White Paper

The Critical Assets Filter for the SOC

Focus discovery and analytics to expedite security investigations

By Barbara Kay, CISSP

With limited analyst time and many alerts going untriaged, security operation centers are getting more discerning about what infrastructure they monitor, analyze, and investigate, and the associated data they store. ExtraHop™ Reveal(x)™ provides auto-discovery, intelligent classification, and service-centric analytics to help beleaguered SOC analysts concentrate their energies on the most important and targeted assets in their enterprise: on-prem or in the cloud. East-west visibility, advanced behavioral analytics, and automated workflows help investigators zero in on the incidents, attack activities, and forensic data required for effective security operations.

Focus on Critical Assets to Unlock Efficiency in the SOC

The analysts in the Security Operations Center (SOC) are often like the kid outside the candy store – noses pressed against the glass and craving. Inside the candy store, the IT ops teams feast on an array of rich data and performance and application analytics tools. They know which data candy is best, and where it is stored. But they (or at least their tools) aren't always good at sharing.

For example, Net Ops and Endpoint Ops and Data Center Ops control their own infrastructure or infrastructure as a service partner. Each group has their particular piece of IT environment instrumented to generate monitoring data:

- Servers, databases, and hosts generate logs.
- Network switches and routers export NetFlow records.
- Applications generate transaction traces and logs.
- EDR tools capture traces.
- PCAP tools capture packets.
- The latest container monitoring tools introduce yet another data silo.

These data sets may be individually obtainable through APIs or syslog messages, but they seldom come with a map about where the good stuff is – which data is most meaningful for security use cases, and how to find it easily.

How does the SOC find the data they really need? Many security teams rely on SIEMs for data integration (including normalization, indexing, and correlation). After the fact reconstruction almost guarantees gaps in data completeness and quality. To compensate for gaps, companies add in even more data, such as vulnerability scan data. Then they invest in threat intelligence and analytics to add context and extract insights from this data set. Even with the fastest SIEMs and most effective AI-driven analytics, SOC investigations are perpetually chasing truth.

While IT operational teams may be content with the status quo of these data silos and after-the-fact reconstructions, security teams face intense pressure. Technology status quo would see security operations lag behind threat techniques and new varieties of risk introduced with new technologies. CISOs and SOC directors also need to compress and automate processes to get more value out of scarce security staff, while containing spiraling data costs for compute, tuning, and storage.

How ExtraHop Helps

ExtraHop has made it practical for security analysts to get inside the enterprise data candy store and quickly locate the good stuff. We combine automated discovery and real-time capture of transaction data on the network with graduated analysis centered on critical assets and asset groups (critical services). This two-part model generates accurate and prioritized data to concentrate ExtraHop's AI-driven behavioral analysis. Analysts get a detailed map to prioritized attack activities that affect the most business-critical services.

Auto-Discovery And Asset Classification

An out-of-band, passive monitoring system uses protocol activity to automatically discover new devices and service elements. Based on the traffic it observes, ExtraHop can classify the role and extrapolate the value of the service element, regardless of its location. For instance, databases interact via predictable protocols and commands with application servers, web servers, active directory servers, and authentication servers on-premises and in the cloud. Databases also most frequently send certain types of data to certain types of endpoints in response to requests. These standard behaviors are good indicators of the type of asset and its role in a service. Auto-discovery means the lists are always current and accurate, not derived from an asset database or logs that can be deleted.

Complete, Immediate Transaction Records

Patented technology enables ExtraHop to decrypt traffic and perform full-stream reassembly in real time, for every transaction and session on the network. We produce a complete, authentic set of data that goes beyond simple NetFlow metrics to include application-layer (Layer 7) metadata across more than 50 protocols and hundreds of thousands of endpoints (IoT sensors, cloud workloads, PCs, databases, and more). The entire conversation between client and server transaction is correlated together and recorded in real time with associated content (the session payload) and packets. The platform indexes and stores your wire data in three complementary formats:

- Correlated, cross-tier metrics provide you with immediate visibility into more than 4,000 metrics that populate customizable, real-time dashboards. You can easily see all communications across your entire environment. These detailed metrics provide inputs for our machine learning engines.
- Transaction, message, and flow records allow you to conduct a multidimensional analysis of your wire data, even if you don't know any query languages.
- Forensic evidence in the form of packets are linked to each specific transaction record. You can click directly to those packets for a deep-dive root cause analysis or to meet chain-of-custody requirements for legal prosecution. You can also compose a new packet query, filtering down to just the kilobytes of packet capture you care about. (Requires Reveal(x) Ultra subscription).

