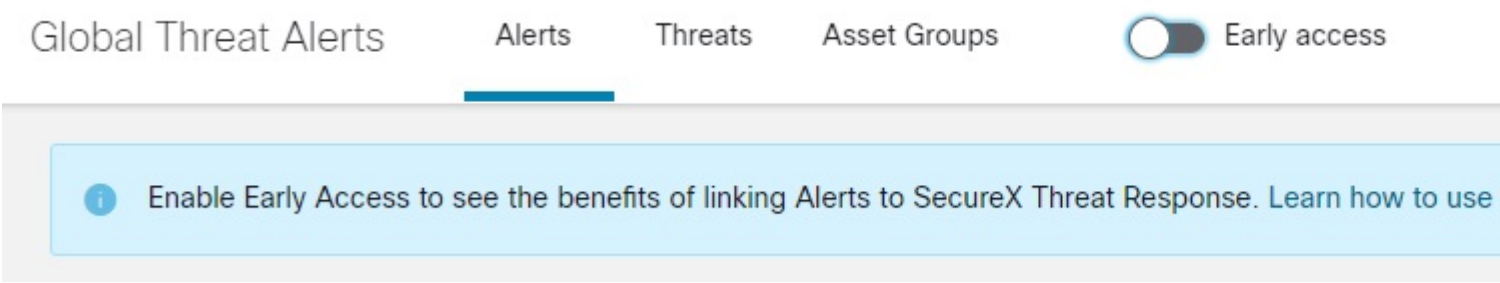
January 2022

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

Alert Promotion to SecureX Incident Manager

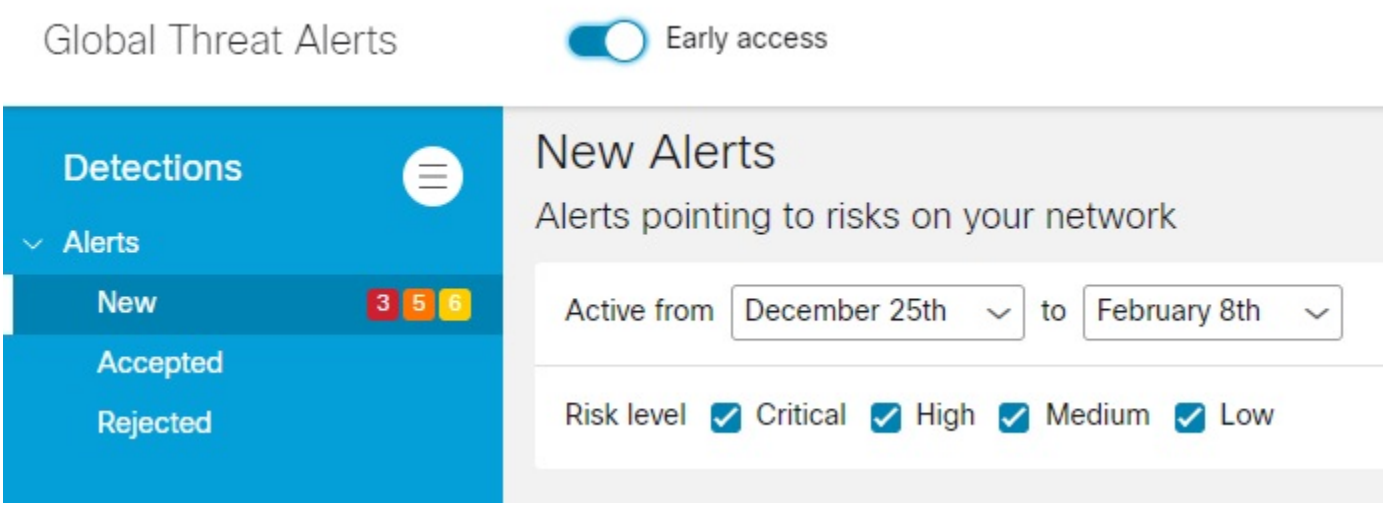
We've added the ability to promote alerts in global threat alerts to the SecureX incident manager. To turn on this feature, enable **Early access** in the header of the global threat alerts console:

