ExtraHop

WHITE PAPER

Response Automation with Reveal(x)

How Reveal(x) Amplifies the Effectiveness of Your Security Toolset

This white paper explains how ExtraHop Reveal(x) works with your existing investments to enable robust incident response, including fully automated responses that block and quarantine threats, as well as support for augmented manual investigation. ExtraHop uses an integration-driven approach to response automation, working with the response solutions your security team has already—including security orchestration and automation (SOAR) products, ticketing systems, network access control, and firewalls.

TABLE OF CONTENTS

Executive Summary

Security teams are expected to run lean operations while also minimizing the time to remediate incidents. This requirement to do more with less has meant relying more on automation. In fact, according to a recent SANS survey, security leaders said that automated response is one of the most desired technologies. But at the same time, one of the technologies that those same leaders were most disappointed by was SOAR (second only to artificial intelligence). So while there is an appetite for automation, existing solutions are not meeting expectations.

It's clear that there is demand for a coherent approach to automating responses to threats, but there's not yet a consensus on how to go about it. While SOAR is an important piece of the puzzle, it's not the complete solution. It's incumbent on network detection and response (NDR) vendors to provide supported integrations and customizability options to enable the appropriate approach for each situation.

ExtraHop has listened to market demands and understands that organizations want their solutions to integrate and work seamlessly together. Reveal(x), the market-leading cloud-native NDR product, offers several out-of-the-box integrations, along with the flexibility to create unique customized solutions.

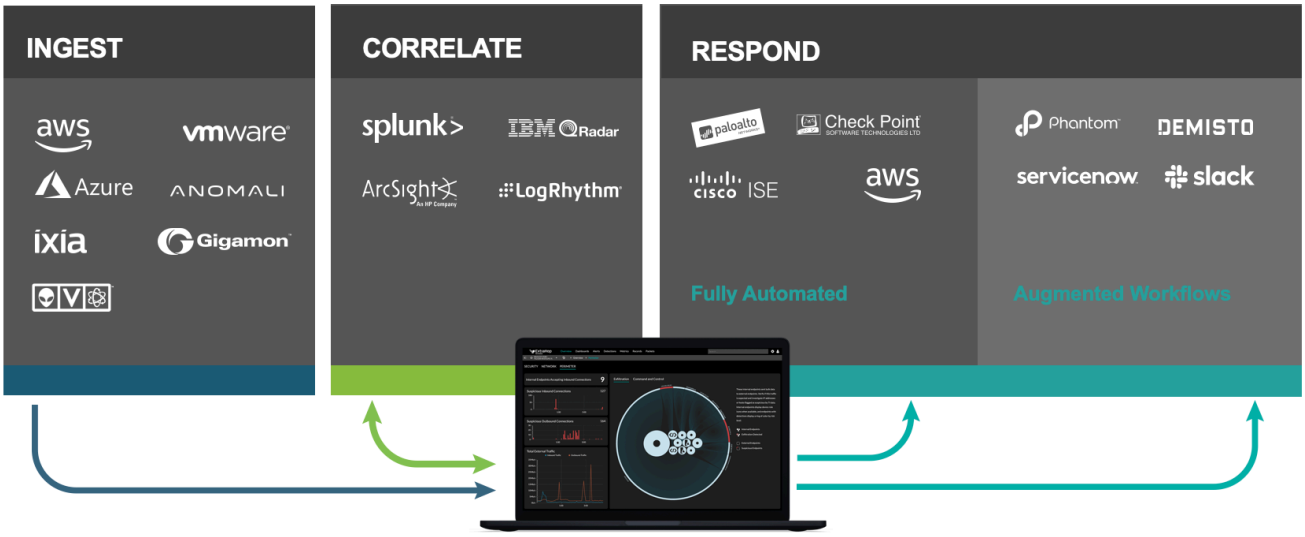

Figure 1. *Reveal(x) offers out-of-the-box integrations with a number of security technologies to help streamline investigation and remediation, including integrations that fully automate remediation.*

Why NDR Integration Matters

Deploying an NDR solution is arguably the most significant single step a security team can take to understand and monitor what's happening in and on an organization's network. An NDR doesn't require installation on all endpoints, and there's no manual tuning, configuration, or logs to read. With a single solution, security analysts can monitor the activity of every device on the network, managed or unmanaged. It's like a closed-circuit security camera for your data center.

