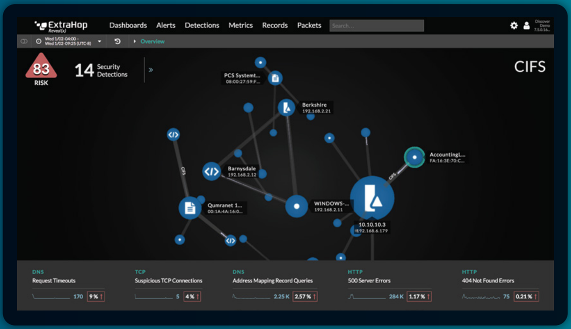
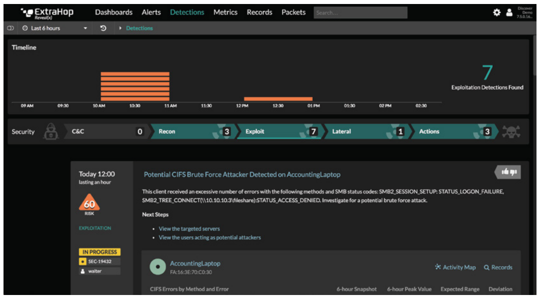
ExtraHop | IBM QRadar

Supercharge Your Security Information and Event Management



With the ExtraHop App for IBM QRadar, you gain accurate, contextual behavioral detections from Reveal(x) and the ability to create new rules based on machine learning-powered detections of anomalous and malicious behaviors.

You can't stop the threats you can't see. If your IBM® QRadar® SIEM relies heavily on log or network flow data, you're left with visibility gaps and context-free detections that lead to alert fatigue and a less secure enterprise. It's time to rise above the noise created by limited visibility and false alerts. ExtraHop® Reveal(x)™ analyzes all network transactions in real time and applies machine learning so that security teams can quickly detect, investigate, and respond to threats. When combined with an IBM QRadar SIEM, Reveal(x) injects high-fidelity behavioral detections into the heart of your security platform, enabling your team to accurately prioritize critical detections, remediate the most serious threats, and protect and accelerate your business.

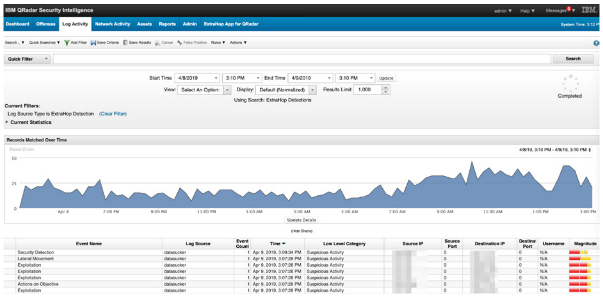


Potential CIFS Brute Force Attacker Detected on AccountingLaptop

This client received an excessive number of errors with the following methods and SMB status codes: SMB2_SESSION_SETUP: STATUS_LOGON_FAILURE, SMB2_TREE_CONNECT(\\10.10.10.3\fileshare):STATUS_ACCESS_DENIED. Investigate for a potential brute force attack.

Next Steps

- View the targeted servers
- View the users acting as potential attackers



The ExtraHop App for IBM QRadar

The ExtraHop App for IBM QRadar automatically imports accurate behavioral detections from Reveal(x) to a single tab conveniently located on your IBM QRadar user interface. Each detection is linked to the Reveal(x) environment, enabling you to quickly pivot to Reveal(x) and extract immediate, contextual details you simply can't get from log and netflow data.

With Reveal(x) detections in IBM QRadar, you have a complete picture of suspicious or anomalous behavior on your network — including previously undiscovered threats hiding in encrypted traffic — and you can sort events by title, risk score, update time, and more. Security teams can also safely search for specific events and quickly drill down to investigate IP addresses of offenders and victims. ExtraHop stores 30 days of metadata lookback and offers optional packet capture, providing tremendous forensic detail for investigations.

