THREAT MANAGEMENT AND RISK MITIGATION – Operative instructions

SNMP

Can be activated in Network Settings. Libraesva provides a Zabbix template and a list of the included checks inside:

SNMP Monitor Settings
Zabbix template

SYSLOG

Can be activated and configred in Network Settings.

Syslog settings

Below you can find a list of the significant events to look for:

Bruteforce attempts (fail2ban)

Logs:

*fail2ban.actions: NOTICE [**$jail**] Ban **$ip***
*fail2ban.actions: NOTICE [**$jail**] **$ip** already banned*

$jail value can be:

sshd – SSH login failed attempts
esg-login – HTTP/HTTPS login failed attempts
esg-token – Passwordless login via Cookie/Token failed attempts
esg-sasl – SMTP Auth login failed attempts

$ip is the IP that has been banned.

Account Takeover Protection (Policy Quota)

Log:

***cbpolicyd**[32463]: module=Quotas, action=**defer**, host=1.1.1.1, helo=helo.example.com,*

from=test@example.com, to=recipient@destdomain.com, reason=quota_match, policy=14, quota=24, limit=38, track=Sender:test@example.com, counter=MessageCount, quota=71.16/70 (101.7%)

These logs can be distinguished from other logs of the "**cbpolicyd**" module due to the presence of the "action" field, which can have the value "**reject** – **defer** – **discard** " based on the configured policy.

Whaling Protection

Log:

*MailScanner[26512]: Message **4Qj9QQ73ZNzJt2V** has been blocked as Whaling attack to **Whale whale@example.com***

The fields in **bold** are dynamic and they indicate:

Message ID
Fullname of the Whale
Email address of the Whale

Informations about messages (sender – recipient – subject)

Log:

*MailScanner[19718]: Delivery of **nonspam**:*
*message **4Qj9Pt4vxTzJt2V** from **sender@senddomain.it** to **recipient@destdomain.com** wi th subject **Important – read now!***

The fields in **bold** are dynamic and they indicate:

Message classification (nonspam – spam)
Message ID
From
To
Subject

Spam Report

Log:

MailScanner[24197]:
*Message **4Qj9Q005gDzJt2Y** from **90.30.65.3** (**sender@senddomain.it**)*
*to **domain.com** is **spam**, SpamAssassin (not cached, score=6.584, required 3.99, BAYES_50*

0.80, BOTNET 1.00, CRM114_SPAM 1.50, ESVA_DMARC -0.01, ESVA_EXTERNAL_SOURCE -0.00, ESVA_QS_BLOCK_IF_SUSPICIOUS 0.00, ESVA_QS_TS 0.00, ESVA_TO_INTERNAL -0.01, FOUND_YOU 3.25, NOTBOTNET -1.00, RDNS_NONE 0.50, SPF_HELO_NONE 0.00, SPF_PASS -0.00, T_ESVA_CORONAVIRUS 0.01, T_ESVA_FTS_HIST_GT3M 0.01, T_ESVA_FTS_HIST_LT6M 0.01, URIBL_GREY 0.42, URIBL_SBL_A 0.10)

The fields in **bold** are dynamic and they indicate:

Message ID
Sender IP (source IP)
Sender email address
Recipient relay domain
Categorization

Virus

Log:

*MailScanner[4924]: Infected message **4R1mw10gJMzJsbC** came from **111.90.144.79***

This log can be used to identify messages containing viruses.

