

Release Notes

FortiSIEM 6.2.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



01/31/2024

FortiSIEM 6.2.0 Release Notes

TABLE OF CONTENTS

Change Log	4
Whats New in 6.2.0	5
New Features	5
MITRE ATT&CK Framework Support	5
Pre-computed Queries	6
Incident Remediation Workflow	6
External Authentication via SAML	6
Scale Out UEBA and State Persistence	7
Key Enhancements	7
Elasticsearch Enhancements	7
Real Time Archive for Elasticsearch	8
SVN-lite for Storing Monitored Files	8
Windows Agent 4.1 Enhancements	9
Event Forwarding from Super/Worker	9
Super Global Dashboard	9
Windows and Linux Agent Health Dashboard	10
Ability to Activate or Deactivate Multiple Rules with One Click	10
System Upgrade	10
Upgrade Overview	10
New Data Work	14
New Device Support	15
Device Support Enhancements	15
Bug Fixes and Minor Enhancements	15
Known Issues	22
Shutting Down Hardware	22
Remediation Steps for CVE-2021-44228	22
Elasticsearch	23
Elasticsearch Based Deployments Terms Query Limit	24
Public Domain Built-in Rules	25

Change Log

Date	Change Description
03/22/2021	Initial version of FortiSIEM 6.2.0 Release Notes.
12/14/2021	Added Known Issues - Remediation Steps for CVE-2021-44228 to 6.x Release Notes.
05/12/2022	Added Known Issue - Elasticsearch Based Deployments Terms Query Limit.
08/15/2022	Added Known Issue - Shutting Down Hardware.

Whats New in 6.2.0

This document describes new and enhanced features for the FortiSIEM 6.2.0 (build) release.

- [New Features](#)
- [Key Enhancements](#)
- [Upgrade Overview](#)
- [New Data Work](#)
- [New Device Support](#)
- [Device Support Enhancement](#)
- [Bug Fixes and Minor Enhancements](#)
- [Known Issues](#)
- [Public Domain Built-in Rules](#)

New Features

- [MITRE ATT&CK Framework Support](#)
- [Pre-computed Queries](#)
- [Incident Remediation Workflow](#)
- [External Authentication via SAML](#)
- [Scale Out UEBA and State Persistence](#)

MITRE ATT&CK Framework Support

The MITRE ATT&CK framework is defined as a comprehensive matrix of tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk. This release adds comprehensive support for the MITRE ATT&CK framework. The currently supported version is 0.8. This release provides the following features:

- Ability to associate a MITRE technique to a FortiSIEM (built in or custom) rule
- Over 950 built in rules to detect a wide variety of MITRE techniques
- Ability to assign techniques and tactics to Rules and search incidents by techniques and tactics
- *ATT&CK Rule Coverage* Dashboard that displays rules associated with a tactic or technique
- *ATT&CK Incident Coverage* Dashboard that displays incidents associated with a tactic or technique
- Enhanced *ATT&CK Incident Explorer* Dashboard that provides a host centric view of hosts triggering various techniques and tactics.

For information on defining a technique to a rule, see Technique in Step 3: Define Actions in [Creating a Rule](#).

For information on searching incidents by technique or tactic, see [Searching for MITRE ATT&CK Incidents](#).

For Rule Coverage Dashboard information, see [Rule Coverage View](#).

For Incident Coverage Dashboard information, see [Incident Coverage View](#).

Note: Attack View in 6.1.x, is now the [MITRE ATT&CK Incident Explorer View](#) in 6.2.x.

Pre-computed Queries

Aggregated searches with large time windows can be expensive, specially in a high EPS environment. This release enables you to set up pre-computation schedules. FortiSIEM will pre-compute search results at user specified intervals, enabling users to run faster searches against pre-computed results.

This feature was introduced for FortiSIEM EventDB in Release 5.3.3 and has been ported over to this release. In addition, pre-computation using Elasticsearch is also supported in this release using Elasticsearch Rollup functionality. For details, see [here](#).

There are two limitations for Elasticsearch based pre-computation:

1. Pre-computation is available only from the time the schedule is defined. Unlike FortiSIEM EventDB, the system does not pre-compute historical results. This limitation is a result of the Elasticsearch APIs.
2. Because Elasticsearch does roll up in a different index, pre-computation based search results may differ significantly from regular search results if the number of events matching the filter condition for the specified pre-computation interval exceeds 100K. Fortinet recommends users to first run the pre-computation query over the interval and make sure that the number of results is less than 100K.

For details on setting up pre-computed searches, see [Setting Up Pre-computation](#).

Incident Remediation Workflow

Currently, any FortiSIEM user with Write permission to the Incident page can remediate an incident by running remediation scripts. In this release, a role permission is introduced to provide finer control over a user who can remediate an incident immediately and a user who requires approval to remediate an incident. The general workflow follows:

- Full Admin users set up Incident remediation roles and users
 - Role and users who can remediate an incident, and role and users who must get approval to remediate an incident
 - Role and users who can approve incident remediation approval requests.
- A user that cannot remediate an incident can request permission to remediate.
- Once an approver approves the request, the user can then remediate the incident.

For details on setting up remediation roles, see [steps 6 and 7](#) in [Adding a New Role](#).

For details on remediating incidents using workflow, see [Creating a Remediation action](#).

For details on approver handling requests, see [Approving a de-anonymization request](#).

An example setup workflow is provided [here](#).

External Authentication via SAML

Currently, FortiSIEM users can be authenticated as (a) local authentication, (b) external authentication via Active Directory or LDAP, and (c) Single Sign On via OKTA. This release generalizes OKTA based authentication to external authentication via Security Association Markup Language (SAML).

A user must first create an External Authentication entry via SAML in FortiSIEM. If the SAML Identity Provider provides Role information, the user has to map the SAML Role to the FortiSIEM Role. Otherwise, the user has to manually define the FortiSIEM Role for SAML users. A role is required for a user to be able to log in to FortiSIEM.

For details, see [Configuring FortiSIEM for SAML Overview](#).

Scale Out UEBA and State Persistence

This release adds two enhancements.

- Scale out design - The AI module now runs on Super and Worker nodes. All Agent activity is routed to one node in a sticky manner. If a Worker is down, Agent events are routed to another Worker. If a Worker is added, then new Agents are routed to that Worker.
- Persistence – AI models are now persisted across AI module restarts.

For information on setting up UEBA, see [here](#).

Key Enhancements

- [Elasticsearch Enhancements](#)
- [Real Time Archive for Elasticsearch](#)
- [SVN-lite for Storing Monitored Files](#)
- [Windows Agent 4.1 Enhancements](#)
- [Event Forwarding from Super/Worker](#)
- [Super Global Dashboard](#)
- [Windows and Linux Agent Health Dashboard](#)
- [Ability to Activate or Deactivate Multiple Rules with One Click](#)
- [System Upgrade](#)

Elasticsearch Enhancements

This release adds the following enhancements to FortiSIEM Elasticsearch support.

- Support for Elastic Cloud
- Support for Elasticsearch version 7.8. - See the [Elasticsearch table](#) for version support in each deployment.
- Support for Cold Data Node – in this node, indices are frozen and saved to disk, thereby saving heap memory. Data can be moved from Hot to Warm to Cold data nodes, either based on disk space, or time duration using the Elasticsearch index lifecycle management (ILM) feature. This allows more event storage in Cold Data Nodes since the heap memory constraint is eliminated. Regardless of the node type, events can be queried wherever they reside. When a query hits Cold nodes, further queries run a bit slower since the indices have to be loaded to memory. This feature is not available on AWS Elasticsearch Service and Elastic Cloud. General workflow information is available [here](#).
- Age based Retention/Index Lifecycle Management (ILM) – in earlier releases, disk thresholds could be specified to determine when data would move from Hot to Cold node. In this release, the number of days can be specified for each data node type. FortiSIEM will move data from Hot to Warm to Cold based on space thresholds or time

duration limit, whichever occurs first. This feature is not available on AWS Elasticsearch Service and Elastic Cloud. Retention configuration details are available [here](#). Default setting information is available [here](#).

- Queries with multi-field term aggregation is now sorted. For example, when the Group By and Display Fields option is used for "Reporting IP" and "Reporting Device" using "COUNT(Matched Events)" in descending (DESC) order, the count appears in descending order.
- Support for Java Transport Client API is removed.
- With Elasticsearch 7.x, the index refresh rate is reduced to 15 seconds. This enables users to search all data, except for the last 15 seconds. Choosing an even lower index refresh rate may lower the event indexing speed.

There are 3 distinct Elasticsearch deployments. This table shows the versions and features supported for each deployment type. Please also see the list of Elasticsearch related known issues in [Known Issues](#) and in the [Appendix](#).

Elasticsearch Deployment	Supported Versions	API (Insertion and Search)	Supported Data Node Types	Disk Space based Retention	Age based retention (ILM)
Self-Managed (On-Prem or Hosted)	5.6, 6.4, 6.8, 7.8	REST	Hot, Warm, Cold	Yes	Yes (6.8 and above)
AWS Elasticsearch Service	6.8, 7.8	REST	N/A	Yes	No
Elastic Cloud	6.8	REST	N/A	Yes	No

Real Time Archive for Elasticsearch

For Elasticsearch deployments, users can choose NFS or HDFS as Archive. Currently, when Elasticsearch disk space capacity is close to full, events are read from Elasticsearch and then archived to NFS or HDFS. For high EPS scenarios, this can be a very expensive operation and may impact Elasticsearch cluster performance.

In this release, users can choose to store events to both Elasticsearch and Archive (NFS or HDFS) in parallel, when the event arrives to FortiSIEM. Events are stored in two stores at the same time, but this reduces the need to archive when Elasticsearch disk space is full or Index Life-cycle Management (ILM) policies kick in. At that time, data is simply purged from Elasticsearch, which is an inexpensive operation.

For details on how to set up Real time Archive for Elasticsearch, see [Setting Up the Database \(NFS\)](#) or [Setting Up the Database \(HDFS\)](#).

SVN-lite for Storing Monitored Files

FortiSIEM can detect file changes in network devices and servers. In earlier releases, these files were stored in SVN. Since SVN stores incremental changes, older files could not be deleted, even when the device is deleted.

In this release, a new [SVN-lite service is introduced to manage files](#). From a user perspective, there is no change except that a user is able to delete files from the GUI. Files are also automatically deleted when a device is deleted. When upgrading from earlier releases to 6.2.0, older files are migrated from SVN to SVN-lite format.

For details on where you can delete files, see the [table](#) in [Viewing Device Information](#).

A few implementation notes:

- Files are stored in `/svn/repos`. Files are organized by `ordId` and then `deviceId`. `deviceId` is the PostgreSQL Device Id. To conserve disk space, a limited number of file revisions are kept based on the following thresholds defined in `/opt/phoenix/config/svn-lite.properties` on the Supervisor node.

```
svn-lite.store.dir = /svn/repos
svn-lite.revisions.keep = 100
svn-lite.revisions.purge = 5
```

`svn-lite.revisions.keep` defines how many revisions are kept for each file. Older revisions are automatically deleted. `svn-lite.revisions.purge` defines how many files are deleted at a time when the upper limit of `svn-lite.revisions.keep` is reached.

- During a 6.2.0 upgrade, up to 100 revisions of each file are migrated to SVN-lite.

Windows Agent 4.1 Enhancements

This release adds the following enhancements for Windows Agent.

- Agent will restart automatically after 1 minute if it is killed. See [here](#).
- Service protection – A user cannot Stop/Restart/Pause the agent from Service Manager. See [here](#).
- Users can change the logging level without restarting service by changing the registry key. See [here](#) for more information. Registry key instructions follow:
 - Open `HKEY_LOCAL_MACHINE\SOFTWARE\AccelOps\Agent` key
 - To update with trace logging, modify “**LogLevel**” value to “2” from “1”.
 - To update with debug logging, modify “**LogLevel**” value to “1” from “2”.
- The Agent Database is used to store Agent configuration parameters and to store events when connectivity to collectors is lost. The default size for your Agent Database is 1GB. This can be changed by modifying the `MaxDBSizeInMB` entry in your Registry Editor. See [here](#) for more information.

Details are documented in [Configuring Windows Agent](#).

