ExtraHop

CLOUD-NATIVE NETWORK DETECTION & RESPONSE

Vince Stross
Principal Security Engineer

ExtraHop

- 500+ employees and global presence
- Trusted by the world's leading enterprises to deliver visibility, detection, and investigation at scale
- 800 customers, 5,000+ deployments, 13 million assets protected
- Innovator in machine learning and analytics

OUR CUSTOMERS

The Home Depot
Morgan Stanley
Lawrence Livermore National Laboratory
Fareportal
Phoenix Children's
Liberty Global

INDUSTRY ACCOLADES

Credit Suisse Disruptive Technology Program Inaugural Selection
InfoSec Awards Winner Cyber Defense Magazine 2019
Innovator 2019 SC Magazine
2018 Fortress Cyber Security Award
EMA Best Joint Application Performance Network Solution
Cybersecurity Breakthrough Awards

SPECTRUM OF RESPONSE AUTOMATION

> You can only automate what you're certain about, and there is still an enormous amount of uncertainty in cybersecurity.
>
> - BRUCE SCHNEIER

AUGMENTED WORKFLOWS

- Create ticket
- Send alert to chat group
- Correlate data with SIEM

Phantom · DEMISTO · servicenow · slack

FULLY AUTOMATED REMEDIATION

- Lock user account
- Block IP address
- Quarantine device

paloalto NETWORKS · cisco ISE · aws

AMPLIFY THE POWER OF YOUR ENTERPRISE TOOLS

INGEST

aws Azure vmware

Packet Brokers

ixia Gigamon

Threat Feeds

ANOMALI

CORRELATE

splunk> IBM QRadar

ArcSight An HP Company LogRhythm

RESPOND

paloalto NETWORKS aws

cisco ISE

Fully Automated

Phantom DEMISTO

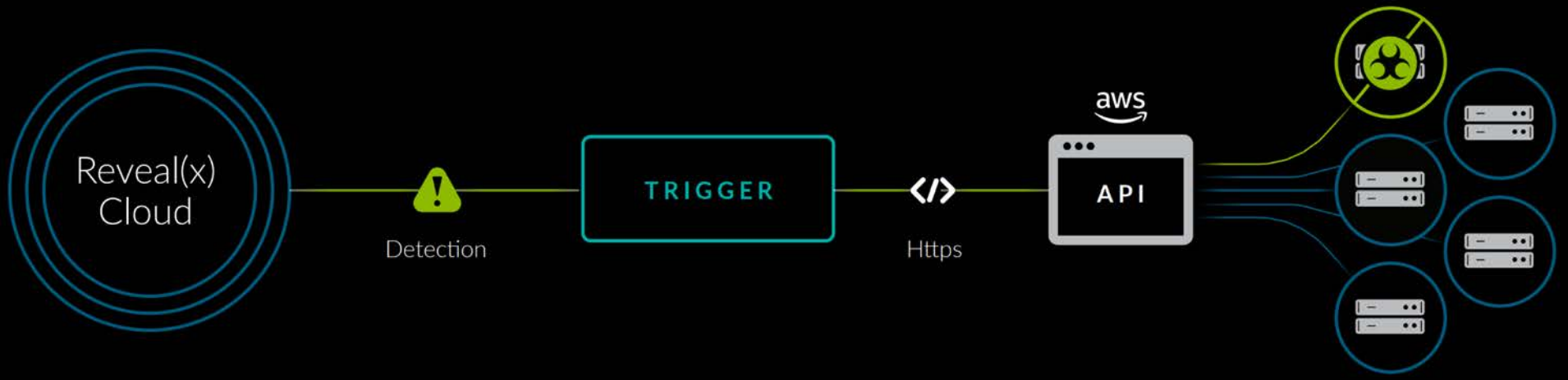
servicenow slack

Augmented Workflows

DETECTION & RESPONSE

AWS QUARANTINING

