Windows PowerShell Get-Help on Cmdlet 'Get-AzSecurityAlert'

PS:\>Get-HELP Get-AzSecurityAlert -Full

NAME

Get-AzSecurityAlert

SYNOPSIS

Gets security alerts that were detected by Azure Security Center

SYNTAX

Get-AzSecurityAlert [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Location <System.String> -Name <System.String> -ResourceGroupName <System.String> [<CommonParameters>]

Get-AzSecurityAlert [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Location <System.String> -Name <System.String> [<CommonParameters>]

Get-AzSecurityAlert [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -ResourceGroupName

<System.String>

[<CommonParameters>]

Get-AzSecurityAlert [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -ResourceId <System.String>

[<CommonParameters>]

DESCRIPTION

Gets security alerts that were detected by Azure Security Center

PARAMETERS

-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>

The credentials, account, tenant, and subscription used for communication with Azure.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Location <System.String>

Location.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Name <System.String>

Resource name.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceGroupName <System.String>

Resource group name.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceId <System.String>

Resource ID.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug,

ErrorAction, ErrorVariable, WarningAction, WarningVariable,

OutBuffer, PipelineVariable, and OutVariable. For more information, see

about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

INPUTS

System.String

OUTPUTS

Microsoft.Azure.Commands.Security.Models.Alerts.PSSecurityAlert

NOTES

---------- Example 1 ----------

Get-AzSecurityAlert

Id : /subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/RSG/providers/Microsoft.Securit
y/locations/centralus/alerts/2518710774294070750_FFF23C70-80EF-4A8B-9122-507B0EA8DFFF
Name : 2518710774294070750_FFF23C70-80EF-4A8B-9122-507B0EA8DFFF
ActionTaken : Undefined
AlertDisplayName : PREVIEW - Vulnerability scanner detected
AlertName : APPS_WpScanner
AssociatedResource :
/subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/RSG/providers/Microsoft.Web/sit
es/testSite1
CanBeInvestigated : True
CompromisedEntity : testSite1
ConfidenceReasons : {}
ConfidenceScore :
Description : Azure App Services activity log indicates a possible vulnerability scanner usage on your App
Service resource.

The suspicious activity detected resembles that of tools targeting WordPress applications.

DetectedTimeUtc : 10/07/2018 11:49:30

Entities : {}

ExtendedProperties : {[sample User Agents, WPScan+v2.9.3+(http://wpscan.org)], [last Event Time, 6/23/2018 12:18:58 AM], [sample URIs, /wp-config.php.original, /wp-includes/css/editor.min.css, /wp-includes/js/wp-emoji.js, /wp-config.old, /xmlrpc.php, /wp-admin/css/wp-admin-rtl.css, /#wp-config.php#, /wp-includes/js/tinymce/plugins/wplink/plugin.js, /wp-includes/js/tinymce/plugins/wordpress/editor_plugin.js, /wp-admin/js/post.js], [sample Referer, https://www.stone.com.br/]...}

InstanceId : fff23c70-80ef-4a8b-9122-507b0ea8dfff

RemediationSteps : 1. If WordPress is installed, make sure that the application is up to date and automatic updates are enabled.
2. If only specific IPs should access to the web application, use IP Restrictions (https://learn.microsoft.com/azure/app-service/app-service-ip-restrictions).

ReportedSeverity : High

ReportedTimeUtc : 10/07/2018 16:31:52

State : Active

SubscriptionId : 487bb485-b5b0-471e-9c0d-10717612f869

SystemSource :

VendorName : Microsoft

WorkspaceArmId :

Id : /subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/providers/Microsoft.Security/locations/centralus/alerts/2518710774894070750_EEE23C70-80EF-4A8B-9122-507B0EA8DFFF

Name : 2518710774894070750_EEE23C70-80EF-4A8B-9122-507B0EA8DFFF

ActionTaken : Undefined

AlertDisplayName : PREVIEW - Spam folder referrer detected

AlertName : APPS_SpamReferrer

AssociatedResource : /subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/providers/Microsoft.Web/sites/testSite2

CanBeInvestigated : True

CompromisedEntity : testSite2

ConfidenceReasons : {}

ConfidenceScore :

Description : Azure App Services activity log indicates web activity that was identified as originating from a web site associated with SPAM activity.
This could occur if your web site is compromised and used for spam activity.

DetectedTimeUtc : 10/07/2018 11:48:30

Entities : {}

ExtendedProperties : {[sample User Agents, Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)], [last Event Time, 6/23/2018 4:53:58 PM], [sample URIs, /acropolis.php, /wp-content/animator.php, /bandpass.php, /wp-content/base.php, /candid.php, /wp-content/uploads/2018/christina.php, /wp-content/climax.php, /wp-content/uploads/conditioning.php, /wp-content/corkscrew.php, /wp-content/uploads/2018/countermeasures.php], [sample Referer, https://google.com/mail/inbox/spam/]...}

InstanceId : eee23c70-80ef-4a8b-9122-507b0ea8dfff

RemediationSteps : Review the URIs in the alert details. Check whether the corresponding files contain malicious or suspicious content.
If they do, escalate the alert to the information security team.

ReportedSeverity : High

ReportedTimeUtc : 10/07/2018 16:31:52

State : Active

SubscriptionId : 487bb485-b5b0-471e-9c0d-10717612f869

SystemSource :

VendorName : Microsoft

WorkspaceArmId :

Id : /subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.Security/locations/westeurope/alerts/2518675199999999999_0501972d-06cd-47c7-a276-036f67d89262

Name : 2518675199999999999_0501972d-06cd-47c7-a276-036f67d89262

ActionTaken : Detected

AlertDisplayName : PROTOCOL-ENFORCEMENT

AlertName : PROTOCOL-ENFORCEMENT

AssociatedResource : /subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.Network/applicationGateways/ContosoWAF

CanBeInvestigated : True

CompromisedEntity : 10.1.0.4

ConfidenceReasons : {}

ConfidenceScore :

Description : Detail:Host header is a numeric IP address 13.69.131.117:80

DetectedTimeUtc : 20/08/2018 16:00:00

Entities : {}

ExtendedProperties : {[hit Count, 1], [source IPs, 177.189.28.238], [management URL, https://portal.azure.com#resource/subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.Network/applicationGateways/ContosoWAF/overview], [resourceType, Networking]}

InstanceId : 0501972d-06cd-47c7-a276-036f67d89262

RemediationSteps :

ReportedSeverity : Low

ReportedTimeUtc : 20/08/2018 17:00:18

State : Active

SubscriptionId : 487bb485-b5b0-471e-9c0d-10717612f869

SystemSource : Azure

VendorName : Microsoft WAF

WorkspaceArmId : /subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourcegroups/defaultresourcegroup-eus/providers/microsoft.operationalinsights/workspaces/defaultworkspace-487bb485-b5b0-471e-9c0d-10717612f869-eus

Id : /subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.Security/locations/westeurope/alerts/2518675235999999999_0cd957d9-8101-47f7-88cc-0c5d0ebdbfd0

Name : 2518675235999999999_0cd957d9-8101-47f7-88cc-0c5d0ebdbfd0

ActionTaken : Detected

AlertDisplayName : PROTOCOL-ENFORCEMENT

AlertName : PROTOCOL-ENFORCEMENT

AssociatedResource : /subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.Network/applicationGateways/ContosoWAF

CanBeInvestigated : True

CompromisedEntity : 10.1.0.4

ConfidenceReasons : {}

ConfidenceScore :

Description : Detail:Host header is a numeric IP address 13.69.131.117

DetectedTimeUtc : 20/08/2018 15:00:00

Entities : {}

ExtendedProperties : {[hit Count, 1], [source IPs, 217.91.251.86], [management URL, https://portal.azure.com#resource/subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.Network/applicationGateways/ContosoWAF/overview], [resourceType, Networking]}

InstanceId : 0cd957d9-8101-47f7-88cc-0c5d0ebdbfd0

RemediationSteps :

ReportedSeverity : Low

ReportedTimeUtc : 20/08/2018 16:00:03

State : Active

SubscriptionId : 487bb485-b5b0-471e-9c0d-10717612f869

SystemSource : Azure

VendorName : Microsoft WAF

WorkspaceArmId : /subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourcegroups/defaultresourcegroup-eus/providers/microsoft.operationalinsights/workspaces/defaultworkspace-487bb485-b5b0-471e-9c0d-10717612f869-eus

Gets all the security alerts that were detected on resources inside a subscription