Event Forwarding from Super/Worker

FortiSIEM can forward the events it receives to a third party system. Normally, events are forwarded by the node (Worker, Collector, Super) that parsed the event. This release allows you to force events to only be forwarded by Workers (and Super). Users can choose this as part of their Event Forwarding policy, see [here](#).

Super Global Dashboard

This release adds the concept of a Super Global dashboard that is only available for Super Global users in service provider installations. All regular dashboards are now only available as Organization level. Super Global users can define their own dashboards that are only visible for Super Global users.

Windows and Linux Agent Health Dashboard

This release provides a separate health dashboard for FortiSIEM agents. See **ADMIN > Health > Agent Health**. For details, see [here](#).

Note: If you've upgraded your FortiSIEM to 6.2.0 from an older version, the dashboard will show an inaccurate agent version, or no version. You will need to re-install your agents with a new version after upgrading FortiSIEM to 6.2.0 to resolve this issue. If an old version is installed for an agent, the dashboard will still show no version or an inaccurate version for that agent. See [Linux](#) and/or [Windows Agent](#) guides for uninstall and installation steps. Upgrading your collectors to 6.2.0 is recommended (please see the FortiSIEM Version Compatibility Matrix for details).

Ability to Activate or Deactivate Multiple Rules with One Click

Users often need to activate or deactivate all rules in one folder, and could only perform this action on individual rules. This release enables users to activate or deactivate multiple rules in one click.

For details, see [Activating/Deactivating Multiple Rules](#).

System Upgrade

This release includes several third party software upgrades - CentOS 8.3, PostgreSQL 13.2, Glassfish 5.0, JDK 1.8.0_272, php 7.4, nodejs 14.15.0, Hibernate 5, and Apache 2.4.37 (patched by Redhat).

Upgrade Overview

For software installations, the upgrade path is pre-5.3.0->5.4.0->6.1.1->6.2.0.

Specifically:

- From pre-5.3.0 releases, first upgrade to 5.4.0, then migrate to 6.1.1, and then upgrade to 6.2.0.
- From 5.4.0, migrate to 6.1.1, and then upgrade to 6.2.0.
- If you are running 6.1.0, 6.1.1, or 6.1.2, then upgrade to 6.2.0.

For hardware installations, 6.1.1 is not available, so the migration path is pre-5.3.0->5.4.0->6.1.2->6.2.0.

Specifically:

- From pre-5.3.0 releases, first upgrade to 5.4.0, then migrate to 6.1.2, and then upgrade to 6.2.0.
- From 5.4.0, migrate to 6.1.2, and then upgrade to 6.2.0.
- If you are running 6.1.2, then upgrade to 6.2.0.

These steps are documented in detail in the [Upgrade Guide](#).

Points to consider before upgrade:

1. For your Supervisor and Worker, do not use the upgrade menu item in configFSM.sh to upgrade from 6.1.x to 6.2.0. This is deprecated, so it will not work. Use the new method as instructed in the [Upgrade Guide](#).
2. The 6.2.0 upgrade will attempt to migrate existing SVN files (stored in `/svn`) from the old svn format to the new svn-lite format. During this process, it will first export `/svn` to `/opt` and then import them back to `/svn` in the new svn-lite format. If your `/svn` uses a large amount of disk space, and `/opt` does not have enough disk space left, then migration will fail. Fortinet recommends doing the following steps before upgrading:

- Check /svn usage
- Check if there is enough disk space left in /opt to accommodate /svn
- Expand /opt by the size of /svn
- Begin upgrade

Steps for expanding /opt disk:

- Go to the Hypervisor and increase the /opt disk by the size of /svn disk
- # ssh into the supervisor as root
- # lsblk

```
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
...
sdb                  8:16    0 100G  0 disk                << old size
└─sdb1                8:17    0 22.4G  0 part [SWAP]
└─sdb2                8:18    0 68.9G  0 part /opt
...
```

- # yum -y install cloud-utils-growpart gdisk
- # growpart /dev/sdb 2
CHANGED: partition=2 start=50782208 old: size=144529408 end=195311616 new:
size=473505759 end=524287967
- # lsblk

Changed the size to 250GB for example:

```
#lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
...
sdb                  8:16    0 250G  0 disk                <<< NOTE the new size for the disk in
/opt
└─sdb1                8:17    0 22.4G  0 part [SWAP]
└─sdb2                8:18    0 68.9G  0 part /opt
...
```

- # xfs_growfs /dev/sdb2

```
meta-data=/dev/sdb2          isize=512    agcount=4, agsize=4516544 blks
      =                       sectsz=512    attr=2, projid32bit=1
      =                       crc=1        finobt=1, sparse=1, rmapbt=0
      =                       reflink=1
data      =                   bsize=4096    blocks=18066176, imaxpct=25
      =                       sunit=0      swidth=0 blks
naming    =version 2          bsize=4096    ascii-ci=0, ftype=1
log       =internal log      bsize=4096    blocks=8821, version=2
      =                       sectsz=512    sunit=0 blks, lazy-count=1
realtime  =none              extsz=4096    blocks=0, rtextents=0
data blocks changed from 18066176 to 59188219
```

- # df -hz

```
Filesystem            Size  Used Avail Use% Mounted on
...
/dev/sdb2              226G  6.1G  220G   3% / << NOTE the new disk size
```

- If you are using AWS Elasticsearch, then after upgrading to 6.2.0, take the following steps:

- Go to **ADMIN > Setup > Storage> Online**.
- Select "ES-type" and re-enter the credential.

4. In 6.1.x releases, new 5.x collectors could not register to the Supervisor. This restriction has been removed in 6.2.0 so long as the Supervisor is running in non-FIPS mode. However, 5.x collectors are not recommended since CentOS 6 has been declared End of Life.
5. If you have more than 5 Workers, Fortinet recommends using at least 16 vCPU for the Supervisor and to increase the number of notification threads for RuleMaster. To do this, SSH to the Supervisor and take the following steps:
 - a. Modify the `phoenix_config.txt` file, located at `/opt/phoenix/config/` with


```
#notification will open threads to accept connections
#FSM upgrade preserves customer changes to the parameter value
#notification_server_thread_num=50
```

Note: The default `notification_server_thread_num` is 20.
 - b. Restart `phRuleMaster`.
6. Upgrading Elasticsearch Transport Client usage - The Transport Client option has been removed as Elasticsearch no longer supports that client. If you are using Transport Client in pre-6.2.0, you will need to modify the existing URL by adding "http://" or "https://" in front of the **URL** field after upgrading, as displayed in **ADMIN > Setup > Storage > Online** > with **Elasticsearch** selected, as shown here.
 - a. Before Upgrade, Elasticsearch appears as:

Elasticsearch

Client: ☒ Java Transport ☐ Rest API

Cluster Name:

Cluster: ☒ IP ☐ Host

HTTP Port: Java Port:

User Name:

Password:

Shard Allocation: ☒ Fixed ☐ Dynamic

Shards:

Replicas:

Per Org Index ☐

- b. After Upgrade: Elasticsearch appears as:

☒ Elasticsearch

URL:

Port:

ES Service Type: ☒ Native ☐ Amazon ☐ Elastic Cloud

User Name:

Password:

Confirm Password:

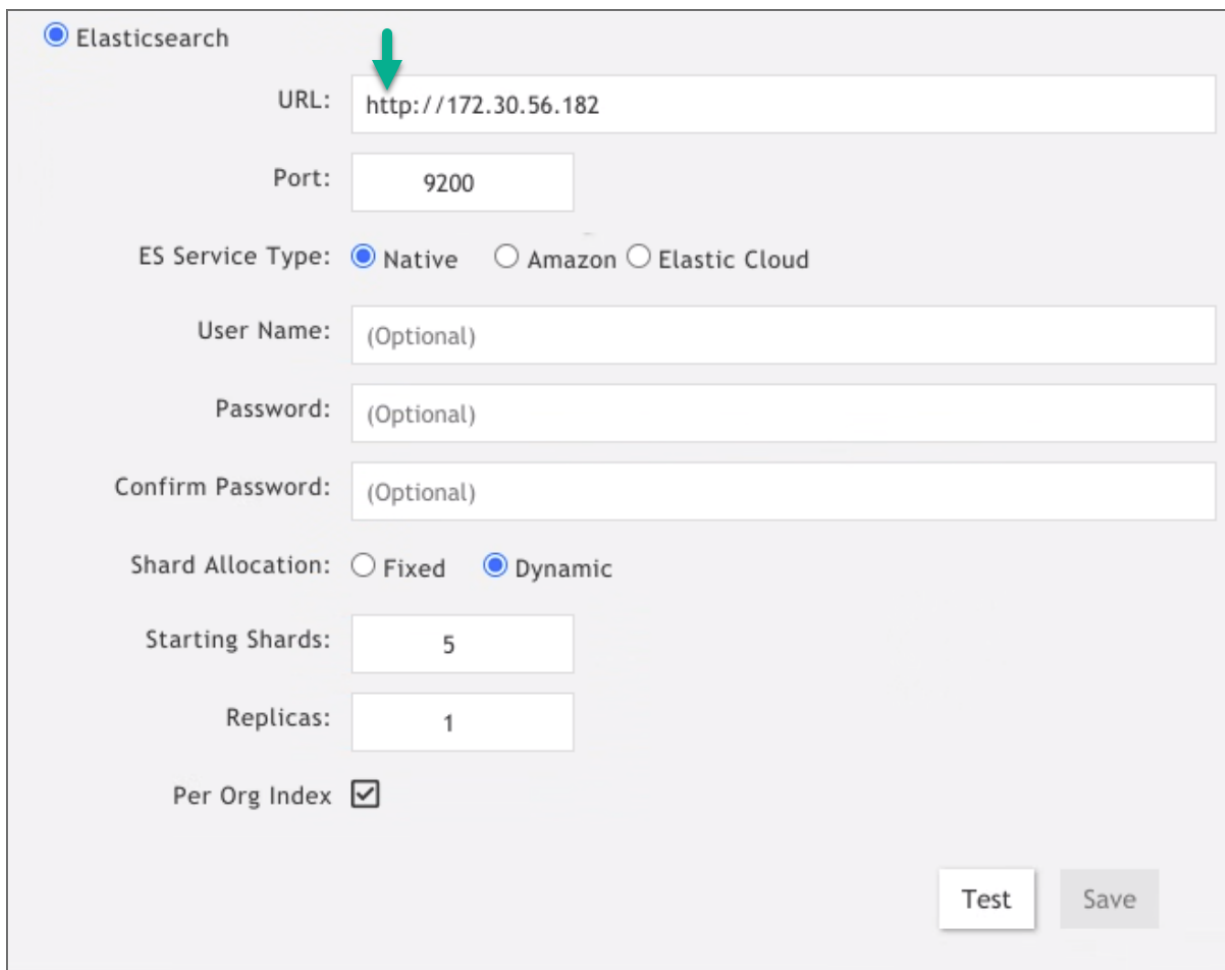
Shard Allocation: ☐ Fixed ☒ Dynamic

Starting Shards:

Replicas:

Per Org Index ☒

- c. In the **URL** field, add "http://" or "https://" to your IP address. Next, select Test to confirm functionality, and select Save to save the updated settings.



The screenshot shows the Elasticsearch configuration interface. At the top, the 'Elasticsearch' radio button is selected. Below it, the 'URL' field contains 'http://172.30.56.182' and is highlighted with a green arrow. The 'Port' field is set to '9200'. Under 'ES Service Type', the 'Native' radio button is selected, with 'Amazon' and 'Elastic Cloud' as options. The 'User Name' and 'Password' fields are marked as '(Optional)'. The 'Confirm Password' field is also marked as '(Optional)'. For 'Shard Allocation', the 'Dynamic' radio button is selected, with 'Fixed' as an alternative. The 'Starting Shards' field is set to '5' and the 'Replicas' field is set to '1'. The 'Per Org Index' checkbox is checked. At the bottom right, there are 'Test' and 'Save' buttons.

7. Prior to upgrading, ensure that hot node and warm node counts are both greater than the number of replicas. Failure to do so will result in Test and Save operation failure after an upgrade. This basic requirement check has been added for version 6.2.0 and later.
8. Remember to remove the browser cache after logging on to the 6.2.0 GUI and before doing any operations.

