

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

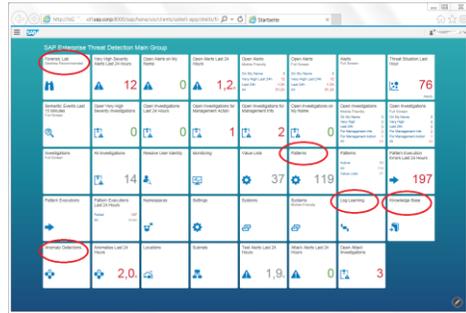
Agenda

What is a trigger?

What are the trigger roles?

Examples of role assignments

Summary

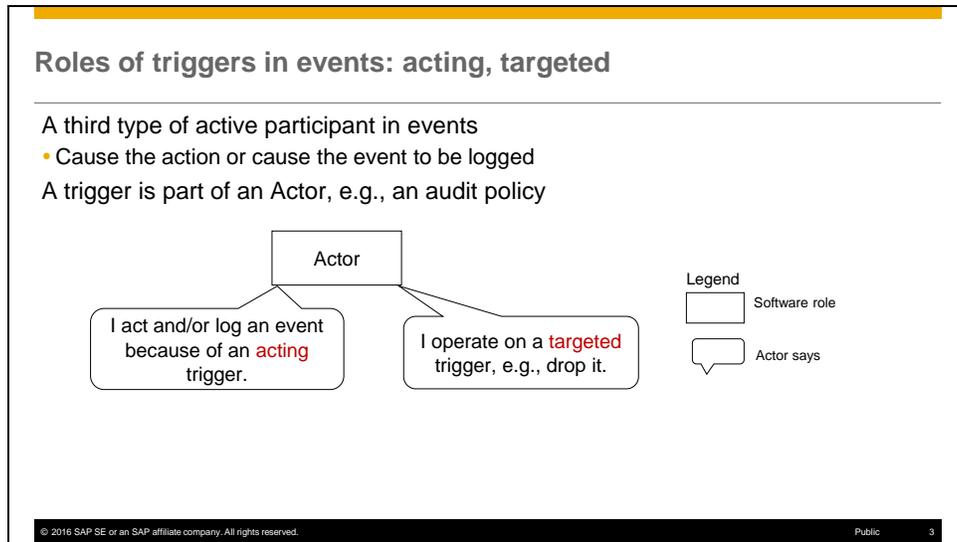


In this session we focus on triggers.

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.



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

Roles of triggers in events, drop audit policy

Triggers are identified by TriggerName and TriggerType.

Path1 Subset2

Download Download as CSV

EventName	EventLogType	TriggerNameActing	TriggerNameTargeted	TriggerTypeActing	TriggerTypeTargeted
System Admin, Audit Policy, Drop	HANA Audit Trail	MandatoryAuditPolicy	SYSTEM_USER	Audit Policy	Audit Policy

Which audit policy is dropped?
What kinds of trigger types are there, besides audit policies?

© 2016 SAP SE or an SAP affiliate company. All rights reserved. Public 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

Roles of triggers in events, drop audit policy

Path1.Subset2

Download Download as CSV

EventName	EventLogType	TriggerNameActing	TriggerNameTargeted	TriggerTypeActing	TriggerTypeTargeted
System Admin, Audit Policy, Drop	HANA Audit Trail	MandatoryAuditPolicy	SYSTEM_USER	Audit Policy	Audit Policy

Which audit policy is dropped? **SYSTEM_USER**

What kinds of trigger types are there? **ACLs, signatures, timers, security configurations, etc**

© 2016 SAP SE or an SAP affiliate company. All rights reserved. Public 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

Roles of triggers in events, security configuration is malformed

Path1.Subset1

[Download](#) [Download as .CSV](#)

EventName	ResourceName	ResourceType	TriggerNameTargeted	TriggerTypeTargeted
System Admin, Security Configuration is Malformed	/usr/sap/Y13/D33/data/proxyinfo	File	ProxyInfo	Security configuration

© 2016 SAP SE or an SAP affiliate company. All rights reserved. Public 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

Roles of triggers in events, allow request due to configuration

The trigger fulfills its intended function, so is acting.

Path1.Subset2

[Download](#) [Download as .CSV](#)

EventName	TriggerNameActing	TriggerNameTargeted	TriggerTypeActing	TriggerTypeTargeted
Communication, RFC Request, Allow	RegInfo		Security configuration	

© 2016 SAP SE or an SAP affiliate company. All rights reserved. Public 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.

Summary of Triggers

Trigger Roles

- Acting
- Targeted

Trigger types

- Audit Policy
 - Purpose is to control what is audited/logged
- Non Audit Policy
 - Purpose is to cause actions like 'block'

If a policy fulfills its purpose, it is acting

- Otherwise it is targeted
 - It has a problem
 - Or is acted upon, e.g., created, dropped, altered, etc.

© 2016 SAP SE or an SAP affiliate company. All rights reserved. Public 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.

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see <http://global12.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.