技术验证

瞻博网络自动威胁检测和补救

Sky Advanced Threat Prevention 和 SRX 系列防火墙

作者：Jack Poller（高级分析师）

2019 年 7 月

本 ESG 技术验证受瞻博网络委托，并在 ESG 许可下发布。

内容

ESG 技术验证

ESG 技术验证的目标是，为各类企业的 IT 专业人士介绍有关信息技术解决方案方面的知识。ESG 技术验证不应取代购买之前的评估流程，而只是提供对这些新兴技术的深入见解。我们的目标是，探索 IT 解决方案中一些比较有价值的特性和功能、展示如何使用它们来解决客户的实际问题并发现需要改进的领域。ESG 验证团队专家提供的第三方观点源于我们的实际测试体验，以及对在生产环境下使用这些产品的客户进行的访谈。

简介

本 ESG 技术验证将主要针对自动威胁检测和补救的效果和效率对瞻博网络 Sky Advanced Threat Prevention (ATP) 和 SRX 系列下一代防火墙进行评估。在本验证过程中，ESG 将通过恶意软件对某个端点进行攻击，并使用 Sky ATP 检测此攻击，同时利用防火墙阻止此端点的南北向流量，并利用本地交换机阻止此端点的东西向流量，最终断开此端点与网络的连接。

背景介绍

ESG 的年度技术支出调查显示，网络安全已成为 IT 组织首当其冲的要务，40% 的组织表示，在未来 12 个月，加强网络安全将成为其技术支出中的一项首要业务增长要素。[1]

这些组织可能会发现，改进网络安全面临诸多问题。根据 ESG 的研究，超过四分之三 (76%) 的组织表示，如今的网络威胁比两年前更加难以检测和应对。受访者认为，威胁检测和应对方面的主要挑战包括威胁数量和复杂性不断提高 (34%)、威胁检测/应对工作量不断增加 (17%)、攻击面不断扩大 (16%)、各种类型的威胁检测/应对工具数量不断增多 (11%)，以及全球网络安全技术持续短缺 (8%)。[2]

认为***加强网络安全***将成为组织未来 12 个月最大技术支出的受访者比例。

认为如今的***威胁检测和应对***比两年前更加困难的受访者比例。

在实践当中，组织会部署多家供应商提供的多种不同的工具来检测并应对威胁，从而需要分析人员登录到各种系统来管理警报并采取相应的保护措施。因此在这种情况下，人工操作必不可少，而这会减慢检测、调查、应对和补救过程的速度，增加平均响应时间 (MTTR)，延长威胁驻留时间。

我们需要的是一种能够汇集多个单点工具功能的解决方案，这种解决方案可通过自动执行威胁检测和应对工作流来简化这些工具的使用和管理。82% 的调查受访者表示，改进威胁检测/应对方法堪称当务之急，87% 的受访者表示，他们在改进威胁检测和应对方面已经制定了正式的计划并划拨了专项资金。[3]

瞻博网络 Sky Advanced Threat Prevention 和 SRX 系列防火墙

瞻博网络的 Sky Advanced Threat Prevention 与瞻博网络 SRX 系列服务网关相结合，可通过为虚拟、分布式及核心位置提供路由、交换和 WAN 接口来实现高性能网络安全和高级威胁缓解功能。

Sky Advanced Threat Prevention

瞻博网络将 Sky Advanced Threat Prevention (ATP) 设计为一款 SaaS 解决方案，可使用来自云端的实时信息进行反恶意软件保护，以防止组织受到高级持续性威胁 (APT) 和勒索软件等网络攻击。Sky ATP 与 SRX 系列下一代防火墙的集成可提供深度包检测以及内联威胁阻止功能。Sky ATP 可利用机器学习、动态分析、反沙箱隐匿技术、静态分析和反病毒签名来检测并防止网络攻击。部署 Sky ATP 的组织可获得以下优势功能：

- **基于云的分析**——潜在有害文件会发送到云端进行高级分析，以确定它们是善意的还是恶意的。
- **恶意软件补救**——检测到的恶意软件会传输到 SRX 系列防火墙，以阻止攻击。

[1] 资料来源：ESG 研究报告，*2019 年技术支出意向调查*，2019 年 2 月。
[2] 资料来源：ESG 主要调查结果，*威胁检测和应对态势*，2019 年 4 月。
[3] 同上。

- **报告和分析**——Sky ATP Web 界面有助于简化包括配置和更新在内的各项管理工作，并通过报告和分析工具来深入了解威胁状况和受损系统。
- **系统隔离**——SRX 系列防火墙可使用来自 Sky ATP 的信息来隔离受损系统。
- **集成式威胁情报**——可与瞻博网络 SecIntel 威胁情报服务进行实时通信，进而与 SRX 系列防火墙共享威胁信息，以便迅速采取行动。Sky ATP 可使用开放的 API 将第三方威胁情报源分发给所有订阅 ATP 的 SRX 防火墙，以便迅速采取行动，减少攻击面。
- **命令和控制防御**——Sky ATP 可与 SRX 系列防火墙进行通信，以防止恶意软件横向移动并阻止与命令和控制服务器的通信。
- **电子邮件及 Web 分析和补救**——机器学习算法可以对电子邮件和 Web 文件进行分析，以检测恶意附件和文件，并通过防火墙阻止这些文件，防止电子邮件成为攻击媒介。
- **集成化管理**——Sky ATP 和 SRX 系列防火墙可以集成到一款集成式应用程序：瞻博网络 Junos Space Security Director 中，该应用程序可利用单一控制台来统一管理所有瞻博网络设备和服务。管理员可利用 Security Director 在安全策略生命周期的所有阶段对有状态防火墙、统一威胁管理、入侵防御、应用程序防火墙、VPN 和 NAT 进行管理。

