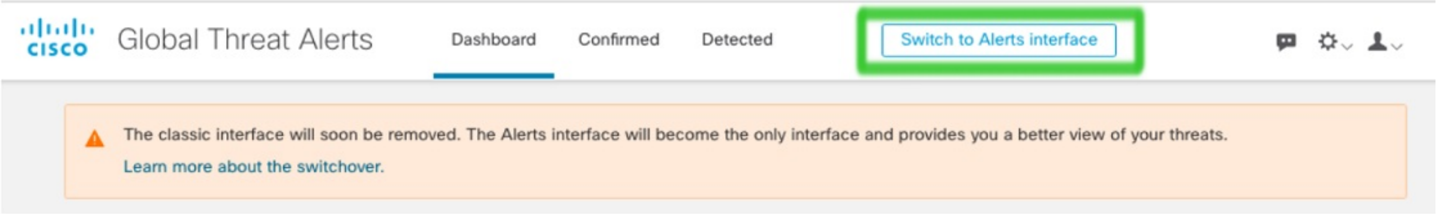
August 2021

Updates released in August of 2021 to Cisco cloud-based machine learning global threat alerts:

Classic Interface Decommissioned

Back in June, we recommended that you switch from the classic interface to the alerts interface.

Figure 1:



The classic interface will soon be removed. The Alerts interface will become the only interface and provides you a better view of your threats.

Learn more about the switchover.

The older classic interface has now been decommissioned, and the newer alerts interface has become the only interface, providing you with an enhanced view of the threats on your network.

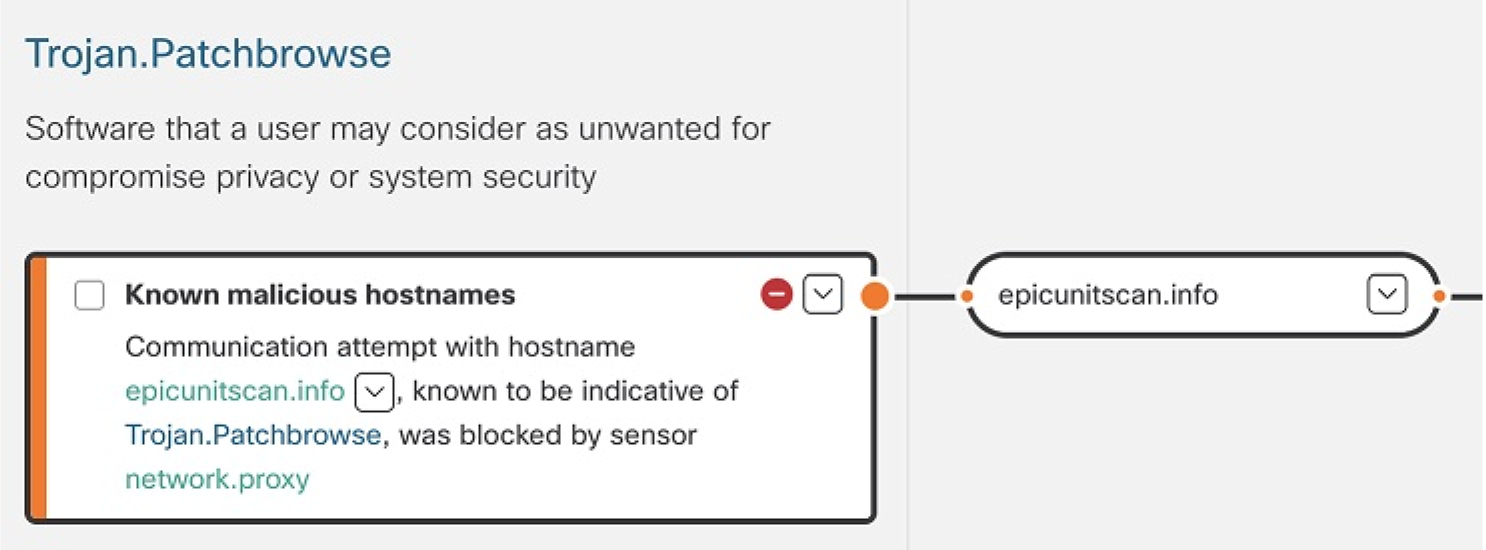
Improved Handling of Scans and Blocked Communications

To reduce the number of false-positives, global threat alerts can now suppress threat detections triggered by horizontal scan communications. It can also now suppress threat detections of proxy-blocked communications in the initial phases of an infection.

To improve the visualization of cases, when an infection is persistent on an endpoint, and a portion of the outbound communication is being blocked by a proxy (or other outbound-control process), global threat alerts describes the particular security event presented as a part of the threat detection.

In this example, an attempt to communicate with a host (known to be indicative of a Trojan) is blocked by a proxy sensor. The security event informs you that this software is considered unwanted, since it may compromise your privacy or the security of your system.

Figure 2: Example: security event informing you that the communication attempt was blocked by proxy



Trojan.Patchbrowse

Software that a user may consider as unwanted for compromise privacy or system security

□ **Known malicious hostnames**

Communication attempt with hostname epicunitscan.info, known to be indicative of Trojan.Patchbrowse, was blocked by sensor network.proxy