IDENTITY AUTOMATION

DO YOU NEED CORRELATION?

Breaking Down Correlation and What it Means to Identity Management

GUIDEBOOK

"DO YOU NEED CORRELATION?"

It's a question you may have received from a security vendor. Or maybe you're even posing it to yourself. It's a topic we increasingly are finding ourselves discussing with customers and prospects, and a subject we believe will continue to get more popular in the future.

However, as the topic continues to become more prevalent, it's clear there's a lack of understanding around correlation and its place in an identity management platform. What is correlation? When is it needed? And how does it support an identity management platform and security infrastructure?

Those are all important questions that we will address in this guidebook. After reading it, we hope you have a greater understanding of correlation and how it fits with identity management technology.

There are three types of correlation: identity correlation, event correlation and behavioral correlation. All can be important to an organization's security strategy, but are very different in implementation, purpose and use case.

Let's examine each type of correlation to understand them better.

Identity Correlation

1

Identity correlation deals with a current state of accounts, giving information about the users involved in systems and applications. It reconciles and validates the proper ownership of disparate user account IDs throughout an organization, and links ownership of those user account IDs to specific individuals through the assignment of a unique identifier. Identity correlation also validates identity attributes themselves, the most important of which is the enabled or disabled state of the identity in every system.

There are several important actions that identity correlation can do for an organization.

Identity correlation provides context to user account IDs. Organizations must find ways to link user account IDs to the actual people they represent. Some use a number system, where Jane Smith exists in their systems as user account ID 12345, but most use an approach where the user account ID is representative of their actual name because it's easier for people to remember. In that scenario, for example, Jane Smith would be known as user account ID JSmith.

Another action that identity correlation handles is linking user account IDs to the access the people representing them should hold. JSmith could exist in the HR system, Active Directory and Google Apps, the systems and applications each of her organization's employees is required to exist in. If she's a Marketing Manager, she would also exist as JSmith in Marketo, Saleforce.com and Hubspot. If JSmith suddenly exists in JIRA, an application only technical people in the organization require access to, then IT understands that they must revoke that access privilege.

The ability to show discrepancies in data is a valuable attribute of identity correlation. If Jane Smith leaves her company, and JSmith no longer exists in the HR system, but an orphaned JSmith account still shows up in Marketo, it's an indication to her organization to fix that discrepancy and remove JSmith from Marketo. Another scenario showing the need for surfacing data discrepancies would be if Jane Smith marries and takes her spouse's surname, becoming Jane Thomas, her user account ID with her organization would become JThomas. If JSmith and JThomas both exist in applications and systems, identity correlation would show that appropriate changes must be made.

Identity Correlation and Identity Management

Identity management platforms should provide identity correlation. When Jane Smith uses JSmith to access each of her applications or systems rather than using disparate unique user account IDs for each one, it's making life easier for Jane, but also for IT. Examining identity correlation is a simpler, quicker process.

2 Event Correlation

Event correlation looks at events occurring in a window of time. It is the process of examining events, pinpointing the interactions of those events and determining which events and event interactions are important. In the context of IT security, event correlation is handled by a Security Information and Event Management system (SIEM) and involves looking at events from multiple source systems to identify potential risks. Event correlation is usually performed in a separate correlation engine, which could receive each event as it happens or read it from SIEM stored data.

Events monitored and managed in IT security could be user authentication, user access to systems and applications, physical access to a building, and output from an Intrusion Detection System.

When properly configured, a SIEM tool will determine event correlations and raise alerts when needed. For instance, if Jane Smith logs into a computer in China, but then swipes her employee badge at a door in San Francisco, that should not be possible. Her organization's SIEM tool would alert IT staff of this event correlation and proper risk containment steps could be initiated.

Event Correlation and Identity Management

SIEM products handle the actual event correlation within an organization, but they receive event logs from systems across the organization, such as operating system logs, application logs, and physical security systems. An identity management platform would be a provider and producer of event data to a SIEM product, which would then build complicated correlation policies to look at events from multiple source systems to identify risks. Most identity management products also support alerts from a SIEM product for taking action on risks. For instance, in the scenario mentioned earlier where Jane Smith appeared to be in both China and San Francisco at the same time, an identity management product could take action, such as disabling her account, after being alerted by an SIEM product.

3 Behavioral Correlation

Behavioral correlation is a relatively new term in IT security because the industry has struggled with identity correlation and event correlation. While identity correlation deals with a current state of accounts and event correlation examines events occurring within a window of time, behavioral correlation looks at a current event and compares it to historical action patterns.

The most basic example of behavioral correlation is account login. For example, Jane Smith typically logs in every weekday between 9am and 6pm from a US host device, which is something that can only be understood over time by collecting her login events. If she travels to Munich and attempts to login, behavioral correlation determines that this login, while successful, does not match her login patterns. These actions could push a pre-set policy for this situation to go into effect, requiring Jane to provide additional information, such as a one-time password sent to her phone.

Behavioral Correlation and Identity Management

Because behavioral correlation is such a new technique in IT security, most identity management platforms do not currently have the infrastructure to handle it. Due to the mass amount of data collected and the speed at which it must be queried, a typical identity management configuration will not suffice. A significant Big Data analytics infrastructure is needed.

In theory, because of the process and data needed, behavioral correlation should live in identity management platforms, so the most innovative identity management vendors are investigating behavioral correlation and examining it as the future of identity management.

"So...do you need correlation?..."

Now that we've identified the three different types of correlation and what they mean, we can get back to the original question.

The short answer is both yes and no, and now that you've learned more about each type of correlation, you can see how it's a difficult question to answer. No identity management vendor can honestly answer the question with a resounding yes, but no vendor should tell you that correlation doesn't involve identity management either.

As it relates to correlation, an ideal identity management platform should include

- Identity correlation as a component of the product.
- The ability to work in conjunction with a SIEM tool to feed it information, receive alerts from it, and send those alerts on to you.
- Future plans, even if those plans are in the exploratory phase, to offer behavioral correlation capabilities.

Not all identity management platforms include these components, so as you're assessing your needs, consider if correlation is one of those. If so, determine which type(s) of correlation and that can help you decide which identity management solution would best fit your needs.

If you'd like further information on correlation and its place within an identity and access management system, contact us to learn more.