SRX 系列服务网关

瞻博网络 SRX 系列服务网关可作为虚拟或物理设备来充当下一代防火墙，为云、分支办公室、中小企业和大型企业、大型数据中心以及服务提供商提供支持。SRX 防火墙可提供以下优势：

- **保障各类组织的安全**——SRX 防火墙形式多样，从一体化、集成式物理和虚拟安全网络设备到基于机箱的高扩展性数据中心解决方案应有尽有。
- **全面的威胁防御**——可通过一整套分层安全服务抵御各种已知和未知的威胁。
- **性能和可扩展性**——可通过扩展支持高达 1Tbps 的吞吐量、高达 285 Gbps 的 IMIX 防火墙、9000 万个并发会话以及 230 Gbps 的 IPS。
- **可靠性**——可通过无中断硬件和软件升级、冗余组件以及高达 99.9999% 的可靠性确保不间断正常运行，从而实现不间断的业务连续性、安全性和应用程序可用性。

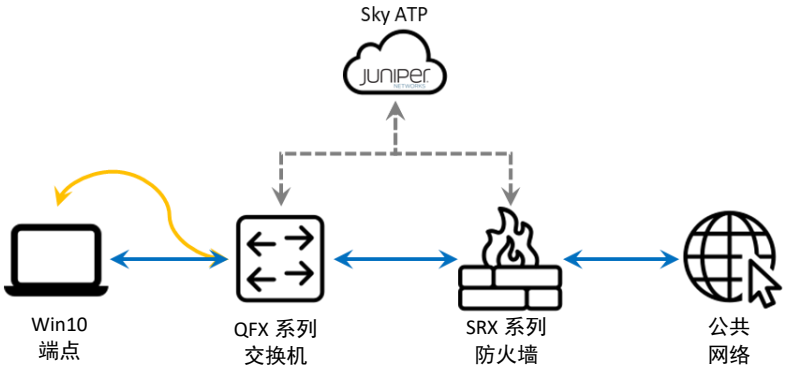
ESG 技术验证

ESG 将对 Sky Advanced Threat Prevention 和 SRX 系列防火墙进行评估和测试，其中包括将恶意文件下载到端点，以及验证该文件是否会由 SRX 防火墙发送到 Sky ATP 进行评估。我们会重点考察在 Sky ATP 检测到端点受感染后执行的自动检测、应对和补救操作。

开始测试

首先，我们会开发一个测试平台，如图 1 所示。我们首先将一个 Windows 10 端点作为虚拟机运行。该端点会连接到 VLAN 4025 上的瞻博网络虚拟 QFX 系列交换机，并能够切换到 VLAN 3025 上的另一个连接。该 QFX 交换机会连接到 SRX 系列虚拟防火墙，然后连接到公共网络。QFX 交换机和 SRX 防火墙与 Sky ATP 集成在一起。

