1,525 companies with revenues of over $1 billion that have recently experienced data security breaches,

2015 -

[setest@gmail.com](mailto:setest@gmail.com)

10.61.100.249

255.255.255.0

10.61.100.1

8.8.8.8

e

ESGi Managed Cloud Services Provider

Managed cloud means we help design, build, and run your cloud workloads with full support from. Don't waste your limited resources on day-to-day IT maintenance. You focus on growing your business. We'll take care of the cloud.

Scenario 1:

1-5 single end users in office with no DC no exchange no email domain

Windows 7 clients.

Solution:

O365 with Laptops

GMAIL with Local Office installed and Laptops

Thin Client in office for in house permanent staff and Laptop for Executive or remote workers

½ Day Audit

Provision Cloud Desktops

Install and configure on site thin clients

Setup Laptops for Remote Workers

Scenario 2:

On premise SMB Physical Server exchange/file/print no virtualisation and using tape backup

Solution:

Audit 1 Day

Migration Planning/ Cutover

Virtualise Hyper V or VMWare

Replicate to Azure or vCloud

Scenario 3:

SME or corporation with on premise exchange server, file server, application servers with no virtualisation

Scenario 4:

SME or corporation with on premise exchange, active directory, file servers, virtualised

CryptoLocker

46.149.111.28 , 62.76.45.1, 83.69.233.25, 83.69.233.176, 95.59.26.43,   
95.172.146.68, 109.234.154.254, 188.65.211.137, 188.120.255.37, 195.2.77.48

As we said, the infection vector is; vulnerable victim lands in an exploit kit infection page, which exploits a web browser vulnerability and executes malware (ransomware in this case). - See more at: https://www.alienvault.com/open-threat-exchange/blog/urausy-ransomware-family-a-quick-internals-overview#sthash.hHtGmaF6.dpuf

Security operators will see this kind of alarms for other similar ransomware families such as Rannoh, Bomba Locker, Galock or Reveton. - See more at: https://www.alienvault.com/open-threat-exchange/blog/urausy-ransomware-family-a-quick-internals-overview#sthash.hHtGmaF6.dpuf

sudo ifconfig en0 alias 192.168.1.100

**234234234@usa.com**

**Sandbox:**

[**https://www.alienvault.com/live-demo-site/demo-environment**](https://www.alienvault.com/live-demo-site/demo-environment)

**guest**

**alienvault**

**Demo:zcxzcxz**

**https://demo01.alienvault.com/ossim/session/login.php**

**admin**

**ossimdemo1234**

**Designate Admin Interfaces:**

**Ossim**

**Setup OSSEC**

/var/ossec/bin/agent\_control -h

/var/ossec/etc/ossec.conf

tail -f /var/ossec/logs/alerts/alerts.log

**Restart Agents:**

/var/ossec/bin/ossec-control start

/var/ossec/bin/ossec-control stop

**Debug OSSEC:**

/var/ossec/logs/ossec.log

/var/ossec/bin/ossec-control restart

**Update Vulnerability Database**:

Cd /usr/share/ossim/scripts/vulmeter ./updateplugins.pl update wget

**Setup AWS Environment**

setup aws cli

wget https://bootstrap.pypa.io/get-pip.py

sudo pip install awscli

sudo apt-get install python-boto

mv /root/.aws/config /root/.aws/credentials

Access Key:

AKIAI4UKCQU2XNXLQCOA

Secret Access Key

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

./getawslog.py -b xxxx ./getawslog.py -b xxxxxx -l foo.log -d -j -D

xx -l foo.log -d -j -D

**Database Value for wizard:**

echo "update config set value=1 where conf='start\_welcome\_wizard';" | ossim-db

echo "update config set value=1 where conf='start\_welcome\_wizard';" | ossim-db

McAffee Plugin:

/etc/freetds

ms sql 2008

/etc/ossim/agent/plugins/epo mcaffee

Backup and install procedure for the mysql DB

USM vs OSSIM is the code base

**Kyle:** Hi Barry,

use this key

AV1002-010530\_Restore\_Test\_4c88d5f850be4f52917d9cdddb5ae467

and go to this link

<http://offlineupdate.alienvault.com/images/>

or i guess, go to the link first, then use the key in there

it will give you all the available versions

tcpdump -vv host 1.2.3.4 and udp port 1514

sysctl net.ipv4.ip\_forward

echo 1 > /proc/sys/net/ipv4/ip\_forward

urlsnarf –I eth0

driftnet -i eth0

ipscan

macchanger –mac mac eth0

ifconfig eth0 down

setup iptables to redirect HTTP Traffic to sslstrip

iptables –t nat –A PREROUTING –I eth0 –p tcp –dport 80 –j REDIRECT –to-port 8000

python sslstrip.py –l 8000

run arp to direct traffic to me

ettercap –I eth0 –T –q

mail -s "Hello World" user@yourmaildomain.com

Personal information

**Name**

SAles TEst

**Primary email**

corksetest0001@gmail.com

**Recovery email**

bomeara@alienvault.com

**Phone**

amazon

AMI ami-a728e1d0 that is for the EU.  The amazon instructions can be found here:

[https://alienvault.bloomfire.com/posts/822348-amazon-alienvault-usm-appliance-quick-start-guide/public](https://alienvault.bloomfire.com/posts/822348-amazon-alienvault-usm-appliance-quick-start-guide/public" \t "_blank)

Here is a license key for the Amazon appliance as well:

AV1404-019675\_Amazon\_BOmeara\_a572d32641ba43de90127fee0bf6c9ad

LAB KEYs

AV1404-019675\_Barry\_Labkey1\_0bba14c877b142a6a355c45e23fb2fd2

AV1404-019675\_Barry\_Labkey2\_8fd8faf6f78845ac9f209bfd0f148c3a

AV1404-019675\_Barry\_Labkey3\_ea256d1481f74cac81cf7b49205d2989

AV1002-010530\_Threat\_Test\_920ddd83b75b46569b43a82f1e6b038c

AWS Server Sydney IIS Server 2008

54.252.196.51

Solaris:

dladm show-link

**ifconfig qfe1 10.0.0.33 netmask 255.0.0.0**

/etc/inet/hosts

# logadm -w /var/apache/logs/access\_log -s 100m

# logadm -w /var/apache/logs/error\_log -s 10m

# cat /etc/logadm.conf

/etc/default/login

/var/ossec/bin/agent\_control -lc

Competitive Licenses

*Solarwinds*

*Tufin*

*Trustwave Siem LP2*

**ShellShock / BASH** Correlation rule and patch released for updates. Read more here:

[http://www.alienvault.com/open-threat-exchange/blog/attackers-exploiting-shell-shock-cve-2014-6721-in-the-wild/](http://www.alienvault.com/open-threat-exchange/blog/attackers-exploiting-shell-shock-cve-2014-6721-in-the-wild/" \t "_blank)

ncrack -p 22 -user root -P password.txt 10.61.100.147

tcpdump -n -i eth0 host 217.XXX.XXX.XXX

for i in {1..5}; do COMMAND-HERE; done

Repair OpenVAS:

/usr/share/ossim/scripts/vulnmeter/[updateplugins.pl](http://updateplugins.pl/" \t "_blank) update wget

echo ‘<**14**>**sourcehost** message text’ | nc -v -u -w 0 **localhost** 514

nc -u -l -p 17500

sudo ipfw add deny src-ip 192.168.1.20  
sudo ipfw add deny dst-ip 192.168.1.20

cat paloalto.log >> /var/log/paloalto.log

tail –f /var/log/alienvault/agent/agent.log

tail –f /var/log/source.log ~ nc 192.168.1.40 12345

nc –dl 1234 > /var/log/destination.log

Add this to the new syslog conf file in /etc/rsyslog.d/newplugin.conf

if $rawmsg contains '%ASA' then /var/log/cisco-asa.log

& ~

<deviceType>urn:schemas-upnp-org:device:InternetGatewayDevice:1</deviceType>

<presentationURL>http://10.61.100.254:80/</presentationURL>

<friendlyName>VMG8324-B10A</friendlyName>

<manufacturer>ZyXEL</manufacturer>

<modelDescription>MitraStar single-chip ADSL router</modelDescription>

<modelName>VMG8324-B10A</modelName>

<modelNumber>1.0</modelNumber>

<UDN>uuid:107bef75-2f98-982f-75ef-7b107b759800</UDN>

<serviceList>

<service>

Hi Andrea,  
  
As far as I know, we do not have a plugin for Carbon Black but we could certainly create one.  Bit9 is a product that also does application whitelisting and we have a plugin for that already (I don't know how good it is in it's current state) but I don't have any personal experience with either product so I could not recommend one over the other.  
  
