ArcSight and User Session Tracking

Prepared By: John Bradshaw
Date: Monday, May 24, 2010
Table of Contents

Table of Contents .............................................................................................................................. ii

User Session Tracking Overview .................................................................................................. 3
  Session Tracking Events .............................................................................................................. 3

ArcSight Solutions and User Session Tracking .............................................................................. 4
  ESM Session Lists ...................................................................................................................... 4
  Active List Technologies ............................................................................................................ 5
  Variables ...................................................................................................................................... 6
  Custom Columns .......................................................................................................................... 7

Putting It All Together ................................................................................................................... 8

Solution Overview .......................................................................................................................... 10
User Session Tracking Overview

Security Analysts deal with all types of threats across a wide variety of systems, applications and devices every day. One of the biggest challenges facing these analysts is being armed with sufficient information that allows a complete picture of who, what, when, where and how. Most event logging sources do not contain every single piece of information required to complete this picture. The most notable gap is the lack of user information within network infrastructure devices logs.

Compounding this problem is the fact that this information can be dynamic in nature. In typical environments, end-user workstations are assigned a dynamic IP Address that has a limited lifespan. In these situations, how does an analyst then tell the difference between a firewall log permitting access to a suspicious site for address 10.0.0.1 at 10:00am vs. the same address accessing another suspicious site at 1:00pm? Was this the same system, or even same user for that matter?

In order to fully and properly assess the situation, SEIM solutions must be able to fill in the missing puzzle pieces by linking dynamically changing information (IP Address allocations, User Login information, etc.) into a single cohesive view.

The purpose of this ArcSight Use Case is to document methods the ArcSight Enterprise Security Manager (ESM) correlation engine can assist security analysts in tracking user session information and tying it back to a single individual.

Session Tracking Events

For the purposes of this Use Case, we are going to demonstrate how ArcSight ESM can track a user’s identity from Login until Logout regardless of the event source. The traffic scenario is as follows:

- User 1 Successfully Logs On To Windows Workstation
- Firewall Logs Traffic From Windows Workstation
- User 1 Logs Out Of Windows Workstation
- User 2 Successfully Logs On To Windows Workstation With Same IP Address (DHCP Leases Changed Between User 1 and User 2)
- Firewall Logs Traffic From Windows Workstation
- User 2 Logs Out Of Windows Workstation

While this Use Case focuses on firewall log traffic to demonstrate how user information can be linked to events that do not contain user data, any event source (ie: NetFlow, Network IDS, Web Proxy Logs) would become linked as a result of the demonstrated capabilities.
ArcSight Solutions and User Session Tracking

ArcSight solutions provide abilities that assist analysts in tracking and analyzing user events. The following capabilities outline embedded technologies in the ArcSight product lines:

ESM Session Lists

Session Lists provide a method of tracking dynamically changing information. Session List information can be updated as a result of a correlation rule trigger or manual user action. Two of the most commonly tracked pieces of information used in user session tracking are User logon/logoffs and DHCP lease allocations.

The above illustration demonstrates how Session Lists work. This particular Session List is tracking User Logon information based on the IP Address assignment of the workstation and the user name associated with the login event. There are two closed sessions where the user logged in and then logged out (noted by the End Time of the session) and one session is still active (noted by the absence of End Time). Session Lists place a time context on any occurring events by establishing this Start/End time.

How does one establish the start/end time of sessions? This is accomplished through ArcSight Correlation Rule Triggers. For the purposes of this Use Case, we will establish that a successful user logon event starts the session and a user logout terminates the session. In your Actions Tab in the Rule Editor it would look like this:
The first rule trigger starts the session while the second rule trigger terminates it (additional checks can be implemented to cover situations such as system reboots, users forgetting to logout, etc., but that is beyond the scope of this Use Case Whitepaper).

From these two simple correlations, we have taken two events and created the possibility of determining which user was assigned to which IP Address at any given point in time.

