Slide 1

This is session five about the Semantic Events and Attributes of SAP Enterprise Threat Detection, as of SPS 04 and above.
It assumes that you have watched the prior sessions.

Slide 2

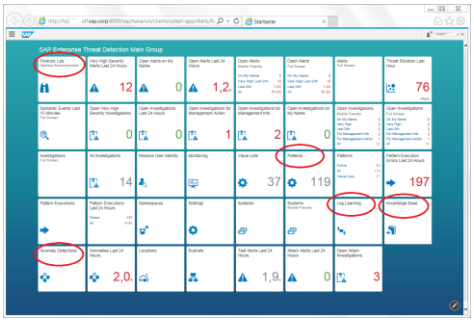
Agenda

What is a trigger?

What are the trigger roles?

Examples of role assignments

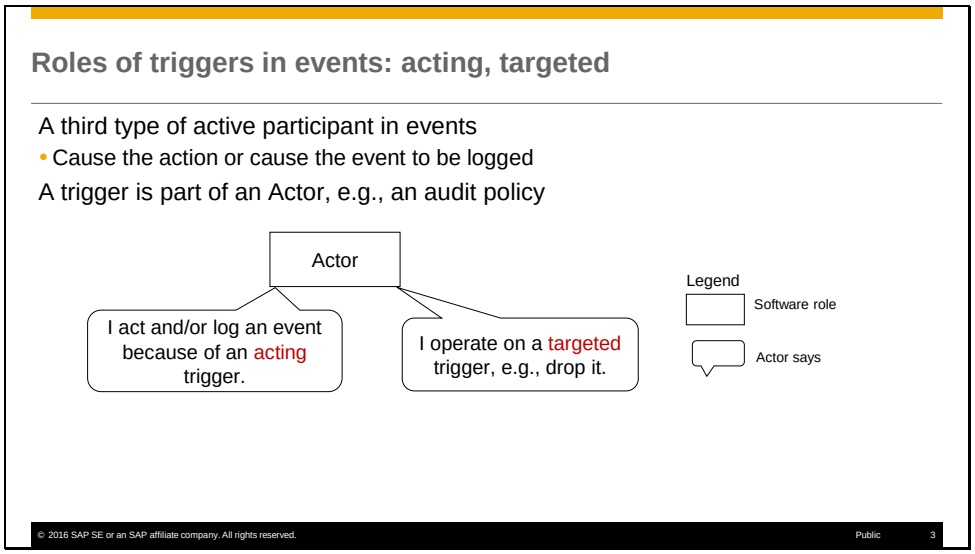
Summary



In this session we focus on triggers.
What are they?
What roles do they have?

We then look at examples of role assignments for triggers to explain how the roles are used.

Slide 3



So far we have seen that machines and users can play different roles in events.
There is a third type of active participant in events, a **trigger**.
A trigger is anything that may cause the action of an event, or cause the event to be logged.

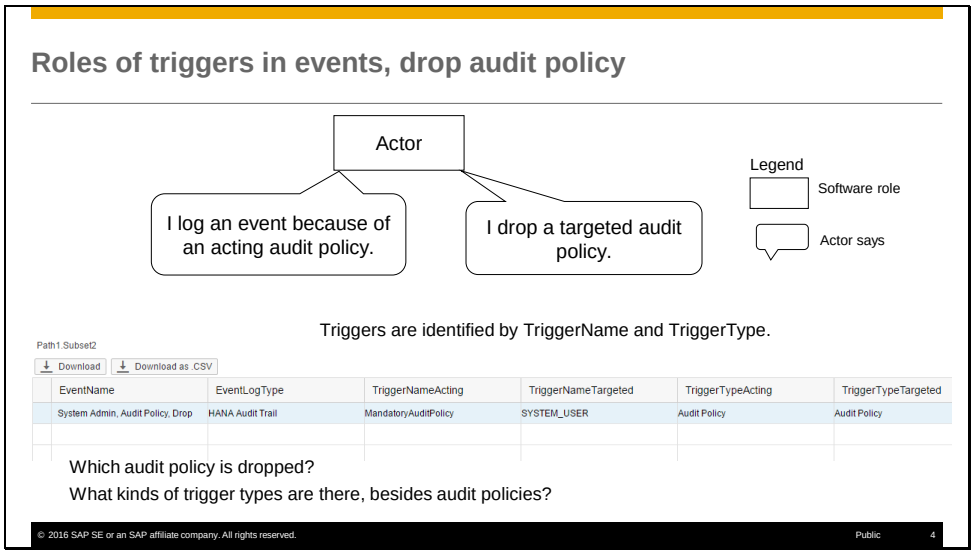
A trigger is part of an actor, for example, an audit policy that controls what is logged by the actor.

A trigger can play one of two roles in an event: **acting** or **targeted:**

At an abstract level, an actor machine might say about an acting trigger:
I act and/or log an event because of an acting trigger.

