Splunk SOAR

# McAfee ePO

<https://splunkbase.splunk.com/app/5812>

This app implements various endpoint based investigative and containment actions by integrating with McAfee ePO.

Supported Actions:

* **test connectivity**: Validate connectivity to McAfee ePO
* **add tag**: Add a tag to an endpoint
* **remove tag**: Remove a tag from the endpoint
* **get device info**: Get information about an endpoint
* **quarantine device**: Send the quarantine tag to the endpoint
* **unquarantine device**: Remove the quarantine tag on the endpoint

# Active Directory LDAP

<https://splunkbase.splunk.com/app/5755>

App specifically designed for interacting with Microsoft Active Directory's LDAP Implementation.

Supported Actions:

* **test connectivity**: Validate the asset configuration for connectivity using supplied configuration
* **add group members**: Adds one or more Active Directory objects to one or more groups
* **remove group members**: Removes one or more Active Directory objects from one or more groups
* **unlock account**: Unlocks a locked Active Directory account
* **disable account**: Disables an Active Directory account
* **enable account**: Enables a disabled Active Directory account
* **reset password**: Resets the password of a user, requiring the user to change password at next login
* **set password**: Set a user's password
* **move object**: Moves an entry in Active Directory
* **run query**: Query Active Directory LDAP
* **get attributes**: Get attributes of various principals
* **set attribute**: Add, delete, or replace an attribute of a user

# Windows Remote Management

<https://splunkbase.splunk.com/app/5875>

This app integrates with the Windows Remote Management service to execute various actions.

Supported Actions:

* **test connectivity**: Validate the asset configuration for connectivity using supplied configuration
* **run command**: Execute a command on the endpoint
* **run script**: Run a PowerShell script on the endpoint
* **list processes**: List the currently running processes
* **terminate process**: Terminate a process
* **list connections**: List all active connections
* **list firewall rules**: List the firewall rules
* **delete firewall rule**: Remove a firewall rule using netsh
* **block ip**: Create a firewall rule to block a specified IP
* **add firewall rule**: Add a firewall rule using netsh
* **logoff user**: Logoff a user
* **list sessions**: List all active sessions
* **deactivate partition**: Deactivate a partition
* **activate partition**: Activate a partition
* **shutdown system**: Shutdown a system
* **restart system**: Restart a system
* **list policies**: List AppLocker Policies
* **block file path**: Create a new AppLocker policy to block a file path
* **delete policy**: Delete an AppLocker policy
* **get file**: Copy a file from the Windows Endpoint to the Vault
* **upload file**: Copy a file from the vault to the Windows Endpoint
* **copy file**: Run the copy command on the Windows Endpoint
* **delete file**: Run the delete command on the Windows Endpoint

# WMI

<https://splunkbase.splunk.com/app/5871>

This App uses the WMI WQL to implement investigative actions that are executed on a Windows endpoint.

Supported Actions:

* **test connectivity**: Validate the asset configuration for connectivity
* **list services**: Get the list of installed services on the system
* **get system info**: Get information about a system
* **list users**: List users configured on a system
* **run query**: Run an arbitrary query using WQL on the system

# SSH

<https://splunkbase.splunk.com/app/5850>

This app supports executing various endpoint-based investigative and containment actions on an SSH endpoint.

Supported Actions:

* **test connectivity**: Validates endpoint connection
* **execute program**: Executes a program on the remote machine
* **list connections**: Lists all the network connections. Requires root privileges. Requires netstat to be installed
* **block ip**: Add an iptables rule to the Linux server. Requires root privileges. Not supported on OS X
* **list firewall rules**: Lists the rules in iptables. Requires root privileges. Not supported on OS X
* **delete firewall rule**: Delete a firewall rule. Requires root privileges. Not supported on OS X
* **reboot system**: Reboot the endpoint (Requires root privileges)
* **shutdown system**: Shutdown the endpoint(Requires root privileges)
* **terminate process**: Terminate a process (Requires root privileges)
* **logoff user**: Logout a user on endpoint (Requires root privileges)
* **list processes**: List processes on endpoint
* **get disk usage**: Retrieve disk usage from endpoint
* **get memory usage**: Retrieve memory usage from endpoint
* **get file**: Retrieve a file from the endpoint and save it to the vault
* **put file**: Put a file from the vault to another location

# HTTP

<https://splunkbase.splunk.com/app/5904>

This App facilitates making HTTP requests as actions.

Supported Actions:

* **test connectivity**: Validate connection using the configured credentials
* **put data**: Perform a REST PUT call to the server
* **patch data**: Perform a REST PATCH call to the server
* **delete data**: Perform a REST DELETE call to the server
* **get headers**: Perform a REST HEAD call to the server
* **get options**: Perform a REST OPTIONS call to the server
* **get data**: Perform a REST GET call to the server
* **post data**: Perform a REST POST call to the server
* **get file**: Retrieve a file from the endpoint and save it to the vault
* **put file**: Put a file from the vault to another location

# DNS

<https://splunkbase.splunk.com/app/5893>

This app implements investigative actions that return DNS Records for the object queried.