As the brains of your security toolset, the NDR applies a spectrum of techniques to detect activity at every stage of the attack lifecycle. NDR also uniquely tracks attackers' activity after they have compromised your environment and are inside your perimeter. In these cases, NDR serves as a vital layer of defense to detect activity such as internal reconnaissance, privilege escalation, and data collection and exfiltration.

But even in the best implementations, NDR can't work in isolation—your NDR solution has to integrate with your current security toolset to be most effective. Your security teams will still work in the SIEM to do triage and manage their queues. And you will continue to depend on the tools you've already installed to remediate threats, such as firewalls and network access control (NAC) systems. Your NDR solution needs to work with all these systems to facilitate seamless responses that are appropriate to the threat.

To give a more concrete example: During an investigation, your security analysts rely on SIEMs to examine log data; endpoint detection and response (EDR) solutions to look at data collected from the endpoints; and NDR solutions to analyze network data. They'll use chat tools and ticketing systems to collaborate with other team members and across security operations and IT operations teams. You need to ensure all of those solutions are integrated to reduce costs and to reduce the "swivel chair" effect where analysts need to correlate data across platforms manually.

Reveal(x) Integrations for Response

With Reveal(x) always on and monitoring, threat responses can be triggered immediately to enable both immediate, fully automated responses as well as augmenting manual investigation and remediation. Reveal(x) is engineered to "play nice" with every component of your security workflow, offering both out-of-the-box and custom integration options for firewalls, SIEM systems, and more.

Fully Automated Responses

Some threats are "fast and destructive," meaning that they do a significant amount of damage before a human incident response team can mobilize. For example, the WannaCry and NotPetya ransomware attacks in 2017 took advantage of a vulnerability in the legacy SMB1 protocol to spread automatically in a worm-like manner. Within a day of the initial infection, the WannaCry worm had infected more than 230,000 systems in 150 countries. It was only stopped because a security researcher found and activated a "kill switch." Damage estimates range from several hundred million dollars to $4 billion. These incidents heightened awareness of organizations' need for fully automated response to mitigate these types of rapid, machine-driven attacks.

Reveal(x) supports the automated response required to stop fast and destructive attacks like these with the ability to send REST API calls to firewalls, NAC, and EDR solutions based on specified classes of detections. For example, detections of ransomware with a high risk score would be good candidates to trigger an automated response. Supported integrations are developed and tested by ExtraHop.

Reveal(x) users can also create their own custom integrations using the Reveal(x) REST API to send detection and contextual information to other systems. These custom integrations are often shared within the ExtraHop user community as downloadable bundles. The ExtraHop Solution Bundles Gallery lists both supported and custom bundles.

Supported Response Integrations

ExtraHop supports several response integrations, right out of the box.

- **Firewall:** Reveal(x) offers supported integrations with the Palo Alto next-generation firewall so that customers who use them can automatically block malicious IPs and domains.
- **Network access control:** In the event of a threat, the system can quarantine devices on the internal network, lock users, or otherwise restrict network access through the Reveal(x) supported integration with Cisco Identity Services Engine.

