Slide 1

This is session four 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

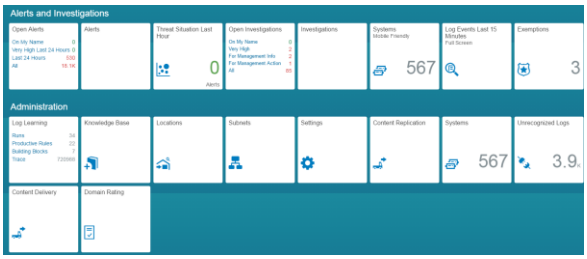
Agenda

Clearing up a misconception

A more accurate conception
- User account domain
- User role
- Pseudonym, person, account

Examples of user roles in events

Summary

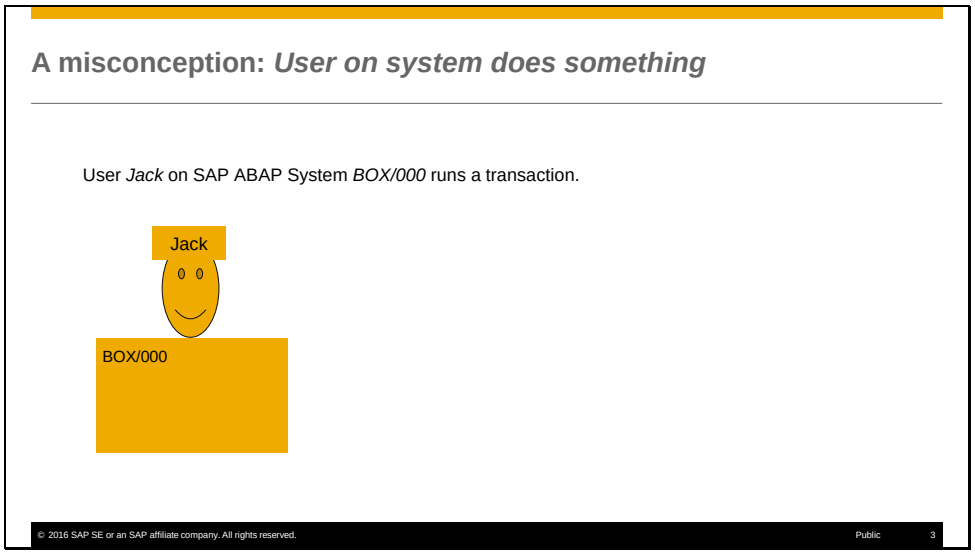


This session is about the roles that users can play in events.
But, first a misconception about users and machines needs to be recognized and cleared up.
Then a more accurate conception is adopted based on the concepts:

- User account domain
- User role
- Pseudonym, person and account.

Then we look at examples of user-related events to show assignments of users to roles.

Slide 3



A common turn of phrase is ‘A user on a system does something.’
For example User Jack on SAP ABAP System Box/000 runs a transaction.’
But, this is a misconception.

Slide 4

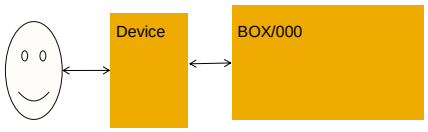
A more accurate model

Concept

It is actually *John* who uses a d*evice* to initiate action by Box/000. Device is Initiator. Box/000 is Actor.

John uses his account *Jack.*

The code on Box/000 runs under the account *Jack*.



John invisible,

only user accounts visible in logs

A more accurate model of the situation distinguishes between persons and user accounts.
It is actually a person, say, John, who uses a device to initiate some action by Box/000.
Recall that these two machines have the roles initiator and actor.
John uses his account *Jack* that is valid on Box/000.
The code on Box/000 runs under the account Jack.
John himself is not visible in the logs, only the user accounts are written to the software logs.

