

# What's New

Published: 2023-06-15

Version 9.3 of Reveal(x) includes several exciting new features, including NPM and NDR modules. Here's a quick overview of what we're announcing.

While [release notes](#) provide a comprehensive view of our release updates, here is a preview of our most exciting features in ExtraHop 9.3.

## ExtraHop Modules

Introducing modules in the ExtraHop system for Network Detection and Response (NDR) and Network Performance Monitoring (NPM), with additional modules for Intrusion Detection Systems (IDS) and Packet Forensics.

Administrators can [grant users role-based access](#) to the NDR module, NPM module, or both.

## Reveal(x) 360

- Identity Provider
  - ExtraHop
- System Access
  - System and access administration
  - System administration
  - Full write
  - Limited write
  - Personal write
  - Full read-only
  - Restricted read-only
- NDR Module Access
  - Full access
  - No access
- NPM Module Access
  - Full access
  - No access
- Packet and Session Key Access
  - Packets and session keys
  - Packets only
  - Packet slices only
  - No access

## Reveal(x) Enterprise

User Privileges

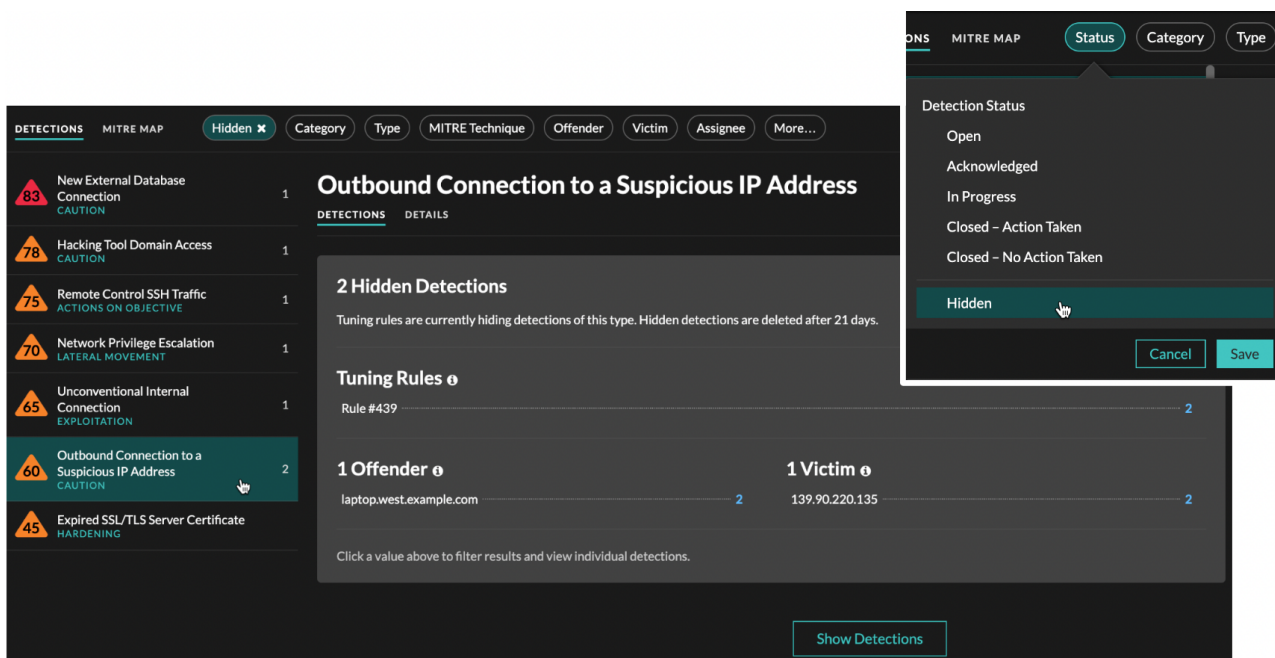
System and access administration

Limited privileges

System Access	NDR Module Access	NPM Module Access	Packet and Session Key Access
<input type="radio"/> Full write <input checked="" type="radio"/> Limited write <input type="radio"/> Personal write <input type="radio"/> Full read-only <input type="radio"/> Restricted read-only <input type="radio"/> No privileges	<input checked="" type="radio"/> Full access <input type="radio"/> No access	<input type="radio"/> Full access <input checked="" type="radio"/> No access	<input type="radio"/> Packets and session keys <input type="radio"/> Packets only <input type="radio"/> Packet slices only <input checked="" type="radio"/> No access

