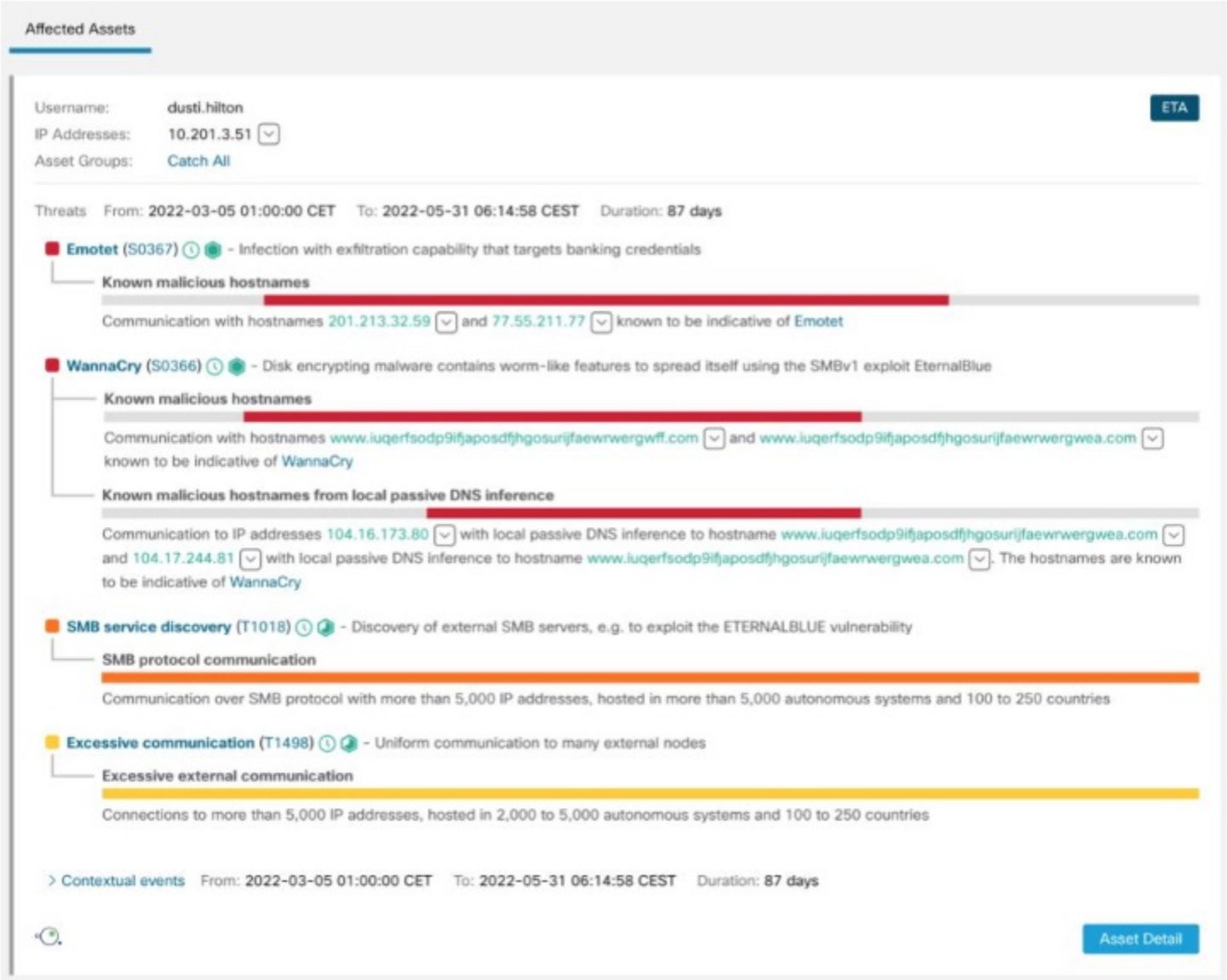
May 2022

Updates released in May of 2022 to Cisco cloud-based machine learning global threat alerts:

Enhanced View of Alert Details

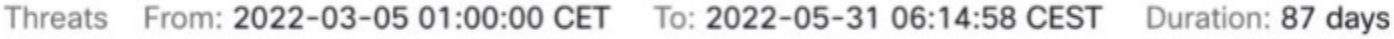
We've enhanced the **Alert Detail** page to now show more information about the **Affected Assets**. Each affected asset includes a new **Threats** section which lists all the threat detections made on that asset, including all the convicting security events.

