

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

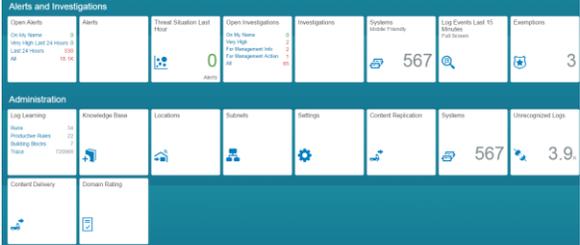
Clearing up a misconception

A more accurate conception

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

Examples of user roles in events

Summary



The screenshot displays the SAP Security Center dashboard. It is divided into three main sections: Alerts and Investigations, Administration, and Constant Delivery. The Alerts and Investigations section includes metrics for Alerts (0), Open Investigations (0), Investigations (567), and Exceptions (3). The Administration section includes metrics for Log Learning (3.9), Knowledge Base, Locations, Subsets, Settings, Content Exploration (567), and Unrecognized Logs (3.9). The Constant Delivery section includes metrics for Domain Rating.

© 2016 SAP SE or an SAP affiliate company. All rights reserved. Public 2

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:

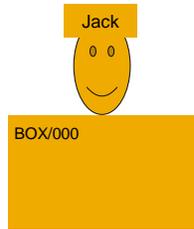
- User account domain
- User role
- Pseudonym, person and account.

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

Slide 3

A misconception: *User on system does something*

User *Jack* on SAP ABAP System *BOX/000* runs a transaction.



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 *device* 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*.

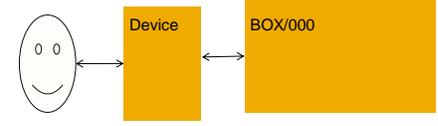
```
graph LR; John((John)) <--> Device[Device]; Device <--> BOX[BOX/000];
```

John invisible,
only user accounts
visible in logs

© 2016 SAP SE or an SAP affiliate company. All rights reserved. Public 4

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.

A more accurate model

Concept	Corresponding Semantic Attributes
<p>It is actually <i>John</i> who uses a device to initiate action by Box/000. Device is Initiator. Box/000 is Actor.</p> <p><i>John</i> uses his account <i>Jack</i>.</p> <p>The code on Box/000 runs under the account <i>Jack</i>.</p>  <p>John invisible, only user accounts visible in logs</p>	<p>Accounts</p> <ul style="list-style-type: none"> • <i>Jack</i> is a user account of <i>John</i>. • How to resolve <i>Jack</i> to <i>John</i>? • Thru triple with domain of validity of <i>Jack</i> • (username, username domain type, username domain name)<role> <p>Triple for this example, without role part?</p>

© 2016 SAP SE or an SAP affiliate company. All rights reserved. Public 5

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.

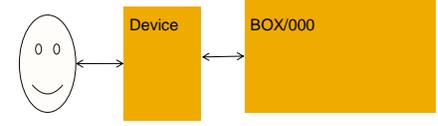
Like an SAP system, the domain is identified by a type and ID, called a name, in this case.

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.

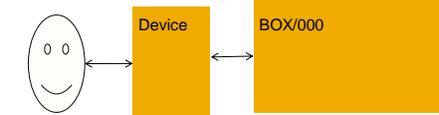
A more accurate model

Concept	Corresponding Semantic Attributes
<p>It is actually <i>John</i> who uses a device to initiate action by Box/000. Device is Initiator. Box/000 is Actor.</p> <p><i>John</i> uses his account <i>Jack</i>.</p> <p>The code on Box/000 runs under the account <i>Jack</i>.</p>  <p>John invisible, only user accounts visible in logs</p>	<p>Accounts</p> <ul style="list-style-type: none">• <i>Jack</i> is a user account of <i>John</i>.• How to resolve <i>Jack</i> to <i>John</i>?• Thru triple with domain of validity of <i>Jack</i>• (username, username domain type, username domain name)<role> <p>Triple for this example?</p> <ul style="list-style-type: none">• Username<role> = 'Jack'• Username Domain Type<role> = 'ABAP'• Username Domain Name<role> = 'BOX/000'

© 2016 SAP SE or an SAP affiliate company. All rights reserved. Public 6

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

A more accurate model

Concept	Corresponding Semantic Attributes
<p>It is actually <i>John</i> who uses a device to initiate action by Box/000. Device is Initiator. Box/000 is Actor.</p> <p><i>John</i> uses his account <i>Jack</i>.</p> <p>The code on Box/000 runs under the account <i>Jack</i>.</p>  <p>John invisible, only user accounts visible in logs</p>	<p>Accounts</p> <ul style="list-style-type: none"> • <i>Jack</i> is a user account of <i>John</i>. • How to resolve <i>Jack</i> to <i>John</i>? • Thru triple with domain of validity of <i>Jack</i> • (username, username domain type, username domain name)<role> <p>Roles of accounts (adjectives), usual meaning</p> <ul style="list-style-type: none"> • initiating, s/w runs under it on initiator <ul style="list-style-type: none"> ■ 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 ?

