一种基于 SaaS 的，由特定供应商提供的安全威胁检测和事件响应工具，可将多种安全产品集成到一个聚合的安全操作系统中”；

Forrester Research 的定义：“EDR 的演进，优化了威胁检测、调查、响应和狩猎。XDR 将与安全相关的端点检测、与来自安全和业务工具（如网络分析和可见性 NAV、电子邮件安全、身份和访问管理、云安全等）的遥测数据统一起来。它是一个基于大数据基础架构构建的云原生平台，可为安全团队提供灵活性、可扩展性和自动化”。

虽然定义有所不同，我们也可以看到它们对 XDR 的认知是有共同点的。2021 年 8 月，曾经 Gartner 的研究 VP，当前 Google Cloud 安全战略负责人 Anton Chuvakin 发起了一个调研，最终总结了几点业界对 XDR 的共识。[2]综合这些信息，可以认为 XDR 具备以下两个基本特征：

XDR 最佳效果是基于云原生的

XDR 的检测能力需要较全面地覆盖已知黑客攻击技战术，同时需要针对新出现的攻击技战术快速开发对应的检测模型 & 算法，以及相关的调查、响应、狩猎功能。因此当前较完善的 XDR 产品均是基于云原生 SaaS 化提供的，可以基于集中的专家、算力、遥测数据和情报资源，更快、更好地快速迭代产品，可以认为云原生是 XDR 快速发展的必要条件。即使一个本地化部署的 XDR 平台，也需要基于云端的持续运营来提供快速的更新。通过云原生提升安全对抗效率，一个典型的案例就是在 2021 年 Log4j2 漏洞爆发时，CrowdStrike 基于其云原生架构，在漏洞披露 24 小时内就提供了检测、处置和修复的完整能力，并且在数天内提供了专项的 Dashboard，这种速度对于单纯依赖本地化平台的产品是难以想象的。[3][4]在用户不同需求场景中，本地化 XDR 也有其存在的必要性，不能完全被 SaaS 化所取代，但想要达到 XDR 最佳效果，充分发挥其价值，基于云原生的 XDR 是最佳实践。

[2] https://medium.com/anton-on-security/anton-and-the-great-xdr-debate-part-1-8ed148c3cee4
[3] https://www.crowdstrike.com/log4j2/
[4] https://www.crowdstrike.com/blog/how-to-baseline-and-hunt-log4shell-with-the-crowdstrike-falcon-platform/

XDR 覆盖检测和响应

XDR 顾名思义包括检测和响应能力，集成全面、完善的检测技术在行业内没有争议，但在响应技术上还有不同的认识。

全面、完善的检测技术，即需要包括：

- 传统的特征检测（攻击特征、漏洞特征）；
- 启发式检测；
- 基于行为的检测（IOA）；
- 最重要的提供各种威胁狩猎能力，包括被动、主动和自动化不同的方式。

在响应技术上的争议，主要因为其存在的两个特殊点：其一响应动作有影响数字业务的可能性，越重要的业务越需要企业自身业务人员的确认；另一个则是当前的响应自动化集中在遏制上，对清除、加固还需要更多的人工介入。但即便如此，XDR 依然需要在整个事件响应的过程中，提供更多自动化的机制来保障响应的及时性，同时对攻击的遏制、清除、加固提供必要的专业指引。通过自动化和专业知识的赋能，XDR 保障安全运营过程中提供最快速的 MTTR（Mean Time To Response，平均响应时间）。

XDR 与其他类似安全解决方案的差异:

与 SOC（Security Operations Center，安全运营中心）的差异

传统 SOC 方案以信息资产为核心，通过对各种安全设备、网络设备、应用和系统的日志、告警进行监控和分析，能够提高安全运营人员响应、处置、溯源的效率。现在较为先进的 SOC 选择围绕数据和情报，结合 AI 或自动化工具来对抗威胁与攻击。多年来看 SOC 在国内的落地遭遇重重挑战，原因除了价格高昂、组织缺乏专业运营人员之外，SOC 方案集成了从资产到数据，从安全到组织能力的众多功能，也使系统越来越繁重，同样在一定程度上限制了它的发展。XDR 具备聚合分析流量和端点一手数据的能力，以及微剧本半自动化响应事件，结合 MDR 的及时支撑，可以作为 SOC 方案的底座，是当前 SOC 现代化改造的重要组成部分。

与 SIEM（Security Information and Event Management，安全信息和事件管理）的差异

XDR 可以认为是 SIEM 在检测和响应领域的一个更深入、完善的实现。一直以来全面的安全可见性需要依赖 SIEM 产品，是多数人的自然想法，因为一直以来 SIEM 就是所有安全数据汇集、分析、统计、呈现的中心。但 SIEM 在高级威胁检测上一直在努力，而 EDR 产品的异军突起，使行业认清了一个之前的误区——错误地认为安全数据收集和分析可以分开进行，实际情况是只有想清楚怎么分析使用才能有效收集数据，如果对分析场景没有深刻的认知，那数据也难以充分发挥价值。因此 XDR 就是先集中精力在检测和响应场景，这已经是一个非常广阔的领域了，只有随着 XDR 的日渐成熟，安全运营的其它能力才可能囊括进来。在 SOAR 上也是同样的道理，做一个编排和自动化引擎也许不难，难的是需要提供资产、漏洞、检测、响应、情报等各个领域专用知识和最佳实践，以形成剧本。因此 XDR 虽然使用了 SOAR 相关的技术，但它聚焦在检测、响应领域。

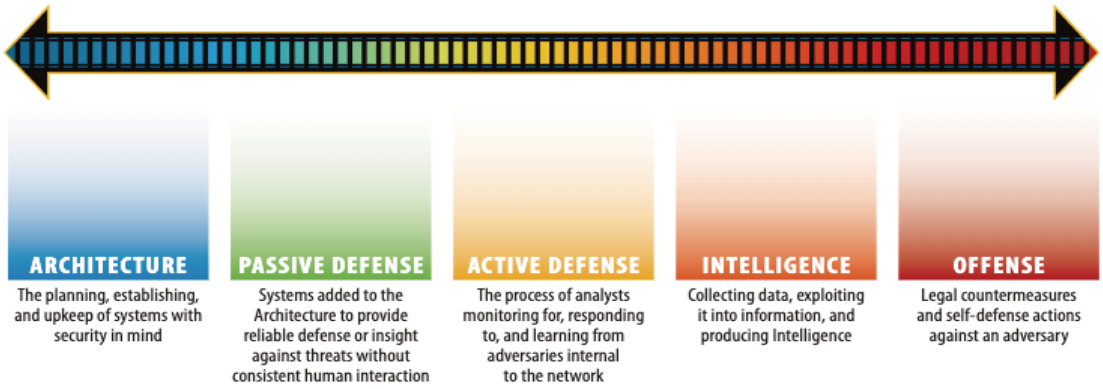
与态势感知的差异

从 NDR 演进而来的态势感知，更关注通过大数据、机器学习算法等技术，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 NDR 设备，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，尽可能地保障用户的资产和信息系统安全。

XDR与防御体系建设

滑动标尺模型是由 Robert M. Lee 于 2015 年，在《The Sliding Scale of Cyber Security》中提出[5]。Robert 曾经是美国空军的网络战专家、威胁情报和事件响应领域专家，同时是工业安全领域公认的先驱，Dragos（ICT/OT 安全领域独角兽企业）的首席执行官兼联合创始人。通过此模型我们能更清晰地理解 XDR 在整个安全体系的定位。

滑动标尺模型将所有的安全措施分为五大类别，它们分别是：



图片来源：《The Sliding Scale of Cyber Security》

01

架构安全（ARCHITECTURE）

在系统规划、建设和维护过程中需要考虑的安全防护措施，如网络分段、访问授权、系统补丁、加密措施等。当前这个类别主要通过零信任的理念来指导建设。

02

被动防御（PASSIVE DEFENSE）

指在无人员介入情况下，附加在系统架构之上可以提供持续威胁防御或者威胁洞察的系统，包括反病毒、IPS 等。一般而言通过好的架构安全建设和被动防御可以抵御绝大多数随机性攻击。

