

# ExtraHop for Security and Compliance IF IT MOVES ACROSS THE WIRE, YOU CAN SEE IT WITH EXTRAHOP

O Latinhan .	2+ investment * Deler				
	Carment as Theorem Bellevie				
hellowelline	Namedian (arrival)	the second second		-11.000	- 1
Signal Tex Crists	100				- 11
	100		1. 1		
Spectister,		atom to the work	ald Research Made	i ikanan	
	- WARDON W AND			Web Property	
Comple Destinants					
10.0					- 11
Dealers			they below here		
216					
-	December Seals				
Serge .	had brought hit string		or otherwork Parlie Sales Broakdown (*	the Parlamethed	
To Darthourth	# harry 2014	# heart 28th	Witness Traction	# term businessing Tem	
Summer Daubbloom No.					
Adulty	- Antertal Auto	hall have -			
Network					-
Der Ope					
	Transmission in Harbod		energ Tracketown		
	Supersonal State		B Internets	III Maller	
	Stall anorther				

The ExtraHop platform enables security operations teams to keep tabs on all the communications and transactions in their environment. By analyzing their wire data, security teams can detect threats and get the context needed to answer what, where, when, and who for any situation.

#### "ExtraHop shows what the applications are actually saying, not just who is talking to whom."

---Micah Rodgers Senior Network Security Engineer, Murphy USA ExtraHop enables security teams to analyze wire data, which is data-in-motion. This new data source effectively brings together the application and security teams to understand data patterns and determine what constitutes a potential threat. The outcome is a simplification of security and policy enforcement, and more effective detection of previously unknown threats.

## MAINTAIN CONTINUOUS AND PERVASIVE VISIBILITY

- · Automatically detect new devices communicating on the network and what protocols they are using
- · Drill down to specific devices and examine lateral activity
- See the geographic location of requests for FTP, HTTP, and more
- Track and alert on anomalous privileged account activity
- Create event triggers to identify data exfiltration attempts
- · Audit TLS/SSL certificates and spot weak ciphers to ensure secure in-flight encryption

## **DETECT AND ALERT ON MALICIOUS ACTIVITY**

- Access-denied events for networked storage
- High and low-intensity brute-force attacks on authentication servers
- Data exfiltration from databases, file servers, and application servers
- · Botnet command & control (C&C) activity that uses DNS TXT records
- · Anomalous behavior across all tiers of your environment



ExtraHop's Geomaps function can track real-time user activity by location to identify potential threats. The screenshot above shows DNS queries to IP addresses in Russia.

	Tele Academic and Television			E-Commerce: Data Breach and Exfitnation
adbadhlas = 1; hadran ann ballant athy athy intent		Bits Assessed Facel South Sout	Contacts from the contact of the con	<ul> <li>Mention detection outputstand with the strength output strength outputstand with the strength o</li></ul>
	Connect on Connect Connect performance (Sec., 1999) In Connect performance (Sec., 1999)	Set Sector (11)	Comment and Central 1 Bits of the Alexandrow	

#### **TRY THE ONLINE DEMO!**

Interested? Check out our free online demo. You can explore the interface for yourself and follow an incident-response scenario.

www.extrahop.com/demo

Certificate Key Expiration		⊙ Last 7 days 👻 ☰	
EXPIRED Certificates - BROKEN (days expired)	GO≫ ≡ 1.5K	If non-zero, the listed	
Server IP: 10.10.9.39   Name: ehio.extrahop.com   Expiration: Sat Aug 27 2011 Server IP: 20879.144.53   Name: ehio.extrahop.com   Expiration: Sat Aug 27 2011	1.5K	certificates may need your attention	
Server IP: 10.10.7.194   Name: zamak.sea.laxtrahop.com   Expiration: Fri May 09 2014 493		Broken certificates put not only your business at risk, but can break essential services for your customers.	
Server IP: 10.10.7.63   Name: zamakseai.extrahop.com   Expiration: Fri May 09.2014. 489 Server IP: 10.10.2.150   Name: bio-00.sea.lextrahop.com   Expiration: Sat Oct. 18.2014 331		* An expired or rogue SSL Certificate in a network environment could have severe	
Server IP: 10.10.20.3   Name: trac.Lextrahop.com   Expirators: Thu Jul 30.2015		repercussions. It takes just one out-of-date or rogue certificate to expose the enterprise—and perhaps more importantly, its customers—to malicious cybercrime.* (Source: Versign's Business Continuity and	
EXPIRING Certificates (days until expiration)	60 » =	Breach Protection: Why SSL Certificate Management Is Critical to Today's Enterprise)	
Days until Certificate Expires 0		*Avoid non-compliance problems such as business disruption, reduced productivity, fees, penalties and other legal and non-legal	

ExtraHop's customizable security dashboards reveal potential vulnerabilities in security as well as augmenting your existing compliance capabilities with real-time visibility of your environment.

## **REAL-WORLD EXAMPLES**

ExtraHop taps into the common element that ties every environment together—wire data—so that security teams can get comprehensive visibility into what is happening in their environment. The following examples show how ExtraHop has helped other organizations improve security.

#### AUTOMATED DETECTION OF HEARTBLEED VULNERABILITIES AND EXPLOITATION ATTEMPTS

The day of the Heartbleed announcement, a network and security ops team deployed the ExtraHop Heartbleed bundle for TLS Heartbeat Tracking, Dashboards, Client Identification and Geomaps. They watched malicious attempts to compromise their servers in real time, and immediately set blocking policies for those clients while they patched their vulnerable systems.

#### **DETECTING DATA EXFILTRATION**

A large government agency needed a way to identify the source of a data leak and detect any future data exfiltration. The security team used the ExtraHop platform to identify a specific machine with abnormal DNS activity as the source of the leak, and they now use ExtraHop as an integral part of their security monitoring and analytics.

#### **TLS/SSL MONITORING**

A large web hosting company used ExtraHop to continuously monitor SSL traffic between the load balancer and the backend servers, and fire off alerts if any traffic was not properly re-encrypted.

### **BYOD: MOBILE MONITORING & NETWORK OPTIMIZATION**

A global enterprise tech company used ExtraHop's auto-discovery and application activity mapping to quantify "bring-your-own-device" (BYOD) activities on secure and guest networks, determining which applications were being accessed and implementing appropriate security controls.

### **SECURITY/ENCRYPTION AUDITING**

A large enterprise with both incoming and outgoing SSL traffic used ExtraHop to view the entire set of SSL behaviors on their network, so they could see which certificates were being used, identify weak cipher suites, and set concrete steps for remediation.

### **BANNED PORTS, PROTOCOLS, AND SERVICES**

A federal government agency used ExtraHop to monitor all connections that are banned per policy, such as protocols that transfer data unencrypted (FTP, telnet, SNMP, Gopher, etc.).

### 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.

#### ExtraHop Networks, Inc.

520 Pike Street, Suite 1700 Seattle, WA 98101

877-333-9872 (voice) 206-274-6393 (fax) info@extrahop.com www.extrahop.com