New Data Work

- Added OT/IoT Rules, Reports and Dashboard.
- Added New Compliance Report - [Center for Internet Security \(CIS\) Controls](#).
- Added [615 new rules](#) and [206 new reports](#) to cover MITRE ATT&CK Tactics and Techniques. Many of the rules are adopted from public domain SIGMA Rules. See [here](#) for details.
- Existing rules mapped to MITRE ATT&CK Tactics and Techniques where applicable.
- Added Rules and Reports for Hafnium Exchange Server attack and Solarwinds Sunburst attack.

New Device Support

The following device support has been added.

- Malwarebytes Breach Detection
- Dragos OT Platform
- Oracle CASB
- Claroty
- Corero Smartwall Threat Defense System (TDS)
- Proofpoint

Device Support Enhancements

- CrowdStrike integration using OAuth2 API
- The following parsers have been updated.
Windows: Security, Sysmon and DNS, FortiGate, FortiEDR, FortiMail, FortiDeceptor, FortiADC, FortiWeb, AWS security Hub, Sourcefire, Office365, F5BigIP, Sentinel One, Tipping Point NMS, AWS Kinesis, CiscoFTDParser, Sophos XG, Bluecoat Proxy SG Device, and Tigera Calico.

Bug Fixes and Minor Enhancements

The current release includes the following bug fixes and minor enhancements:

Bug ID	Severity	Module	Description
656383	Major	App Server	Malware Hash import from a CSV file fails when the CSV file contains 75,000 or more Malware Hash entries.
684128	Major	App Server	Scheduled bundle reports fail after migration.
655781	Major	App Server	Update Malware Hash via API does not work as expected, producing "duplicate" errors.
624133	Major	App Server	Cisco Meraki log discovery does not add devices to CMDB.
695082	Major	GUI	FortiSIEM does not recognize a UEBA perpetual license, so users with a UEBA perpetual license are unable to add UEBA for their devices.
694897	Major	Inline Report Engine	For Elasticsearch cases with inline report mode set to 2, the ReportMaster memory may grow quickly.

Bug ID	Severity	Module	Description
701383	Major	Java Query Server	The Java Query Server has a file descriptor leak which may cause a loss of connection to the Elasticsearch Coordinating node.
682751	Major	Query Engine	Malware IP, Domain, and URL Group lookup performance slower than expected.
670053	Major	Rule Engine	Security incidents always indicate "System Cleared" after 24 hours, even if <code>auto_clear_security_incidents=0</code> is set.
676614	Major	Rule Engine	SSL communication sockets between rule worker and rule master are not always closed properly, leading to rules not triggering.
589656	Major	Rule Engine	Rules with a pattern-based clearing condition do not always clear even if the condition is met. This is because the clear rule's time window is sometimes read incorrectly.
645987	Minor	App Server	Scheduled CSV formatted report finishes, but is never received by a user if the "do not send scheduled email if report is empty" flag is set.
679164	Minor	App Server	Incident subcategory names are incorrectly displayed in PDF export.
668989	Minor	App Server	STIX/Taxii Integration does not work for certain websites.
671564	Minor	App Server	An empty value of Source Interface SNMP Index in Report Result causes App Server to throw <code>NullPointerException</code> when parsing it.
683528	Minor	App Server	After Java starts up, rule exceptions with watchlists do not take effect.
685100	Minor	App Server	Logs are unnecessarily pulled from unmanaged devices, and then dropped. This sometimes causes event pulling to lag behind.
658886	Minor	App Server	Identity and Location Tables show data from a different organization when enriched (no collector environment).
678695	Minor	App Server	An error is thrown when a user navigates to CMDB > Business Services > IT Srvs > Select the Service > Edit > Device/Application > User App .
658755	Minor	App Server	Rule exceptions do not work for Source User in LDAP group.
682184	Minor	App Server	In rare circumstances, different incidents with identical incident IDs are created.
661353	Minor	App Server	The rule test function does not work. Note: This was due to an issue when updating a rule definition or conditions.

Bug ID	Severity	Module	Description
672285	Minor	App Server	After configuring important interfaces, if the device's hostname is changed, the modification for the name change /merge does not trickle down into the important interface table.
671376	Minor	App Server	From incident notification emails, links to a specific FortiSIEM incident in the FortiSIEM GUI do not work.
674077	Minor	App Server	Sophos Central Credential Configuration shows orgs with collectors in drop-down list.
639827	Minor	App Server	The event <code>PH_DEV_MON_LOG_DEVICE_DELAY_HIGH</code> is not generated correctly in accordance with the thresholds defined.
670750	Minor	App Server	Data leak issue occurs on rule exceptions in Analytic Search Results against CMDB Rules. When running a query using CMDB Attributes and choosing a target RULE, the user can see the exception condition from the query result from org 1 while running a report at a different org (org 2).
662400	Minor	App Server	Excessive <code>PH_APPSERVER_INCIDENT_UPDATE_FAILED</code> errors occur for user names longer than 255 characters.
676038	Minor	App Server	Initial load of Redis had performance issues. This required a check against loading active inline reports with missing query ID to resolve the issue.
648730	Minor	App Server	Remediation pop up populates the "Enforce on" field with incorrect values.
672934	Minor	App Server	Cloning a rule does not copy the Watchlist Entry from the original rule.
611553	Minor	App Server	Accounts that cannot edit rules can see rule definitions in the Incidents page.
609289	Minor	App Server	API query for monitor/critical interfaces does not give correct information.
602340	Minor	App Server	LDAP/AD discovery causes a user to be removed from custom user groups.
639397	Minor	App Server	The GUI shows a negative unused device count in org if device provisioning is changed after an initial provisioning.
597456	Minor	App Server	For orgs without collectors, virtual IP entries do not prevent devices from merging.
608133	Minor	App Server	In CMDB Report Results, the "App Group Name" appears empty, even if an application is defined against a device.
659853	Minor	App Server	FortiSIEM SNMP TRAP output has a duplicate field (<code>iso.3.6.1.4.1.35409.101.5.0</code>).

Bug ID	Severity	Module	Description
659028	Minor	App Server	When importing a CSV file with Malware Hash, a "Full" data update does not work as expected.
630329	Minor	App Server	Radius External Authentication fails due to shared secret not getting updated in the database.
645660	Minor	App Server	From the Identity and Location Dashboard, when exporting a PDF report, the filter parameters are ignored while the report is generated.
618475	Minor	App Server	The Incident Group (e.g. Security, Availability, etc.) is missing in the exported rule XML file.
653427	Minor	App Server	Exporting a custom watchlist to CSV format fails. Note: Exporting a custom watchlist to PDF works fine.
696873	Minor	App Server	Clean up of expired watch list entries occur at 2:00 am of each day. Clean up must occur hourly.
670247	Minor	Data	Syslog from Meraki AP are miscategorized as Meraki Firewall.
672320	Minor	Data	The Incident Title is incorrect for some rules.
673177	Minor	Data	Many built-in AWS Security Hub Events reports are missing Group BY attributes.
661691	Minor	Data	"Excessive End User Mail" and "Excessive End User Mail To Unauthorized Mail Gateways" rules are generating false positive for UDP protocol. Fixed with AddTCP restriction to the two rules.
645659	Minor	Data	The Netflow/Sflow Parser does not parse Link Aggregation Control Protocol (LACP) counter sample.
658760	Minor	Data	The Windows Agent DNS Parser parses incorrectly in a few scenarios.
658990	Minor	Data	PAN OS VPN LOGIN Events are categorized under DEVICE Logon success / failed when they should be classified as VPN Logon success / failure events.
670672	Minor	Data	Tenable integration (vulnerability scanning) needs to parse more attributes, specifically CVSS Score, OS, SCSS3 Base Score, and Vulnerability Priority Rating (VPR).
686051	Minor	Discovery	When attempting to import over 200 users using a CVS file for Okta integration, the operation fails, and no errors appear in the log.
660690	Minor	GUI	When trying to display interfaces on a dashboard, the dashboard freezes when there are more than 10K interfaces for a device.
671868	Minor	GUI	In an Incident Notification policy, sometimes selected a rule or affected items are not saved.

Bug ID	Severity	Module	Description
669876	Minor	GUI	In ADMIN > Health > Collector Health > Tunnels , the “Close Tunnel” button is always inaccessible (grayed out).
617943	Minor	GUI	Removing a value from a customize device property does not reset the property to "Undefined".
663653	Minor	GUI	The Parser test fails when a regex pattern and regex tags are on different lines.
645657	Minor	GUI	Unable to sort incidents when multiple categories are selected.
655536	Minor	GUI	Email subject and rawEvents tag does not appear in the email preview pop up.
647709	Minor	GUI	In Incident Search, filter by category "Security" does not capture new Incidents without a refresh.
659851	Minor	GUI	After saving discovery entries, the list reloads and resets to the first discovery page.
604148	Minor	GUI	Integration Policy > Org Mapping , located by navigating to ADMIN > Settings > External Integration clicking New and Organization Mapping, does not handle special characters.
624771	Minor	GUI	When editing an Event Organization (ADMIN > Settings > Event Handling > Event Org Mapping), two save and two cancel buttons appear.
653753	Minor	GUI	The Identity & Location Dashboard does not refresh with the correct information.
592961	Minor	GUI	The Dashboard single line widget shows a needle below the chart graphic if stretched too long.
637722	Minor	GUI	Importing a watchlist while in Organization fails.
607810	Minor	GUI	Editing an interface forces the user to enter an IP address, even if the interface did not have one originally.
647105	Minor	GUI	In Notification Policy, the seconds and time zone region are not saved.
644186	Minor	GUI	If the user goes to the INCIDENTS > List by Time view, selects an incident, navigates to another page, and returns to the Incidents page, the selected incident position is lost.
626043	Minor	GUI	The user is logged out before the log off expiration time period elapses.
683801	Minor	Java Query Server	Elastic Search Cluster disconnects from FortiSIEM once a week.
661333	Minor	Java Query Server	Analytic search fails to retrieve the Destination and Source TCP/IP Port value from Elastic search index.

Bug ID	Severity	Module	Description
659018	Minor	Java Query Server	Elasticsearch insert sometimes fails when a raw message contains non UTF-8 characters.
698147	Minor	Java Query Server (Elasticsearch)	The Java Query Server does not properly close sockets in all cases, which can lead to its inability to communicate with the App Server.
592607	Minor	Parser	EPS Usage per node is higher than the global Used EPS.
676294	Minor	Parser	Office365 GCC High Authentication does not work due to hard coded URLs.
669837	Minor	Parser	Event Type comparison in Drop Rule needs to be case insensitive.
659180	Minor	Parser	Sometimes, excessive collector time skew is generated when the App Server is busy. This occurs when phMonitor on Collector mistakenly caches a timestamp when failing to communicate with the App Server.
670324	Minor	Parser	For Service Provider Install, the Org name in Events is not the same as the Org Association in the Credential page.
648732	Minor	Parser	AD/LDAP user details metadata is not always added to incidents.
662899	Minor	Parser	The Test Parser function with <code>resolveDNSName</code> does not work when DNS lookup is enabled.
635113	Minor	Parser	The Windows Parser sometimes adds reporting device metadata from DNS lookup instead of reporting it from another event.
637631	Minor	Query Engine	When you export (CSV format) from a date before a Daylight Saving Time change when Daylight Saving Time has occurred, a difference of one hour is observed.
670060	Minor	Rule Engine	Incident Exceptions do not work when time period exceptions are set for Monday and Friday.
657601	Minor	System	In <code>phoenix_config.txt</code> , the setting <code>http_client_verify_peer=no</code> changes to <code>yes</code> upon upgrade.
658491	Minor	System	After an Archive configuration has been set up (NFS/HDFS), ADMIN > Setup > Storage > Archive , the user is unable to clear and remove the archive from the GUI.
577821	Minor	System	In Cloud Health, workers and super always incorrectly report 100% CPU utilization.
696873	Minor	Windows Agent	After Windows Agent 4.0.0 installation, an unnecessary system reboot may occur.
607443	Enhancement	App Server	LAST (Event Receive Time) is shown in Epoch Time format for PDF export in Elastic Storage setup.

