通过 Prisma Access 和 Cortex XSOAR 自动建立全球的安全访问

成千上万的用户从不同的地理位置和多种类型的端点连接到企业的网络，访问不同类型的应用。最终导致的结果是，安全运营中心 (SOC) 和网络管理员需要处理太多的日志和警报。安全团队没有足够的资源来快速对这些警报进行分类，而且他们没有足够的情境来了解这些警报，以确保采取正确的操作。此外，补救操作大多是手动执行的，导致操作迟缓或根本来不及实施操作，因而会让企业面临风险。

优势

- 通过自动化剧本协调远程访问和事件监控操作
- 消除重复的手动任务，提高安全管理员的工作效率
- 可扩展以高效、快速地支持成千上万个远程用户

兼容性

Prisma Access、Cortex XSOAR 5.5 及更高版本

集成功能

随着远程办公的大规模兴起，Prisma™ Access 开始为世界各地的大量员工提供云交付的安全和访问。无需额外的硬件或基础架构部署，即可快速支持远程办公人员，并且可以随着工作人员的增加而自动扩展。在 Palo Alto Networks，利用我们自己的解决方案，我们在全球 39 个办公地点的 7,000 多名员工现在完全实现了远程办公。此外，我们已经成功地将自己的内部 SOC 转变为全面运行的远程模式，通过 Prisma Access 和 Cortex™ XSOAR 持续监控威胁并保护我们的用户群。

Cortex XSOAR 使用 Prisma Access 和 Cortex Data Lake 作为情报来源。这些情报来源可能包括与 SOC 分析师或网络管理员相关的警报（例如，出口 IP 通知）或威胁指标（例如，恶意或异常的用户行为）。收到这些触发后，Cortex XSOAR 可以自动关联其他来源的数据，丰富数据，并采取正确的操作，例如允许出口 IP、注销用户或禁用用户帐户。所有这些操作都是通过自动化剧本来执行的，以实现快速和一致的事件响应。

Cortex XSOAR 使企业能够：

- 自动分类远程连接和用户活动警报。
- 实时自动管理指标块列表（添加、访问、删除）。
- 基于 Prisma Access 和 Cortex Data Lake 的洞察，利用数百个第三方产品集成来协调各安全职能部门的响应。
- 在与其他分析师和 Cortex XSOAR 聊天机器人协作的同时，通过 ChatOps 界面交互运行数百个命令（包括针对 Prisma Access）。

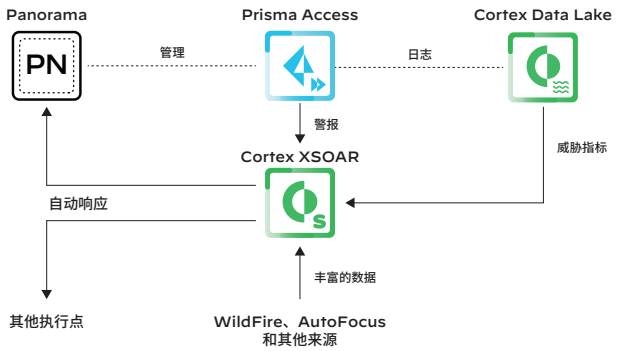

图 1： Prisma Access 和 Cortex XSOAR 集成

自动化基于源 IP 的允许列表

挑战

当您在公有云中部署工作负载时，通过设置适当的安全组或防火墙规则来执行基于源 IP 的限制是一种安全最佳实践。例如，只允许特定 IP 地址集 SSH 访问云实例的规则。要允许您的用户通过 Prisma Access 访问此实例，您需要将 Prisma Access 出口 IP 添加到允许列表中。

Prisma Access 可根据远程办公人员的激增自动扩展。每当发生自动扩展事件时，或者配置了新的 Prisma Access 位置时，都需要将这些新的出口 IP 添加到允许列表中，以确保用户能够持续连接到这些工作负载。如果采用传统安全方法，管理员必须在发生此类事件时手动更新其所有安全组和防火墙规则，这使得很难快速扩展或实时响应任何变化。

解决方案

使用 Prisma Access 和 Cortex XSOAR，当出现自动扩展或新的配置事件时，相关的 Cortex XSOAR 剧本会立即获取 Prisma Access 出口 IP 的新列表，并自动更新云平台上的相关安全组或防火墙规则。这样可以确保业务连续性，不会对需要访问这些工作负载或软件即服务 (SaaS) 应用的用户造成任何损失或中断。