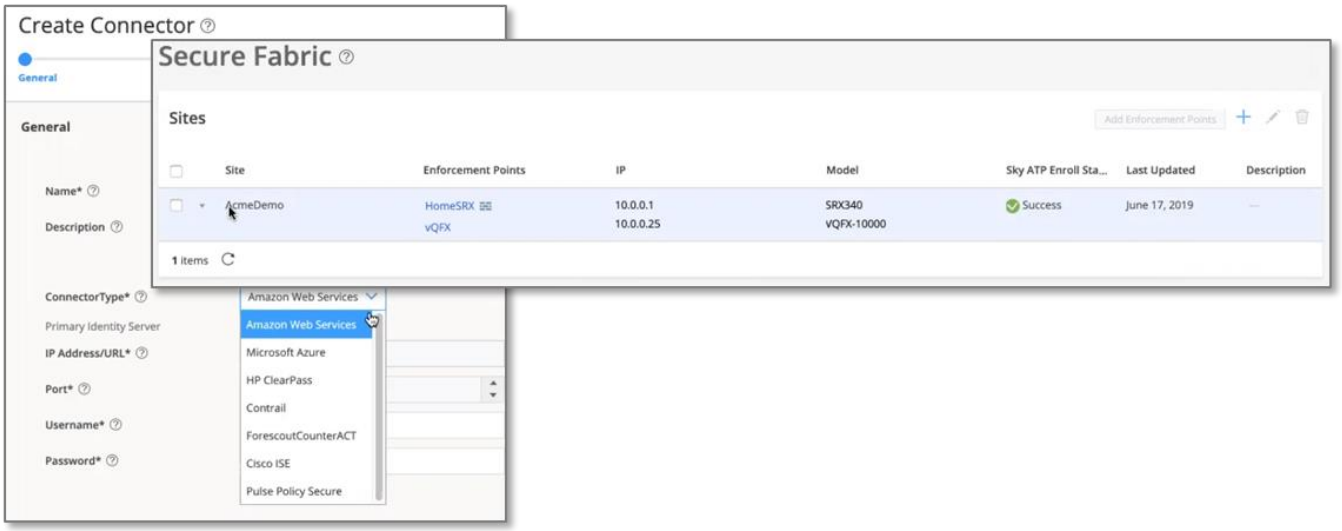
图 1. ESG 测试平台



资料来源：Enterprise Strategy Group

我们使用瞻博网络 Junos Space Security Director 作为统一的控制台来管理所有瞻博网络系统。如图 2 所示，我们会创建一个安全交换矩阵，用于将防火墙和交换机作为一个安全域进行管理。此外，我们还会考察创建连接器的功能，Sky ATP 可以通过此连接器连接到第三方服务和交换机，包括 AWS、Azure、ClearPass、Contrail、Forescout CounterACT、Cisco ISE 和 Pulse Policy Secure。

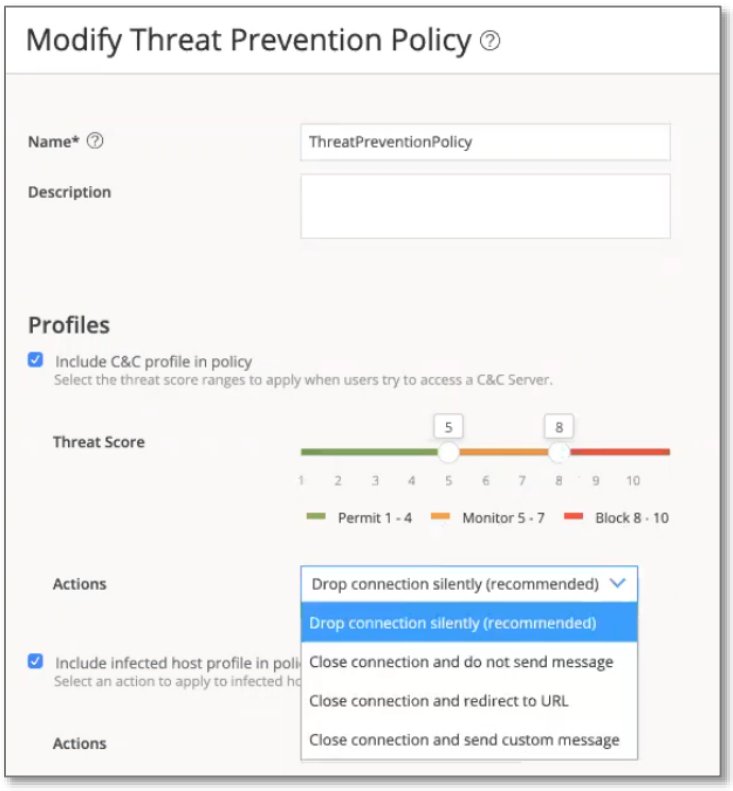
图 2. Sky ATP 安全交换矩阵和连接器



资料来源：Enterprise Strategy Group

接下来，我们会考察 Sky ATP 的威胁防御策略。如图 3 所示，通过 Sky ATP，我们可以根据威胁得分设置预先确定的应对措施。我们会选择将威胁得分 ≥ 8 的对象断开连接且不提供任何提示。

图 3. Sky ATP 威胁防御策略



资料来源：Enterprise Strategy Group

这为何重要

网络安全问题本身就十分复杂且极具挑战性，如果缺乏经验丰富或训练有素的员工，加之需要协调来自不同供应商的多种单点工具且这些工具的用户体验与界面又截然不同，从而使威胁的检测和防御变得愈加困难。为了降低这种复杂性，组织就需要通过一种解决方案来简化网络安全基础架构和流程。

ESG 的验证结果表明，瞻博网络提供的方案可以简化部署——我们可以轻松地创建安全交换矩阵。我们可以为不同系统组成的组定义并设置策略，而无需单独为每个设备设置策略。定义安全策略就像使用滑块为不同级别的风险设置阈值和应对措施一样简单。