Supported Actions:

* **test connectivity**: Validate the asset configuration for connectivity
* **lookup domain**: Query DNS records for a Domain or Host Name
* **lookup ip**: Query Reverse DNS records for an IP

# MongoDB

<https://splunkbase.splunk.com/app/5822>

This app supports CRUD operations in a MongoDB database.

Supported Actions:

* test connectivity: Validate the asset configuration for connectivity using supplied configuration
* post data: Add data to the database
* get data: Get data from the database
* update data: Update documents which match a given filter
* delete data: Delete documents which match a given filter
* list tables: List all the collections in the database

# Microsoft SQL Server

<https://splunkbase.splunk.com/app/6143>

This app supports investigative actions against a Microsoft SQL Server.

Supported Actions:

* **test connectivity**: Validate the asset configuration for connectivity using supplied configuration
* **list columns**: List all the columns in a table
* **list tables**: List all the tables in the database
* **run query**: Run a query against a table or tables in the database

# CSV Import

<https://splunkbase.splunk.com/app/6294>

Ingest CSV files into Phantom.

Supported Actions:

* **ingest csv**: Read contents of a CSV and create artifact
* **csv from artifacts**: Create the csv in the vault from the artifacts of container

# Cisco ISE

<https://splunkbase.splunk.com/app/5885>

This app implements investigative and containment actions on a Cisco ISE device.

Supported Actions:

* **test connectivity**: Validate the asset configuration for connectivity. This action logs into the device using a REST API call to check the connection and credentials
* **list endpoints**: List the endpoints configured on the system
* **get device info**: Get information about a specific endpoint
* **update device info**: Update information or attributes for a specific endpoint
* **list sessions**: List the sessions currently available on the Monitoring node
* **terminate session**: Terminate sessions
* **list resources**: Lists all the resources configured on the system of a particular resource
* **get resources**: Get the information about resource if resource\_id is provided. Fetch the list of resources match with the key-value filter
* **delete resource**: Delete a resource
* **create resource**: Create a resource
* **update resource**: Update a resource
* **apply policy**: Apply policy on selected Ip address or MAC address
* **clear policy**: Clear policy on selected Ip address or MAC address
* **list policies**: Lists all the ANC policies available
* **add policy**: Add a new ANC Policy
* **delete policy**: Delete a policy

# Check Point Firewall

<https://splunkbase.splunk.com/app/5777>

This app supports a variety of endpoint and network based containment actions on Check Point Firewall.

Supported Actions:

* **test connectivity**: Validate the asset configuration for connectivity
* **list policies**: List policies
* **list layers**: List access layers
* **block ip**: Block an IP/subnet
* **unblock ip**: Unblock an IP/subnet
* **list hosts**: List hosts
* **add host**: Add host
* **delete host**: Delete host
* **add network**: Create network object
* **delete network**: Delete network object
* **update group members**: Update group members
* **logout session**: Logout of an existing session
* **install policy**: Executes the install-policy on a given list of targets
* **add user**: Create a new user based on a pre-built template
* **delete user**: Delete existing user

# Microsoft Exchange On-Premise EWS

<https://splunkbase.splunk.com/app/5788>

This app performs email ingestion, investigative and containment actions on an on-premise Exchange installation.

Supported Actions:

* **test connectivity**: Validate the asset configuration for connectivity using supplied configuration
* **run query**: Search emails
* **delete email**: Delete emails
* **copy email**: Copy an email to a folder
* **move email**: Move an email to a folder
* **get email**: Get an email from the server
* **list addresses**: Get the email addresses that make up a Distribution List
* **lookup email**: Resolve an Alias name or email address, into mailboxes
* **update email**: Update an email on the server
* **on poll**: Ingest emails from the server into Phantom

# Microsoft SCOM

<https://splunkbase.splunk.com/app/5914>

This app integrates with Microsoft System Center Operations Manager (SCOM) to execute investigative actions.

Supported Actions:

* **test connectivity**: Validate the asset configuration for connectivity using supplied configuration
* **list endpoints**: List all the endpoints/sensors configured on the device
* **list alerts**: List all active alerts
* **get device info**: Get information about device

# Microsoft SCCM

<https://splunkbase.splunk.com/app/5816>

This app integrates with Microsoft System Center Configuration Manager (SCCM) to execute investigative and generic actions.

Supported Actions:

* **test connectivity**: Validate the asset configuration for connectivity using supplied configuration
* **deploy patch**: Deploy patch
* **list patches**: List all software patches
* **list device groups**: List all device groups

# Azure DevOps

<https://splunkbase.splunk.com/app/6628>

This app integrates with Azure DevOps to perform investigative and generic actions.

