2.11 - SIEM and HP ArcSight

1. Introduction

PrivateServer provides a generic interface for Security Information Event management (SIEM), that can be extended to support different SIEM products.

We currently have a connector for **HP ArcSight** product to monitor security of internal IT assets and trigger proper alarms whenever required. They require that PrivateServer is properly integrated and could report in real-time any relevant security event to their infrastructure.

Security events are stored in PrivateServer 's operational database and sent to local syslog daemon, which in turn can forward them to HP ArcSight.

Events are formatted according to CEF specification. It's also possible to log security events locally, in case they cannot be sent to point of delivery.

2. Glossary

Here some terms used within ArcSight;

- **Application**: SW component intended to perform core business functionality
- **Application Security Configuration Parameter**: any configuration item with direct impact on application's security
- **Application Security Configuration Target Value:** the value of Application Security Configuration Parameter
- **Application Security Event:** any distinct, time-limited, identifiable activity with direct impact on Application's security
- **Application Security Event Message:** the technical log generated by an Application in reaction to Application Security Event
- **Monitoring:** near real-time validation of Application Security Event Messages, against defined level of escalation (Alert, Record, Log)
- **Application Security Scenario:** identify patterns with respect to defined conditions and trigger action
- **Application Security Scenario Exception:** any exception to define scenario
- **Escalation level:**
    - **Alert:** requires immediate escalation and quick evaluation
    - **Record:** to be included in a report for frequent review
    - **Log:** to be logged with less frequent review

3. List of events

Here follows the list of generated and logged events.

Event Code	Event Name
CC01	Application configuration change
CC02	Security configuration change
HB01	Heartbeat
LL01	Successful User Login
LL02	Successful User Logoff
LL03	User Login failure
LL04	Password change success
LL05	Password change failure
PA01	Successful privileged operation access
PA02	Failed privileged operation access
SA01	Add User
SA02	Amend User
SA03	Delete User
SA04	New Profile
SA05	Amend Profile
SA06	Delete Profile
SA07	Password reset

SA08	Lock user
SA09	Unlock User
SS01	Application Start
SS02	Application Stop
SS03	Application Data Dump
SS04	Application Data Restore
SS05	Logging Change
VU01	Add SIP user
VU02	Edit SIP user
VU03	Delete SIP user
VU04	Activation link sent
VU05	SIP user activated
VU06	SIP user new license activated

4. Pluggable SIEM manager

Given that different customers can have different SIEM systems and/or requirements, we provide a modular and configurable architecture in PrivateServer , to be able to customize these behaviors.

The default implementation generated event in CEF format (suitable for HP ArcSight) and, if properly configured, can send them to local rsyslog daemon.

SIEM configuration is available only via manual file editing.

4.1. Sender configuration

Sending CEF events works this way: the application servr collects events from event database and logs it using log4j. The logging framework sends events to local rsyslogd daemon, which forward them to remote host, usually ArcSight or another CEF compatible SIEM manager.

4.1.1. Log4j configuration

Edit file /data/shared/privateserver/Config.groovy and insert following snipped:

```
import log4j.appender.CustodianDailyRollingFileAppender
// standard configuration to send security events to local rsyslog daemon
log4j = {
    appenders {
        appender    new log4j.appender.AdvSyslogAppender(
                name:      "arcsyslog",
                layout:    pattern(conversionPattern: '%m'),
                facility:  "local7",
                tag:       "Privateserver",
                threshold: org.apache.log4j.Level.INFO,
                syslogHost:"localhost",
                header:    true,
                timeZone:  "GMT"
                )
        appender new CustodianDailyRollingFileAppender(name:'logFile',
                file:"/var/log/tomcat/Privateserver.log",
                datePattern:"'.'yyyy-MM-dd",
                layout: pattern(conversionPattern:'%d [%t] %-5p %c{2} %x - %m%n'),
                compressBackups : 'true',
                maxNumberOfDays : '7')
    }
    root {
        error 'logFile'
    }
    info arcsyslog: "privateserver.siem.CEFSender", additivity : false
}
```

Once you're done just save the file and restart tomcat service so that it loads new configuration:

```
/data/bin/restart-http.sh
```

4.1.2. Rsyslogd configuration

In order to use syslog to receive and forward security events, some changes are required on PrivateServer 's syslog configuration /etc/rsyslog.conf. Open the file and add lines as in following steps:

> ⚠ Message format and priority are fixed and defined.

1. You first need to enable syslog so to listen on UDP port 514:

   ```
   # Provides UDP syslog reception
   $ModLoad imudp.so
   $UDPServerRun 514
   ```

2. Configure template format:

   ```
   $template EVSSFormat,"<%pri%>%timestamp% %hostname% %syslogtag%%msg%\n"
   ```

3. Redirect all events to a local file (this step is optional and often used for debugging purpose):

   ```
   local7.INFO                                                /var/log/arcsight.log;EVSSFormat
   ```

4. Redirect also all the events to a remote host (please note that "remote-host" has to be changed in actual host's name or IP address to make this work):

   > ⚠ Be aware that also remote port 514 has to be checked as a valid one. You better receive remote host configuration parameters and then apply them into rsyslog configuration file

   ```
   local7.INFO @@remote-host:514;EVSSFormat
   ```

   > ℹ Please take note that @@ means TCP connection, as @ is for UDP one

> ⚠ If you configure both forwarding and logging to local files, it is suggested to put forwarding statement AFTER local file statement: if for some reasons, forwarding does not work, you will still have immediate logging on local file. The opposite order could introduce some delay.

Once you're done just save and close /etc/rsyslog.conf. Now you can restart rsyslog so that it loads new configuration:

```
service rsyslog restart
```

> ℹ Here is a list of all available syslog property

4.2. Customer specific formatter configuration

Security event formatter takes many information as inputs and emits one string containing properly formatted event, ready to be forwarded to SIEM. For specific customers' needs, PrivateWave Italia S.r.l. can develop some custom formatter/filters.

If you own yours custom formatter, then you need to enable it appending the following line to file /data/privateserver/Config.groovy so to specify actual formatter class:

```
privateserver.siem.formatter = privateserver.siem.CEFCustomFormatter
```