	Name	Source		Destination	Action
		Address	User	Address	
10	Quarantined Devices Outbound	Quarantined Devices	any	any	Deny
11	Quarantined Devices Inbound	any	any	Quarantined Devices	Deny

Figure 2. *The Reveal(x) integration with Palo Alto's NGFW applies policy rules to block traffic to and from those devices.*

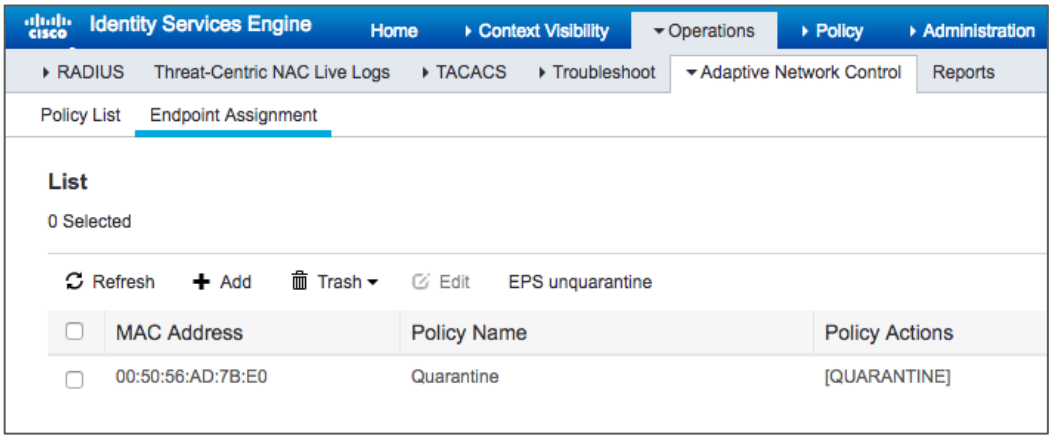

Figure 3. *Example quarantine policy applied to an endpoint in Cisco ISE based on a detection from ExtraHop Reveal(x).*

Augmented Manual Response Workflows

Many attacks are "low and slow" and require analysts to validate detected anomalies and then initiate the incident response process rather than relying on a fully automated response. For example, Reveal(x) may detect behavior that looks like internal reconnaissance. This type of behavior may be malicious, but it could also be legitimate scanning activity. This requires a trained analyst to consider the context and make a decision about next steps. As security expert Bruce Schneier writes, "You can only automate what you're certain about, and there is still an enormous amount of uncertainty in cybersecurity."

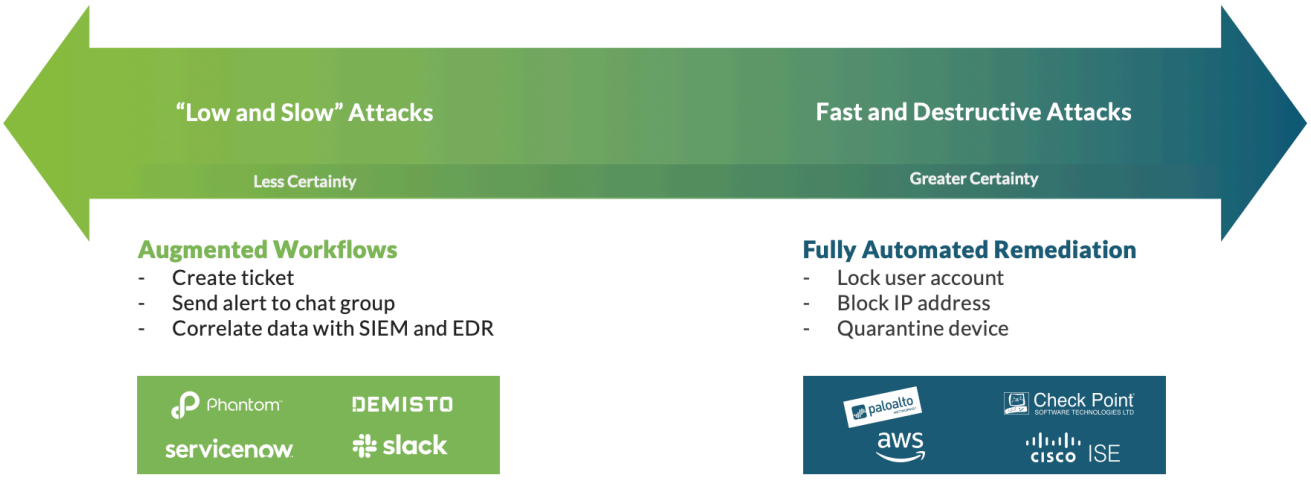

Figure 4. *Reveal(x) works with a number of security products to enable either augmented workflows or fully automated responses.*

