tufin The Security Policy Company.

IBM

IBM Security SOAR和Tufin Orchestration Suite网络智能

混合、异构环境中的事件响应

今天的安全事件很少局限于单个主机。几乎每个事件都涉及攻击周期某个阶段的大量控制。遗憾的是，大多数事件响应和安全运营团队对其负责防御的访问和连接点配置一无所知。当今网络的动态性质越来越强，这意味着提供给响应者的网络数据事件电子表格会立即过时，导致错误的结论或不完整的调查。

有了IBM Security SOAR，事件响应和安全运营团队可将其独特的事件响应流程编入工作流，自动化处理不需要人工干预的任务，将资源用于需要人工操作的任务。令人信赖的自动化核心在于完整和准确的数据。基于不完整或不准确数据的自动化会导致事件被错误分类，甚至采取错误的遏制措施。使用IBM Security SOAR实现的自动化则

用于事件响应的网络智能和变更自动化

十多年来，Tufin一直是安全策略管理方面的领导者，擅长管理企业周围最复杂的异构环境。Tufin Orchestration Suite（TOS）被全球安全、云和网络运营团队用来在多厂商、混合云环境中提供准确的安全策略管理、网络拓扑信息、合规性管理以及变更设计和自动化。事件响应和安全运营团队也可以使用值得信赖的TOS功能来管理全球企业的复杂连接，以深入了解安全控制情况并执行自动威胁遏制。

访问和连接洞察实现科学合理的自动化

正确的上下文对于可靠的自动化工作流和决策制定至关重要。在事件分类和调查阶段收集的不可靠或不完整的上下文信息会导致决策不力，从而造成效率损失，更糟的是，潜在的安全事件仍然没有被发现。当今现代企业的动态性质意味着，在生产环境中使用的静态网络文档（如配置数据库的电子表格）效率低下，很快就会过时。

对企业的好处：

- 通过在事件响应工作流中自动收集关键网络情报，改善组织的安全态势。
- 解决和评估复杂的网络拓扑结构，并根据实际设备配置和安全策略进行路径分析。
- 通过在异构安全控制中自动进行从设计到实施的所有变更，提高工作效率。
- 在事件响应过程中保持合规性和完整的变更审计跟踪。