Imagine hearing a conversation between 5 people at an airport. You likely won’t catch every word. If they speak a language that you don’t, you will miss out entirely. In contrast, ExtraHop tells you who said what to whom, in order, as complete sentences, for more than 50 languages (protocols). We also provide the meaning of the conversation, including if it was normal or suspicious. Optional packet capture permits you to replay it.

Cloud And Virtualization Evidence

With visibility into all activities between systems and services, we see everything happening over the wire, including within workloads and containers. For instance, ExtraHop can capture and characterize the pre-, during, and post spin up and spin down behaviors of a workload to show you changes in these critical steps. In a world of microservices, wire data provides evidence after the container, service, workload, entity has evaporated.

For example, imagine an orchestrator creates a new instance of a containerized service to accommodate heavy load. An attacker compromises this service and uses it to access a customer

database, and the service is then decommissioned. ExtraHop discovers the anomalous behavior and maintains a forensic record of it, even after the service is long gone.

Auto-Prioritization of Critical Services

By combining visibility into the protocols, commands, applications, and devices involved in an activity, we automatically discover the role and importance of a specific asset. Based on these interactions, we note assets that are critical, and group together the assets that together make up a critical service.

> False positives can be a problem for some machine learning systems, but the critical asset focus brings that concern to near zero for ExtraHop Reveal(x).

Tuning Possible, Not Required

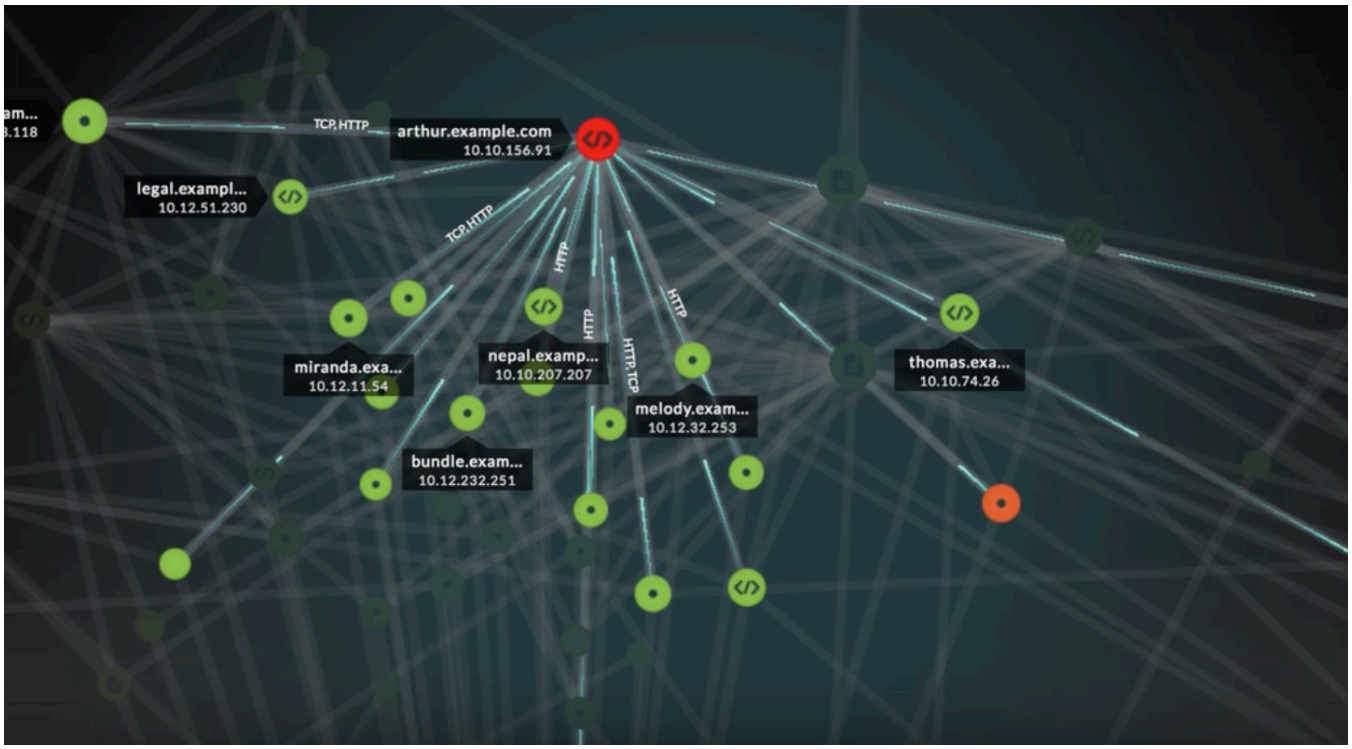
ExtraHop users can programmatically prioritize endpoints, endpoint groups, and activity groups that are critical. Both static and dynamic groups can be ordered for the most flexibility. This means that you can create a group based on custom criteria such as a tag or CIDR block, and then prioritize that group for Advanced or Standard Analysis. Or you can prioritize an activity group, such as LDAP, HTTPS, or DNS Servers, to prioritize any endpoint that actively communicates over a specific protocol.