HOW THE EXTRAHOP APP FOR IBM QRADAR HELPS DRIVE PROACTIVE SECURITY

EXTRAHOP APP FOR IBM QRADAR USE CASES

The ExtraHop App for IBM QRadar supplements the log and network flow data you're already using to protect your enterprise with anomalous and malicious behavioral detections powered by machine learning. Armed with these real-time insights, your security team can quickly identify and respond to threats.

USE CASE 1: Access Reveal(x) Detections

When Reveal(x) identifies unusual or malicious network activities and behavior, a dedicated tab in the IBM QRadar dashboard shows details such as IP addresses of offenders and victims. Analysts can click on the detection to pivot from IBM QRadar to ExtraHop to learn more about the detection or device details and relationships.

USE CASE 2: Create New Rules Based on ExtraHop Detections

With the ExtraHop App, a SOC analyst can take any detection — a suspicious SSH activity that looks like data exfiltration, for example — and create a rule to open offenses in IBM QRadar when Reveal(x) detects this type of behavior.

USE CASE 3: Create Security Hygiene Reports

Reveal(x) detects a wide range of security hygiene issues, such as expired SSL certificates, that can be used to create a report in IBM QRadar that aggregates expired certificates and provides security operations with a daily or weekly view of their security posture.

USE CASE 4: Correlate Detections with Logs

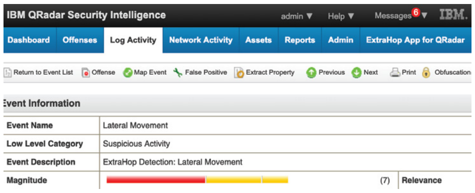
The ExtraHop App enables analysts to correlate Reveal(x) detections with flow logs and firewall logs in IBM QRadar, providing the rich context needed to investigate with confidence. With the ExtraHop App's saved search functionality, you can quickly and easily find Reveal(x) detections over a time frame ranging from hours to up to 30 days.

EXTRAHOP APP FOR IBM QRADAR AND REVEAL(X) ACTIONS

The ExtraHop App for IBM QRadar provides several actions that enable security analysts to protect the enterprise from core to edge to cloud.

Discovery and Classification: Automatically discovers and classifies every asset on your network.

Import Detections: Automatically imports detections to a tab on your IBM QRadar UI.



Event Information

Event Name	Lateral Movement	
Low Level Category	Suspicious Activity	
Event Description	ExtraHop Detection: Lateral Movement	
Magnitude	(7)	Relevance

Saved Search: Enables searches for specific events stored in the ExtraHop App tab.

Event Sorting: Sorts events by title, risk score, update time, and more.

Data Decryption: Decrypts network traffic, including TLS 1.3 protected with Perfect Forward Secrecy.

Packet Analysis: Analyzes every packet that flows across your enterprise at up to 100 Gbps.

Forensic Investigation: ExtraHop stores 30 days of lookback for metadata reflecting 4700 metrics, and provides the option to capture packets using your own storage model, allowing easy access to forensic detail that can save you 50% on packet storage. Extended lookback means you can search for transactions weeks or months in the past as easily as those happening right now.

IBM QRadar

IBM QRadar is an industry-leading Security Information and Event Management (SIEM) product that excels at collecting and consolidating large amounts of data, and then aggregating events into single alerts for fast incident response and remediation. QRadar is purpose built for security, allowing analysts to conduct in-depth forensic investigations of malicious activity without requiring significant customization. Learn more at www.ibm.com/us-en/marketplace/ibm-qradar-siem

ABOUT EXTRAHOP NETWORKS

ExtraHop provides enterprise cyber analytics that deliver security and performance from the inside out. Our breakthrough approach analyzes all network interactions and applies advanced machine learning for complete visibility, real-time detection, and guided investigation. With this approach, we help the world's leading enterprises rise above the noise of alerts, organizational silos, and runaway technology. Whether you're investigating threats, ensuring delivery of critical applications, or securing your investment in cloud, ExtraHop helps you protect and accelerate your business.

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