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

A more accurate model

Concept	Corresponding Semantic Attributes
<p>It is actually <i>John</i> who uses a <i>device</i> to initiate action by <i>Box/000</i>. Device is Initiator. Box/000 is Actor. <i>John</i> uses his account <i>Jack</i>. The code on <i>Box/000</i> runs under the account <i>Jack</i>.</p>	<p>Accounts</p> <ul style="list-style-type: none">• <i>Jack</i> is a user account of <i>John</i>.• How to resolve <i>Jack</i> to <i>John</i>?• Thru triple with domain of validity of <i>Jack</i>• (username, username domain type, username domain id)<role> <p>Roles of accounts (adjectives), usual meaning</p> <ul style="list-style-type: none">• initiating, s/w runs under it on initiator<ul style="list-style-type: none">■ 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 ? <i>Acting</i>

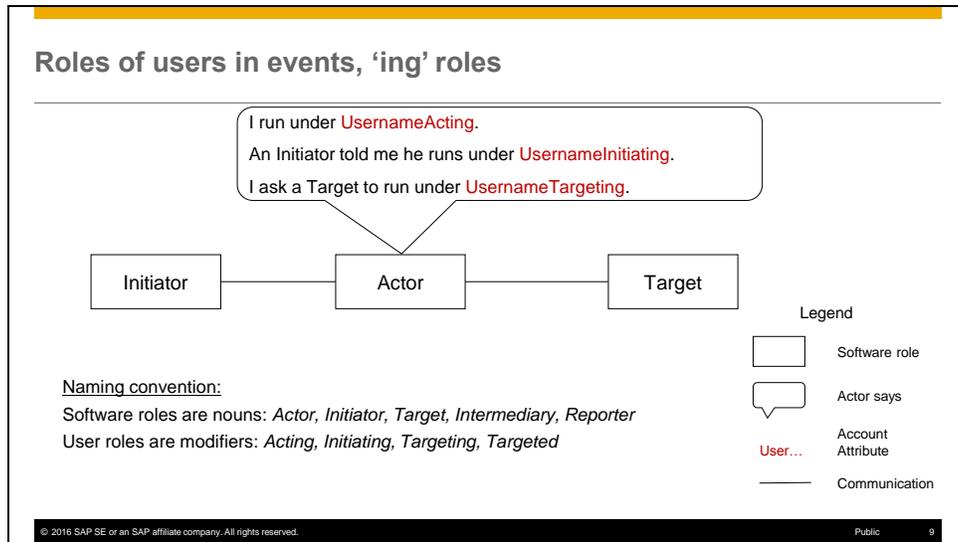
```
graph LR; John((John)) <--> Device[Device]; Device <--> BOX[BOX/000];
```

John invisible,
only user accounts
visible in logs

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

Public 8

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



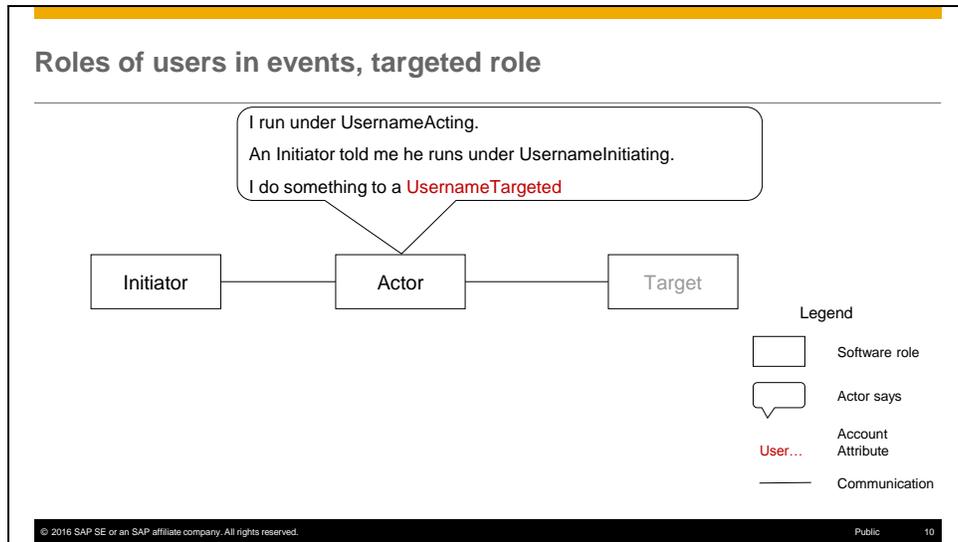
Here is a graphical summary of the user account roles ending in 'ing'. Note that 'user' means 'user account', as opposed to a person.

