Detecting the disabling of security tools

To avoid detection and ensure barrier-free operation during attacks, attackers can use tactics such as modifying the configuration of security tools or disabling them to prevent them from running.

These searches look for activity consistent with attackers attempting to disable different security mechanisms.

Required data

Endpoint data

- To complete these processes, your deployment needs to ingest data that records process activity from your hosts, and logs with both the process name and command line from your endpoints. You should also ensure you are ingesting normalized endpoint data, populating the Processes node of the Endpoint data model in the Common Information Model (CIM). For information on installing and using the CIM, see the Common Information Model documentation.
- Some commands, parameters, and field names in the searches below may need to be adjusted to match your environment. In addition, to optimize the searches shown below, you should specify an index and a time range when appropriate.

How to use Splunk software for this use case

► Sc.exe manipulating Windows services

This search looks for arguments made to sc.exe, indicating the creation or modification of a Windows service.

Using sc.exe to manipulate Windows services is uncommon. However, there may be legitimate instances of this behavior that you should validate and investigate as necessary.

```
| rename "Processes.*" AS "*"
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime)
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime)
```

► Unload Sysmon filter driver

This search looks for process fltMC.exe used to unload a Sysmon driver that will stop Sysmon from collecting data.
► Attempt to add certificate to untrusted store

This search looks for attempts to add a certificate to the untrusted certificate store.

False positives from this search might occur since there may be legitimate reasons for administrators to add a certificate to the untrusted certificate store, typically done on a large number of systems.

► Processes launching netsh

The search looks for processes spawned by netsh.exe which execute commands via the command line. Netsh can be used as a persistence proxy technique to execute a helper DLL when netsh.exe is executed.

False positives from this search might occur since some VPN applications can launch netsh.exe. Outside of these instances, it is unusual for an executable to launch netsh.exe and run commands.

Next steps
The content in this article comes from Splunk Enterprise Security (ES). As a Splunk premium security solution, ES solves a wide range of security analytics and operations use cases including continuous security monitoring, advanced threat detection, compliance, incident investigation, forensics and incident response. Splunk ES delivers an end-to-end view of an organization's security posture with flexible investigations, unmatched performance, and the most flexible deployment options offered in the cloud, on-premises, or hybrid deployment models. If you have questions about this use case, see the Security Research team's support options on GitHub.

In addition, these Splunk resources might help you understand and implement this use case:

- E-book: Ransomware, malware and cyberthreats
- Blog: Hunting with Splunk: The basics