ExtraHop

Reveal(x)
PROOF OF CONCEPT

An ExtraHop Reveal(x) proof of concept (POC) provides you with a unique opportunity to identify, investigate, and respond to suspicious activity that you currently cannot see, as well as uncover security hygiene issues such as insecure protocols, cryptographic compliance, or other policy violations that increase your attack surface.

In addition, the POC will allow you to evaluate how Reveal(x) can improve your organization's security posture through faster detection and reduced noise. You will have an opportunity to work with ExtraHop experts to understand how Reveal(x) can support your program's unique asset and application priorities, workflows, and risk posture.

ExtraHop engineers will install an appliance at an agreed point in your network—near the core switch for visibility into East-West communications, in the DMZ if you want heightened visibility into North-South traffic—giving you the ability to see for yourself how Reveal(x) can light up the darkspace in your environment.

CRITERIA TO TEST FOR IN A POC

CAPABILITY	WHY IT MATTERS
Real-world Anomalies and Threats	A network traffic analytics POC should test how well the product detects real anomalies and threats, not synthetic test traffic, and performs within real-world traffic loads. For this reason, ExtraHop strongly recommends that you deploy Reveal(x) in your production environment.
Investigative Workflow	Network traffic analytics should enable rapid investigations of threats once they are detected. The product should provide upfront context about the threats to assist analysts in prioritizing investigations, and then provide the ability to quickly understand the scope. Analysts should have the ability to perform ad hoc search and query, and then obtain packets for forensic analysis.
Asset Discovery, Classification, and Prioritization	A POC will demonstrate what level of work is required to discover, classify, and prioritize assets in your environment. Keep in mind that the product will need to dynamically keep up with changes and you will want to minimize the amount of ongoing work required.
Decryption	Without decryption, analysis of network traffic is limited to packet headers and flow-type metrics. Attackers know this and use encryption to hide their activities. As encryption rates inside the datacenter increase, the ability to decrypt transaction payloads will become more critical, making it a key criteria for your POC.
Protocol Support	Threat detection and investigation are dramatically enhanced with data parsed from application-level protocols (Layer 7 protocols). Your POC evaluation should consider the breadth and depth of protocols analyzed as this will impact event detection accuracy and correlation.
Throughput of Analysis	If a network traffic analytics product cannot scale well, that means you will have to purchase more appliances to support your environment. Consider what amount of throughput will be required in three to five years' time and whether your network traffic analytics solution will be able to scale economically.

Identify Threats in Your Production Environment
Your Reveal(x) POC will uncover suspicious, malicious, or just out-of-policy activity that you didn't know about. These activities can include active reconnaissance, privilege escalation, and sensitive file access, as well as more mundane but important risks such as weak ciphers and insecure protocol usage.

Automatically Discover and Classify New and Rogue Assets
Reveal(x) automatically compiles a real-time inventory of devices communicating on your network, classifying them according to their observed roles, for example as a DNS server or VoIP client. Within 10 minutes of installation, you can explore what devices are actually operating in your environment and what their dependencies are.

Threat Assessments, Investigation Coaching, and Response Initiation
As part of the POC process, your sales team will deliver Threat Assessment reports in a working session, during which time you can investigate the findings using Reveal(x). This process not only enables you to identify and resolve critical issues but also learn how Reveal(x) speeds up key security operations workflows and facilitates threat scoping and threat hunting.

PROOF OF CONCEPT TIMELINE

TIMELINE	STEPS	TAKE-AWAYS
BEFORE	• Schedule installation • Discuss deployment	**Understanding of the passive Reveal(x) deployment model and technical architecture**
DAY 1	• Install Reveal(x) appliance • Set up passive data feed through port mirror or network tap • Reveal(x) automatically discovers and classifies devices • Users have immediate access to interface and data analysis, along with a Reviewers Guide	**Auto-discovery and classification of all devices in the data feed and their dependencies**
WEEK 1	• Machine learning is enabled to build behavioral baselines for every device, network, and application • SE sets up device groups (critical assets, workstations, etc.) and network localities (remote sites, web properties, etc.) • First working session and data review focus on understanding the existing attack surface, learning time-saving workflows, and how to customize Reveal(x)	**Opportunities for reducing risk and optimizing key analyst workflows**
WEEK 2	• Second working session features threat hunting exercises and a data review to go through additional findings	**Proactive measures simplified by Reveal(x)**
WEEK 3	• Third working session can include forensic analysis and potential auto-response integrations, along with a data review to go through additional findings • Present strategy and quote for production deployment	**Integrating Reveal(x) into your security toolset for orchestration and automation**
WEEK 4	• Presentation of Executive Summary, ROI Document, and Final Data Findings Report	**Business case for the project**

RESOURCES REQUIRED

Passive Data Feed
The Reveal(x) appliance requires a passive feed of network traffic. This is commonly provided through a port mirror (SPAN port), a network tap, or a network data broker.

Secure Connection
For the POC, the ExtraHop sales engineer and analysts will need to occasionally remotely access the POC appliance for the purposes of troubleshooting and management, as well as assessing findings for the working sessions.

Findings Reviews and Working Sessions

We recognize the value of your time. The Reveal(x) POC does require a commitment on your part—to run the POC in production and spend one day per week in working sessions. This is for the purpose of seeing how make the most of your time—detecting issues earlier, validating events faster, and investigating root cause in a matter of clicks.

Privacy & Legal Considerations

Reveal(x) is a completely passive solution and will not interfere with your production network or applications. The product does include a cloud-based machine learning component, and information on the security and privacy of this connection available in our Security, Privacy, and Trust overview. If you do not wish to proceed beyond the POC, data is deleted in a secure manner.

520 Pike Street, Suite 1600
Seattle, WA 98101
www.extrahop.com