Bug ID	Severity	Module	Description
627546	Enhancement	App Server	The Incident Notification Email link needs to have Super FQDN in addition to IP.
609102	Enhancement	App Server	The PDF Report does not display Incident category name.
649588	Enhancement	App Server	Custom Device Properties cannot be queried via CMDB Report.
580110	Enhancement	App Server	In CMDB > CMDB Report , add a scope attribute to display whether a property is either system or user defined.
611929	Enhancement	Data	Enhance the Cisco Meraki Parser to handle Air Marshall events.
670414	Enhancement	Data	The CloudTrail Parser does not parse the User and User Type for event type = AWS-CloudTrail-SIGNIN-ConsoleLogin-Success.
661692	Enhancement	Data	Event Type Categorization is inconsistent for ipsec/VPN log off.
669102	Enhancement	Data	The Unix Parser doesn't handle the user attribute when the rhost field is a hostname, and not an IP.
653421	Enhancement	Data	The "Multiple admin Login Failure" rule name should be renamed as there is no indicator of admin role usage.
530467	Enhancement	Data	FortiSIEM does not detect certain event SSH/Audit events using the Unix Parser.
660734	Enhancement	Data	The Aruba Parser does not parse Event Name and causes high CPU usage.
625194	Enhancement	Data	Enhance the Windows OS Parser update to pass terminal services logs.
652184	Enhancement	Data	Support the Unix Parser with a new timestamp format.
649496	Enhancement	Data	Enhance the Windows Parser fix for Alternate UPN domain suffix support.
624070	Enhancement	Data	Parse the Cisco ASA-722051 event ID.
650998	Enhancement	Discovery	Enhance AD discovery to import Manager field if it is populated in AD.
663218	Enhancement	GUI	User input for the Report Design Cover Page is not clear. This should be improved.
673543	Enhancement	GUI	There is no user input validation in Rule Exception definition. Input validation should be implemented for Rule Exceptions.
515571	Enhancement	GUI	HourOfDay(Event Receive Time) BETWEEN / NOT BETWEEN should be supported.
611518	Enhancement	GUI	For Rule Exception, the user cannot define more than 7 time period schedules. The user should be able to define more than 7 time period schedules.

Bug ID	Severity	Module	Description
670230	Enhancement	Parser	The Event Forwarder needs to retry forwarding events if it encounters a network connection.
642389	Enhancement	Parser	Parser: compare function needs to be extended to support >= and <= operators.
586569	Enhancement	System	Monitor Raid Health should be added for 3500F and 2000F HW appliances.

Known Issues

Shutting Down Hardware

On hardware appliances running FortiSIEM 6.6.0 or earlier, FortiSIEM `execute shutdown` CLI does not work correctly. Please use the Linux `shutdown` command instead.

Remediation Steps for CVE-2021-44228

Three FortiSIEM modules (SVNLite, phFortInsightAI and 3rd party ThreatConnect SDK) use Apache log4j version 2.14, 2.13 and 2.8 respectively for logging purposes, and hence are vulnerable to the recently discovered Remote Code Execution vulnerability ([CVE-2021-44228](#)).

These instructions specify the steps needed to mitigate this vulnerability without upgrading Apache log4j to the latest stable version 2.16 or higher. Actions need to be taken on the [Supervisor](#) and [Worker](#) nodes only.

On Supervisor Node

1. Logon via SSH as root.
2. Mitigating SVNLite module:
 - a. Run the script `fix-svn-lite-log4j2.sh` ([here](#)). It will restart SVNlite module with `Dlog4j2.formatMsgNoLookups=true` option and print the success/failed status.
3. Mitigating 3rd party ThreatConnect SDK module:
 - a. Delete these log4j jar files under `/opt/glassfish/domains/domain1/applications/phoenix/lib`
 - i. `log4j-core-2.8.2.jar`
 - ii. `log4j-api-2.8.2.jar`
 - iii. `log4j-slf4j-impl-2.6.1.jar`
4. Mitigating phFortInsightAI module:
 - a. Delete these log4j jar files under `/opt/fortiinsight-ai/lib/`
 - i. `log4j-core-2.13.0.jar`
 - ii. `log4j-api-2.13.0.jar`
5. Restart all Java Processes by running: `"killall -9 java"`

On Worker Node

1. Logon via SSH as root.
2. Mitigating phFortiInsightAI module:
 - a. Delete these log4j jar files under `/opt/fortiinsight-ai/lib/`
 - i. `log4j-core-2.13.0.jar`
 - ii. `log4j-api-2.13.0.jar`
3. Restart all Java Processes by running: `"killall -9 java"`

Elasticsearch

1. With pre-compute queries via Rollup, sorting on `AVG()` is not supported by Elasticsearch. See [here](#).
2. Elasticsearch pre-compute is done using the Elasticsearch Rollup API, which requires raw events matching the pre-compute search condition be populated into a separate Elasticsearch index. This operation can become expensive if a large number of events match the pre-compute search filter condition. Fortinet recommends that the user set up a report for pre-compute only if the search filter conditions for the pre-compute interval result in less than 100K entries. This allows the pre-computed result to exactly match the adhoc report for faster operation. Specifically, follow these steps:
 - a. Suppose you want to run a report in pre-compute mode, with the operation running pre-computations hourly. This means the report will be run hourly, and when a user runs for a longer interval, the pre-computed results would be combined to generate the final result.
 - b. Check for pre-compute eligibility.
 - i. Run the report in adhoc mode for 1 hour by removing group by conditions.
 - ii. If the number of rows is less than 100K, then the original report is a candidate for pre-computation. **Note:** This is for Elasticsearch only. If the number of results in #Bii is more than 100K, then the pre-computed results and adhoc results will be different since FortiSIEM caps the number of results retrieved via Rollup API to be less than 100K.
3. AWS Managed Elasticsearch 7.x limits `search.max_buckets` to 10K. In 6.8 there was no such limit. This may cause Elasticsearch to throw an exception and not return results for aggregated queries. Contact AWS Managed Elasticsearch Support to increase `search.max_buckets` to a large value (recommended 10M). There is an API to change this value, but this does not work in AWS Managed Elasticsearch. Therefore you must contact AWS Managed Elasticsearch Support before running queries.
 - a. For general discussion about `search.max_buckets`, see [here](#).
 - b. For general discussion about this issue, see [here](#).
 - c. Elasticsearch does not consistently handle sorting functions when there are NULL values. For example:
 - i. `AVG()`: NULL values are at the bottom.
 - ii. `MIN()`: NULL values are considered to be the largest value possible, so if you choose ASC (respectively DESC) order, NULL values appear at the bottom (respectively top).
 - iii. `MAX()`: NULL values are considered to be the smallest value possible, so if you choose ASC (respectively DESC) order, NULL values appear at the top (respectively bottom).
4. Pre-compute queries do not work with the `HAVING` clause. Currently, the FortiSIEM GUI is preventing this operation. For public discussion about Rollup search and query scripts, see [here](#).
5. The `HourOfDay(Event Receive Time)` and `DayOfWeek(Event Receive Time)` calculations are incorrect if Elasticsearch and Supervisor are in different time zones.
6. In Elasticsearch, a non-aggregated query spanning multiple display pages requires 1 open scroll context per shard. This enables the user to visit multiple pages and see the results. Elasticsearch has a (configurable) limit on open

scroll contexts. This is defined in `phoenix_config.txt` on the Supervisor node. By default, FortiSIEM limits to 1000 open scroll contexts and each context remains open for 60 seconds, as shown.

```
[BEGIN Elasticsearch]
```

```
...
```

```
max_open_scroll_context=1000
```

```
scroll_timeout=60000
```

```
...
```

```
[END Elasticsearch]
```

When the open scroll context limit is reached, Elasticsearch throws an exception and returns partial results. When 80% of the search context limit is reached, FortiSIEM writes a log in `/opt/phoenix/log/javaQueryServer.log`, as shown.

```
com.accelops.elastic.server.task.ChoresTask - [PH_JAVA_QUERYSERVER_WARN]:
[eventSeverity]=PHL_WARNING, [phEventCategory]=3, [procName]=javaQueryServer,
[phLogDetail]=node=node236, openContexts=1000, it has 80 percent of available
search contexts open
```

- You can increase `max_open_scroll_context`. However, AWS Elasticsearch does not allow more than 500 open scroll contexts, and will enforce a 500 limit. Be careful in choosing very high `max_open_scroll_context`. It is strongly recommended to use a test instance to experiment with your number prior to production.
- After changing `max_open_scroll_context`, you need to apply Test & Save from the GUI for changes to take effect. This is because `max_open_scroll_context` is a cluster level setting.
- You can change `scroll_timeout`, but after changing this value, you must restart the Java Query Server on the Supervisor for the change to take effect.

For Elasticsearch discussion forum information on this topic, see [here](#).

7. The maximum number of group by query result is 2,000 by default. You can change the setting in `phoenix_config.txt` on the Supervisor node by taking the following steps.
 - a. Change the setting: `aggregation_size=2000`
 - b. Restart the JavaQueryServer.

Elasticsearch Based Deployments Terms Query Limit

In Elasticsearch based deployments, queries containing "IN Group X" are handled using Elastic Terms Query. By default, the maximum number of terms that can be used in a Terms Query is set to 65,536. If a Group contains more than 65,536 entries, the query will fail.

The workaround is to change the "max_terms_count" setting for each event index. Fortinet has tested up to 1 million entries. The query response time will be proportional to the size of the group.

Case 1. For already existing indices, issue the REST API call to update the setting

```
PUT fortisiem-event-*/_settings
{
  "index" : {
    "max_terms_count" : "1000000"
```



```
}
}
```

Case 2. For new indices that are going to be created in the future, update fortisiem-event-template so those new indices will have a higher max_terms_count setting

1. `cd /opt/phoenix/config/elastic/7.7`
2. Add `"index.max_terms_count": 1000000` (including quotations) to the "settings" section of the `fortisiem-event-template`.

Example:

...

```
"settings": {
  "index.max_terms_count": 1000000,
```

...

3. Navigate to **ADMIN > Storage > Online** and perform **Test** and **Deploy**.
4. Test new indices have the updated terms limit by executing the following simple REST API call.

```
GET fortisiem-event-*/_settings
```

Public Domain Built-in Rules

The following table shows the public domain built-in rules incorporated into FortiSIEM.

Rules that are adopted from the SIGMA rule set are licensed under the Detection Rule License available [here](#).

FortiSIEM Rule	Author	Source Link
AWS CloudTrail Important Changes	vitaliy0x1	https://github.com/SigmaHQ/sigma/blob/master/rules/cloud/aws_cloudtrail_disable_logging.yml
AWS EC2 Userdata Download	faloker	https://github.com/SigmaHQ/sigma/blob/master/rules/cloud/aws_ec2_download_userdata.yml
Linux: Attempt to Disable CrowdStrike Service	Ömer Günal	https://github.com/SigmaHQ/sigma/blob/master/rules/linux/lnx_security_tools_disabling.yml
Linux: Attempt to Disable CarbonBlack Service	Ömer Günal	https://github.com/SigmaHQ/sigma/blob/master/rules/linux/lnx_security_tools_disabling.yml
Windows: Turla Service Install	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_apr_carbonpaper_turla.yml
Windows: StoneDrill Service Install	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_apr_stonedrill.yml

FortiSIEM Rule	Author	Source Link
Windows: Turla PNG Dropper Service	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_aprt_turla_service_png.yml
Windows: smbexec.py Service Installation	Omer Faruk Celik	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_hack_smbexec.yml
Windows: Malicious Service Installations	Florian Roth, Daniil Yugoslavskiy, oscd.community (update)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_mal_service_installs.yml
Windows: Meterpreter or Cobalt Strike Getsystem Service Installation	Teymur Kheirkhabarov, Ecco	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_meterpreter_or_cobaltstrike_getsystem_service_installation.yml
Windows: PsExec Tool Execution	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/other/win_tool_psexec.yml
Windows: Local User Creation	Patrick Bareiss	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_user_creation.yml
Windows: Local User Creation Via Powershell	@ROxPinTeddy	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/powershell_create_local_user.yml
Windows: Local User Creation Via Net.exe	Endgame, JHasenbusch (adapted to sigma for oscd.community)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_net_user_add.yml
Windows: Suspicious ANONYMOUS LOGON Local Account Created	James Pemberton / @4A616D6573	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_local_anon_logon_created.yml
Windows: New or Renamed User Account with \$ in Attribute SamAccountName	Ilyas Ochkov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_new_or_renamed_user_account_with_dollar_sign.yml
Windows: AD Privileged Users or Groups Reconnaissance	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_account_discovery.yml
Windows: Administrator and Domain Admin Reconnaissance	Florian Roth (rule), Jack Croock (method)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_net_recon_activity.yml