Slide 5

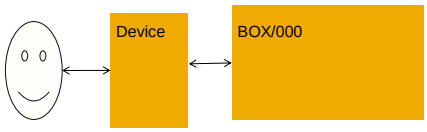
A more accurate model

Concept

It is actually *John* who uses a d*evice* to initiate action by Box/000. Device is Initiator. Box/000 is Actor.

John uses his account *Jack*.

The code on Box/000 runs under the account *Jack*.



John invisible,

only user accounts visible in logs

Corresponding Semantic Attributes

Accounts

- *Jack* is a user account of *John*.
- How to resolve *Jack* to *John*?
- Thru triple with domain of validity of *Jack*
- (username, username domain type, username domain name)<role>

Triple for this example, without role part?

This more accurate conception results in a set of Semantic Attributes that model user accounts and the roles they play in events.
For logs which contain user accounts, the question is how to resolve the account to a person, e.g., how to resolve Jack to John.
The answer is to add the domain of validity to the account name.
You can think of the ‘domain of validity’ as where you can go to resolve Jack to the person John.
Like an SAP system, the domain is identified by a type and ID, called a name, in this case.
Thus, accounts are always a triple of attributes: username, domain type and domain name.
Username contains the account name.
You can probably guess what the triple is for this example. Just leave the role unspecified for now.

Slide 6

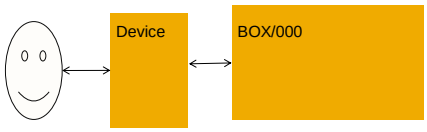
A more accurate model

Concept

It is actually *John* who uses a d*evice* to initiate action by Box/000. Device is Initiator. Box/000 is Actor.

John uses his account *Jack*.

The code on Box/000 runs under the account *Jack*.



John invisible,

only user accounts visible in logs

Corresponding Semantic Attributes

Accounts

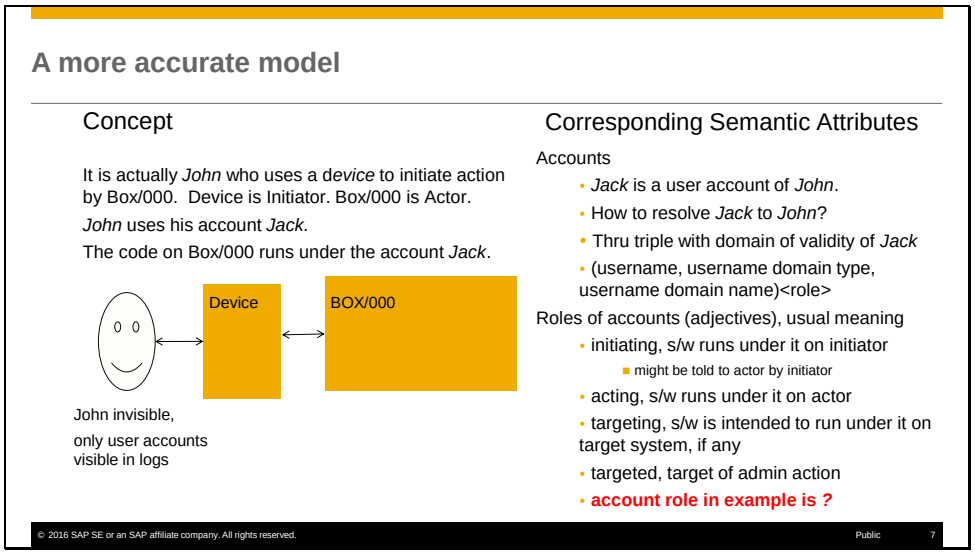
- *Jack* is a user account of *John*.
- How to resolve *Jack* to *John*?
- Thru triple with domain of validity of *Jack*
- (username, username domain type, username domain name)<role>

Triple for this example?

- Username<role> = 'Jack'
- Username Domain Type<role> = 'ABAP'
- Username Domain Name<role> = 'BOX/000'

The answer is:
The Username is 'Jack', the account name.
The domain type is 'ABAP',
and the domain name is box/000.

