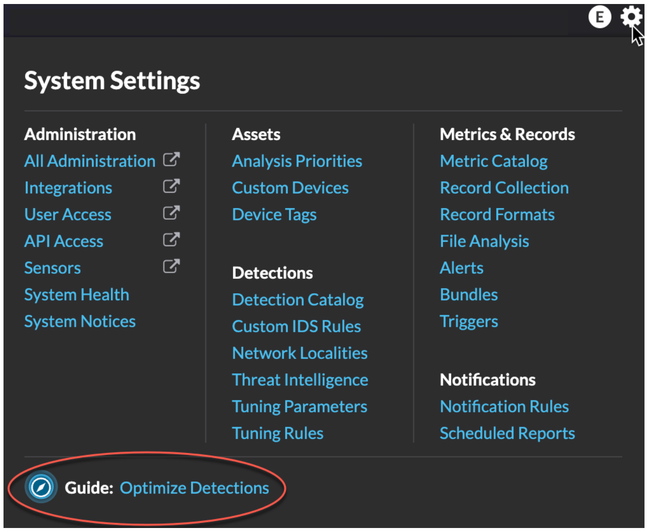
Optimizing detections

Published: 2025-04-05

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.

Tip: Click the System Settings icon ⚙ to open an in-product Detection Optimization Guide for additional information and resources. (NDR module only)



System Settings

Administration
- All Administration
- Integrations
- User Access
- API Access
- Sensors
- System Health
- System Notices

Assets
- Analysis Priorities
- Custom Devices
- Device Tags

Detections
- Detection Catalog
- Custom IDS Rules
- Network Localities
- Threat Intelligence
- Tuning Parameters
- Tuning Rules

Metrics & Records
- Metric Catalog
- Record Collection
- Record Formats
- File Analysis
- Alerts
- Bundles
- Triggers

Notifications
- Notification Rules
- Scheduled Reports

Guide: Optimize Detections

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.

High Value Devices

This setting helps you identify devices that are critical to your organization as high value. The ExtraHop system will automatically identify devices that provide authentication or support essential services as high value, but you can identify other critical devices manually.

For example, if you identify the laptop of an executive as a high value device, any detection involving the laptop will be recommended for triage, and any machine learning detection the laptop is involved in will receive an elevated risk score.

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.

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.

Notification Rules

These settings help automate communication within your organization and export detections to your next-gen SIEM. You create rules ↗ that send emails or call webhooks when events occur that are related to detections, recommended investigations, threat briefings, or other important system events.

For example, you can create a notification rule that sends a message to your team over Slack when a new threat briefing is published.

Security Operations Report

This setting helps you create a report ↗ that summarizes ExtraHop data related to detections, investigations, and network health.

For example, you can create a report that only contains information about open detections and investigations and is automatically delivered to your leadership on the first of every month.

Detection Research Team Access (RevealX 360 only)

This setting grants the ExtraHop Detection Research Team read-only access to your detections, metrics, and records to help improve the quality of detections.

IDS Module

This licensed module ↗ enables you to merge extended rule-based coverage of an IDS with the investigation and management workflows of your ExtraHop system.

For example, directly from the Detections page, you can filter, analyze, investigate, and tune detections based on cloud-updated Proofpoint ET Pro and ET Open rulesets.

Threat Intelligence

These settings enable you to add your own threat collections ↗ to default ExtraHop and CrowdStrike threat intelligence.

For example, you can configure a TAXII feed that you curate yourself or receive from a trusted third-party provider.

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 ↗.