卡巴斯基 Next XDR 专家版

更强 更好 更快 更多

kaspersky

是游戏规则改变者，还是一个噱头？

XDR：扩展检测与响应

这是许多人常提到的首字母缩略词，但像所有相对较新的技术一样，并非每个人都确切地知道它是什么或者它对他们的业务有什么益处。有一点是确定的 — XDR 涉及从被动反应到主动应对的战略转变，因为“等待并观望”在网络安全中是不可行的。内行人士将 XDR 视为一种战略，而不仅仅是一个产品。

那么，XDR 究竟是一个最新的技术噱头，还是一个潜在的游戏规则改变者？问题是确实存在的，从全球技能短缺、IT 安全人员超负荷工作、不断变化的威胁形势，到警报过载、不同的工具、匮乏的威胁情报和不断扩大的攻击面。IDC 表示，XDR 将是“一股颠覆性力量，影响 SIEM、EDR、SOAR、网络情报和威胁分析平台以及外部威胁情报提供商的销售”[1]，Forrester 认为，差异化的 XDR 技术“将在短期内取代端点检测与响应 (EDR)，长远来看将取代 SIEM”[2]。

XDR 面向的对象：

XDR 面向具有成熟的安全体系架构、需要单一平台提供完整连贯的信息来了解基础设施情况的组织。

XDR 将成为一股颠覆性力量 — IDC

更多设备、更多应用、更多网络流量、更多数据、更多威胁…

XDR 面向的对象 — 它可以解决哪些挑战？

XDR 面向具有成熟的安全体系架构、需要单一平台提供完整连贯的信息来了解基础设施情况的组织。

这些组织面临的网络安全挑战是一致且根深蒂固的。ESG Research 调查了多家拥有超过 100 名员工的组织的 IT 和网络安全专业人员[3]，这些组织超过 80% 是涉及多个垂直领域的企业。以下是一些主要发现：

难以跟上 SOC 技术的运行要求

由于难以跟上 SOC 技术在数据管道中的可扩展性、负载均衡处理引擎、增加存储容量等方面的运营需求，现在管理安全操作比过去两年的任何时候都更加困难。

1 来源：IDC，《全球安全产品分析：从 Power Point 到强大的产品，XDR 的现状如何？》，2022 年

2 来源：Forrester，《扩展检测与响应 (XDR) — 惯例与创新之争》，高级分析师 Allie Mellen，2021 年

3 来源：ESG 研究报告，《SOC 现代化和 XDR 的作用》，2022 年

不断增长和不断变化的攻击面以及整体威胁格局

更多设备、更多应用、更多网络流量、更多数据、更多威胁。威胁形势不断变化，而且随着新工具的不断涌现，网络威胁的数量和复杂性也在不断演变。同时，黑客的进入门槛比以往更低，一方面是低技能的买家在暗网购买廉价的打包威胁，另一方面是高技能、有耐心的黑客在构建复杂的攻击。别忘记还有内部威胁和供应链漏洞。

管理安全性需要大量手动流程

有更多的安全数据需要收集和处理，而手动处理低效低能。这会严重影响可扩展性，导致过度依赖人工干预，并在总体上降低应对威胁的效率。

无法制定检测规则

由于缺乏时间、资源和技能，无法制定检测规则、微调安全控制以及快速有效地识别和处理威胁。组织并不总是拥有合适的技能或员工来跟上安全分析和运营的步伐。这直接引出了下一个痛点……

真正的全球技能短缺

尽管全球网络安全专业人员的数量达到 470 万的历史最高水平，但仍存在 340 万人的 人员 缺口有待填补。这一缺口的扩大速度是从业人员增长速度的两倍，同比增长 26.2%。[4]

[4] 来源：(ISC)²，《网络安全人力研究》，2022 年

现有工具经常难以

检测和调查高级威胁，需要专门的技能来使用和管理它们。

工具不契合用途

当工具本身成为问题的一部分时，就必须做出改变了。现有工具经常难以检测和调查高级威胁，而需要专门的技能来使用和管理它们。研究[5]表明，目前的工具通常不能有效关联警报，IT 安全人员苦于需要使用多种不相关的不同工具来处理不同的数据。这种做法效率低下、繁琐、混乱并且昂贵。另一个挑战是目前的工具无法扩展以应对不断扩大的攻击面，并且在云检测和响应能力方面存在很大差距。[6]

难怪您的首席信息安全官看起来压力很大

好消息是，改进安全运营已成为当务之急，并且获得了资金支持 — 88% 的组织今年将投入更多资金，66% 的组织表示工具整合是优先事项，并且现代应用程序开发和部署速度已加快，需要新的技能。[7]

88%

的组织今年将投入更多资金来改进安全运营

66%

表示工具整合是优先事项

XDR 的作用

以下是 XDR 直面这些挑战的方式。

XDR 更好地检测高级威胁

XDR 的威胁检测功能涵盖端点、网络和云环境。它使用机器学习算法和行为分析来识别复杂威胁，包括恶意软件、勒索软件和高级持续性威胁 (APT)。

自动响应和执行补救措施

XDR 可自动执行响应和执行补救措施，使组织能够快速遏制威胁并最大程度地减少任何潜在损害。它可以自动隔离或孤立受损端点、阻止恶意活动并修复漏洞，从而减少手动操作和响应时间。