Slide 7



Now let's look at the roles for accounts.
They are named using adjectives, whereas machine roles are named with nouns. It's one way to tell them apart, and to remember them.
Recall that machines have 5 roles: initiator, actor, target, intermediary and reporter.

Accounts have 4 roles:

- Initiating, which is the account the initiator machine runs under. The actor is sometimes told this by the initiator.
- Acting, which is the account the actor machine runs under.
- Targeting, which is the account that software on a target machine is intended to run under.
- And, finally targeted, which is the target of an administrative action like 'delete account'.

So, what do you think the account role is in this example?

Slide 8

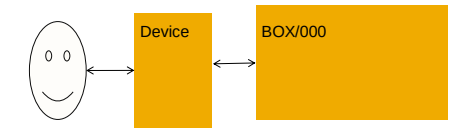
A more accurate model

Concept

It is actually *John* who uses a d*evice* to initiate action by Box/000. Device is Initiator. Box/000 is Actor.

John uses his account *Jack.*

The code on Box/000 runs under the account *Jack*.



John invisible,

only user accounts visible in logs

Corresponding Semantic Attributes

Accounts

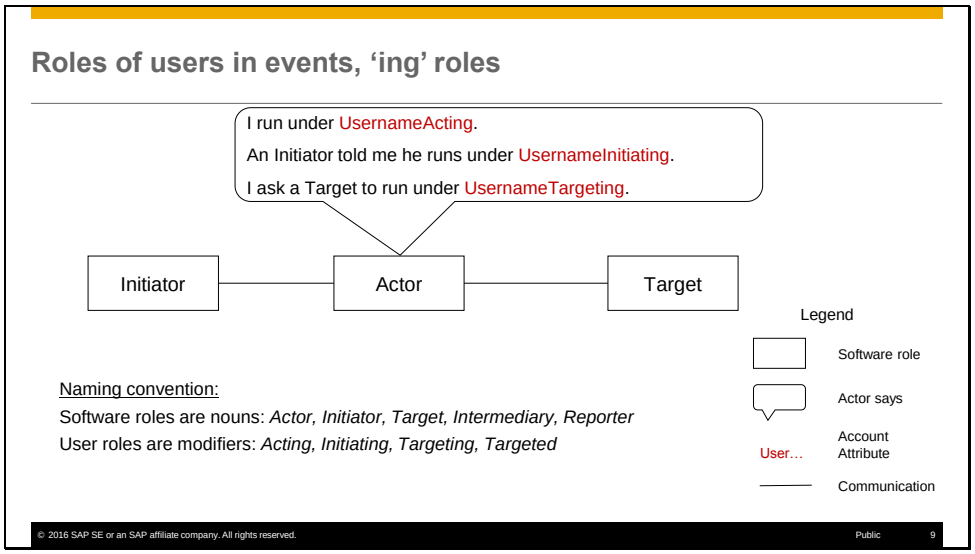
- *Jack* is a user account of *John*.
- How to resolve *Jack* to *John*?
- Thru triple with domain of validity of *Jack*
- (username, username domain type, username domain id)<role>

Roles of accounts (adjectives), usual meaning

- initiating, s/w runs under it on initiator
  - might be told to actor by initiator
- acting, s/w runs under it on actor
- targeting, s/w is intended to run under it on target system, if any
- targeted, target of admin action
- **account role in example is *?* *Acting***

The answer is acting, because the account is the one that the code runs under on the actor machine.

