Senior SOC KB

Prepared by: Aravind C

Senior SOC Analyst

Contents

[Why is the ES Incident Review page still lists deleted Correlation Searches in the Multiselect box "Correlation Search Name"? 3](#_Toc61966878)

[Lookup multiple fields 3](#_Toc61966879)

[7 metrics to measure SOC 3](#_Toc61966880)

[Incident report questionnaire 4](#_Toc61966881)

[Get logged in user from remote computer 5](#_Toc61966882)

[how to delete notables from Splunk ES 5](#_Toc61966883)

[Splunk MSI Agent installation parameters 5](#_Toc61966884)

[To get user account list from windows host 5](#_Toc61966885)

[Retrieve Splunk Password 5](#_Toc61966886)

[Symantec linux client installation 7](#_Toc61966887)

[Socket vs cpu vs core vs threads 8](#_Toc61966888)

[**Rsyslog 8.x configuration** 8](#_Toc61966889)

# Why is the ES Incident Review page still lists deleted Correlation Searches in the Multiselect box "Correlation Search Name"?

* This was built by design because currently the list is populated based on "any correlation we've ever known about"
* This was done because you could potentially have notable events for that correlation even though the correlation was deleted
* There's a proposed enhancement under **SOLNESS-12987** to switch this over to a list that's more intelligent using the notable events on the system

**Workaround:**  
1.) make sure there are no outstanding notable events tied to this correlation search  
2.) remove the correlation search from the kvstore with an inputlookup / outputlookup by the \_key for that correlation search

Example for correlation search "UC-104-TEST"  
Process:  
1) Find the key for the correlation search (e.g. "UC-104-TEST")  
| inputlookup correlationsearches\_lookup | search rule\_name = "UC-104-TEST" | table \_key, rule\_name

Returns:  
"Threat - UC-104-TEST - Rule" for the \_key field

2) Delete the correlation search by using the key  
| inputlookup correlationsearches\_lookup | search \_key!="Threat - UC-104-TEST - Rule" | outputlookup correlationsearches\_lookup

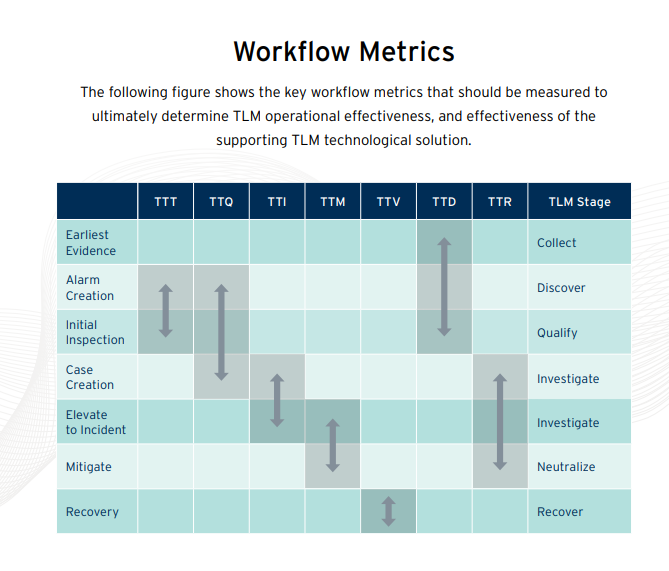
# Lookup multiple fields

1. Note: The lookup command can accept multiple lookup and local fields and destfields. For example:
2. lookup <lookup-table-name> <lookup-field1> AS <local-field1>, <lookup-field2> AS <local-field2> OUTPUTNEW <lookup-destfield1> AS <local-destfield1>, <lookup-destfield2> AS <local-destfield2>

# 7 metrics to measure SOC

* Alarm time to triage
* Alarm time to qualify
* Threat time to investigate
* Time to mitigate
* Time to recover
* Incident time to detect
* Incident time to response

Workflow metrics



# Incident report questionnaire

* What is mode of network communication on this machine, including routing(for e.g. machine is connected via a lease line/wifi and directly connected to internet) ?
* Do the communication going in any way through DU security controls, like Firewall, proxy etc.?
* Is there any Antivirus installed on machine, if yes, which one and when was the last update installed?
* Is there any detection in AV logs?
* From the users experience who were in shifts, did anyone browse or clicked any link from phishing email, any user-based activity.
* Do the users and common account passwords for SDP domain (SOC/NOC/CNOC-Users) have been changed?

