

WHITEPAPER

Kopplung der ExtraHop Wire Data Analyse
Lösung mittels des Compliance Moduls von
macmon NAC

1. Einleitung
2. Konfiguration ExtraHop
3. Konfiguration macmon
4. Ablauf im Falle eines Angriffs
5. Weitere Szenarien

1. Einleitung

Die ExtraHop Wire Data Analyse Appliance analysiert die gesamte Layer 2- bis Layer 7-Kommunikation und bietet durch die so korrelierten Daten essentielle Informationen über die Performance von genutzten Applikationen, die Verfügbarkeit sowie über die Sicherheit. Dabei erkennbare Angriffe erfordern in der Regel sofortige Maßnahmen, die durch die Network Access Control-Lösung macmon in Echtzeit umgesetzt werden können. Die direkte Kopplung der beiden Systeme und die damit verbundene automatisierbare Reaktion auf Angriffe und Anomalien werden in diesem Whitepaper erläutert.

2. Konfiguration ExtraHop

Konfiguration Open Data Stream (ODS):

Die Konfiguration des ODS erfolgt über folgende Menüs:

Settings -> Administration _> Open Data Streams

Configuration	
Running Config	Change
Geomap Data Source	Change
Datastore & Customizations	Change
Open Data Streams	Change
Capture	Change
Trends	Change

Im Menü *Open Data Stream* den Unterpunkt HTTP auswählen.

Open Data Streams	
Syslog Systems	Change
MongoDB	Change
HTTP	Change

Auf der folgenden Seite entweder die Einstellungen für „default“ ändern (hier kann jedoch der Name nicht geändert werden) oder, sofern „default“ bereits anderweitig genutzt wird, einen neuen Namen anlegen. ExtraHop ermöglicht es, bis zu 16 verschiedene Open Data Stream-Empfänger einzurichten.

Data Stream Configuration #2

Name:

Type:

Host:

Port:

Skip Certificate Verification:

Pipeline Requests:

Use Basic Authentication:

User:

Password:

Additional HTTP Header:

Signing Method:

[Add New](#)

Unter dem Menüpunkt „Host:“ wird dann entweder ein FQDN (fully qualified domain name) oder die entsprechende IP der macmon Appliance eingetragen.

Wird für die macmon-Appliance kein „echtes“ Zertifikat eingesetzt, so ist in der Checkbox „Skip Certificate Validation“ auszuwählen.

Um Ereignisse an macmon zu übergeben, erfolgen die weiteren Konfigurationen in der ExtraHop-Appliance über Trigger:

Über den sogenannten „Extrahop-Trigger“ kann jedes Ereignis, das von ExtraHop in Echtzeit im Datenstrom erfasst wird, unverzüglich an die macmon-Appliance weitergeleitet werden.

Trigger Script: [API Reference](#) [Info](#) [Settings](#)

```
8  * Event: DB_RESPONSE
9  * Has "USER_SET": True
10 * /
11
12 // Capture client flow
13 var client_ip = Flow.client.ipaddr;
14 var user = DB.user;
15
16 // Capture sever flow
17 var server_ip = Flow.server.ipaddr;
18 var method = DB.method;
19 var user = DB.user;
20
21 // USER_SET: Super User account name
22 if (user == "root" || user == "sa")
23 {
24     var db_login_info = "client_IP " + client_ip + " : "
25                       + " server_IP " + server_ip + " : "
26                       + " user=" + user;
27
28     Network.metricAddCount("db_login_access", 1);
29     Network.metricAddDetailCount("db_login_info", db_login_info, 1);
30
31     //debug
32     debug(db_login_info);
33 }
34
35 var mypath = "/macutil/?select=refmacs&C=[last_ip]='client_ip'&pipe[]=macdeac";
36 var mypath_2 = "/macutil/?compliance&address=00-19-B9-5D-8D-DE&source=ExtraHop&reason=Illegal login db_login_info&status=nonc";
37 |
38 Remote.HTTP('macmon').get( {path: mypath_2 } );
39
```

Der zu übertragende „Pfad“ der *macutil*-Schnittstelle kann im Trigger auch entsprechend als Variable gesetzt werden. Die Verbindung zur macmon-Appliance erfolgt über den Befehl Remote.HTTP ('macmon').

Sollte der „default“-Eintrag verwendet werden, kann auch auf den Befehlszusatz ('macmon') verzichtet werden. In diesem Fall ist Remote.HTTP.get. ausreichend.

