ExtraHop

SECURITY HYGIENE & COMPLIANCE WITH REVEAL(X)

Network Traffic Analytics to Illuminate the Darkspace

- ESTABLISH COMPREHENSIVE VISIBILITY
- AUTO-DETECT & CLASSIFY EVERY DEVICE
- AUDIT WEAK CIPHERSUITES IN REAL TIME
- DETECT EXPIRED & EXPIRING CERTIFICATES

Effective security hygiene requires proactive preparation to minimize the enterprise's attack surface and harden its defenses.

The enterprise will need best-of-breed tools in these three categories to achieve the level of real-time visibility that is necessary for world class security hygiene and compliance.

Auto-Discovery & Monitoring Should Encompass the Entire Enterprise Infrastructure.

Perimeter Monitoring – Traditional North-South controls will generate logs and NetFlow, for L2-L4 visibility, letting you know about communications between services and devices and the ports and protocols used. Additional monitoring at the DMZ can provide visibility to application traffic and content leaving the enterprise.

Endpoint Monitoring – Agent-based monitoring can generate logs and insights about what happens within a device, and the user, software, and system activities over time.

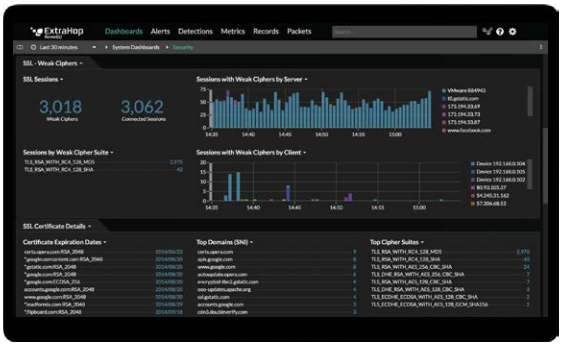
Network Traffic – Internal East-West traffic is the least instrumented today, yet it represents a high proportion of enterprise traffic and creates dark space where attackers and insider threats thrive. ExtraHop Reveal(x) offers a solution.

AUTO-DISCOVER & CLASSIFY EVERY DEVICE

Of the Center for Internet Security (CIS) controls for cybersecurity best practices, the very first one is that every organization should "Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory."

ExtraHop Reveal(x) is the best way to meet this goal. Reveal(x) automatically detects and classifies all devices communicating across the network by reconstructing every conversation and parsing over 50 enterprise protocols at up to 100Gbps, so it knows what's on the network, what each device is saying, and sees immediately when new devices connect. This is a foundational capability for security operations, and Reveal(x) provides it faster, with greater fidelity, than any other product.

DETECT WEAK CIPHERS IN USE ON THE NETWORK IN REAL TIME



Using strong encryption on their internal networks is a must for any company whose data is valuable or regulated. If you handle PCI or HIPAA regulated data, encrypting is literally required, but everyone should be protecting sensitive data with strong encryption. Since Reveal(x) sees all communications on the network, and parses application-layer (L7) transactions, it can immediately detect when weak ciphersuites are in use on the network. Older ciphers like SSLv3, anything using MD5 hashes, and older RSA versions are not sufficient, but they're still in use by many legacy systems, creating serious vulnerabilities for some businesses.

Reveal(x) provides a real-time view into all weak ciphersuites in use, and can warn SecOps teams when new instances pop up, so enabling a level of visibility and control not available from any other audit mechanism.

DETECT EXPIRED & EXPIRING CERTIFICATES

Maintaining current SSL certificates is another vital practice for businesses hoping to protect sensitive data. A certificate expiring can set off a chain of events that knocks production applications offline and impacts the bottom line quickly. Reveal(x) can warn SecOps teams when certificates are about to expire (and when they've already expired), to prevent application outages or ongoing security degradation.

ILLUMINATE THE DARK SPACE WITH NETWORK TRAFFIC ANALYTICS FOR THE ENTERPRISE

Every legacy monitoring solution has blind spots. Logs and endpoint monitoring systems are regularly tampered with or disabled by sophisticated attackers, and perimeter security systems offer no answers about attackers that are already inside the network. Once a single attacker gets into the East-West corridor they're essentially free to conduct reconnaissance, move laterally to access sensitive systems, and exfiltrate valuable data.

Reveal(x) is an out-of-band, passive solution, meaning that it sees all communications inside the network and conducts analytics in real time without impacting network performance. Hackers can't tamper with it, or avoid being seen by it since every sophisticated attack, by necessity, must communicate across the network. Reveal(x) sees these communications, and can decrypt them if necessary, parsing TLS 1.3 in real time, even with perfect forward secrecy enabled. Reveal(x) lets SecOps see into the dark spaces left behind by other solutions.

Launch Our Live and Interactive Demo

EXTRAHOP.COM/DEMO

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.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com