In cases where a human needs to be in the response loop, Reveal(x) integrates with SOAR platforms, collaboration tools, and ticketing systems that organizations currently have in place to support augmented response workflows. Not only does Reveal(x) send alerts to the appropriate tools, it can also speed investigations by presenting contextual information, such as:

- A timeline of related detections for the same offender or targets
- Details for the devices involved, including whether they are internal or external to the network
- Links to associated metrics or transaction records, such as the files read or user account logins attempted
- Recommended next steps for investigation
- Third-party information about the vulnerability or attacker tactic, technique, or procedure (TTP)
- The status and assignee of the associated ticket

This ensures the security analyst has the information needed to validate the alert. Reveal(x) helps security teams get closer to certainty as quickly as possible.

Supported Augmented Manual Workflow Integrations

- **SOAR:** Security orchestration, automation, and response technologies such as Demisto and Phantom promise to speed up response workflows, tying together various security and collaboration tools and automating runbooks. Where these solutions are present, Reveal(x) can act as the always-on eyes and ears of the security operations center (SOC) and provide high-quality detections to kick off fully and partially automated workflows.
- **ChatOps:** Reveal(x) can send information about detections to Slack or other collaboration platforms through a REST API. For organizations that rely on these chat platforms to coordinate workflows, especially when they involve multiple teams, this integration can help team members arrive at a common understanding of an event and its severity.
- **Ticketing systems:** Reveal(x) integrates with ticketing systems such as ServiceNow, automatically creating tickets for analyst triage queues. In turn, Reveal(x) can ingest ticket information to display beside a detection, showing the assigned ticket number, analyst, and status.

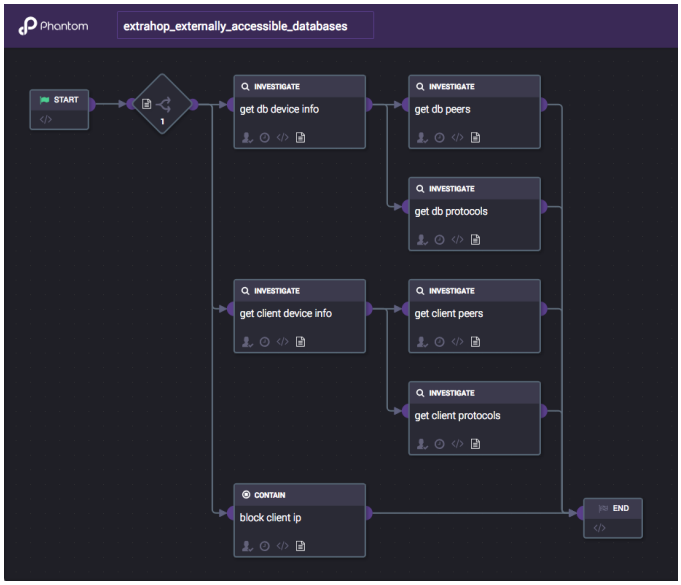

Figure 5. *Response workflow template from the Splunk Phantom integration with ExtraHop Reveal(x).*

Investigation Integrations

During investigations, analysts need instant access to information so they can make decisions quickly—whether validating an alert, pursuing a threat hunting hypothesis, or determining the scope of a data breach. You can improve the productivity of your security teams in the SOC by making it easier to correlate data from various systems. Analysts primarily rely on three data sources to understand security events, each with their pros and cons—logs, endpoint data, and network packet data. Reveal(x) integrates with SIEM systems to reduce the friction of correlating data from various sources.

