ExtraHop

Automated Retrospective Detection with ExtraHop Reveal(x) 360

Reveal the Unknown. Unmask the Attack.

Introduction

With Automated Retrospective Detection, reveal the unknown and unmask past attacks by instantly applying threat intelligence to historical records. Detect malware and zero-day exploits that were missed before threat intelligence was published. No need to waste time manually searching and waiting for an attacker's next move, Automated Retrospective Detection searches for the latest indicators of compromise (IOCs) in your historical records so you instantly know if you've been hit.

How do you know if you've been compromised?

When news of the SolarWinds SUNBURST attack broke on December 13, 2020, security teams across industries were dealt the arduous task of determining whether their organizations were affected by it.

Analysis of new network data wouldn't show signs of the initial malware compromise; it would only show signs of a new SUNBURST attack. To figure out if the SUNBURST malware was already on their organizations' systems, security analysts and investigators needed the ability to look for indicators of compromise (IOCs) in older network data.

No one could quickly get to the ground truth and confidently answer the big question: have we been hit? They lacked a quick, easy and cost effective way to automatically search through past network data for IOCs indicating they had already been infected with the malware. It took organizations weeks to determine if they had been impacted.

Benefits of ExtraHop ARD

- Mitigates business risk by accelerating detection and investigation.
- Closes security gaps with precision detection of past attacks and behaviors.
- Automates threat hunting and detection; eliminates the grueling work of running manual queries against threat intelligence feeds.
- Provides relevant and actionable intelligence at scale

> Automated Retrospective Detection automatically triggers detections based on historical records. This capability eliminates a significant blind spot for customers, enabling them to see more, know more, and stop more threats.

Automatically search for IOCs through past network data

ExtraHop now offers Automated Retrospective Detection (ARD), an included feature of Reveal(x) 360, at no additional cost. ARD produces detections based on a huge amount of the most up-to-date threat intelligence by automatically searching historical network data in the ExtraHop Reveal(x) 360 cloud record store for related IOCs. Instead of waiting for the security team to check historical records or waiting for the security tool to detect an attacker's next move, Automated Retrospective Detection automatically triggers detections based on historical records. This capability eliminates a significant blind spot for customers, enabling them to see more, know more, and stop more threats.

ARD automatically correlates new IOCs from threat intelligence data with packets and all other historical network activity to quickly spot threats that previously slipped past other security tools. ARD continually assesses and verifies the security of an organization's network as soon as new IOCs are ingested. It lets security teams know whether their organization was compromised before IOCs were available and allows organizations to catch past compromises.

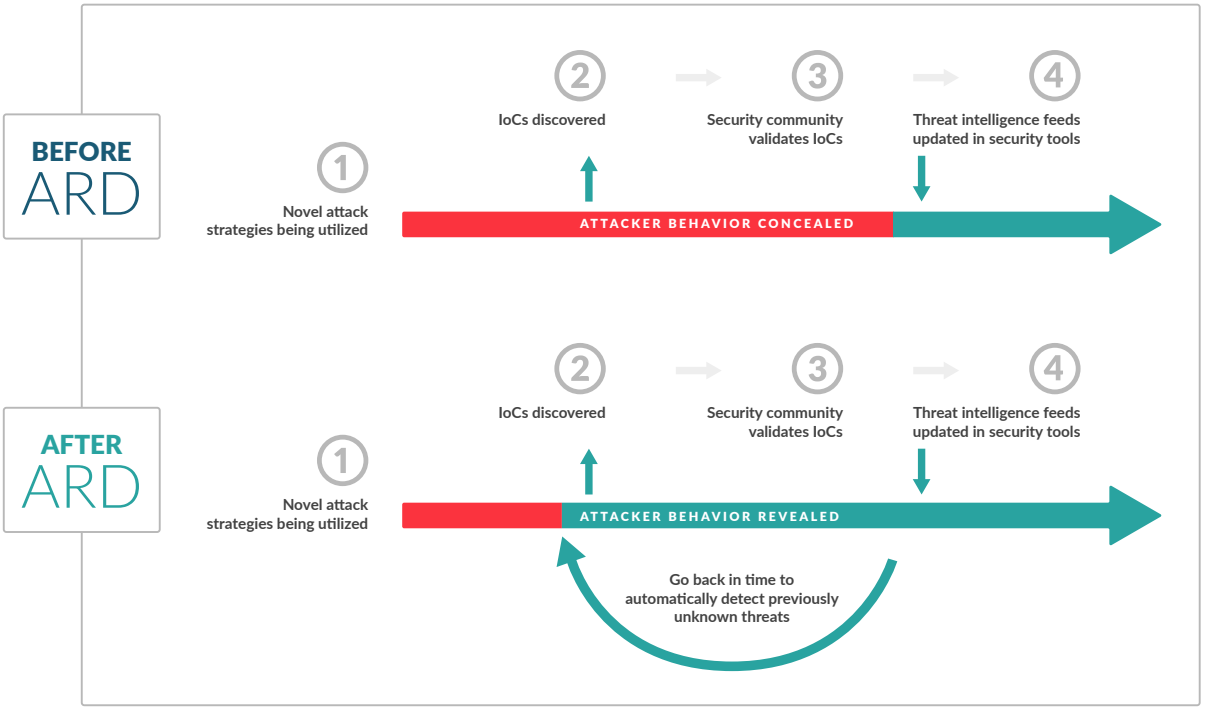
With ARD, analysts no longer have to pick and guess which new IOCs may be worth manually searching for among the thousands in a threat intelligence feed. In many cases, security teams must conduct these cumbersome manual searches during an active emergency, but with ARD, they can drastically reduce threat research time and instead, focus on responding.