About a targeted trigger it might say:
I operate on a targeted trigger, e.g., drop it.

Slide 4

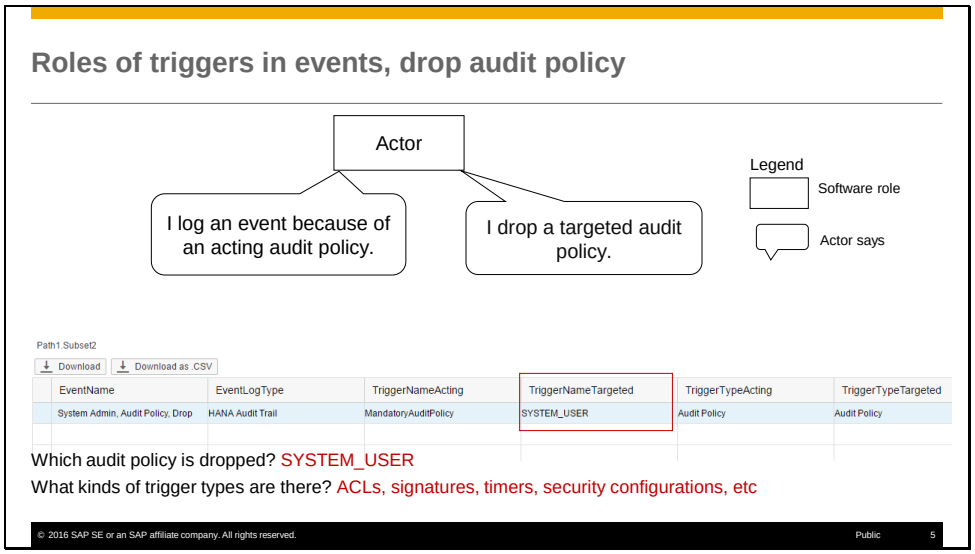


To be more specific, if the actor machine drops an audit policy it says:
'I drop a targeted audit policy.'

This screenshot shows a 'drop audit policy' event that was logged by a HANA System.
HANA Audit Policies control which events are logged in the HANA Audit Trail.

Database administrators can create, drop, alter, enable and disable audit policies.
'Drop' is the same as 'delete'.
As the screenshot shows, triggers are identified by a TriggerType, here 'Audit Policy' and a TriggerName.
Two questions to think about at this point are:
Which audit policy is dropped?
What kinds of trigger types can you think of, besides audit policies?

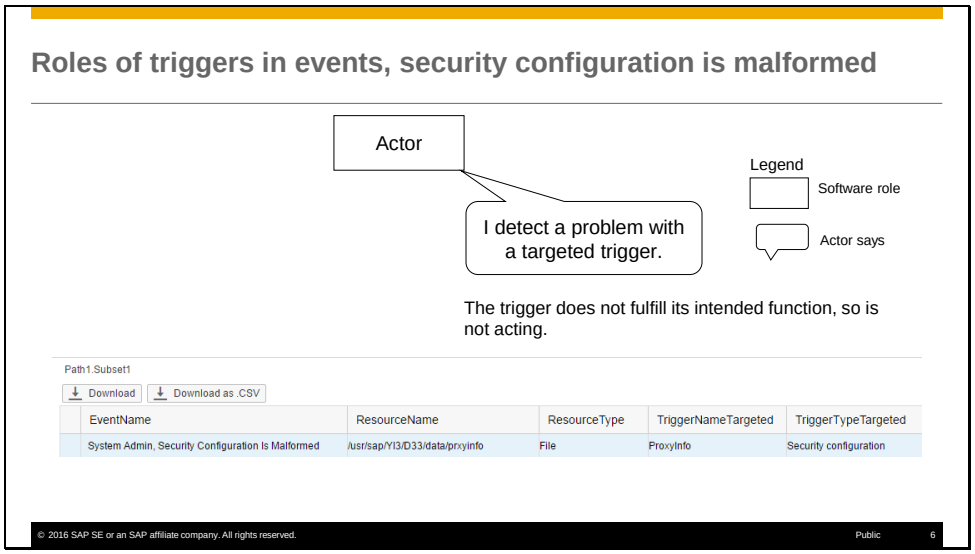
Slide 5



It is the SYSTEM_USER audit policy that is dropped.
It is the targeted policy, because it is the target of the drop action.
The MandatoryAuditPolicy, on the other hand, is the audit policy that caused the event to be logged. It is the acting policy.

What kinds of triggers are there?
If you deal with network logs, one you may have thought of is: access control rules, also called lists or ACLs, for short
Other types are: signatures, timers, and security configurations or policies.
These are all some of the things that may cause an actor machine to perform an action.
An acting ACL, for example, can cause a firewall to block network traffic that matches the ACL.

