网络安全检查清单

主动防御的 57 个建议

保护您的企业安全是一段旅程，而非目的地

您负责决定在何处集中实施防御措施。可能无法阻止违规行为，但可在违规发生前做好充分准备。通过立即采取行动，您可以确保企业不易成为威胁攻击者的目标，并且限制攻击者在您的网络中进行传播的能力，从而在发生网络攻击时最大限度地减少损失。您需要提前确定企业必须采取哪些措施来消除威胁、恢复正常运营及从攻击中恢复。

以下建议基于实时事件响应案例，并根据我们的 2022 年 Unit 42 事件响应报告进行总结。这些内容分为几个部分，助您集中精力进行查看，并为您的安全计划提高灵活性。

全面建议，提升企业安全性

身份和访问管理 (IAM)

- 尽可能将单点登录 (SSO) 平台用于 Web 应用和多因素身份验证 (MFA)。
- 定期审核 Active Directory 中新创建的帐户、邮箱和无法识别的组策略对象。
- 配置服务器以阻止未经授权的访问和目录列表。实施强有力的访问控制。
- 如果员工被解雇，应迅速采取行动撤销其访问权限（例如，活动会话、令牌、帐户、MFA 设备和轮换凭据），然后验证访问权限是否已被撤销。确保保存员工的系统和数据，以备调查之需。
- 限制特权帐户的使用，仅在有效业务需要时使用，或者用户需要特权帐户来完成其工作任务时，并且不重复使用本地管理员帐户密码。
- 如果相关人员的工作内容无需使用管理界面和调试工具，为其禁用。

7 个最有可能遭受攻击的行业

为金融业、专业法律服务、制造业、医疗保健业、高科技行业以及批发和零售业。

风险、漏洞和修补程序管理

- 确定企业的关键资产和最有价值的资产。其中包括对关键资产进行清点，以了解您的价值最高的目标，以及这些目标是否需要更多保护措施。
- 实施开源代码时进行研究，了解代码是否存在任何已公布的漏洞，且仅使用经过审查和修补的代码。
- 对所有面向公众的基础架构进行定期网络应用/代码审查和年度渗透测试，寻找漏洞，并遵循补救建议。
- 在您的开发环境中根据最佳实践配置安全设置。
- 进行定期扫描，包括配置检查，并定期进行系统审核，以发现错误配置。
- 实施变更控制协议，要求对配置变更进行审查和确认。
- 修补程序管理对操作系统和本地应用至关重要，APT 攻击者将非常迅速地利用漏洞。在尽职调查允许的情况下尽快解决新发布的漏洞。

数据和软件安全

- 了解敏感数据的位置，并实施强力的访问控制来保护这些数据，并定期监控及审核访问权限。限制敏感数据的访问权限，仅限于企业内有需要的人员和第三方。
- 对笔记本电脑和可移动设备实行全磁盘加密。制定应急计划来禁用丢失或被盗的设备。
- 实施及利用能够定位和/或远程擦除设备的移动设备管理应用。
- 建立 DLP 程序，负责对数据进行分类和标记，并在敏感信息或其他公司确定的相关信息脱离企业管控时发出警报。

威胁检测和响应

- 考虑使用凭据入侵检测服务和/或攻击面管理解决方案，以帮助跟踪易受攻击的系统和潜在入侵行为。
- 充分利用 EDR 或 XDR 解决方案，并确保您的安全运营团队了解如何利用该技术来保持整个网络的全面可视性。
- 制定事件响应和补救计划。即使付出了最大努力，仍可能发生事件，因此要有一个经过测试的全面计划，确保事件发生时快速采取行动。如果您有网络保险（推荐），请确保将保单的关键流程和联系人整合到计划中。

其他建议

- 维护日志保留存储库，并定期检查所有日志和登录尝试，以发现异常的行为模式。确保将日志存储适当时间，履行所有法律或法规义务。Unit 42 顾问人员建议保留一年及以上，如果不可能，至少保留 90 天。

- 利用日志聚合系统（如安全信息和事件管理 (SIEM) 系统）来提高日志保留率、完整性和可用性。
- 每年定期对承包商等所有用户进行安全意识培训。考虑使用值得信赖的培训平台，助您将为用户量身定制的目标整合到培训课程中。
- 避免使用平面网络。隔离网络和 Active Directory，细分敏感数据，并利用安全的虚拟局域网 (VLAN)。
- 采用深度防御方法，在 Web 应用堆栈的每一层实施安全措施。这可能包括 Web 应用防火墙、操作系统强化、应用输入控制、文件完整性监控以及用于数据库访问和行业标准加密的最低访问权限用户帐户。
- 为员工提供合法经营业务的方法，仅仅阻止某些载体可能会导致错过明智的解决方法。
- 考虑根据常见拼写错误或企业名称的变体购买域名。这会使威胁攻击者更难入侵您的企业。

