THREAT DETECTION AND RESPONSE WITH REVEAL(X)

Network Traffic Analytics to Illuminate the Darkspace

- Advanced Behavioral Analysis
- Critical Asset Prioritization
- Automated Investigations
- Threat Intel and Orchestration Integrations

THREAT DETECTION AND RESPONSE

Detecting and responding to threats is a security operations team's bread and butter. Many teams currently rely on firewall logs, server logs, and signature-driven alerts to meet their detection and response needs, but the lack of high-fidelity data means the team spends more time dealing with false positives than they do responding to real threats. There's a better way.

ExtraHop Reveal(x) uses unprecedented visibility into the darkspace of East-West traffic to derive definitive insights and immediate answers for SecOps teams. First, Reveal(x) auto-discovers and classifies every device using the network, then analyzes every transaction in real time, decoding over 50 enterprise protocols and decrypting SSL/TLS traffic, even with forward secrecy enabled, at up to 100 Gbps. With this complete knowledge of traffic contents, our behavioral analysis and investigative workflows are able to show relationships and subtle activities that make threat detection and response efficient, thorough, and conclusive.

BEYOND SIGNATURES

Legacy threat detection technologies rely on signatures and indicators of compromise (IOCs) to detect "known bad" activity on the network, including malware, suspicious domains and IP addresses, and other things that have been previously associated with malicious behavior. That's useful, but this approach will not catch never-before-seen threats, nor will it catch threat behaviors that are difficult to signature-match, such as command-and-control traffic, lateral movement, and data exfiltration.

WHAT IS ADVANCED BEHAVIORAL ANALYSIS?

Reveal(x) uses high-fidelity wire data and a cloud-based machine-learning system to identify activities based on suspicious behaviors rather than signatures. It learns what looks normal on your network and applies advanced machine learning models to detect anomalous behavior, identify threats, apply risk scores, and automate the data gathering and correlation steps required for any deeper investigation.

Reveal(x) also ingests threat feeds in the widely used STIX format, so its advanced behavioral analysis can be enriched with existing knowledge about malicious URIs, hosts, and malware. By combining behavior analysis with an inventory of third party threat intelligence in an easy-to-understand UI, Reveal(x) enables analysts to prioritize tasks and execute investigation and remediation more quickly and effectively.

FOCUS ON CRITICAL ASSETS AND WORKFLOW EFFICIENCY

Reveal(x) helps analysts prioritize their investigations by automatically discovering and prioritizing the the most critical assets on your network based on their network activities. You can opt to customize based on your risk posture, choosing PCI databases, executive laptops, DNS servers, or development fileshares. Unlike static CMDBs , Reveal(x) works continuously, so new and rogue devices can be immediately discovered and classified. Reveal(x) then applies advanced behavioral analysis to these assets' communications, so any sign of malicious or suspicious behavior is instantly discovered and presented, along with a risk score, offering actionable visibility into late stage attack activities, and immediate access to transaction details and full decrypted packets within a few clicks from anywhere in the interface, so analysts can act quickly with confidence.

WHAT ABOUT RESPONSE?

Upon observing suspicious behavior, Reveal(x) works with other systems to initiate, automate, and orchestrate workflows while respecting enterprise procedures and best practices. Automating response and remediation is far from a one-size-fits-all proposition. The range of "correct" responses to threats covers a spectrum from "Do Nothing" to "Shut Everything Down." Some responses, such as blocking known malicious IP addresses, are safe to fully automate, and Reveal(x) APIs and partnerships make it easy to integrate with your existing operational tools and countermeasures according to your own policies and procedures. However, many responses can impact operations, especially if they require quarantining or remediating important systems that may be affected by a threat. This requires human expertise and decision making, often by IT operational teams, not the SOC. Reveal(x) helps the SOC provide the right decision-making information as quickly as possible, enabling the approved response teams to make confident decisions when time is of the essence.

Reveal(x) enables both total automation and fast, informed decision making for a balanced approach to response and remediation. For example, Reveal(x) integrates with Phantom, a security automation and orchestration product that allows Reveal(x) to work quickly and seamlessly with Palo Alto Networks, Nessus, Anomali, and hundreds of other security products to stop the progress of threats in the network. Integration with ServiceNow can prompt case management and response as well. Or you can use REST APIs to integrate with your preferred internal, open source, or commercial tools.

INTEGRATE. AUTOMATE. WIN.

ABOUT EXTRAHOP NETWORKS

ExtraHop makes data-driven IT a reality. By applying real-time analytics and machine learning to all digital interactions, ExtraHop delivers instant and unbiased insights. IT leaders turn to ExtraHop first to help them make faster, better-informed decisions that improve performance, security, and digital experience. Just ask the hundreds of global ExtraHop customers, including Sony, Lockheed Martin, Microsoft, Adobe, and Google.

520 Pike Street, Suite 1700
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com