tufin The Security Policy Company. + CORTEX XSOAR BY PALO ALTO NETWORKS

解决方案概览

自动安全策略管理和上下文丰富的事件响应

概览

当今的安全环境瞬息万变，各团队疲于在不同的环境中协调日常操作和事件响应。为了灵活地开展业务，企业往往需要异构的物理网络和混合云平台，但这会导致缺乏可见性和零散的安全流程。安全团队需要一个能够提供深入、实时的网络可见性平台，并利用这些信息来推动整个安全环境的自动化行动。

Tufin Orchestration Suite与Cortex XSOAR的安全编排和自动化功能相结合，使安全团队能够提高端到端的企业可见性，加速事件响应。

安全团队可以通过标准化和自动化的操作手册任务，从 Cortex XSOAR 中的SecureTrack访问细化策略、网络拓扑和对象数据。无论变更过程是直接通过SecureChange还是通过Cortex XSOAR启动，企业都可以启动自动威胁遏制，同时保持与现有变更控制过程的一致性和完全可审计性。

集成功能：

- 可视化网络拓扑结构和应用程序连接，为调查人员提供更高的可见性，以快速准确地评估事件范围
- 使用操作手册和Tufin工作流自动启动、设计和实施网络访问变更（例如，遏制潜在的受感染系统）
- 在整个事件中始终遵守变更控制流程，且完全可审计
- 利用数百个Cortex XSOAR产品集成，进一步丰富Tufin SecureTrack数据，反之亦然，同时协调所有安全功能的响应
- 通过ChatOps界面提供支持，运行数以千计的命令，包括Tufin Orchestration Suite操作手册，同时与其他分析人员和Cortex XSOAR聊天机器人协作

用例1：自动化事件丰富与响应

挑战：面对广泛的威胁面和多供应商异构环境，安全分析人员不得不在各工具间交叉引用数据、获取进一步的策略上下文并协调遏制和响应，这类重复任务非常耗时。由于处理事件的分析人员不同，流程也不同，导致响应质量参差不齐。

解决方案：安全团队可以在Cortex XSOAR内通过标准化、自动化的操作手册任务访问Tufin SecureTrack的细化策略、网络拓扑结构和对象数据。只要在相关的安全工具（如SIEM、云安全工具和漏洞扫描器）上检测到警报，就会触发这些操作手册，并协调整个安全产品堆栈的操作。

好处：

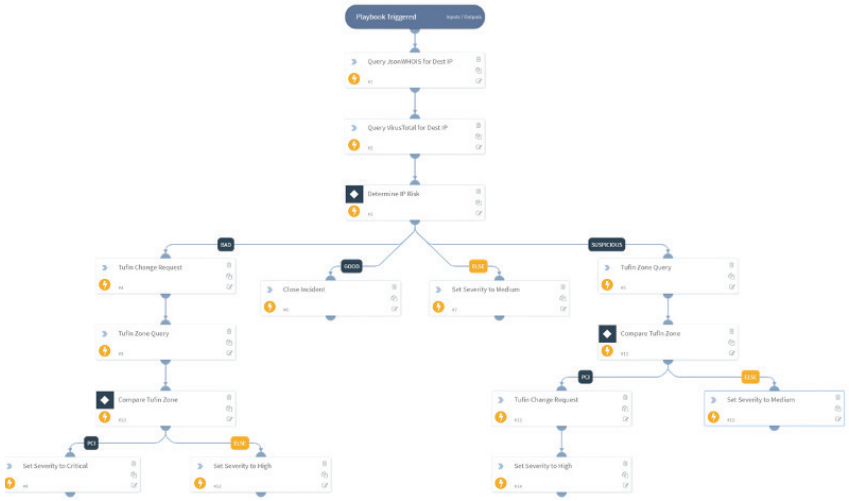
- 在Cortex XSOAR中利用Tufin SecureTrack丰富的网络可见性数据，实现自动化、手册驱动的响应。
- 使用Cortex XSOAR的编排功能，在一个中央控制台上，统一Tufin SecureTrack的网络情报、Tufin SecureApp的应用上下文和来自其他安全工具的数据。
- 通过在Cortex XSOAR中发起的、借助Tufin SecureChange实施的响应行动，确保安全、可审计和合规的变更管理。
- 通过集中协作、调查、记录，以及瞬间（而非几天或几个月）实施变更来提高分析人员的效率。
- 通过自动执行关键任务、进行前瞻性风险分析并结合分析人员评审，缩短决策周期。