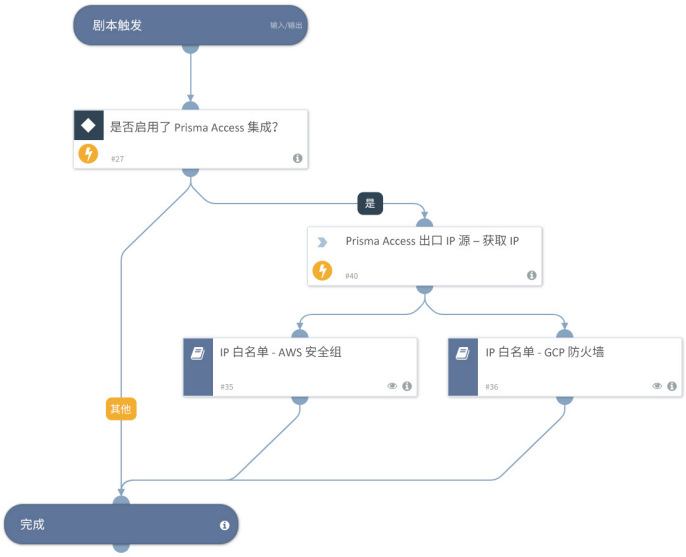

图 2： 剧本自动化 IP 允许列表

自动执行多重身份验证

挑战

您的远程访问策略可能包括针对从不可信或未知 IP 连接的用户的多重身份验证 (MFA)。这是在您的身份和访问管理 (IAM) 解决方案中配置的，例如在 Okta 中定义可信 IP。例如，当用户从总部、分支机构或通过 Prisma Access 进行连接时，都被视为可信网络，就不需要 MFA。但是，当同一用户从公共 Wi-Fi 热点连接时，则需要 MFA。

随着自动扩展或配置新位置，为您的企业分配的 Prisma Access IP 列表将发生变化。这些新出口 IP 的允许列表是手动完成的（因此通常很慢），因此连接到这些新 Prisma Access 实例的用户可能仍然需要执行 MFA，即使通过可信网络访问其 SaaS 应用。这导致用户体验不佳和连接不畅。

解决方案

由传入的自动扩展或新的配置事件触发的 Cortex XSOAR 剧本会立即获取 Prisma Access 出口 IP 的新列表，并自动更新 IAM。因此，当连接到这些新的 Prisma Access 实例的用户访问 SaaS 应用时，IAM 会将其正确识别为从可信网络连接的用户，而不会强制其执行 MFA。不再会因为人工干预而造成滞后时间。

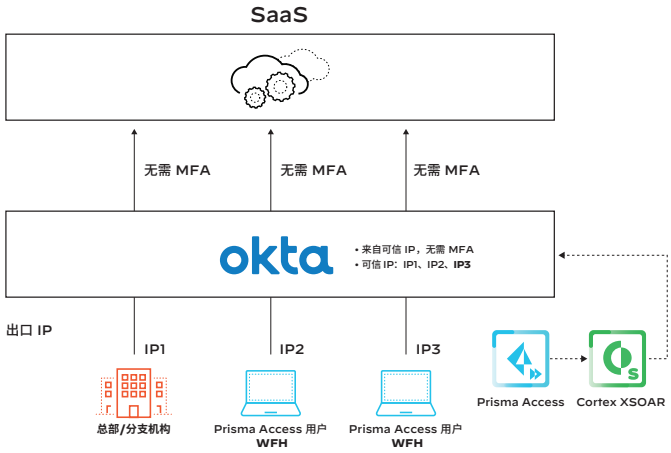

图 3： 自动执行 MFA

自动进行恶意用户活动响应

挑战

许多现代企业允许用户通过公司管理的设备以及个人设备进行连接。当一个端点的安全状况不可信时，或者当您的用户访问钓鱼站点或恶意域时，您需要跟踪这些端点和用户，以便采取纠正措施。手动跟踪用户登录和分类恶意登录是重复和耗时的，大量的威胁日志和警报很难及时解析和解决，这使攻击者有了可乘之机。

解决方案

威胁日志或与命令和控制服务器对话的遭到入侵的端点等警报可触发 Cortex XSOAR 剧本自动从 Active Directory 等目录中提取用户详细信息，注销用户，强制执行 MFA 和/或禁用用户帐户。该剧本可以监控活动的用户并采取行动，例如在发生未经授权的活动时注销用户，或者更新防火墙上的用户标记，所有这些都是通过 Cortex XSOAR 界面完成的。

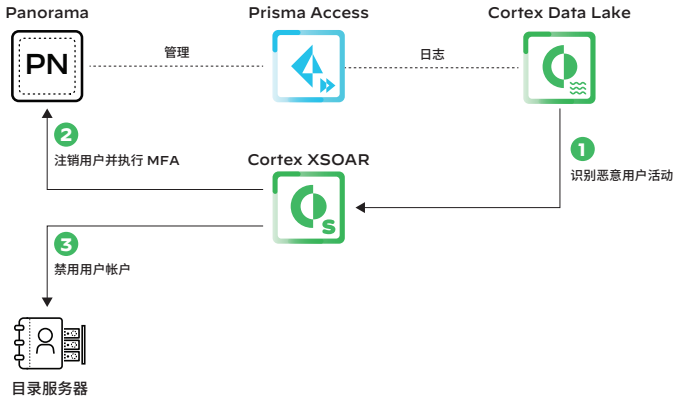

图 4： 自动分类恶意用户活动

分支机构之间受损隧道的监控与警报

挑战

在安全团队繁忙的一天中，没有时间主动监控潜在的连接故障，因为工作人员通常忙于处理紧急事务和对关键事件进行分类。这使得很难跟踪所有 VPN 隧道的运行状况，以确保用户 100% 的正常运行时间。