# Get logged in user from remote computer

wmic/node:172.28.250.28 computersystem get username

# how to delete notables from Splunk ES

index=notable search\_name="\*your notable title\*" | delete

# Splunk MSI Agent installation parameters

msiexec.exe /i [\\172.28.62.61\OperationsTeam\Splunk\splunkforwarder-7.0.1.msi](file:///\\172.28.62.61\OperationsTeam\Splunk\splunkforwarder-7.0.1.msi) DEPLOYMENT\_SERVER="SP1LVLXSKUS01:8089" LAUNCHSPLUNK=1 AGREETOLICENSE=Yes SERVICESTARTTYPE=auto WINEVENTLOG\_SEC\_ENABLE=1 SET\_ADMIN\_USER=1 /quiet

# To get user account list from windows host

Get-WmiObject -ComputerName localhost -Class Win32\_UserAccount -Filter LocalAccount=”True”| Select PSComputername, Name, Status, Disabled, AccountType, Domain | Out-GridView

To get local group members net localgroup "administrators"

# Retrieve Splunk Password

Splunk’s passwords can be decrypted.

Splunk provides the means to decrypt the passwords.

#### Splunk Versions 7.2.2+

Use the **show-decrypted** CLI command to get the password value.

/opt/splunk/bin/splunk show-decrypted --value $hash

You can also use the **show-encrypted** CLI command to do the reverse if a need arose.

/opt/splunk/bin/splunk show-encrypted --value changeme

#### Splunk Versions 6.3.0 – 7.2.1

This trick is useful for times where your old admin didn’t share the pass4SymmKey or other “encrypted” fields in the config. This method became possible after 6.3.0 when passwords.conf was introduced.

#### Splunk Password Basics

Splunk provides a nice [write up](https://docs.splunk.com/Documentation/Splunk/7.3.0/Security/Deploysecurepasswordsacrossmultipleservers) of how secrets are stored within configuration files on the file system. It’s important to note that when a clear-text password is detected in a “secret” field, the next restart of Splunk will cause this value to become encrypted using the splunk.secret value. This value is generated upon first install and is normally different between Splunk installations, meaning that your encrypted values would be different even if the original clear-text value was identical.

#### Passwords.conf

Add a passwords.conf file in your favorite config directory, ie. /opt/splunk/etc/apps/search/local/passwords.conf, with the following contents.

[credential::admin:]

password=<encrypted\_value\_to\_decrypt>

The example from my test instance.



#### Debug Refresh

Perform a debug refresh to force Splunk to load this new file into active config. Perhaps a restart if you’re getting a Forbidden on this link. (Free users)

https://<your\_ip>:8000/debug/refresh

#### Splunk API for Clear Text

Use the Splunk API to view all the passwords (the one you just added) managed by Splunk via passwords.conf.