FortiSIEM Rule	Author	Source Link
Windows: Access to ADMIN\$ Share	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_admin_share_access.yml
Windows: Login with WMI	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_wmi_login.yml
Windows: Admin User Remote Logon	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_admin_rdp_login.yml
Windows: RDP Login from Localhost	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_rdp_localhost_login.yml
Windows: Interactive Logon to Server Systems	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_interactive_logons.yml
Windows: Pass the Hash Activity	Ilias el Matani (rule), The Information Assurance Directorate at the NSA (method)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_pass_the_hash.yml
Windows: Pass the Hash Activity 2	Dave Kennedy, Jeff Warren (method) / David Vassallo (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_pass_the_hash_2.yml
Windows: Successful Overpass the Hash Attempt	Roberto Rodriguez (source), Dominik Schaudel (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_overpass_the_hash.yml
Windows: RottenPotato Like Attack Pattern	@SBousseaden, Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_rottenpotato.yml
Windows: Hacktool Ruler	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_alert_ruler.yml
Windows: Metasploit SMB Authentication	Chakib Gzenayi (@Chak092), Hosni Mribah	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_metasploit_authentication.yml
Windows: Kerberos Manipulation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_kerberos_manipulation.yml
Windows: Suspicious Kerberos RC4 Ticket Encryption	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_rc4_kerberos.yml

FortiSIEM Rule	Author	Source Link
Windows: Persistence and Execution at Scale via GPO Scheduled Task	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_GPO_scheduledtasks.yml
Windows: Powerview Add-DomainObjectAcl DCSync AD Extend Right	Samir Bousseaden; Roberto Rodriguez @Cyb3rWard0g; oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_account_backdoor_dcsync_rights.yml
Windows: AD Object WriteDAC Access	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_ad_object_writedac_access.yml
Windows: Active Directory Replication from Non Machine Account	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_ad_replication_non_machine_account.yml
Windows: AD User Enumeration	Maxime Thiebaut (@0xThiebaut)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_ad_user_enumeration.yml
Windows: Enabled User Right in AD to Control User Objects	@neu5ron	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_alert_active_directory_user_control.yml
Windows: Eventlog Cleared	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_eventlog_cleared.yml
Windows: MSHTA Suspicious Execution 01	Diego Perez (@darkquassar), Markus Neis, Swisscom (Improve Rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_mshta_execution.yml
Windows: Dumpert Process Dumper	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_hack_dumpert.yml
Windows: Blue Mockingbird	Trent Liffick (@tliffick)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/win_mal_blue_mockingbird.yml
Windows: Windows PowerShell Web Request	James Pemberton / @4A616D6573	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/win_powershell_web_request.yml
Windows: DNS Tunnel Technique from MuddyWater	@caliskanfurkan_	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/sysmon_apt_muddywater_dnstunnel.yml

FortiSIEM Rule	Author	Source Link
Windows: Advanced IP Scanner Detected	@ROxPinTeddy	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_advanced_ip_scanner.yml
Windows: APT29 Detected	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_apt29_thinktanks.yml
Windows: Baby Shark Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_babys shark.yml
Windows: Judgement Panda Credential Access Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_bear_activity_gtr19.yml
Windows: Logon Scripts - UserInitMprLogonScript	Tom Ueltschi (@c_APT_ure)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/sysmon_logon_scripts_userinitmprlogonscript_proc.yml
Windows: BlueMashroom DLL Load	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apt_bluemashroom.yml
Windows: Password Change on Directory Service Restore Mode DSRM Account	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_dsrm_password_change.yml
Windows: Account Tampering - Suspicious Failed Logon Reasons	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_failed_logon_reasons.yml
Windows: Backup Catalog Deleted	Florian Roth (rule), Tom U. @c_APT_ure (collection)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_backup_delete.yml
Windows: Failed Code Integrity Checks	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_codeintegrity_check_failure.yml
Windows: DHCP Server Loaded the CallOut DLL	Dimitrios Slamaris	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_dhcp_config.yml
Windows: Suspicious LDAP-Attributes Used	xknow @xknow_infosec	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_ldap_dataexchange.yml

FortiSIEM Rule	Author	Source Link
Windows: Password Dumper Activity on LSASS		https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_lsass_dump.yml
Windows: Generic Password Dumper Activity on LSASS	Roberto Rodriguez, Teymur Kheirkhabarov, Dimitrios Slamaris, Mark Russinovich, Aleksey Potapov, oscd.community (update)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_lsass_dump_generic.yml
Windows: Suspicious PsExec Execution	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_psexec.yml
Windows: Suspicious Access to Sensitive File Extensions	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_raccess_sensitive_ext.yml
Windows: Secure Deletion with SDelete	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_sdelete.yml
Windows: Unauthorized System Time Modification	@neu5ron	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_time_modification.yml
Windows: Windows Defender Exclusion Set	@BarryShooshooga	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/other/win_defender_bypass.yml
Windows: Windows Pcap Driver Installed	Cian Heasley	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/other/win_pcap_drivers.yml
Windows: Weak Encryption Enabled and Kerberoast	@neu5ron	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_alert_enable_weak_encryption.yml
Windows: Remote Task Creation via ATSVS Named Pipe	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_atsvc_task.yml
Windows: Chafer Activity	Florian Roth, Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apl_chafer_mar18.yml
Windows: WMIExec VBS Script	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apl_cloudhopper.yml

FortiSIEM Rule	Author	Source Link
Windows: CrackMapExecWin Activity	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apr_dragonfly.yml
Windows: Elise Backdoor	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apr_elise.yml
Windows: Emissary Panda Malware SLLauncher Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apr_emissarypanda_sep19.yml
Windows: Empire Monkey Activity	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apr_empiremonkey.yml
Windows: Equation Group DLL-U Load	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apr_equationgroup_dll_u_load.yml
Windows: EvilNum Golden Chickens Deployment via OCX Files	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apr_evilnum_jul20.yml
Windows: GALLIUM Artefacts Via Hash Match	Tim Burrell	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apr_gallium.yml
Windows: GALLIUM Artefacts Via Hash and Process Match	Tim Burrell	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apr_gallium.yml
Windows: Windows Credential Editor Startup	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/sysmon_hack_wce.yml
Windows: Greenbug Campaign Indicators	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apr_greenbug_may20.yml
Windows: Hurricane Panda Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apr_hurricane_panda.yml
Windows: Judgement Panda Exfiltration Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apr_judgement_panda_gtr19.yml
Windows: Ke3chang Registry Key Modifications	Markus Neis, Swisscom	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apr_ke3chang_regadd.yml

FortiSIEM Rule	Author	Source Link
Windows: Lazarus Session Hijacker	Trent Liffick (@tliffick), Bartłomiej Czyz (@bczyz1)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apl_lazarus_session_highjack.yml
Windows: Mustang Panda Dropper Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apl_mustangpanda.yml
Windows: Defrag Deactivation	Florian Roth, Bartłomiej Czyz (@bczyz1)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apl_slingshot.yml
Windows: Sofacy Trojan Loader Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apl_sofacy.yml
Windows: Ps.exe Renamed SysInternals Tool	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apl_ta17_293a_ps.yml
Windows: TAIDOOOR RAT DLL Load	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apl_taidoor.yml
Windows: TropicTrooper Campaign November 2018	@41thexplorer, Microsoft Defender ATP	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apl_tropictrooper.yml
Windows: Turla Group Commands May 2020	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apl_turla_comrat_may20.yml
Windows: Unidentified Attacker November 2018 Activity 1	@41thexplorer, Microsoft Defender ATP	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apl_unidentified_nov_18.yml
Windows: Unidentified Attacker November 2018 Activity 2	@41thexplorer, Microsoft Defender ATP	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apl_unidentified_nov_18.yml
Windows: Winnti Malware HK University Campaign	Florian Roth, Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apl_winnti_mal_hk_jan20.yml
Windows: Winnti Pipemon Characteristics	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apl_winnti_pipemon.yml
Windows: Operation Wocao Activity	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apl_wocao.yml

FortiSIEM Rule	Author	Source Link
Windows: ZxShell Malware	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apr_zxshell.yml
Windows: Active Directory User Backdoors	@neu5ron	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_alert_ad_user_backdoors.yml
Windows: Mimikatz DC Sync	Benjamin Delpy, Florian Roth, Scott Dermott	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_dcsync.yml
Windows: Windows Event Auditing Disabled	@neu5ron	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_disable_event_logging.yml
Windows: DPAPI Domain Backup Key Extraction	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_dpapi_domain_backupkey_extraction.yml
Windows: DPAPI Domain Master Key Backup Attempt	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_dpapi_domain_masterkey_backup_attempt.yml
Windows: External Disk Drive or USB Storage Device	Keith Wright	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_external_device.yml
Windows: Possible Impacket SecretDump Remote Activity	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_impacket_secretdump.yml
Windows: Obfuscated Powershell IEX invocation	Daniel Bohannon (@Mandiant/@FireEye), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_invoke_obfuscation_obfuscated_iex_services.yml
Windows: First Time Seen Remote Named Pipe	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_lm_namedpipe.yml
Windows: LSASS Access from Non-System Account	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_lsass_access_non_system_account.yml
Windows: Credential Dumping Tools Service Execution	Florian Roth, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_mal_creddumper.yml

FortiSIEM Rule	Author	Source Link
Windows: WCE wceaux dll Access	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_mal_wceaux_dll.yml
Windows: MMC20 Lateral Movement	@2xxeformyshirt (Security Risk Advisors) - rule; Teymur Kheirkhabarov (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_mmc20_lateral_movement.yml
Windows: NetNTLM Downgrade Attack	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_net_ntlm_downgrade.yml
Windows: Denied Access To Remote Desktop	Pushkarev Dmitry	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_not_allowed_rdp_access.yml
Windows: Possible DCShadow	Ilyas Ochkov, oscd.community, Chakib Gzenayi (@Chak092), Hosni Mribah	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_possible_dc_shadow.yml
Windows: Protected Storage Service Access	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_protected_storage_service_access.yml
Windows: Scanner PoC for CVE-2019-0708 RDP RCE Vuln	Florian Roth (rule), Adam Bradbury (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_rdp_bluekeep_poc_scanner.yml
Windows: RDP over Reverse SSH Tunnel	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_rdp_reverse_tunnel.yml
Windows: Register new Logon Process by Rubeus	Roberto Rodriguez (source), Ilyas Ochkov (rule), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_register_new_logon_process_by_rubeus.yml
Windows: Remote PowerShell Sessions	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_remote_powershell_session.yml
Windows: Remote Registry Management Using Reg Utility	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_remote_registry_management_using_reg_utility.yml
Windows: SAM Registry Hive Handle Request	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_sam_registry_hive_handle_request.yml

FortiSIEM Rule	Author	Source Link
Windows: SCM Database Handle Failure	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_scm_database_handle_failure.yml
Windows: SCM Database Privileged Operation	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_scm_database_privileged_operation.yml
Windows: Addition of Domain Trusts	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_add_domain_trust.yml
Windows: Addition of SID History to Active Directory Object	Thomas Patzke, @atc_project (improvements)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_add_sid_history.yml
Windows: Failed Logon From Public IP	NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_failed_logon_source.yml
Windows: Failed Logins with Different Accounts from Single Source System	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_susp_failed_logons_single_source.yml
Windows: Remote Service Activity via SVCCTL Named Pipe	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_svcctl_remote_service.yml
Windows: SysKey Registry Keys Access	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_syskey_registry_access.yml
Windows: Tap Driver Installation	Daniil Yugoslavskiy, Ian Davis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_tap_driver_installation.yml
Windows: Transferring Files with Credential Data via Network Shares	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_transferring_files_with_credential_data_via_network_shares.yml
Windows: User Added to Local Administrators	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_user_added_to_local_administrators.yml
Windows: Failed to Call Privileged Service LsaRegisterLogonProcess	Roberto Rodriguez (source), Ilyas Ochkov (rule), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_user_couldnt_call_privileged_service_lsaregisterlogonprocess.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious Driver Loaded By User	xknow (@xknow_infosec), xorxes (@xor_xes)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_user_driver_loaded.yml
Windows: Suspicious Driver Load from Temp	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/driver_load/sysmon_susp_driver_load.yml
Windows: File Created with System Process Name	Sander Wiebing	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_creation_system_file.yml
Windows: Credential Dump Tools Dropped Files	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_cred_dump_tools_dropped_files.yml
Windows: Detection of SafetyKatz	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_ghostpack_safetykatz.yml
Windows: LSASS Memory Dump File Creation	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_lsass_memory_dump_file_creation.yml
Windows: Microsoft Office Add-In Loading	NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_office_persistence.yml
Windows: QuarksPwDump Dump File	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_quarkspw_filedump.yml
Windows: RedMimicry Winnti Playbook Dropped File	Alexander Rausch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_redmimicry_winnti_filedrop.yml
Windows: Suspicious ADSI-Cache Usage By Unknown Tool	xknow @xknow_infosec	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_susp_adsi_cache_usage.yml
Windows: Suspicious desktop.ini Action	Maxime Thiebaut (@0xThiebaut)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_susp_desktop_ini.yml
Windows: Suspicious PROCEXP152 sys File Created In TMP	xknow (@xknow_infosec), xorxes (@xor_xes)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_susp_procexplorer_driver_created_in_tmp_folder.yml