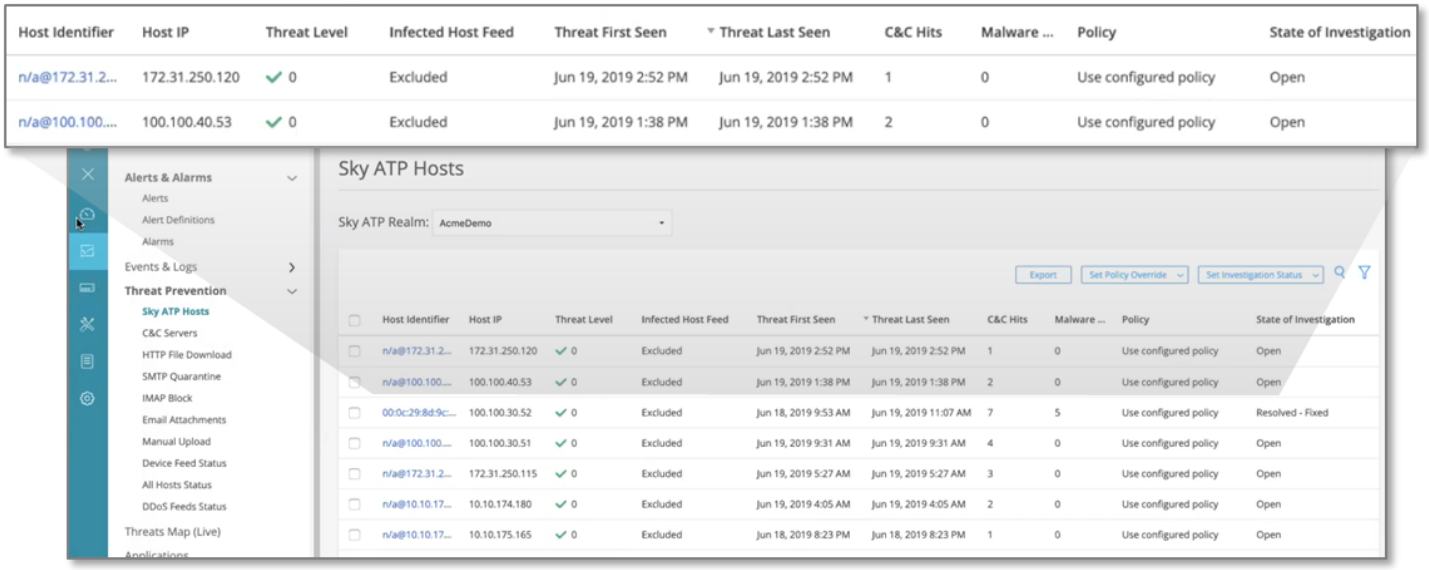
此外，ESG 的验证结果还表明，我们能够为任何虚拟和物理瞻博网络设备组定义并设置策略，从而简化复杂环境下的安全和网络管理工作。借助 Sky ATP 和 SRX 防火墙，安全分析师便无需花费太多的时间来配置和管理工具，可以将更多的时间用在应对警报、调查威胁和攻击等关键活动上。

感染、检测和应对

ESG 对下载文件时瞻博网络防御威胁的过程进行了观察。我们会将恶意软件下载到端点上，而 SRX 防火墙则将下载的文件发送到 Sky ATP 进行分析。Sky ATP 会分析该文件并确定其是否为恶意软件并已感染主机，之后，Sky ATP 会指示 SRX 防火墙和 QFX 交换机断开此端点与网络的连接，从而阻止南北向流量（SRX 防火墙）和东西向流量（QFX 交换机）。

首先，我们会考察当前环境状况，如图 4 所示。Sky ATP 会将测试用的 Windows 10 端点列在受管端点列表中，而将 IP 地址为 100.100.40.53 的端点从***受感染的主机源***中***排除***。Sky ATP 会使用此列表来跟踪受攻击主机。

图 4. Sky ATP 主机监控



资料来源：Enterprise Strategy Group

接下来，我们登录到虚拟 SRX 防火墙和虚拟 QFX 交换机，并验证此配置是否会使该端点正确地进行内部通信（东西向）和外部通信（南北向）。

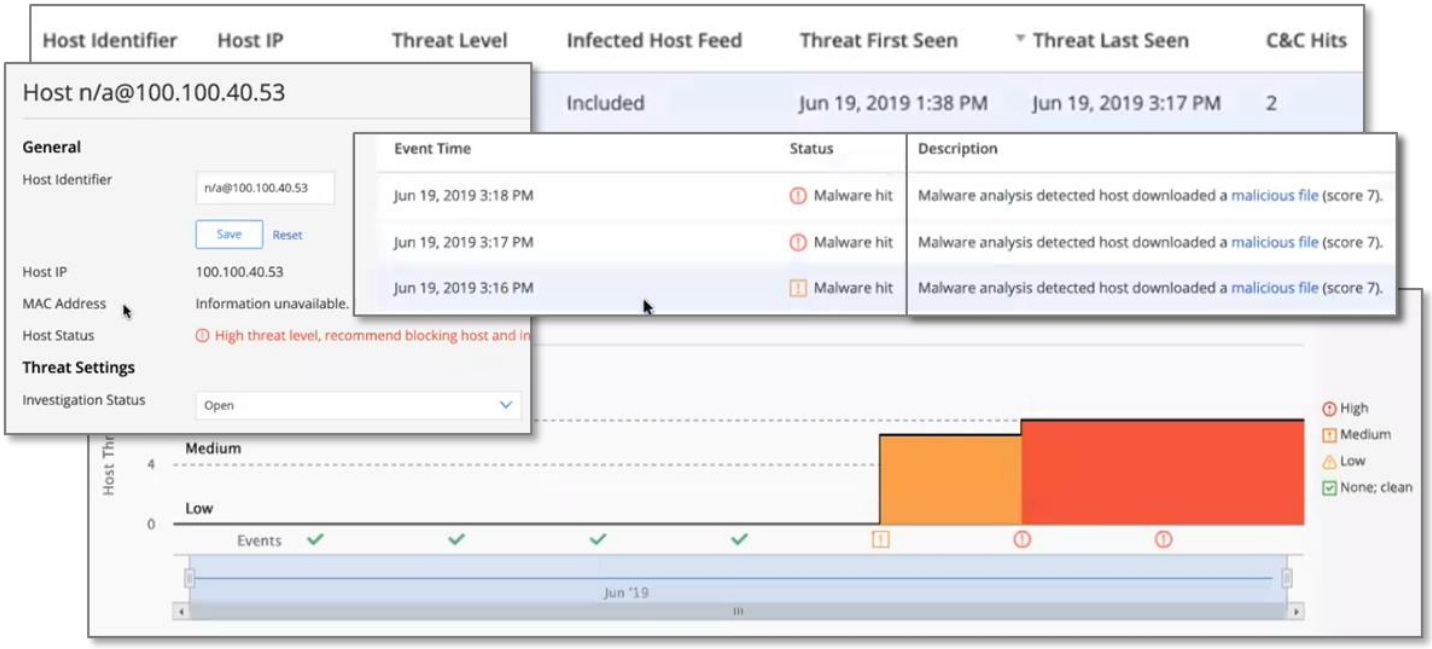
我们会登录到 Windows 10 端点，使用 Web 浏览器导航到一个含有恶意软件样例的网站，并下载三个恶意文件。