Log Data	*Endpoint Data*	*Wire Data*
Logs are a mainstay of security operations and function as shorthand notes of actions performed on a system, taken by the system itself. One drawback to depending on log data for threat analysis is that attackers can turn off logging and erase or modify logs. IT operations and applications teams sometimes prefer not to log certain performance-sensitive systems such as databases, or at least not turn on verbose logging.	Endpoint data provided by an EDR solution is necessary for any layered defense and can provide valuable insight into what users and software are doing on systems. Visibility into internal processes cannot be obtained in any other way. The downside is that EDR agents can be easily disabled, and they cannot provide context about the broader attack campaign.	Network packets are recognized as the ground truth. Some in the security industry say, "Packets or it didn't happen," meaning that packet capture is required to prove that an exploit or attack behaved in a certain way. Passive network analysis is also the most challenging method of defensive observation for attackers to evade or circumvent. Wire data does not provide visibility into internal processes on the endpoint.

Supported Investigation Integrations

SIEM: SOC analysts spend most of their time in the SIEM, the system that collects and correlates telemetry and event data from throughout the enterprise in a single place. Reveal(x) can stream any data to SIEM systems to correlate with log data collected there. Many customers use Reveal(x) to obtain information that would otherwise be impractical to get from logs, such as database transaction and DNS request details that are often not logged for overhead and cost reasons. Reveal(x) can summarize that data before sending to the SIEM to reduce storage costs.

Reveal(x) supports two-way integrations for Splunk and IBM QRadar that enable security analysts to click from the SIEM back into Reveal(x) and view activity maps, search transaction records, or download packet details. Customers have also developed custom integrations for ArcSight and LogRhythm.

