ExtraHop Extends XDR Partnership with CrowdStrike, Introduces Native Push-Button Response for Precision Threat Quarantine

Submitted by: Positive Marketing
Tuesday, 12 July 2022

New capabilities build on existing detection, investigation, and response integrations between ExtraHop Reveal(x) and CrowdStrike Falcon platform, adding highly-targeted, intelligence-backed response to CrowdXDR alliance

SEATTLE, JULY 12, 2022 – ExtraHop, the leader in cloud-native network intelligence, today announced an integration with CrowdStrike, a leader in cloud-delivered protection of endpoints, cloud workloads, identity, and data, that takes security analysts from detection to threat containment to investigation with a single click. The new push-button response integration expands the best-of-breed extended detection and response (XDR) partnership between the two companies, enabling users to quarantine individual assets from a detection directly within Reveal(x) and then pivot seamlessly into an investigation workflow. Armed with this capability, defenders can act with speed and precision, accelerating response times and minimizing the impact to the business.

The new native push-button response feature within ExtraHop Reveal(x) gives defenders the tools they need to dramatically accelerate containment while minimizing disruption to the organization. Unlike automated response offerings, push-button response gives security analysts the ability to control how and when assets are quarantined based on high-fidelity detections and enriched intelligence that extends from the network to the endpoint.

“Over the past five years, the security pendulum has started to swing more meaningfully towards a detect-and-respond model that assumes even the best perimeter defenses will eventually be breached,” said Jesse Rothstein, co-founder and CTO, ExtraHop. “But many organizations remain reluctant to invest more in this approach due to the complexity of playbook-driven response. With our new native push-button response, we’re continuing to build on our partnership with CrowdStrike and existing response integration capabilities to give defenders the ability to rapidly and precisely quarantine compromised devices without causing massive disruption to the organization.”

“This new capability enables faster remediation and faster time to respond, letting teams focus on critical assets and resources,” said Chris Kissel, research director, security and trust, IDC. “The focus on streamlining the work of the overburdened SOC analyst adds real value for defenders.”

The push-button response integration builds upon ExtraHop’s existing partnership with CrowdStrike which offers integrations throughout the CrowdStrike Falcon platform, including Falcon X, Threat Graph, Falcon Insight (with Real Time Response integration), Humio, and Falcon XDR, to deliver best-of-breed XDR to their joint customers around the world.

- Unified Threat Intelligence: Reveal(x) 360 correlates indicators of compromise (IOCs) from CrowdStrike Falcon X and security telemetry from the CrowdStrike Falcon platform with network details and behavioral insights to deliver complete coverage. The data is correlated and contextualized in the Reveal(x) console.

- Real-time Detection: With the integration of Reveal(x) 360 and the CrowdStrike Falcon platform, security teams can rapidly detect threats observed on the network such as network privilege escalation, lateral movement, suspicious remote access connections, and data exfiltration. They also can thwart attack techniques occurring on the endpoint, including ransomware, local file enumeration, process spawning, and code execution. This provides complete coverage across the entire attack surface.

- Instant Response: With the new push-button response offering, security analysts can use the network containment capability of the CrowdStrike Falcon platform to instantly quarantine a device with a single click within the Reveal(x) platform. This approach cuts off attacker access to network resources and endpoints, stopping an attack in progress without disrupting business or slowing an analyst's investigation workflow.

- Continuous Endpoint Visibility: With automatic device discovery and classification, Reveal(x) continuously updates and maintains a list of devices impacted by threats, even on devices where the CrowdStrike Falcon agent is not yet present. This alerts CrowdStrike customers to newly connected and potentially compromised devices that need instrumentation for device-level visibility. It also extends edge visibility to include IoT, bring your own device (BYOD), and devices incompatible with agents.

Learn more about the power of ExtraHop + CrowdStrike (https://www.extrahop.com/partners/tech-partners/crowdstrike/)

"With new advanced and evolving threats challenging organizations daily, security teams must act with impeccable speed and accuracy to safeguard the business from a breach," said Geoff Swaine, vice president of global programs, store, and alliances at CrowdStrike. "Our tight partnership and breadth of integration with ExtraHop helps to unify security telemetry across network and endpoints, providing customers with enhanced detection and response capabilities to stop advanced threats faster. This new capability offered in the ExtraHop platform helps deepen our integration, enabling security teams to quickly and precisely take action for more effective threat detection, investigation, and response across IT environments."

ExtraHop is also a launch partner of the CrowdXDR alliance, joining forces to establish common XDR language for data sharing between security tools and processes to enrich detections and threat hunting capabilities. A recent joint webinar (https://www.brighttalk.com/webcast/14671/549523) explains how to make XDR a reality.

Additional Resources

- Get ExtraHop Reveal(x) 360 in the CrowdStrike Store (https://store.crowdstrike.com/apps/extrahop-reveal-x-360)
- Experience ExtraHop Reveal(x) in our live online demo (https://www.extrahop.com/demo/)
- Learn more about the CrowdStrike and ExtraHop push-button response capabilities (https://www.extrahop.com/partners/tech-partners/crowdstrike/)
- Watch the Webinar, How XDR Gets Real: Stop Advanced Threats with CrowdStrike and ExtraHop (https://www.brighttalk.com/webcast/14671/549523)

About ExtraHop

Cyberattackers have the advantage. ExtraHop is on a mission to help you take it back with security that can’t be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, helps organizations detect and respond to advanced threats—before they compromise your business. We apply cloud-scale AI to petabytes of traffic per day, performing line-rate decryption and behavioral analysis across all infrastructure, workloads, and data-in-flight. With complete visibility from ExtraHop, enterprises can detect malicious behavior, hunt advanced threats, and forensically investigate any incident with confidence. ExtraHop has been recognized as a market leader in network detection and response by IDC, Gartner, Forbes, SC Media, and numerous others. Learn more at www.extrahop.com.

Press Contact

Ashley Stewart
ExtraHop
pr@extrahop.com

UK PR

Jake Galland
Account Manager, Positive
jgalland@positivemarketing.com
07780866874