3. Konfiguration macmon

Sollen MACs, die nicht den Firmenrichtlinien entsprechen, nur in ein VLAN oder ein VLAN mit gleichem Namen, aber verschiedenen VLAN-IDs geschaltet werden, aktiviert man die Standard-Regel 0140 (grün gerahmt) und hinterlegt unter „Einstellungen“ – „Scan-Engine“ im Feld „remediation_vlans“ VLAN-Namen oder -ID.

Aktiv	Name	Ereignis	Periode	Bedingungen	Kommando	Benutzergruppe
<input checked="" type="checkbox"/>	compliant_DB_Login	new_compliant	24x7	compliant	set_compliant	
<input checked="" type="checkbox"/>	DisablePort_on_Unauthorized	unauthorized	24x7		disable_port	
<input checked="" type="checkbox"/>	email_on_new_unauthorized	newunauthorized	24x7		email	admins
<input checked="" type="checkbox"/>	Neue-Regel	footprint_changed	business_hours		prioritymail	admins
<input checked="" type="checkbox"/>	noncompliant_DB_Login	new_noncompliant	24x7	DB_Login_NonCompliant	set_noncompliant_vlan11	
<input checked="" type="checkbox"/>	set_vlan_on_wrong_vlan	wrong_vlan	24x7		set_vlan	

Um differenziert auf bestimmte Compliance-Status (z.B. wegen anderem „Reason“) zu reagieren, nutzt man zusätzlich zur Regel „set_vlan_on_wrong_vlan“ (grün gerahmt) eine oder mehrere Regeln analog zu der hier dargestellten Regel „noncompliance_DB_Login“ (rot gerahmt), setzt jedoch keinen Wert für das Feld „remediation_vlans“ in den Einstellungen. Hiermit wird ein VLAN

direkt an der MAC hinterlegt, die eine höhere Priorität hat, als das MAC-Gruppen-VLAN.

Mit der Regel „compliant_DB_Login“ (rot gerahmt) wird das VLAN, das direkt an der MAC konfiguriert wurde, wieder entfernt und das MAC-Gruppen-VLAN wird wieder aktiv.

Die Kommandos werden wie rechts dargestellt konfiguriert. Sie nutzen die Schnittstelle „macutil“, um die MAC für das gewünschte Verhalten zu modifizieren.

The screenshot shows the 'Ereignisse - Kommandos' configuration page in the macmon interface. The left sidebar contains navigation options like 'Endgeräte', 'Benutzer', 'Netz', 'Richtlinien', 'Compliance', etc. The main content area has tabs for 'Regeln', 'Perioden', 'Bedingungen', and 'Kommandos'. The 'Kommandos' tab is active, showing a table of commands.

Name	Kommando	Parameter	Art
disable_and_enable_port	internal	[DEVICE_ID],[IFINDEX]	schreibend
disable_mac	internal	[MAC]	schreibend
disable_port	internal	[DEVICE_ID],[IFINDEX]	schreibend
email	internal		nicht schreibend
enable_port	internal	[DEVICE_ID],[IFINDEX]	schreibend
nolog	internal		nicht schreibend
prioritymail	internal		nicht schreibend
restore_vlan	internal	[DEVICE_ID],[IFINDEX]	schreibend
set_vlan	internal	[TARGET_VLAN],[DEVICE_ID],[IFINDEX]	schreibend
shutdown	internal		schreibend
syslog	internal		nicht schreibend
trap	internal		nicht schreibend
Printer	/opt/macmon/engine/macutil.php	macmod [MAC] -q Drucker	schreibend
set_compliant	/opt/macmon/engine/macutil.php	macmod [MAC] -vlan "" -c ""	nicht schreibend
set_noncompliant_vlan11	/opt/macmon/engine/macutil.php	macmod [MAC] -vlan 1 -c "noncompliant"	nicht schreibend
Set_To_No_Go	/opt/macmon/emd/modules/setvlan.php	-a set_vlan_by_id -vi 99 -si [DEVICE_IP] -i [IFINDEX] -f	schreibend

A 'Speichern' button is located at the bottom left of the table area.

Die in den Regeln verwendeten Bedingungen sind folgendermaßen zu erstellen.

The screenshot shows the 'Ereignisse - Bedingungen' configuration page in the macmon interface. The left sidebar is the same as in the previous screenshot. The main content area has tabs for 'Regeln', 'Perioden', 'Bedingungen', and 'Kommandos'. The 'Bedingungen' tab is active, showing a table of conditions.