Slide 9

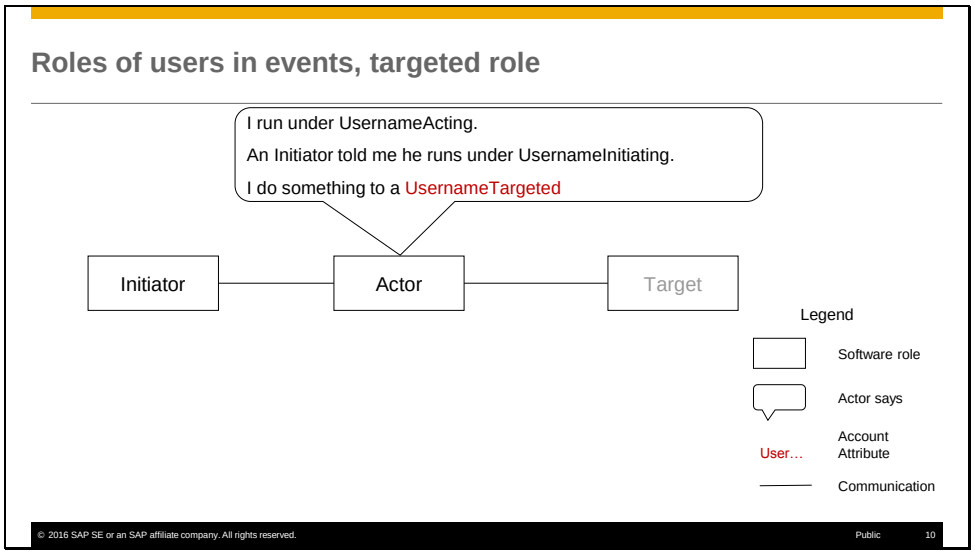


Here is a graphical summary of the user account roles ending in ‘ing’. Note that ‘user’ means ‘user account’, as opposed to a person.
An actor machine tells you what it does and which accounts are involved.
It says:

- I run under UsernameActing.
- An Initiator machine told me that he runs under UsernameInitiating.
- I ask a Target machine to run under UsernameTargeting.

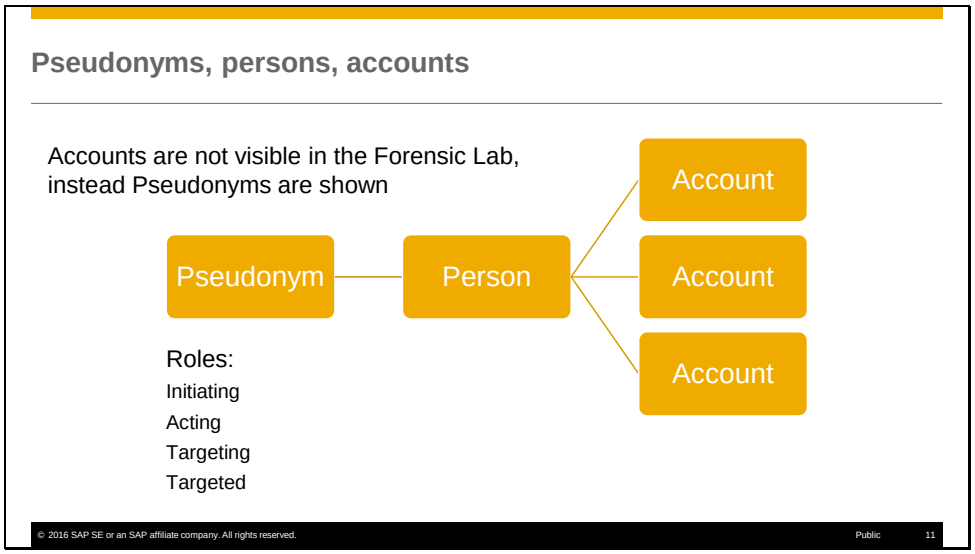
As said, by convention the roles of machines are nouns, and the roles of accounts are modifiers/adjectives. Notice also the correspondence between ‘ing’ roles and machine roles.