Thanks,  
Tom

Scan

Nmap –sS –sV 192.168.1.90

Ncrack

Ncrack –vV –U myusername.txt –P mypassword.txt 192.168.1.90:3389

tail -f /var/log/alienvault/agent/agent.log this is the agent log

core sites

all in one

**nmap --iflist**

**nmap -e eth7 -S 10.154.14.138 10.25.17.45**

<http://www.securonix.com/>

/etc/init.d/ossim-agent restart

sysctl -w net.inet.ip.forwarding=1

**Save field into a variable**

**Jose:** (?P<fieldName>regexp) is a regular expression to save the regexp match into the fieldName variable

in regular expressions this called a named group

inside an alienvault event we have multiple pre-defined fields like src\_ip or dst\_ip ok?

in each plugin rule we need to assign the right information from the event to the right pre-defined (or built-in as you prefer) field. ok?

this src\_ip={$sourceIP} is the way to do it.

**me:** ok cool

can I have access to your system to show multiple connected sensors

we have requests to provide mssp demo

**Jose:** [presales7.alienvault.com](http://presales7.alienvault.com/)is a fed server

[presales11.alienvault.com](http://presales11.alienvault.com/) is a customer aio

this can be useful for you?

I will be rebuilding the system today and tomorrow. when do you have the demo?

**me:** yeah just to show not configure

I am in london next week so its to show then

username and password

**Jose:** admin - alienadmin

 Sent at 10:22 AM on Thursday

**Jose:** in precisely if you want to see alarms from p11 (customer) filter by p11 label

s/precisely/[presales7.alienvault.com](http://presales7.alienvault.com/)

**me:** cool thanks

**Jose:** no prob

datasource group with the right directive events and

apply this group in the policy definition.

while :; do clear; your\_command; sleep 2; done

**Jose:** find the process id

kill -45 xxxx where xxxx is the process id

then tail -f /var/log/alienvault/server/server.log

in sensor is more easy

**me:** eh that will kill the process

**Jose:** no this will send signal 45 to the process

to kill signal is 9

sensor EPS : tail -f /var/log/alienvault/agent/agent.log | grep -i eps

Sensor Update

10.104.10.10 senor disabled

Grouping

Nagios

Email Notification

Null sessions being allowed

False positives handling

Verified logfiles mac address conflict in logfiles

EPS healthy

11,million + in database events

log retention

Hypervisor activity

24,167

23,961

205 free

Support Disabled

Active Directory is one of the most important areas of Windows that should be monitored for intrusion prevention and the auditing required by legislation like HIPAA and Sarbanes-Oxley. I say that because Active Directory is home to objects most associated with user access: user accounts, groups, organizational units and group policy objects. This article deals with monitoring users and groups using the Windows Security Log.

The basic operations of creation, change and deletion of user accounts in AD are tracked with event IDs 624, 642 and 630, respectively. Each of these event IDs provides the name of the user who performed the operation and the name of the user account that was affected as you can see below in the example of event ID 642 which was taken from a Windows 2000 domain controller:

#deb http://http.kali.org/ /kali main contrib non-free

# alienvault-api add\_system

system\_ip or system\_id option needed

Usage: alienvault-api add\_system [--system-ip=<system\_ip> | --system-id=<system\_id>] --password=<root password>

%SystemDrive%\inetpub\logs\LogFiles

cisco router

ssh -c aes256-ctr [root@10.61.100.1](mailto:root@10.61.100.1)

<http://192.168.1.42/?mod=%3Ealert(document.cookie)%3C/script%3E&op=browse>

[61.160.213.190](javascript:void(0);)

netstat -a | egrep 'Proto|LISTEN'

VirtualUSMAllInOne:~# tcprewrite --infile=adobe.pcap --outfile=adobe1.pcap --dstipmap=0.0.0.0/0:192.168.1.95 --enet-dmac=08:00:27:BA:1B:7D

VirtualUSMAllInOne:~# tcprewrite --infile=adobe1.pcap --outfile=adobe2.pcap --srcipmap=0.0.0.0/0:192.168.1.90 --enet-dmac=08:00:27:DC:22:A4

VirtualUSMAllInOne:~# tcprewrite --infile=adobe2.pcap --outfile=adobecomplete.pcap --fixcsum

VirtualUSMAllInOne:~# sudo tcpreplay --intf1=eth0 final.pcap

VBoxManage modifyvm <vmname> –nic# <none or null or nat or bridged or intnet or hostonly>

Aws deployment

Setup Tools

http://docs.aws.amazon.com/AWSEC2/latest/CommandLineReference/set-up-ec2-cli-linux.html#setting\_up\_ec2\_command\_linux

