macmon
nac smartly simple

WHITEPAPER
Linking ExtraHop Wire Data Analytics solution with the compliance module of macmon NAC

TABLE OF CONTENTS

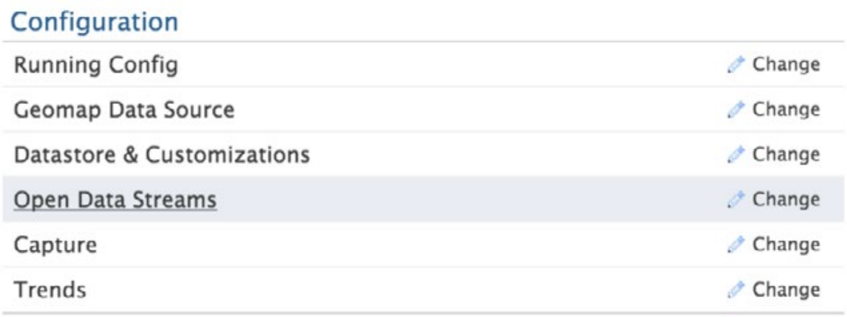
1. Introduction

The ExtraHop Wire Data analysis appliance analyzes the entire Layer 2 to 7 communications and provides through the so correlated data essential information on the performance of popular applications, availability and security. Recognizable attacks generally require immediate action that can be implemented in real time by the macmon Network Access Control solution. The direct coupling of the two systems and the associated automated response to attacks and anomalies will be explained in this paper.

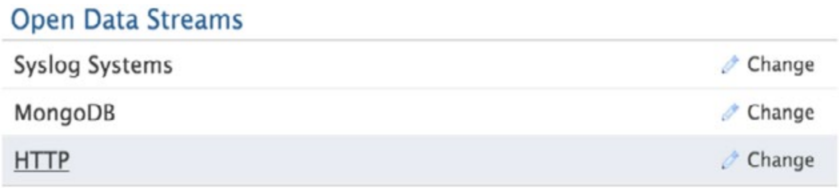
2. Configuration ExtraHop Configuration Open Data Stream (ODS):

The configuration of ODS is done via following menu:

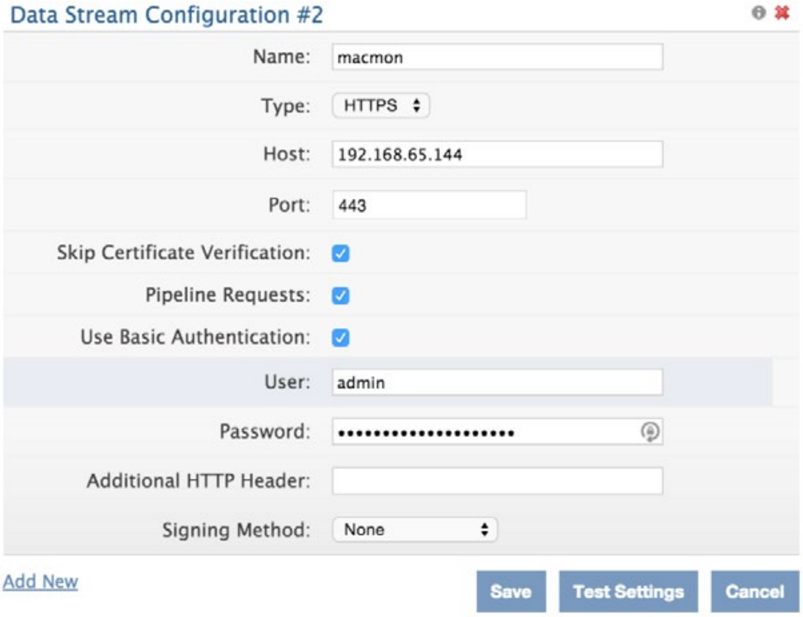
Settings -> Administration -> Open Data Streams



In the menu Open Data Stream choose the subset HTTP.



On the following page change either the settings fort he “default“ entry (the name “default“ cannot be changed), or if default is already in use by another receiver, add a new name. ExtraHop allows up to 16 different Open Data Stream receivers to be configured.



