Application switch to Active Directory multi-tenant access

Multi-tenant access allows accounts from any Active Directory or even personal accounts to access an application, rather than only those from one specific directory. You might need to see which applications have been switched to multi-tenancy 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 seeing if any applications have been opened up to multi-tenancy.

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="Update application" operationType=Update result=success targetResources{}.modifiedProperties{}.displayName=AvailableToOtherTenants | table activityDateTime initiatedBy.user.userPrincipalName targetResources{}.displayName additionalDetails{}.value
```

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

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourcetype=&quot;azure:aad:audit&quot;</td>
<td>Search only Azure Active Directory audit data.</td>
</tr>
<tr>
<td>activityDisplayName=&quot;Update application&quot;</td>
<td>Search for the &quot;update application&quot; action.</td>
</tr>
<tr>
<td>operationType=Update</td>
<td></td>
</tr>
<tr>
<td>result=success</td>
<td>Search for updates that successfully made a resource available to other tenants.</td>
</tr>
<tr>
<td>targetResources{}.modifiedProperties{}.displayName=AvailableToOtherTenants</td>
<td></td>
</tr>
</tbody>
</table>

| table activityDateTime initiatedBy.user.userPrincipalName targetResources{}.displayName additionalDetails{}.value | Display the results in a table with columns in the order shown. |

### Result

The [Microsoft Azure Add-on for Splunk](https://www.splunk.com/marketplace/add-ons/microsoft-azure-add-on) has additional searches and pre-built security content for Azure data that can help you interpret these results and take additional steps to res...