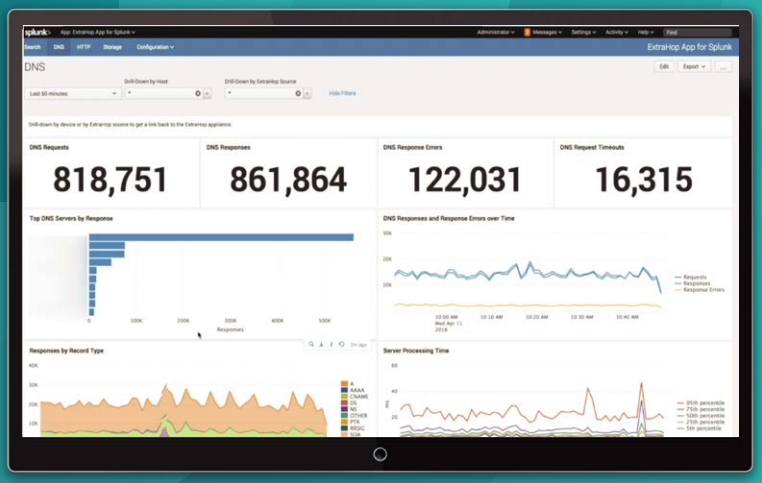
ExtraHop + splunk>

UNPRECEDENTED VISIBILITY. DEFINITIVE INSIGHTS. IMMEDIATE ANSWERS.

Combine machine data and wire data so IT Ops and Sec Ops can act with confidence.



USE CASE: WITH DNS METRICS FROM EXTRAHOP, VIEWED IN SPLUNK. USERS CAN LOOK AT ALL DNS METRICS, DRILL DOWN TO METRICS FOR AN INDIVIDUAL HOST, OR EASILY NAVIGATE BACK TO THE EXTRAHOP INTERFACE TO INVESTIGATE HOST BEHAVIOR.

WHY INTEGRATE EXTRAHOP AND SPLUNK?

- Instant access to thousands of high-fidelity metrics, including DNS, web, VDI, database, storage and more for broad coverage without requiring you to ingest high volumes of logs
- Rich correlation between wire data and logs for rapid diagnosis and response to performance issues and security threats.
- Pivot instantly to correlated packets in ExtraHop for rapid forensic investigation

AUTOMATE WORKFLOWS WITH EXTRAHOP AND PHANTOM

ExtraHop's rich wire data allows the confident automation and orchestration of security investigation and response.

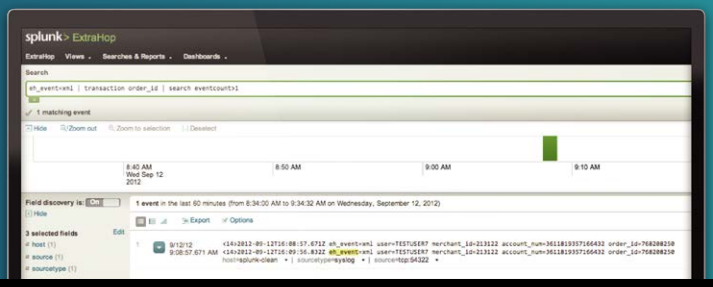
Learn more about our simple integration and automated security playbooks with Phantom

> “Find the ultimate truth in the wire. Even the most granular logs are not enough to be the truth.

YOUNG CHO
SR. INDUSTRIAL IOT PRACTITIONER, SPLUNK

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)
- Authentication servers (LDAP, RADIUS, and Diameter)
- Storage devices
- Database servers (IBM DB2, IBM Informix, MySQL, Oracle, PostgreSQL, Microsoft SQL Server, and Sybase ASE)
- Network services (DNS)
- Network devices (including load balancers and firewalls)



ExtraHop + splunk>

EXTRAHOP CAN EXTRACT PAYLOAD DATA AND EVEN DECRYPT TLS 1.3 WITH PERFECT FORWARD SECRECY FOR IMMEDIATE FORENSIC INVESTIGATION.

The ExtraHop App for Splunk, available on Splunkbase, enables users to forward transaction-level details and metadata from ExtraHop to Splunk. The result is a system for correlating real-time wire data and logs for unprecedented visibility across the environment.

VALUABLE METRICS

The ExtraHop app for Splunk enables the collection of thousands of high-value built-in metrics, including:

- **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

USE CASE: INVESTIGATING DNS ISSUES

Let's look at a specific example, DNS metrics, and explore how both IT and Security operations teams can get a ton of value from integrating Splunk and ExtraHop.

IT OPS

DNS issues can cause frustrating latency or total unavailability of applications and websites while also consuming undue network resources, all of which can be difficult to diagnose if DNS isn't being logged due to cost and effort.

ExtraHop for IT Ops has built-in performance metrics that can instantly surface DNS issues based on observed network traffic instead of logs. These metrics can be easily explored through the ExtraHop interface and pulled into Splunk through the REST API for correlation with other log data.

SECURITY

DNS is a commonly used vector for attackers seeking to steal information and/or remotely control compromised hosts inside a target network. When worries arise of a DNS-driven attack, and SecOps tries to investigate, they may find they lack the visibility needed to understand the situation if DNS isn't being logged due to cost and effort.

With just a few clicks in the ExtraHop app for Splunk, SecOps can get all the DNS metrics they need for every DNS server, with no agents and no network performance overhead.

By removing the manual effort of instrumenting DNS logging, this integration removes the barrier to monitoring a common but often overlooked cause of performance issues and security vulnerability. Applying the same process across many other protocols and metrics available through ExtraHop can materially reduce manual effort and improve results for both IT Ops and SecOps teams.

ABOUT EXTRAHOP NETWORKS

ExtraHop is the leader in analytics and investigation for the hybrid enterprise. We apply real-time analytics and advanced machine learning to every business transaction to deliver unprecedented visibility, definitive insights, and immediate answers that enable security and IT teams to act with confidence. The world's leading organizations trust ExtraHop to support core digital business initiatives like security, IT modernization, and application service delivery. Hundreds of global ExtraHop customers, including Sony, Microsoft, Adobe, and DIRECTV, already use ExtraHop to accelerate their digital businesses. To experience the power of ExtraHop, explore our interactive online demo. Connect with us on Twitter and LinkedIn.

ExtraHop

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