03

主动防御（ACTIVE DEFENSE）

为了有效防御意志坚定、资源充裕的定向攻击者，就需要建构积极防御的安全能力，即基于攻击者的技战术知识掌握，进行主动的威胁狩猎、监控、事件响应和经验总结的过程。

04

情报生产（INTELLIGENCE）

基于之前阶段的数据收集、分析的信息，进一步完善加工，生成情报并分享使用的过程。具备了情报生产能力，可以将积极防御阶段的能力转化为被动防御的规则，在更大范围内、使用更小成本去对抗攻击者；同时提升对攻击者能力、意图、技战术的理解，以进一步优化积极防御能力。

05

进攻反制（OFFENSE）

针对攻击者的法律措施或者其它自卫反击行动。进攻反制的成本高昂，同时对于民间机构选择这类行为的合法性具有高度争议，这里就不再展开。

[5] https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240

基于这种模型划分，可以认为 XDR 是主动防御阶段安全能力的集中整合，是针对定向攻击者最关键的防御利器。但 XDR 要发挥最大价值，和其它安全能力的建设也有着密不可分的关系：

架构安全和被动防御是 XDR 实施的基础

只有具备较好的架构安全和被动防御能力，可以较好地实施对流行、随机性攻击的实时防御时，才能够有足够的资源和时间关注在真正重要的定向攻击或者高水平攻击者上，没有这个基础就会被淹没在大量低风险事件中，成了高射炮打蚊子。

XDR 的分析结果可以进一步完善架构安全和被动防御

XDR 的检测 & 响应分析结果，可以明确攻击者怎样进来，怎样进行横向移动，这些信息揭示了架构安全和被动防御中的不足，可以推动相关能力的进一步完善。

XDR 是情报生产的基础

基于 XDR 发现、处理的攻击事件，通过分析形成战术情报（攻击者使用的互联网基础设施、攻击工具等）、运营情报和战略情报，这些情报可以用来大规模地排查或者实施全网实时防御，这种方式最大化降低整体防御成本，使安全行业真正在对抗中获取主动权。没有 XDR 的检测、分析，并对攻击过程的完整回溯，高水平的情报生产就只是无源之水，无根之木。

XDR国内外发展现状

鉴于 XDR 技术的许多先进优势，国外的许多厂商选择通过相互合作的方式来探索 XDR 前进方向，目前国外网络安全界已经成立了三大 XDR“联盟”，旨在增大研发力度、统一数据传输格式、完善 XDR 技术堆栈。据 Grand View Research 研究显示，到 2028 年，XDR 市场规模预计将达到 20.6 亿美元，2021-2028 年的复合年增长率将达到 19.9%。

研究机构 Gartner 发布的报告显示，2021 年全球信息安全和风险管理技术与服务支出预计将达到 1504 亿美元。为了面对日益增长的威胁攻击，企业将规范化威胁检测和响应活动，增加投入成本。但与此同时，由于网络安全人才匮乏、安全运营经验缺失，复杂大型的集成架构难以落地形成效果，因此中型企业和小型企业对 XDR 有着强烈的需求。

XDR 作为融合了“EDR+NDR+SOAR+ 威胁情报 + 安全中台 +X”的一站式安全检测与响应平台，能够面对现今复杂的 IT 环境，不论是传统老架构，还是公有云、私有云、单云、多云、混合云架构，XDR 都能够更快、更准确地发现网络攻击活动，为企业提供快速应对各类繁琐枯燥的安全任务的能力，并且多维安全视野聚合，也能有效应对当前安全设备海量告警过载的难题。

当前，各类产业主体都在积极围绕 XDR 展开探索。在有科技产业界风向标之称的 Hype Cycle（技术成熟度曲线）中，XDR 技术在端点安全和安全运维被多次提及。此外，研究机构调查了 339 位企业安全负责人面对 XDR 的态度，58% 的人认为 XDR 可以通过增强、改进、聚合当前的安全分析功能来实现 SOC 的现代化，55% 的人认为 XDR 可以通过与 SOAR 集成来实现安全流程自动化。

明白 XDR 在整个安全体系建设中的重要地位，就不难理解近年为什么有大批的安全厂商都投入到 XDR 相关建设和产品开发中了。特别是在国际上，不同类型的安全厂商都进入这个赛道，其中比较知名的厂商就有数十个之多，它们包括：

EDR&NDR 厂商：CrowdStrike、Bitdefender、Cybereason、Darktrace、Fidelis Cybersecurity、Kaspersky、SentinelOne、Sophos、VMware、F-Secure、McAfee 等；

SIEM 厂商：Elastic、Exabeam、FireEye、LogRhythm、Securonix、Splunk、RSA 等；

MSP 厂商：Secureworks；

综合类厂商：Microsoft、Palo Alto Networks、Rapid7 、Cisco、Trend Micro 等

同时专门针对 XDR 的托管服务厂商（MDR）也大量涌现，它们包括提供 XDR 产品的厂商，也包括专门的托管服务提供商，如：Expel、CrowdStrike、Binary Defense、Secureworks、Red Canary、Rapid7、SentinelOne、Cybereason、deepwatch、Trustwave、Kudelski Security、NCC Group、Arctic Wolf、eSentire。

图片来源：《Forrester Wave: Managed Detection And Response, Q1 2021》

国外 XDR 发展较国内相比起步较早，有一些安全厂商的 XDR 产品已经具有一定规模，其中的一些概念和技术也趋于成熟：

Palo Alto——Cortex XDR

Palo Alto 是最初提出 XDR 概念的厂商，其 Cortex XDR 是一个基于 AI 的开放式集成安全平台，通过集成网络、终端和云端的多种来源数据，对外提供威胁发现和狩猎的功能，以及自动化调查和威胁响应，并用机器学习和分析改进安全运营的每个阶段。Cortex XDR 分析存储于 Cortex 数据湖中的网络、端点和云数据，提供高效运营方法以存储行为分析所需的大量数据，同时利用现有安全投资作为传感器和执行点。

Cisco——SecureX

SecureX 是一款云原生内置平台，它能将 Cisco Secure 产品组合与企业基础设施紧密相连。它以集成、开放的设计简化了安全防护工作，在单一界面中提供全面的可视性，并通过自动化工作流最大程度提高运维效率。从根本上减少威胁驻留时间和人工操作，帮助企业抵御攻击，保持合规。

Fortinet——FortiXDR

FortiXDR 是一种云原生、跨产品检测和响应解决方案，可在其安全结构中添加全自动事件识别、调查和风险补救措施。

McAfee——MVisionXDR

McAfee MVisionXDR 是一个基于 SaaS 的平台，通过减少响应周期来显著提高 SOC 效率，节省多达 95%的威胁评估成本。它还可以实现安全工具之间的检测相关性，以得出高可信度的警报和决策。它提供的 API 允许组织轻易将第三方设备与其对接，从而简化网络威胁管理。

目前，国内 XDR 也在蓬勃发展，许多安全厂商发布了自己的 XDR 产品，从产品演进路线上看，大致分为三种：从 NDR 技术路线演进，代表厂商有深信服、奇安信、安恒、启明星辰等；从 EDR 技术路线演进，代表厂商有亚信安全、青藤云等；从 SIEM 技术路线演进，代表厂商有日志易等。从产品形态和交付模式上看，又分为本地化、SaaS 化两种，也有一些厂商如深信服，可以同时具备两种交付方式。

XDR关键技术

XDR KEY TECHNOLOGY

作为一个平台型产品，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 需要覆盖数据收集、检测、分析、遏制、清除、加固等多个阶段，甚至还可能包括情报的生产和共享。

但 XDR 的定位出发，可以认为有 3 种技术的重要性最为突出：

全面的遥测数据采集

XDR 将网端云采集的遥测数据进行聚合与分析，可以深度了解所保护或监控的对象中是否存在安全风险与攻击，甚至可以回溯之前以及发生过的安全事件，让网络安全具备高度可见性。全面遥测数据采集是安全大数据分析上的巨大进步，通过节省带宽与数据成本，为规模化和 SaaS 化部署奠定了基础。