与端点保护工具集成

与 EPP 的集成是一个关键问题，XDR 利用丰富的端点遥测数据和行为分析来提供对端点活动的深入洞察。它采用先进的机器学习算法来识别可疑行为和攻击指标 (IOA)，促进早期发现复杂威胁。

5 来源：ESG 研究报告，《SOC 现代化和 XDR 的作用》，2022 年 5 月

6 来源：ESG 研究报告，《SOC 现代化和 XDR 的作用》，2022 年

7 来源：ESG 研究报告，《SOC 现代化和 XDR 的作用》，2022 年 5 月

XDR 如何融入 EDR、MDR、SOAR 和 SIEM 生态系统

关键在于 X — 扩展。XDR 可扩展 EDR 提供的功能，主动跨多个基础设施级别检测复杂威胁，并自动响应和应对这些威胁。

集成方法是关键

通过集成多个工具和安全应用程序，并监控端点、网络、云、Web 服务器、邮件服务器等的数据，XDR 能进一步检测和消除威胁，同时通过自动化跨产品交互来简化信息安全管理。

Forrester 认为，在大多数情况下，XDR 不会完全取代安全分析平台，同时指出“XDR 正在发展中，[我们] 预计在未来五年，安全分析平台和 XDR 将会融合”。

SIEM 的用例不仅限于威胁检测，SOAR 的可定制性很有用，但在涉及到检测和应对威胁时，XDR 增强保护的高级分析是首屈一指的。

提供实时可见性

XDR 提供对组织安全态势的实时可见性。它收集并分析来自端点、服务器、防火墙和云平台等各种来源的数据，在单个控制台中提供对持续威胁和可疑活动的全面洞察。这使其真正具备主动性 — 主动的威胁搜寻和更快的事件响应。整体视图帮助安全团队更有效地识别可疑活动和潜在的安全事件。

将数据和威胁情报情境化

当 XDR 利用高质量威胁情报和全面的威胁情报数据库时，可以提供非常有用的有关威胁和攻击者的情境信息。这种丰富的威胁情报简化了调查警报和事件处理，并帮助安全团队了解威胁行为者的策略、技术和动机，从而促进更有效的事件响应和主动防御措施。

实现简化的安全运营

经过适当集成的最佳解决方案可轻松融入您当前的基础设施，以提供自动化的最佳结果，并提供全面的可视性和感知，而无需更换已在使用中的第三方安全解决方案。而且不要忘记，通过提供全面的安全事件和用户行为视图，集成可支持合规性。

显然，XDR 可以实现其承诺：控制、稳定性和最重要的优势。但并非所有 XDR 产品都是一样的... 如何选择适合您的产品？

比较 XDR 供应商和解决方案时需要考虑的 5 个关键事项

以下是 XDR 直面这些挑战的方式。

1

XDR 解决方案的质量与供应商的 EPP 和 EDR 之间的协同作用存在直接联系

在端点级别对复杂网络威胁进行高级检测和响应的 EDR 解决方案是 XDR 的关键要素。同时，EDR 需要强大的端点保护平台 (EPP) 来自动筛选海量大规模威胁。必须仔细查看端点保护功能，并检查是否支持所有类型的端点 – PC、笔记本电脑、虚拟机、移动设备和各种操作系统。

2

最新的威胁情报以及对网络犯罪分子策略和技术的全面了解对于应对网络威胁至关重要

这不是难以理解的事 — 任何真正有价值的 XDR 解决方案都具备这两种功能，与其他情境一起改进和加快事件调查和响应。

3

与第三方解决方案的集成更具可持续性和成本效益

XDR 解决方案与第三方的集成程度是另一个绝对关键的问题，因为互操作性使购买从一开始就成为更具可持续性的投资。提供大量真正集成选项的 XDR 解决方案将收集更多数据源，并提供更全面的基础设施情况。

4

独立审查、全球认可和独立测试结果很重要

当您投资于像网络安全这样对业务至关重要的方面时，不要忽视独立测试。要求提供独立测试的结果。查看 Forrester、IDC 等机构的国际认可情况。解决方案是否在全球范围内实施？要求提供案例研究。

5

您的投资是否面向未来？

技术不会停滞不前，尤其是像 XDR 这样相对较新的技术，您应该了解供应商的持续发展路线图。

为何选择卡巴斯基

久经考验。屡获殊荣。卡巴斯基保护。

卡巴斯基是一家成熟的全球网络安全公司，拥有丰富的安全专业知识。25年来，我们一直在保护世界各地的组织，我们的产品和服务获得了无数奖项和荣誉。2013 年至 2022 年间，卡巴斯基产品：

587

获得 587 次第一名

685

获得前三名

827

参加了 827 次独立测试和评审

2023 年，卡巴斯基被全球领先的技术研究和咨询公司 ISG 评为 XDR 解决方案市场的领导者。ISG 将"领导者"定义为拥有全面的产品和服务，并代表创新实力和竞争稳定性。

了解更多

卡巴斯基EDR

了解更多

www.kaspersky.com.cn

#卡巴斯基
#引领未来