What's New in ArcSight Enterprise Security Management v5.0

June 15, 2010

ArcSight Enterprise Security Management (ESM) v5.0 introduces new feature sets that broaden its security and event-management platform, and its identity-correlation functionality. This functionality includes user modeling through Actors, a customizable event schema, and improved variable authoring through the introduction of global variables. ArcSight ESM v5.0 also includes enhancements in custom-view dashboards, field-set authoring, active list enhancement, Suite B encryption support, and event case-preservation and reporting.

ESM v5.0 provides the ability to monitor and model your network and user behavior, quickly customizing the product to your needs so you can leverage its core technology to solve security challenges such as user activity monitoring, external threat management, regulatory compliance, transactional activity amongst other scenarios.

Actors

ESM v5.0 introduces a new feature called Actors that provides a new way of mapping users and their behaviors to their application and network activity, enabling easy-to-configure correlation analysis. Using the Actor Model Import Connector, customers can populate and maintain the Actor model in sync with their Identity Management System (such as Active Directory).

Actors is a separately licensed feature made available with an IdentityView Solution purchase.

Domain Field-Sets

ESM v5.0 introduces the concept of domain field-sets, which allows you to uniquely identify and group events that possess common attributes relevant to a business vertical, such as transaction monitoring (e.g., credit cards, online banking, or stock transactions). Domain field-sets make it easy to monitor, correlate, and analyze events not only for traditional security use cases, but also for any specialized business-related use cases.

Domain Field-Sets is a separately licensed feature made available with a FraudView purchase.

Global Variables

Global Variables offer the ability to author variables which derive particular values from existing data, from a centralized location, and to re-use them in multiple places, simplifying the content-authoring process. As part of global variables, ESM v5.0 also introduces the ability to promote resource-specific variables into global ones by a simple button click.

ESM Service Layer

As part of this release ESM introduces a new Service Layer through which you can integrate your applications, using functionality such as Web Services. ESM Service Layer uses a

service-oriented architecture (SOA) that supports multiple Web Service clients written in different languages.

Suite B Support

As part of ESM v5.0 ArcSight introduces the ability to deploy the product, and all its corresponding components, with Suite B-supported cryptographic algorithms. Suite B's cryptographic algorithms are issued by the National Security Agency (NSA) as part of national cryptographic technology.

ArcSight ESM System Enhancements:

Manager Enhancements

Schema and Data Type Expansion

As part of ESM v5.0 the security event-schema has been enhanced to be more flexible, extensible, and customizable for ranges of application beyond traditional network security. The ESM v5.0 base schema now offers:

- IPv6 and Floating-point field-type support
- Custom string fields have been increased to support 4000 bytes
- Additional Schema, custom and category fields

Asset Aging

ESM Asset management now offers the ability to update actor-model confidence, based on an asset's age, further based on its last scan update, and the ability to delete/expire an asset past a certain age.

Case Event Preservation

ESM v5.0 introduces the ability to preserve events associated with a case, beyond the event-retention policy.

Reusable Field-Sets

As part of ESM v5.0, Field-Sets have been broken out into their own resource, enabling creation of custom field-sets based on resource type (e.g., actors, cases, and event fields).

Hierarchical Deployment Enhancement

ESM has been enhanced to introduce the ability to automatically include base-events when forwarding correlated events in a hierarchical deployment. As part of this process all forwarded events will annotated as forwarded.

Correlation Enhancements

Active List

Active Lists offer support for multi-mapping a key field to multiple values, which return as a list through the introduction of multi-map active lists. Active lists have also been enhanced to offer partially cached active lists, which store and retrieve additional entries, beyond that held in-memory from the database.

New Variable Function

ArcSight ESM v5.0 enhances variables with these functions:

Timestamp Functions

- Get Year
- Get Day of Year

Alias
- Alias Field

Type Conversion
- String to List
- Convert Address to String

String Functions
- Concatenate Three

Actors
- Has Relationship

Trend Actions

As part of ESM v5.0, Trends have been enhanced to populate active lists with trend data, making trend results readily available for use in rules, filters, active channels, and so forth.

Case Event Reporting

ESM v5.0 introduces the ability to show any combination of case fields and associated events fields within a case report such as a workflow summary report.

Console Enhancements

Custom View Dashboards

Dashboards now support custom views, which enable users to create custom-layout views for dashboards, and display data monitors over an imported image.

Data Monitor Drill-Downs

You can now select a field-set in a data monitor and drill down to define which columns (fields) show in the drill-down channel.

Query Editor

In ArcSight ESM v5.0, the Query Editor has been enhanced within the query definition panel. The Select, Group By, and Order By fields have improved ease-of-use, with drag-and-drop capability and all three options on a single view.

Platform Support

Please review the *ArcSight ESM v5.0 Platform Product Lifecycle* document for details on OS platform support for the Manager, Database, Console, and ArcSight Web components. Here are some highlights concerning newly added platform support:

Red Hat Enterprise Linux 5.4 (RHEL 5)

ArcSight ESM v5.0 Manager, Database and ArcSight Web support will be offered for Red Hat Enterprise Linux 5.4(RHEL 5)

Microsoft Windows Server 2008 SP2

ArcSight ESM v5.0 Database support will be offered for Microsoft Windows Server 2008 SP2.