AI 驱动的威胁狩猎

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。

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，才可能有效地提升 MTTR。

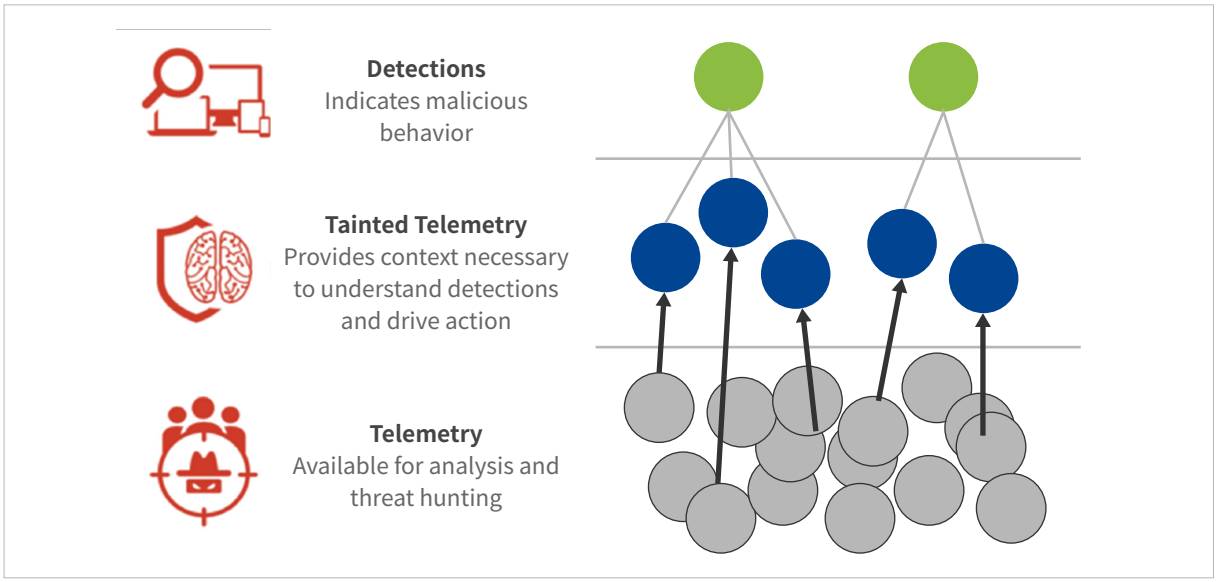
下面就对这 3 个关键技术进行进一步的阐述。

全面遥测数据采集

10 年前行业就形成一个共同认识——数据驱动安全。具体的方法、技术，行业也一直在探索。起始阶段，大多数人会直觉地相信数据越多越好，在具体工程实践中甚至希望做全量的 PCAP 采集，这种方法很快被发现成本很高同时也难以支持检测 / 分析工作；重点很快转换到元数据采集上，即主要记录应用协议的头部信息，以及极少的内容层关键信息（如：HTTP 的 Post 部分，Telnet 中的具体命令等），这种方式极大压缩了数据存储的成本，同时结构化的数据也更好地支持检测 / 分析工作，曾经被认为是一种较好的选择。

但元数据的方式还是存在问题，首先是数据量虽然比较小（大约 PCAP 方式的 5% 左右），但是这些数据绝大部分后续都不会使用，因为它们是明确的白流量；同时依托这种数据要直接发现攻击行为，需要分析人员有非常高的知识积累和实践经验，毕竟这些数据本身和攻击、异常行为等缺少显式的联系。又经过数年的摸索，行业内终于找到了一条更合理的技术路线，即以遥测数据为中心的采集机制。

在网络安全行业遥测数据的概念有其特殊性，一般而言遥测是泛指各类传感器收集的数据，但网络安全行业经过多年的发展形成了独特的意义。基于 2021 年 MITRE 的 ATT&CK 评估测试中对遥测的定义，它是：“经过最小化处理的数据，是为了证明特定攻击行为而产生的，可以明确表明特定行为发生了并且和特定的攻击机制相关（确实发生或者可能发生）”。也就是说，遥测数据更倾向于需要优先收集和攻击行为有一定关联性的第一手数据，这种遥测数据和元数据最大的不同是它是和特定的攻击技战术行为相关，CrowdStrike 将其称之为“污点遥测”：[6]



图片来源：《MITRE ATT&CK: Why Detections and Tainted Telemetry are Required for an Effective EDR Solution》

这种遥测采集有如下特点：

以威胁为中心的采集

这种遥测数据采集，在可用数据技术上，进一步做了过滤和上下文富化。通过以威胁为中心的方式，选择出和后续检测、分析有关联的那部分数据，这些数据或者有助于完成检测报警，或者有助于报警后对攻击的理解和分析。在早期的大数据安全分析中，这种过滤工作依赖有较高技能水平的分析师手动完成筛选，而这种遥测数据消除了大量的分析工作，并提升运维工作效率，同时也为基于 AI 的威胁狩猎进一步奠定了基础。

[6] https://www.crowdstrike.com/blog/mitre-attck-why-detections-and-tainted-telemetry-are-required-for-an-effective-edr-solution/

动态 & 按需采集

遥测数据既然是为检测和分析专门准备的，就存在一种情况——之前没有覆盖或者出现的一种攻击技战术，需要进行检测模型开发以及事件分析。这其中必然隐含了之前没有预想到的遥测数据采集要求，考虑到这种情况，遥测数据采集往往具备动态机制，可以通过规则升级等方式，动态调整遥测数据的采集，以适应不断演进的攻防对抗。

同时在数据采集上还有按需采集的特点，在分析过程中，有可能需要特定的取证数据（特定 PCAP、当前的进程列表、注册表启动项等），这种数据每个时间点都有不同，同时数据量也会比较大，因此采用按需采集的方式，只有需要进行相应的分析工作时，才会从终端或者网络设备中临时抓取或者找到预先准备好的数据，传送到 XDR 的分析中心。

通过动态采集和按需采集的方式，可以保证 XDR 的分析中心和传感器之间传输的数据量最小，这样既可以支撑更大规模的部署，同时也有效地节省了带宽和存储成本，对于 SaaS 的方式尤其具备重要意义。

总体看，遥测作为新型的网络监控测量技术在网络安全领域中应用，对遥测点主动收集与攻击行为相关性的数据，具备更强的时效性及更多的状态信息。将各遥测点采集的遥测数据进行聚合与分析，可以深度了解所保护或监控的对象中是否存在安全风险与攻击（含隐蔽的），甚至可以回溯之前已经发生过的相关安全事件，让网络安全具备高度可见性。遥测数据采集是安全大数据分析上的巨大进步，降低了对安全分析师技能的要求，减少了重复性的劳动，同时通过节省带宽、数据成本，为规模化和 SaaS 化部署奠定了基础。

自动化威胁狩猎

威胁狩猎被认为是发现隐藏攻击最有效的方法，它以失陷为假设前提，依赖威胁相关的知识，在数据中主动寻找相关的证据。威胁狩猎有不同的形式，可以分为 3 种[7]：

	非结构化狩猎	结构化狩猎	AI 驱动自动化狩猎
方法 / 思路	以数据驱动，基于明确特征的匹配来发现网络中存在的威胁	以特定的技战术行为特征为中心，检测针对关键资产的攻击	基于 AI 模型方式，对攻击者可能使用的技战术行为进行持续、自动化检测
检测能力	能够识别已知恶意软件、工具和网络 & 主机的攻击特征	能够识别特定高级攻击者的战术、技术工具和攻击过程	能够识别各类攻击者的战术、技术工具和攻击过程，覆盖广度大
专家依赖	低	高	低
触发机制	新的 IOC、IOA 情报 Feed	特定攻击事件或者技战术行为的情报分析报告	常态化检测
适用场景	根据相关行业 & 企业提供的威胁情报，或者事件响应获取的 IOC&IOA，进行大范围的排查	依赖分析师手动工作，因此适合针对特定原因触发的，对特定技战术的检测场景资产和攻击行为	持续检测内部可能出现的失陷资产和攻击行为

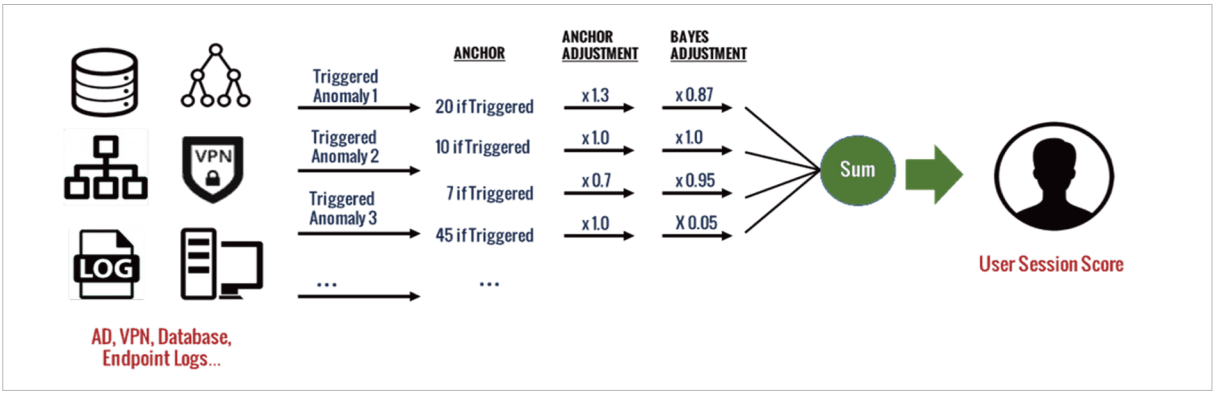
这 3 种狩猎方式，各有适合的场景，比如对于内网检测而言，AI 驱动的自动化狩猎无疑是最重要的：

