KPMG

智能安全运营体系

毕马威网络安全

毕马威中国

kpmg.com/cn

日益严峻的安全形势

威胁形势在不断变化

全球数字犯罪估计为4500亿美元/年，网络威胁的影响也在不断扩大。如今，高度依赖信息化的组织正面临着双重挑战：越来越严重、复杂的网络安全攻击，以及新技术带来的安全风险。各组织积极应对以上挑战，在部署防火墙、防病毒、IPS\IDS、WAF、堡垒机的基础上，同时新增新一代检测安全设备（情报、流量分析、沙箱、EDR、蜜罐等），但是通过调查发现，不同成熟度的组织仍面临以下一个或多个问题：

- 如何建设一个有效的智能安全运营中心 / 体系，提升全局可视化和威胁响应效率，而不仅仅是设备堆砌
- 各安全检测设备可能为组织提供了一流的技术，但是各安全检测设备的独立运营将为组织在面临安全威胁时的细节实时拼凑和调查分析带来极大困难
- 统一收集和汇总各安全设备后，出现告警增多、重复和误报现象，如何持续优化告警，提升分析和处置效率
- 自主构建与组织自身的安全环境、安全资产相关的威胁框架检测模型，可独立于平台且持续动态更新
- 如何构建有效的 SOAR 平台，实现安全分析、安全响应和安全处置的全过程自动化，而不仅仅是封堵 IP

安全合规已上升至国家法律层面，并将带来严重经济损失

自 2017 年 6 月 1 日，《中华人民共和国网络安全法》施行以来，各相关部委、行业均更新或发布了相关标准要求，如《信息系统安全等级保护 2.0》、《个人信息安全规范》等。同时加大了安全检查“力度”和“粒度”，在去年全国性的安全检查中，统计被攻陷的组织的大多数原因仍为合规控制问题，如 VPN\ 邮箱弱口令、网站代码执行漏洞未整改、互联网资产未梳理、堡垒机等安全设备未符合安全控制要求等。因此，即使近几年各组织均建立了自身安全管理体系，但安全合规作为整个安全体系的基石，仍面临如下挑战：

- 各组织对自身攻击面缺少全面了解
- 被动检查，无法实时并主动监测，且控制措施有效性无法量化
- 安全合规检查停留在基线检查层面，缺少全局的安全合规态势展示
- 各安全管理要求众多，无法有效整合和实施检查
- 安全资产多且架构复杂，无法保证检查的全面覆盖
- 更多依靠人员检查，存在舞弊和低效率的情况

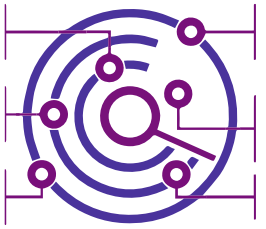
组织的安全运营能力需持续适应最新安全形势

未来的安全运营

安全运营需要超越传统的被动响应，借助数字化转型的机会，利用大数据、机器学习和自动化等技术来应对所面临的挑战，实现主动并持续监测，但仍要记住SOC不仅仅是技术，需要人员、技术和流程的协同运作。

标准化

明确SOC衡量指标，做好分类、分级与流程标准化，以一致的方式覆盖整个组织，以确保避免盲点，并持续优化，与安全形势一致。



KPMG- 未来安全运营的六大关键能力

风险导向

威胁模型建立与持续跟进，同时为适用于您组织的威胁提供有效的检测能力，利用威胁情报、资产、漏洞实时、动态确定风险的优先级并决定您应如何应对。

智能

使用开放的体系结构、灵活和自适应的分析工具，使组织能够根据实时的洞察力做出有效、快速的决策。

自动化

将安全运营全过程操作形成标准操作手册，利用SOAR（安全协调、自动化和响应）工具将其固化，加快响应速度，提高生产力，并允许您的团队将注意力集中在真正重要的地方。

敏捷

能够快速应对外部安全形势的变化，组织变化、IT/安全环境变化，以及攻击面快速转移，内、外部IOC的闭环更新与衔接。

数字化整合

数字平台支撑安全威胁、安全合规和业务安全三大场景，实现业务整合，整合网络检测和响应能力，并确定协同效应。

无论投资多少，组织都无法一夜间完成期望的或符合自身需求的安全运营中心/体系，所以这项任务更像一场马拉松，而不是五十米冲刺。基于自身需求的差距分析，制定增量计划，明确一系列的里程碑目标是成功的关键，可引导组织实现优化的安全分析、响应和处置。一旦确认需求和目标，更重要的是要认识到构建一个SOC 需要多功能的团队或人员,不同的安全设备或系统，以及不通的流程之间的协作和通信。

来自：2015年SANS发布的《构建世界级 SOC 的路径》

© 2020毕马威华振会计师事务所(特殊普通合伙) — 中国合伙制会计师事务所及毕马威企业咨询 (中国) 有限公司 — 中国有限责任公司，均是与英国私营担保有限公司 — 毕马威国际有限公司(“毕马威国际”)相关联的独立成员所全球性组织中的成员。版权所有，不得转载。在中国印刷。