Name	Bedingungen
compliant	[OVERALL_STATUS]= "compliant"
DB_Login_NonCompliant	[OVERALL_STATUS]= "noncompliant" and [REASON]= "Several_DB_Login_Attempts"
Example_VMWare	[OUI_VENDOR] = "VMWARE"

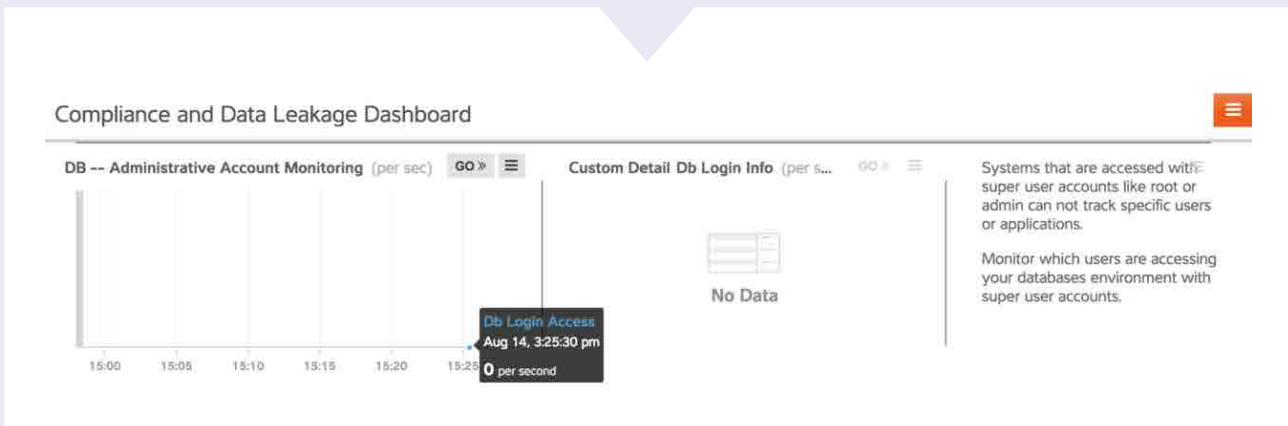
Um für verschiedene Szenarien oder Standorte unterschiedliche VLANs zu setzen, werden weitere „noncompliant“-Bedingungen, ähnlich der Bedingung „DB_Login_NonCompliant“, benötigt.

4. Ablauf im Falle eines Angriffs

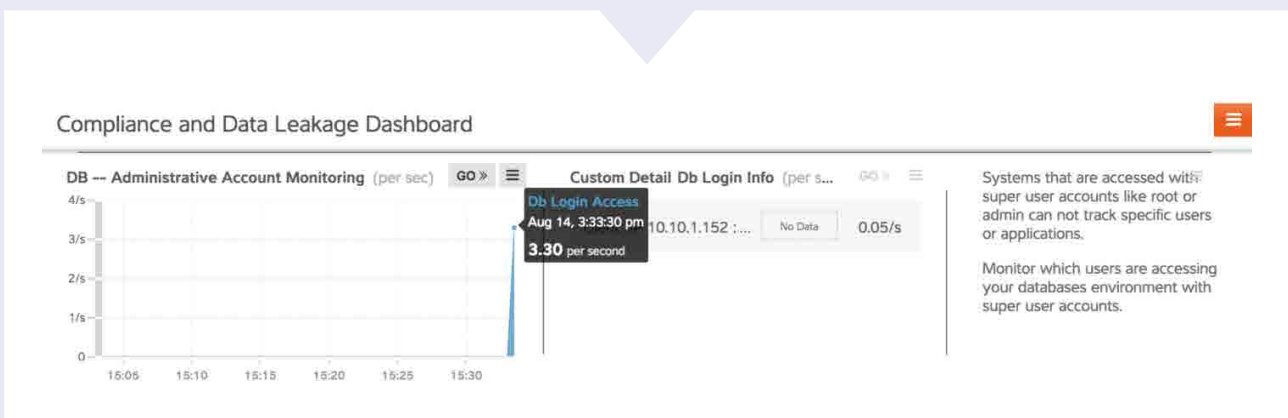
Zur Demonstration der Funktionalität dient folgendes Ereignis:

Ein Gerät aus dem Netzwerk (LAN) versucht, sich mittels Benutzerrechten an einer Datenbank anzumelden.

Ansicht des ExtraHop Dashboards vor dem Eintritt des Ereignisses:



Sobald das Ereignis eintritt, erkennt ExtraHop sofort eine Menge an Logins mit Admin-Rechten auf allen möglichen Datenbanken, z. B. MySQL, Postgres, Oracle, MS-SQL, Informix, DB2, Sybase, Sybase IQ und MongoDB.