Data Stream Configuration #2

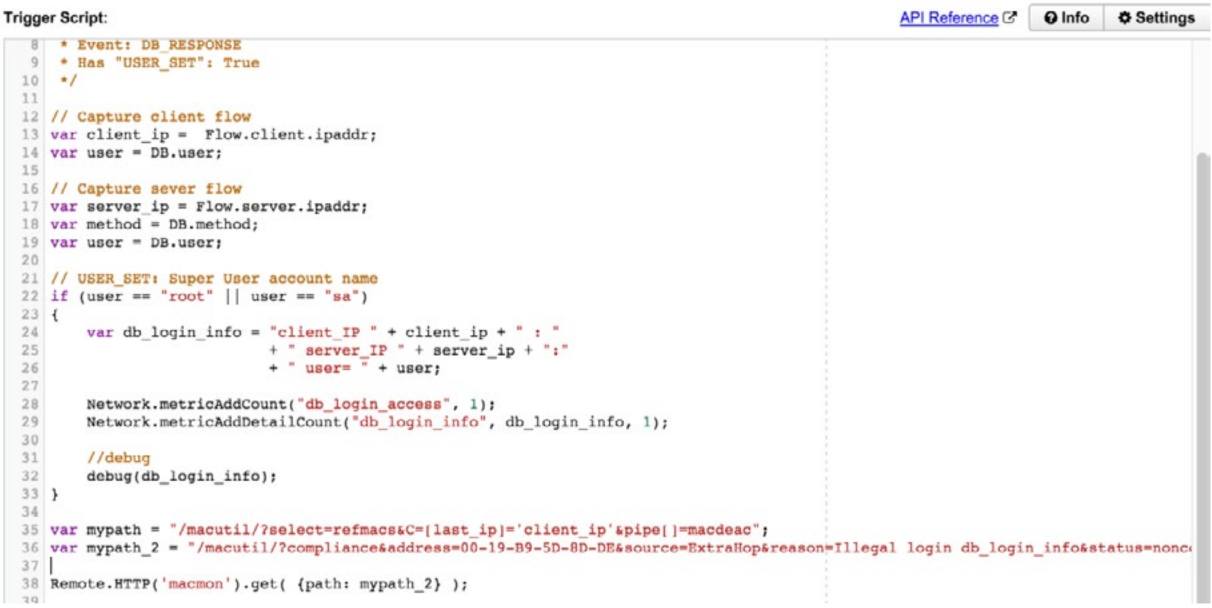
Name:	macmon
Type:	HTTPS
Host:	192.168.65.144
Port:	443
Skip Certificate Verification:	☑
Pipeline Requests:	☑
Use Basic Authentication:	☑
User:	admin
Password:	••••••••••••••••••••
Additional HTTP Header:	
Signing Method:	None

At the line “Host:“ you can either choose to insert an FQDN (fully qualified domain name) or the corresponding IP address of the macmon appliance.

Is there only a “self-signed” certificate placed on the macmon appliance, make sure to check the checkbox “Skip Certificate Validation”.

To hand over events to “Triggers” within the ExtraHop Appliance then do all further configuration the macmon appliance:

With a so-called ExtraHop Trigger, it is possible to hand over every event that can be detected within the real time DataStream to the macmon appliance immediately.



Trigger Script:

