**Authentication data**

Network and local authentication data shows sign-on and sign-off events, the status of such events, the source and destination addresses, the service name, and time of occurrence. These values are used to track who succeeded in gaining access to a computing asset, when the access took place, access duration, and the frequency of access. It also tracks failed access attempts. Additionally this data source often tracks authorization settings so that after an identity is authenticated, what that identity is authorized for can be verified. Authentication data includes:

- **Active Directory**: a distributed directory in which organizations define user and group identities, security policies and content controls.
- **LDAP**: an open standard defined by the IETF and is typically used to provide user authentication (name and password). It has a flexible directory structure that can be used for a variety of information such as full name, phone numbers, email and physical addresses, organizational units, workgroup and manager.
- **Identity Management**: identity management is the method of linking the users of digital resources—whether people, IoT devices, systems or applications—to a verifiable online ID.
- **Single Sign-On (SSO)**: a process of using federated identity management to provide verifiable, attestable identities from a single source to multiple systems. SSO significantly increases security by tying user credentials to a single source, allowing changes to user rights and account status to be made once, and reflected in every application or service to which the user has access. SSO is particularly important for users with elevated security rights such as system or network administrators that have access to a large number of systems.

In the Common Information Model, authentication data is typically mapped to the Authentication data model.

**Application**

**Security**

- Monitoring for signs of Windows privilege escalation attacks
- Detecting techniques in the Orangeworm attack group
- Securing a work-from-home organization
- Conducting an Azure new user census
- Detecting lateral movement with Active Directory data
- Identifying and disabling inactive users on AWS

**Compliance**

- Complying with General Data Protection Regulation
- Monitoring NIST SP 800-53 rev5 control families
- Processing DMCA notices
Observability

• Managing Azure cloud infrastructure

Sources

Guidance for onboarding data can be found in the Splunk Documentation, *Getting Data In* (Splunk Enterprise) or *Getting Data In* (Splunk Cloud). In addition, these Splunk Add-Ons and Apps are helpful for working with authentication data.

• Splunk Add-on for Cisco Identity Service
• Splunk Supporting Add-on for Active Directory
• Microsoft Windows security logs
• *nix security logs

*Looking for more information on data types? Download the Splunk Essential Guide to Machine Data.*