Catch Unknown Threats & Accelerate Response Time with Integrated NDR + SIEM

Integrate ExtraHop network detection and response (NDR) with your security information and event management (SIEM) to modernize your security operations center (SOC) to catch more unknown threats and accelerate time to detect and respond. Enable next-gen security postures, such as Zero Trust and extended detection and response (XDR).

CHALLENGES

Advanced threats know how to erase logs and avoid endpoint agents to evade detection. Attackers hide their tracks in unmonitored traffic, unmanaged devices, and encrypted data while they expand their access, escalate their privileges, and move laterally before ultimately exfiltrating data.

SOLUTION

By integrating ExtraHop Reveal(x) 360 network detection and response (NDR) with your existing security information and event management tool (SIEM), you gain greater detection capabilities against unknown threats using advanced evasion tactics and techniques. Reveal(x) discovers and identifies every device to provide an always-current inventory. Reveal(x)'s decryption capability provides instant access to correlated forensics, and works seamlessly with your security orchestration automation and response tool (SOAR) to automate response.

KEY BENEFITS

CATCH UNKNOWN THREATS WITH FEWER FALSE ALERTS

Many attack tactics can only be detected on the network. By integrating NDR and SIEM together, you get greater threat coverage.

GET COMPLETE VISIBILITY

Reveal(x) 360 conducts behavioral analysis and also decrypts network traffic. Uncover critical details quickly to detect and respond to threats hiding in regular traffic.

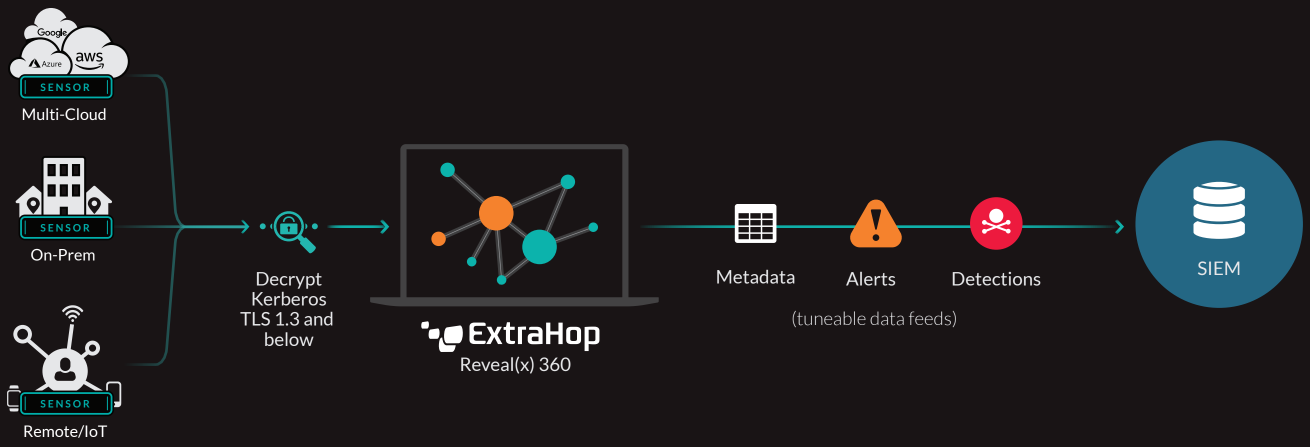
INVESTIGATE AND RESPOND WITH CONFIDENCE

Correlating network detections and forensic details with SIEM logs, enables faster investigation and gives you confidence in your response.

BUILD UP YOUR SECURITY TALENTS

The rich data and context from NDR allows junior security analysts to rapidly learn and respond with confidence to build your in-house security talent.

HOW IT WORKS



Use Cases

ACCESS REVEAL(X) 360 DETECTIONS IN YOUR SIEM UI

For many SOCs, the SIEM is the primary console from which security detections and investigations are conducted. By pulling in vital NDR detections, you get seamless access to more confident detections and forensic details.

DECRYPT NETWORK TRAFFIC FOR FASTER DETECTION AND INSTANT FORENSICS

Reveal(x) 360 captures and decrypts packets for instant access to forensic details in any investigation. Integrate with SIEM to correlate network forensics with log details for a complete view of the attack campaign.

ACHIEVE GREATER MITRE ATT&CK SECURITY COVERAGE

If you want to detect every attacker technique on the MITRE framework, you need NDR in your lineup. ExtraHop is the only NDR provider listed as a contributor to the MITRE ATT&CK framework.

GAIN A PASSIVE, ALWAYS-CURRENT INVENTORY OF EVERY DEVICE

The CIS controls (v8, 2021) recommends a passive asset discovery tool to identify assets connected to the network. Reveal(x) NDR delivers this promise, assuring always-up-to-date inventory and complete monitoring coverage.

AUTOMATE RESPONSE THROUGH SOAR AND EDR PARTNERS

Reveal(x) 360 uses robust REST APIs and our OpenDataStream technology to enable turnkey integration with the SOAR and EDR vendor of your choice to enable rapid, automated response to threats, using the technology that best meets your needs.

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

info@extrahop.com
www.extrahop.com