Get-MDEInvestigationPackage Playbook

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

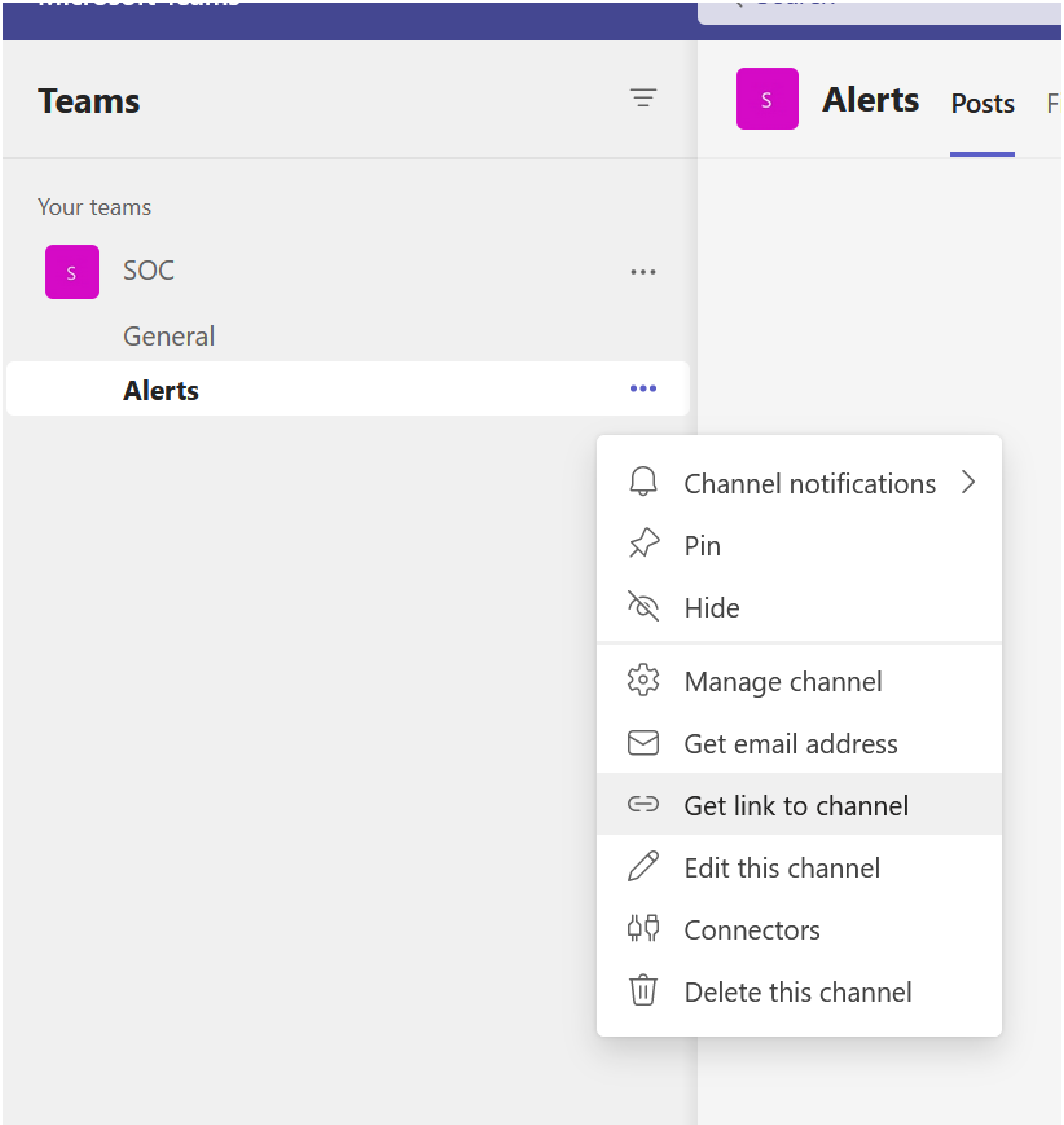
This playbook will call the collect investigation package in MDE. It will then loop until thats complete, once complete it will add a comment to the incident and post a message in teams with the URL to download the package.

Quick Deployment

Go to https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks/Get-MDEInvestigationPackage

Prerequisites

1. **Get the Teams ID and Channel ID**



Example: https://teams.microsoft.com/l/channel/ <**channel id**>/Alerts?groupId=<**groupid**>&tenantId=00000000-0000-0000-0000-000000000000

2. **Grant the following permissions to the managed identity by running the commands in the Cloud Shell.**

For Machine.CollectForensics permission

```
$MIGuid = " enter managed identity here "
$MI = Get-AzureADServicePrincipal -ObjectId $MIGuid

$MDEAppId = "fc780465-2017-40d4-a0c5-307022471b92"
$PermissionName = "Machine.CollectForensics"

$MDEServicePrincipal = Get-AzureADServicePrincipal -Filter "appId eq '$MDEAppId'"
$AppRole = $MDEServicePrincipal.AppRoles | Where-Object {$_.Value -eq $PermissionName -and $_.AllowedMemberTyp
New-AzureAdServiceAppRoleAssignment -ObjectId $MI.ObjectId -PrincipalId $MI.ObjectId `
-ResourceId $MDEServicePrincipal.ObjectId -Id $AppRole.Id
```

For Machine.ReadWrite.All permission

```
$MIGuid = " enter managed identity here “
$MI = Get-AzureADServicePrincipal -ObjectId $MIGuid

$MDEAppId = "fc780465-2017-40d4-a0c5-307022471b92"
$PermissionName = "Machine.ReadWrite.All"

$MDEServicePrincipal = Get-AzureADServicePrincipal -Filter "appId eq '$MDEAppId'"
$AppRole = $MDEServicePrincipal.AppRoles | Where-Object {$_.Value -eq $PermissionName -and $_.AllowedMemberTyp
New-AzureAdServiceAppRoleAssignment -ObjectId $MI.ObjectId -PrincipalId $MI.ObjectId `
-ResourceId $MDEServicePrincipal.ObjectId -Id $AppRole.Id
```

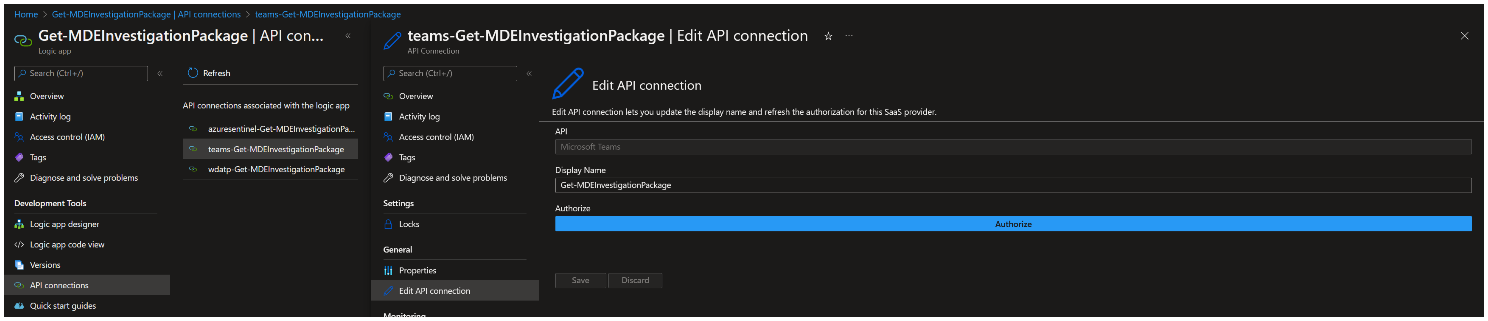
For Machine.Read.All permission

```
$MIGuid = "" enter managed identity here "
$MI = Get-AzureADServicePrincipal -ObjectId $MIGuid

$MDEAppId = "fc780465-2017-40d4-a0c5-307022471b92"
$PermissionName = "Machine.Read.All"

$MDEServicePrincipal = Get-AzureADServicePrincipal -Filter "appId eq '$MDEAppId'"
$AppRole = $MDEServicePrincipal.AppRoles | Where-Object {$_.Value -eq $PermissionName -and $_.AllowedMemberTyp
New-AzureAdServiceAppRoleAssignment -ObjectId $MI.ObjectId -PrincipalId $MI.ObjectId `
-ResourceId $MDEServicePrincipal.ObjectId -Id $AppRole.Id
```

3. **Authorize teams-Get-MDEInvestigationPackage API connections. This is to ensure that the logic app will send the message to the Teams channel.**



API connections associated with the logic app

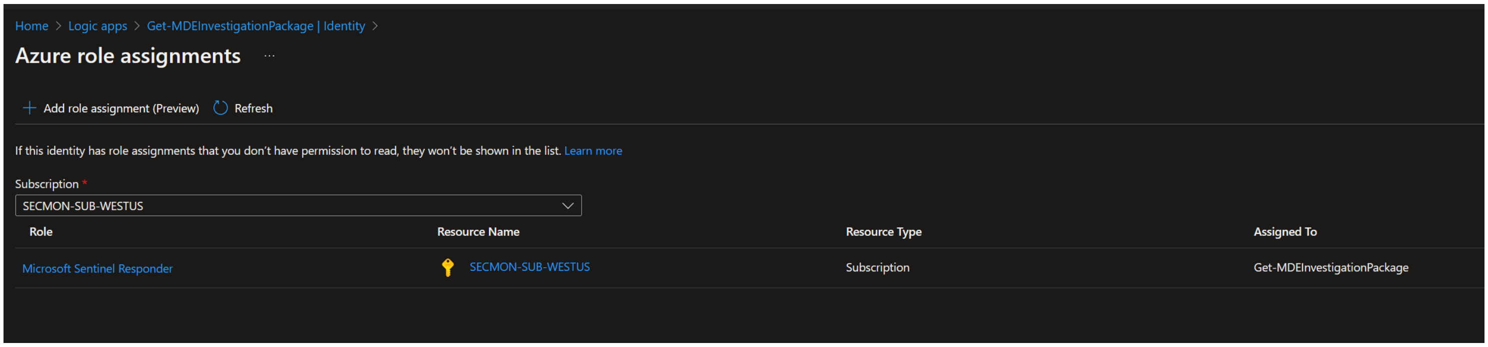
- azuresentinel-Get-MDEInvestigationPa...
- teams-Get-MDEInvestigationPackage
- wdatp-Get-MDEInvestigationPackage

Edit API connection lets you update the display name and refresh the authorization for this SaaS provider.

API: Microsoft Teams

Display Name: Get-MDEInvestigationPackage

4. **Apply Microsoft Sentinel Responder permissions to managed identity.**



Home > Logic apps > Get-MDEInvestigationPackage | Identity >

Azure role assignments ...

+ Add role assignment (Preview)   Refresh

If this identity has role assignments that you don't have permission to read, they won't be shown in the list. Learn more

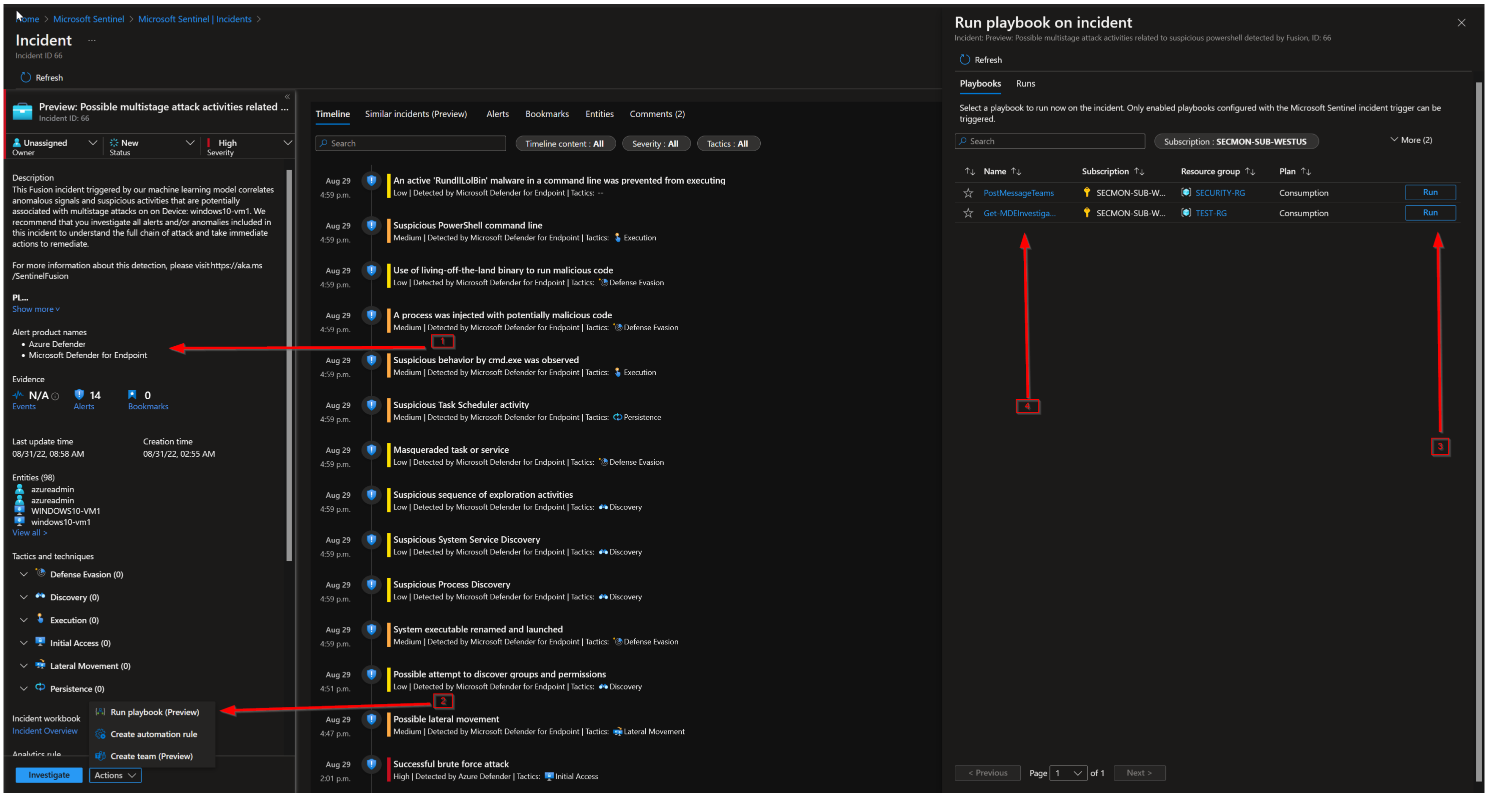
Subscription *

SECMON-SUB-WESTUS

Role	Resource Name	Resource Type	Assigned To
Microsoft Sentinel Responder	SECMON-SUB-WESTUS	Subscription	Get-MDEInvestigationPackage

How to use the logic app

1. Simulate a MDE or M365 Defender incident.
2. Click Actions - choose Run Playbook
3. Run the Get-MDEInvestigationPackage playbook.
4. Once the playbook triggered successfully, click the playbook name to view the status.



Home > Microsoft Sentinel > Microsoft Sentinel | Incidents >

Incident ...

Incident ID 66

Refresh

Preview: Possible multistage attack activities related ...

Incident ID: 66

Unassigned Owner | New Status | High Severity

Description

This Fusion incident triggered by our machine learning model correlates anomalous signals and suspicious activities that are potentially associated with multistage attacks on on Device: windows10-vm1. We recommend that you investigate all alerts and/or anomalies included in this incident to understand the full chain of attack and take immediate actions to remediate.

For more information about this detection, please visit https://aka.ms/SentinelFusion

PL...

Show more

Alert product names

- Azure Defender
- Microsoft Defender for Endpoint

Evidence

N/A Events   14 Alerts   0 Bookmarks

Last update time 08/31/22, 08:58 AM   Creation time 08/31/22, 02:55 AM

Entities (98)

azureadmin
azureadmin
WINDOWS10-VM1
windows10-vm1
View all >

Tactics and techniques

- Defense Evasion (0)
- Discovery (0)
- Execution (0)
- Initial Access (0)
- Lateral Movement (0)
- Persistence (0)

Incident workbook

Incident Overview

Analytics rule

Run playbook (Preview)

Create automation rule

Create team (Preview)

Investigate   Actions

Timeline   Similar incidents (Preview)   Alerts   Bookmarks   Entities   Comments (2)

Search   Timeline content : **All**   Severity : **All**   Tactics : **All**

Aug 29 4:59 p.m. — An active 'RundllLolBin' malware in a command line was prevented from executing
Low | Detected by Microsoft Defender for Endpoint | Tactics: --

Aug 29 4:59 p.m. — Suspicious PowerShell command line
Medium | Detected by Microsoft Defender for Endpoint | Tactics: Execution

Aug 29 4:59 p.m. — Use of living-off-the-land binary to run malicious code
Low | Detected by Microsoft Defender for Endpoint | Tactics: Defense Evasion

Aug 29 4:59 p.m. — A process was injected with potentially malicious code
Medium | Detected by Microsoft Defender for Endpoint | Tactics: Defense Evasion

Aug 29 4:59 p.m. — Suspicious behavior by cmd.exe was observed
Medium | Detected by Microsoft Defender for Endpoint | Tactics: Execution

Aug 29 4:59 p.m. — Suspicious Task Scheduler activity
Medium | Detected by Microsoft Defender for Endpoint | Tactics: Persistence

Aug 29 4:59 p.m. — Masqueraded task or service
Low | Detected by Microsoft Defender for Endpoint | Tactics: Defense Evasion

Aug 29 4:59 p.m. — Suspicious sequence of exploration activities
Low | Detected by Microsoft Defender for Endpoint | Tactics: Discovery

Aug 29 4:59 p.m. — Suspicious System Service Discovery
Low | Detected by Microsoft Defender for Endpoint | Tactics: Discovery

Aug 29 4:59 p.m. — Suspicious Process Discovery
Low | Detected by Microsoft Defender for Endpoint | Tactics: Discovery

Aug 29 4:59 p.m. — System executable renamed and launched
Medium | Detected by Microsoft Defender for Endpoint | Tactics: Defense Evasion

Aug 29 4:51 p.m. — Possible attempt to discover groups and permissions
Low | Detected by Microsoft Defender for Endpoint | Tactics: Discovery

Aug 29 4:47 p.m. — Possible lateral movement
Medium | Detected by Microsoft Defender for Endpoint | Tactics: Lateral Movement

Aug 29 2:01 p.m. — Successful brute force attack
High | Detected by Azure Defender | Tactics: Initial Access

Run playbook on incident

Incident: Preview: Possible multistage attack activities related to suspicious powershell detected by Fusion, ID: 66

Refresh

Playbooks   Runs

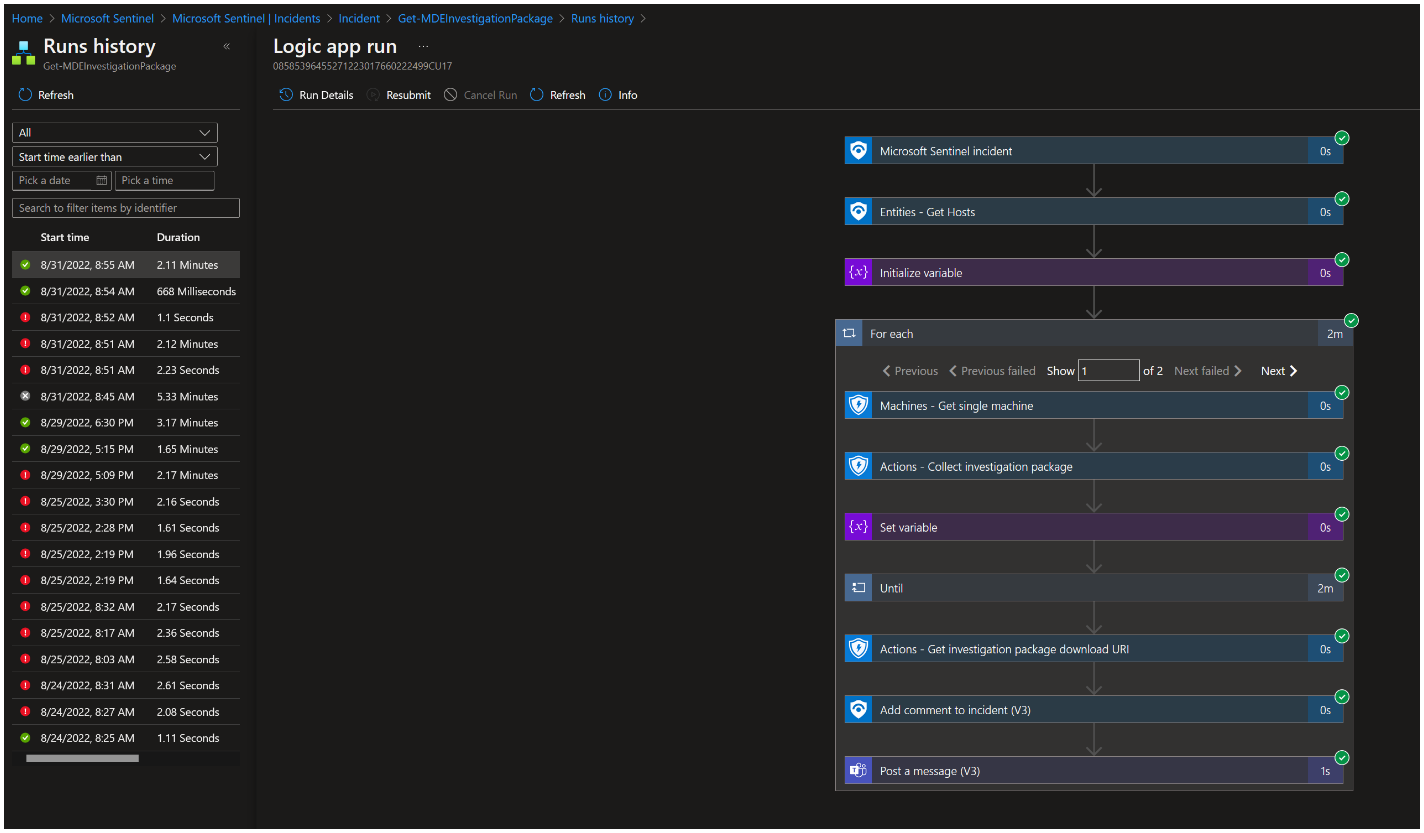
Select a playbook to run now on the incident. Only enabled playbooks configured with the Microsoft Sentinel incident trigger can be triggered.

Search   Subscription : **SECMON-SUB-WESTUS**   More (2)

	Name	Subscription	Resource group	Plan	
☆	PostMessageTeams	SECMON-SUB-W...	SECURITY-RG	Consumption	Run
☆	Get-MDEInvestiga...	SECMON-SUB-W...	TEST-RG	Consumption	Run

< Previous   Page 1 of 1   Next >

5. Please note that it will take about 2-3 minutes until it shows the result.

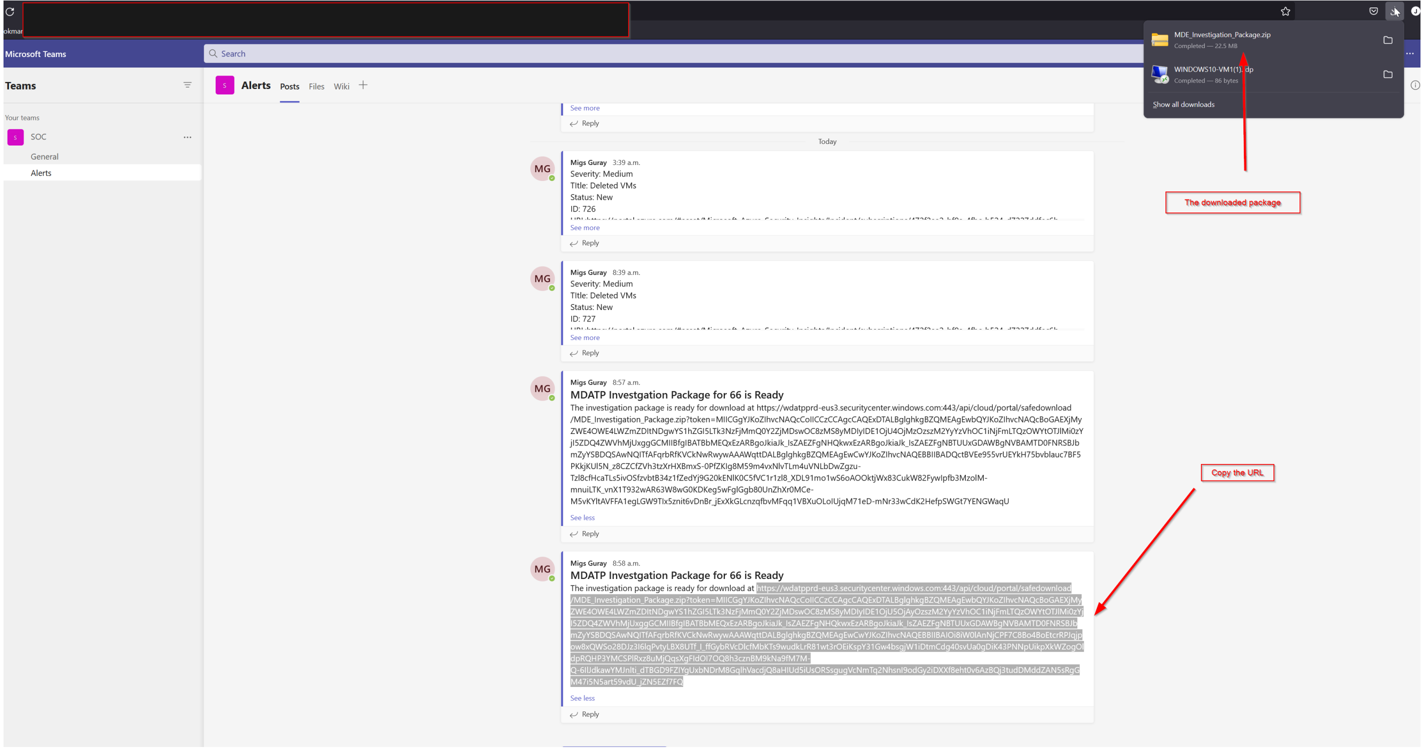

Home > Microsoft Sentinel > Microsoft Sentinel | Incidents > Incident > Get-MDEInvestigationPackage > Runs history >
Runs history
Get-MDEInvestigationPackage
Refresh
All
Start time earlier than
Pick a date
Pick a time
Search to filter items by identifier
Logic app run
08585396455271223017660222499CU17
Run Details
Resubmit
Cancel Run
Refresh
Info

Start time	Duration
8/31/2022, 8:55 AM	2.11 Minutes
8/31/2022, 8:54 AM	668 Milliseconds
8/31/2022, 8:52 AM	1.1 Seconds
8/31/2022, 8:51 AM	2.12 Minutes
8/31/2022, 8:51 AM	2.23 Seconds
8/31/2022, 8:45 AM	5.33 Minutes
8/29/2022, 6:30 PM	3.17 Minutes
8/29/2022, 5:15 PM	1.65 Minutes
8/29/2022, 5:09 PM	2.17 Minutes
8/25/2022, 3:30 PM	2.16 Seconds
8/25/2022, 2:28 PM	1.61 Seconds
8/25/2022, 2:19 PM	1.96 Seconds
8/25/2022, 2:19 PM	1.64 Seconds
8/25/2022, 8:32 AM	2.17 Seconds
8/25/2022, 8:17 AM	2.36 Seconds
8/25/2022, 8:03 AM	2.58 Seconds
8/24/2022, 8:31 AM	2.61 Seconds
8/24/2022, 8:27 AM	2.08 Seconds
8/24/2022, 8:25 AM	1.11 Seconds

Microsoft Sentinel incident 0s
Entities - Get Hosts 0s
Initialize variable 0s
For each 2m
Previous Previous failed Show 1 of 2 Next failed Next
Machines - Get single machine 0s
Actions - Collect investigation package 0s
Set variable 0s
Until 2m
Actions - Get investigation package download URI 0s
Add comment to incident (V3) 0s
Post a message (V3) 1s

6. If it runs successfully, go to Teams and check the message in the channel.

7. Copy the URL and paste it on another tab to download the package.


[redacted]

The downloaded package

Migs Guray 3:39 a.m.
Severity: Medium
TItle: Deleted VMs
Status: New
ID: 726

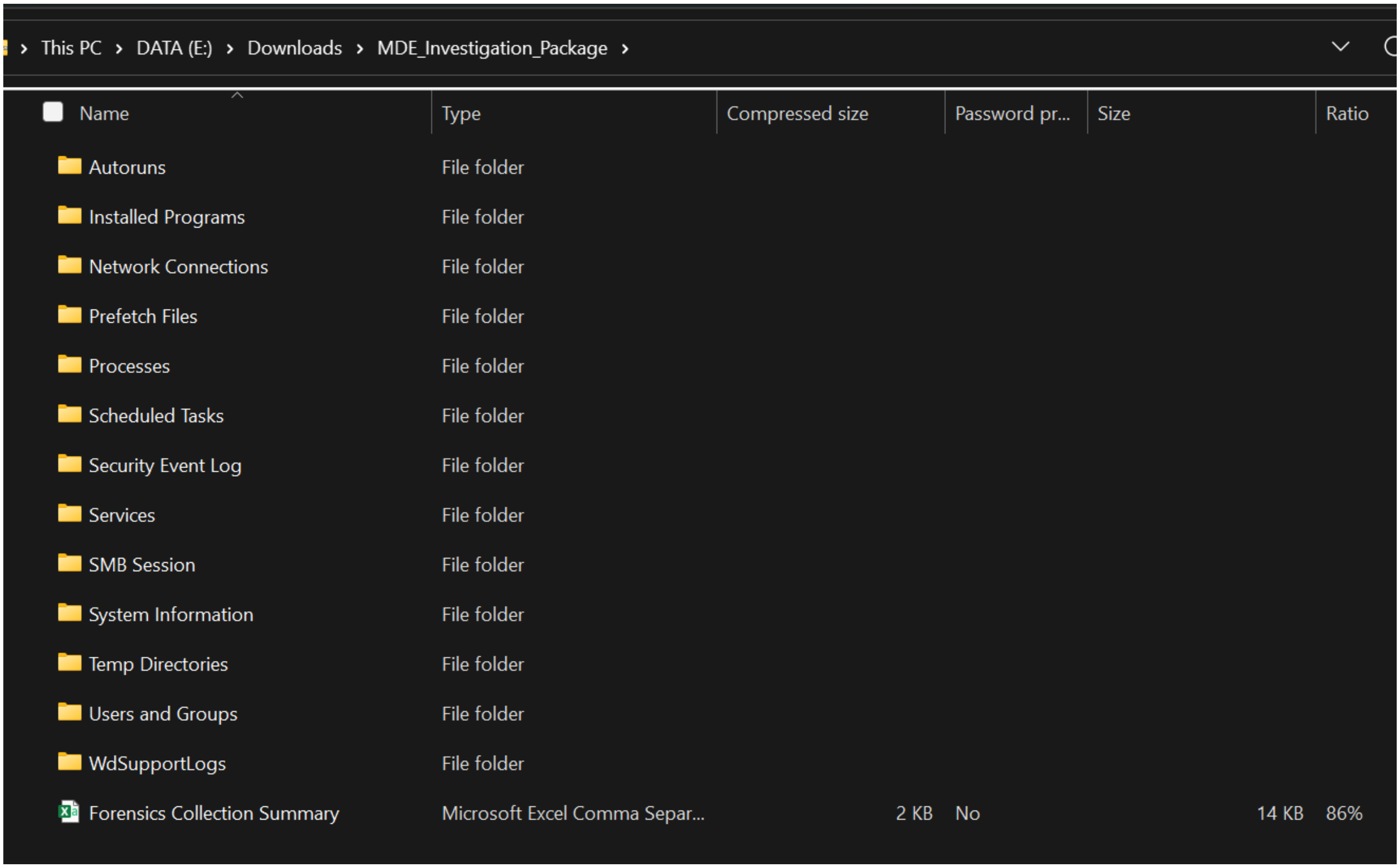
Migs Guray 8:39 a.m.
Severity: Medium
TItle: Deleted VMs
Status: New
ID: 727

Migs Guray 8:57 a.m.
MDATP Investgation Package for 66 is Ready
The investigation package is ready for download at https://wdatpprd-eus3.securitycenter.windows.com:443/api/cloud/portal/safedownload/MDE_Investigation_Package.zip?token=MIICGgYJKoZIhvcNAQcCoIICCzCCAgcCAQExDTALBglghkgBZQMEAgEwbQYJKoZIhvcNAQcBoGAEXjMyZWE4OWE4LWZmZDItNDgwYS1hZGI5LTk3NzFjMmQ0Y2ZjMDswOC8zMS8yMDIyIDE1OjU4OjMzOzszM2YyYzVhOC1iNjFmLTQzOWYtOTJlMi0zYjI5ZDQ4ZWVhMjUxggGCMIIBfgIBATBbMEQxEzARBgoJkiaJk_IsZAEZFgNHQkwxEzARBgoJkiaJk_IsZAEZFgNBTUUxGDAWBgNVBAMTD0FNRSBJbmZyYSBDQSAwNQITfAFqrbRfKVCkNwRwywAAAWqttDALBglghkgBZQMEAgEwCwYJKoZIhvcNAQEBBIIBADQctBVEe955vrUEYkH75bvblauc7BF5PKkjKUl5N_z8CZCfZVh3tzXrHXBmxS-0PfZKIg8M59m4vxNlvTLm4uVNLbDwZgzu-Tzl8cfHcaTLs5ivOSfzvbtB34z1fZedYj9G20kENlK0C5fVC1r1zl8_XDL91mo1wS6oAOOktjWx83CukW82FywIpfb3MzolM-mnuiLTK_vnX1T932wAR63W8wG0KDKeg5wFglGgb80UnZhXr0MCe-M5vKYltAVFFA1egLGW9TIx5znit6vDnBr_jExXkGLcnzqfbvMFqq1VBXuOLoIUjqM71eD-mNr33wCdK2HefpSWGt7YENGWaqU
See less
Reply

Migs Guray 8:58 a.m.
MDATP Investgation Package for 66 is Ready
The investigation package is ready for download at https://wdatpprd-eus3.securitycenter.windows.com:443/api/cloud/portal/safedownload/MDE_Investigation_Package.zip?token=MIICGgYJKoZIhvcNAQcCoIICCzCCAgcCAQExDTALBglghkgBZQMEAgEwbQYJKoZIhvcNAQcBoGAEXjMyZWE4OWE4LWZmZDItNDgwYS1hZGI5LTk3NzFjMmQ0Y2ZjMDswOC8zMS8yMDIyIDE1OjU5OjAyOzszM2YyYzVhOC1iNjFmLTQzOWYtOTJlMi0zYjI5ZDQ4ZWVhMjUxggGCMIIBfgIBATBbMEQxEzARBgoJkiaJk_IsZAEZFgNHQkwxEzARBgoJkiaJk_IsZAEZFgNBTUUxGDAWBgNVBAMTD0FNRSBJbmZyYSBDQSAwNQITfAFqrbRfKVCkNwRwywAAAWqttDALBglghkgBZQMEAgEwCwYJKoZIhvcNAQEBBIIBAIOi8iW0lAnNjCPF7C8Bo4BoEtcrRPJqjpow8xQWSo28DJz3I6lqPvtyLBX8UTf_I_ffGybRVcDlcfMbKTs9wudkLrR81wt3rOEiKspY31Gw4bsgjW1iDtmCdg40svUa0gDiK43PNNpUikpXkWZogOldpRQHP3YMCSPlRxz8uMjQqsXgFIdOI7OQ8h3cznBM9kNa9fM7M-Q-6IlJdkawYMJnlti_dTBGD9FZIYgUxbNDrM8GqlhVacdjQ8aHIUd5iUsORSsgugVcNmTq2NhsnI9odGy2iDXXf8eht0v6AzBQj3tudDMddZAN5sRgGM47i5N5art59vdU_jZN5EZf7FQ
See less
Reply

Copy the URL

8. Here's the contents of the zip file.

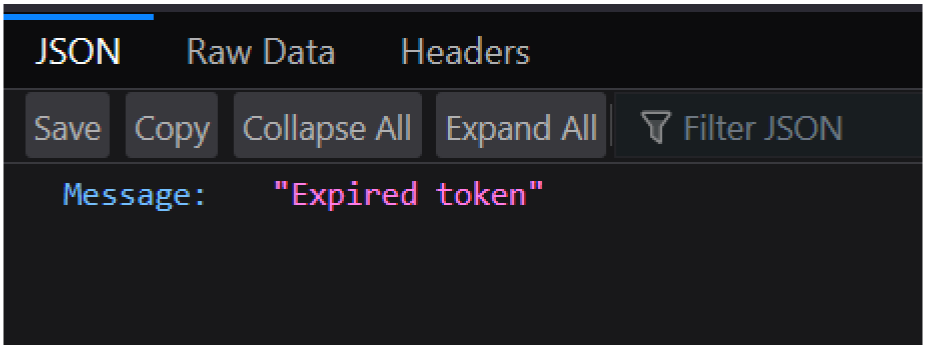


› This PC › DATA (E:) › Downloads › MDE_Investigation_Package ›

Name	Type	Compressed size	Password pr...	Size	Ratio
Autoruns	File folder				
Installed Programs	File folder				
Network Connections	File folder				
Prefetch Files	File folder				
Processes	File folder				
Scheduled Tasks	File folder				
Security Event Log	File folder				
Services	File folder				
SMB Session	File folder				
System Information	File folder				
Temp Directories	File folder				
Users and Groups	File folder				
WdSupportLogs	File folder				
Forensics Collection Summary	Microsoft Excel Comma Separ...	2 KB	No	14 KB	86%

Common Issues

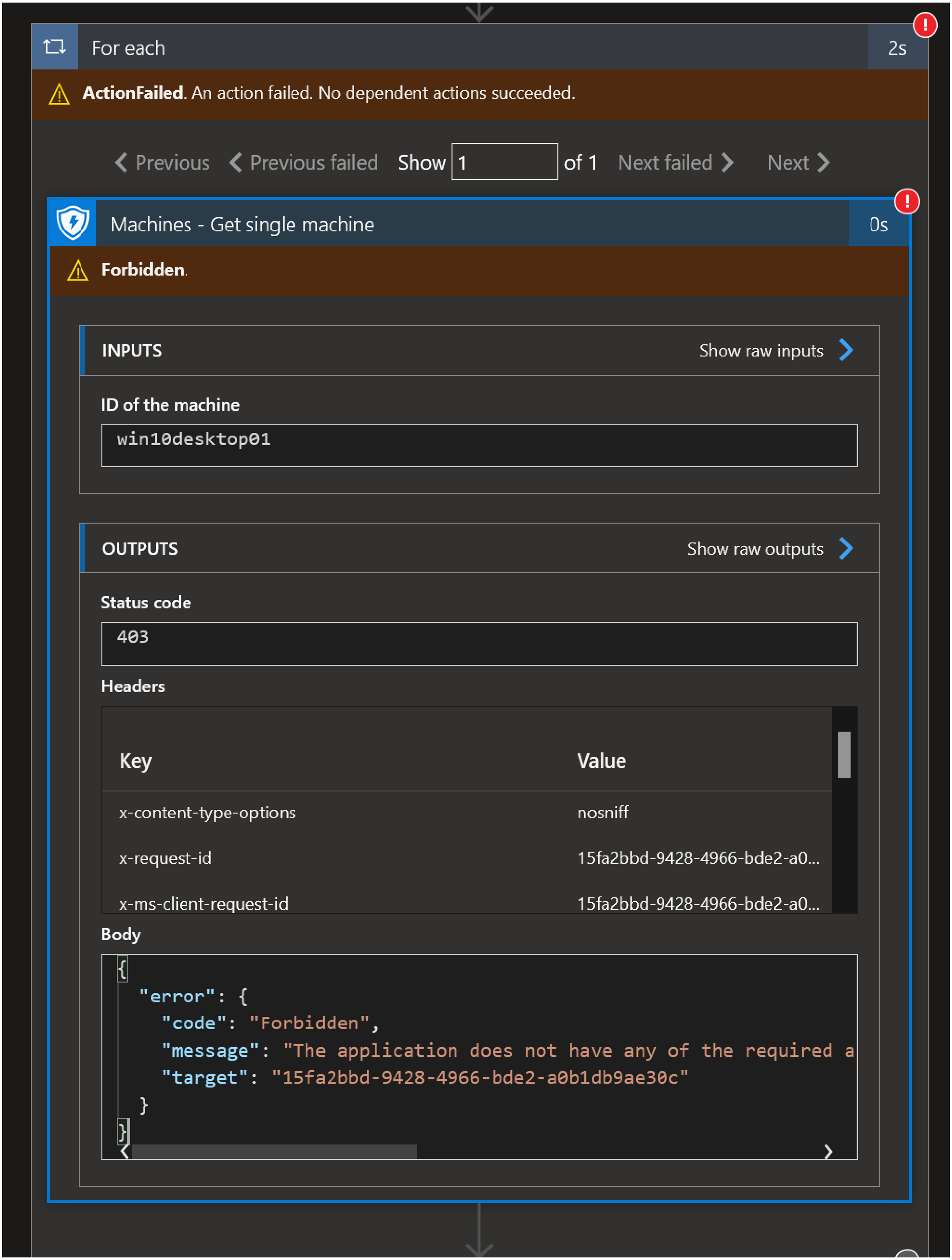
The playbook generated a URI for downloading the package, but an expired token appears. Please inform the customer that the URI must be immediately (within 1 minute). https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/get-package-sas-uri?view=o365-worldwide#response



```
Message:    "Expired token"
```

The customer runs the playbook, but received an error "'message': 'The application does not have any of the required application permissions (Machine.Read.All, Machine.ReadWrite.All) to access the resource".

Solution: Ensure that the customer has added Machine.Read.All, Machine.ReadWrite.All permissions to the managed identity. Check no. 2 of prerequisites.



ActionFailed. An action failed. No dependent actions succeeded.

Forbidden.

INPUTS

ID of the machine

win10desktop01

OUTPUTS

Status code

403

Headers

Key	Value
x-content-type-options	nosniff
x-request-id	15fa2bbd-9428-4966-bde2-a0...
x-ms-client-request-id	15fa2bbd-9428-4966-bde2-a0...

Body

```
{
  "error": {
    "code": "Forbidden",
    "message": "The application does not have any of the required a
    "target": "15fa2bbd-9428-4966-bde2-a0b1db9ae30c"
  }
}
```

Actions - Collect investigation package