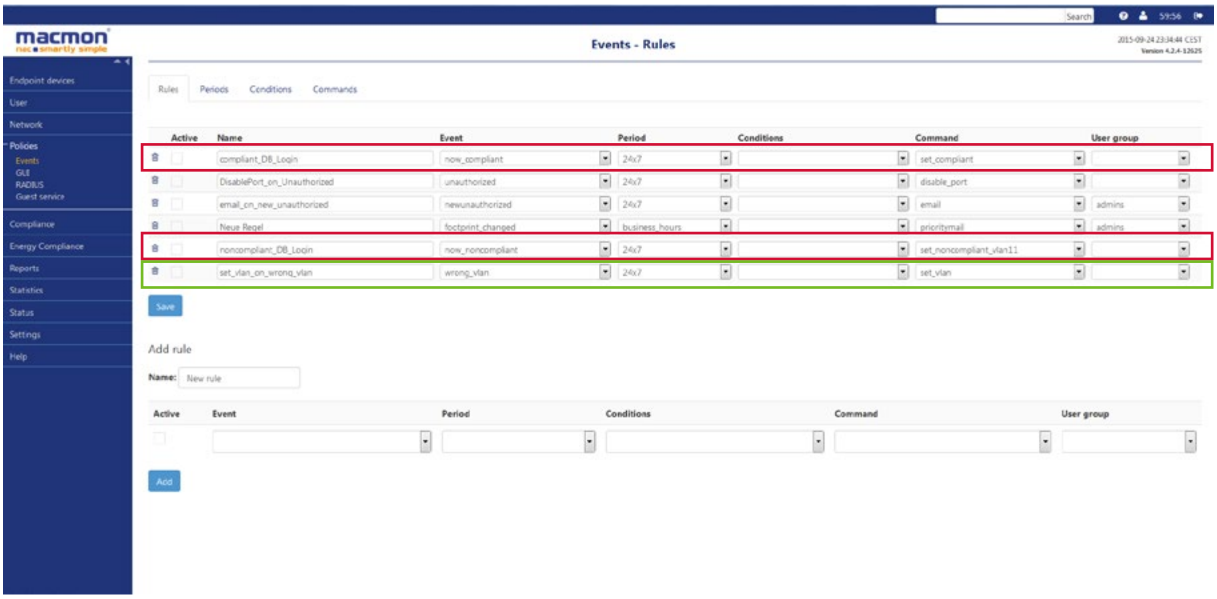
```
 * Event: DB_RESPONSE
 * Has "USER_SET": True
 */

// Capture client flow
var client_ip =  Flow.client.ipaddr;
var user = DB.user;

// Capture sever flow
var server_ip = Flow.server.ipaddr;
var method = DB.method;
var user = DB.user;

// USER_SET: Super User account name
if (user == "root" || user == "sa")
{
    var db_login_info = "client_IP " + client_ip + " : "
                        + " server_IP " + server_ip + ":"
                        + " user= " + user;

    Network.metricAddCount("db_login_access", 1);
    Network.metricAddDetailCount("db_login_info", db_login_info, 1);

    //debug
    debug(db_login_info);
}

var mypath = "/macutil/?select=refmacs&C=[last_ip]='client_ip'&pipe[]=macdeac";
var mypath_2 = "/macutil/?compliance&address=00-19-B9-5D-8D-DE&source=ExtraHop&reason=Illegal login db_login_info&status=nonc

Remote.HTTP('macmon').get( {path: mypath_2} );
```

The used path to hand over events to the macutil interface can be set as a variable within the trigger. The connection towards the macmon appliance is done with the command Remote. HTTP('macmon').get , where 'macmon' corresponds to the name given to the ODS connection in section 2.

If the default ODS Entry is used, the command addition of ('macmon') can be ignored. In this specific case the command Remote.HTTP.get will be enough.

3. Configuration macmon

Should MACs, which do not meet company policy, only be switched to a VLAN or a VLAN with the same name but different VLAN-ID, you should activate the standard rule "set_vlan_on_wrong_vlan" (marked green below) and deposit within "Settings" – "Scan-Engine" in the field "remediation_vlans" the VLAN name or –ID.



Events - Rules

2015-09-24 23:34:44 CEST
Version 4.2.4-12625

Active	Name	Event	Period	Conditions	Command	User group
□	compliant_DB_Login	now_compliant	24x7		set_compliant	
□	DisablePort_on_Unauthorized	unauthorized	24x7		disable_port	
□	email_on_new_unauthorized	newunauthorized	24x7		email	admins
□	Neue Regel	footprint_changed	business_hours		prioritymail	admins
□	noncompliant_DB_Login	now_noncompliant	24x7		set_noncompliant_vlan11	
□	set_vlan_on_wrong_vlan	wrong_vlan	24x7		set_vlan	

