

简译版

XDR：安全的新前沿

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	XDR: Security' s new frontier		
原文作者	杰拉尔德·雷迪特 (Gerald Reddig)	原文发布日期	2021 年 6 月 30 日
作者简介	杰拉尔德·雷迪特是诺基亚全球产品组合营销总监。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/06/30/xdr-security/		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	无论通信服务提供商（CSP）选择 XDR 的原因是什么，很明显的一点是，该技术可以为在各方面带来很大的价值，包括猎杀威胁、调查安全漏洞和聚合数据等。XDR 能够提高安全团队的可见性，缩短响应时间，提高生产力。这使其成为真正独一无二的解决方案，应该被更多企业所采用。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

XDR：安全的新前沿

杰拉尔德·雷迪特

2021 年 6 月 30 日

随着企业开始转变其 IT 环境和员工队伍，他们需要找到正确的安全方法，这对于获得成功至关重要。如果没有适当的保护措施，将服务迁移到云会带来很大的风险。

要想开发出真正面向未来的安全解决方案，企业应跳出框框思考。“扩展检测和响应”（XDR）提供了更简单的单一面板视图，可将多个安全产品无缝集成到一个系统中，使企业能够超越典型的安全功能。XDR 旨在帮助安全团队识别复杂的威胁并提高响应速度，是作为“只能够提供一层可见性的解决方案”的替代方案开发的。

为了实现 XDR 安全运营的现代化，通信服务提供商（CSP）首先要收集正确的信息。这意味着，他们要使用一种能够持续管理、更新和高度关联的集中安全管理平台。

但是在实践中，从任何应用程序、网络元素、联网资源或设备中挖掘大量数据，会带来很大的挑战，很少有企业能够应对这种挑战。

如今，企业通常拥有庞大的网络，这些网络涵盖数十个甚至数百个移动员工和设备、家庭办公室、SD-WAN 连接的分支机构、多个云和“软件即服务”（SaaS）应用程序，以及 OT 系统和分布式物联网（IoT）设备。因此，安全团队不得不管理越来越多的数据。

许多企业会为每个新网段提供新的安全解决方案，来临时性地处理上述问题。但是，这种方法缺乏中央应急响应计划或安全策略，导致安全运营团队在其网络中平均设置了 40 种不同的产品。

此外，许多解决方案都是孤立运行的。它们无法共享或收集威胁情报报告，也无法与其他解决方案轻松集成以在网络的同一部分（更不用说跨不同环境）进行威胁响应。安全运营团队无法通过端点、网络和云集中编排或管理策略分发、执行或配置。

5G 网络的应用导致安全数据的生成呈现多样性、海量性和高速性。因此，XDR 技术必须以现代数据管道为基础，并能够跨混合 IT 环境大规模收集和处理安全数据。

集成、互操作、安全

为了识别最迫在眉睫的威胁，安全管理人员和数据分析师需要一个通用情报来源，以便跨网络快速、准确地关联情报。

为此，CSP 的安全工具必须具有极高的互操作性。无论这些工具位于何处，都需要与其他安全工具共享告警和威胁数据，以及利用常见的安全情报源。

要想实现这一目标，最简单、最有效的方法是：使用可以连接不同供应商的安全工具的集成安全平台，构建通用安全框架。此类平台需要具备：

- 集成的安全运营：这能够提供跨网络的单一视图，使运营商能够在威胁影响到服务之前予以阻止。
- 精简的安全工具：通过精简安全套件，CSP 可以更自信地扩展其网络，同时保持其完整性。
- 增强的威胁情报：通过全面了解威胁形势，CSP 可以确保网络的完整性，减少识别主要威胁的需求。

虽说 CSP 通常采用“安全编排、自动化和响应”（SOAR）解决方案来协调其整个安全运营中心（SOC）和网络运营中心（NOC）的分布式安全系统，但他们也可以利用 XDR 解决方案来实现更加统一和安全的响应。

通过 XDR 实现 SOC 的现代化

许多 CSP 将 XDR 计划作为其“安全信息和事件管理”（SIEM）解决方案的补充。SIEM 是 SOC 的基础组成部分。大多数企业会使用 XDR 补充 SIEM，以帮助分析师对事件进行分类、提高告警保真度，或添加用于威胁检测的高级分析。

其他 CSP 则将 XDR 计划的重点放在：为 SaaS 应用程序和基于云的工作负载添加响应和威胁检测功能，并检测潜在的攻击者、恶意软件或其他网络异常。

无论他们选择 XDR 的原因是什么，很明显的一点是，该技术可以为在各方面带来很大的价值，包括猎杀威胁、调查安全漏洞和聚合数据等。XDR 能够提高安全团队的可见性，缩短响应时间，提高生产力。这使其成为真正独一无二的解决方案，应该被更多企业所采用。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问：<http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问：<http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问：<http://www.avlsec.com>