- 对分析专家没有强依赖，可以进行持续化检测；
- 以自动化方式大范围地覆盖攻击者使用的技战术行为，切实保障检测的效果。

[7] https://www.crowdstrike.com/cybersecurity-101/threat-hunting/

可以认为只有实现了基于 AI 驱动的自动化狩猎，高级威胁检测才完善起来，但也要理解并不能单纯依赖 AI 方式狩猎——对于新出现的攻击技战术，需要一定的时间去开发 AI 模型，在这个时间段内，其他不同的狩猎方式互补的必要性就显现出来了。

自动化狩猎不是单纯依赖机器的力量，而是把专家经验和人工智能的优点做了完美的融合。和攻击技战术相关的所有异常点采集（遥测数据的关键部分）、异常点和具体技战术的对应关系，以及触发异常的可信度分数，都是安全专家根据实战经验和安全研究的成果分配的。但在特定环境下，一些异常点往往属于正常行为，因此大规模触发，会显著影响精确度。为了解决这个问题，AI 狩猎的方式会基于环境因素动态调整可信度分数，以减少频繁出现的误报；进一步再基于特定异常点的组合分析，来确定某些技战术对应攻击行为发生的可能性，把其中可能性最高的优先提供给安全分析人员或者激发自动化响应机制。这种 AI+ 安全专家共同构建的自动化狩猎机制，已经使用在 EDR、NDR 或 XDR 产品中。下面就是 Exabeam 提供的一个示意图:[8]



图片来源：《A User and Entity Behavior Analytics Scoring System Explained》

总而言之，自动化狩猎同时也是专家驱动的，基于专家知识使异常检测和攻击技战术有了紧密的联系，提供了单纯 AI 难以实现的告警解释性难题，同时使用 AI 驱动提供了专家难以实现的技战术覆盖度、持续性和环境适应性难题。

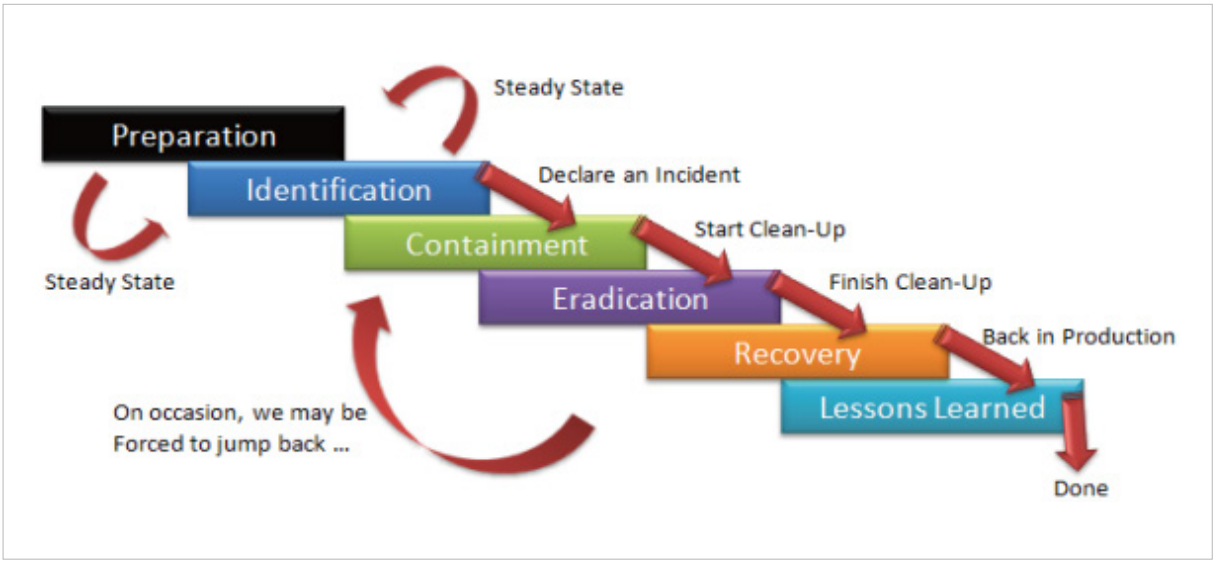
自动化响应

从很多安全厂商的报告中可以发现一个事实：攻击者能力正在变得越来越强。其中很典型的一个表现特征，就是它们在受害者环境中横向移动的速度越来越快，时间越来越短。根据 CrowdStrike 在《2021 Threat Hunting Report》中提到其 MDR 团队的发现，在 36% 的入侵中，攻击者可以在 30 分钟内横向移动到其它的主机上[9]。这是一个影响重大的变化，因为在很长一段时间，业界更多遵循的是“1-10-60”原则，即在检测和响应机制中，时效指标是 1 分钟检测到失陷，10 分钟调查了解，然后 60 分钟控制和缓解。“1-10-60”原则建立的基础是绝大多数的横向移动时间接近 2 小时，因此 60 分钟内控制是可以防止其在内网的进一步渗透的。但现在随着攻击者能力逐渐提高，相当一部分的攻击事件在 30 分钟内就能完成横向移动，说明传统事件响应机制已经难以适应快速发展的攻防对抗技术。对此业界给出的答案就是——自动化响应。

自动化响应有些时候会被和 SOAR 混为一谈，但两者并不完全一致。SOAR 的自动化脚本和编排引擎的机制可以帮助完成部分的自动化响应工作，包括事件的上下文富化、自动分类分级、自动化遏制等，但这并不是自动化响应的全部。同样的，对于 SOAR 而言自动化响应相关的用例是最重要的部分，但 SOAR 需要完成的工作还包括漏洞管理 & 协调、情报 IOC&IOA 收集管理等等存在可重复同时流程相对固化的工作，SOAR 也不仅仅是自动化响应。

根据 SANS 的事件响应框架，整个响应流程包括准备、识别、遏制、根除、恢复和总结 6 个阶段。基于 30 分钟内控制横向移动的攻防对抗实际要求，最需要优先实现自动化的是识别和遏制。而从现实的技术发展看，各 XDR 厂商实现自动化程度最高的也是在识别和遏制阶段相关机制流程上，而根除和恢复不可避免地需要更深度的人员介入。

[8] https://www.exabeam.com/ueba/user-entity-behavior-analytics-scoring-system-explained/
[9] 《2021 Threat Hunting Report Insights From the Falcon OverWatch Team》



图片来源：《SANS SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling》

在事件响应过程中的识别阶段，最重要的是尽快确定告警的真实性、基于初步识别的攻击意图、攻击阶段和事件类型判定其严重性。要完成以上工作最重要的是对报警进行上下文富化，这里面需要依赖：