Nach Eintritt des Ereignisses und durch die Ausführung eines HTTP Get-Befehls auf die macutil-Schnittstelle, stellt sich die Reportseite der macmon Oberfläche ausgelöst durch einen „Trigger“ von ExtraHop folgendermaßen dar:

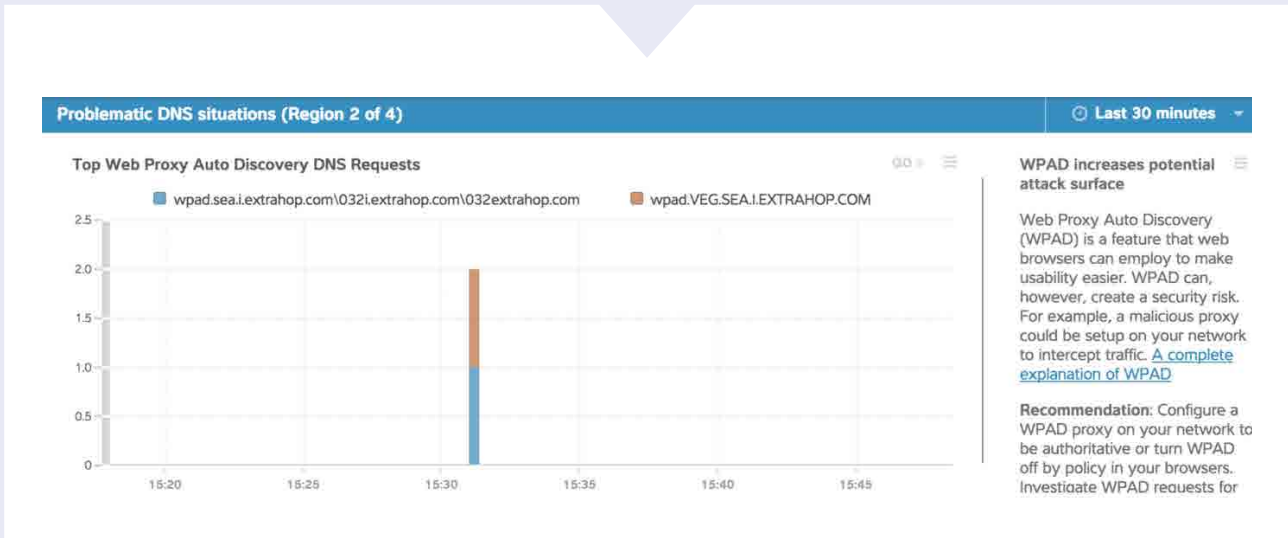
The screenshot shows the 'macmon' interface with the 'Berichte' (Reports) section. It displays a table of compliance events with columns for MAC, Last IP, Last DNS Name, Group, Status, Source, and Reason. The table lists several 'Non-compliant' events triggered by ExtraHop, such as 'Additional WFAD', 'LDAP Brut Force Attack', 'DNS-TXT Requests', and 'Too many logins'. A 'Compliant' event for 'All patches installed' is also listed.

MAC	Letzte IP	Letzter DNS-Name	Gruppe	Status	Quelle	Grund
9C-19-61-17-54-82	192.168.101.14	Notebook0748	Notebooks	non-compliant	ExtraHop	Additional WFAD
5C-C3-7B-83-96-C3	192.168.101.13	Notebook0234	Notebooks	non-compliant	ExtraHop	LDAP Brut Force Attack
2B-C8-56-4D-66-B9	192.168.101.12	Notebook0374	Notebooks	non-compliant	ExtraHop	DNS-TXT Requests
1D-89-CD-96-C1-8D	192.168.101.11	Notebook0364	Notebooks	non-compliant	ExtraHop	Additional WFAD
45-89-43-84-13-0A	192.168.101.10	Notebook0675	Notebooks	non-compliant	ExtraHop	Synflood
9F-48-3B-87-57-58	192.168.101.8	Werkstation0168	SalesPCs	non-compliant	ExtraHop	Too many logins
7C-9B-44-B9-D6-9C	192.168.101.8	Werkstation0442	SalesPCs	compliant	WSUS	All patches installed

Nachdem macmon von ExtraHop benachrichtigt worden ist und dort die entsprechenden Policies hinterlegt sind, wird gemäß den Regeln ein Kommando ausgeführt.