FortiSIEM Rule	Author	Source Link
Windows: Hijack Legit RDP Session to Move Laterally	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_tsclient_filewrite_startup.yml
Windows: Windows Web shell Creation	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_webshell_creation_detect.yml
Windows: WMI Persistence - Script Event Consumer File Write	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_wmi_persistence_script_event_consumer_write.yml
Windows: Suspicious Desktopimgdownldr Target File	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/win_susp_desktopimgdownldr_file.yml
Windows: In-memory PowerShell	Tom Kern, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_in_memory_powershell.yml
Windows: PowerShell load within System Management Automation DLL	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_powershell_execution_moduleload.yml
Windows: Fax Service DLL Search Order Hijack	NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_fax_dll.yml
Windows: Possible Process Hollowing Image Loading	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_image_load.yml
Windows: .NET DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_office_dotnet_assembly_dll_load.yml
Windows: CLR DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_office_dotnet_clr_dll_load.yml
Windows: GAC DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_office_dotnet_gac_dll_load.yml
Windows: Active Directory Parsing DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_office_dsparse_dll_load.yml

FortiSIEM Rule	Author	Source Link
Windows: Active Directory Kerberos DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_office_kerberos_dll_load.yml
Windows: VBA DLL Loaded Via Office Applications	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_winword_vbadll_load.yml
Windows: WMI DLL Loaded Via Office Applications	Michael R. (@nahamike01)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_susp_winword_wmidll_load.yml
Windows: Loading dbghelp dbgcore DLL from Suspicious Processes	Perez Diego (@darkquassar), oscd.community, Ecco	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_suspicious_dbghelp_dbgcore_load.yml
Windows: Svchost DLL Search Order Hijack	SBousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_svchost_dll_search_order_hijack.yml
Windows: Unsigned Image Loaded Into LSASS Process	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_unsigned_image_loaded_into_lsass.yml
Windows: Suspicious WMI Modules Loaded	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_wmi_module_load.yml
Windows: WMI Persistence - Command Line Event Consumer	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_wmi_persistence_commandline_event_consumer.yml
Windows: Registry Entries Found For Azorult Malware	Trent Liffick	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/mal_azorult_reg.yml
Windows: Registry Entries Found For FlowCloud Malware	NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/win_mal_flowcloud.yml
Windows: Octopus Scanner Malware Detected	NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/win_mal_octopus_scanner.yml
Windows: Registry Entries For Ursnif Malware	megan201296	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/win_mal_ursnif.yml

FortiSIEM Rule	Author	Source Link
Windows: Dllhost.exe Internet Connection	bartblaze	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_dllhost_net_connections.yml
Windows: Suspicious Typical Malware Back Connect Ports	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_malware_backconnect_ports.yml
Windows: Notepad Making Network Connection	EagleEye Team	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_notepad_network_connection.yml
Windows: PowerShell Network Connections	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_powershell_network_connection.yml
Windows: RDP Over Reverse SSH Tunnel	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_rdp_reverse_tunnel.yml
Windows: Regsvr32 Network Activity	Dmitriy Lifanov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_regsvr32_network_activity.yml
Windows: Remote PowerShell Session	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_remote_powershell_session_network.yml
Windows: Rundll32 Internet Connection	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_rundll32_net_connections.yml
Windows: Network Connections From Executables in Suspicious Program Locations	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_susp_prog_location_network_connection.yml
Windows: Outbound RDP Connections From Suspicious Executables	Markus Neis - Swisscom	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_susp_rdp.yml
Windows: Outbound Kerberos Connection From Suspicious Executables	Ilyas Ochkov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_suspicious_outbound_kerberos_connection.yml ;

FortiSIEM Rule	Author	Source Link
		https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_suspicious_outbound_kerberos_connection.yml
Windows: Microsoft Binary Github Communication	Michael Haag (idea), Florian Roth (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_win_binary_github_com.yml
Windows: Microsoft Binary Suspicious External Communication	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_win_binary_susp_com.yml
Windows: Data Compressed - Powershell	Timur Zinniatullin, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/powershell_data_compressed.yml
Windows: Dnscat Execution	Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/powershell_dnscat_execution.yml
Windows: PowerShell Credential Prompt	John Lambert (idea), Florian Roth (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/powershell_prompt_credentials.yml
Windows: Powershell Profile ps1 Modification	HieuTT35	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/powershell_suspicious_profile_create.yml
Windows: Credentials Dumping Tools Accessing LSASS Memory	Florian Roth, Roberto Rodriguez, Dimitrios Slamaris, Mark Russinovich, Thomas Patzke, Teymur Kheirkhabarov, Sherif Eldeeb, James Dickenson, Aleksey Potapov, oscd.community (update)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_cred_dump_lsass_access.yml
Windows: Suspicious In-Memory Module Execution	Perez Diego (@darkquassar), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_in_memory_assembly_execution.yml
Windows: Suspect Svchost Memory Access	Tim Burrell	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_invoke_phantom.yml

FortiSIEM Rule	Author	Source Link
Windows: Credential Dumping by LaZagne	Bhabesh Raj	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_lazagne_cred_dump_lsass_access.yml
Windows: LSASS Memory Dump	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_lsass_memdump.yml
Windows: Malware Shellcode in Verclsid Target Process	John Lambert (tech), Florian Roth (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_malware_verclsid_shellcode.yml
Windows: Mimikatz through Windows Remote Management	Patryk Prauze - ING Tech	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_mimikatz_trough_winrm.yml
Windows: Turla Group Lateral Movement	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_apr_turla_commands.yml
Windows: Hiding Files with Attrib.exe	Sami Ruohonen	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_attrib_hiding_files.yml
Windows: Modification of Boot Configuration	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_bootconf_mod.yml
Windows: SquiblyTwo	Markus Neis / Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_bypass_squiblytwo.yml
Windows: Change Default File Association	Timur Zinniatullin, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_change_default_file_association.yml
Windows: Cmdkey Cached Credentials Recon	jmallette	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_cmdkey_recon.yml
Windows: CMSTP UAC Bypass via COM Object Access	Nik Seetharaman	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_cmstp_com_object_access.yml
Windows: Cmd.exe CommandLine Path Traversal	xknow @xknow_infosec	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_commandline_path_traversal.yml

FortiSIEM Rule	Author	Source Link
Windows: Unusual Control Panel Items	Kyaw Min Thein, Furkan Caliskan (@caliskanfurkan_)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_control_panel_item.yml
Windows: Copying Sensitive Files with Credential Data	Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_copying_sensitive_files_with_credential_data.yml
Windows: Fireball Archer Malware Install	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_crime_fireball.yml
Windows: Maze Ransomware	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_crime_maze_ransomware.yml
Windows: Snatch Ransomware	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_crime_snatch_ransomware.yml
Windows: Data Compressed - rar.exe	Timur Zinniatullin, E.M. Anhaus, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_data_compressed_with_rar.yml
Windows: DNS Exfiltration and Tunneling Tools Execution	Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_dns_exfiltration_tools_execution.yml
Windows: DNSCat2 Powershell Detection Via Process Creation	Cian Heasley	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_dnscat2_powershell_implementation.yml
Windows: Encoded FromBase64String	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_encoded_frombase64string.yml
Windows: Encoded IEX	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_encoded_iex.yml
Windows: COMPlus-ETWEnabled Command Line Arguments	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_etw_modification_cmdline.yml
Windows: Disabling ETW Trace	@neu5ron, Florian Roth, Jonhnathan Ribeiro, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_etw_trace_evasion.yml

FortiSIEM Rule	Author	Source Link
Windows: Exfiltration and Tunneling Tools Execution	Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exfiltration_and_tunneling_tools_execution.yml
Windows: Exploit for CVE-2015-1641	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2015_1641.yml
Windows: Exploit for CVE-2017-0261	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2017_0261.yml
Windows: Droppers Exploiting CVE-2017-11882	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2017_11882.yml
Windows: Exploit for CVE-2017-8759	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2017_8759.yml
Windows: Exploiting SetupComplete.cmd CVE-2019-1378	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2019_1378.yml
Windows: Exploiting CVE-2019-1388	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2019_1388.yml
Windows: Exploited CVE-2020-10189 Zoho ManageEngine	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2020_10189.yml
Windows: Suspicious PrinterPorts Creation CVE-2020-1048	EagleEye Team, Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2020_1048.yml
Windows: DNS RCE CVE-2020-1350	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_exploit_cve_2020_1350.yml
Windows: File/Folder Permissions Modifications Via Command line Utilities	Jakob Weinzettl, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_file_permission_modifications.yml
Windows: Grabbing Sensitive Hives via Reg Utility	Teymur Kheirkhabarov, Endgame, JHasenbusch, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_grabbing_sensitive_hives_via_reg.yml

FortiSIEM Rule	Author	Source Link
Windows: Bloodhound and Sharpbound Hack Tool	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hack_bloodhound.yml
Windows: Koadic Execution	wagga	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hack_koadic.yml
Windows: Rubeus Hack Tool	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hack_rubeus.yml
Windows: SecurityXploded Tool	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hack_secutyxploded.yml
Windows: HH exe Execution	E.M. Anhaus (originally from Atomic Blue Detections, Dan Beavin), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hh_chm.yml
Windows: CreateMiniDump Hacktool	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hctl_createminidump.yml
Windows: HTML Help Shell Spawn	Maxim Pavlunin	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_html_help_spawn.yml
Windows: Suspicious HWP Sub Processes	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hwp_exploits.yml
Windows: Impacket Lateralization Detection	Ecco	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_impacket_lateralization.yml
Windows: Indirect Command Execution	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_indirect_cmd.yml
Windows: Suspicious Debugger Registration Cmdline	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_install_reg_debugger_backdoor.yml
Windows: Interactive AT Job	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_interactive_at.yml

FortiSIEM Rule	Author	Source Link
Windows: Invoke-Obfuscation Obfuscated IEX Invocation when to create process	Daniel Bohannon (@Mandiant/@FireEye), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_invoke_obfuscation_obfuscated_iex_commandline.yml
Windows: Windows Kernel and 3rd-Party Drivers Exploits Token Stealing	Teymur Kheirkhabarov (source), Daniil Yugoslavskiy (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_kernel_and_3rd_party_drivers_exploits_token_stealing.yml
Windows: MSHTA Spawned by SVCHOST	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_lethalhta.yml
Windows: Local Accounts Discovery	Timur Zinniatullin, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_local_system_owner_account_discovery.yml
Windows: LSASS Memory Dumping Using procdump	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_lsass_dump.yml
Windows: Adwind Remote Access Tool JRAT	Florian Roth, Tom Ueltschi	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mal_adwind.yml
Windows: Dridex Process Pattern	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_dridex.yml
Windows: DTRACK Malware Process Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_dtrack.yml
Windows: Emotet Malware Process Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_emotet.yml
Windows: Formbook Malware Process Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_formbook.yml
Windows: QBot Process Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_qbot.yml