This model has many practical benefits in adapting technology to your business requirements. For example, if you have a development team working on highly proprietary technology, you would want to prioritize analysis of all the workstations that have access to the build server that stores source code. Each organization will have unique prioritization rules like this that they will want to implement—ExtraHop makes it possible to easily do so.

Dynamic Classification of New Systems

The solution can also flag new endpoints and services that come online whose behavior indicates the new discovery should be considered “critical.” The defined endpoint groups and activity groups can let the ExtraHop solution automatically adjust and manage new endpoints based on the rules that make sense for you, promoting new discoveries appropriately into advanced analysis.

If you need to prioritize analysis of your authentication servers, you would simply prioritize the AAA activity group in ExtraHop. That way, if a new endpoint comes online that is acting as a AAA server, it would immediately receive the highest level of analysis. This dynamic classification is especially crucial as IT environments become more fluid and permeable.



Detailed understanding of the activities of each system helps ExtraHop Reveal(x) identify critical assets.

Graduated Analysis

While all assets remain in Standard monitoring mode with customizable dashboards and analytics (including comparison options), assets designated as part of critical services graduate to Advanced analysis. This graduated analytics model effectively overlays surgical analytics on continuous health monitoring.

100% Signal

The rich detail used in classifying the asset is also beneficial in monitoring its behavior. Security-specific metadata about critical services is anonymized and sent to cloud-based machine learning systems for behavioral anomaly detection. In simple terms, this service is the equivalent of an army of analysts who never stop looking for unusual and malicious behavior of the services your business cares most about.

False positives can be a problem for some machine learning systems, but the critical asset focus brings that concern to near zero for ExtraHop Reveal(x). Because the prioritization filter is applied before the machine learning system is applied, the ensuing data and alerts are very targeted and meaningful. ExtraHop delivers these anomalies in a dedicated user interface that models the attack chain, with one-click access to live activity maps, transaction records, and associated packets.

Acting on the Good Stuff

Through these analytics, ExtraHop reduces the technical knowledge required to evaluate incidents. SOC analysts can make confident decisions about what to escalate and investigate further without being as

expert in each part of the infrastructure involved. Although data is visualized and easy to navigate, the technical data remains available for forensics. That data also facilitates deeper discussions with the network, endpoint, and other operational teams when an investigation shifts into appropriate remediation, mitigation, and preventative measures. This approach reduces friction while facilitating collaboration.

Easy Integration and Orchestration

The precise, real-time events and metrics that we capture can also be streamed to a SIEM, ticketing, or orchestration system, or used to directly kick off immediate responses, such as host quarantine. We support many third parties off the shelf, and offer Open Data Stream functionality as syslog messages or a REST API. It's easy for the SIEM to ingest and use with its other data sources, visualizations, and reports. [More details here.]

CONCLUSION

Auto-discovery, auto-classification, and service-centric analytics help SOC analysts gain confidence that they are seeing an up to date picture of their infrastructure's assets, paying the most attention to the most important assets and service groups, and confirming the incident with high-quality data. As the SOC interfaces with operational teams, high-fidelity, highly actionable data helps both groups resolve incidents in less time, bringing critical assets back to health and contributing to enterprise services.

Experience the power of ExtraHop Reveal(x) in our interactive online demo.

ABOUT EXTRAHOP

ExtraHop is the first place IT turns for insights that transform and secure the digital enterprise. By applying real-time analytics and machine learning to all digital interactions on the network, ExtraHop delivers instant and accurate insights that help IT improve security, performance, and the digital experience. Just ask the hundreds of global ExtraHop customers, including Sony, Lockheed Martin, Microsoft, Adobe, and Google.

ExtraHop Networks, Inc.
520 Pike Street, Suite 1700
Seattle, WA 98101 USA

www.extrahop.com
info@extrahop.com
T 877-333-9872
F 206-274-6393

Customer Support support@extrahop.com
877-333-9872 (US)
+44 (0)845 5199150 (EMEA)