ExtraHop

Microsoft 365

Secure Microsoft 365 with Reveal(x) Network Detection and Response

ExtraHop Reveal(x) 360 network detection and response delivers Microsoft 365 detections with rich network context. By extending your visibility to Microsoft 365 in a single console, you can respond faster and more accurately against risky and malicious actions.

CHALLENGES

Security teams must secure a wide range of users and assets, including SaaS services such as Microsoft 365. SOC analysts are often forced to pivot from their primary security tools over to a separate console for their Microsoft 365 security needs. This introduces friction, and slows down investigations.

SOLUTION

Reveal(x) 360 monitors Microsoft 365 activity for suspicious or risky behavior, and correlates Microsoft 365 detections with powerful machine learning-driven network threat detection. This delivers immediate access to detailed contextual evidence, related detections, and full decrypted packet capture, in a single, simple console.

KEY BENEFITS

SIMPLIFIED DETECTION ACCESS

Access Microsoft 365 security detections and Reveal(x) 360 NDR detections in one intuitive interface.

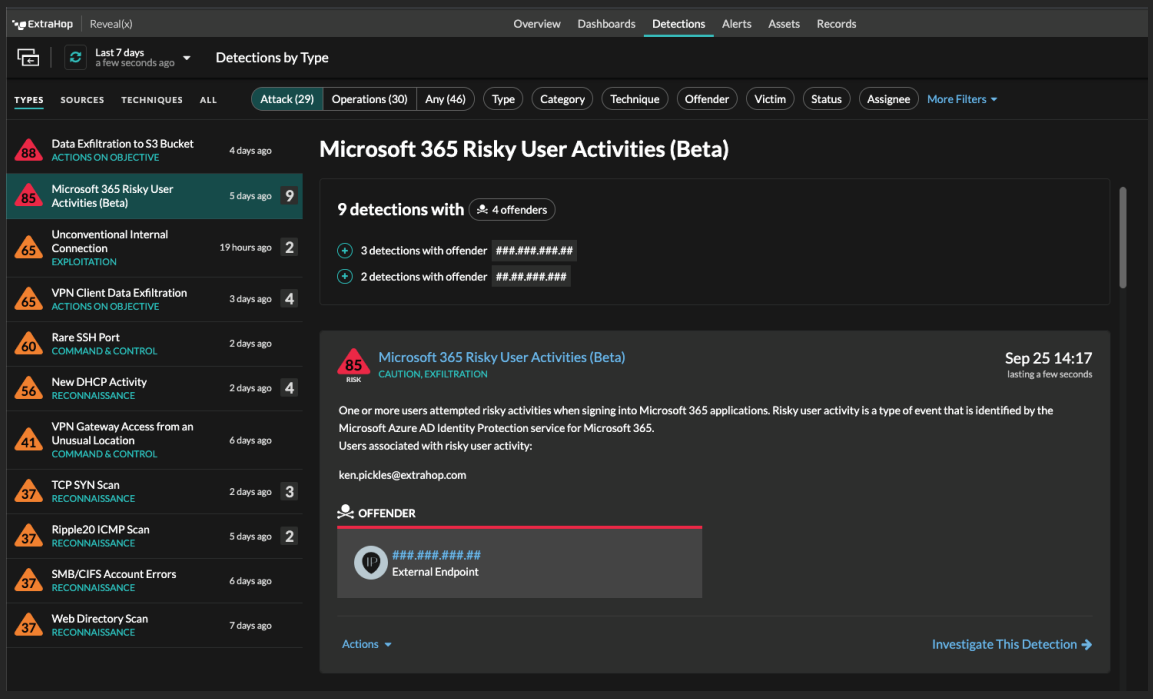
COMPREHENSIVE SECURITY COVERAGE

Gain deeper visibility into Microsoft 365 events, correlated with network context from Reveal(x) 360, enabling greater security hygiene and risk management.

FASTER THREAT RESOLUTION

Get to root cause faster with one-click access to detailed records, related detections involving the same assets, and full, decrypted packet capture for forensics.

Detections with Actionable Context



Use Cases

DETECT RISKY USER BEHAVIOR

Catch users communicating with known-malicious domains or IPs. Detect suspicious behavior and indicators that a user's account may have been compromised.

INCREASE YOUR MITRE ATT&CK COVERAGE

Reveal(x) detects attack tactics from the MITRE framework that can only be seen on the network and correlates with Microsoft 365 data to provide a complete picture.

CORRELATE SAAS, ON-PREMISES, AND CLOUD SECURITY CONTEXT

Reveal(x) correlates detections from your on-premises environment with Microsoft 365 users and behaviors, filling in visibility gaps, letting you respond faster and more accurately.

CUSTOMIZE DETECTIONS ON MICROSOFT 365 BEHAVIOR

Build detections tailored to your enterprise's unique needs, fuelled by both rich NDR analysis and Microsoft 365 events and user behaviors.

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