Figure 1: Click Early Access to Enable this New Feature



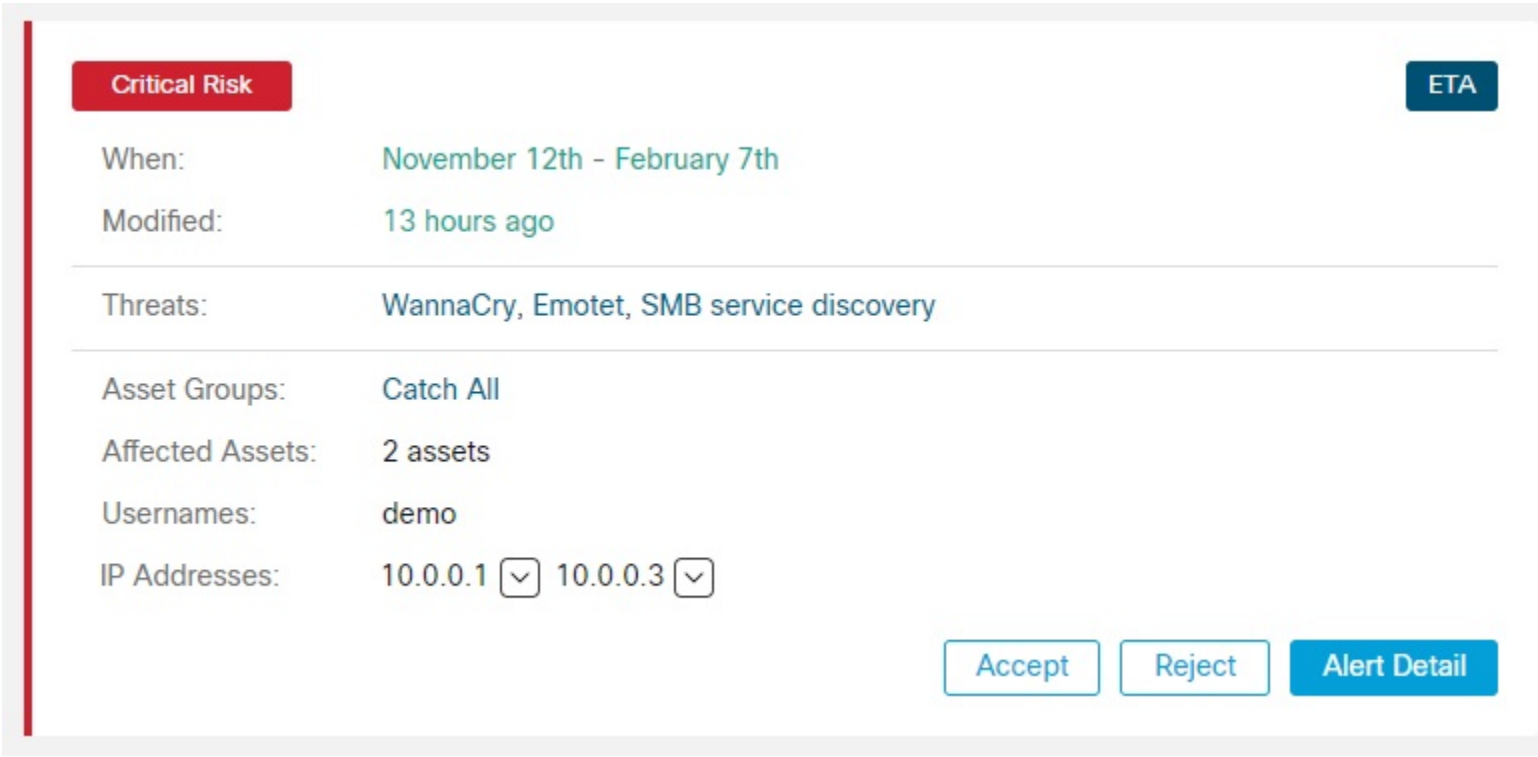
Once enabled, the SecureX incident manager replaces the existing workflow in global threat alerts. Alerts are then categorized into **New**, **Accepted**, or **Rejected**:

Figure 2: Alerts in SecureX Incident Manager



A new alert can be moved to either state using the **Accept** or **Reject** button:

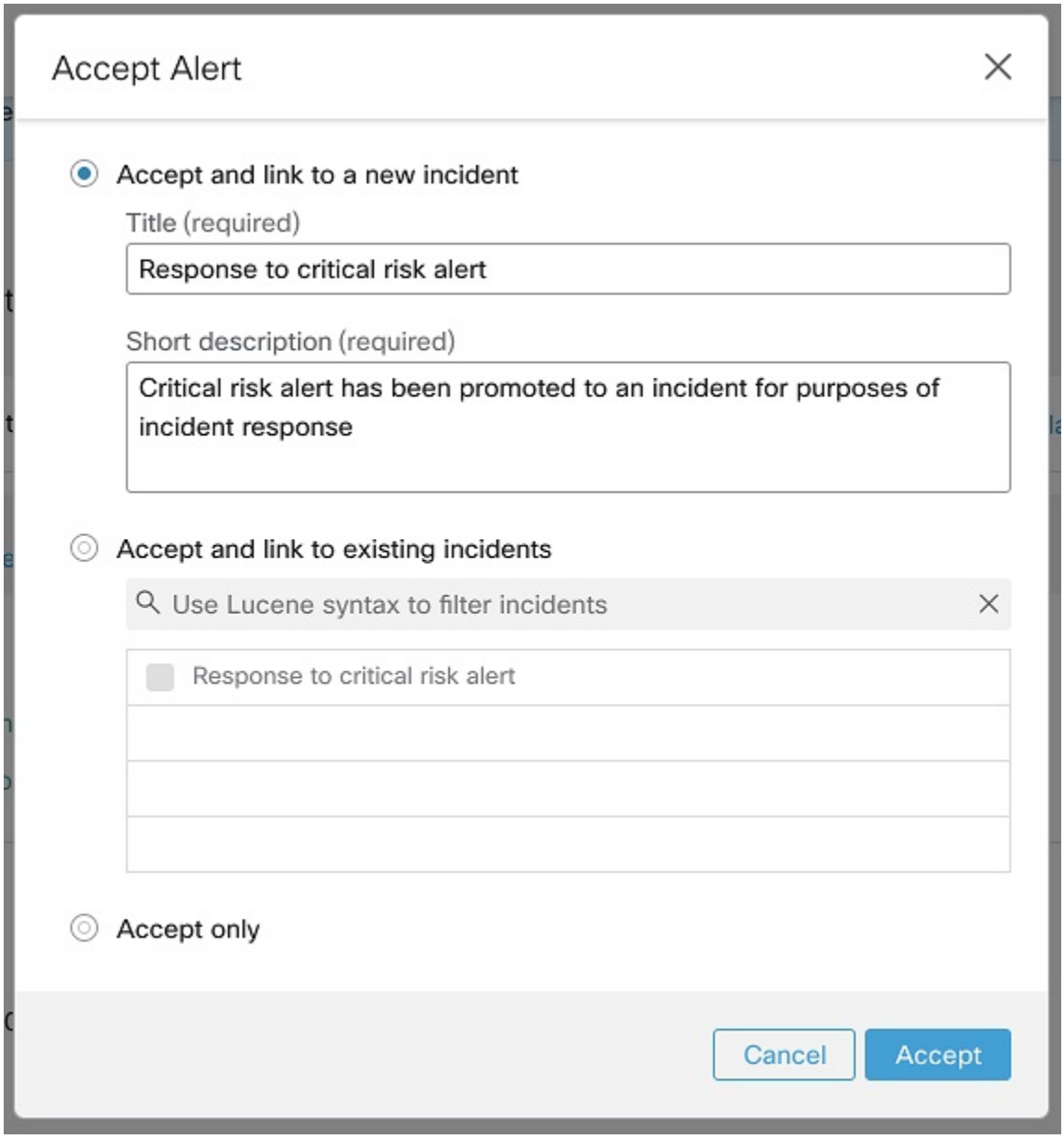
Figure 3: Accept or Reject Alert



While global threat alerts continues to focus on its core competencies, such as extended detections and efficient alert triage, it now integrates more tightly with the SecureX ecosystem, using just one click to promote detections to the incident response workflow in SecureX.

When an alert is accepted, it can be linked to an existing or new incident in the SecureX incident manager:

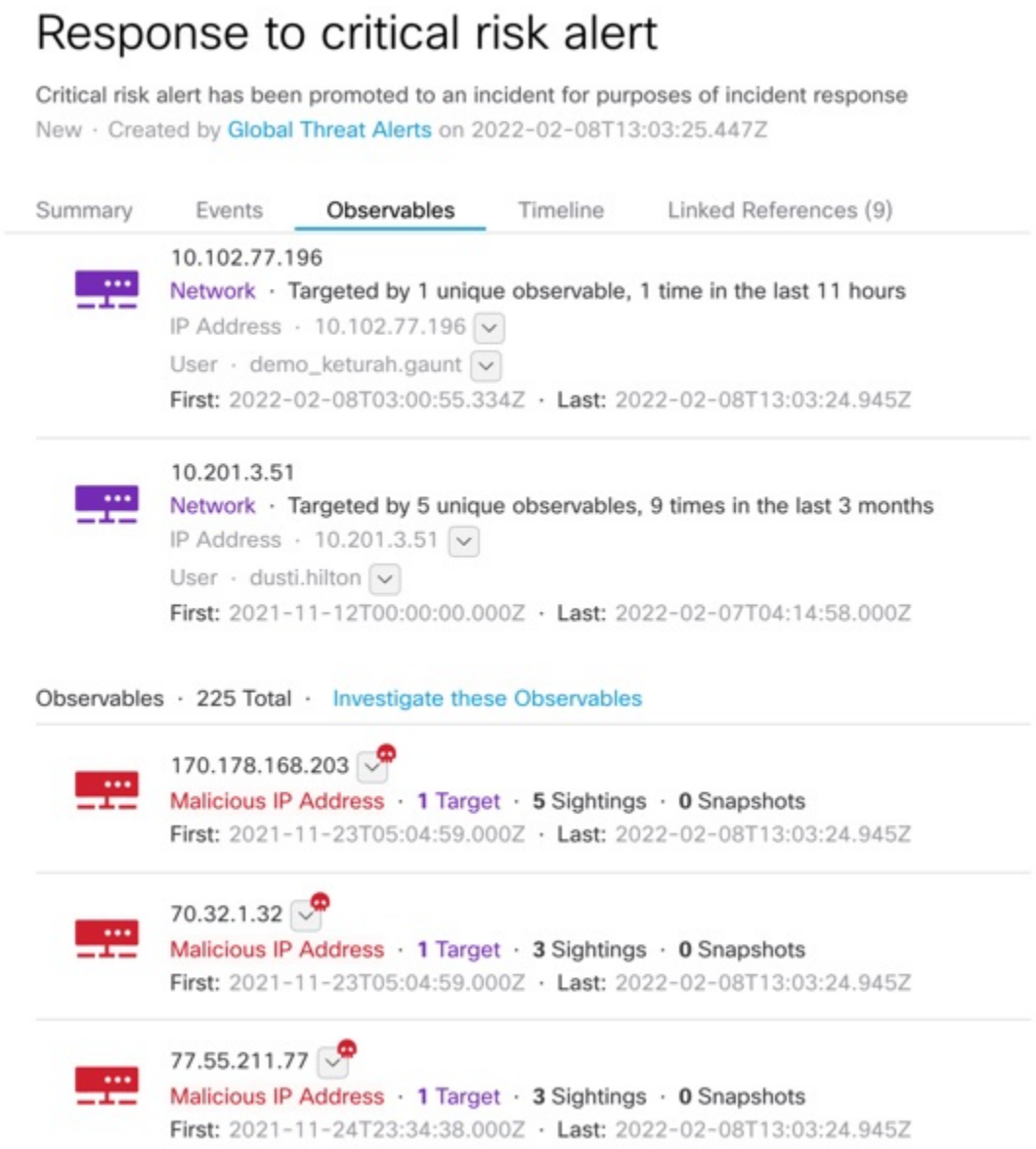
Figure 4: Accept Alert with Option to Link to Incident



In the SecureX incident manager, the incident contains details such as a **Summary** and all the security **Events** and **Observables** from the original alert. You can then investigate and respond further, using SecureX features such as investigation, enrichment, and orchestration.

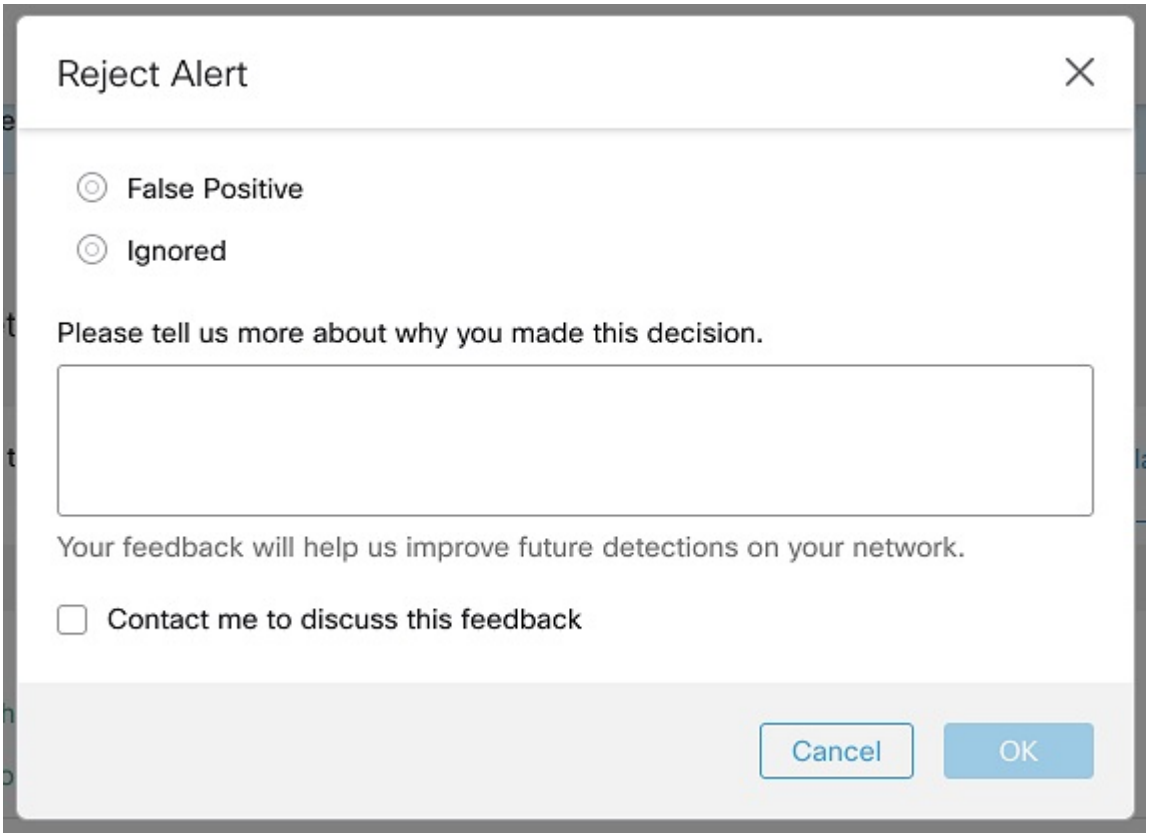
Figure 5: Example of Incident Summary

Figure 6: Example of Incident Observables



When it's undesirable to promote an alert as an incident, you can reject it. In this case, you can also provide feedback to the team at Cisco, telling us why you rejected the alert. Thank you, your valuable feedback helps us improve future detections on your network.

Figure 7: Reject Alert and Provide Feedback



Additional Threat Detections

We've added more new threat detections to our portfolio, including:

- IcedID
- Lemon Duck

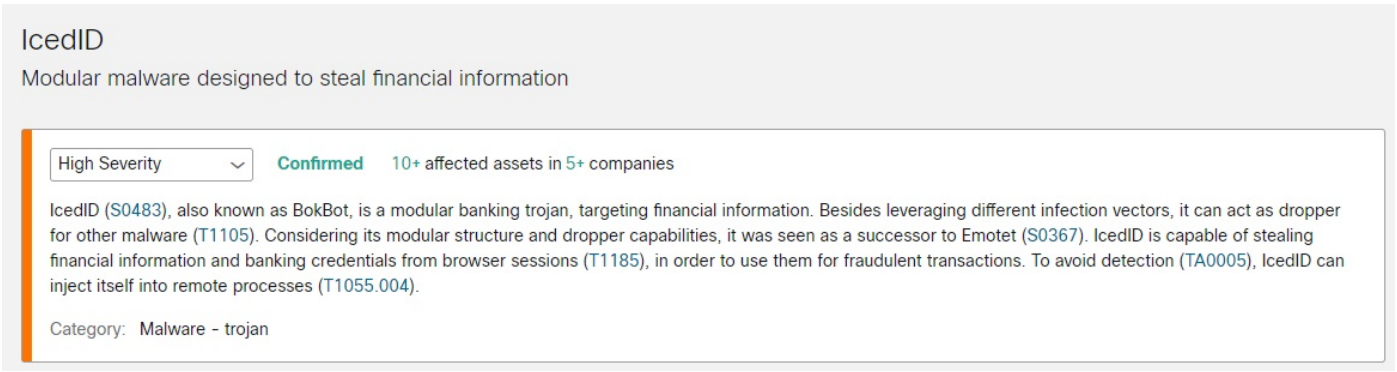
Numerous lower-risk threat detections have also been enriched.

IcedID

IcedID (S0483), also known as BokBot, is a modular banking Trojan, targeting financial information. Besides leveraging different infection vectors, it can act as a dropper for other malware (T1105). Considering its modular structure and dropper capabilities, it was seen as a successor to Emotet (S0367). IcedID is capable of stealing financial information and banking credentials from browser sessions (T1185), in order to use them for fraudulent transactions. To avoid detection (TA0005), IcedID can inject itself into remote processes (T1055.004).

To see if IcedID has been detected in your environment, click IcedID Threat Detail to view its details in global threat alerts.

Figure 8:



Lemon Duck

Lemon Duck is a file-less PowerShell malware family for mining cryptocurrency. This malware has been seen using EternalBlue exploits, pass-the-hash, and password brute-forcing to spread to other machines on the local network. Cryptocurrency miners use a large amount of CPU or GPU resources to mine cryptocurrency such as Bitcoin or Monero.

To see if Lemon Duck has been detected in your environment, click Lemon Duck Threat Detail to view its details in global threat alerts.

Figure 9: