Newly added Active Directory service principals

An Azure service principal is an identity created for an application, such as Active Directory. Its access rights can be restricted in a number of ways, such as by resource group, specific resources, a validity period, or a role. You might need to find newly added Active Directory service principals 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 hunting for newly added service principals for Active Directory.

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 service principal"
| stats values(activityDisplayName) AS Action, 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
| 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"`
- `activityDisplayName="Add service principal"`

| stats values(activityDisplayName) AS Action, 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 | Calculate aggregate values for the modified properties as shown and group results by correlationId. |
| | | Remove the correlationId field from the results. |

### Result

After identifying new service principals, you might also want to search for new credentials added to existing service principals. Additionally, the Microsoft Azure Add-on for Splunk has 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 newly added service principals for Active Directory.