ExtraHop + aws

FEATURED INTEGRATION

Automated Remediation with Endless Possibilities

Take automated action on compromised instances. You set the policy, Reveal(x) Cloud helps stop the threat.

Take control of your cloud incident response with the new automation integration for ExtraHop Reveal(x) Cloud.

Understaffed security teams, new and evolving threats, and response automation based on unreliable data all leave your workloads in AWS less secure.

Some products promise automated response, but can only take a single action such as sending a TCP reset packet to kill a connection. Reveal(x) Cloud empowers you to take a nuanced approach to response automation for threats ranging from low-and-slow to fast-and-destructive attacks.

The new integration supports automated quarantining of compromised EC2 instances based on high-fidelity Reveal(x) Cloud detections. Security teams can also create nearly limitless custom response automations.

As a bi-directional integration, the Reveal(x) Cloud automation bundle combines the richest inputs in the cloud—data from network traffic and machine-learning powered behavioral detections—with AWS security group policies to automatically take action on a compromised workload.

The Reveal(x) Cloud automation bundle comes with a trigger to communicate with an AWS API in your Amazon VPC, and an easy-to-navigate dashboard that includes record format and metrics for audit logs.

Customizable Automated Response

Real-Time Threat Detection

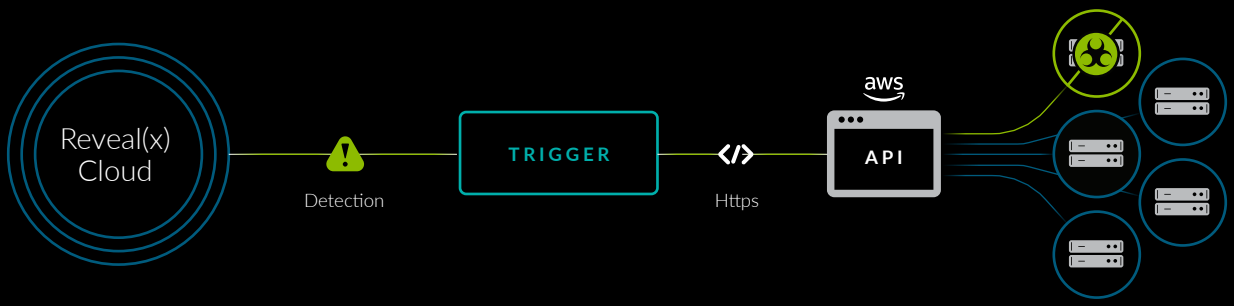
86 RISK

High-Fidelity Alerts

Automated Investigation Steps

HOW THE AUTOMATED RESPONSE INTEGRATION WORKS

When Reveal(x) Cloud surfaces a detection or behavior that violates your security policies, we fire a trigger to an AWS API so that an automated action can be taken on the offending workload. Responses can range from changing an EC2's security group to quarantine or block the instance, or to ticketing, tagging, and more.



QUARANTINE

When a detection exceeds a risk score threshold set by your team, Reveal(x) Cloud directs an AWS API to add the offending workload to a quarantine group, isolating it from everything else on the network.

INTEGRATED RESPONSE AUTOMATION

Blocking
By correlating high-fidelity detections against known threats, Reveal(x) Cloud kills a connection between a system communicating with an IP address that is on a threat intelligence list.

Ticketing
After detecting a ransomware-infected workstation, Reveal(x) Cloud alerts a ticketing system, and the workstation is wiped clean, re-imaged and reloaded to the instance.

Tagging
Reveal(x) Cloud automatically imports AWS metadata and leverages that information to drive policy-based automated response by adding and/or removing tags on resources.

ABOUT EXTRAHOP NETWORKS

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Whether you're investigating threats, ensuring the availability of critical applications, or securing your cloud investment, ExtraHop's breakthrough approach helps you rise above the noise so you can protect and accelerate your business. Learn more at www.extrahop.com.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101