As soon as threat intelligence is updated, analysts automatically know if a new IOC is relevant and if it was ever spotted on the network. ARD provides analysts with high-fidelity, correlated, contextualized alerts right away. ARD pinpoints threats and affected machines, resulting in faster detection, investigation, and response. Moreover, automated queries that search for past compromises unburden analysts and improve SOC productivity. And by providing historical coverage, correlation and automation in one tool, Reveal(x) 360 offers security leaders new opportunities to simplify their complex security tech stacks and reduce costs.

Automated Retrospective Detection: How It Works

Reveal(x) 360 combines three powerful and differentiated capabilities to deliver ARD: a curated threat intelligence feed, the Reveal(x) 360 cloud record store, and a cloud analytics engine able to automate querying while continuously analyzing network traffic using AI/ML. The cloud analytics engine with query automation, the record store, and threat intelligence all ingest to a single platform with no limitations or constraints around deployment model (for example, cloud, on-premises, or hybrid).

The record store, because it's hosted in the cloud, provides the cost-efficient elasticity and scalability required to store historical network packets and related telemetry. Meanwhile, the cloud-scale machine learning capabilities built into Reveal(x) 360 are capable of continuously analyzing billions of events to cut through the noise, eliminate false positives, and pinpoint and prioritize relevant threats.



Stop Advanced Threats with Reveal(x) 360

ExtraHop has opted to offer ARD at no additional cost because it's that important to improving organizations' network and threat visibility. It's one of many reasons ExtraHop is the industry leader in Network Detection and Response, outpacing the market compound annual growth rate (CAGR) over the last two years. Our flagship products, Reveal(x) Enterprise and Reveal(x) 360, were named in the 2022 Gartner® Market Guide for Network Detection and Response and the Forrester Network Analysis and Visibility Landscape, Q1 2023. Both bolster network intelligence, performance, intrusion detection, and response—all in one solution.

We continue to expand strategic partnerships and integrations with leading security providers, including CrowdStrike, Splunk, and Palo Alto Networks. Both Crowdstrike and Extrahop are members of the CrowdXDR Alliance and together empower extended detection and response (XDR) capabilities to automatically quarantine impacted devices with a single click.

Automated Retrospective Detection At a Glance

The challenge:

Organizations lack the ability to automatically re-run detections on old network data in search of novel malware and zero day exploits that their other tools may have missed because those tools lacked IOCs.

What is Automated Retrospective Detection?

ARD is a feature of ExtraHop Reveal(x) 360 that produces detections by automatically correlating the latest IOCs from a massive threat intelligence feed with organizations' historical network data.

Benefits:

- Eliminates the need to manually search for IOCs in historical records during active attacks
- Automatically uses the latest threat intelligence to determine whether you were protected in the past
- Helps accelerate identification of broad attack campaigns and minimize dwell time

	Threat Intelligence	Threat Intelligence with ARD
Protection going forward	✓	✓
Automated IOC detection	✓	✓
Detection of past compromises	✗	✓
Automated record queries	✗	✓
Faster MTTD, MTTI, MTTR	✗	✓
APT protection	✗	✓
Reduced dwell time	✗	✓
Proactive detection	✗	✓

Ask your security team

- How do you make sure your organization hasn't already been hit by a new 0-day when it gets announced?
- How confident are you that you haven't already been hit by an attack that just got added to your threat intelligence feed?
- How would your security team figure this out?
- How long does it take your team to search for an indicator of compromise in previous records?

version 1.1 - 04.18.2023

ABOUT EXTRAHOP NETWORKS

ExtraHop is the cybersecurity partner enterprises trust to reveal the unknown and unmask the truth. The company's Reveal(x) 360 platform is the only network detection and response solution that delivers the 360- degree visibility needed to uncover the cybertruth. When organizations have full network transparency with ExtraHop, they see more, know more and stop more cyberattacks.
Learn more at www.extrahop.com

ExtraHop
info@extrahop.com
www.extrahop.com