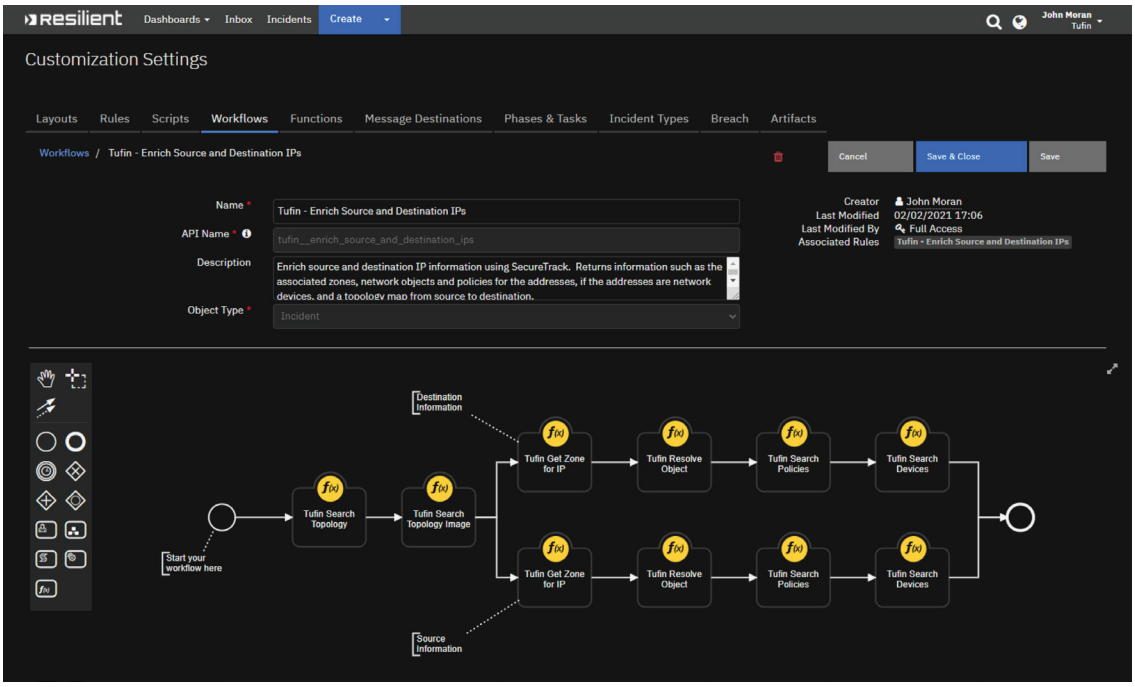

图1 工作流示例 - IP丰富化

Tufin丰富的拓扑结构图和安全策略信息使事件响应团队能够及时、准确地了解企业网络状况。通过对“什么可以与什么对话”以及“谁可以与谁对话”的洞察，使分析人员和自动工作流能够根据最新的拓扑结构做出准确的分类决策，快速识别安全事件、漏洞或其他初始事件构成的实际风险。

集中的可视化与路径分析

了解整个企业资产的连接性和服务接入，对于正确界定潜在安全事件的范围至关重要。然而，在混合环境中，这项简单的任务极具挑战性，因为环境中使用了许多不同的供应商解决方案，由不同的团队管理不同的控制点。以往，这需要手动查询不同的供应商工具和数据库，并手动关联信息，浪费了关键时间和分析周期。

Tufin利用对当前安全控制措施和相关策略的洞察，建立起了一个准确、互动的拓扑图，详细呈现整个混合网络的连接情况。这种拓扑图可从IBM Security SOAR自动查询，显示流量从源头到目的地的路线，快速识别潜在日志信息的其他来源。更重要的是，Tufin可立即确定流量是否被策略所允许，自动化工作流上报对企业构成更大风险的事件。

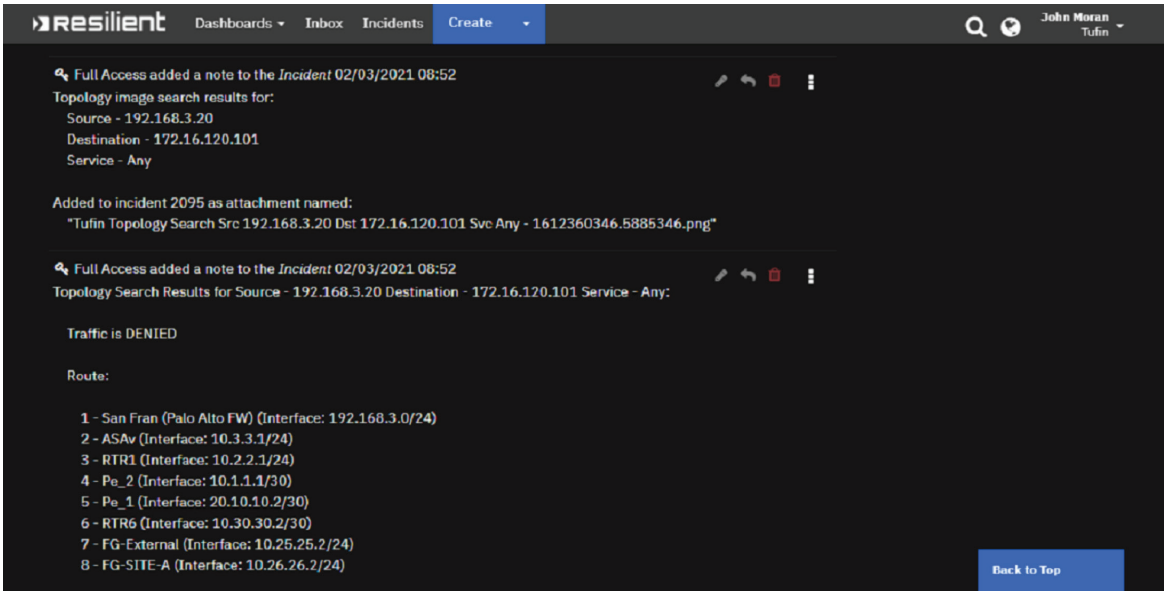

图2 Tufin拓扑结果

自动化的多厂商变更设计和配置

在复杂、混合、多厂商环境中设计安全策略变更是一个耗时的过程，需要手动审查当前拓扑结构和现有的安全策略。使用工作流逻辑和多个供应商的集成准确地编写脚本极其困难，甚至根本无法实现。