丰富的遥测

跨端点、工作负载和身份捕获数万亿个安全事件，并利用威胁情报、上下文和相关标记进行丰富；

深度分析

揭示数据元素之间的上下文关系，通过应用图形分析和机器学习算法实时识别和响应新的和不寻常的威胁；

强大的搜索

强大的查询和搜索引擎为响应者提供当前和历史取证详细信息以进行威胁调查；

数据可用性

通过强大的可视化仪表板按需访问丰富的数据，帮助调查人员了解对任何受影响主机的攻击的完整背景，无论位于何处；

威胁情报

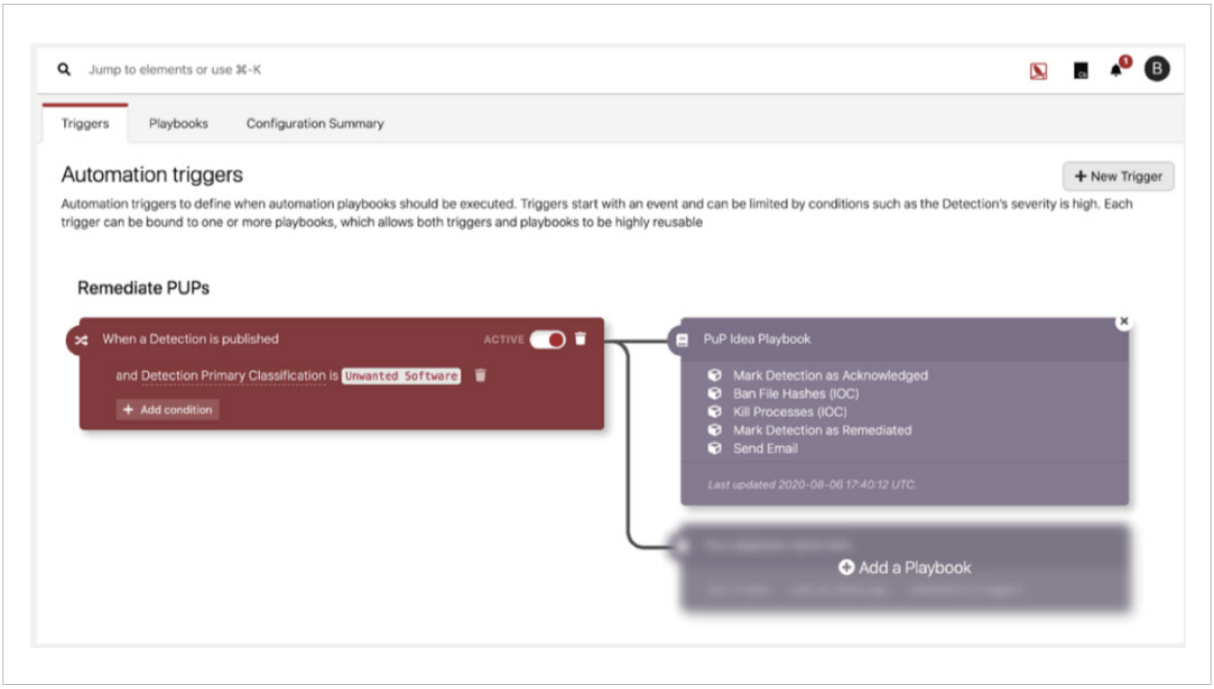
对于一个基于 AI 发现的恶意软件，如果是社区已知恶意软件，我们可以通过情报信息来了解它是否属于特定的恶意软件家族、恶意软件的攻击影响、传播方式，以及恶意软件在主机上最主要的恶意行为特征等。

基于这些信息，无论是人工还是自动化的方式，都可以迅速确定是否需要将报警升级为事件，需要使用哪种类型事件的响应剧本来进行后续的工作。

对于遏制威胁产生的影响，可供选择的行动策略很多，包括阻止、干扰、降级、欺骗和销毁。但在绝大多数企业环境中，优先考虑的还是阻止，其它措施往往在一些特殊对抗情况下才会使用。具体的阻止动作包括很多选择，不同的事件类型需要采取的动作不完全相同，同时一个安全事件的遏制动作通常可能不止一个：

- 阻断外部的 C&C 通信；
- 阻断失陷主机的网络连接；
- 中止恶意进程；
- 删除恶意文件；
- 删除失陷账号或修改其密码。

在自动化响应中，可以基于事件类型调取对应的剧本，完成相应的操作。这种情况下提高了事件响应的效率，也避免了当时的响应人员因为缺乏对应的专业知识，没有选择正确的行动策略，最终没能避免攻击范围的进一步扩大。



来源：redcanary.com

自动化遏制执行的某些特定动作，部分企业往往会担心存在影响业务的风险，因此在相关自动化流程中也可能调用相应的通信工具，将需要采取的动作发送给预设的人员，在相关人员远程确认后再自动化进行后续的操作。

自动化遏制在当前也逐步和 AI 结合，通过 AI 模型对发现失陷主机后可能的攻击范围做智能分析，来更好地确定遏制动作涉及的范围。在这个方向上 DarkTrace 是一个比较早开始尝试的厂商，并且相应的技术已经应用到其产品中。[10]

自动化响应当前在事件响应的分析、遏制阶段取得了实际的进步和效果。采用相关的自动化技术可以大幅度降低事件响应需要的时间和专家资源，保障在一个更短的时间内阻止攻击者的横向移动和其它进一步的攻击动作，防止严重风险的发生。

[10] https://www.darktrace.com/en/autonomous-response/

XDR核心价值

XDR CORE VALUE

XDR 有诸多的安全价值，经常被提起的诸如：

- 优化海量的告警噪音信息；
- 提供开箱即用的易用性；
- 让检测和响应更及时；
- 有统一的安全数据可供组织分析和查询；
- 提供安全运营的自动化；
- ……

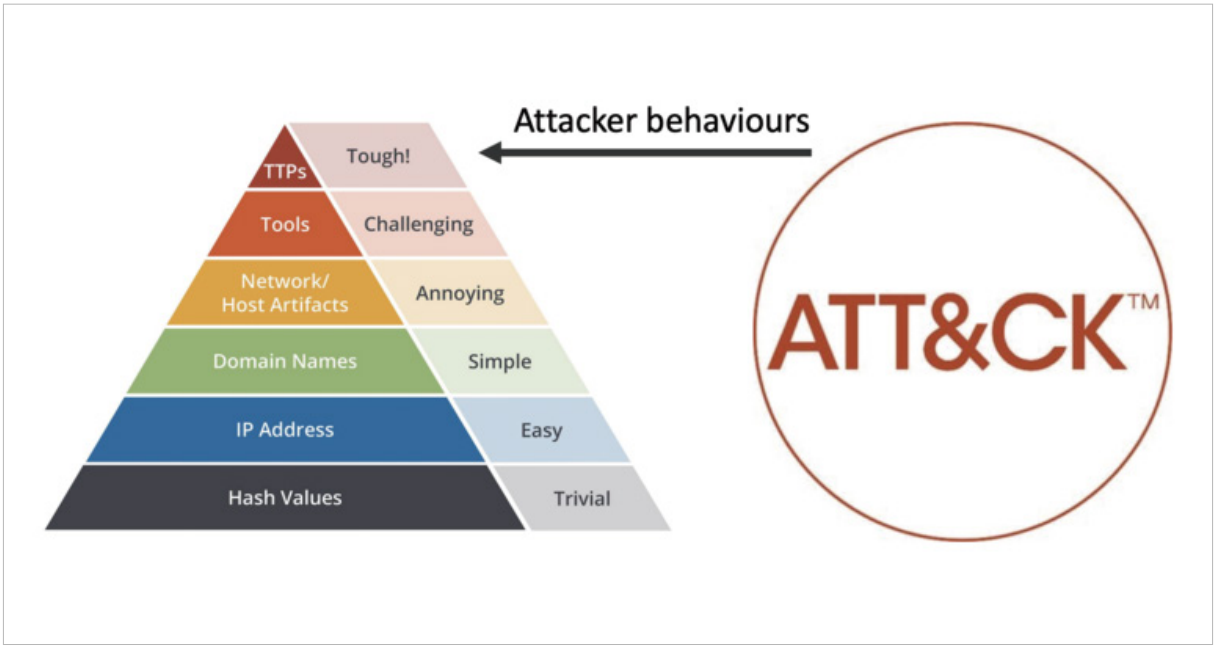
这些无疑是 XDR 可以提供的，但也许并不是只有 XDR 可以提供，如果结合独特性考虑，以下四点也许可以成为 XDR 的核心价值：

- 应对潜伏威胁；
- 根除攻击影响；
- 多维安全视野；
- 攻击可视化。

应对潜伏威胁

当前有组织的网络犯罪和网络间谍成为网络攻击的主流[11]，攻击者更精密的专业分工、更充裕的资源投入，使得有针对性的攻击越来越难以发现，这种隐蔽的威胁成为数字业务和基础设施的最大风险来源。如何有效对抗这种攻击对手，业界已形成共识：通过检测攻击者的技战术（TTPs）来规避其易于变化的部分，而专门针对攻击者最大的痛点。基于研究 TTPs 的需要，后续出现了 MITRE ATT&CK[12]，它基于社区方式，实现了一个基于现实世界实际发生的攻击者战术和技术知识库。ATT&CK 成为开发特定威胁模型和方法的基础。这个方法于 2013 年由 David J.Bianco 在《The Pyramid of Pain》[13]一文中提出，并迅速被业内认同。