User 1 successfully Logged In On Workstation with IP Address 10.0.0.1

Any events during this time period are attributed to User 1

User 1 Logs Out On Workstation

Active List Technologies

ArcSight Active Lists are used to complete the picture. In fact, the key components to Identity Tracking is the capability to pinpoint a moment in time when an event belongs to a particular user identifying attribute plus the ability to take that user attribute and map it to a single unique identifier of an individual.

For instance, how many user attributes are used within your organization? What about:

- User Logon ID(s)
- E-Mail Address(s)
- Phone Number (Office, Cell, Fax)
- Badge ID

A typical large organization has at least 5 – 10 attributes that map back to a single individual. Do analysts and auditors want to backtrack through millions of events per day attempting to piece together which attribute belongs to which user...as well as map events that do not contain user attribute information back to the user that generated the events? No.

Part of the ArcSight IdentityView solution is to provide Identity Model Connectors that synchronize information from Identity Management solutions (ie: ActiveDirectory, Oracle IDM) within Active/Session Lists.
Variables

Within ArcSight resources (Active Channels, Field Sets, Correlation Rules, etc.) there is the capability to create and act on variables. Variables are used in this Use Case to extract required information from the appropriate Active/Session list and populate the displays with the appropriate user information.

In my correlation rule tracking logons, I need to take the user attribute (the Login ID) and map it to the unique identifier for that individual. Variable definitions allow me to extract that information from the Active List and assign it to a variable that can then be used in rule trigger actions.

For additional clarity, we will also use a Session List containing information about the user’s role within the organization. Session Lists are used for this type of information because just like IP Addresses and Login times, a user’s role can change within the organization over time.
Custom Columns

Did you know you are not limited to displaying only information contained within the event in an Active Channel display? The ArcSight Analyst Console provides the ability to rename columns to more meaningful titles as well as integrate other information into the display.
We will use this capability to drive home the ability to provide useful displays to the Security Analyst responsible for assessing incidents within the organization.

## Putting It All Together

Now that we’ve covered the underlying capabilities that will achieve our end goal, let’s put it all into action and see the results.

The following Active Channel/Field Set represents the base events without the benefit of Session or Identity Correlation.

### Active Channel 1: Basic Event Information

As you can see, the only user identifiable information is in the login/logout events that contain the login ID of the user. Fortunately this information seems to be in a relatively easy format (First Initial, Last Name) but that is not always the case. Also, the firewall events contain no user information attributed to them without the benefit of Session/Identity Correlation.
Active Channel 2:  Session / User Information

This Active Channel now incorporates information obtained from the Session List tracking as well as the Identity Mapping Active Lists discussed earlier. I can now clearly see that the first series of users logged into the workstations and their sessions communicated across the firewall to several foreign countries.

Then those individuals logged out.

Afterward, a different set of individuals logged into systems that were assigned the same IP Addresses within the same Zones (ArcSight Zone Mapping is an excellent way of ensuring overlapping IP Address space within your organization is uniquely identified) is tracked. Those individuals also communicated with several foreign countries.

In reality, I would have thousands, if not millions, of firewall events occurring within my site every day. I doubt any analyst would want to scroll through these events trying to piece meal actionable and relevant incidents that have occurred within their protection domain. We then combine traditional threat protection correlation rules with the Custom Column definitions mentioned earlier to create an Active Channel showing only relevant events that require attention while enhancing the user identification displays.
This Active Channel display now represents a fuller picture of relevant incidents that are occurring within the environment. Now, instead of seeing all firewall events, I am looking at event traffic involving suspicious source/destinations.

Additionally, I am able to not only correlate a unique attribute to an individual, but I’m also able to tie-in other information about the user including: organization, department, title/rank as well as their photograph!
Solution Overview

Either through increased requirements for security analysis, more stringent auditing requirements or external regulatory compliance reporting; organizations are being required to collect and analyze event data from more varied sources than ever before. The ability to create focused, actionable data from these various disparate sources has become a critical capability in sifting through the millions of events per day most organizations face.

ArcSight’s state of the art correlation engine provides methods that can identify, track and correlate user information across various sources, even those that contain no user information to begin with and are dynamically changing, so that the analyst can focus on prioritize, actionable and relevant incidents within their environment.