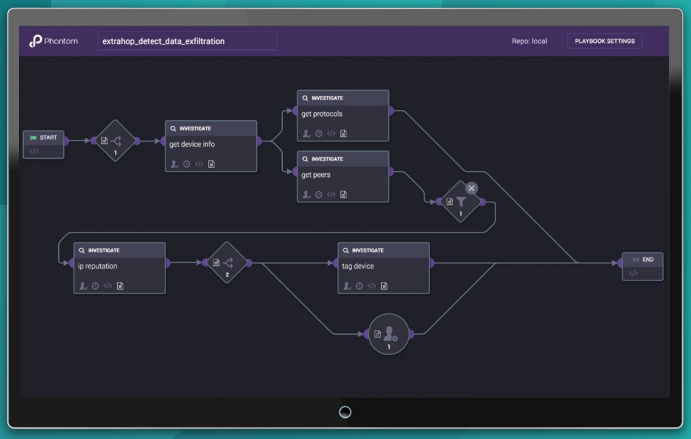
ExtraHop + Phantom™

AUTOMATE, ORCHESTRATE, AND ACCELERATE YOUR SECURITY INVESTIGATIONS

ExtraHop offers unprecedented visibility into your network with automatic discovery and classification of every asset, and 100Gbps analytics on every transaction, including encrypted communications. Through Phantom, ExtraHop's advanced network behavior analytics and investigation workflows team up with SIEM, endpoint, and other infrastructure to automate security operations and forensics.



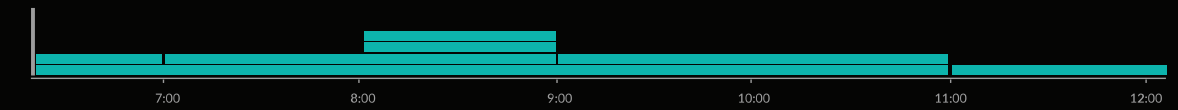
The Reveal(x) Advantage

ExtraHop Reveal(x) analyzes wire data to discover and classify every asset communicating on your environment, and uses machine learning to develop a running baseline for what normal behavior looks like. Reveal(x) provides rich data about every asset, and can do even deeper analysis on assets defined as critical: things like databases, file servers, executive laptops, or medical imaging devices. Reveal(x) sees who's acting on your critical assets, and what they're doing, right down to the DB queries or file manipulation commands they're executing. When something abnormal happens that indicates a security threat, Reveal(x) raises the flag, guiding you to the context and scope of the event, its role in an attack chain, and how it relates to other events, in a seamless workflow.

With Phantom, this data can be used to accelerate your current investigation processes, and automate rapid responses so that attacks can be stopped and investigated quickly enough to prevent further damage. Reveal(x) then pulls data back into the platform to provide full forensic context for further investigation and reporting.

INSTANT PRODUCTIVITY

ExtraHop Reveal(x) organizes likely attack activities according to an attack chain model. Out of the box, Reveal(x) supports the most common security and compliance use cases.



7
Security Anomalies

Command & Control 1	Reconnaissance 3	Lateral Movement 2	Exfiltration 1
Outbound Activity	Port Scans	Share Access	Data Movement
Suspicious Connection	Login Attempts	File Access	Geolocation
DNS Lookups	Transaction Failures	SSH Usage	Sensitive Data
More detections	More detections	More detections	More detections

HOW EXTRAHOP REVEAL(X) & PHANTOM AUTOMATE SECURITY WORKFLOWS

PLAYBOOKS

Phantom enables simple automation and orchestration of complex processes through playbooks. With playbooks, Phantom users can take data from hundreds of products and use a simple drag-and-drop interface to send data between platforms and automate investigation and response actions.

PLAYBOOK 1: Scan new DNS servers for Vulnerabilities

This playbook discovers new DNS servers on your network and initiates Nessus vulnerability scans. Whether it's a rogue DNS server or your IT department's newly configured DNS server, this playbook enables an immediate and automated identification and in-depth scan.

PLAYBOOK 2: Block External Access to Internal Databases

This playbook processes an ExtraHop detection of an internal database being accessed externally and blocks the corresponding external client IP Address on a Palo Alto Networks Firewall. Any instance of an external client accessing a sensitive database is worth investigating, and this playbook uses insights from Reveal(x) to automatically detect and contain such access, and provide immediate forensic data for further investigation.

PLAYBOOK 3: Investigate Data Exfiltration Anomalies

This playbook processes an ExtraHop machine learning anomaly indicating potential data exfiltration on your network. When potential data exfiltration is detected from an asset, ExtraHop automatically gets a list of all clients that communicated with that asset in the last 30 minutes, then gets the IP reputation scores for all non-private IP addresses on that list. Known bad IPs are auto-tagged in ExtraHop for further investigation, and the analyst is notified.

ACTIONS

The ExtraHop Reveal(x) app for Phantom provides several actions as building blocks for playbooks. These actions can be used to pull data from Reveal(x), pass data from Phantom to Reveal(x), tag specific devices, get lists of newly discovered devices, and many other tasks that would formerly have taken manual effort.

Reveal(x) Actions

GET DEVICE INFO: get device details from Reveal(x)

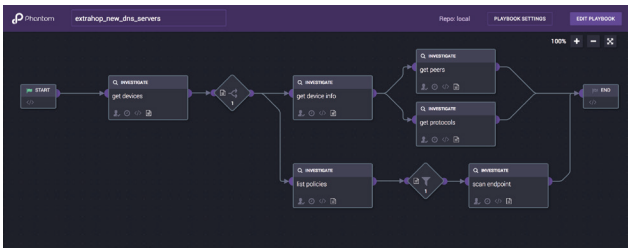
GET DEVICES: get a list of newly discovered devices on your network

GET PEERS: get a list of peers that a device communicated with in a specific time interval

GET PROTOCOLS: get a list of protocols that a device communicated over in a specific time interval

CREATE DEVICE: create a new custom device on Reveal(x)

TAG DEVICE: tag an existing device within Reveal(x)



Nessus Professional ANOMALI paloalto NETWORKS

Phantom

Phantom is the leading Security Operations Platform. Its extensible automation and orchestration capabilities help you work smarter, respond faster, and strengthen your defenses. With Phantom, you can integrate your team, processes, and existing tools together to support a broad range of SOC functions including event and case management, collaboration, and reporting. Learn more at www.phantom.us

ABOUT EXTRAHOP NETWORKS

ExtraHop provides network security analytics powered by AI, with unprecedented depth and breadth of visibility, advanced behavioral analytics, and investigation automation capabilities. Using real-time analytics and machine-learning-driven anomaly detection, ExtraHop enables security teams to accelerate investigations, reduce false positives, and optimize the capabilities of expert security analysts. To learn more visit www.extrahop.com/revealx

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com