“WannaCry”突显勒索软件的威胁：思科 ISE 一路为您保驾护航

资产可视性和合规性快速威胁

遏制

软件定义的分段

如果您错过了影响巨大的 WannaCry 勒索软件攻击，思科 TALOS 团队的研究人员可通过这篇博文带您一同回顾。WannaCry 波及到了世界各地成千上万台计算机。该恶意软件以蠕虫方式进行传播，会扫描并感染网络上其他易受攻击的设备。勒索要求？被感染的用户需要在六小时内支付价值 300 美元的比特币，否则赎金的数额还将增加。

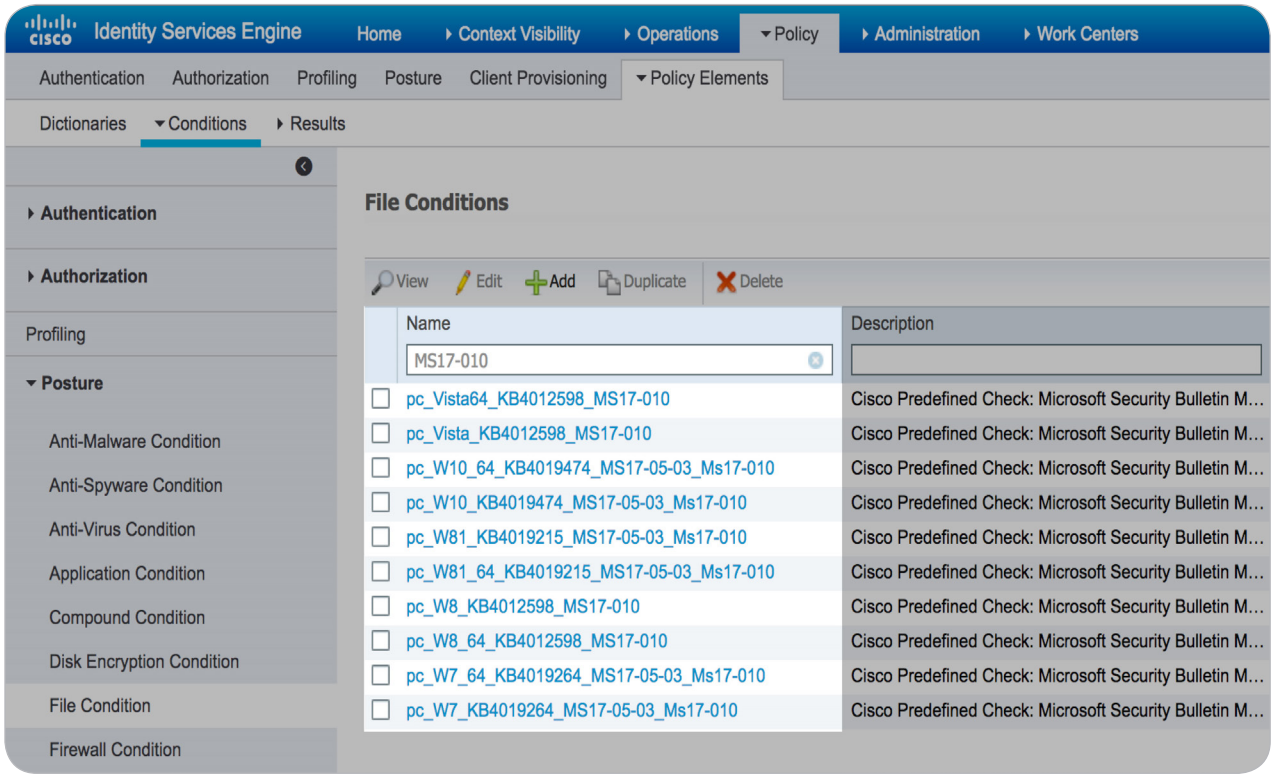
使用思科 ISE 的客户则拥有保护，可免受此类攻击影响。事实上，ISE 可通过多种方式为您提供保护，预防、阻止甚或缓解勒索软件的威胁。

针对勒索软件的思科 ISE

有关如何使用针对勒索软件的思科 ISE 的更多信息，请访问 cisco.com/go/ise。

资产可视性和合规性：

能够真正看到网络上有哪些设备是至关重要的，因为如果不能看到，就无法提供保护。这意味着不仅要看到用户和设备的详细信息，还要了解特定设备的操作系统、防病毒软件、应用、硬件、防火墙覆盖等实际情况。