Slide 6



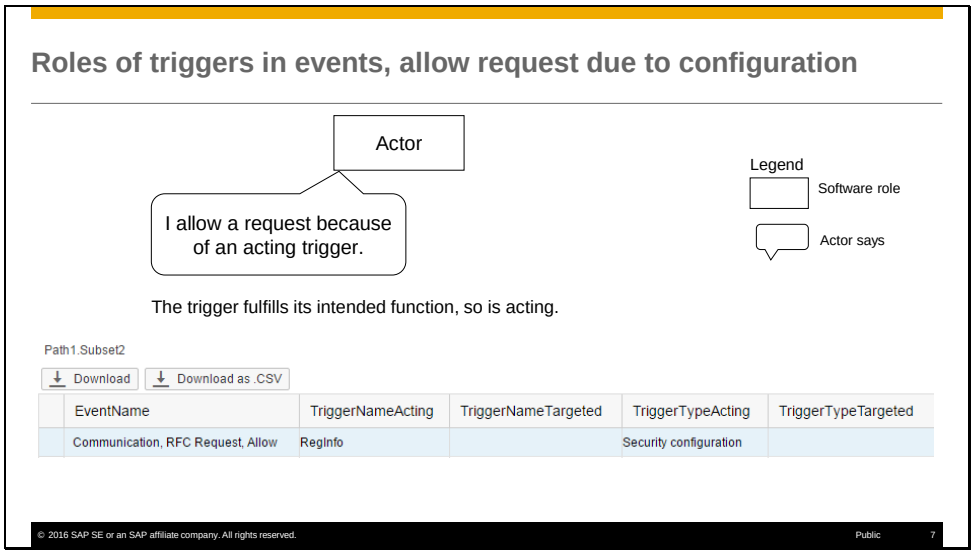
A trigger which is the subject of an observation is also the targeted trigger, as shown in this screenshot.
It displays an event from the RFC Gateway that reports a problem with a security configuration named ProxyInfo.

ProxyInfo is a type of trigger that controls which proxy requests are allowed and which are blocked.

You can think of this event as the Gateway inspecting the trigger and detecting a problem with it. In other words, the trigger is the target or object of a *detect* action performed by the Gateway.

The trigger did not fulfill its intended function of controlling access, so is not the acting trigger.

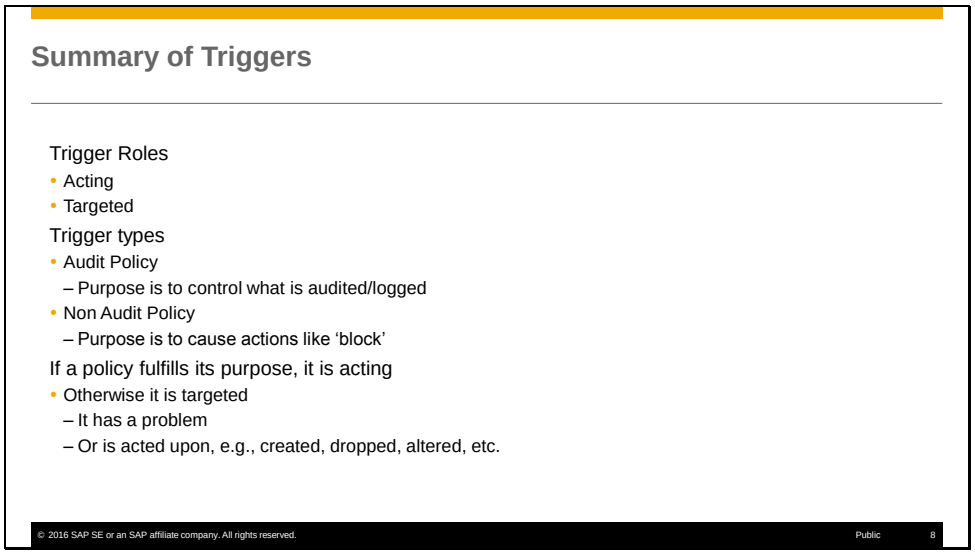
Slide 7



Only when it fulfills its purpose and causes a request to be allowed or blocked is the trigger playing the acting role, as opposed to the targeted role.

An example of this is shown in this screenshot where the RegInfo Security configuration, a type of trigger, caused a request to be allowed.

Slide 8



In summary, a trigger can play one of two roles in a specific event; **acting** or **targeted.**

There are also basically two types of triggers:

- **Audit policies** whose purpose is to control what is audited, that is, logged,
- and **non-audit-policies,** whose purpose is to cause actions, e.g., allow or block requests.

When a trigger fulfills its purpose it plays the acting role in an event, otherwise it plays the targeted role.

As seen in the examples, a targeted trigger is one that is found to have a problem, or one that is acted upon, e.g., created, dropped, altered, etc.

Slide 9