Slide 10



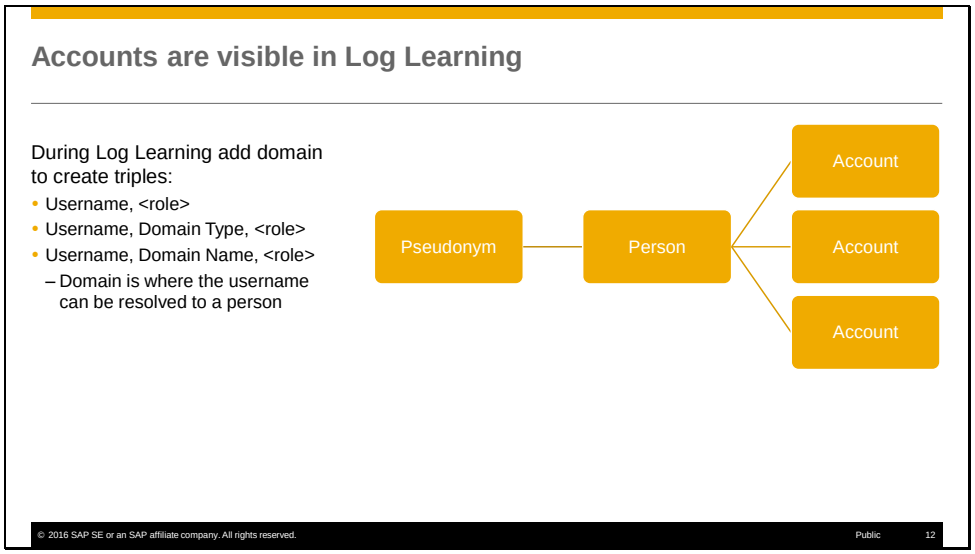
The targeted role is different from the ‘ing’ roles.
Rather than identifying an account that software runs under, it identifies an account that is acted upon.
For example, the account may be deleted.
Note that in the case of centralized user management the domain of the targeted account may differ from the domain of the acting account.

Slide 11



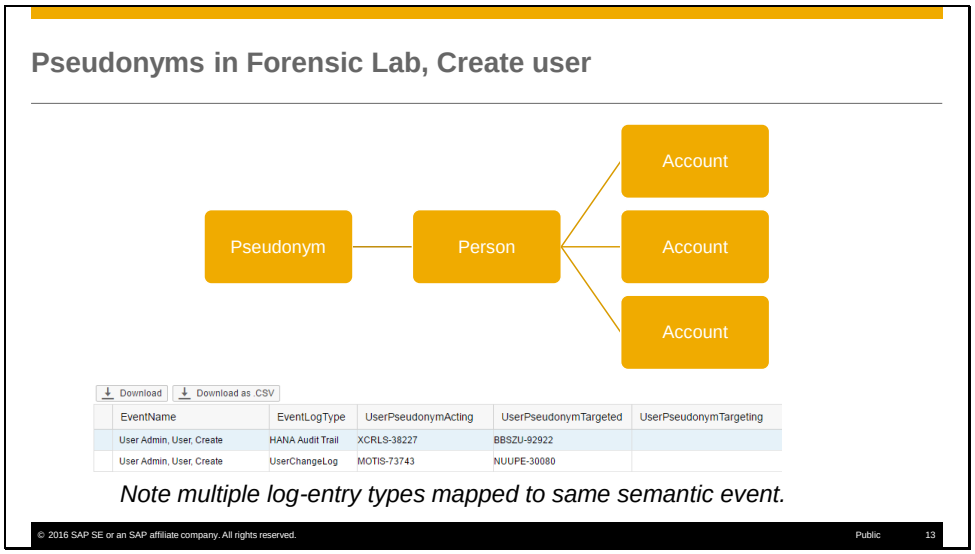
For privacy reasons, user accounts are not visible in the forensic lab.
Instead pseudonyms are shown.
So, how do pseudonyms relate to user accounts?
The answer is that each pseudonym is intended to represent one person. And that person can have multiple accounts.
Person to account relationships can be loaded into ETD from outside sources, so that persons and accounts are accurately associated.
Since they correspond to accounts, the pseudonyms can have the same roles as the accounts: initiating, acting, targeting and targeted.