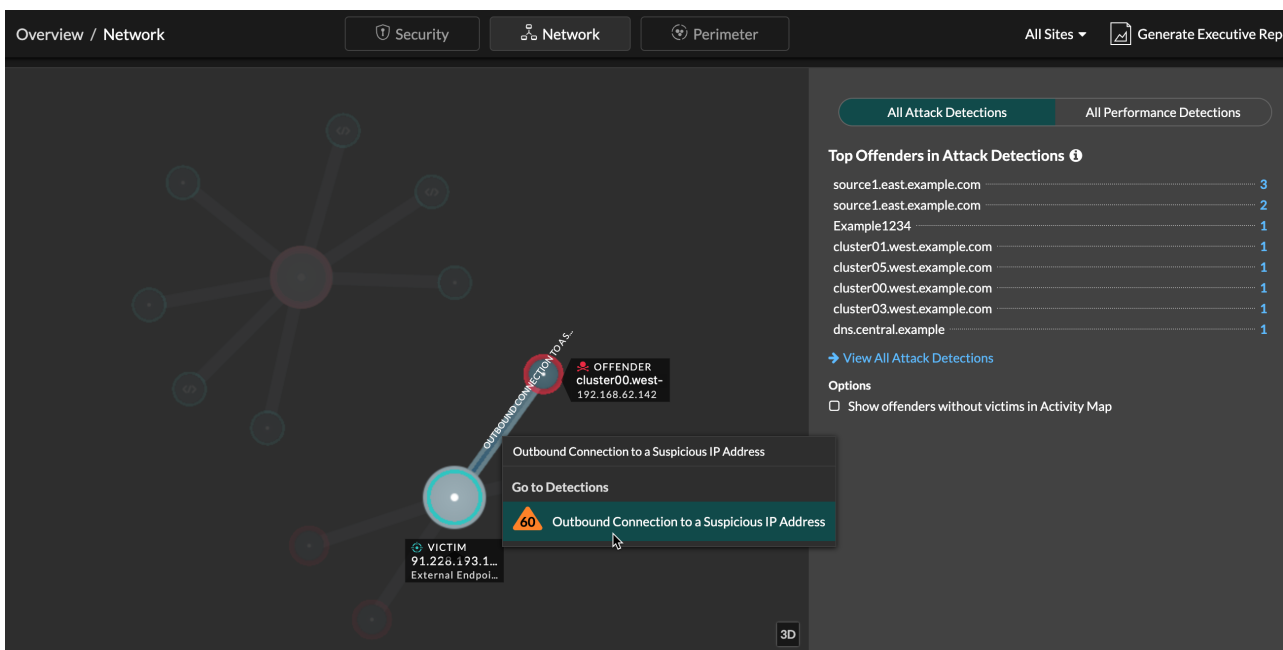
## Detections

On the Detections page, you can now apply the Hidden status to [view only detections that are currently hidden](#) by a tuning rule.



## Network Overview

The [Network Overview page](#) now displays a map of the detections on your network and a list of the top offenders by detection count.



## Reveal(x) 360

You can integrate with CrowdStrike Falcon LogScale to export Reveal(x) 360 security detections.

Administration / CrowdStrike Falcon LogScale Integration

### CrowdStrike Falcon LogScale Integration

Integrate ExtraHop Reveal(x) 360 with CrowdStrike Falcon LogScale to view network threat detections and behavioral insights in LogScale.