解决方案

进入 Jobs，这是 Cortex XSOAR 的一个功能，它可以运行剧本，帮助 SOC 实现主动安全操作的自动化。可安排自动 VPN 隧道监控剧本，以定期轮询 Prisma Access 连接状态，并在隧道发生故障时发送 Slack® 警报以采取补救措施。

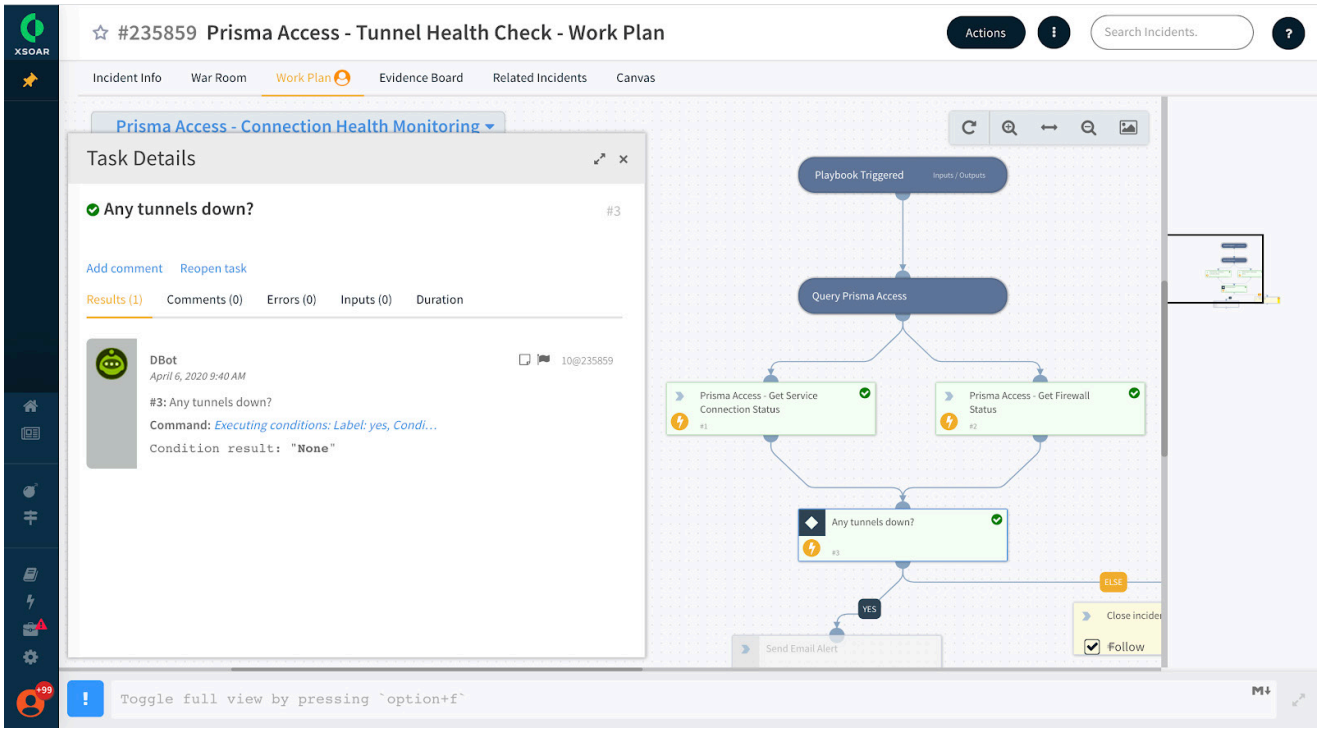

图 5：隧道健康检查剧本

关于 Prisma Access

Prisma Access 是一种安全访问服务边缘 (SASE)，通过从云端提供联网和网络安全服务，帮助企业利用云端和移动设备。随着传统网络安全设备保护范围外的用户、分支机构、服务以及大量数据数量不断增加，企业需要一种汇聚这些功能的云基础架构。Prisma Access 提供一致的安全服务以及对通过公共框架提供的云应用的访问（包括公有云、私有云和软件即服务），帮助实现无缝的用户体验。Prisma Access 作为云服务从 76 个国家/地区的 100 多个地点交付，为移动用户、分支机构和零售店带来可靠的连通性和安全性。

关于 Cortex XSOAR

Cortex XSOAR 在行业首个扩展安全编排、自动化和响应产品中统一案例管理、自动化、实时协作和威胁情报管理。SOC 团队可以使用全球最全面的企业安全操作平台来提高效率，从而管理所有来源的警报，通过剧本进行流程标准化，对威胁情报采取行动，并自动响应任何安全用例，使响应时间缩短 90%，需要人工干预的警报减少 95%。

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

© 2020 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。

automate-global-secure-access-with-prisma-access-and-cortex-xsoar-b-060820