Slide 12



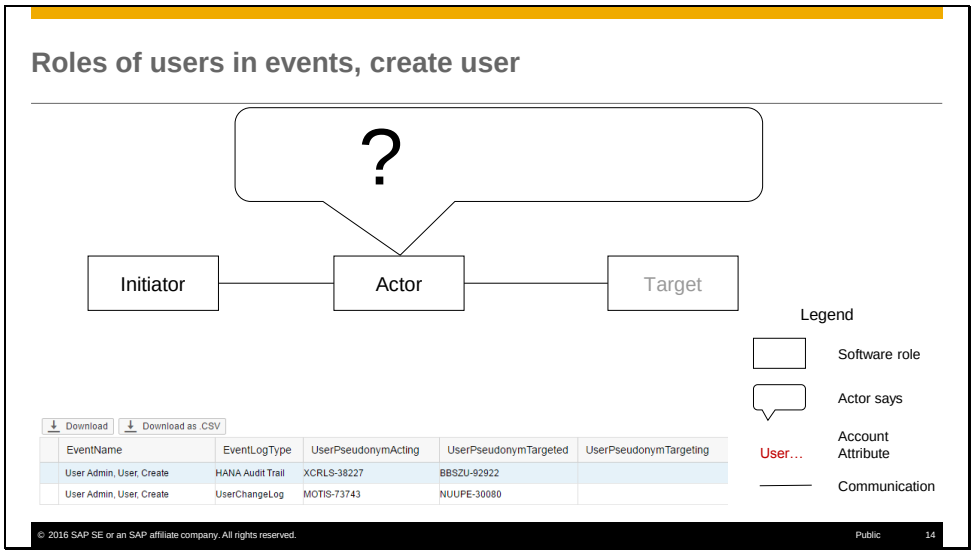
You will see accounts in Log Learning, if you learn a log that contains them.
Normally, the domain will not be in the log, so you need to add it during Log Learning.
Then you will have account triples and will know the domain of validity of the account, that is, where to go to resolve the account to a person.

Slide 13



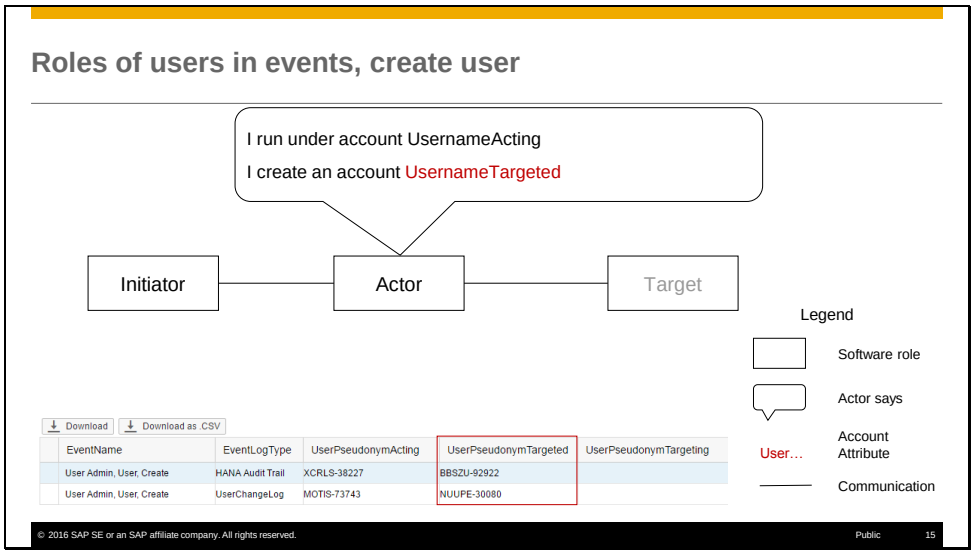
Here is an example of user roles in two ‘create user’ events, as seen in the Forensic Lab.
One thing to note is that the two events come from two different sources, one from a HANA system, and one from a User Change Log of an SAP ABAP system.
This is an example of how Semantic Events enable cross-log correlation. Here, a search for one semantic event finds events from multiple sources.

