Home > Taegis Knowledge Base > Understanding Alerts and Alert Severity Levels

Understanding Alerts and Alert Severity Levels

tanyazehnder
Secureworks Employee

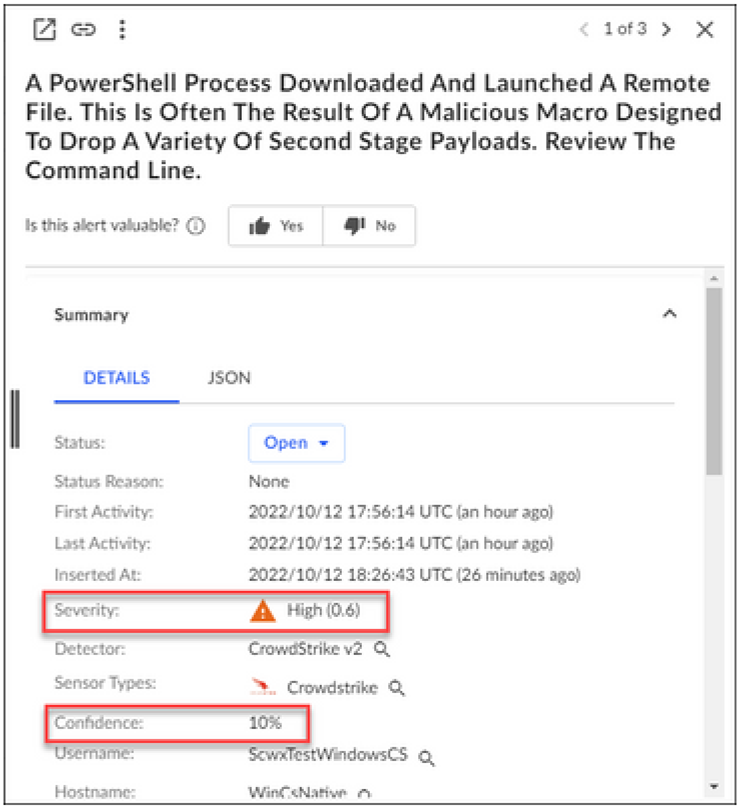
10-17-2022 04:06 PM - edited 10-26-2022 02:34 PM

Summary

Taegis™ XDR is responsible for creating security alerts from the telemetry sent from customer environments. This article describes the severity and confidence scores that Taegis XDR assigns to alerts it creates and how those values are calculated.

Solution

Alerts in Taegis XDR are created by detectors. Each detector is designed to identify certain types of malicious activity based on the security telemetry sent to Taegis from a customer's environment. Alerts generated by detectors have severity and confidence values assigned by the detector.



A PowerShell Process Downloaded And Launched A Remote File. This Is Often The Result Of A Malicious Macro Designed To Drop A Variety Of Second Stage Payloads. Review The Command Line.

Status: Open
Status Reason: None
First Activity: 2022/10/12 17:56:14 UTC (an hour ago)
Last Activity: 2022/10/12 17:56:14 UTC (an hour ago)
Inserted At: 2022/10/12 18:26:43 UTC (26 minutes ago)
Severity: High (0.6)
Detector: CrowdStrike v2
Sensor Types: Crowdstrike
Confidence: 10%
Username: ScwxTestWindowsCS
Hostname: WinCsNative

Severity and Confidence Scores

Severity and confidence scores make it easier for you to prioritize alert triage in your environment and address the most pressing alerts first. Find the severity and confidence for an alert in the Alert Details panel.

Severity

Severity is a measure of how much of a potential threat the activity poses to your environment. The severity score ranges from 0-1. The higher the score, the bigger the potential threat posed by the activity. Severities have the following ratings:

- Informational: < .2
- Low: >= .2 and < .4
- Medium: >= .4 and < .6
- High: >= .6 and < .8
- Critical: >= .8

When alerts are added to an investigation, the severity of alerts do not automatically affect the severity of an investigation. When a user creates an investigation, they can assign any severity value to that investigation (as well as change that severity later in their investigation). For example, multiple high severity alerts could be assigned to an investigation with critical severity. This allows an organization to recognize that a combination or pattern of alerts pose a larger risk than individual alerts present.

Confidence

Confidence is a measure of how confident our systems are that the alert is accurate and represents malicious activity. The confidence score ranges from 1%-100%. The higher the score, the more confident we are that the alert indicates genuine malicious activity.

How Are Severity and Confidence Determined?

Each detector collects varying data from your environment to monitor for malicious activity, and uses varying aspects of this data to determine a severity and confidence score.

For example, the DGA Detector is a machine learning model-based detector that computes the probability that a domain is an indicator of malicious activity. Both severity and confidence scores are based on the probability computed by the detector.

Other detectors define both severity and confidence statically, such as the Tactic Graphs™ Detector, which has a static severity and confidence score defined per adversary tactic. Similarly, Secureworks Taegis XDR watchlist detectors use a static severity and confidence score set by the security researchers who created the watchlist.

Third-Party Alerts

Third-party alerts ingested into Taegis XDR are interpreted for severity level and confidence differently depending on the originating device. In general, Taegis XDR maps the highest two severity levels of third-party alerts to High and Critical severity, unless the activity was blocked; Taegis XDR decreases alert severity for blocked activity to Low severity.

Resources

Alerts by Detector

Using the Alert Triage Dashboard

Alerts Detectors Informational Taegis XDR

0 Kudos

COMMENT

Powered by Khoros