ExtraHop + splunk>

Combine Wire Data from ExtraHop and Machine Data from Splunk

Both Splunk and ExtraHop offer new and better ways of gaining visibility for IT operations. Together, these complementary solutions provide complete IT operational intelligence, with ExtraHop sending real-time wire data into Splunk for correlation with machine data.

"Concur uses ExtraHop to extract the precise information we're looking for and immediately export it to Splunk, where we can perform deep analytics. This combination of wire data and machine data enables us to quickly answer questions that would not be able to answer otherwise."

—John Tharp
Lead Software Configuration Engineer
Concur Technologies

In enterprise IT, each significant technology is designed and operated according to a deliberate architecture: network and security architecture, SOA and application architecture, and even database and storage architecture. Remarkably, the one place where all these technologies meet, IT operations, typically lacks a planned framework, resulting in massive collections of niche tools, significant gaps in visibility, high coordination costs, and inefficiencies in incident escalation.

Together, ExtraHop and Splunk provide the framework for a rationalized IT Operations Analytics (ITOA) architecture. ExtraHop transforms raw packets into structured wire data in real time, including event-driven metrics and payload information that is otherwise impractical or impossible to log. These metrics can be streamed into Splunk and other IT management products through Open Data Stream.

ExtraHop captures metrics for network performance, transaction timing, database internals, file-based storage, and locked-down environments like mainframes. With the flexibility to mine both wire data and machine data, IT teams have the complete operational intelligence they need to answer IT and business questions.

EXTRAHOP PROVIDES CORRELATED, CROSS-TIER VISIBILITY FOR THE ENTIRE APPLICATION ENVIRONMENT:

- Web servers (Apache, Microsoft IIS, and more)
- Application servers (Apache Tomcat, ASP.NET, Ruby on Rails, and more)
- Mail and collaboration servers (including Microsoft SharePoint)
- Database servers (IBM DB2, IBM Informix, MySQL, Oracle, PostgreSQL, Microsoft SQL Server, and Sybase ASE)
- Storage devices
- Authentication servers (LDAP, RADIUS, and Diameter)
- Network services (DNS)
- Network devices (including load balancers and firewalls)

ExtraHop and Splunk work together to empower a range of teams, including IT Operations, Network, Application, Virtualization, DBAs, Storage, Security, and Business Management.

SPLUNK APP FOR EXTRAHOP

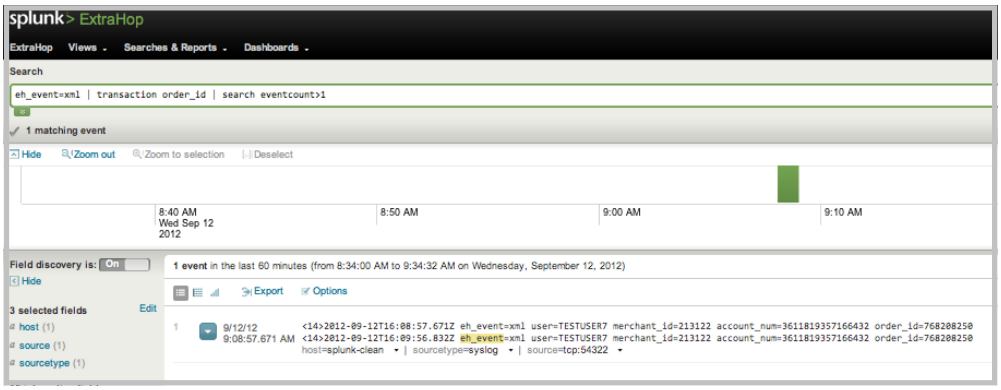
The Splunk app for ExtraHop enables users to forward transaction-level details from ExtraHop to Splunk through rsyslog. The result is a mechanism for precision logging the wealth of previously untapped wire data.

In addition to the precision-logging capability, the extensible Splunk app for ExtraHop collects the following metrics:

- **Web metrics** – Responses over time, average transaction response times, JSON, AJAX, and SOAP/XML payload, status codes with detail, and web traffic throughput
- **Web services metrics** – External and internal API calls, events over time, top active account numbers, top active users, and other customizable metrics such as duplicate order IDs
- **Database metrics** – All methods, queries, response times, transaction response times, errors, top methods, and top users
- **Storage metrics** – Responses over time, average transaction response times, errors, top methods, and top users
- **Memcache metrics** – Transactions over time, average access time, errors, message sizes, top response codes, top methods

You can also add other elements, including the following, to your Splunk app for ExtraHop:

- **Transaction metrics** – Anything in the payload can be measured in real-time for IT operations analytics and business intelligence
- **Mainframe** – MQ and CICS methods, status, and transactions
- **FIX and SMPP** – Transactions, response times, and payload information.



ExtraHop can extract payload data, such as transaction order IDs and account numbers, for real-time and forensic analysis in Splunk.

GET THE WHOLE PICTURE

Extract real-time wire data and combine it with other machine data from throughout the datacenter in Splunk.

- Record consistent metrics across all tiers, including the network, web, middleware, application, database, memcache, and storage.
- Capture holistic metrics such as end-to-end response time.
- Monitor locked-down environments such as mainframe deployments, including DB2 environments.
- Log payload data, including transaction details such as order ID, merchant ID, and account number.
- Correlate network performance and application performance.

ANSWER IT AND BUSINESS QUESTIONS

Quickly the find the answers to questions that would be nearly impossible to find otherwise.

- Identify missed business opportunities by analyzing transactional data by account and user.
- Parse data by top methods and top users.
- Define new metrics not available through the logging options available on web, database, and storage servers.
- Gain real-time insight into database performance without having to run profilers.

SIMPLE DEPLOYMENT

Gain immediate value and minimize total cost of ownership with an elegant network-based deployment.

- Start collecting meaningful events off the wire with no system overhead.
- Automatically discover and classify applications and devices.
- Avoid brittle agents that can lock you into a specific vendor or version and cost valuable resources to deploy and maintain.

ExtraHop Networks Singapore Pte. Ltd.

+65-3158 5513

apac-info@extrahop.com

www.extrahop.com

ABOUT EXTRAHOP NETWORKS

ExtraHop is the global leader in real-time wire data analytics. The ExtraHop platform analyzes all L2-L7 communications, including full bidirectional transactional payloads. This provides the correlated, cross-tier visibility essential for today's complex and dynamic IT environments. The ExtraHop platform scales up to 40 Gbps, require no agents, and delivers value immediately upon deployment.