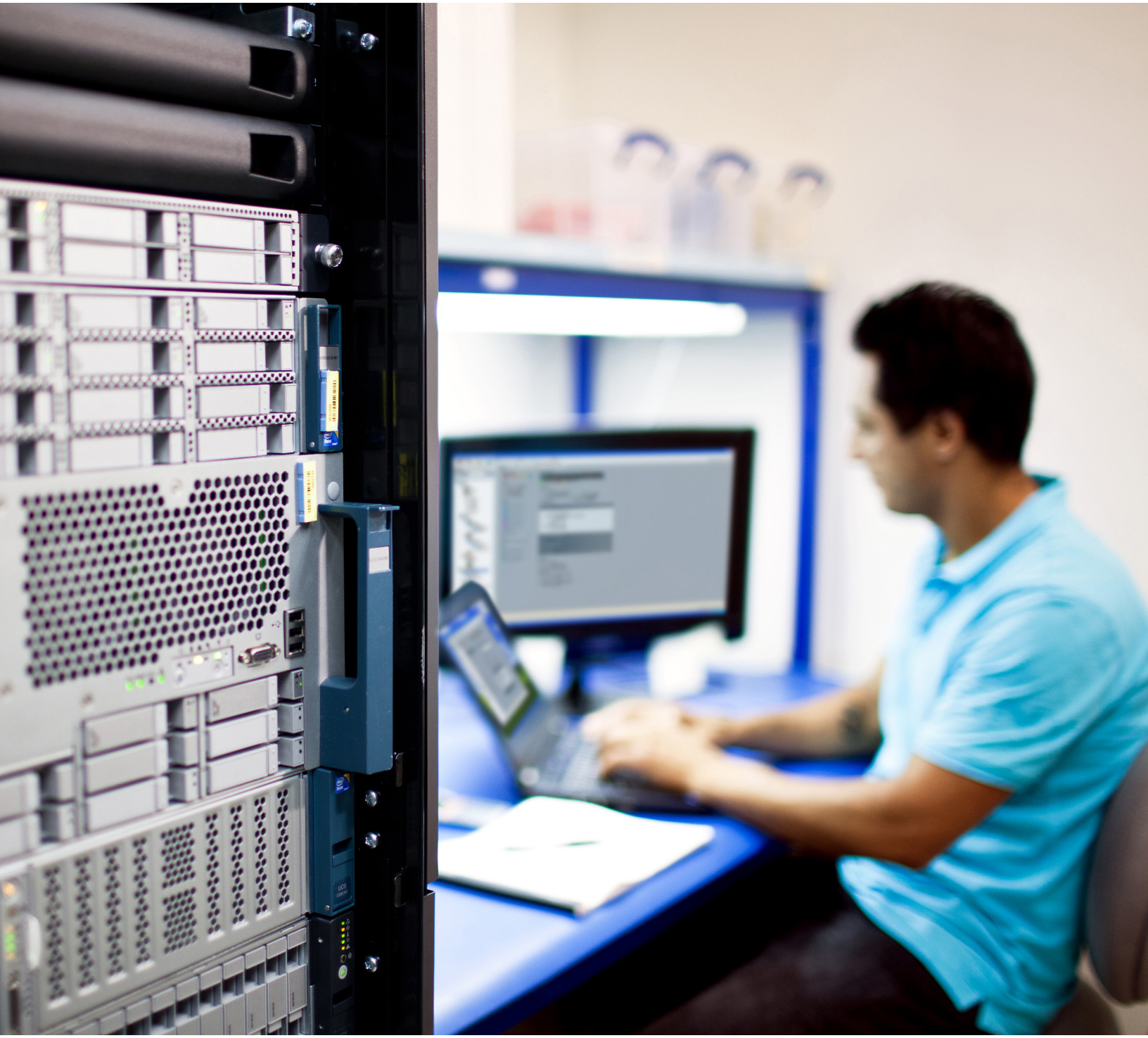
七种可疑活动类型：网络可视性要点总结



您知道您的网络已经受到侵害。您应该如何应对?

解决这一问题的关键在于网络可视性。网络可视性功能可让您深入了解攻击者在您环境中的行为和位置，帮助防止安全事件演变为大范围的数据泄露。

我们利用自己的高级可视性工具，对数百家组织的网络进行了评估。评估中，我们发现了许多令人担忧的问题，从使用定制恶意软件窃取数据，到利用受感染的服务器攻击政府网络，网络威胁可谓无处不在。

此要点总结列出每一安全团队需要有能力了解的七种最常见类型的网络盲点和可疑活动。如果无法有效检测这些活动，就意味着威胁将能够藏匿在您的网络中不被发现。

未经授权的 DNS 使用

组织使用 DNS 实施策略并保护用户免受恶意网站侵害。但是，使用未经批准的 DNS 服务器可能是恶意活动或违反策略行为的迹象。将近 92% 的恶意软件在攻击中使用 DNS[1]，并且在我们评估的组织中，超过 70% 在其网络中存在未经授权的 DNS 使用。

欺诈服务器活动

欺诈服务器是指不受组织管理员控制的服务器，它们会对安全构成严重威胁。无论是由善意员工或者由威胁发起者设置，这些服务器均允许威胁在网络中持续存在，并窃取敏感数据。

服务器消息块风险

服务器消息块 (SMB) 协议在许多组织中使用，并且攻击者利用它掩盖恶意活动。具有破坏性的定向恶意软件（例如 Conficker）还会利用 SMB 部署代理工具、安装后门、破坏数据，并导致服务器离线。

涉及可疑国家/地区的流量

大多数组织的业务范围仅限于特定地理区域。识别来自这些区域以外的流量是检测威胁的有效方式。如果一家美国西部的公共设施提供商有大量流量来自东欧或亚洲，则可能是威胁活动的迹象。

远程访问漏洞

远程访问是大多数组织中的常见做法，但是，攻击者也会将其作为一种获取企业网络特权访问的方式。通过检测远程访问用户中的异常或可疑行为，可识别被盗访问证书或内部威胁的情况。

Telnet 活动

Telnet 是一种不安全的旧协议，传输未加密数据，这让攻击者可以拦截未加密数据，从而获取密码和其他敏感信息。大多数组织认为他们没有使用此协议，但是我们的评估发现，67% 的组织在其网络中存在 Telnet 活动。

其他异常行为

高级威胁能够快速变化和适应以逃避检测，而且许多威胁依靠窃取合法证书来避开防御。对于已知的恶意行为或明显异常的行为，监控其网络活动可帮助安全操作人员检测最高级的威胁活动。

相关详细信息

有关网络可视性的更多信息，请阅读我们白皮书《解决可视性缺口》。

[1] 《思科 2016 年度安全报告》

C11-737513-01 03/17