New application permissions granted through Active Directory

You might need to see whether accounts have been granted access to sensitive applications through Active Directory when doing the following:

- Detecting lateral movement with Active Directory data

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
- Microsoft Azure Active Directory audit data
- Microsoft Azure Add-on for Splunk

Example

Your company uses SolarWinds Orion business software, which suffered the Sunburst Backdoor attack. You want to identify any lateral movement associated with attack by looking for newly granted permission to sensitive applications.

To optimize the search shown below, you should specify an index and a time range.

1. Run the following search:

   sourcetype="azure:aad:audit" activityDisplayName="Add app role assignment to service principal" OR activityDisplayName="Add delegated permission grant" OR activityDisplayName="Add application" |
   stats values(initiatedBy.user.userPrincipalName) AS UPN, values(targetResources{}.displayName) AS Target, values(targetResources{}.modifiedProperties{}.displayName) AS "Modified Resources", values(targetResources{}.modifiedProperties{}.oldValue) AS "Old Values", values(targetResources{}.modifiedProperties{}.newValue) AS "New Values" |
   BY correlationId activityDisplayName |
   fields - correlationId

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.
**Splunk Search**

```
sourcetype="azure:aad:audit"
```

**Explanation**

Search only Azure Active Directory audit data.

```
activityDisplayName="Add app role assignment to service principal" OR
activityDisplayName="Add delegated permission grant" OR activityDisplayName="Add application"
```

**Explanation**

Search for any one of the three permissions-related actions shown.

```
| stats values(initWith.user.userPrincipalName) AS UPN, values(targetResources{}.displayName) AS Target,
values(targetResources{}.modifiedProperties{}.displayName) AS "Modified Resources",
values(targetResources{}.modifiedProperties{}.oldValue) AS "Old Values",
values(targetResources{}.modifiedProperties{}.newValue) AS "New Values" BY correlationId activityDisplayName
```

**Explanation**

Calculate aggregate values for the modified properties as shown and group results by correlationId and action.

```
| fields - correlationId
```

**Explanation**

Remove the correlationId field from the results.

---

**Result**

The [Microsoft Azure Add-on for Splunk](https://www.splunk.com/marketplace/add-ons/microsoft-azure) has additional searches and pre-built security content for Azure data that can help you interpret these results and take additional steps to resolve security concerns related to new application permissions being granted through Active Directory.

---

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.