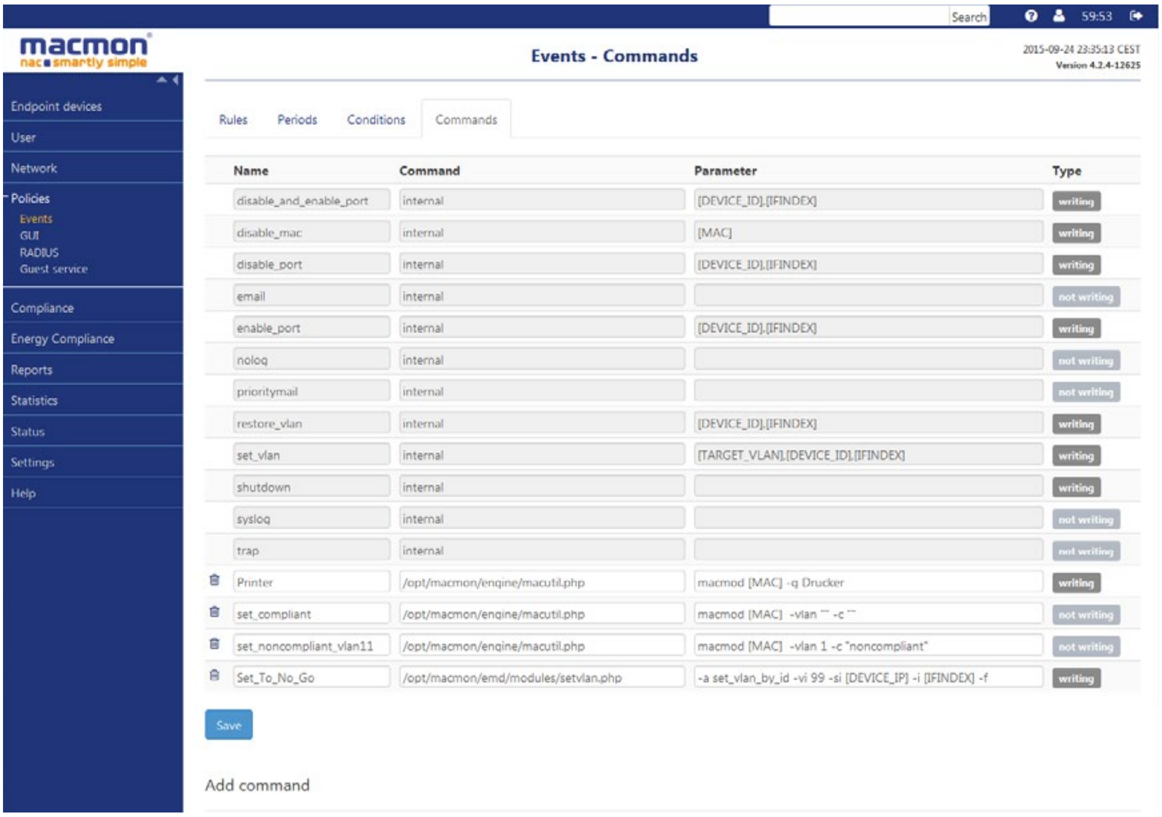
Add rule

Name: New rule

Active	Event	Period	Conditions	Command	User group
□					

In order to respond differentiated to specific compliance statuses (e.g. due to other "Reason"), one uses in addition to the rule "set_vlan_on_wrong_vlan" (green framed) one or more rules analogous to the rule "noncompliant_DB_Login" shown here (red framed), but does not set value for the field "remediation_vlan" in the settings. Herewith a VLAN will be deposited directly to the MAC, which has a higher priority than the MAC group VLAN. With the rule "compliant_DB_Login (framed in red) is the VLAN that has been configured directly on the MAC removed again and the MAC group VLAN becomes active again.

The commands are configured as seen on the right. The interface “macutil” is used to modify MACs for the desired behavior.