https://<your\_ip>:8089/services/admin/passwords



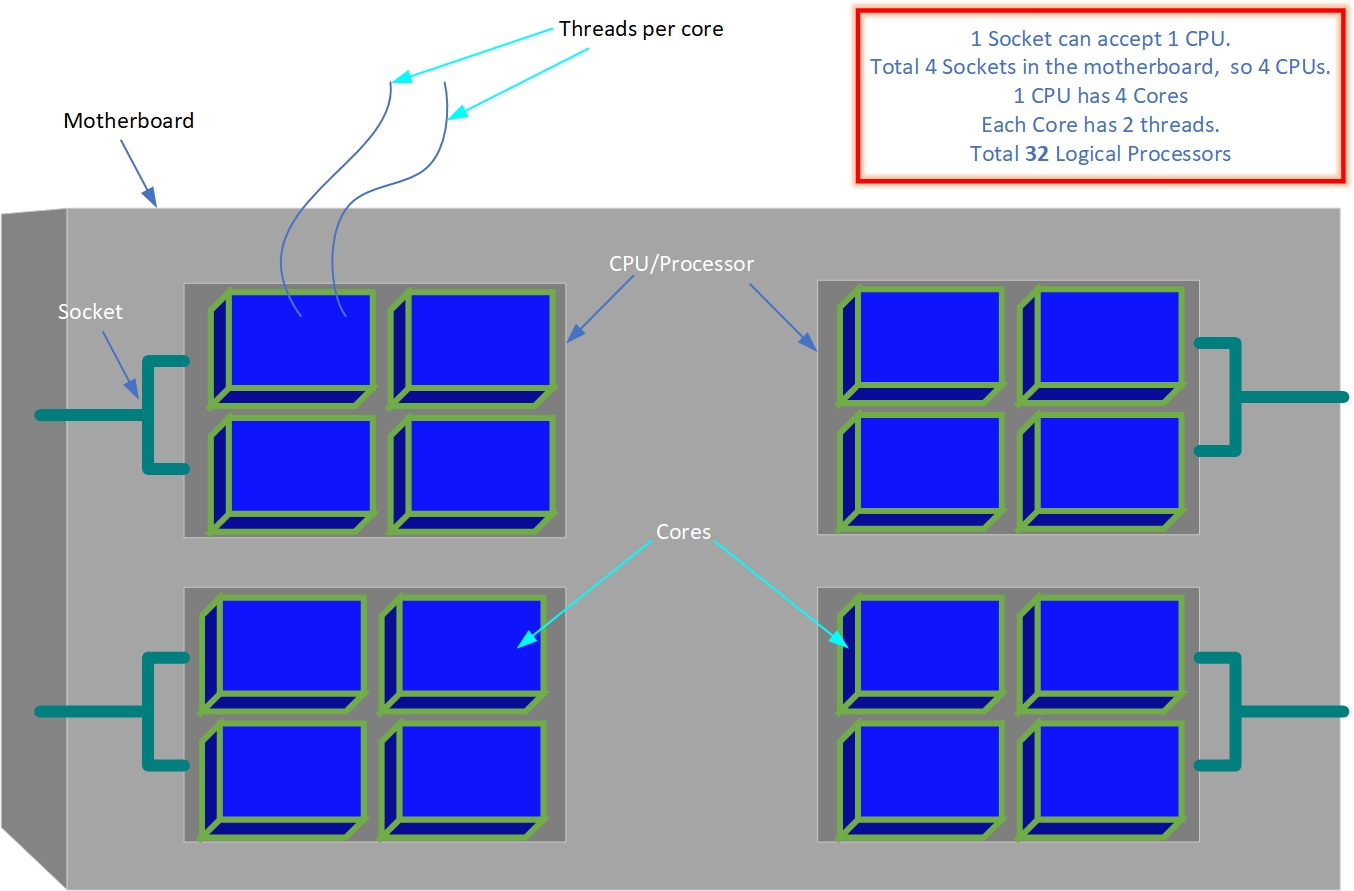
You’ll find the clear-text in the clear\_password field.

Hope this helps with recovering an unknown password.

# Symantec linux client installation

<https://knowledge.broadcom.com/external/article?legacyId=tech255077>

# Socket vs cpu vs core vs threads



# Rsyslog 8.x configuration

/etc/rsyslog.conf

module(load="imudp") # needs to be done just once. **Uncomment to load udp server**

module(load="imtcp") # needs to be done just once. **Uncomment to load tcp server**

/etc/rsyslog.d/abc.conf

#=============================================================================#

input(type="imudp" port="514" ruleset="remote-syslog")

input(type="imudp" port="5514" ruleset="remote-syslog")

#=============================================================================#

input(type="imtcp" port="514" ruleset="remote-syslog")

input(type="imtcp" port="5514" ruleset="remote-syslog")

#=============================================================================#

######## CUSTOM RULESET FOR REMOTE SYSLOG RECEPTION ############

template (name="remote-syslog-write" type="string" string="/your/location/%HOSTNAME%/%$YEAR%%$MONTH%%$DAY%%$HOUR%.log")

ruleset (name="remote-syslog")

{action(type="omfile" dirOwner="loguser" fileOwner="loguser" dirCreateMode="0600" fileCreateMode="0600" dynaFile="remote-syslog-write")}