从网络攻击中恢复

事件发生后有效且高效地恢复运营。

一个全面的安全恢复战略包括以下环节

减轻攻击的影响 → 重建受损的服务和设备 → 恢复运营 → 分析事件，吸取教训

通过以下步骤提高网络安全成熟度

1. **控制事件发展态势**
   断开受影响的系统与网络的连接，禁用受感染的帐户并阻止进一步的损害。
2. **恢复系统/设备**
   重建受损系统、重新安装软件并应用安全修补程序和更新。
3. **数据恢复**
   从备份中恢复数据或使用专门的数据恢复技术来检索丢失或加密的文件。
4. **取证分析**
   检查攻击机制和被利用的漏洞，防止今后发生类似事件。
5. **事件响应评估**
   恢复后，评估流程以确定需要改进的方面。
6. **利用 AI/ML**
   通过快速识别受影响的系统和数据并自动执行备份恢复过程来加速恢复。

网络恢复要靠团队协作才能实现。

专业服务与合作关系

网络安全合作伙伴提供宝贵的专业知识和资源：

- 取证分析
- 明确造成漏洞的原因
- 制定措施，避免今后发生类似的事件

了解有关实施全面网络安全战略的更多信息。

浏览电子书 →

DELL Technologies