DELL Technologies

提升网络安全和零信任成熟度

不要让安全风险扼杀创新

了解您的网络安全现状

了解需要达成的目标

在当今错综复杂且瞬息万变的威胁形势下，组织期望持续推行强有力的网络安全实践，却常常在资源和专业知识方面受限。提升网络安全和零信任成熟度对于应对不断变化的网络威胁至关重要，可确保环境安全无虞，同时又不会扼杀创新。

不妨使用以下核对表评估网络安全成熟度，以了解当前状态。通过了解贵组织的优势和劣势，您就能采取正确的后续举措，从而提高网络安全成熟度。

目录

了解详情

详细了解如何提升网络安全和零信任成熟度

核对表：

减小受攻击面

受攻击面是指环境中可被网络攻击者攻击或利用的所有可能点或区域。这些点可能包括软件漏洞、配置错误、身份验证机制薄弱、系统未修补、用户权限过多、开放式网络端口、物理安全性较差，等等。以下问题可帮助您确定如何尽可以减少恶意行为者入侵可能利用的漏洞和入口。

是	否	
☐	☐	贵组织是否会定期进行评估、渗透测试或漏洞攻击模拟，以确定系统和网络中存在的漏洞和薄弱环节，从而及时进行修正和改进？
☐	☐	贵组织是否会定期对员工进行安全培训？
☐	☐	贵组织是否使用多因素身份验证 (MFA) 和基于角色的访问控制 (RBAC)？
☐	☐	贵组织是否实施了网络分段来隔离关键资产并限制网络不同部分之间的访问？
☐	☐	贵组织是否实施安全编码实践、定期进行安全测试和代码审查，并使用 Web 应用程序防火墙 (WAF) 来帮助保护防范常见的应用程序级攻击，同时减少 Web 应用程序的受攻击面？
☐	☐	贵组织是否会选择能证明其流程和程序可确保供应链安全的 IT 供应商？
☐	☐	贵组织是否正在实施零信任原则，以取代传统的基于边界的安全措施？
☐	☐	贵组织是否会利用最低权限原则来对用户和系统帐户加以限制，使其仅具有执行相应任务所需的最低访问权限？
☐	☐	贵组织是否会定期修补您的系统和软件？
☐	☐	贵组织的安全工具是否利用 AI/ML 功能来帮助您主动识别漏洞？

核对表：

检测和响应威胁

检测和响应网络威胁是任何安全战略的重要一环。这包括监视和分析网络流量、系统日志和其他方面以及安全数据，以识别未经授权的访问、入侵、恶意软件感染、数据泄露或其他网络威胁的迹象。以下问题可帮助您确定贵组织如何主动识别并积极解决计算机网络、系统或组织内潜在的安全事件和恶意活动。

是	否	
☐	☐	贵组织是否使用安全工具和技术（扩展检测和响应 [XDR]、入侵检测系统 [IDS]、入侵防御系统 [IPS]、SIEM 和日志分析）持续监视网络和系统活动？
☐	☐	贵组织是否会分析收集的数据，以识别可能表明存在潜在网络威胁的模式、异常情况以及入侵指标 (IoC) 和/或攻击指标 (IOA)？
☐	☐	贵组织是否部署了全新可见性和监视工具，以快速检测潜在威胁并发出警报？
☐	☐	贵组织是否会监视网络流量，以发现可能表明正在发生网络攻击的异常模式或可疑活动？
☐	☐	贵组织是否实施了任何 AI/ML 工具，助您实时分析异常数据模式或行为来检测网络威胁？
☐	☐	贵组织是否考虑过实施下一代 SIEM 解决方案，以便更好地管理安全警报并开始将整个 IT 生态系统中的安全事件数据关联起来？
☐	☐	贵组织是否会进行漏洞测试和管理来确定现有漏洞的优先级并解决这些漏洞，同时高效地响应新漏洞？
☐	☐	贵组织是否制定了事件响应计划来调查和缓解已确认的安全事件？
☐	☐	贵组织是否采用安全编排、自动化和响应 (SOAR) 工具来加快事件响应操作，助力减少网络攻击的蔓延？
☐	☐	贵组织的事件响应计划是否考虑到了遏制策略、沟通计划、合规性要求、取证分析和恢复流程？

核对表：

从网络攻击中恢复

从网络攻击中恢复是指在安全事件发生后，将受影响的系统、网络和数据还原到安全且可运行状态的过程。这包括采取措施减轻攻击造成的损害、重建遭到入侵或中断的服务和设备、分析事件以防范未来攻击，并恢复组织的正常运营。以下问题可帮助您确定贵组织是否会有效地从网络攻击中恢复。

是	否	
☐	☐	贵组织是否实施了任何事件遏制措施来隔离和遏制网络攻击？
☐	☐	在事件得到遏制后，贵组织是否制定了系统和/或设备还原流程？
☐	☐	贵组织是否利用数据隔离、不可变性或网络存储区来保护您的数据？
☐	☐	贵组织是否建立了在数据受损、进行加密或遭到删除时干净地恢复数据的程序？
☐	☐	贵组织是否借助 AI/ML 技术自动或加速从网络攻击中恢复？
☐	☐	在遭受攻击并进行恢复后，贵组织是否会持续评估事件并确定需要改进的领域？
☐	☐	贵组织是否进行了取证分析，以便了解攻击方法、确定泄露程度、识别受影响的系统和数据并收集证据，助力提升安全性并追究法律责任或进行纪律处分？
☐	☐	贵组织是否知道要告知相关方（例如客户、合作伙伴和供应商）发生的网络攻击以及对其数据或运营造成的任何潜在影响？
☐	☐	贵组织是否每年会多次演练恢复策略，以增强恢复业务的信心并满足 SLA 要求？
☐	☐	贵组织是否与服务提供商合作来协助贵组织进行恢复？

提升网络安全和零信任成熟度

为提升网络安全，IT 组织必须为最坏的情况做好应对计划并建立多层防御，这一点至关重要。在不断变化的网络安全威胁形势下，持续推进安全实践并采用零信任原则至关重要。这包括：

减小受攻击面

尽可能减少可能被用于侵入环境的漏洞和入口。

检测和响应网络威胁

主动识别并解决潜在的安全事件和恶意活动。

从网络攻击中恢复

在发生安全事件后，将企业恢复到之前已知的安全运营状态。

戴尔可助力组织利用专业服务提供商的专业知识并与值得信赖的业务合作伙伴开展合作，从而建立全面的安全态势，以防范不断变化的网络威胁。随着技术的不断进步，我们的网络安全方法也必须与时俱进，以保护我们的数字基础架构，维护数字领域的信任。

DELL Technologies

关于 Dell Technologies

Dell Technologies 帮助组织和个人打造数字未来，实现工作、生活和娱乐方式的转变。我公司为客户提供业界较为全面，而且具有创新意义的技术和服务产品组合，让他们为数据时代做好准备。

更多详情，请访问 www.dell.com/securitysolutions