CISCO
SECURE

立场文件
思科公开信息

XDR 入门指南：
简化安全运维，大有可为

目录

引言

提到安全运维中心 (SOC)，您会想到什么？一群安全专家挤在办公室里，紧张地对大量警报进行分类？还是会想到一个大房间，里面挂满了巨幅的威胁地图？

安全运维堪称业内最艰巨的工作之一。多年来，伴随着全数字化转型的推进和新技术的广泛采用，SOC 在组织中发挥着越来越重要的作用，复杂程度也更甚以往。

根据最近的一份 ESG 报告，一半以上的组织在开展安全运维工作时使用超过 26 种不同的市售工具、自行开发的工具或开源工具。[1] 新技术的采用本应简化 SOC 团队的工作，但事实往往并非如此。

万物互联的影响

随着混合办公模式的兴起和云的采用，我们实现了前所未有的高度互联。组织运维已转变为以综合生态系统为中心，企业、客户、供应商和合作伙伴之间的边界日渐模糊。万物互联的新时代已经来临，虽然这对商业和个人生活都有诸多好处，但也会导致受攻击面不断扩大，复杂网络攻击的数量不断攀升。

我们深知，很多企业会寄希望于通过采用最新技术，解决新型安全问题。但现实是，如果没有一种可以简化整个安全体系的解决方案，使用的工具越多，就只会使得已然支离破碎的安全环境越发混乱。这样可能会导致更多的安全漏洞并拖慢工作进程，而我们的真正目标本来是为了加速检测威胁并确定响应的优先级。

> “要真正发挥解决方案的效力，网络安全供应商必须乐意共享数据和情景信息，以便对尽可能多的威胁媒介使用高级分析功能，快速检测出威胁，成功应对世界上极其复杂的威胁发起者团伙。”
>
> – AJ Shipley
> **威胁检测与响应产品管理副总裁**

时间就是金钱

让我们直面现实，在安全方面，时间就是金钱。平均而言，公司发现并遏制一个漏洞需要 277 天的时间。这意味着攻击者可在企业毫不知情的情况下在企业中潜伏近 10 个月，每天肆意访问各种内部应用，窃取私人数据。企业绝不能容忍这种情况!

安全分析师每天竭尽全力对数以千计的警报进行分类，确定其优先级，希望找到最有效的威胁检测和补救方法；但大多数人都疲于应对。要真正解决上述问题，我们必须考虑安全团队成效不佳的根本原因:

1. **集成效果不佳，无法充分利用现有安全投资**

   大多数公司在构建整个安全基础设施时依赖多家供应商的工具，这意味着他们往往有多个独立的解决方案，很少甚至没有集成或共享遥测数据。如果这些解决方案无法协同工作，就会产生滚雪球效应。

   如果集成效果不佳，共享的遥测数据和情报数量就会受限，无法创建情景丰富的统一视图。如果无法洞察整个企业面临的所有威胁，便无法大规模有效缓解风险，甚至可能根本无法缓解风险。

   思科威胁检测与响应产品管理副总裁 AJ Shipley 说得好：“多年来，网络攻击者一直在利用各种可能的漏洞进一步实施攻击，比如，由于缺乏数据共享，企业无法有效地对多家供应商精确度不高的警报进行关联分析，从而实现高度准确的检测。要真正发挥解决方案的效力，网络安全供应商必须乐意共享数据和情景信息，以便对尽可能多的威胁媒介使用高级分析功能，快速检测出威胁，成功应对世界上极其复杂的威胁发起者团伙。” 安全团队需要一种开放且可扩展的方法，确保解决方案能够更出色地协同工作。

2. **警报过载**

   ESG 最近的一份 SOC 现代化研究表明，37% 的 IT 和安全专业人员坦承，由于安全警报数量增加而且复杂程度更甚以往，2022 年安全运维工作比两年前更加难以管理。分析师不仅要正确识别威胁，还要确定其优先级，以便确定最佳补救策略，最大限度地减少对业务的影响，为了在这两个方面之间寻求平衡，分析师举步维艰。

   如果分析师没有足够的威胁情报或情景感知能力，几乎不可能根据业务影响确定威胁的优先级。其结果很可能是，系统会收到大量警报，而分析师却无法准确区分哪些警报如果被忽视，可能会使公司损失 500 万美元，哪些警报几乎不会产生任何影响。

3. 技能短缺

大多数公司都缺乏具有平衡上述职责所需技能的分析师，这进一步加剧了孤立系统和警报疲劳对安全运维的影响。根据 ESG 的研究，81% 的 IT 和网络安全专业人员认为，其安全运维工作受到全球网络安全技能短缺的影响。[2]

公司需想方设法提高分析师的技能，确保发现并重视合适且可行的洞察，避免遗漏或忽略重大威胁。全球和本地威胁情报的集成可提供额外情景信息，助力团队准确标记威胁并确定其优先级，进而弥合差距。这可以提高分析师的认识，帮助他们了解哪些威胁具有较高风险且应立即加以解决以提高安全效力，从而提高团队成效，摆脱其经验和技能的限制。