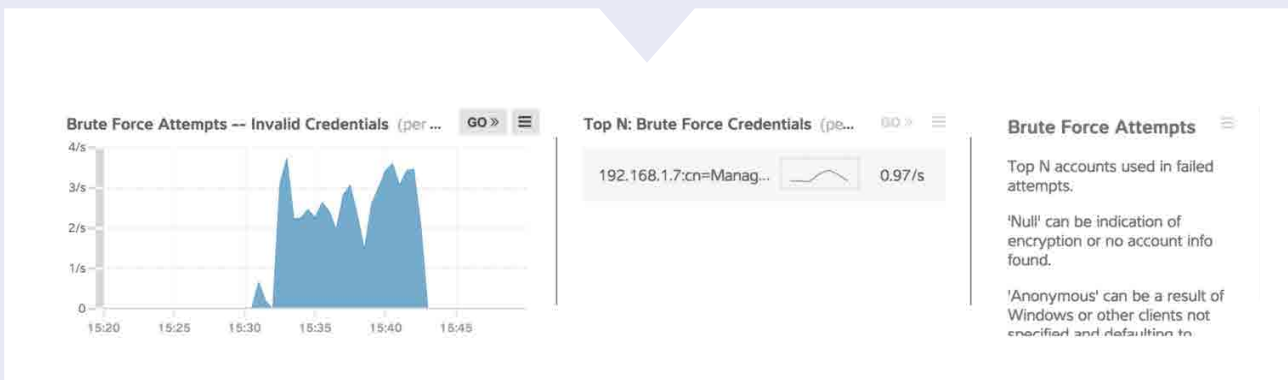
5. Weitere Szenarien

Erkennen eines Proxys mittels WPAD im Netzwerk:

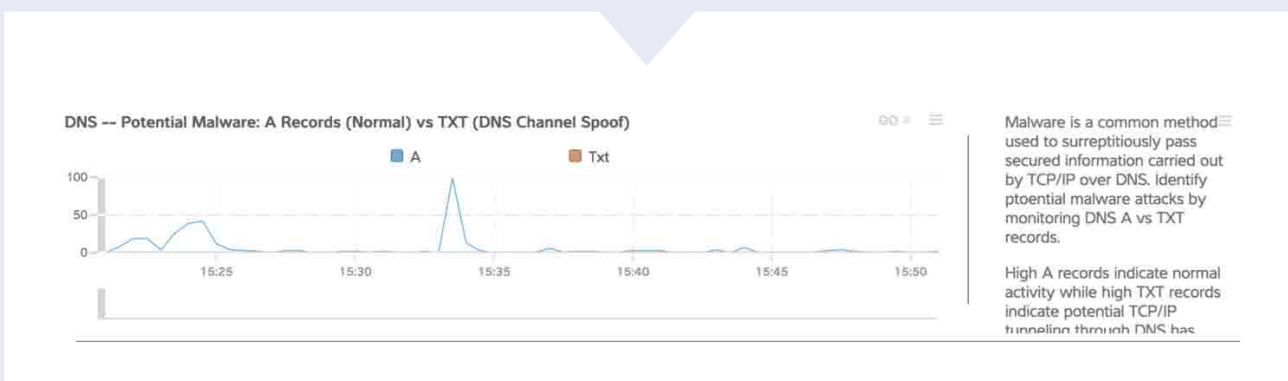


Wenn z.B. ein weiterer Proxy auftaucht, könnte dieses auf einen Angreifer hindeuten, der das Verhalten von WPAD ausnutzt, um jeglichen Webverkehr mitzuschneiden.

LDAP-Brute-Force-Angriffen:



Nachweis von DNS-TXT-Anfragen:



Anfragen via DNS-TXT können auf einen Versuch hindeuten, Protokolle (z.B. SSH, HTTPS) über DNS zu tunneln. Das betroffene Gerät verzeichnet dann ein erhöhtes Aufkommen an DNS-TXT-Anfragen.

Prinzipiell bestehen keinerlei Einschränkungen für mögliche Einsatzszenarien, sofern diese in irgendeiner Form im Datenverkehr erkannt werden können. Voraussetzung dafür ist, dass die ExtraHop Appliance den entsprechenden Datenverkehr scannen kann. Ein weiteres Beispiel wäre die Erkennung von auffälligem Verhalten eines Hosts im Netzwerk (z.B. DNS-Anfragen, Syn-Floods, etc.). Ferner können Anomalien im Datenverkehr als Events getriggert und an die *macutil*-Schnittstelle übergeben werden.

Kontak

macmon secure GmbH
Alte Jakobstraße 79-80 | 10179 Berlin
Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu

Kontakt ExtraHop Networks, Inc.

Christian Buhrow, Sales Director DACH
Mob: +49 172 6639905
cbuhrow@extrahop.com | www.extrahop.com