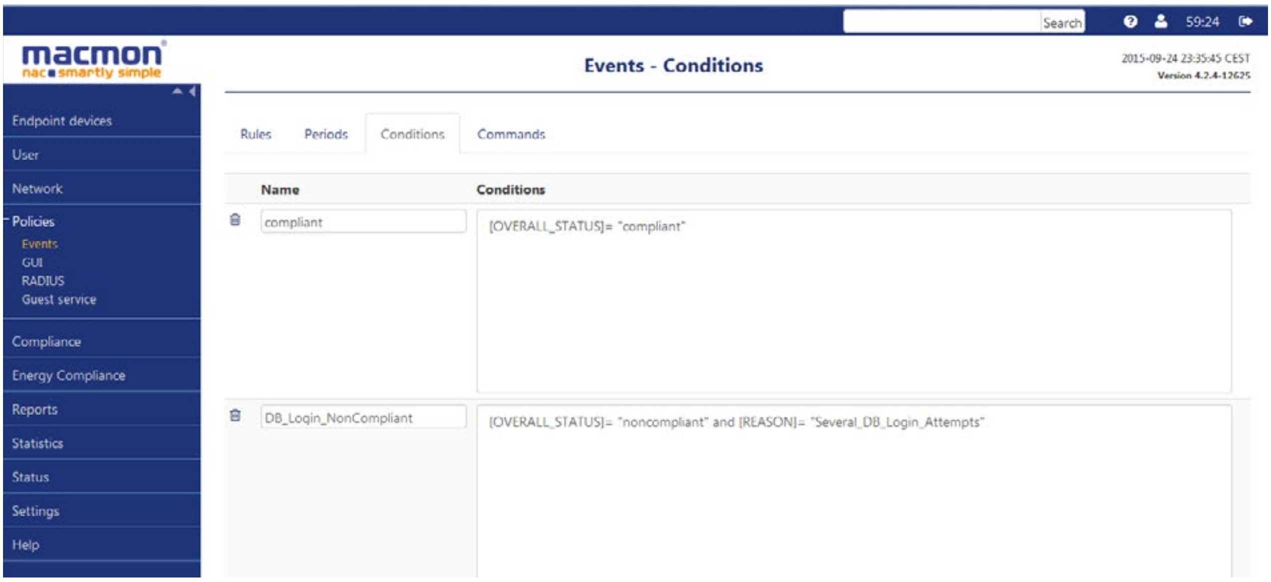
Events - Commands

2015-09-24 23:35:13 CEST
Version 4.2.4-12625

Name	Command	Parameter	Type
disable_and_enable_port	internal	[DEVICE_ID],[IFINDEX]	writing
disable_mac	internal	[MAC]	writing
disable_port	internal	[DEVICE_ID],[IFINDEX]	writing
email	internal		not writing
enable_port	internal	[DEVICE_ID],[IFINDEX]	writing
nolog	internal		not writing
prioritymail	internal		not writing
restore_vlan	internal	[DEVICE_ID],[IFINDEX]	writing
set_vlan	internal	[TARGET_VLAN],[DEVICE_ID],[IFINDEX]	writing
shutdown	internal		writing
syslog	internal		not writing
trap	internal		not writing
Printer	/opt/macmon/engine/macutil.php	macmod [MAC] -q Drucker	writing
set_compliant	/opt/macmon/engine/macutil.php	macmod [MAC] -vlan "" -c ""	not writing
set_noncompliant_vlan11	/opt/macmon/engine/macutil.php	macmod [MAC] -vlan 1 -c "noncompliant"	not writing
Set_To_No_Go	/opt/macmon/emd/modules/setvlan.php	-a set_vlan_by_id -vi 99 -si [DEVICE_IP] -i [IFINDEX] -f	writing

Add command

The conditions used in the rules are generated as follows.



Events - Conditions

2015-09-24 23:35:45 CEST
Version 4.2.4-12625

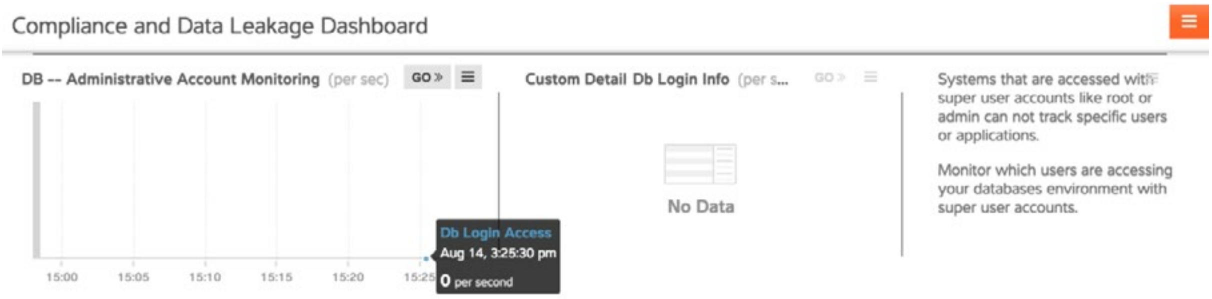
Name	Conditions
compliant	[OVERALL_STATUS]= "compliant"
DB_Login_NonCompliant	[OVERALL_STATUS]= "noncompliant" and [REASON]= "Several_DB_Login_Attempts"

In order to set different VLANs for several scenarios or sites there are further “noncompliant” conditions, likewise the condition “DB_Login_NonCompliant” needed.

4. Flow in case of attack

To demonstrate the functionality serves the following event:
A device in the network (LAN) tries to log on by means of user rights on a database.

View of the ExtraHop dashboards before the occurrence of the event:



Compliance and Data Leakage Dashboard

DB -- Administrative Account Monitoring (per sec)

Custom Detail Db Login Info (per s...