[11]《Data Breach Investigations Report 2022》
[12]https://attack.mitre.org/wiki/Main_Page
[13]http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html



来源：http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

通过下面的 ATT&CK 矩阵我们可以看到攻击者如果要造成数据外泄或者加密勒索等实际业务损失，必须通过矩阵前方的 12 个纵向队列，如果我们可以在某个关键纵向队列挡住攻击者，他们就无法达到目的，而如果我们同时在多个纵向队列形成检测和响应机制，那么攻击者就面对着一个层层布防的坚固阵地，即使偶尔逃避过某一个纵列，也会被后续的纵列所阻挡，陷入无能为力的境地。

来源：https://attack.mitre.org/

ATT&CK 的提出具有两方面的重大意义，首先，ATT&CK 框架提供了描述入侵者行为的统一语言，同时也是一门网络安全行业的“世界语言”，让攻防交流不再有障碍。在 ATT&CK 框架提出之前，攻防双方，各个厂商组织之间对于入侵行为的描述是各不相同，导致攻防双方交流以及入侵技战法的普及存在较大困难。

其次，ATT&CK 框架是入侵者的“全景图谱”，改变了长期以来“防”落后于“攻”的境地，从“未知攻焉知防”步入到“已知攻而专注于对抗”，防御者可以专注于思考如何破解招数，长期落后的防守一方终于看到了攻防对抗对等的曙光。

根据 MITRE 官方的推荐，ATT&CK 适用的场景很多，包括对手模拟、红队建设、行为分析开发、威胁情报、防御差距评估、安全运营成熟度评估。不难发现这其中的很多场景都与 XDR 的建设体系密不可分，因此尽可能多覆盖 ATT&CK 中的技战术，是整个 XDR 探索与建设过程的重要目标。理论上对矩阵更全面的覆盖，无疑可以达到最优的检测效果，甚至大多数威胁，无论是从低级、破坏性低的低成本自动化攻击，还是到高级隐蔽、破坏性大的 APT 攻击，都将在 XDR 下无处遁形。

根除攻击影响

在事件响应过程中，往往容易出现的错误就是“脚疼医脚、头痛医头”，仅针对报警相关的某个资产进行处置，这样就容易出现两个问题：

未能彻底清除攻击影响

在发现失陷的情况下，内网被控制的主机往往已经不止某一台，而是数台、数十台之多，这种情况下如果没有对攻击影响范围做分析，往往会使某些攻击者持续存在于企业网络中，甚至造成巨大的影响。

攻击者使用相同的攻击面，重复攻击

攻击者可以进入到企业内部，必然是因为存在确定可以被穿透的攻击面，如果只是对失陷主机进行处理，而不去寻找攻击者如何进入的原因，那么后续的攻击和失陷情况必然源源不断地出现。

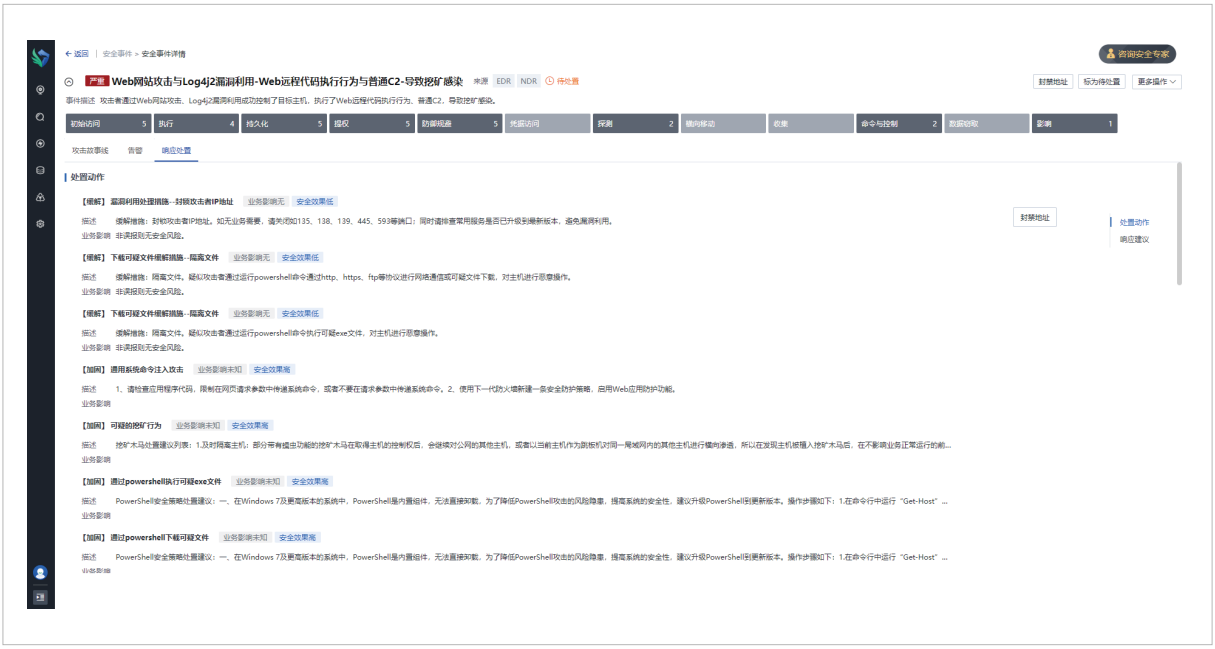
在 XDR 中，针对这个问题，提供了专门的分析机制——根因分析。根因分析不但要确认攻击的影响范围、攻击者的整个攻击链条，甚至还需要对攻击意图做进一步的研判分析，以此来进一步确定事件的响应级别。根因分析在实现上包括了产品功能，以及对应的 MDR 服务。

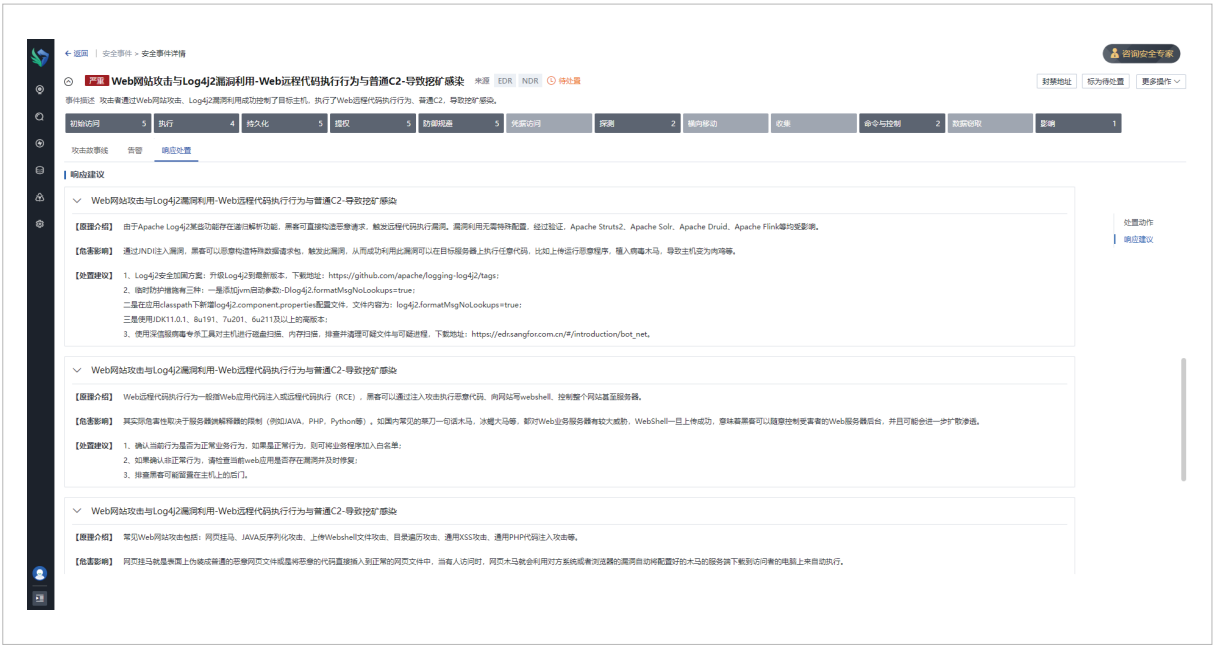
根因分析的产品功能，主要体现在四个方面：威胁关联分析、进程链还原、历史威胁回溯、潜在入口分析。旨在为分析人员提供对安全事件的全局把控，从而彻底清除事件影响、复盘企业信息系统弱点，构建更完善的防御体系。当前在根因分析中也在逐渐引入 AI 的方式，在现实中，分析人员的绝大部分工作时间，都是用来收集相关数据的，根因分析的可视化界面因为完成了这部分繁杂、耗时的工作，是对分析师效率的一个巨大提升，同时有序组织、可视化呈现的数据也降低了对分析师的专业要求，使更多人可以快速上手，这也是对分析工作的一大促进。

