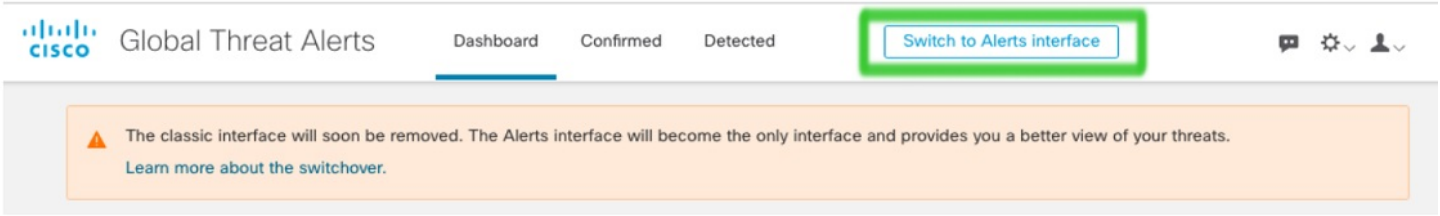
2021 年 8 月

2021 年 8 月发布的思科基于云的机器学习全局威胁警报更新。

已停用传统接口

早在 6 月，我们便建议您从传统接口切换到警报接口。

图 *1:*



较旧的经典接口现已停用，而较新的警报接口已成为唯一接口，为您提供网络威胁的增强视图。

改进了对扫描和受阻通信的处理

为了减少误报的数量，全局威胁警报现在可以抑制由水平扫描通信触发的威胁检测。它现在还可以在感染的初始阶段抑制对代理阻止的通信的威胁检测。

为了提高案例的可视化效果，当感染持续存在于终端，并且部分出站通信被代理（或其他出站控制进程）阻止时，全局威胁警报将描述作为一部分呈现的特定安全事件威胁检测。

在本例中，代理传感器阻止了与主机（已知为特洛伊木马）通信的尝试。安全事件通知您此软件被视为不需要，因为它可能会危害您的隐私或系统安全。

图 *2:* 示例：通知您通信尝试已被代理阻止的安全事件