---------- Example 2 ----------

Get-AzSecurityAlert -ResourceGroupName "myService1"

Id : /subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.Security/locations/westeurope/alerts/2518675199999999999_0501972d-06cd-47c7-a276-036f67d89262

Name : 2518675199999999999_0501972d-06cd-47c7-a276-036f67d89262

ActionTaken : Detected

AlertDisplayName : PROTOCOL-ENFORCEMENT

AlertName : PROTOCOL-ENFORCEMENT

AssociatedResource :
/subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.
Network/applicationGateways/ContosoWAF

CanBeInvestigated : True

CompromisedEntity : 10.1.0.4

ConfidenceReasons : {}

ConfidenceScore :

Description : Detail:Host header is a numeric IP address 13.69.131.117:80

DetectedTimeUtc : 20/08/2018 16:00:00

Entities : {}

ExtendedProperties : {[hit Count, 1], [source IPs, 177.189.28.238], [management URL, https://portal.azure.com#resource/
subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.N
etwork/applicationGateways/ContosoWAF/overview], [resourceType, Networking]}

InstanceId : 0501972d-06cd-47c7-a276-036f67d89262

RemediationSteps :

ReportedSeverity : Low

ReportedTimeUtc : 20/08/2018 17:00:18

State : Active

SubscriptionId : 487bb485-b5b0-471e-9c0d-10717612f869

SystemSource : Azure

VendorName : Microsoft WAF

WorkspaceArmId :
/subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourcegroups/defaultresourcegroup-eus/provid
ers/microsoft.operationalinsights/workspaces/defaultworkspace-487bb485-b5b0-471e-9c0d-10717612f869
-eus

Id : /subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.
Security/locations/westeurope/alerts/2518675235999999999_0cd957d9-8101-47f7-88cc-0c5d0ebdbfd0

Name : 2518675235999999999_0cd957d9-8101-47f7-88cc-0c5d0ebdbfd0

ActionTaken : Detected

AlertDisplayName : PROTOCOL-ENFORCEMENT

AlertName : PROTOCOL-ENFORCEMENT

AssociatedResource :
/subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.
Network/applicationGateways/ContosoWAF
CanBeInvestigated : True
CompromisedEntity : 10.1.0.4
ConfidenceReasons : {}
ConfidenceScore :
Description : Detail:Host header is a numeric IP address 13.69.131.117
DetectedTimeUtc : 20/08/2018 15:00:00
Entities : {}
ExtendedProperties : {[hit Count, 1], [source IPs, 217.91.251.86], [management URL, https://portal.azure.com#resource/s
ubscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.Ne
twork/applicationGateways/ContosoWAF/overview], [resourceType, Networking]}
InstanceId : 0cd957d9-8101-47f7-88cc-0c5d0ebdbfd0
RemediationSteps :
ReportedSeverity : Low
ReportedTimeUtc : 20/08/2018 16:00:03
State : Active
SubscriptionId : 487bb485-b5b0-471e-9c0d-10717612f869
SystemSource : Azure
VendorName : Microsoft WAF
WorkspaceArmId :
/subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourcegroups/defaultresourcegroup-eus/provid
ers/microsoft.operationalinsights/workspaces/defaultworkspace-487bb485-b5b0-471e-9c0d-10717612f869
-eus

Id : /subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.
Security/locations/westeurope/alerts/2518675235999999999_3cc2c984-3d3d-4af2-a2d9-ed7c6d078315
Name : 2518675235999999999_3cc2c984-3d3d-4af2-a2d9-ed7c6d078315
ActionTaken : Detected
AlertDisplayName : PROTOCOL-ENFORCEMENT
AlertName : PROTOCOL-ENFORCEMENT
AssociatedResource :

/subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.
Network/applicationGateways/ContosoWAF
CanBeInvestigated : True
CompromisedEntity : 10.1.0.5
ConfidenceReasons : {}
ConfidenceScore :
Description : Detail:Host header is a numeric IP address 13.69.131.117
DetectedTimeUtc : 20/08/2018 15:00:00
Entities : {}
ExtendedProperties : {[hit Count, 1], [source IPs, 217.91.251.86], [management URL, https://portal.azure.com#resource/s
ubscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.Ne
twork/applicationGateways/ContosoWAF/overview], [resourceType, Networking]}
InstanceId : 3cc2c984-3d3d-4af2-a2d9-ed7c6d078315
RemediationSteps :
ReportedSeverity : Low
ReportedTimeUtc : 20/08/2018 16:00:04
State : Active
SubscriptionId : 487bb485-b5b0-471e-9c0d-10717612f869
SystemSource : Azure
VendorName : Microsoft WAF
WorkspaceArmId :
/subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourcegroups/defaultresourcegroup-eus/provid
ers/microsoft.operationalinsights/workspaces/defaultworkspace-487bb485-b5b0-471e-9c0d-10717612f869
-eus

Id : /subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.
Security/locations/westeurope/alerts/2518675307999999999_bbbda0ad-b149-49f4-a4ba-3e95540cbf1c
Name : 2518675307999999999_bbbda0ad-b149-49f4-a4ba-3e95540cbf1c
ActionTaken : Detected
AlertDisplayName : PROTOCOL-ENFORCEMENT
AlertName : PROTOCOL-ENFORCEMENT
AssociatedResource :
/subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.

Network/applicationGateways/ContosoWAF

CanBeInvestigated : True

CompromisedEntity : 10.1.0.4

ConfidenceReasons : {}

ConfidenceScore :

Description : Detail:Host header is a numeric IP address 13.69.131.117:80

DetectedTimeUtc : 20/08/2018 13:00:00

Entities : {}

ExtendedProperties : {[hit Count, 1], [source IPs, 177.86.202.171], [management URL, https://portal.azure.com#resource/subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.Network/applicationGateways/ContosoWAF/overview], [resourceType, Networking]}

InstanceId : bbbda0ad-b149-49f4-a4ba-3e95540cbf1c

RemediationSteps :

ReportedSeverity : Low

ReportedTimeUtc : 20/08/2018 14:00:36

State : Active

SubscriptionId : 487bb485-b5b0-471e-9c0d-10717612f869

SystemSource : Azure

VendorName : Microsoft WAF

WorkspaceArmId : /subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourcegroups/defaultresourcegroup-eus/providers/microsoft.operationalinsights/workspaces/defaultworkspace-487bb485-b5b0-471e-9c0d-10717612f869-eus

Gets all the security alerts that were detected on resources inside the "myService1" resource group

---------- Example 3 ----------

Get-AzSecurityAlert -ResourceGroupName "myService1" -Location "westeurope" -Name "2518675235999999999_0cd957d9-8101-47f7-88cc-0c5d0ebdbfd0"

Id : /subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Micr-esoft.

Security/locations/westeurope/alerts/2518675235999999999_0cd957d9-8101-47f7-88cc-0c5d0ebdbfd0

Name : 2518675235999999999_0cd957d9-8101-47f7-88cc-0c5d0ebdbfd0

ActionTaken : Detected

AlertDisplayName : PROTOCOL-ENFORCEMENT

AlertName : PROTOCOL-ENFORCEMENT

AssociatedResource :
/subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.
Network/applicationGateways/ContosoWAF

CanBeInvestigated : True

CompromisedEntity : 10.1.0.4

ConfidenceReasons : {}

ConfidenceScore :

Description : Detail:Host header is a numeric IP address 13.69.131.117

DetectedTimeUtc : 20/08/2018 15:00:00

Entities : {}

ExtendedProperties : {[hit Count, 1], [source IPs, 217.91.251.86], [management URL, https://portal.azure.com#resource/s
ubscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourceGroups/myService1/providers/Microsoft.Ne
twork/applicationGateways/ContosoWAF/overview], [resourceType, Networking]}

InstanceId : 0cd957d9-8101-47f7-88cc-0c5d0ebdbfd0

RemediationSteps :

ReportedSeverity : Low

ReportedTimeUtc : 20/08/2018 16:00:03

State : Active

SubscriptionId : 487bb485-b5b0-471e-9c0d-10717612f869

SystemSource : Azure

VendorName : Microsoft WAF

WorkspaceArmId :
/subscriptions/487bb485-b5b0-471e-9c0d-10717612f869/resourcegroups/defaultresourcegroup-eus/provid
ers/microsoft.operationalinsights/workspaces/defaultworkspace-487bb485-b5b0-471e-9c0d-10717612f869
-eus

Gets a specific security alert that were detected on resources inside the "myService1" resource group

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.security/Get-AzSecurityAlert