Slide 14



Some questions are:
What does the actor machine say in the log entries corresponding to the ‘create user’ event?
For which pseudonyms were accounts created?

Slide 15

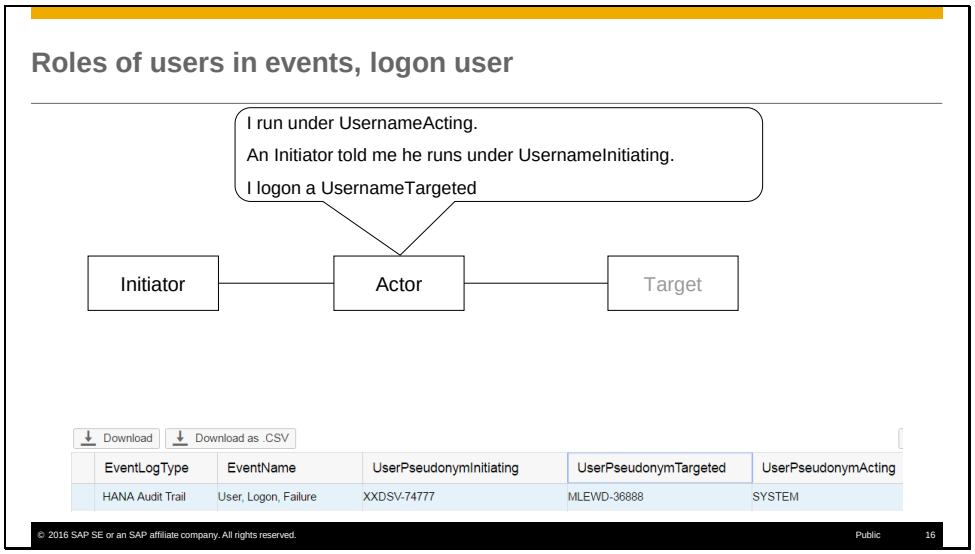


The answer is that the actor machine says in its log:

- I run under account UsernameActing,
- I create an account UsernameTargeted.

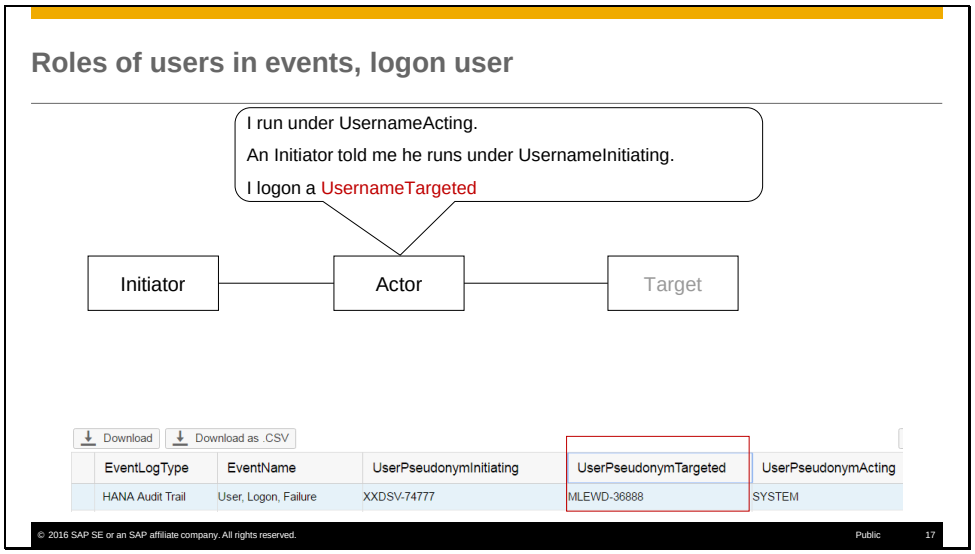
In the Forensic Lab the user accounts become the corresponding pseudonyms.
So, the pseudonyms in the UserPseudonymTargeted column had accounts created.