77% 的入侵可能由三种初始访问载体导致：网络钓鱼、已知软件漏洞利用和暴力凭据攻击，这些入侵主要集中在远程桌面协议 (RDP) 上。

阻止网络钓鱼攻击的建议

- ☐ 打造“安全意识文化”。公司领导层必须意识到网络安全和支持的重要性，推广更多网络培训计划，并重视公司通信的安全性。
- ☐ 利用值得信赖的培训供应商或平台，根据企业和员工职位定制课程，并考虑威胁攻击者采用的方法具有快速变化的特点。
- ☐ 帮助用户轻松举报可疑的钓鱼邮件，确保举报得到及时审查，并对此类信息采取行动。
- ☐ 利用视觉元素提醒用户注意来自外部发件人的附件。这可能有助于识别与公司网域相似的假冒网域。
- ☐ 开发完善的培训课程，包括网络钓鱼和鱼叉式网络钓鱼及更多内容。涵盖其他社交工程问题，包括物理安全、防止设备丢失的行业最佳实践、内部威胁指标等。
- ☐ 为单个小组量身定制基于 Web 的模块，这些模块与小组角色及其可能遭遇攻击的方式息息相关，帮助员工轻松发现和避免可能针对他们的攻击策略。
- ☐ 每年为所有员工举行全面培训，并在年中进行基于特定重点领域（如先进技术）的“培训内容更新”。
- ☐ 设定目标、实现目标所需的规则、奖励或激励、反馈机制和排行榜，以此增加安全培训的趣味性，吸引员工。企业之间可以互相竞争。
- ☐ 跟踪网络钓鱼测试的领先性能指标，以便根据企业需求调整网络钓鱼的内容和难度。
- ☐ 鼓励用户通过与基于角色的访问控制分享的文件而非电子邮件来存储敏感信息。

- ☐ 充分利用可扫描附件、邮件内容以及评估发件人信誉的电子邮件安全解决方案。
- ☐ 使用反欺骗和电子邮件身份验证技术，如发件人策略框架 (SPF)。
- ☐ 如果正常业务运营不需要，可根据地理位置阻止帐户登录。
- ☐ 采用高级网络钓鱼防护/机器学习解决方案或其他第三方解决方案来检测和阻止复杂的网络钓鱼活动。考虑实现网络钓鱼响应活动自动化，减少所需人工。

有助于企业系统保持最新的修补建议

- ☐ 通过自动化发现工具清点整个分布式企业的所有 IT 资产（包括存储、交换机、笔记本电脑等），清晰了解您必须管理的内容。
- ☐ 优先考虑您的修补需求。根据企业的风险承受能力确定哪些漏洞代表高、中或低风险，以及这些漏洞的业务优先级。
- ☐ 定期制定部署修补程序的计划。最大限度减少修补频率，如每月一次，必要时可以选择不定期部署高优先级补丁。
- ☐ 在开发质检环境中测试您的补丁，以确保一旦部署到生产环境中，这些补丁不会“破坏系统”。
- ☐ 部署补丁后，监控其稳定性。这可能还包括监控网络稳定性。
- ☐ 删除在不受支持的操作系统上运行的系统。

65% 的已知云安全事件是由于错误配置造成的。

保护云环境安全的建议

- ☐ 定期评估哪些数据可以在面向公众的互联网上访问或公开。
- ☐ 考虑采用攻击面管理解决方案来帮助跟踪易受攻击的系统和未托管云资产。
- ☐ 充分利用每个平台的云安全专业知识。管理云环境的安全性需要可满足每个平台细微差别的专业知识。平台越复杂，可能无意中泄露数据的机会就越多。
- ☐ 确保拥有云控制访问权限的用户在每个云环境中都已经过全面培训。
- ☐ 如果您没有内部专业知识，或者如果您的云资产特别复杂且处于持续变化的状态，请评估您的托管安全服务选项。
- ☐ 控制对云环境的访问权限。云中的 CSP 控制台、API 和 CLI 等云控件的访问权限应该仅限于所需之人。这种 RBAC 对于最大限度降低配置和其他安全错误的风险而言至关重要。

- ☐ 将管理凭据和用户凭据分开，并将日常用户限制在生产环境中。
- ☐ 尽可能实施允许列表，从而进一步限制对已知和受信任端点的访问。
- ☐ 定期审核您的云数据，以了解您拥有哪些敏感数据以及这些数据的位置。
- ☐ 加密敏感数据（基本操作）并对其进行细分，使用 RBAC 提供访问权限并定期轮换密钥。评估与云提供商共同维护密钥以及在您的企业内单独维护密钥这两种方案，确定最佳选择，但要确保您有密钥安全策略来限制密钥访问和风险暴露。