Tufin SecureChange利用深入的安全策略和拓扑结构的可见性来自动识别目标资产，并设计新的安全策略来启动所需的变更。有了SecureChange，管理员可以根据现有的变更控制流程设计自定义工作流，根据组织的偏好调整自动化等级。Tufin可自动配置变更，不在受供应商技术的制约，并自动验证变更是否被正确配置。

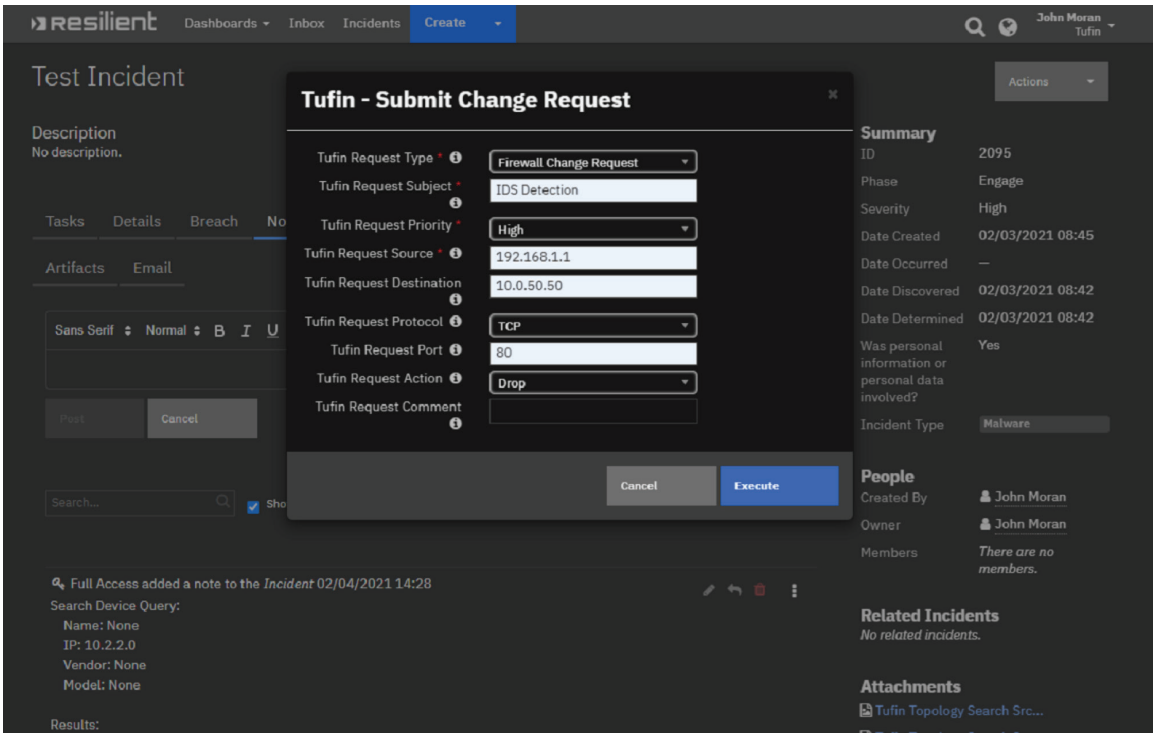

图3 提交变更请求

持续合规与审计

安全事件可能是一个混乱的事件，要优先遏制潜在威胁和减轻风险。为了迅速采取行动，通常会绕过手动文档和正常的变更控制流程。但这样做并不能保证更快解决问题，反而会带来副作用：使变更难以审计或不符合规定。

Tufin Unified Security Policy提供安全策略屏障，以一致的方式应用于所有安全控制。除了检测现有安全策略中的违规情况外，Tufin还主动评估每个变更请求的潜在违规风险，确保在提供之前识别所有潜在风险。Tufin设计和提供的策略变更还能进行自动审计跟踪，记录变更的时间、理由和操作人员。

总结

Tufin与IBM Security SOAR的整合使事件响应和安全运营团队能够及时、准确地了解安全策略和拓扑结构。与Tufin整合后，工作流可以根据访问和连接的当前状态做出更准确的自动决策，减少分析人员的工作量并缩短响应的平均时间。Tufin行业领先的变更管理解决方案使企业能够在混合、异构环境中快速遏制威胁，同时确保在整个事件期间保持可审计性和合规性。

DP20210518-TD20210810