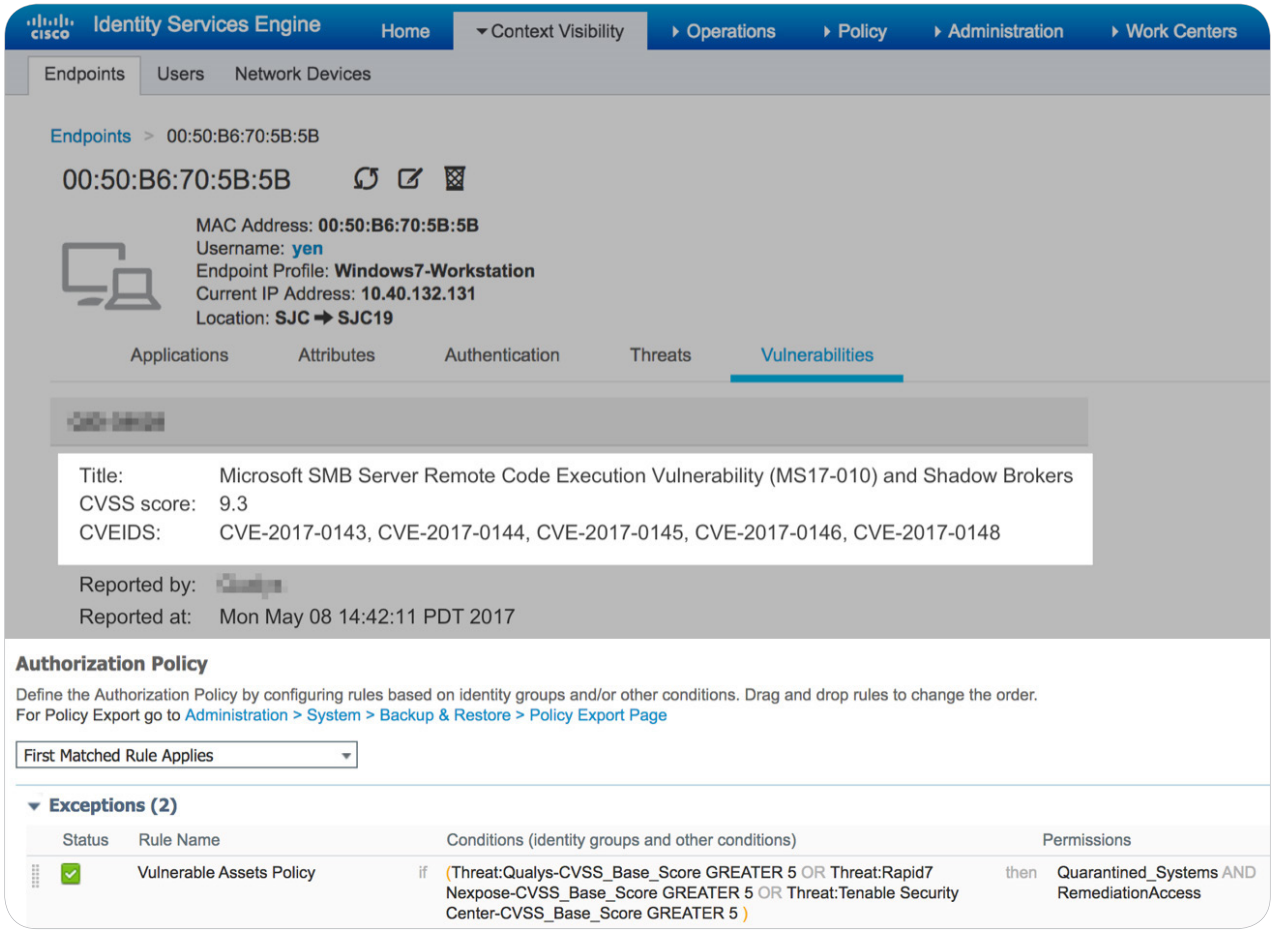


对于 Wannacry，思科 ISE 可根据已应用哪些补丁，确定用户是否容易受到此类攻击。在应用适当的补丁之后，它可以根据这种可视性实施适当的合规性策略。

您甚至可以专门编写一条安全状态策略，查找初始文件投放位置“C:\Windows\mssecsvc.exe”，然后立即在网络中隔离受感染的设备。

快速威胁遏制：

ISE 通过其他思科安全产品和第三方解决方案获取威胁和漏洞情报，以控制终端的访问级别。思科 AMP 与 CTA 可以根据终端行为提供 STIX 格式的终端威胁评分，并且 ISE 可遏制受感染的终端进一步访问网络。它还可与 Qualys、Rapid7 和 Tenable 等漏洞评估供应商产品集成，这意味着能够在终端上扫描漏洞，以确定 WannaCry 能否利用 ETERNALBLUE 漏洞攻击。如果确定为能，ISE 将获得自动警报并反映具有“高”CVSS 分数的终端的漏洞状态并阻止相应设备。