An actor machine tells you what it does and which accounts are involved.

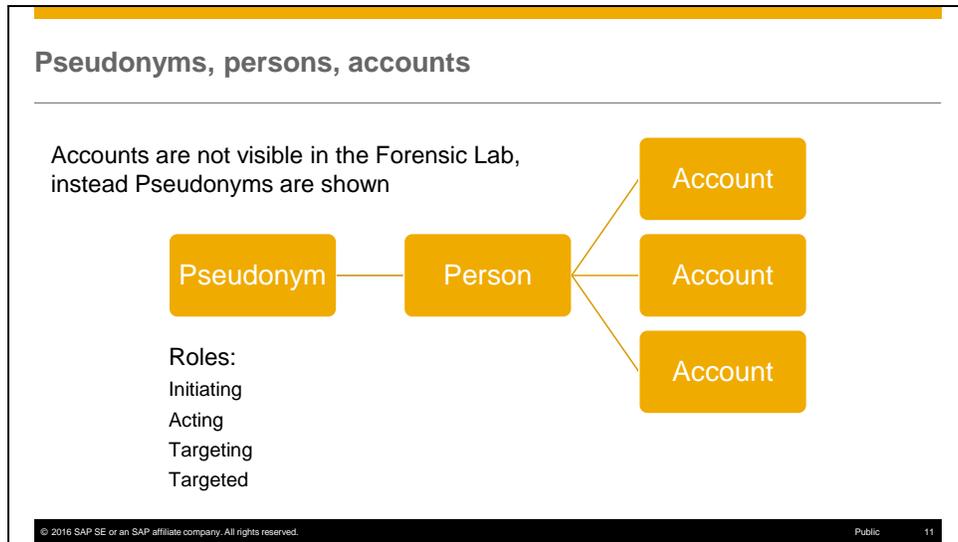
It says:

- 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.



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.



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

Accounts are visible in Log Learning

During Log Learning add domain to create triples:

- Username, <role>
- Username, Domain Type, <role>
- Username, Domain Name, <role>

– Domain is where the username can be resolved to a person

```
graph LR; Pseudonym --- Person; Person --- Account1[Account]; Person --- Account2[Account]; Person --- Account3[Account];
```

The diagram illustrates the relationships between different entities. A box labeled 'Pseudonym' is connected to a box labeled 'Person'. From the 'Person' box, three lines radiate outwards to three separate boxes, each labeled 'Account', indicating that a person can have multiple accounts.

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

Pseudonyms in Forensic Lab, Create user

```

graph LR
    Pseudonym --- Person
    Person --- Account1[Account]
    Person --- Account2[Account]
    Person --- Account3[Account]
    
```

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

EventName	EventLogType	UserPseudonymActing	UserPseudonymTargeted	UserPseudonymTargeting
User Admin, User, Create	HANA Audit Trail	XCRLS-38227	BBSZU-92922	
User Admin, User, Create	UserChangeLog	MOTIS-73743	NUIPE-30080	

Note multiple log-entry types mapped to same semantic event.