每个文件下载结束时，SRX 防火墙都会将此文件的一份副本发送到 Sky ATP 进行分析。Sky ATP 会对每个文件进行一系列检查，包括将其签名与恶意软件数据库进行对比、使用机器学习进行静态分析、执行动态沙箱分析和行为分析等。通过这些检查，Sky ATP 确定每个文件都包含恶意软件。根据自动分析阶段收集的信息，Sky ATP 会为每个文件分配一个威胁得分，然后会计算该端点的总威胁得分。

根据这一总威胁得分以及先前配置的威胁防御策略（见图 3），Sky ATP 会将主机状态设置为***高威胁级别***，将调查状态设置为***待调查***，并将端点添加到受感染的主机列表（即***受感染的主机源***）中，如图 5 所示。

按照安全分析师的典型工作流，我们会通过单击主机标识符链接开始调查，此链接会呈现更多信息，其中包括感染该主机的恶意软件列表以及一个展示感染情况随时间变化的图形。我们发现这些信息对我们开始调查、分析根本原因、对端点采取补救措施和解决问题非常有用。

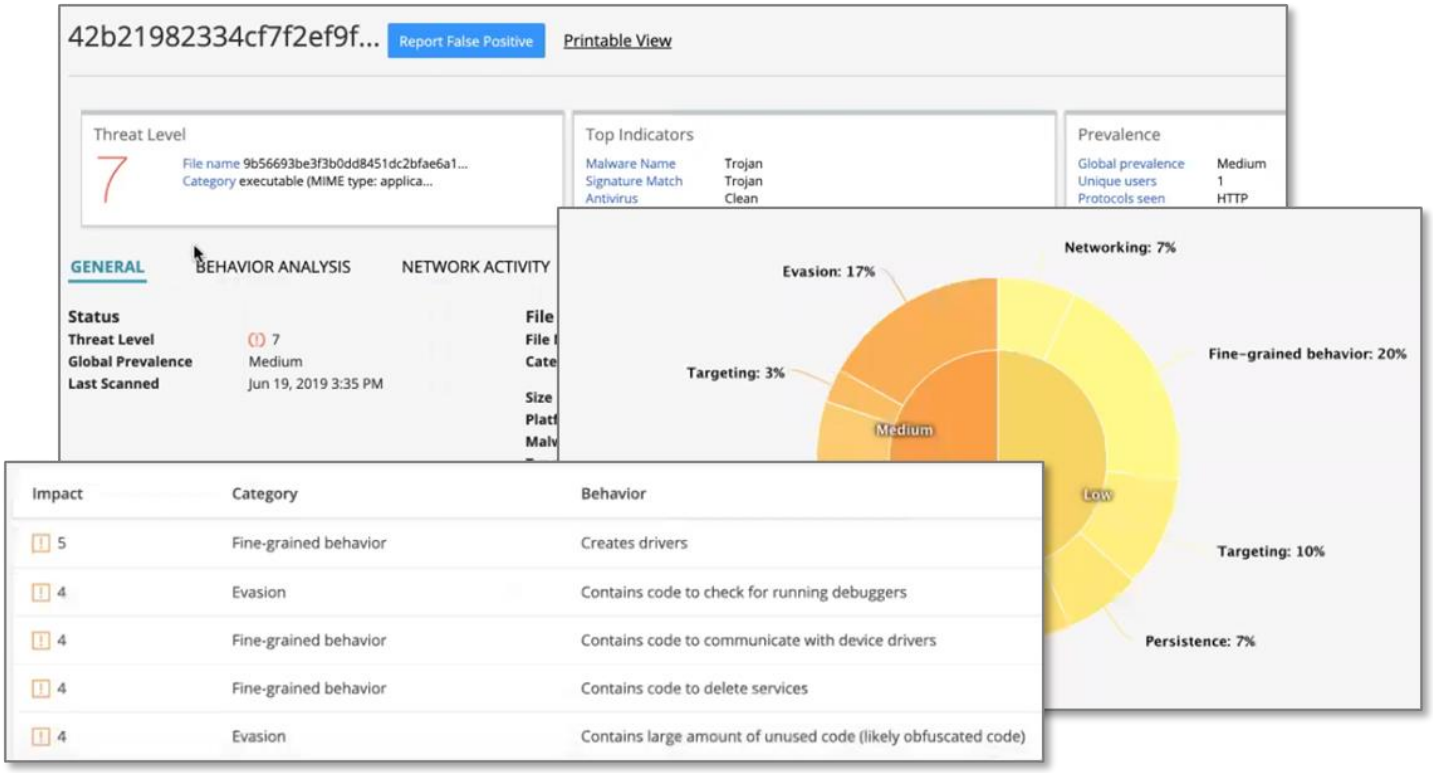
图 5. 受感染主机详细信息



资料来源：Enterprise Strategy Group

之后，我们会单击已下载的恶意软件对应的链接，Sky ATP 会提供有关感染情况的更多信息，如图 6 所示。顶部会显示一些摘要信息，包括威胁级别、首要指标和威胁感染范围等。摘要数据下方的选项卡式窗格会显示一些常规信息。单击“行为分析”选项卡会弹出一个基于风险的饼图，其中根据风险对不同的行为进行了分类。该恶意软件被归类为木马，包括中等风险的隐匿和定向技术，以及低风险的网络连接、隐匿、定向和持久性技术。此外，Sky ATP 还会显示一个表格，详细说明所发现的每个行为。而另一个选项卡则会详细显示该恶意软件的网络活动。