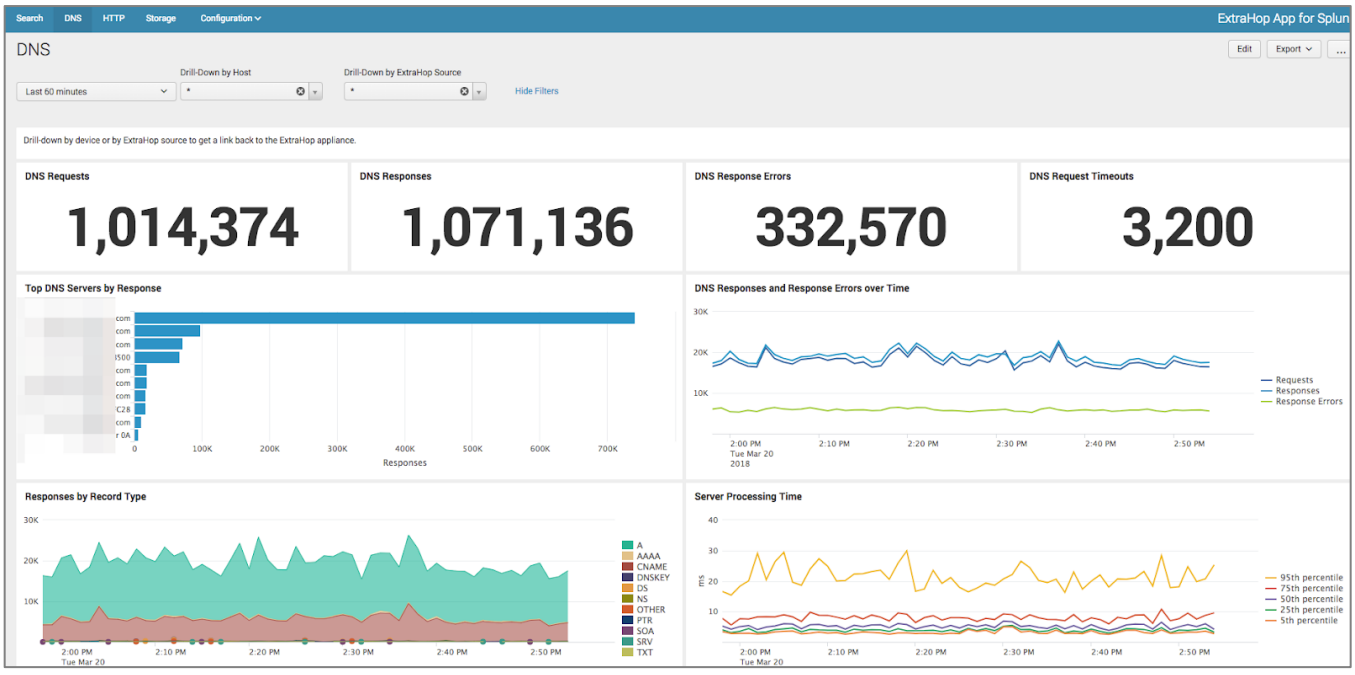

Figure 6. *ExtraHop App for Splunk*

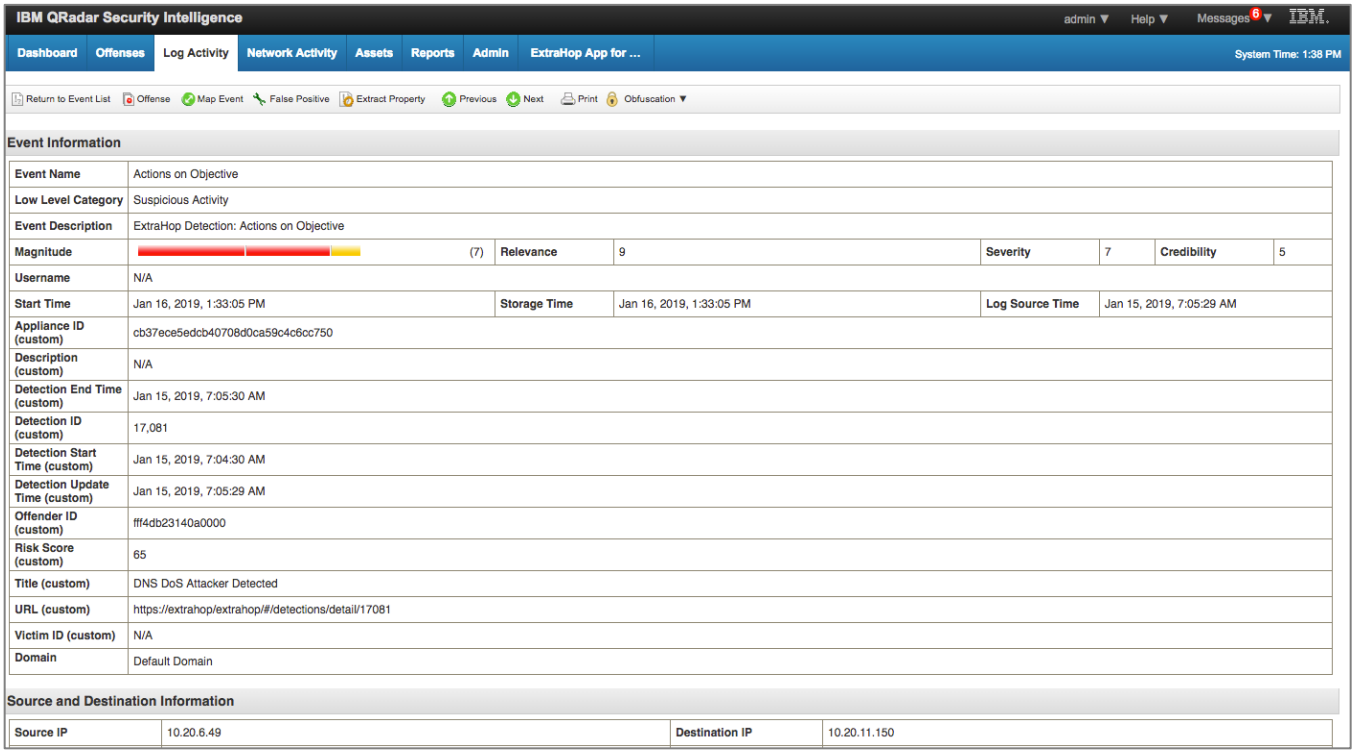

Figure 7. *ExtraHop App for IBM QRadar*

Data Source Integrations

Reveal(x) integrates with a variety of infrastructure platforms and technologies to receive data for analysis.