AUTOMATED REMEDIATION WITH ENDLESS POSSIBILITIES



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

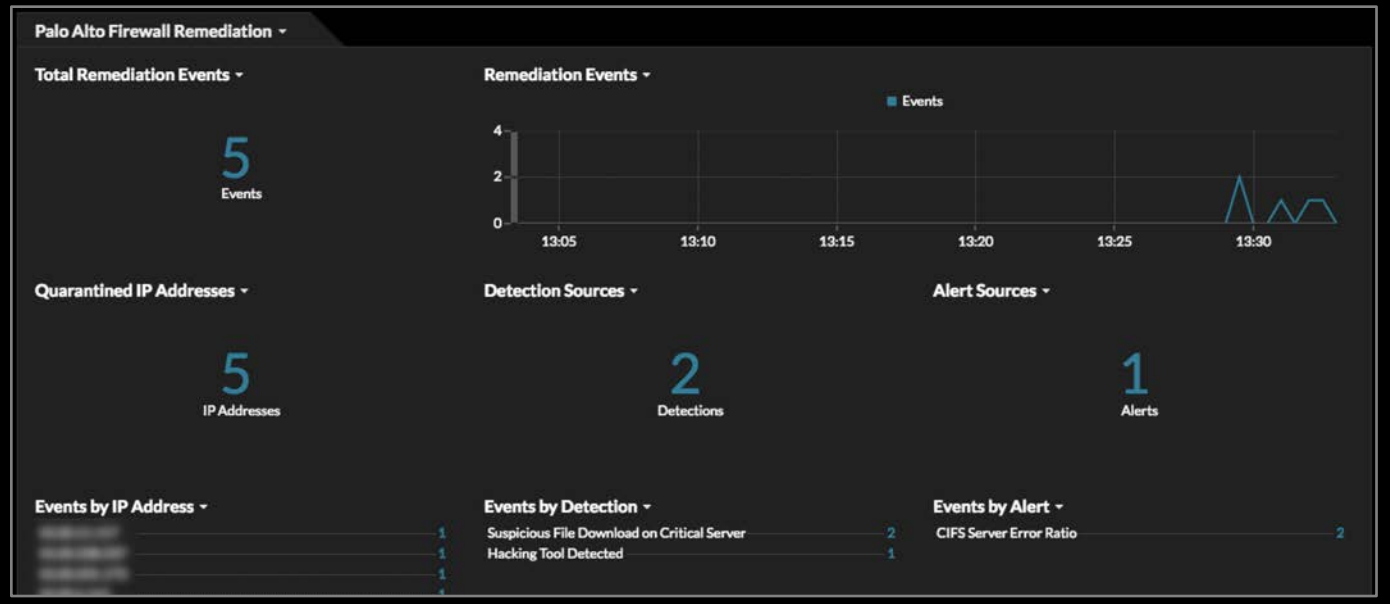
Reveal(x) Cloud automatically imports AWS metadata and leverages that information to drive policy-based automated response by adding and/or removing tags on resources.

EXTRAHOP INTEGRATION WITH PALO ALTO NETWORK NGFW

NGFW AND PANORAMA INTEGRATION

Quarantine compromised devices and block malicious traffic

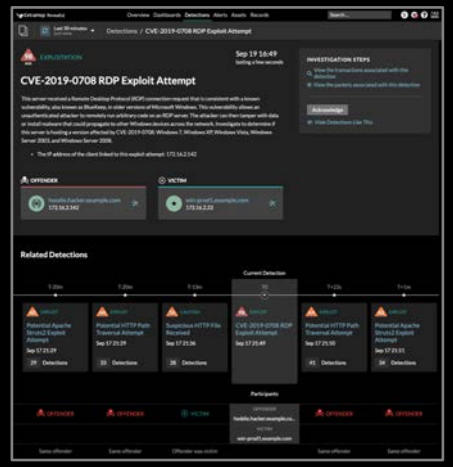
1. ExtraHop detects suspicious activity indicating a compromised device, such as a ransomware or data exfiltration.
2. An ExtraHop trigger extracts details from the detection and adds the device to an address group on a Palo Alto Networks Next-Generation Firewall or in Panorama.
3. Firewall policies that block traffic to and from the address group are automatically applied to the compromised device.



	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

SHOWCASE RESPONSE INTEGRATION: EXTRAHOP + DEMISTO

SUPERCHARGE YOUR INCIDENT RESPONSE

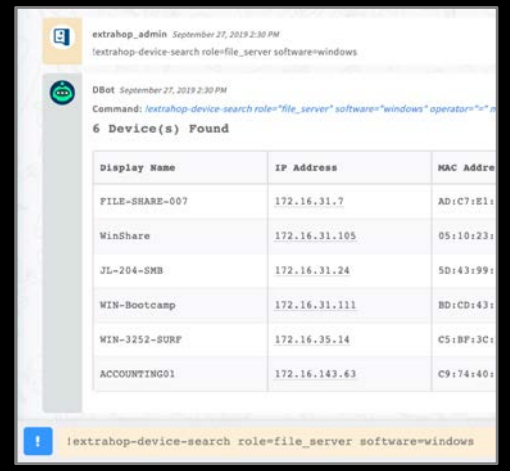


Best-in-class detections, with context

Create detection-based incidents in Demisto with rich contextual details from Reveal(x)

Automated investigation and remediation playbooks

Kick off orchestrated response for CVE exploitation attempts and more



War Room details at your fingertips

Run Demisto commands against Reveal(x) to search for devices, retrieve network peers and active protocols, query records, download packets, and more

AUTOMATED THREAT DETECTION AND RESPONSE

DEMO

TRY IT YOURSELF AT EXTRAHOP.COM/DEMO