/Users/bomeara/Documents/ec2

./ec2-import-instance "/Users/bomeara/VirtualBox VMs/AlienVault 13/VMWARE-AlienVault\_USM\_All-in-One\_Trial\_4.13.0\_rc772-disk1.vmdk" -f VMDK -t t2.micro -a x86\_64 -b esgirelandtest -o AKIAI736SIPQTP3CQ32Q –w --owner-sak ZgUJrPW1NrK/7YnJrooRWneoSboi7zCLpvtjwHWv -p Linux

ec2-import-instance OpenVAS-7-DEMO-2.2-disk1.vmdk --instance-type t2.micro --format VMDK --architecture x86\_64 --platform Linux --region us-west-1 --owner-akid $AWS\_ACCESS\_KEY --owner-sak $AWS\_SECRET\_KEY --bucket mybucket

curl http://checkip.amazonaws.com

/usr/share/ossim/scripts/regexp.py /var/log/acs.log /etc/ossim/agent/plugins/cisco-acs.cfg y

/var/log/alienvault/device/ipOfDevice

export JAVA\_HOME=$(/usr/libexec/java\_home)

export EC2\_HOME=/Users/bomeara/Documents/ec2

apachectl –V

VPC ID 02

DEFAULT SECURITY GROUP 502

0e8

<agent\_config name="dhcpserver">  
  
  <localfile>  
    <location>%windir%/sysnative/Dhcp/DhcpSrvLog-%a.log</location>  
    <log\_format>syslog</log\_format>  
  </localfile>  
  
</agent\_config>

sudo ifconfig p2p0 ether 3e:68:5e:a7:63:85

openssl rand -hex 6 | sed 's/\(..\)/\1:/g; s/.$//'

sudo /opt/local/bin/etterfilter ig.filter -o ig.ef

ettercap -T -q -F ig.ef -M ARP // //

sudo /opt/local/bin/ettercap -i en0 -T -q -F ig.ef -M ARP /// ///

sudo /opt/local/bin/ettercap -i en0 -T -q -F ig.ef -M ARP /10.61.100.126// ///

mysql -h 192.168.1.42 -u root -e "show databases;";

Net Cat Send Syslog

nc -w0 -u 192.168.1.50 514 <<< "logging from remote"

Access Key ID:

AKIAJ2OLRF6Z4P3DZNOA

Secret Access Key:

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

shipping company multiple container ports

have splunk

after demo like

on premise costs are high due to esxi

vulnerability scan of small sites

10KG Order Profit Margin Calculation:

Total Cost = 200euro Delivered to site.

Unit Weight = 80gm

Total Bars per order = 200 / 80 = 122Bars

Minimum Cost Price Per Unit = 1.70 = 122 \* 1.7 = 207.4

Packaging Costs

596 = 3000 Boxes

596 / 3000 = .20 per box

10KG Total Unit Inc Box Sale Price

Total Price for 122 boxes

.22 x 122 = 26.84

Total Price for 100 Boxed Units

207.4 + 26.84 = 234.24

New Minimum Total Cost Price Including Box

234.24

New Minimum Unit Sales Price:

2.0 = 234.24 = 2.0 x 122 = 244

Extend Trial  
Log in via SSH and jailbreak

Execute ossim-db and enter the following command:

update config set value = '' where conf='license';

\*note that the '' in value = '' is actually two single qoutes

Run alienvault-reconfig and refresh the web UI

OSSEC – Main Registry Keys To Watch

Typically high risk registry keys are:

* HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\\*
* HKEY\_LOCAL\_MACHINE \SYSTEM\CurrentControlSet\Control\Session Manager\\* particularly PendingFileRenameOperations
* HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
* HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\\*
* HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\\*
* HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\\*
* HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\\*

Access Key ID:

AKIAIAWKW4IVK3ZLMN6Q

Secret Access Key:

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

Enterprise logger

so with 5TB we can work for 1024 days

with 9 TB 1843 Days

with 12 TB 2457 days

at 5G per day

172.28.5.247

To fix the issue, re-enable the initial setup wizard (assuming it has already disabled itself) and set the log collection interface to "Not in use."  Not sure if you have needed to re-enabled the setup wizard before so here are the instructions to do that in case you need them:

Log in to the AIO via SSH

Jailbreak to get to the command line

Run 'ossim-db' at the command line

Run the following SQL statement at the "mysql>" prompt

update config set value=1 where conf='start\_welcome\_wizard';

Exit out of the SSH session

Go to the AlienVault web UI and log in - the wizard should start up immediately upon login (if you are already logged in to the web UI, you will need to log out and log back in to start the wizard)

Also, there is a bug in the auto-deployment feature that breaks the auto-deploy when using domain credentials.  We had an email thread that I think you were on but I'll forward that to you just in case.

I hope that all helps but let me know if you have any questions.

Thanks,