ExtraHop Reveal(x) NDR Quick Reference

Top reasons an engineer would want this

1. Wire data as the source of truth, shows what is actually happening on the network, not abstracted into logs, not depending on what audit settings are enabled, not what "is supposed to happen", but what is actually traversing the network.

2. That wire data is shown as "conversations". First anything that is SSL/TLS encrypted is decrypted at line rates. Then ExtraHop understands 70+ Layer 7 enterprise protocols:
    - Authentication (LDAP, Kerberos, RADIUS, …)
    - Network file systems (CIFS, NFS, FTP, …)
    - Databases (SQL, Oracle, …)
    - Web Server (HTTP, SSL, …)
    - Network infrastructure (DNS, DHCP, …)
    - Remote access servers (PCoIP, Citrix, …)
    - Those conversations provide context for further analysis.

3. Metadata (5,000+ metrics) is sent to the cloud for Machine Learning based analysis. Machine Learning in this context has three function categories:
    - Perception
    - Detection
    - Investigation

    In each of these categories the cloud-based Machine Learning is providing vast resources to identify things happening that are known bad, or out of the ordinary, or are causing errors.

    Because ExtraHop has historical data it can spot anomalous behavior. In the Security space this would include users connecting to a server for the first time, or servers "talking" to other servers that they don't normally to talk to and which their peer group of servers don't normally talk to.

    In the Performance use case, it can spot servers that are taking longer to respond than is normal or are returning error messages in response to web requests. Severe enough anomalies or incidents can be bubbled up to a human for further investigation.

4. Guided investigation and remediation. "Problem to Insight in 3 clicks." For all three use cases –
    - Security
    - Network Performance
    - Application Analysis

    ExtraHop provides guided investigation and help towards remediation.

5. Surgical packet analysis when needed. The Trace appliance keeps the customers packet data onsite, only metrics go to the cloud, and allows drilling down to the packet level for a specific

device, a specific conversation, a specific incident in a surgical manner, showing just the packets of interest without writing filters or using 3rd party tools like wireshark to provide details.

6. One system for on-prem and cloud.

7. One system for Sec Ops and Net Ops, providing opportunities to reduce the number of tools in use and provide for easier hand off between Net Ops and Sec Ops groups.

ExtraHop Reveal(x) questions

Know your audience and ask relevant questions. Don't answer your own questions – endure the silence and see what they will tell you (your answer might be wrong anyways)

Where are your gaps in visibility across the enterprise?

How do you see what is happening east/west?

Can you see on-prem and cloud in same tool?

Are you decrypting SSL/TLS traffic for analysis?

How many monitoring tools do you own and use to respond to incidents?

Do you have a SIEM today and how would you characterize it's value? Is it noisy?

Do you have too many alerts from existing monitoring systems?

Do you know you have a problem before the phone rings?

Tool Consolidation

ExtraHop Blog post about tool consolidation

The "tool consolidation" pitch is based around

Pain points:

- We've been adding a variety of tools for security and performance monitoring
- A lot of those tools aren't integrated, they don't talk to each other
- You may have to use more than one tool when investigating a security incident or performance issue
- All these tools cost money to buy and renew
- All these tools take time to manage, time to learn

ExtraHop, in one tool, provides solutions to Pain Points:

- Security, network performance monitoring, app analysis use cases (one tool)
- Full integration between various use cases (one tool)
- Context from high level dashboard, to incident level, down to packet trace if needed (one tool)
- Simple deployment with hardware or virtual sensors, virtual or hardware packet storage
- Cloud based management and analysis platform, less maintenance (one tool)
- One tool to learn/One tool to pay for