Supported Data Source Integrations

- **AWS and Azure:** Reveal(x) integrates with AWS CloudTrail and CloudWatch and Azure Security Center to receive telemetry and event details in the public cloud. That information is used to enrich Reveal(x) analysis. With a unified analytics and investigation environment that spans the entire hybrid attack surface, SOC teams can confidently manage cloud risks, detect threats quickly, and respond before the business is affected.
- **VMware:** Reveal(x) works with the vRealize Operations Manager to quickly deploy in hyper-converged and other virtual environments and obtain packet data between virtual hosts inside those environments.
- **APCON, Arista, Big Switch, Gigamon, Ixia:** Reveal(x) works with network packet broker solutions to obtain de-duplicated traffic feeds from throughout large, complex enterprise environments.
- **Threat intelligence:** Reveal(x) takes in threat intelligence feeds in the STIX format to match malicious IP addresses and domains observed during analysis. These matches and the contextual threat intelligence are highlighted in Reveal(x) visualizations, transaction metrics, and records.

Examples of NDR Integrations

An NDR solution that is integrated with existing security systems provides critical capabilities to help speed up the fight against attacks, breaches, and simple human error. Here are some scenarios to show how Reveal(x) works on the front lines.

Fully Automated Response Example – Ransomware Infection

In the ordinary course of business, with always-on network traffic analysis, ransomware activity is detected by Reveal(x). Since the organization has integrated Reveal(x) with its NAC solution, this category of detection automatically quarantines the infected device. Immediately alerted, the SOC team uses Reveal(x) to ascertain the initial point of compromise and what other devices in the environment might be infected. An automated response coupled with quick action saves the organization weeks of headaches and potentially devastating loss of data.

Augmented Manual Workflow Example – Privilege Escalation

Reveal(x) automatically discovers and classifies everything communicating both across and within the network and uses advanced behavioral analysis to detect anomalous behavior and threats against critical assets. In this example, Reveal(x) detects a developer workstation accessing critical assets with higher levels of privilege than it usually does. This detection shows up in the team Slack channel, and an analyst can quickly investigate to determine what caused the anomalous activity. It turns out that a developer was pulling an image from an ESXi server using a different mechanism than usual, but it was not a malicious event.

Summary

It's no secret that speed is one of the most important elements of incident response. Reveal(x) not only detects attacks, it integrates with your existing systems to allow you to streamline or even fully automate your emergency responses, minimizing business disruption and limiting privacy violations.

Network detection and response (NDR) products are a vital layer of defense in detecting suspicious activity at every stage of the attack lifecycle. Many security teams realize that an NDR solution should work in concert with other security systems to automate threat response at every stage of the attack lifecycle. However, enabling automated response should not require that you purchase and deploy an entirely new technology. Instead, the ideal NDR solution integrates seamlessly with existing defenses, like firewalls, security information event management (SIEM) tools, and other network access control (NAC) products.

Adding network detection and response capabilities is one of the most significant steps an organization can take to detect threats that may have bypassed traditional defenses. By integrating the Reveal(x) NDR with an existing security portfolio, an organization can dramatically speed up the response to newly detected threats with appropriate level of human interaction. Reveal(x) offers both supported, out-of-the-box NDR integrations, as well as the ability to create customized solutions that meet individual organizations' unique needs.

ABOUT EXTRAHOP
ExtraHop is the first place IT turns for insights that transform and secure the digital enterprise. By applying real-time analytics and machine learning to all digital interactions on the network, ExtraHop delivers definitive insights and instant answers that help IT improve security, performance, and the digital experience.

ExtraHop Networks, Inc.
520 Pike Street, Suite 1600
Seattle, WA 98101 USA

http://www.extrahop.com/
info@extrahop.com
T 877-333-9872
F 206-274-6393