ExtraHop

splunk>

ExtraHop Reveal(x)
Supercharge Splunk SOAR with Network Intelligence

ACCELERATE SECURITY OPERATIONS

Gain greater, more reliable threat context and speed investigations with high-fidelity network intelligence.

Challenge

Security operations work is rife with manual, repetitive tasks, especially at the Tier 1 analyst level. Hopping between various threat intel products to manually gather context and performing the same mind-numbing set of tasks can require as much as 30 minutes to investigate a single alert. With enterprises receiving thousands of alerts per day, teams can't get through them fast enough.

Security orchestration, automation and response (SOAR) platforms gather data from multiple security tools, enabling analysts to see context in a single interface. But without valuable data, the usefulness from SOAR can be limited. Logs alone are unreliable and can be inaccurate, disabled, or destroyed by adversaries. Some attack tactics can only be detected in network traffic. Can you trust your detections? Are you confident in the automated response?

Solution

By integrating Splunk SOAR with Reveal(x) network detection and response (NDR), companies can expand visibility with packet-level insights from IoT to the cloud, including unmanaged devices and legacy systems. Reveal(x) automatically discovers and identifies every host that talks on the network.

Key Benefits

Get more complete threat intelligence in seconds

Detect threats hiding in encrypted traffic, such as SQL injection or cross-site scripting

Detect the latest threats and vulnerabilities with cloud-scale, always-on ML models

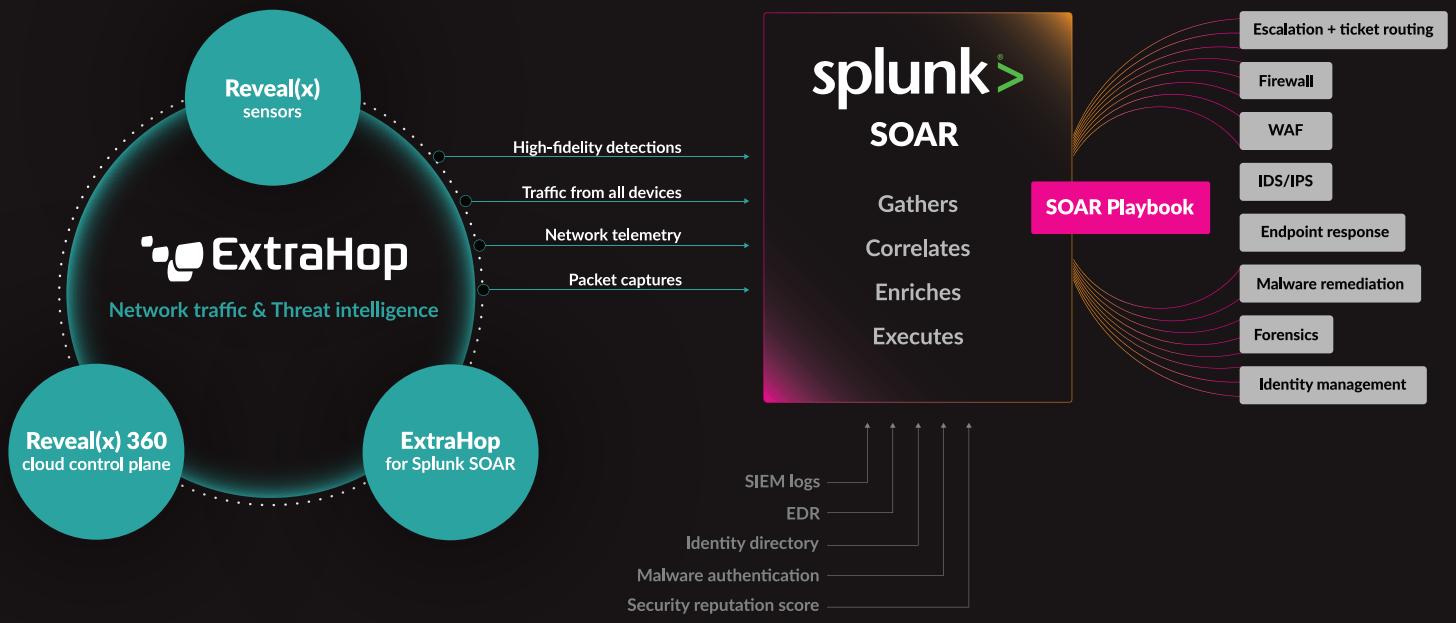
Cover 90% of network-detectable MITRE ATT&CK techniques

Fuel more accurate playbooks and empower better decisions

Perform deep forensics at scale from high-level metrics all the way to network packets

USE CASES	SOLUTION	BENEFITS
Enrich alerts	Supercharge a tool your team is already expertly using everyday—Splunk SOAR—and get more complete threat intelligence all in one single interface. Enrich alerts with high-fidelity network intelligence on: • Detections • Devices • Network artifacts • Packet captures	Automatically gather more complete, correlated context before an analyst starts investigating
Automate investigation and response	Use out-of-the-box playbooks built into ExtraHop for Splunk SOAR: • Investigate database exfiltration anomalies • Detect new unauthorized domain servers • Block connections coming from external hosts to sensitive assets • Create ServiceNow tickets based on detections Or fuel any other playbook that retrieves detection or device data, network artifacts, or packet capture.	Decrease your average time to detect, investigate, and remediate threats

HOW IT WORKS



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, Reveal(x) 360, uses cloud-scale AI to help enterprises detect and respond to advanced threats—before they compromise your business. With complete visibility from ExtraHop, enterprises can detect intrusions, hunt threats, and investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security uncompromised.

ExtraHop

info@extrahop.com
www.extrahop.com