The fields in **bold** are dynamic and they indicate:

Message ID
Sender IP (source IP)

Attachmens Filters

Logs:

*MailScanner[16868]: Filetype Checks: File type "**executable**" not allowed (**4R1mtV39SPzJsb6 SHIPPING DOC..exe**)*

*MailScanner[28990]: Filename Checks: File extension "**crt**" not allowed (**4R1ln30NdYzJsYF file.crt**)*

Regex: /File(type|name) Checks: File .* not allowed/

The fields in **bold** are dynamic and they indicate:

File type/name identified (executable, crt, etc…)
Message ID

File name

Quicksand

Logs (regex format)

QuickSand removed file (.?) in ([0-9a-f.]*) because it's encrypted*
QuickSand authorized encrypted archive (.?) in ([0-9a-f.]*)*
QuickSand ignored file (.?) in message ([0-9a-f.]*) because it's allowed by filename rules*
QuickSand ignored file (.?) of size (.*?) in message ([0-9a-f.]*) because it's too big for analysis*
QuickSand blocked message ([0-9a-f.]) with active code because of spam rules*
QuickSand found no active content in file (.?) in ([0-9a-f.]*)*
QuickSand disarmed file (.?)in ([0-9a-f.]*)*
QuickSand disarmed file (.?) from archive (.*?) in ([0-9a-f.]*)*
QuickSand removed archive .? in ([0-9a-f.]*) because it isn't possible to cleanup suspicious content*
QuickSand removed file (.?) from archive (.*?) in ([0-9a-f.]*) because it cannot be disarmed*
QuickSand removed file (.?) from archive (.*?) in ([0-9a-f.]*) because it contains suspicious non cleanable content*
QuickSand removed file (.?) in ([0-9a-f.]*) because it's suspicious and cannot be disarmed*
QuickSand removed file (.?) from archive (.*?) in ([0-9a-f.]*) because it's suspicious*
QuickSand removed file (.?) in ([0-9a-f.]*) because it's suspicious*

The fields extracted from these regex are:

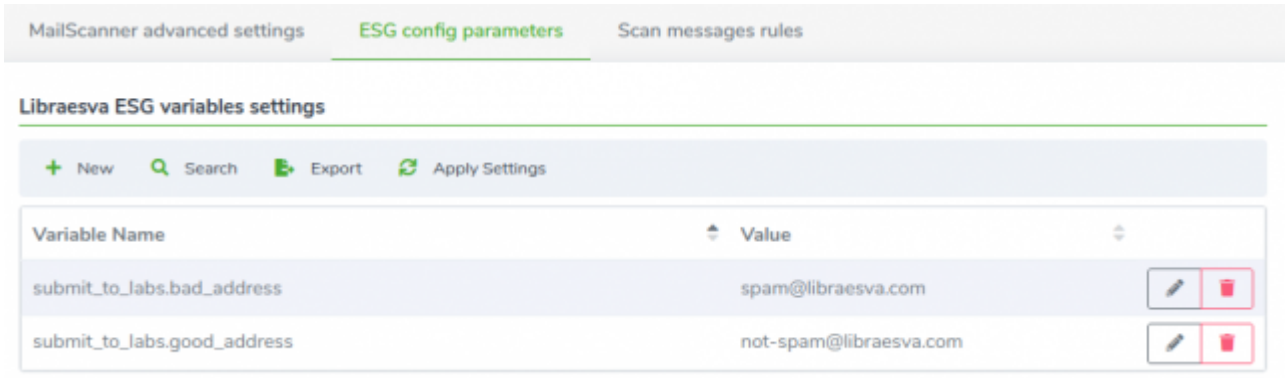
File name / Archive name, size
Message ID

Submit as Good/Bad

It is possible to configure the SOC's address to which you can submit samples from the "Advanced Settings", which can be reached from *https://your-esg/admin/libra_esva_advanced_settings.php*

In this page, select the second tab "**ESG Config Parameters"** and add the following variables, with the desired value:

submit_to_labs.good_address – address to which False Positives are reported
submit_to_labs.bad_address – address to which False Negatives are reported


MailScanner advanced settings
ESG config parameters
Scan messages rules
Libraesva ESG variables settings
New
Search
Export
Apply Settings
Variable Name
Value
submit_to_labs.bad_address
spam@libraesva.com
submit_to_labs.good_address
not-spam@libraesva.com