ExtraHop

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

ExtraHop Reveal(x) 360 delivers machine-learning-driven network threat detection and behavioral insights to Exabeam Fusion SIEM. Correlate network insights with SIEM logs to detect unknown threats faster, and automate response actions via SOAR.

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 NDR with your Exabeam Fusion 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

COVERT, TAMPERPROOF SECURITY

Attackers know how to tamper with activity logging and delete logs on compromised endpoints. But no attacker can avoid the network. When the attacker can't tell you're watching, and can't cut off your visibility, you have a better chance of catching them before they succeed in stealing your data.

COMPLETE VISIBILITY

Integrating multiple data sources is an undisputed good for security operations teams. Activity logs, network monitoring, and endpoint data provide different, complementary perspectives on advanced threat tactics attackers use to breach enterprise networks.

UNPARALLELED DETECTION OF UNKNOWN THREATS

By integrating Reveal(x) network detection and response (NDR) with Exabeam's threat detection, investigation and response (TDIR) capabilities, you gain a high-level view of observed network threat behaviors and activity logs from impacted devices. This enables faster, more confident detection of unknown threats, which drives more specific and effective automated response.

Use Cases

STREAMLINE INVESTIGATIONS

Reveal(x) enables [84% faster threat response]. By correlating Reveal(x) NDR with Exabeam Fusion SIEM or Exabeam Fusion XDR, you give analysts the tools to stop breaches faster.

ACHIEVE FULL-SPECTRUM COVERAGE

Reveal(x) [discovers and identifies every device on the networks], and can tell whether or not it is transmitting activity logs to a SIEM or being monitored with an endpoint agent, so your team can monitor and manage every device.

DETECT MORE MITRE ATT&CK TECHNIQUES

Many post-compromise attack techniques require network visibility for detection. By integrating Reveal(x) with Exabeam Fusion SIEM or Exabeam Fusion XDR, you [achieve greater MITRE ATT&CK coverage].

DECRYPT DATA FOR DETECTION AND FORENSICS

Advanced attackers hide their behaviors in encrypted channels. Reveal(x) [securely decrypts traffic] for high-fidelity detection with fewer false positives and instant access to decrypted packets for forensics.

AUTOMATE RESPONSE THROUGH SIEM/SOAR

Reveal(x) [detects threats that may be invisible to other tools], and can be used to trigger earlier response actions, to cut off an attacker's progress before they do damage.

Driving Extended Detection and Response (XDR) Forward

HOW REVEAL(X) NDR COMPLETES YOUR OPEN XDR ARCHITECTURE

XDR is a model, framework, and architecture for integrating the right tools for your security operations. No XDR approach is complete without NDR, SIEM, EDR, TDIR, and some method of closely integrating those solutions, such as a SOAR product or direct, API-driven integration between each product.

Reveal(x) delivers greater visibility, fewer false positives, and enables 84% faster resolution of threats, making it the ideal NDR solution to complete your open XDR approach.

ExtraHop is the founding, and currently only NDR vendor in the XDR Alliance, a group of like-minded vendors spearheaded by Exabeam to promote an open ecosystem approach to cybersecurity, so that every security team can achieve the XDR approach that works best for their business. Read more about the XDR Alliance on [our blog].

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform uses cloud-scale AI to help enterprises detect and respond to advanced threats—before they can compromise your business. When you don't have to choose betweenprotecting your business and moving it forward, that's security, uncompromised.

ExtraHop

info@extrahop.com
www.extrahop.com