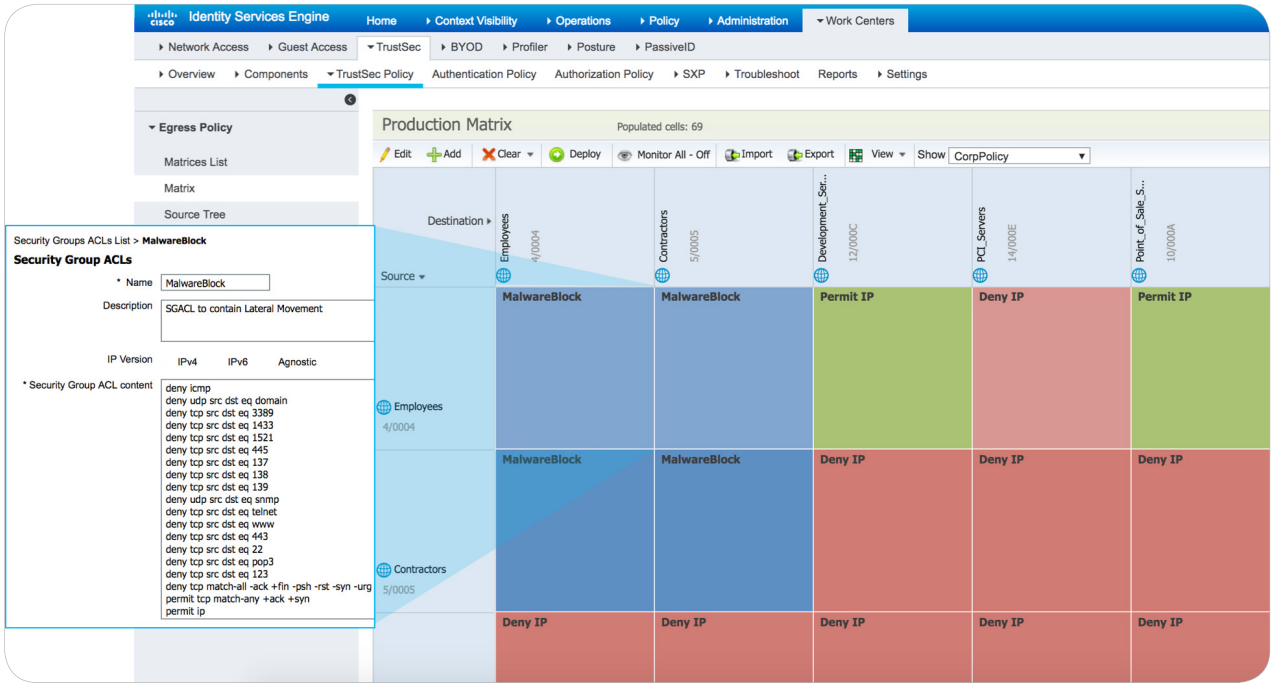


ISE 还可以获得直接将已感染设备隔离的警报。无论 ISE 是否与思科 Firepower、Stealthwatch 或众多思科技术合作伙伴之一产品集成，您都可以自动响应并立即遏制威胁。例如，Stealthwatch 会触发 WannaCry 安全事件，具体取决于以下攻击阶段：

在端口 445/tcp 上进行 Addr_Scan 扫描、执行大量 SMB 对等体活动、执行蠕虫活动、传播蠕虫以及连接到 Tor。一旦确定为恶意事件，点击按钮即可通知 ISE 从网络中隔离违规设备。

软件定义分类：

发生漏洞攻击的可能性非常高。无论是零日攻击，还是“WannaCry”这样利用未修补系统中已知漏洞的攻击，可扩展、可升级的网络分段对于减少勒索软件在系统之间的传播都至关重要，甚至可以将其彻底消除。思科 TrustSec 是一款革命性产品，可实现软件定义的分段，以便快速、敏捷地实施基于组的策略。它使横向移动限制可用于任何规模的网络，甚至可实现同类用户/设备的微分段。[了解详情](#)。



DEFCON 策略集可显著增强事件响应攻略，使其能够切换至对系统攻击的预定义响应。不同于更改单个用户和设备的授权或者手动实施策略更改，更改 DEFCON 状态将更改用于定义用户、设备和系统如何彼此通信的 TrustSec 策略，如同升起“网络”吊桥以保护您的关键数据并维护关键服务。例如，您可以定义 DEFCON 4 来为所有访客切断网络，可以定义 DEFCON 3 来为所有自带设备 (BYOD) 用户切断网络，可以定义 DEFCON 2 来限制点对点流量，还可以定义 DEFCON 1 来严格限制对您的“最高权限内容”的访问。

您可以看到，思科 ISE 有许多应对勒索软件攻击的方式。考虑到当今威胁环境的规模和复杂性，没有哪种灵丹妙药能解决所有问题。因此，思科提供了一系列简单、开放且自动化的解决方案，有效地保证安全性。

有关如何使用针对勒索软件的思科 ISE 的更多信息，请访问 cisco.com/go/ise。