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

Roles of users in events, create user

Initiator — Actor — Target

Legend

- Software role
- Actor says
- Account Attribute
- Communication

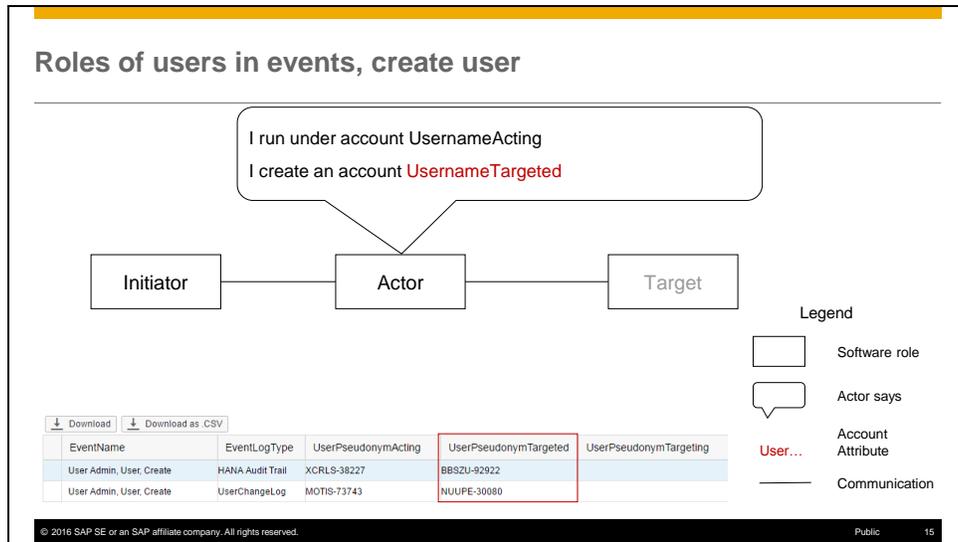
EventName	EventLogType	UserPseudonymActing	UserPseudonymTargeted	UserPseudonymTargeting
User Admin, User, Create	HANA Audit Trail	XCRLS-38227	BBSZU-92922	
User Admin, User, Create	UserChangeLog	MOTIS-73743	NUUPE-30080	

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



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.

Roles of users in events, logon user

I run under UsernameActing.
 An Initiator told me he runs under UsernameInitiating.
 I logon a UsernameTargeted

```

    graph LR
      Initiator[Initiator] --- Actor[Actor]
      Actor --- Target[Target]
    
```

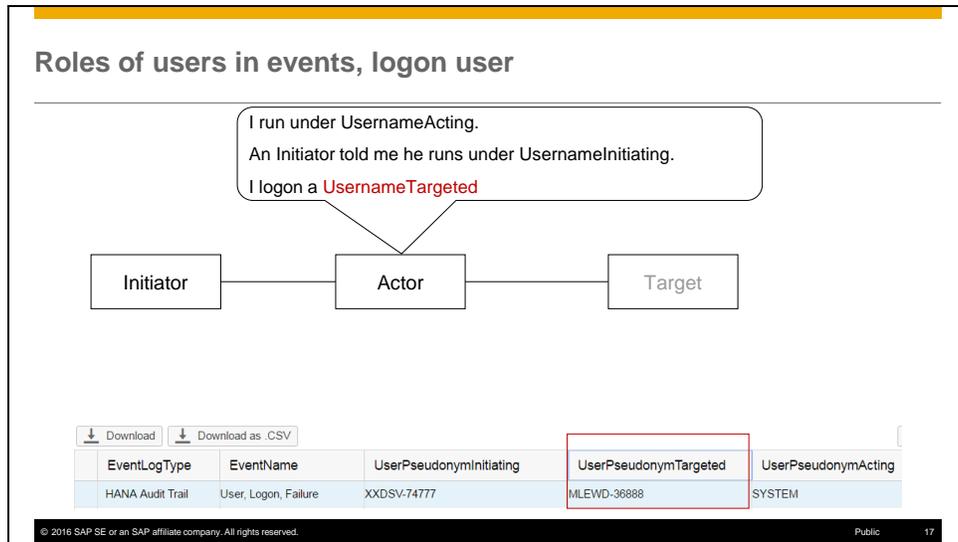
Download Download as .CSV

EventLogType	EventName	UserPseudonymInitiating	UserPseudonymTargeted	UserPseudonymActing
HANA Audit Trail	User, Logon, Failure	XXDSV-74777	MLEWD-36888	SYSTEM

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

Summary of User Roles

Misconception: User on system
A more accurate conception

- Initiator Device, Person, Account Domain, Account
- Triple: account, domain type, domain name

User roles: Acting, Initiating, Targeting, Targeted

- 'ing' is account under which software runs on corresponding machine:
 - actor, initiator, target
- Targeted role is acted upon: create, delete, logon, etc.

Forensic lab Pseudonyms

- Correspond to persons, which correspond to accounts

Log learning

- Logs contain accounts
- Need to add domain of validity to create triple

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

© 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.