FortiSIEM Rule	Author	Source Link
Windows: Ryuk Ransomware	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/malware/win_mal_ryuk.yml ; https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_ryuk.yml
Windows: WScript or CScript Dropper	Margaritis Dimitrios (idea), Florian Roth (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_script_dropper.yml
Windows: Trickbot Malware Recon Activity	David Burkett, Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_trickbot_recon_activity.yml
Windows: WannaCry Ransomware	Florian Roth (rule), Tom U. @c_APT_ure (collection)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_malware_wannacry.yml
Windows: MavInject Process Injection	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mavinject_proc_inj.yml
Windows: Meterpreter or Cobalt Strike Getsystem Service Start	Teymur Kheirkhabarov, Ecco	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_meterpreter_or_cobaltstrike_getsystem_service_start.yml
Windows: Mimikatz Command Line	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mimikatz_command_line.yml
Windows: MMC Spawning Windows Shell	Karneades, Swisscom CSIRT	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mmc_spawn_shell.yml
Windows: Mouse Lock Credential Gathering	Cian Heasley	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mouse_lock.yml
Windows: Mshta JavaScript Execution	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mshta_javascript.yml
Windows: MSHTA Spawning Windows Shell	Michael Haag	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_mshta_spawn_shell.yml

FortiSIEM Rule	Author	Source Link
Windows: Quick Execution of a Series of Suspicious Commands	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_multiple_suspicious_cli.yml
Windows: Windows Network Enumeration	Endgame, JHasenbusch (ported for oscd.community)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_net_enum.yml
Windows: Netsh RDP Port Opening	Sander Wiebing	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_allow_port_rdp.yml
Windows: Netsh Port or Application Allowed	Markus Neis, Sander Wiebing	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_fw_add.yml
Windows: Netsh Program Allowed with Suspicious Location	Sander Wiebing	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_fw_add_susp_image.yml
Windows: Network Trace with netsh exe	Kutepov Anton, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_packet_capture.yml
Windows: Netsh Port Forwarding	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_port_fwd.yml
Windows: Netsh RDP Port Forwarding	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_port_fwd_3389.yml
Windows: Harvesting of Wifi Credentials Using netsh exe	Andreas Hunkeler (@Karneades)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_netsh_wifi_credential_harvesting.yml
Windows: Network Sniffing	Timur Zinniatullin, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_network_sniffing.yml
Windows: New Service Creation via sc.exe	Timur Zinniatullin, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_new_service_creation.yml
Windows: Non Interactive PowerShell	Roberto Rodriguez @Cyb3rWard0g (rule), oscd.community (improvements)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_non_interactive_powershell.yml

FortiSIEM Rule	Author	Source Link
Windows: Microsoft Office Product Spawning Windows Shell	Michael Haag, Florian Roth, Markus Neis, Elastic, FPT.EagleEye Team	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_office_shell.yml
Windows: MS Office Product Spawning Exe in User Directory	Jason Lynch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_office_spawn_exe_from_users_directory.yml
Windows: Executable Used by PlugX in Uncommon Location	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_plugx_susp_exe_locations.yml
Windows: Possible Applocker Bypass	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_possible_applocker_bypass.yml
Windows: Detection of Possible Rotten Potato	Teymur Kheirkhabarov	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_possible_privilege_escalation_using_rotten_potato.yml
Windows: Powershell AMSI Bypass via NET Reflection	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_amsi_bypass.yml
Windows: Audio Capture via PowerShell	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_audio_capture.yml
Windows: PowerShell Base64 Encoded Shellcode	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_b64_shellcode.yml
Windows: Suspicious Bitsadmin Job via PowerShell	Endgame, JHasenbusch (ported to sigma for oscd.community)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_bitsjob.yml
Windows: Suspicious PowerShell Execution via DLL	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_dll_execution.yml
Windows: PowerShell Downgrade Attack	Harish Segar (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_downgrade_attack.yml
Windows: Download via PowerShell URL	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_download.yml

FortiSIEM Rule	Author	Source Link
Windows: FromBase64String Command Line	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_frombase64string.yml
Windows: Suspicious PowerShell Parameter Substring	Florian Roth (rule), Daniel Bohannon (idea), Roberto Rodriguez (Fix)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_suspicious_parameter_variation.yml
Windows: Suspicious XOR Encoded PowerShell Command Line	Sami Ruohonen, Harish Segar (improvement)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powershell_xor_commandline.yml
Windows: Default PowerSploit and Empire Sctasks Persistence	Markus Neis, @Karneades	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_powersploit_empire_schtasks.yml
Windows: Windows Important Process Started From Suspicious Parent Directories	vburov	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_proc_wrong_parent.yml
Windows: Bitsadmin Download	Michael Haag	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_process_creation_bitsadmin_download.yml
Windows: Process Dump via Rundll32 and Comsvcs dll	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_process_dump_rundll32_comsvcs.yml
Windows: PsExec Service Start	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_psexesvc_start.yml
Windows: Query Registry	Timur Zinniatullin, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_query_registry.yml
Windows: MSTSC Shadowing	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_rdp_hijack_shadowing.yml
Windows: RedMimicry Winnti Playbook Execute	Alexander Rausch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_redmimicry_winnti_proc.yml

FortiSIEM Rule	Author	Source Link
Windows: Remote PowerShell Session for creating process	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_remote_powershell_session_process.yml
Windows: System Time Discovery	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_remote_time_discovery.yml
Windows: Renamed Binary	Matthew Green - @mgreen27, Ecco, James Pemberton / @4A616D6573, oscd.community (improvements), Andreas Hunkeler (@Karneades)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_binary.yml
Windows: Highly Relevant Renamed Binary	Matthew Green - @mgreen27, Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_binary_highly_relevant.yml
Windows: Renamed jusched exe	Markus Neis, Swisscom	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_jusched.yml
Windows: Execution of Renamed PaExec	Jason Lynch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_paexec.yml
Windows: Renamed PowerShell	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_powershell.yml
Windows: Renamed ProcDump	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_procdump.yml
Windows: Renamed PsExec	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_renamed_psexec.yml
Windows: Run PowerShell Script from ADS	Sergey Soldatov, Kaspersky Lab, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_run_powershell_script_from_ads.yml
Windows: Possible Shim Database Persistence via sdbinst exe	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_sdbinst_shim_persistence.yml

FortiSIEM Rule	Author	Source Link
Windows: Manual Service Execution	Timur Zinniatullin, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_service_execution.yml
Windows: Stop Windows Service	Jakob Weinzettl, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_service_stop.yml
Windows: Shadow Copies Access via Symlink	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_shadow_copies_access_symlink.yml
Windows: Shadow Copies Creation Using Operating Systems Utilities	Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_shadow_copies_creation.yml
Windows: Shadow Copies Deletion Using Operating Systems Utilities	Florian Roth, Michael Haag, Teymur Kheirkhabarov, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_shadow_copies_deletion.yml
Windows: Windows Shell Spawning Suspicious Program	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_shell_spawn_susp_program.yml
Windows: SILENTTRINITY Stager Execution	Aleksey Potapov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_silenttrinity_stage_use.yml
Windows: Audio Capture via SoundRecorder	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_soundrec_audio_capture.yml
Windows: Possible SPN Enumeration	Markus Neis, keepwatch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_spn_enum.yml
Windows: Possible Ransomware or Unauthorized MBR Modifications	@neu5ron	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_bcdedit.yml
Windows: Application Allowlisting Bypass via Bginfo	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_bginfo.yml
Windows: Suspicious Calculator Usage	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_calc.yml

FortiSIEM Rule	Author	Source Link
Windows: Possible App Allowlisting Bypass via WinDbg CDB as a Shell code Runner	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_cdb.yml
Windows: Suspicious Certutil Command	Florian Roth, juju4, keepwatch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_certutil_command.yml
Windows: Certutil Encode	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_certutil_encode.yml
Windows: Suspicious Commandline Escape	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_cli_escape.yml
Windows: Command Line Execution with Suspicious URL and AppData Strings	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_cmd_http_appdata.yml
Windows: Suspicious Code Page Switch	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_codepage_switch.yml
Windows: Reconnaissance Activity with Net Command	Florian Roth, Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_commands_recon_activity.yml
Windows: Suspicious Compression Tool Parameters	Florian Roth, Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_compression_params.yml
Windows: Process Dump via Comsvcs DLL	Modexp (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_comsvcs_procdump.yml
Windows: Copy from Admin Share	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_copy_lateral_movement.yml
Windows: Suspicious Copy From or To System32	Florian Roth, Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_copy_system32.yml
Windows: Covenant Launcher Indicators	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_covenant.yml
Windows: CrackMapExec Command Execution	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_crackmapexec_execution.yml

FortiSIEM Rule	Author	Source Link
Windows: CrackMapExec PowerShell Obfuscation	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_crackmapexec_powershell_obfuscation.yml
Windows: Suspicious Parent of Csc.exe	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_csc.yml
Windows: Suspicious Csc.exe Source File Folder	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_csc_folder.yml
Windows: Suspicious Curl Usage on Windows	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_curl_download.yml
Windows: Suspicious Curl File Upload	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_curl_fileupload.yml
Windows: Curl Start Combination	Sreeman	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_curl_start_combo.yml
Windows: ZOHO Dctask64 Process Injection	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_dctask64_proc_inject.yml
Windows: Suspicious Desktopimgdownldr Command	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_desktopimgdownldr.yml
Windows: Devtoolslauncher.exe Executing Specified Binary	Beyu Denis, oscd.community (rule), @_felamos (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_devtoolslauncher.yml
Windows: Direct Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_direct_asep_reg_keys_modification.yml
Windows: Disabled IE Security Features	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_disable_ie_features.yml
Windows: DIT Snapshot Viewer Use	Furkan Caliskan (@caliskanfurkan_)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_ditsnap.yml

FortiSIEM Rule	Author	Source Link
Windows: Application Allowlisting Bypass via Dnx.exe	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_dnx.yml
Windows: Suspicious Double File Extension	Florian Roth (rule), @blu3_team (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_double_extension.yml
Windows: Application Allowlisting Bypass via Dxcap.exe	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_dxcap.yml
Windows: Suspicious Eventlog Clear or Configuration Using Wevtutil or Powershell or Wmic	Ecco, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_eventlog_clear.yml
Windows: Executables Started in Suspicious Folder	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_exec_folder.yml
Windows: Execution in Non-Executable Folder	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_execution_path.yml
Windows: Execution in Webserver Root Folder	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_execution_path_webserver.yml
Windows: Explorer Root Flag Process Tree Break	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_explorer_break_proctree.yml
Windows: Suspicious File Characteristics Due to Missing Fields	Markus Neis, Sander Wiebing	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_file_characteristics.yml
Windows: Findstr Launching Ink File	Trent Liffick	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_findstr_Ink.yml
Windows: Firewall Disabled via Netsh	Fatih Sirin	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_firewall_disable.yml
Windows: Fsutil Suspicious Invocation	Ecco, E.M. Anhaus, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_fsutil_usage.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious GUP.exe Usage	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_gup.yml
Windows: IIS Native-Code Module Command Line Installation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_iss_module_install.yml
Windows: Windows Defender Download Activity	Matthew Matchen	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_mpcmdrun_download.yml
Windows: Suspicious MsiExec Directory	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_msiexec_cwd.yml
Windows: MsiExec Web Install	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_msiexec_web_install.yml
Windows: Malicious Payload Download via Office Binaries	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_msoffice.yml
Windows: Net.exe Execution For Discovery	Michael Haag, Mark Woan (improvements), James Pemberton / @4A616D6573 / oscd.community (improvements)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_net_execution.yml
Windows: Suspicious Netsh.DLL Persistence	Victor Sergeev, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_netsh_dll_persistence.yml
Windows: Invocation of Active Directory Diagnostic Tool ntdsutil.exe	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_ntdsutil.yml
Windows: Application Allowlisting Bypass via DLL Loaded by odbccf.exe	Kirill Kiryanov, Beyu Denis, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_odbccf.yml
Windows: OpenWith.exe Executing Specified Binary	Beyu Denis, oscd.community (rule), @harr0ey (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_openwith.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious Execution from Outlook	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_outlook.yml
Windows: Execution in Outlook Temp Folder	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_outlook_temp.yml
Windows: Ping Hex IP	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_ping_hex_ip.yml
Windows: Empire PowerShell Launch Parameters	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_empire_launch.yml
Windows: Empire PowerShell UAC Bypass	Ecco	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_empire_uac_bypass.yml
Windows: Suspicious Encoded PowerShell Command Line	Florian Roth, Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_enc_cmd.yml
Windows: PowerShell Encoded Character Syntax	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_encoded_param.yml
Windows: Malicious Base64 Encoded PowerShell Keywords in Command Lines	John Lambert (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_hidden_b64_cmd.yml
Windows: Suspicious PowerShell Invocation Based on Parent Process	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_parent_combo.yml
Windows: Suspicious PowerShell Parent Process	Teymur Kheirkhabarov, Harish Segar (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_parent_process.yml
Windows: Suspicious Use of Procdump	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_procdump.yml

FortiSIEM Rule	Author	Source Link
Windows: Programs starting from Suspicious Location	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_prog_location_process_starts.yml
Windows: PowerShell Script Run in AppData	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_ps_appdata.yml
Windows: PowerShell DownloadFile	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_ps_downloadfile.yml
Windows: Psr.exe Capture Screenshots	Beyu Denis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_psr_capture_screenshots.yml
Windows: Rar with Password or Compression Level	@ROxPinTeddy	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_rar_flags.yml
Windows: Suspicious RASdial Activity	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_rasdial_activity.yml
Windows: Suspicious Reconnaissance Activity via net group or localgroup	Florian Roth, omkar72	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_recon_activity.yml
Windows: Suspicious Regsvr32 Usage	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_regsvr32_anomalies.yml
Windows: Regsvr32 Flags Anomaly	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_regsvr32_flags_anomaly.yml
Windows: Renamed ZOHO Dctask64	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_renamed_dctask64.yml
Windows: Renamed SysInternals Debug View	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_renamed_debugview.yml
Windows: Suspicious Process Start Locations	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_run_locations.yml
Windows: Suspicious Arguments in Rundll32 Usage	juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_rundll32_activity.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious DLL Call by Ordinal	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_rundll32_byOrdinal.yml
Windows: Scheduled Task Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_schtask_creation.yml
Windows: WSF JSE JS VBA VBE File Execution	Michael Haag	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_script_execution.yml
Windows: Suspicious Service Path Modification	Victor Sergeev, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_service_path_modification.yml
Windows: Squirrel Lolbin	Karneades / Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_squirrel_lolbin.yml
Windows: Suspicious Svchost Process	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_svchost.yml
Windows: Suspect Svchost Activity	David Burkett	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_svchost_no_cli.yml
Windows: Sysprep on AppData Folder	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_sysprep_appdata.yml
Windows: Suspicious SYSVOL Domain Group Policy Access	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_sysvol_access.yml
Windows: Taskmgr Created By Local SYSTEM Account	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_taskmgr_localsystem.yml
Windows: Process Launch from Taskmgr	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_taskmgr_parent.yml
Windows: Suspicious tscon.exe Created By Local SYSTEM Account	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_tscon_localsystem.yml
Windows: Suspicious RDP Redirect Using tscon.exe	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_tscon_rdp_redirect.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious Use of CSharp Interactive Console	Michael R. (@nahamike01)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_use_of_csharp_console.yml
Windows: Suspicious Userinit Child Process	Florian Roth (rule), Samir Bousseaden (idea)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_userinit_child.yml
Windows: Whoami Execution	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_whoami.yml
Windows: Suspicious WMI Execution	Michael Haag, Florian Roth, juju4	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_wmi_execution.yml
Windows: Sysmon Driver Unload	Kirill Kiryanov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_sysmon_driver_unload.yml
Windows: System File Execution Location Anomaly	Florian Roth, Patrick Bareiss	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_system_exe_anomaly.yml
Windows: Tap Installer Execution	Daniil Yugoslavskiy, Ian Davis, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_tap_installer_execution.yml
Windows: Tasks Folder Evasion	Sreeman	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_task_folder_evasion.yml
Windows: Terminal Service Process Spawn	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_termserv_proc_spawn.yml
Windows: Domain Trust Discovery	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community, omkar72	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_dsquery_domain_trust_discovery.yml ; https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_trust_discovery.yml
Windows: Bypass UAC via CMSTP	E.M. Anhaus (originally from Atomic Blue Detections, Endgame), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_uac_cmstp.yml

FortiSIEM Rule	Author	Source Link
Windows: Bypass UAC via Fodhelper.exe	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_uac_fodhelper.yml
Windows: Bypass UAC via WSReset.exe	E.M. Anhaus (originally from Atomic Blue Detections, Tony Lambert), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_uac_wsreset.yml
Windows: Possible Privilege Escalation via Weak Service Permissions	Teymur Kheirkhabarov	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_using_sc_to_change_service_image_path_by_non_admin.yml
Windows: Java Running with Remote Debugging	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_vul_java_remote_debugging.yml
Windows: Webshell Detection With Command Line Keywords	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_webshell_detection.yml
Windows: Webshell Recon Detection Via CommandLine Processes	Cian Heasley	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_webshell_recon_detection.yml
Windows: Shells Spawned by Web Servers	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_webshell_spawn.yml
Windows: Run Whoami as SYSTEM	Teymur Kheirkhabarov	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_whoami_as_system.yml
Windows: Windows 10 Scheduled Task SandboxEscaper 0-day	Olaf Hartong	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_win10_sched_task_0day.yml
Windows: WMI Backdoor Exchange Transport Agent	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_wmi_backdoor_exchange_transport_agent.yml
Windows: WMI Persistence - Script Event Consumer	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_wmi_persistence_script_event_consumer.yml

FortiSIEM Rule	Author	Source Link
Windows: WMI Spawning Windows PowerShell	Markus Neis / @Karneades	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_wmi_spwns_powershell.yml
Windows: Wmiprvse Spawning Process	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_wmiprvse_spawning_process.yml
Windows: Microsoft Workflow Compiler	Nik Seetharaman	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_workflow_compiler.yml
Windows: Wsreset UAC Bypass	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_wsreset_uac_bypass.yml
Windows: XSL Script Processing	Timur Zinniatullin, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_xsl_script_processing.yml
Windows: Leviathan Registry Key Activity	Aidan Bracher	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_apr_leviathan.yml
Windows: OceanLotus Registry Activity	megan201296	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_apr_oceanlotus_registry.yml
Windows: Pandemic Registry Key	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_apr_pandemic.yml
Windows: Autorun Keys Modification	Victor Sergeev, Daniil Yugoslavskiy, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_asep_reg_keys_modification.yml
Windows: Suspicious New Printer Ports in Registry CVE-2020-1048	EagleEye Team, Florian Roth, NVISO	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_cve-2020-1048.yml
Windows: DHCP Callout DLL Installation	Dimitrios Slamaris	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_dhcp_calloutdll.yml
Windows: Disable Security Events Logging Adding Reg Key MiniNt	Ilyas Ochkov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_disable_security_events_logging_adding_reg_key_minint.yml
Windows: DNS ServerLevelPluginDll Install	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_dns_serverlevelplugindll.yml

FortiSIEM Rule	Author	Source Link
Windows: COMPlus-ETWEnabled Registry Modification	Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_etw_modification.yml ; https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_etw_disabled.yml
Windows: Windows Credential Editor Install Via Registry	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_hack_wce_reg.yml
Windows: Logon Scripts UserInitMprLogonScript Registry	Tom Ueltschi (@c_APT_ure)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_logon_scripts_userinitmprlogonscript_reg.yml
Windows: Narrator s Feedback-Hub Persistence	Dmitriy Lifanov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_narrator_feedback_persistence.yml
Windows: New DLL Added to AppCertDlls Registry Key	Ilyas Ochkov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_new_dll_added_to_appcertdlls_registry_key.yml
Windows: New DLL Added to AppInit-DLLs Registry Key	Ilyas Ochkov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_new_dll_added_to_appinit_dlls_registry_key.yml
Windows: Possible Privilege Escalation via Service Permissions Weakness	Teymur Kheirkhabarov	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_possible_privilege_escalation_via_service_registry_permissions_weakness.yml
Windows: RDP Registry Modification	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_rdp_registry_modification.yml
Windows: RDP Sensitive Settings Changed	Samir Bousseaden	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_rdp_settings_hijack.yml
Windows: RedMimicry Winnti Playbook Registry Manipulation	Alexander Rausch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_redmimicry_winnti_reg.yml

FortiSIEM Rule	Author	Source Link
Windows: Office Security Settings Changed	Trent Liffick (@tliffick)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_reg_office_security.yml
Windows: Windows Registry Persistence COM Key Linking	Kutepov Anton, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_registry_persistence_key_linking.yml
Windows: Windows Registry Persistence COM Search Order Hijacking	Maxime Thiebaut (@0xThiebaut)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_registry_persistence_search_order.yml
Windows: Windows Registry Trust Record Modification	Antonlovesdnb	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_registry_trust_record_modification.yml
Windows: Security Support Provider SSP Added to LSA Configuration	iwillkeepwatch	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_ssp_added_lsa_config.yml
Windows: Sticky Key Like Backdoor Usage	Florian Roth, @twjackomo	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_stickykey_like_backdoor.yml
Windows: Suspicious RUN Key from Download	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_download_run_key.yml
Windows: DLL Load via LSASS	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_lsass_dll_load.yml
Windows: Suspicious Camera and Microphone Access	Den luzvyk	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_mic_cam_access.yml
Windows: Registry Persistence via Explorer Run Key	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_reg_persist_explorer_run.yml
Windows: New RUN Key Pointing to Suspicious Folder	Florian Roth, Markus Neis, Sander Wiebing	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_run_key_img_folder.yml
Windows: Suspicious Service Installed	xknow (@xknow_infosec), xorxes (@xor_xes)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_susp_service_installed.yml

FortiSIEM Rule	Author	Source Link
Windows: Suspicious Keyboard Layout Load	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_suspicious_keyboard_layout_load.yml
Windows: Usage of Sysinternals Tools	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_sysinternals_eula_accepted.yml
Windows: UAC Bypass via Event Viewer	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_uac_bypass_eventvwr.yml
Windows: UAC Bypass via Sdclt	Omer Yampel	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_uac_bypass_sdclt.yml
Windows: Registry Persistence Mechanisms	Karneades	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_win_reg_persistence.yml
Windows: Azure Browser SSO Abuse	Den luzvyk	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/image_load/sysmon_abusing_azure_browser_sso.yml
Windows: Executable in ADS	Florian Roth, @0xrawsec	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_ads_executable.yml
Windows: Alternate PowerShell Hosts Pipe	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_alternate_powershell_hosts_pipe.yml
Windows: Turla Group Named Pipes	Markus Neis	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_apr_turla_namedpipes.yml
Windows: CactusTorch Remote Thread Creation	@SBousseaden (detection), Thomas Patzke (rule)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_cactustorch.yml
Windows: CMSTP Execution	Nik Seetharaman	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/registry_event/sysmon_cmstp_execution.yml
Windows: CobaltStrike Process Injection	Olaf Hartong, Florian Roth, Aleksey Potapov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_cobaltstrike_process_injection.yml
Windows: CreateRemoteThread API and LoadLibrary	Roberto Rodriguez @Cyb3rWard0g	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_createremotethread_loadlibrary.yml

FortiSIEM Rule	Author	Source Link
Windows: Cred Dump Tools Via Named Pipes	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_cred_dump_tools_named_pipes.yml
Windows: Malicious Named Pipe	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_mal_namedpipes.yml
Windows: Password Dumper Remote Thread in LSASS	Thomas Patzke	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_password_dumper_lsass.yml
Windows: Possible DNS Rebinding	Ilyas Ochkov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_possible_dns_rebinding.yml
Windows: Raw Disk Access Using Illegitimate Tools	Teymur Kheirkhabarov, oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_raw_disk_access_using_illegitimate_tools.yml
Windows: PowerShell Rundll32 Remote Thread Creation	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_susp_powershell_rundll32.yml
Windows: Suspicious Remote Thread Created	Perez Diego (@darkquassar), oscd.community	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_suspicious_remote_thread.yml
Windows: WMI Event Subscription	Tom Ueltschi (@c_APT_ure)	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_wmi_event_subscription.yml
Windows: Suspicious Scripting in a WMI Consumer	Florian Roth	https://github.com/SigmaHQ/sigma/blob/master/rules/windows/sysmon/sysmon_wmi_susp_scripting.yml



www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.