网络安全中的人为因素

想象一下最坏的情况。

您的整个数据中心因复杂勒索攻击而瘫痪。销售、客服和财务系统全面停摆。您是一名高级 IT 主管，正全力主导系统还原工作，但解决方案始终悬而未决。

您的团队本就人手不足，如今已连续数周超负荷运转，几乎没有休息时间。部分从业人员甚至**不眠不休奋战了 36 个**小时。更令人担忧的是，决策者因极度疲劳可能导致判断失误，甚至危及整个恢复进程。

当前亟需能立即投入支援的外部资源 — 但该从何处调兵遣将？

这看似小说开篇的场景，实则是戴尔客户真实遭遇的困境。这揭示了当今网络安全环境中的一个重大问题：人为因素。

最新数据显示，全球网络安全专业人才缺口已接近 500 万。危机爆发时方觉资源告急，而解决方案早在隐患潜伏时便已生根。

从构建和壮大人才管道着手

确保资源储备的第一步是构建人才梯队：

校园招聘和实习
与本地高校及技术院校合作，可以输送源源不断的初级人才。通过系统培养，这些新生力量将逐步成长为核心团队成员。

持续培训和开发
在时间与预算的双重压力下，网络安全专业人员必须同步应对工具和威胁的变化。

聚焦人才留存
优秀的从业人员（尤其是具备实战经验者）始终是市场争夺焦点。若无法留住顶尖人才，他们终将为他人所用。

即便精锐团队也可能难以独自承受攻击带来的管理高压，因此需提前规划外部支援：

评估第三方资源
网络安全咨询与人员扩充服务商，可在日常运营与突发事件期间为团队提供助力。即便当前暂无需求，也应提前与这些公司建立关系，确保紧急时刻能快速调用资源。

戴尔提供虚拟首席信息安全官 (vCISO)、事件响应及网络安全咨询等一系列服务，可与现有团队相辅相成。

利用 AI
利用网络安全工具中内置的全新 AI 功能 — 包括日志分析、异常检测、低级别警报分诊或专项训练等，既能弥补资源缺口、满足运营需求，又可解放团队成员，使其专注于更高优先级的任务。

网络攻击期间，资源挑战最严峻

正如开篇场景所示，重大网络攻击可能使贵组织陷入瘫痪 — 核心系统停摆，业务运营中断。每分钟都在造成经济损失，安全团队承受着解决问题的巨大压力。

确保团队始终保持最新知识储备，将直接影响事件响应效率并有效缓解团队压力。

请记住，安全培训必须扩展到全体员工而不仅仅局限于专业安全人员，因为他们才是防御的第一道防线。

这个案例揭示了一个核心挑战：防御者终究是人类。人类存在能力上限，当突破这些极限时，即使是最精锐的专业人士也会失误。精神疲劳、压力和倦怠如今已成为影响网络安全态势的关键因素。

虽然没有单一的解决方案可以应对这一挑战，但以下战略可显著改善局面：

建立强大的团队和人才管道
解决这个问题的根本方法是防患于未然 — 建立具备人员冗余的强大团队。

针对攻击的人为方面进行规划
事件响应计划至关重要，且必须包括人员管理、安排和员工调休计划。

利用第三方资源
外部网络安全顾问能够与您的团队相辅相成。以戴尔的事件响应服务为例，专家团队可在数小时内抵达现场 — 随时开展评估、遏制并立即开始补救。我们已助力众多客户成功抵御网络攻击。

AI 可以提供助力，但却并非万能的解决方案

AI 为增强网络安全工具和计划带来了巨大的前景。从预测性分析到开发量身定制的培训计划，再到在威胁蔓延之前主动应对威胁，它的功能最终将全方位发挥作用。

或许更重要的是，AI 可以在事件期间为防御者提供实时支持系统。基于历史攻击数据训练的机器学习模型，可参照类似事件推荐操作方案。

伴随着自然语言处理技术在网络安全工具中的应用，分析师将能够直接与系统交互、识别威胁并部署解决方案。

AI 还可以监控行为模式，当分析人员因疲惫等原因反复出现失误时及时发出警示 — 提示轮岗或引入新视角。

尽管网络安全工具正在快速集成更复杂的 AI 工具，但许多强大的功能仍在开发阶段。截至目前，AI 尚无法替代经验丰富的从业人员的技能，**尤其是具备实战攻击经验的**从业人员。

利用 AI 的建议：

了解这些工具如何帮助您实现安全运营
详细分析 AI 工具，并在有效环节部署实施。可快速见效的领域包括：高级威胁检测、重复任务自动化，以及身份管理中的 AI 应用。

规划 AI 的未来
了解新功能何时可用，它们将如何让您的团队受益，并制定实施计划。

将 AI 融入员工队伍规划
由于自动化减少了手动任务，您的安全团队的组成可能需要发生变化。您可能需要更高级别的资源来分析和处理安全信息，而不是编译安全信息。请相应地调整您的招聘和培养战略。

AI 必将（或已经）成为网络安全运营的重要组成部分。但请记住，没有任何东西可以取代一个技能熟练、经验丰富的从业人员。AI 的目标应该是使用 AI 来实现运营自动化并提高人力资源的效率，最终防止攻击并尽可能减少攻击发生时的影响。

循序渐进提升网络安全成熟度

正如网络安全领域的其他工作，人员因素管理是持续演进的过程而非终点。渐进式的改进，哪怕是微小进步，经年累月也能产生质变。必须始终牢记：即便最尖端的技术和安全工具，其效能上限始终取决于操作者水平。

> “与合作伙伴签订常驻服务协议，由其负责事件响应、补救及恢复，是行业最佳实践。”
>
> **Jason Rosselot**
> Dell Technologies 网络安全和业务部门安全官副总裁

戴尔产品和解决方案，可以助您一臂之力

精选戴尔解决方案	说明
事件响应服务	行业认证的网络安全专家团队随时待命，在发生网络攻击时快速做出响应。在恢复正常运营之前，我们将与您并肩合作，直至全面消除威胁。
网络安全咨询服务	提供专家指导，可帮助您发现和解决安全战略中的盲点、保护您的资产和数据，并实现持续的警惕和治理。
vCISO	虚拟首席信息安全官和网络安全专家，可协助识别和管理风险，并指导战略决策。
管理检测和响应	通过提供跨端点、网络和云的监控、威胁检测、调查和快速响应，该系统减少了手动工作量并简化了日常安全运营。客户选择首选的 XDR 平台（Secureworks® Taegis™ XDR、CrowdStrike Falcon® XDR 或 Microsoft Defender XDR），并获得专家指导、季度报告以及长达 40 小时的年度事件响应时间。

了解如何应对当今一些主要的网络安全挑战：**dell.com/cybersecuritymonth**

DELL Technologies