兼容：

- Cortex XSOAR
- Tufin SecureTrack
- Tufin SecureChange
- Tufin SecureApp

例如，操作手册可以查询Tufin SecureTrack的NAT策略和特定设备的规则，交叉引用这些数据与SIEM情报，处理智能工具，并再次查询SecureTrack以确定策略变更是否得到授权。

好处：按照共同的Cortex XSOAR操作手册，利用SecureTrack独特的网络安全策略信息以及来自其他产品的数据，提高效率，最大限度地减少手动核对数据，将安全团队从重复性工作中解放出来。



Cortex XSOAR操作手册丰富并简化了事件管理和响应

用例2：对复杂威胁进行交互式实时取证

挑战：除运行自动操作外，攻击调查还包括其他实时任务，如从一个可疑指标转到另一个指标，以收集关键证据，绘制事件之间的关系，抓取和归档证据，并启动补救措施。在调查期间和调查结束后的文档跟踪期，为了运行这些命令，分析人员不得不在各种安全供应商管理控制面板之间来回切换。

解决方案：运行新的操作手册后，分析人员只需在Cortex XSOAR War Room中运行SecureTrack命令，即可实时、准确地了解攻击情况并获取新的可操作信息。例如，如果操作手册的结果显示初始信息，分析人员可以利用tufin-policy-search和tufin-search-topology命令来分别搜索策略和拓扑细节，为事件上下文增加重要信息。分析人员还可使用Tufin SecureChange的自动化操作手册，在主动分析影响和假设情景后，运行命令来启动安全设备变更。

好处：War Room使分析员能够从一个通用窗口快速调整和运行与他们环境中的事件有关的独特命令。所有参与的分析员都对该过程有充分的任务级可见性，并能够从一个统一的控制台运行和记录命令。他们可以确信，这些变更是通过一个完善的工作流程完成的，而不是临时的、未经授权的变更，后者会导致调查结束后，相关人人员需要完成复杂的合规、审计和安全工作。

在Tufin SecureChange中创建票据以启动服务器退役的命令。

Tufin（NYSE：TUFN）简化了世界上一些最大、最复杂的网络的管理，这些网络由数以千计的防火墙和网络设备以及新兴的混合云基础设施组成。
企业选择Tufin Orchestration Suite™来灵活应对不断变化的业务需求，同时保持强大的安全态势。该套件可减少攻击面，实现对安全可靠的应用连接的更大可见性。自成立以来，Tufin已拥有超过2000家客户，其网络安全自动化帮助企业在几分钟内而不是几天内实施变更，同时改善其安全态势和业务敏捷性。

Cortex XSOAR是Palo Alto Networks公司的产品，是唯一的安全编排、自动化和响应（SOAR）平台，它将安全编排、事件管理和互动调查相结合，在事件的整个生命周期为安全团队提供服务。有了Cortex XSOAR，安全团队可以将流程标准化，将可重复的任务自动化，并在其安全产品堆栈中管理事件，以缩短响应时间，提高分析人员的工作效率。如需了解更多信息，请访问https://www.paloaltonetworks.com/cortex/xsoar

Tufin、Unified Security Policy、Tufin Orchestration Suite和Tufin 徽标是Tufin的商标。
本文提及的所有其他产品名称是其各自所有者的商标或注册商标。

Copyright © 2021 Tufin
TD20211805-20211008