Figure 1:



At the top of the **Threats** section is the total observation period for all the detected threats and their convicting security events on the particular asset.

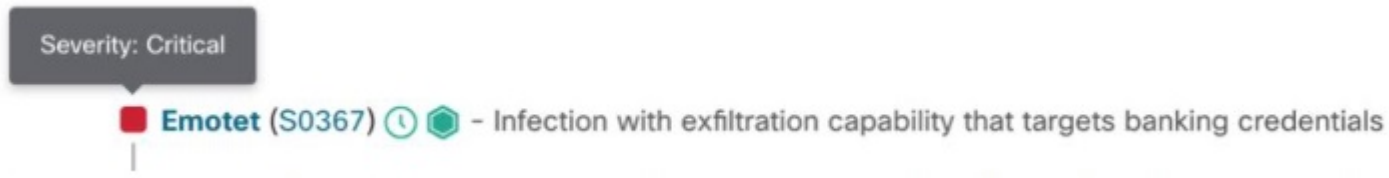
Figure 2:



Each threat detection shows its name, MITRE link, description, and:

- Severity

Figure 3:

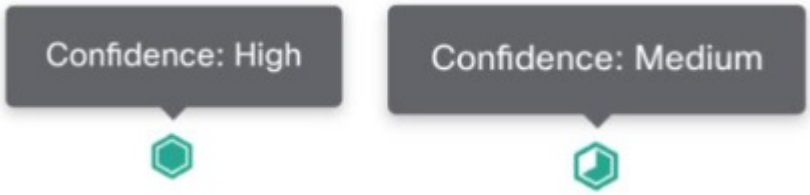


- Observation period

Figure 4:

- Confidence

Figure 5:



Each threat detection is backed by the security event(s) below it. Many of the events contain rich security annotations that provide the evidence which led to the creation of the event.

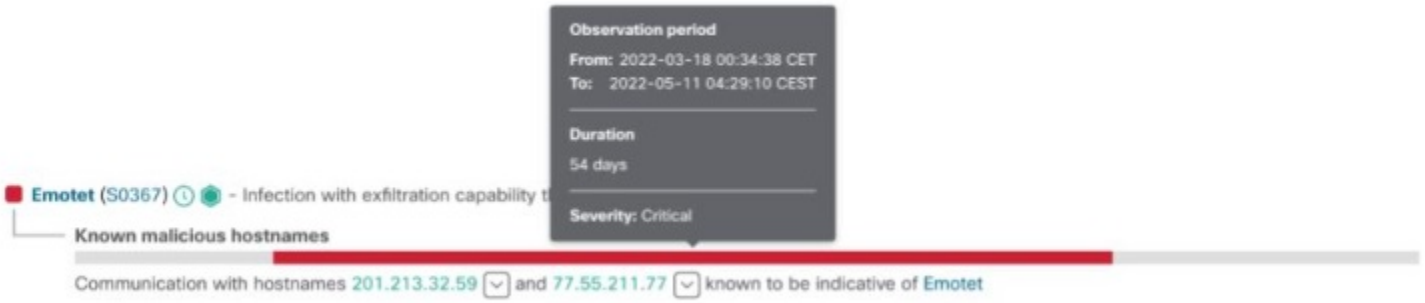
Figure 6:

An event annotation may also contain a drop-down menu that enables you to pivot to other Cisco Security products and pull in additional information and intelligence about the observables.

Figure 7:

Each security event includes a timeline showing the timing and occurrence of the behavior within the context of the **Threats** total observation period.

Figure 8:



The new **Contextual events** section can be expanded to show more events that could provide additional context about what was happening on the asset.

Figure 9: