Cognito® Platform Software Update

In August 2021, the Vectra® X-series appliances and S-series sensors were updated to Cognito® software release Version 6.10.

The Version 6.10 release introduces the Operational Metrics Report and an enhancement to the External Remote Access detection. Cognito® platform enhancements and bug fixes are also included in this release.

New Features

Operational Metrics Report — Cognito Detect for Network

Release 6.10 introduces the Operation Metrics Report. This report helps organizations to understand how effective their teams are in investigating suspicious events in their network. This report uses information from the Assignment Workflow feature which was released in 6.8.

Explicitly assigning entities and closing investigations with a label now allows the report to show how the organization is responding to different events. There is now a breakdown for three different metrics Time to Prioritize (TTP), Time to Acknowledge (TTA), Time to Respond (TTR). The report will also show how many events have occurred in the previous month and calculates averages of the metrics based on which label an assignment was closed with.

For this report to provide accurate information, the organization does need to adopt the Assignment Workflow feature.

Detection Enhancement: External Remote Access — Cognito Detect for Network

Vectra's External Remote Access detection finds attackers using custom protocols to remotely control hosts. In this release the coverage for attackers leveraging these types of command and control channels has been increased to better cover scenarios where the channel occurs over a network proxy. Customers may see a small increase in detection volumes as a result of this change.

Bug Fixes

CS-5070: Services setting page returning 500 error.

Fixes issue where the services setting page was returning a 500 error based on proxy configurations.