来源：深信服可扩展检测响应平台 XDR 攻击进程链可视化界面

虽然 XDR 产品提供的根因分析功能降低了对分析师的要求，也节省了大量重复的工作时间，但对于部分企业来说，依然缺少相对应的分析人员，或者相对而言觉得人员成本太高，这时 XDR 的一个附带服务 MDR 就可以发挥作用了。MDR 服务中除了结构化 / 非结构化威胁狩猎，最重要的就是根因分析。对于确定性的事件，MDR 服务人员可以出完整的影响面、攻击链、攻击意图分析，还会提供对应的处理建议，使企业不但明确知道发生了什么，为什么，还能够使用最有效的方式去应对、处理。

以 2021 年爆发的史诗级漏洞 Log4j2 为例，该漏洞被黑客大量利用于挖矿攻击，下图是国内的深信服 XDR 针对该类事件的处置动作、响应建议页面：





多维安全视野

可见性一直是网络安全不懈的追求，只有看到问题，才能解决问题。全面的多维度安全视野，意味着可以从终端、网络、服务器、云环境等不同的安全组件中获取数据，做到 360 度无死角的监控。

为了做到全面的安全视野，XDR 在 SIEM 的产品的经验中吸取了养分。传统的 SIEM 首先尝试将所有可能的数据引入到平台“以防万一”，[14]认为这样就不会错过任何可能与安全相关的信息。但不幸的是不同类型的威胁，具有不同的相关性，不同的优先级，需要不同的数据，采用不同的检测方案和调查流程，传统方法不但需要大量繁重的工作和定制，并且这根本不是使安全运营成熟的有效方法。因此在 SIEM 领域也有人提出了“输出驱动”的 SIEM[15]，建议大家摒弃掉“现在就收集”、然后“弄清楚以后如何使用它”这样无效的方式，而提倡除非你知道如何利用和呈现它，否则不会进入到 SIEM 中。这种思想在 XDR 中获得了发扬光大，形成了以威胁为中心的方式，针对更有效的全周期解决单个威胁类型来自动化收集和检测，然后逐渐覆盖主要的攻击者的技战术行为矩阵。这就是 XDR 的核心技术——全面的遥测数据采集——的核心意义。同时这也意味着只有在 EDR、NDR 的基础之上，才能够去构建 XDR 的安全视野。

XDR 即使使用了以威胁为中心的遥测采集方式，同时还需要考虑对云、网、端、身份等信息全面覆盖。特别是网和端，两者各有特点，互为补充，只有通过完整的整合 EDR、NDR 能力，才可以构建全面的安全视野。NDR 产品部署相对容易，在合适的位置可以以较低的成本获得较大范围的网络可见性，同时当前网络中如果存在难以部署终端 Agent 的情况：IoT 设备、非标准 Windows、Linux、MacOS 等，还包括很多设备处于非管理状态，这些情况下都只有依赖 NDR 带来的网络可见性。而 EDR 产品也有大量自身独有的优势，如：可以看到攻击者非常详尽的具体行为，包括进程、注册表和文件等操作，还可以在网络流量加密后的情况下，看到在端侧已经解密的流量。

XDR 通过整合网、端、云的可见性到一个平台上，进而获得了全面的安全视野，这种全面性带来了诸多好处：使安全分析人员可以在一个平台上集中完成所有的监控和分析工作；使威胁告警能够关联攻击故事线中的更多维数据，从而更加精准，误报更少；使研判和分析整个的攻击过程及影响面更有效，为形成最合理的处置决策建立牢固的基础。

[14]https://www.exabeam.com/information-security/an-xdr-prerequisite-prescriptive-threat-centric-use-cases/
[15]https://blogs.gartner.com/anton-chuvakin/2012/09/24/on-output-driven-siem/

攻击可视化

随着网络攻击入侵的手段不断进步，现有的网络攻击不再局限于单步攻击，通过单步攻击引发网络安全设备产生的告警往往无法代表攻击者的目的，仅代表复杂的多步攻击的一个步骤，通常需要关联每一步的攻击行为才能发现其真实攻击意图。近年来与网络安全相关的黑色产业链层出不穷，大多数的黑产团伙也是采用多步攻击才能实现成功入侵受害主机。XDR 作为一个拥有全局安全视野的平台，如果能够提供每个威胁攻击过程的高度可视化，就能使得安全运营更高效，安全态势把握更准确，乃是攻防对抗场景中面对攻击者的一把利器。

真实的安全运营往往需要有经验的安全专家来分析多家安全厂商的产品提供的告警等信息，并结合其自身的专业知识去调查取证分析，进而还原出攻击者完整的攻击路径，然后在攻击路径的每一环节上进行应急处置。该过程的时间消耗一方面取决于攻击手段复杂程度、安全产品所能提供的信息多少，另一方面取决于安全专家对该攻击手段的熟悉程度等因素。整个过程存在时间成本高、高度依赖人工的缺点。因此，自动地提供可视化的攻击路径是网络空间防御体系向着智能化方向发展的重要基础。

攻击可视化实际上从视野由小到大分为四种形式：

终端失陷溯源可视化

在大多数攻击场景中，攻击者往往是先获取网络中的单个 PC 或服务器的权限后，以其作为跳板开展后续的横向移动行为，并逐步扩大影响；黑产中的病毒传播亦是如此，首先感染 0 号主机，之后按照一定的攻击手法感染其他主机与资产。安全分析师进行溯源分析的过程中，首先是需要找到一个典型的失陷主机，查清楚当前主机中攻击者的入口、入侵顺序与技术手法，以便于溯源。基于单主机的溯源调查分析，是多主机关联分析安全事件必不可少的基础。因此单主机溯源可视化至少要包括入口点定位、恶意行为记录的功能，帮助安全分析师快速复现当前主机失陷过程，对症下药进行处置，并跟进攻击者后续行为以减少后续危害扩散。

攻击影响面可视化

攻击影响面评估是在单主机生成了威胁告警之后的下一步研判行为，需要明确失陷主机是否攻击过其他主机、访问过其他服务器、进行了哪些网络通信行为。基于此，安全分析师重点筛选出其他可能的受害者主机，划分此次事件影响范围，做出相应的处置行为如网络划分隔离等。攻击影响面评估为后续多主机的关联起到了承上启下的作用，主要聚焦在单个资产的横向移动、外联行为的发现等。

多主机事件关联可视化

通过对已失陷主机资产的分析、确认不同失陷主机的安全状态后，安全分析师或者平台算法可以根据一定条件将此类事件进行关联分析，就好像警察面对刑事案件时进行并案侦查一样，汇聚成一个跨主机的攻击链事件，还原攻击者的真实目的何在、攻击路径如何。此项可视化能够展现一次复杂攻击事件的全景，为企业复盘安全事件、寻找信息系统薄弱点提供巨大便利。

攻击者画像可视化

对于当前安全事件分析后提取对应的 TTPs（攻击行为特征），结合行业独有的威胁情报与攻击趋势，XDR 可以描绘出当前在企业内外侧的攻击者画像，通过对攻击者的位置、常用漏洞、基础设施、IOC、样本、攻击手法、近期活动趋势等信息进行汇总，帮助企业对当前攻击者有更加全面详尽的认知，知己知彼，方能百战不殆。同时如果可以与 SaaS 能力相结合，将攻击者可视化画像通过云端下发到同行业，就如同通缉令一般，起到防患于未然的作用，形成更强有力的防守壁垒。

攻击可视化是安全运营快速演进、高度发展下的必要产物，XDR 作为一个集威胁发现、防御与响应为一体的安全运营平台，提供先进的可视化技术，才能与平台后端高速发展的检测与分析技术相匹配，也是让安全运营人员省时、省力、省心的最直接手段。

发展问题及建议

DEVELOPMENT ISSUES AND SUGGESTIONS

平衡效率与隐私，逐步接受SaaS

从国外安全行业的发展看，SaaS 化带来了巨大的市场价值，对于解决当前行业面临的问题越发显得重要：

01

降低人员成本

通过 SaaS 化，集中分析、处理安全事件，可以形成规模化，进一步完成精细分工，提升专业人员的效率，使更多用户可以享受专家级服务；

02

提升防护水平

SaaS 化使安全厂商第一时间将最新的成果，包括功能、检测模型、服务等系统级业务交付给用户，这对于看重时效性的攻防对抗领域至关重要；

03

促进技术进步

通过汇集不同环境的遥测数据，可以真实提升 AI 模型的精度和检出 / 分析能力，促进防护能力的提升；

04

优化人员产出

通过 SaaS 化，可以将单纯攻防领域的任务交付第三方，而组织自身的安全团队聚焦在和业务关联性更强的工作中，保障整体的产出成果。

正是因为 SaaS 化这些难以替代的优势，很多国家对它的态度已经从拒绝转变为推广。在 2021 年 5 月美国白宫在关于改善国家网络安全的行政命令中，明确提到“现代化联邦政府网络安全……加速专项安全云服务，包括 SaaS、IaaS 和 PaaS，集中和简化对网络安全数据的访问，以推动用于识别和管理网络安全风险的分析”[15]。

[15] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

同时对 SaaS 化带来的隐私方面的风险，很多行业、部门已经逐步形成了相对有效的解决方案：

数据泄露风险

遥测数据的引入，使安全数据和业务数据、隐私数据之间有了明显的区隔，遥测数据更多和底层系统相关、和关联威胁的异常相关，遥测数据中不包含高层次的业务和隐私数据；同时以安全为目的的数据采集和存储，强调时效性，除非用户要求一般仅存放 30 天。

事件披露问题

在成熟的 SaaS 化平台中，安全事件数据和组织信息是分开独立存放的，除了特殊授权情况下，只有用户企业能够将事件和组织关联在一起。这就避免了非必要人员了解企业发生的安全事件的可能性。

从趋势上看，SaaS 化已经是一个必然的方向，如何能够从自身业务出发，逐步探索利用 SaaS 来给企业带来更大价值，成为每个组织都需要考虑的问题。

关注AI+安全，提升行业生产力

人工智能在过去十年取得了特别惊人的进展，突破了视觉识别、自然语言理解、语音识别、自动推理等技术。AI 在网络安全中发挥的价值越来越明显。在 XDR 中，AI 技术可以提供有效的威胁事件优先级、支持自动化响应，以解决攻防对抗中速度和规模的难题。采用 AI 方式快速分析和关联数十亿数据的模式，XDR 显示出秒级追踪各种网络威胁的巨大希望。

人工智能带来的自动化和大规模检测、优先级排序和响应能力，不但可以减轻网络安全专业人员的负担，还可以帮助解决不断扩大的安全行业劳动力缺口——根据 ISC 2021 网络安全劳动力研究，全球网络安全专业人员短缺 272 万；[17]美国劳工局估计，从 2020 年到 2030 年，网络安全就业机会年度增长 33%，是平均水平的 6 倍，但进入该领域的人数远远没有达到相应的速度[18]。同时，安全运营团队要分析的告警通常比分析人员能处理的多，从而导致错过的告警演变成为安全事故。趋势科技的一项调查表明，51% 的人认为它们的团队被海量的告警淹没，55% 的人对自己有效确定告警优先级和响应事件的能力没有信心，27% 的时间花在了处理误报上。[19]

在这种背景下，行业内的安全公司需要尽可能关注人工智能，通过不同的手段提升相关能力，促进整体行业的生产力提升：

- 注重人工智能在网络安全上应用的教育和培训，加强行业从业者的相关能力培养；
- 投资 AI+ 安全，利用机器学习、推理和自动化来检测、响应并保护网络杀链的每个步骤；
- 建立跨公司、科研机构的合作伙伴关系，以促进围绕网络安全数据集、最佳实践和研究的共享和合作。

[17] https://www.isc2.org/News-and-Events/Press-Room/Posts/2021/10/26/ISC2-Cybersecurity-Workforce-Study-Sheds-New-Light-on-Global-Talent-Demand

[18] https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[19] https://newsroom.trendmicro.com/2021-05-25-70-Of-SOC-Teams-Emotionally-Overwhelmed-By-Security-Alert-Volum

建立互通标准，推动生态建设

XDR 相对于 SIEM 产品，已经把焦点集中在检测和响应之中，即使在这个相对具体的领域也是充满了技术挑战，虽然需要将不同的安全组件深度集成在一起，但现实中却存在一定的挑战：

- 一个 XDR 厂商，即使可以提供各种需要的安全组件，但客观来说，研发能力局限性很难保障它能够将任何组件都做到业内领先；
- 如果希望深度整合多家厂商的安全组件，但因为组件之间的开放性不够，整合的深度很低，难以在统一平台上充分发挥其价值。

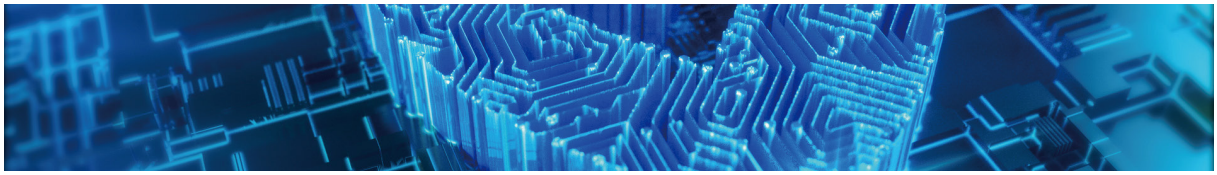
基于此国际厂商逐步采用了生态合作的方式：

- 2021 年 8 月，多个厂商共同建立了 XDR 联盟[20]，包括 ARMIS、Exabeam、Expel、ExtraHop、Google、Mimecast、Netskope、SentinelOne、CyberARK、RecordedFuture 等。希望由此：
  - a) 定义、推广和发展具有包容性和开放性的 XDR 定义和架构，以满足当前和未来的用户需求；
  - b) 提高 XDR 方法和最佳实践的认知；
  - c) 帮助推动 XDR 工具和服务的改进；
  - d) 通过教育和联合营销活动，促进 XDR 的开放性和包容性。
- 2021 年 10 月，CrowdStrike 牵头成立 CrowdXDR 联盟[21]，期望通过联盟建立一个共享数据交换模式，以使用最相关、特定供应商的安全遥测来丰富 XDR 数据，达到跨产品集成、大规模提升安全效能和效率、通过共享遥测进行深度防御以及简化运营效率的目的。其核心伙伴包括：Google Cloud、ServiceNow、Zscaler、Netskope、Proofpoint、Extrahop、Mimecast、Claroty、Corelight。它们分布从云环境、SASE、邮件、网络等方面和 CrowdStrike 的优势终端能力整合，形成各方面均较为领先的 XDR。

这种形势下，我国依据网络安全技术发展的现状，也逐步开始构建相关的标准，如 2022 年 4 月 8 日以中国信息通信研究院牵头、联合深信服科技、启明星辰、安恒等企业成立的《网络安全产品互操作标准体系研究》项目正式立项，进一步推动了厂商间的安全生态构建。后续在此基础上还需要尽快构建相关标准，具体包括：

- 构建以遥测数据共享交换为中心的数据标准体系；
- 构建以自动化根因分析 / 自动化遏制为目的的事件响应接口标准体系。

通过这些标准的建立，以及推动厂商提供符合标准的产品，不同厂商产品间的深度集成成为可能性，进而推动整个产业的协同合作，聚焦各自优势技术领域快速发展安全能力，以尽快提升产业整体的安全水平。



[20] https://www.xdralliance.com/

[21] https://www.crowdstrike.com/press-releases/crowdstrike-sets-the-standard-for-xdr-through-new-crowdxdr-alliance/

深信服科技股份有限公司

地址：深圳市南山区学苑大道1001号

联系电话：400-806-6868

邮编：518055

www.sangfor.com.cn

中国信息通信研究院

地址：北京市海淀区花园北路52号

联系电话：+86 10 62300559

邮编：100191

www.caict.ac.cn

网络安全卓越验证示范中心

地址：北京市海淀区东冉北街9号院

宝蓝·金园网络安全服务产业园A幢A2-005

联系电话：010-62308680

邮编：100195