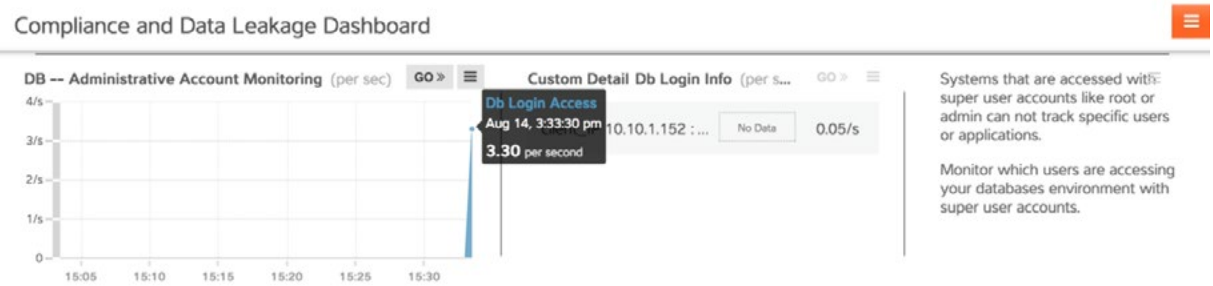
No Data

Systems that are accessed with super user accounts like root or admin can not track specific users or applications.

Monitor which users are accessing your databases environment with super user accounts.

Db Login Access
Aug 14, 3:25:30 pm
0 per second

As soon as the event occurs, ExtraHop immediately recognizes a lot of logins with admin rights on any databases, z. B. MySQL, Postgres, Oracle, MS-SQL, Informix, DB2, Sybase, Sybase IQ and MongoDB.



Compliance and Data Leakage Dashboard

DB -- Administrative Account Monitoring (per sec)

Custom Detail Db Login Info (per s...

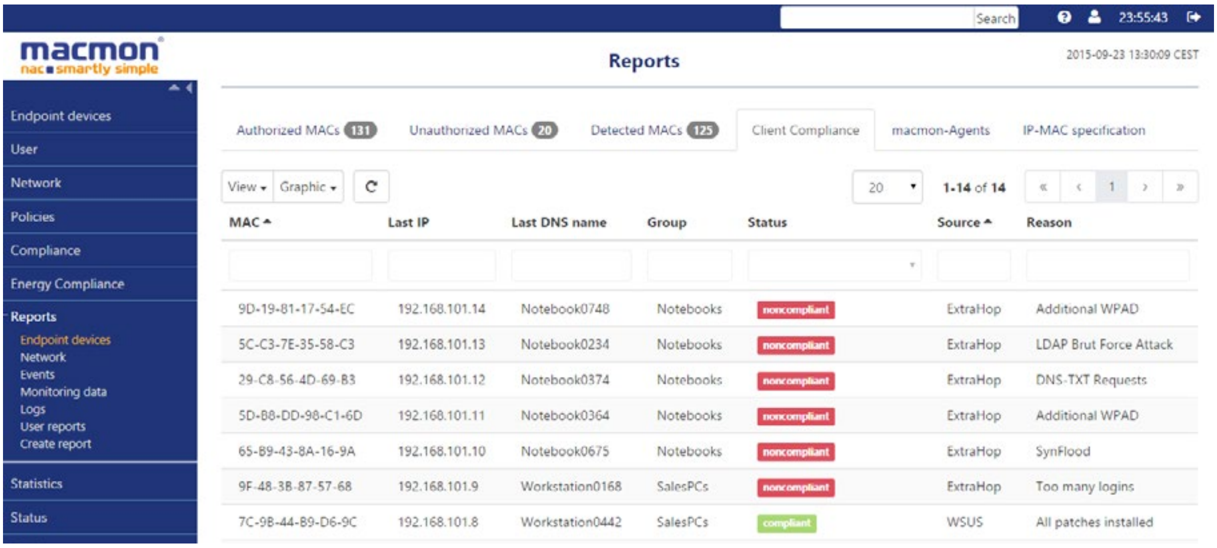
10.10.1.152 : ... No Data 0.05/s

Systems that are accessed with super user accounts like root or admin can not track specific users or applications.

Monitor which users are accessing your databases environment with super user accounts.

