Optimizing detections

Published: 2024-11-02

Here are some best practices you should implement to improve your detections: add details about your network, enable the ExtraHop system to see potentially-suspicious traffic, and filter your page view by your priorities.

Most of these settings provide context about your network that you can provide to enhance both machine-learning and rules-based detections—these settings are sometimes overlooked and can affect the quality of your detections.

Configure decryption

Encrypted HTTP traffic is a common vector for attacks, in part because attackers know the traffic is typically hidden. And if your network has Active Directory, a number of detections are hidden in encrypted traffic across the domain.

We strongly recommend that you enable decryption for TLS and Active Directory.

Configure Tuning Parameters

This setting improves the accuracy of rules-based detections. You provide the ExtraHop system with details about your network environment to provide context about the observed devices.

For example, a rules-based detection is generated when an internal device communicates with external databases. If traffic to an external database is expected or the database is part of a legitimate cloud-based storage or production infrastructure, then you can set a tuning parameter to ignore traffic to the approved external database.

Configure Network Localities

This setting enables you to classify internal or external endpoints that you trust, such as a CIDR block of IP addresses that your devices regularly connect to. Machine-learning detections and system metrics rely on device and traffic classifications.

For example, if your devices regularly connect to an unknown but trusted domain that is classified as an external IP address, detections are suppressed for that domain.

Create tuning rules

These settings enable you to hide detections after the system has generated them. If you see a detection that does not add value, you can reduce the noise from your overall view.

For example, if a detection is generated with an offender, victim, or other criteria that is not a concern for your network, you can hide all past and future detections with that criteria from view.

Share plaintext external data

This option allows the Machine Learning Service to collect IP addresses, hostnames, and domains that are associated with suspicious activity.

By enabling this option you add to a collective dataset of potential threats that can help you and the contribute to the security community.

Track detections

This option enables you to assign a detection to a user, add notes, and update the status from acknowledged to closed. Then, you can filter the Detections page to clear resolved issues from view or to check on detections.