XDR 正在改变固有模式

随着威胁变得越来越复杂，基于独立单点安全解决方案构建的传统检测和响应模式已经无法满足需求。很多团队已改用 SIEM 和 SOAR 等解决方案，试图统一各种孤立的环境并减少警报数量，但问题仍然存在。当今的安全团队需要一种解决方案，能够将各种来源的数据转换为可靠的警报和洞察，以便胸有成竹地快速采取行动。

过去几年中，扩展检测与响应（简称 “XDR”）这一新兴技术发展势头强劲，有望通过一种开放、统一的方法快速有效地预防、检测和应对威胁，填补市场空白。

51%

根据 ESG 的研究，51% 的专业人员表示，目前使用的安全工具难以检测和调查高级威胁。[2]

但是 XDR 究竟是什么？简而言之，XDR 解决方案可收集多种安全工具的遥测数据，形成集中式数据存储库，然后将收集的数据经过规范化处理后进行分析，以检测恶意行为，更快地应对检测到的恶意行为，并采取补救措施。借助有效的 XDR，各个级别的分析师都能更轻松地专注于全面检测威胁，按风险程度对事件进行优先级排序并予以响应，提高工作效率。

以风险为中心的 XDR 解决方案可利用全球威胁情报和本地情景信息，快速量化、验证威胁并确定威胁的优先级。

开展数据关联分析，随时随地检测最复杂的威胁

很多数据需要保护，这些数据遍布网络、终端、电子邮件和应用。

我们深知，绝大多数组织利用多供应商安全体系来调查和应对威胁。这些解决方案彼此孤立，只能针对给定时间所发生的情况提供部分可视性，但是如果这些可视性数据进行整合，便可转化为切实可行的有用洞察。

把握重点，快速行动

各企业面临的实际情况不尽相同。如果对您的企业而言最重要的系统和运维长期面临威胁，可能会有损品牌声誉或导致财务损失。更糟糕的是，分析师通常没有时间对每天发现的大量警报进行准确的优先级排序。

但是，以风险为中心的 XDR 解决方案可利用全球威胁情报和本地情景信息，根据重大风险的概率快速量化、验证威胁并确定威胁的优先级。实际上，XDR 可以实现全球和本地情景信息的统一，直观洞察整个攻击过程，帮助分析师了解根本原因和全部影响范围。

正确实施 XDR 的五大要素

1. 提供按优先级排序且切实可行的遥测数据，随时随地为您所用
2. 支持统一检测，不受媒介和供应商的影响
3. 快速、准确应对威胁
4. 提供统一调查视角，简化用户体验
5. 提供机会，提高工作效率，加强安全态势

提高效率，最大限度地提升价值并加速实现成果

除了攻击者之外，情景信息、技能和时间不足也是企业在安全方面面临的主要挑战。但是，有了统一的 XDR 控制台，即使是资源和时间有限的团队也能大幅缩短威胁驻留时间。

XDR 方法可将安全数据汇聚到一个中心位置，助力各经验水平的团队更轻松、快速、准确地分析最关键的威胁，确定其优先级并做出响应。内置的协调和自动化功能可帮助团队减少重复性任务，帮助团队将有限的资源用于最需要的地方。

安全弹性之旅

当今之世，不确定性乃是必然。为应对不确定性，公司大力投资，以期全面提升业务弹性。如果没有安全弹性，企业很容易受到不可预测的威胁和变化的影响。

我们的 XDR 解决方案是 Cisco Security Cloud 开放式集成平台的一部分，即使是在最复杂的混合多云环境中，也能融合安全弹性。随着越来越多的解决方案接入 XDR，您可以在所有必要的媒介中加强检测，执行更全面的响应操作。

为什么选择 Cisco XDR？

客户是思科一切工作的核心。因此，我们提供了一款全面的 XDR 解决方案，其中包含由领先安全供应商提供的广泛第三方集成库，可实现最大程度的灵活性。

与未实施 XDR 的组织相比，实施成熟 XDR 的组织在安全弹性方面有 **45%** 所提高。[3]

我们明白，您肯定不希望加剧复杂性，因此我们创建了一个一体化控制台，安全和 SOC 分析师只需点击几下即可检测、调查威胁并采取补救措施。我们的解决方案具有开放性、可扩展性和云优先等特点，让您可以优化现有安全投资，在整个环境中实现统一的安全检测。

Cisco XDR 助力团队逐步实现目标

- 整合解决方案和技术
- 统一切实可行的遥测数据
- 协调检测与响应
- 实现工作流程自动化，扩大部署规模
- 优化、发展和微调安全策略

[1] ESG 全面调查结果：SOC 现代化和 XDR 的作用，Enterprise Strategy Group (ESG)，2022 年 9 月
https://www.esg-global.com/research/esg-complete-survey-results-soc-modernization-and-the-role-of-xdr

[2] SOC 现代化和 XDR 的作用，Enterprise Strategy Group (ESG)，2022 年 6 月
https://www.cisco.com/c/en/us/products/security/soc-modernization-xdr

[3] 安全成果报告第 3 卷，思科，2022 年 12 月
https://www.cisco.com/c/en/us/products/security/security-outcomes-report.html