图 6. 恶意软件详细信息



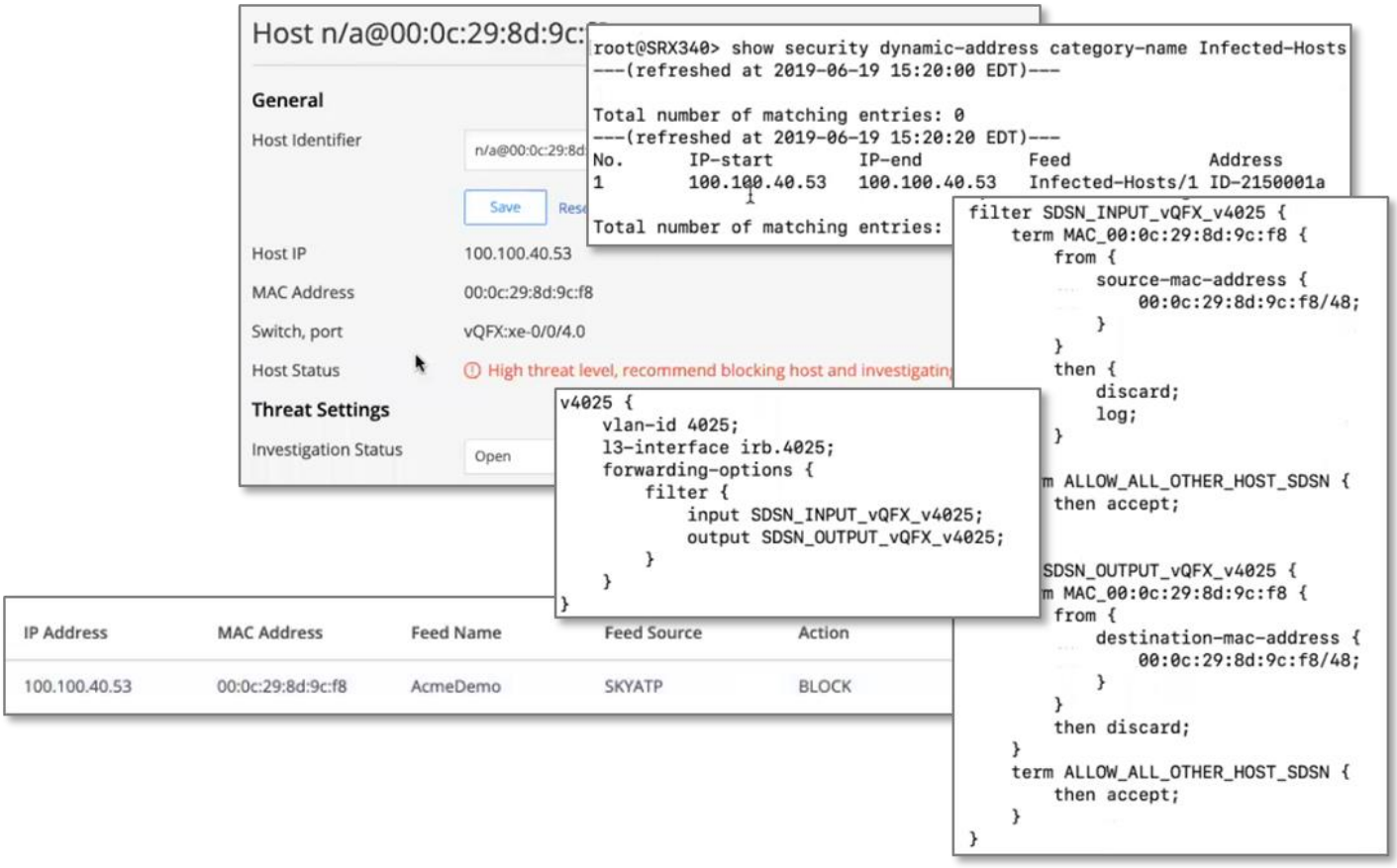
资料来源：Enterprise Strategy Group

在下载文件后的五分钟内，我们确定该端点已经与网络隔离——我们无法对内部或外部 IP 地址执行 ping 操作，从而证明 Sky ATP 的自动威胁补救措施起到了作用。将端点添加到受感染主机源会使 SRX 防火墙阻止该端点进行南北向通信。此外，该端点的 DHCP 租约会被撤销，并且该端点会失去 IP 地址。

由于 IP 地址无效，Sky ATP 会更新其数据库，以便按 MAC 地址引用受感染端点，如图 7 所示。

Sky ATP 可通过内置的连接器与所有瞻博网络设备进行通信，Sky ATP 会指示 QFX 交换机对端点进行分区，以阻止东西向流量。该交换机会创建一个过滤器，以阻止数据包进出该端点的 MAC 地址 (00:0c:29:8d:9c:f8)。该过滤器会应用于该端点的 VLAN (4025)。

图 7. 自动补救



资料来源：Enterprise Strategy Group