Db Login Access
Aug 14, 3:33:30 pm
3.30 per second

After occurrence of the event and by the execution of an HTTP GET command to the macutil interface, the Report page of macmon surface caused by a "trigger" of ExtraHop looks like following:



Reports

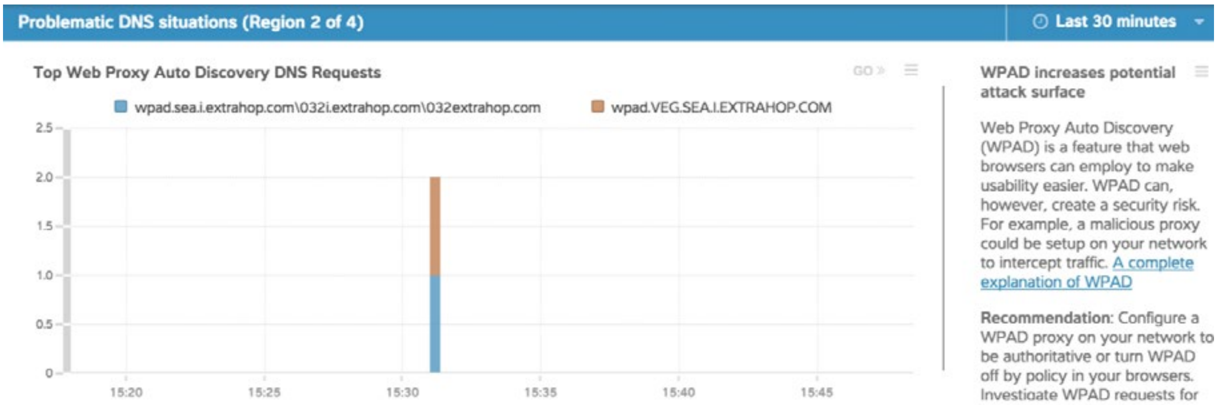
2015-09-23 13:30:09 CEST

MAC	Last IP	Last DNS name	Group	Status	Source	Reason
9D-19-81-17-54-EC	192.168.101.14	Notebook0748	Notebooks	noncompliant	ExtraHop	Additional WPAD
5C-C3-7E-35-58-C3	192.168.101.13	Notebook0234	Notebooks	noncompliant	ExtraHop	LDAP Brut Force Attack
29-C8-56-4D-69-B3	192.168.101.12	Notebook0374	Notebooks	noncompliant	ExtraHop	DNS-TXT Requests
5D-B8-DD-98-C1-6D	192.168.101.11	Notebook0364	Notebooks	noncompliant	ExtraHop	Additional WPAD
65-B9-43-8A-16-9A	192.168.101.10	Notebook0675	Notebooks	noncompliant	ExtraHop	SynFlood
9F-48-3B-87-57-68	192.168.101.9	Workstation0168	SalesPCs	noncompliant	ExtraHop	Too many logins
7C-9B-44-B9-D6-9C	192.168.101.8	Workstation0442	SalesPCs	compliant	WSUS	All patches installed

After macmon has been notified by ExtraHop and the appropriate policies are stored there, a command is executed in accordance with the rules.

5. Further Use Cases

Recognizing a WPAD (Web Proxy Auto Discovery) request in the network


Problematic DNS situations (Region 2 of 4)
Last 30 minutes
Top Web Proxy Auto Discovery DNS Requests
GO »
wpad.sea.i.extrahop.com\032i.extrahop.com\032extrahop.com
wpad.VEG.SEA.I.EXTRAHOP.COM
2.5
2.0
1.5
1.0
0.5
0
15:20
15:25
15:30
15:35
15:40
15:45

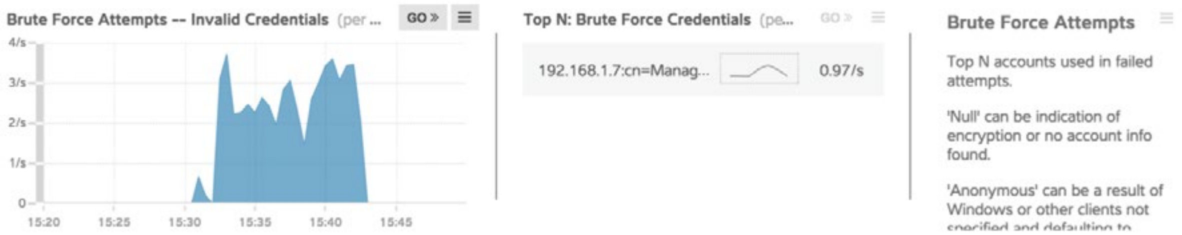
WPAD increases potential attack surface

Web Proxy Auto Discovery (WPAD) is a feature that web browsers can employ to make usability easier. WPAD can, however, create a security risk. For example, a malicious proxy could be setup on your network to intercept traffic. A complete explanation of WPAD

Recommendation: Configure a WPAD proxy on your network to be authoritative or turn WPAD off by policy in your browsers. Investigate WPAD requests for

For example a malicious proxy could be setup on your network to intercept traffic.