With this integration you can export security detections from Reveal(x) 360 to LogScale to view detection data in a centralized system, enhancing context around detections and decreasing the time to confirm threats.

#### Integration Features

- ✓ Export Reveal(x) 360 detections

[Go to Integration Documentation](#)

Status: ● Integration Enabled

[Send Test Event](#)
[Change Credentials](#)
[Disable Integration](#)

#### Integration Options

Export Reveal(x) 360 security detections

Specify criteria to determine which detections to export. If no criteria is specified, all new detections are exported.

Category = All Attack Detections ✕

Add Criteria ▾

[Save](#)

You can now configure [email notifications](#) for metric alerts. Add one or more email addresses to an alert configuration to generate email notifications when the alert condition is met.

## Create Alert

**Name**

**Author**

**Description**

**Alert Type**

**Assigned Sources**

**Monitored Metric**  
  
 divided by

Ratio

**Alert Condition**  
 Value during the last  is

**Alert Behavior**  
 Alert once when alert condition is met  
 Alert every  while alert condition is met

**Severity**

**Notifications**

**Options**  
 Enable alert  
[Show Advanced Options](#)

**Actions**  
[Copy Alert](#)

Reveal(x) 360

## HTTP errors on responses

April 28, 2021 09:18:30 UTC-08:00

**Severity:** Error

**Description:**  
Triage level 3

**Alert Value:** 2  
**Monitored Metric:** HTTP Server Errors / HTTP Server Responses  
**Alert Condition:** Count during last 30 seconds is ≥ 1

**Alert Source**

workstation-12  
 10.10.6.155  
 MAC: 77:DC:1A:66:93:1F  
 Site: corp-sea-01

[View Alert Source](#)

You can now [create and edit scheduled dashboard reports](#) from System Settings.

## Create Dashboard Report

**Properties**

**Report Name**  
System Usage

**Description**

**Owner**  
shellie

**Report Contents**  
Select a dashboard...  
Dashboard: System Usage

**Schedule**

**Time Interval**  
Last

**Report Frequency**  
 Hourly  Daily  Weekly

At

On  M  T  W  Th  F  S  Su

[Add Schedule](#)

**Format**

**Style**

**Theme**  
 Dark  Space  Light  Contrast

**Send Email**

**Recipients**

**Subject**  
 Automatic  Custom

### For Administrators

[Migrate existing users](#) to grant role-based access to your licensed module

Reveal(x) Enterprise and Reveal(x) 360 administrators can configure endpoint lookup links to external IP address tools. When you click or hover over an IP address within the ExtraHop system, lookup links are displayed.

### Endpoint Lookup

Display links to an external IP address lookup tool for endpoints in the ExtraHop system by typing the URL of the tool. The URL must include the \$ip variable, which is replaced with the IP address of the endpoint.

**URL Template**

**Display Name**

**Display Options**

Show this link on all endpoints  
 Show this link on external endpoints  
 Show this link on internal endpoints  
 Do not show this link

**URL Template**

**Display Name**

**Display Options**

Show this link on all endpoints  
 Show this link on external endpoints  
 Show this link on internal endpoints  
 Do not show this link

[Add Endpoint Lookup Link](#)

**workstation-08**  
 1192.168.2.2  
 Site: seattle-branch

---

Apple MacBook Pro (13-inch, 2017)  
 PC

---

**Software**  
 MacOS

---

**Users**  
 emily@workgroup

---

First Seen 6 months ago Oct 25 18:15  
 Last Seen just now Apr 25 14:33

---

**Go To**

- [ARIN Whois Lookup](#)
- [VirusTotal Lookup](#)
- [Detections](#)
- [Activity Map](#)
- [Records](#)
- [Packets](#)

[Go to Device Overview](#)

Added a [10 Gbps IDS virtual sensor](#).

### For API Developers

You can now [manually update ExtraHop system resources](#) with the [POST /extrahop/cloudresources operation](#). These resources are automatically updated when the system is [connected to ExtraHop Cloud Services](#).