发现端点无法与网络通信并认为网络可能出现问题后，用户会感到十分沮丧，可能会尝试使用其他以太网端口。我们会模拟这种情况，使用虚拟化服务器来切换虚拟网络，将端点从 VLAN 4025 切换到 VLAN 3025。切换后，该端点会立即获得一个新的 IP 地址，并能够进行内部和外部通信。

大约五分钟后，内部和外部通信再次被阻止。Sky ATP 和 SRX 防火墙会持续对网络进行监控，并通过 MAC 地址识别此端点。由于该端点已经位于受感染主机源上，因此 SRX 防火墙会应用一个新的南北向块。Sky ATP 会指示 QFX 交换机更新其无状态防火墙，以便在 VLAN 3025 上应用此 MAC 地址块。

这为何重要

由于长期以来缺乏网络安全技术方案，组织无力采用需要长期经验积累的多种复杂产品，因此需要付出大量的精力并利用人工流程来检测和防御威胁。

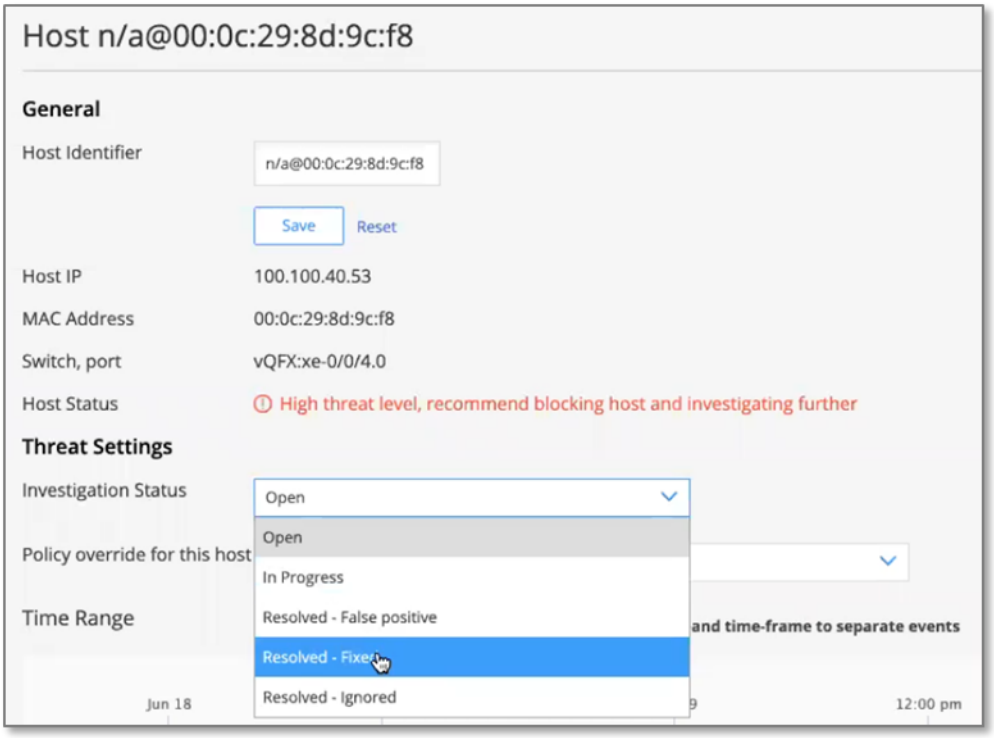
ESG 通过验证发现，瞻博网络 SRX 系列防火墙会自动将下载的文件转发到 Sky ATP 进行恶意软件分析和检测。一旦 Sky ATP 确定端点被感染，该端点就会被添加到受感染站点列表中。内置的自动化和编排功能会将端点与网络断开，以阻止内部和外部通信。

使用 Sky ATP 和 SRX 系列防火墙可以帮助组织尽可能快地检测到网络攻击，阻止网络攻击链的发展，从而保护关键资产的安全，减少恶意软件驻留的时间。

管理方案和补救措施

ESG 模拟了典型的安全分析师工作流，通过删除主机上的所有恶意软件文件对主机进行杀毒处理。接下来，我们会使用 Sky ATP 界面更改调查状态，将问题标记为“调查完成”。在主机监控部分，单击相应主机。使用下拉框选择调查状态：***已解决 - 已修复***。如图 8 所示，安全分析师可以将调查状态设置为***待调查***、***调查中***、***已解决 - 误报***、***解决 - 已修复***或***解决 - 已忽略***。

图 8. 更新调查状态



资料来源：Enterprise Strategy Group

将调查状态设置为任何已解决的选项，表明系统不再受感染，可以恢复网络上的通信。Sky ATP 会将该系统从受感染主机源中删除，SRX 防火墙和 QFX 交换机会删除该主机对应的任何防火墙条目。在将调查状态设置为“已解决 - 已修复”后不久，我们便发现该端点可以进行内部和外部通信。

这为何重要

随着组织需要应对的网络攻击日益增多且日趋复杂，安全分析师必须持续、及时地对可能受损的系统进行调查。由于缺乏集成、自动化和编排工具，分析师不得不将大量的时间和精力花在单调而重复的任务上。

而 ESG 通过验证发现，安全分析师一旦将调查标记为完成，瞻博网络自动化工具就会与所有适当的防火墙和交换机进行通信，以删除网络通信块，使主机能够进行内部和外部通信。这样，分析师便无需再手动确定需要更新哪组交换机和防火墙、登录到每个设备、更新规则并保存新配置了。瞻博网络自动化工具不仅可以减轻安全分析师的工作量，还有助于避免人为错误。

更重要的事实

如今，网络安全态势正在变得日趋复杂且难以管理。知识产权、客户信息和财务数据正在面临日益严峻的网络攻击风险，这种风险甚至可能会造成严重的后果，包括经济处罚、对品牌和公司估值的影响以及法律诉讼。同时，企业还必须对数量急剧增加的安全事件进行调查并采取相应的应对措施。新系统和应用程序激增会增加安全事件出现的几率，而更优质的检测工具也会生成更多的警报。2019 年，53% 的企业反映网络安全技术方案存在严重短缺的现象，这一比例与 2018 年的 51% 相比[4]有所提高，因此，各个组织正在苦苦寻觅可以提高效率和效果的技术方案，并纷纷转向自动化以及可实现自动化的工具，以减轻重复性人工任务的负担。

瞻博网络设计的 Sky ATP 可实现网络安全自动化，它可以利用实时情报来防御恶意软件威胁。SaaS 解决方案可通过各种连接器与 SRX 系列下一代防火墙和一整套瞻博网络产品以及第三方产品实现集成。Sky ATP 可通过威胁情报、防病毒签名、静态和动态分析、机器学习以及其他技术来自动检测威胁并采取补救措施。

SRX 系列下一代防火墙可以将下载的文件、电子邮件附件和其他潜在的恶意对象自动转发给 Sky ATP 进行分析。一旦检测到威胁，SRX 防火墙便会与 Sky ATP、QFX 系列交换机以及其他网络设备相配合，切断受感染系统与网络的连接，从而自动阻止南北向流量，防止恶意软件从命令与控制服务器窃取数据，并自动阻止东西向流量，防止其横向移动。

ESG 的验证结果表明，Sky ATP 可以简化部署、配置和管理工作。我们可以通过定义安全的交换矩阵（即网络设备集合）来简化操作，以控制大型系统组，这一点对于大型、复杂环境十分有用。清晰简洁的用户界面有助于更快地定义安全策略并让该操作变得轻松自如。

我们通过验证发现，SRX 系列防火墙可将可疑对象自动转发到 Sky ATP 进行恶意软件分析和检测。如果 Sky ATP 将主机归类为受感染主机，则 SRX 防火墙会自动断开该主机与网络的连接，从而防止南北向流量的产生。此外，Sky ATP 和 SRX 自动化功能会与 QFX 交换机相配合，将受感染系统与东西向流量断开连接。这种自动化功能有助于防止横向移动并与命令与控制服务器进行通信。

Sky ATP 可以帮助用户对受感染主机进行调查，并提供所需的准确信息，以确定感染情况、感染的根本原因以及纠正措施。修复问题并将调查标记为已解决后，Sky ATP 和 SRX 防火墙会自动恢复网络连接，使安全分析师的工作流省去一项单调而复杂的人工流程。

如果组织想要避免复杂而易错的手动工作流，并在整个环境中利用自动化和编排工具来检测和防御威胁，瞻博网络的 Sky ATP 和 SRX 系列下一代防火墙值得一试。

[4] 资料来源：ESG 研究报告，*2019 年技术支出意向调查*，2019 年 2 月。

Enterprise Strategy Group 是一家从事 IT 分析、调研、验证和策略的公司，致力于为全球 IT 行业提供市场情报以及切实可行的深入见解。

 www.esg-global.com

 contact@esg-global.com

 电话：508.482.0188