Slide 16



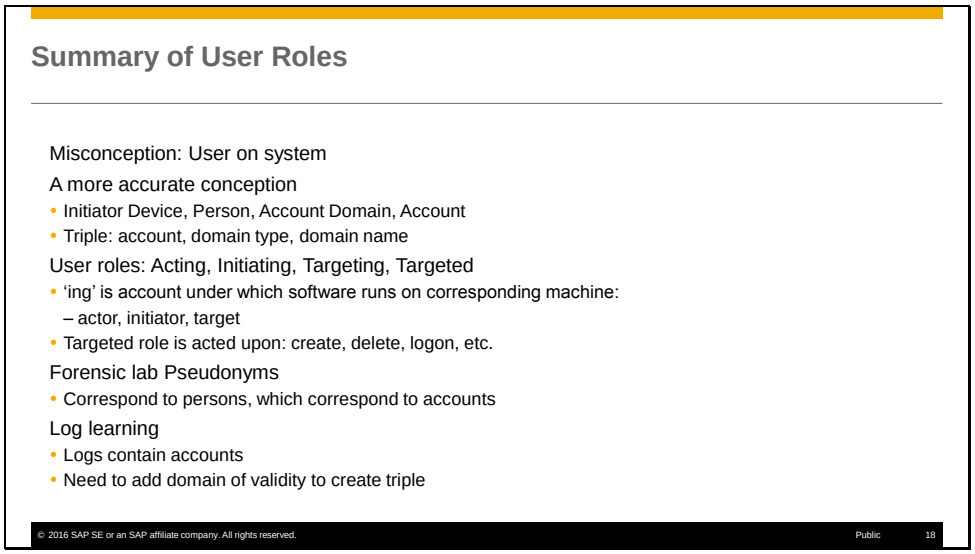
We just saw that a created account has the targeted role.
A logon event, whether successful or not, is treated analogously.
So, which of these pseudonyms corresponds to the account that was logged on by the actor machine?

Slide 17



The answer is the one in the targeted role.
The actor machine was running under the system account, and tried to log on the targeted account.
In addition, the actor was told by the initiator machine that it was running under an account in the initiating role.
This use of roles may seem surprising, if you take the user's point of view.
But, it seems quite natural, if the event is seen from the point of view of the actor machine.
An actor machine running under an acting account logs on a targeted account.
This role assignment is also consistent with the assignment for other actions on accounts, like create, delete or modify.

Slide 18



In this session we saw a common misconception that a user is 'on' the machine that performs some action at his request.
Then we adopted a more accurate conception that adds an initiator device, a person and an account domain to the picture.
The domain tells you where to resolve the account to a person.
Adding the domain let us fully identify an account by a triple: account, domain type and domain name.
There is no longer any assumption that the account's domain of validity is the actor system, for example.

We also saw that there can be multiple accounts in an event.
They can be distinguished by their role in the event: Acting, Initiating, Targeting or Targeted.
All the 'ing' roles identify an account under which the software is run on the corresponding machine: actor, initiator, target.
Targeted is the odd man out. It is the account acted upon, e.g., created, deleted, **logged on**, logged off, etc.

In the Forensic Lab the accounts are associated to persons and turned into pseudonyms to protect privacy.
In Log Learning, on the other hand, there may be accounts in the logs, so you will need to add the domain to create the account triples.

Slide 19