LDAP Brute Force attacks:


Brute Force Attempts -- Invalid Credentials (per ...
GO »
4/s
3/s
2/s
1/s
0
15:20
15:25
15:30
15:35
15:40
15:45
Top N: Brute Force Credentials (pe...
GO »

192.168.1.7:cn=Manag... 0.97/s

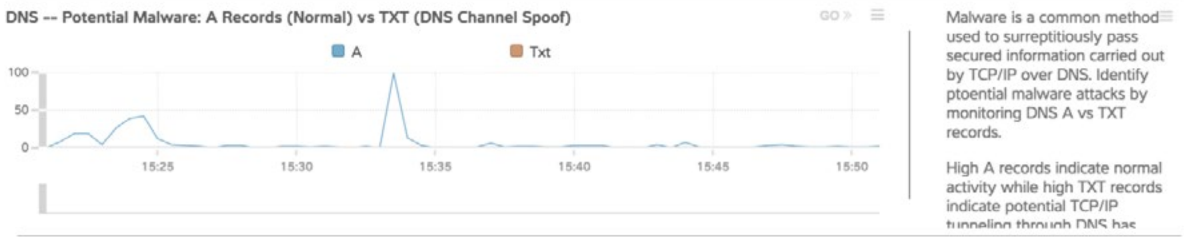
Brute Force Attempts

Top N accounts used in failed attempts.

'Null' can be indication of encryption or no account info found.

'Anonymous' can be a result of Windows or other clients not specified and defaulting to

Detection of DNS TXT queries :


DNS -- Potential Malware: A Records (Normal) vs TXT (DNS Channel Spoof)
GO »
A
Txt
100
50
0
15:25
15:30
15:35
15:40
15:45
15:50

Malware is a common method used to surreptitiously pass secured information carried out by TCP/IP over DNS. Identify ptoential malware attacks by monitoring DNS A vs TXT records.

High A records indicate normal activity while high TXT records indicate potential TCP/IP tunneling through DNS has

DNS-TXT request may indicate an attempt to tunnel protocols (e.g. SSH, HTTPS) via DNS. The affected device then recorded an increased volume of DNS TXT queries.

In principle there are no limitations for possible deployment scenarios, where they may be recognized in some way in traffic (The prerequisite is that the ExtraHop appliance can scan the relevant traffic). A further example would be the detection of behavioral problems of a host on the network (e.g. Russian DNS requests, SYN floods, etc.). Further anomalies can be triggered as events in data traffic and handed over to the macutil interface.

macmon secure GmbH

macmon secure is a German software developer, specialized in network security. The manufacturer-independent and modular NAC solution macmon protects the network against unauthorized, not secured devices and internal attacks. Customers take advantage of the security know-how, projectable costs and a very high security level of the software, with simple handling and operation, the implementation of intelligent technologies, the coupling of macmon with other leading security products and the ongoing broadening of the functional profile, in accordance to the newest developments and standards. The customer base includes international companies from various branches and of various orders of magnitude. The headquarters of macmon secure GmbH are located in Berlin. macmon secure is a member of the Trusted Computing Group and actively participates in various research projects.

ExtraHop

ExtraHop is the global leader in real-time wire data analytics. The ExtraHop Operational Intelligence platform analyzes all L2–L7 communications, including full bidirectional transactional payloads. This innovative approach provides the correlated, cross-tier visibility essential for application performance, availability, and security in today's complex and dynamic IT environments. The winner of numerous awards from Interop, TechTarget, and others, the ExtraHop platform scales up to 40 Gbps in a single appliance, deploys without agents, and delivers tangible value immediately upon deployment. Learn what we mean at www.extrahop.com.

Headquarters of macmon secure GmbH:

Christian Bücker, CEO
Robert Billington, Country Manager
Alte Jakobstraße 79-80 | 10179 Berlin
Phone: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu

Contact ExtraHop Networks, Inc.:

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