Supported Actions:

* **test connectivity**: Validate the asset configuration for connectivity using supplied configuration
* **get work item**: Get information about a single work item
* **add work item**: Creates a single work item
* **list iterations**: Get team's iteration
* **add comment**: Add a comment on a work item
* **add attachment**: Add an attachment to a project

# ServiceNow

<https://splunkbase.splunk.com/app/5932>

This app integrates with ServiceNow to perform investigative and generic actions.

Supported Actions:

* **test connectivity**: Run a query on the device to test connection and credentials
* **add work note**: Add a work note to a record
* **add comment**: Add a comment to a record
* **describe service catalog**: Fetches the details of a catalog
* **request catalog item**: Requests a catalog item
* **describe catalog item**: Fetches the details of a catalog item
* **list services**: Get a list of items
* **list categories**: Get a list of categories
* **list service catalogs**: Get a list of catalogs
* **list tickets**: Get a list of tickets/records
* **create ticket**: Create a new ticket/record
* **get ticket**: Get ticket/record information
* **update ticket**: Update ticket/record information
* **get variables**: Get variables for a ticket/record
* **run query**: Gets object data according to the specified query
* **query users**: Gets user data according to the specified query, username, or system ID
* **on poll**: Ingest tickets from SNOW

# SMTP

<https://splunkbase.splunk.com/app/5847>

This app provides the ability to send email using SMTP.

Supported Actions:

* **test connectivity**: Validate the asset configuration for connectivity. This action logs into the device and sends a test email to check the connection and credentials
* **send email**: Sends an email
* **send rawemail**: Takes a fully specified email and sends it unmodified to the smtp server. Sender and Recipient(s) will be extracted from message headers; Suggest using the standard email package to build message and export with the .as\_string() method
* **send htmlemail**: Sends a html email with optional text rendering. Attachments are allowed a Content-ID tag for reference within the html

# Splunk

<https://splunkbase.splunk.com/app/5848>

This app integrates with Splunk to update data on the device, in addition to investigate and ingestion actions.

Supported Actions:

* **test connectivity**: Validate the asset configuration for connectivity. This action logs into the device to check the connection and credentials
* **get host events**: Get events pertaining to a host that have occurred in the last 'N' days
* **on poll**: Ingest logs from the Splunk instance
* **run query**: Run a search query on the Splunk device. Please escape any quotes that are part of the query string
* **update event**: Update a notable event
* **post data**: Post data to Splunk

# vSphere

<https://splunkbase.splunk.com/app/5943>

This app implements investigative, containment and VM management actions on VMware ESXi or vCenter server.

Supported Actions:

* **test connectivity**: Validate the asset configuration for connectivity. This action logs into the device to check the connection and credentials
* **list vms**: Get the list of registered VMs
* **get system info**: Get information about a VM
* **start vm**: Start a stopped or suspended VM
* **revert vm**: Revert VM to a named snapshot if name is specified, otherwise revert to the current snapshot
* **stop vm**: Stop a VM
* **suspend vm**: Suspend a VM
* **snapshot vm**: Take a snapshot of the VM

# NMAP Scanner

<https://splunkbase.splunk.com/app/6144>

This app integrates with NMAP in order to provide detailed network information.

Supported Actions:

* **test connectivity**: Validate the asset configuration for connectivity. This action runs nmap on the IP mentioned in the configuration parameters
* **scan network**: Execute NMAP scan against a host or subnet

# Splunk IT Service Intelligence for SOAR

<https://splunkbase.splunk.com/app/6540>

This app integrates with Splunk IT Service Intelligence (ITSI) to provide operations on Splunk IT Service Intelligence episodes, services, entities, and object maintenance.

Supported Actions:

* **end maintenance window**: End Splunk ITSI maintenance window
* **update maintenance window**: Update Splunk ITSI maintenance window
* **add maintenance window**: Add Splunk ITSI maintenance window
* **get maintenance window**: Get Splunk ITSI maintenance window information
* **update service status**: Update Splunk ITSI service status
* **get service entities**: Get entities of a Splunk ITSI service
* **get service**: Get Splunk ITSI service information
* **get entity**: Get Splunk ITSI entity information
* **get episode tickets**: Get ticket information for a Splunk ITSI episode
* **add episode ticket**: Add a ticket to a Splunk ITSI episode
* **get episode events**: Get latest events for Splunk ITSI episode
* **close episode**: Close a Splunk ITSI episode
* **break episode**: Break a Splunk ITSI episode
* **add episode comment**: Add a comment to a Splunk ITSI episode
* **update episode**: Update Splunk ITSI episode status, severity and owner
* **get episode**: Get Splunk ITSI episode information
* **test connectivity**: Validate the asset configuration for connectivity using supplied configuration