KPMG 安全运营服务

我们能协助您：

我们能为您带来：

计划

我们可以规划您的安全运营目标、运营模式，协助您建设与组织总体安全目标相一致的安全运营能力

以风险为导向，建立一个强大的安全运营能力可保护您持续免受特定威胁，并满足合规要求

第一次就把能力建设做好，最大限度地提高你的安全运营投资

评估

我们可以基于网安法、等级保护、个人信息、安全管理中心等要求对组织的 SOC 进行差距分析；我们可以基于国际 \ 国内最佳实践对组织的 SOC 进行成熟度评估

了解与法律、法规的差距，识别改进点；

了解 SOC 安全运营成熟度，以有效地提高你的能力，

设计/优化

我们可以设计以 SIEM 为安全大脑的安全运营功能框架，有效协调各安全系统与设备；

我们可以设计匹配客户环境的威胁框架模型、互联网威胁、内网威胁、安全合规、信息泄露等场景，

我们可以设计基于规则的操作手册和自动化需求，以及风险自动评价模型

自主可控的威胁监测模型，可持续保持最新威胁的更新；

用户案例详细分析检测方法；

以标准化的风险评级模型，安全操作流程和适用的用户案例为基础，建立有效的安全运营功能；

合规场景预检模型，可持续保持等级保护 2.0、ISO 27001、个人信息规范等合规要求的总体合规计算展示、自动化检查；

运营

我们可以按照客户需求提供驻场或非驻场的漏洞管理、安全威胁监测与分析、威胁情报管理、调查取证等安全运营服务

我们可以通过部署工具为客户提供智能安全合规订阅服务，自动或半自动化的提供合规预检查、自评估的态势展示、报告和实时监测

客户期望的安全运营服务，包括安全监控（一线 / 二线），取证分析，漏洞管理、情报分析，案例运营；

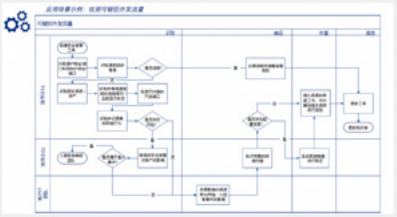
客户期望的智能安全合规订阅服务；

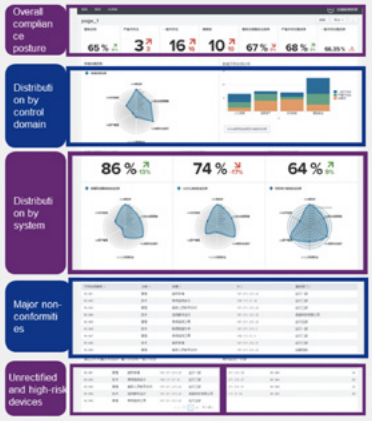
快速的交付：熟悉国际、国内 SIEM，安全漏洞、网络流量分析、威胁情报等商业或开源工具；

SOC 能力模型

SOC 成熟度评估

Playbook 与SOAR需求





基于ATT&CK & Kill chain 威胁框架与用户案例设计

协助您完成安全的数字化转型，主动防御，持续监控，快速并有效的响应与处置，为业务保驾护航！

© 2020毕马威华振会计师事务所(特殊普通合伙) — 中国合伙制会计师事务所及毕马威企业咨询 (中国) 有限公司 — 中国有限责任公司，均是与英国私营担保有限公司 — 毕马威国际有限公司(“毕马威国际”)相关联的独立成员所全球性组织中的成员。版权所有，不得转载。在中国印刷。

联系我们

石浩然
毕马威中国
网络与信息安全咨询
合伙人
Tel: +852 2143 8799
henry.shek@kpmg.com

张令琪
毕马威中国
网络与信息安全咨询
合伙人
Tel: +86 (21) 2212 3637
richard.zhang@kpmg.com

黄芃芃
毕马威中国
网络与信息安全咨询
总监
Tel: +86 (21) 2212 2355
quin.huang@kpmg.com

郝长伟
毕马威中国
网络与信息安全咨询
总监
Tel: +86 (10) 8508 5498
danny.hao@kpmg.com

张倪海
毕马威中国
网络与信息安全咨询
总监
Tel: +852 2847 5062
brian.cheung@kpmg.com

邬敏华
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (21) 2212 3180
fm.wu@kpmg.com

宋智佳
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (21) 2212 3306
jason.song@kpmg.com

李振
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (10) 8508 5497
jz.li@kpmg.com

赵隽贤
毕马威中国
网络与信息安全咨询
副总监
Tel: +852 2847 5096
john.chiu@kpmg.com

周文韬
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (21) 2212 3149
kevin.wt.zhou@kpmg.com

范承恩
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (21) 2212 2200
kc.fan@kpmg.com

王晖
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (10) 8553 3630
oh.wang@kpmg.com

袁之骏
毕马威中国
网络与信息安全咨询
副总监
Tel: +852 3927 4697
andy.yuen@kpmg.com

许琦敏
毕马威中国
网络与信息安全咨询
副总监
Tel: +86 (21) 2212 4633
william.q.xu@kpmg.com

kpmg.com/cn/socialmedia

如需获取毕马威中国各办公室信息，请扫描二维码或登陆我们的网站：
https://home.kpmg.com/cn/zh/home/about/offices.html

所载资料仅供一般参考用，并非针对任何个人或团体的个别情况而提供。虽然本所已致力提供准确和及时的资料，但本所不能保证这些资料在阁下收取时或日后仍然准确。任何人士不应在没有详细考虑相关的情况及获取适当的专业意见下依据所载资料行事。

© 2020 毕马威华振会计师事务所 (特殊普通合伙) — 中国合伙制会计师事务所及毕马威企业咨询 (中国) 有限公司 — 中国有限责任公司，均是与英国私营担保有限公司 — 毕马威国际有限公司 (“毕马威国际”) 相关联的独立成员所全球性组织中的成员。版权所有，不得转载。在中国印刷。

毕马威的名称和标识均属于毕马威国际的注册商标或商标。