Enterprise Strategy Group | Getting to the bigger truth.™

利用 MDR 弥合安全运营缺口

破坏性网络攻击风险不断升级，为予以应对，您不得不从核心业务目标中分出精力和预算，因此组织必须通过加强网络安全计划来做出响应。安全运营 (SecOps) 负责监视和保护数字攻击面的各个方面，是所有网络安全计划的核心。

尽管投入大量资源，安全运营难度仍持续上升

超过一半
的受访者认为，与两年前相比，如今的 SecOps **更困难一些。**

» **SecOps 面临更多困难的五大原因。**

1. **41%**
威胁形势正在迅速发展和变化

2. **39%**
攻击面不断变化和发展

3. **37%**
安全警报的数量和复杂度不断增加

4. **34%**
我的组织越来越多地使用公有云服务

5. **33%**
很难满足安全运营技术的运营需求

重新思考计划战略

攻击面和威胁态势的规模和复杂性都在增长，相应地，安全控制措施也是如此，这就生成了成千上万的警报和海量安全数据。安全团队正在重新思考总体计划运营，以进一步整合来自 IT 和业务线团队的资产和风险数据，专注于那些对组织目标构成更大风险的威胁。

98%
的组织要么已与 MDR 提供商达成合作，要么计划在未来 12 个月内与其合作。

88%
的此类组织计划在未来 12 个月内增加 MDR 的使用量。

» **MDR 参与的关键价值驱动因素。**

运营改进和效率。
MDR 可帮助组织通过多种方式（如基础架构、人员和管理）降低安全运营的总成本。它还可解决"警报疲劳"问题，可更有效地显著降低误报。

提高了网络安全效力并降低了风险。
MDR 可帮助组织阻止已经侵入的威胁，改进对潜在威胁和高级持续性攻击的检测，开始主动纠察威胁，并设立更强有力的控制机制以识别和预防未来攻击。

» **贵组织使用或计划使用托管服务的主要原因。**

55%
重点：
我的组织希望安全人员专注于更具战略意义的安全计划上，而不是将时间花在安全运营任务上

52%
服务：
我的组织认为服务提供商在安全运营方面可以做得比我们更好

49%
增强：
我的组织相信服务提供商可以在安全运营方面增强我们的 SOC 团队

42%
技能：
我的组织没有足够的安全运营技能

> **许多早期 MDR 解决方案的设计和实施只适合过去那个时代，**那时没有那么数据和威胁，检测也更简单。"
>
> - Dave Gruber, ESG 首席分析师

对 MDR 的新要求

许多早期 MDR 解决方案的设计和实施只适合过去那个时代，那时没有那么数据和威胁，检测也更简单。下一代 MDR 解决方案必须做足准备，以保护更多样化的攻击面，检测更复杂的威胁，要更多地围绕风险并以此为方法进行优先级排序并缓解威胁。

- 全天候监视事件和日志。
- 就可疑活动和警报的数量、位置和类型提供快速、清晰的信息。
- 持续且可扩展的网络监视和威胁分析。
- 针对上下文响应选项的 AI 驱动型建议。
- 监管合规性报告。
- 与内部团队直接联系的"人力"安全顾问。
- 基于威胁检测、分类、调查和取证的详细实时分析。
- 漏洞评估、优先级排序和缓解指导。

在考虑能够提供一些、大部分甚至全部外包 MDR 功能的大量潜在服务提供商时，**组织应寻找能够具备以下能力的合作伙伴：**

- 上下文威胁情报。
- 经验证在组织地理覆盖范围、垂直市场和法规概况方面具有出色的业绩记录。
- 展示出威胁搜索功能。
- 长期致力于基于云的 MDR。
- 在多云和混合云环境、零信任和云安全责任共担模型方面具有全面的能力。
- 经验证，可基于创新技术、经验证的流程以及员工展现出的专业知识，随时间推移扩展其服务。

更重要的事实

破坏性网络攻击风险不断升级，为予以应对，您不得不从核心业务目标中分出精力和预算，因此组织必须加强网络安全计划。虽然应用场景各不相同，但大多数组织都在利用 MDR 服务提供商来扩展其计划。

Dell Technologies 采用先进的托管检测和响应方法，结合了灵活、智能且可扩展的技术与经验丰富的网络安全专业人员，可帮助规模不一、资源储备各异的组织加速并强化安全计划。

了解详情

DELL Technologies

来源：ESG 完整问卷调查结果，《SOC Modernization and the Role of XDR》，2022 年 8 月。
© 2022 TechTarget, Inc. 保留所有权利。