使用 Cortex 支持安全操作

众所周知，安全运营会在运行过程中在人员、流程和技术之间取得微调平衡。为此，我们想向您介绍一整套专为 SOC 设计的安全解决方案。

Cortex 产品组合提供端到端安全解决方案，帮助您提高整个安全运营的检测和运营效率。这些技术为我们的 Palo Alto Networks SOC 和全球数千个 SecOps 提供支持。

Cortex XDR 提供领先的端点保护，并在网络、云、端点和几乎任何数据源中提供企业级威胁检测和响应，帮助您的企业抵御攻击。获得专利的行为和机器学习分析可精确定位规避性威胁，并提供您需要的情报，以便在入侵发生之前做出响应。不要等到攻击发生后才把这些内容进行联系，违规行为发生*之前*就阻断。

Cortex XSOAR 为您的 SOC 提供一个可管理事件和自动化工作流程的平台，助您实现最高的运营效率。检查清单中列出的任何手动和重复流程都可以实现自动化。借助为用户访问控制、网络钓鱼响应、漏洞管理、云安全等关键流程提供的 900 多个预构建自动化包，XSOAR 可以充当您在 SOC 中的虚拟合作伙伴，以加快事件响应速度并减轻分析师的日常工作负载。

Cortex Xpanse 了解您的云环境在不断变化，并暴露出安全漏洞。攻击者只需一个漏洞就能入侵您的网络。Xpanse 可持续监控您的攻击面，为您提供面向互联网的云资产和错误配置的最新清单。在攻击者之前发现影子 IT。

通过端到端的原生集成和互操作性，SOC 团队可以通过整个 Cortex 生态系统的持续协同作用来结束威胁。所有三种产品协同工作，以监控威胁情况，并提供最强大的检测、响应和调查能力：

- Cortex XDR 和 Cortex Xpanse 为包括远程员工在内的互联网攻击面、端点、云和网络提供最佳可视性和检测。
- Cortex XDR 可以利用 XSOAR 来自动化恶意软件调查和响应。
- Cortex Xpanse 和 XSOAR 协同工作，利用 Xpanse 资产信息自动丰富事件，并自动修复新发现的资产。
- Cortex XSOAR 通过所有 Palo Alto Networks 产品和数百种其他安全工具获取警报和威胁情报，以促进事件调查并推动自动化事件响应。

使用 Unit 42 MDR 全天候检测和响应网络攻击

Unit 42 安全专家运用他们多年来保护企业安全的经验来监控您的环境并寻找可疑活动。我们的分析师利用 Cortex XDR 整合来自端点、网络和云的安全遥测数据并识别来源，然后利用高精度威胁情报和人工智能分析来预防、检测及响应最高级的威胁。

Unit 42 MDR 团队搭配使用专属流程、基础架构和升级功能，通过加速检测、响应和威胁搜寻快速阻止可能影响您企业的恶意活动。

在 Unit 42 顾问人员的帮助下快速响应

在发现违规行为时，时钟会立即开始计时。如果您不立即遏制违规并确定根本原因，攻击者将再次回到您的环境中。

在 Unit 42 顾问人员的帮助下，您可以将快速拨号设置为我们的专家，使其成为您团队的辅助力量，助您快速响应，以便最大限度地减少攻击的影响，并快速恢复业务。

下一步怎么做？XSIAM 的发展前景

尽管 Cortex 产品满足了 SOC 对可视性、保护和自动化的主要要求，但大多数企业仍然将 SIEM 作为 SecOps 的核心组件。但 SIEM 产品无法提供有效的集中威胁检测和响应，导致分析师需要处理大量警报并采取手动操作。安全团队需要集中式平台，此平台可将多个安全功能集成并自动化到一个基础解决方案中，同时具备对企业级安全数据的可视性。

扩展安全情报和自动化管理 (XSIAM) 专为满足这一需求而设计，利用人工智能驱动的自动化的力量从根本上改善安全结果，并改变手动 SecOps 模式。通过构建智能数据基础并自动化统一的 SOC 功能，XSIAM 加快了响应速度、在威胁发生之前采取行动，并显著简化了分析师的活动。

有关 Cortex 产品套件如何提供一流的威胁检测、防御、攻击面管理和安全自动化功能的更多信息，请下载我们的白皮书：

使用 Cortex 构建虚拟 SOC 平台

如何在今天规划未来的 SOC

查看 Unit 42 2022 事件响应报告，深入了解当今的网络威胁形势，以及威胁攻击者最喜欢使用的策略。

paloalto NETWORKS

免费咨询热线：400 9911 194
网址：www.paloaltonetworks.cn
邮箱：contact_salesAPAC@paloaltonetworks.com

© 2022 Palo Alto Networks, Inc. Palo Alto Networks 是 Palo Alto Networks 的注册商标。本公司的商标列表可在以下网址找到：https://www.paloaltonetworks.com/company/trademarks.html。此文档中提及的所有其他商标可能是各相应公司的商标。
unit42_cybersecurity-checklist-57-tips_112222