OBSERVEIT INSIDER THREAT LIBRARY

FOR INTENTIONAL AND UNINTENTIONAL THREAT DETECTION

Note: This document was written for ObserveIT Enterprise version 7.0.0.

ObserveIT's Insider Threat Library contains more than 200 rules that cover common scenarios of risky user activities across operating systems, applications, and different type of users, that might generate alerts.

The Library comes with 7 built-in user lists that have common risk characteristics; they include Everyday Users, Privileged Users, Remote Vendors, Executives, Developers and DevOps, Users in Watch List, and Termination List. Each rule in the ObserveIT Insider Threat Library is assigned only to the relevant user list with the appropriate risk level. After installation, once these 7 user lists are manually populated with users and groups based on Active Directory or built-in system groups, the system is ready to go.

Some of the rules have built-in notification policies (in the form of messages displayed to end users) that are designed to increase the security awareness of users, and reduce overall company risk.

The following scenarios, combined with additional scenarios that you can easily add, construct the overall risk score of your monitored users, allowing you to:

- ✓ Enforce policies and educate users at the moment of out-of-policy or risky behavior
- ✓ Block prohibited actions attempted by users
- ✓ Automatically highlight those users performing the riskiest activities
- ✓ Discover any unfolding series of activities that are leading towards a data breach
- ✓ Fully understand what really occurred using powerful metadata and full Video recordings

Common Alert Scenarios

The following scenarios are some examples of risky user activities that might generate alerts in ObserveIT (click for details):

- ✓ **Logging-in locally or remotely to unauthorized servers by unauthorized users or from unauthorized clients**
- ✓ **Sending sensitive documents to a local/network printer during irregular hours**
- ✓ **Copying files or folders that are either sensitive or located in a sensitive location during irregular hours**
- ✓ **Connecting a USB storage device (or mobile phone) in order to copy sensitive information**
- ✓ **Using Cloud storage backup or large file-sending sites that are not allowed by company policy**
- ✓ **Running unauthorized command by non-admin user in command line tools such as CMD, PowerShell, Putty and Terminal (Mac)**
- ✓ **Typing text that contains workplace violence words that should not be used in digital communication**
- ✓ **Typing text that contains sensitive intellectual property-related words in personal communication tools such as web mail, Chat, IM or Social Media sites**
- ✓ **Storing passwords in files that can be easily detected by password harvesting tools**
- ✓ **Clicking links within emails that open Phishing websites**
- ✓ **Browsing contaminating websites with high potential security risk**
- ✓ **Browsing websites with unauthorized content (gambling, adults, etc.)**
- ✓ **Being non-productive by wasting time on Social Networks, Chat, Gaming, Shopping sites, and so on**
- ✓ **Searching the Internet for information on malicious software, such as steganography tools (for hiding text-based information within images)**
- ✓ **Accessing the Darknet using TOR browsers**
- ✓ **Performing unauthorized activities on servers, such as, running webmail or Instant Messaging services**
- ✓ **Running malicious tools such as, password cracking, port scanning, hacking tools, or non-standard SETUID programs on Linux/Unix**
- ✓ **Hiding information and covering tracks by running secured/encrypted email clients, clearing browsing history, zipping files with passwords, or tampering with audit log files**
- ✓ **Attempting to gain higher user privileges (for example, via the su or sudo commands, running an application as Administrator**
- ✓ **Performing copyright infringement by browsing copyright-violating websites or by running P2P tools**
- ✓ **Changing the root password by regular user or searching for directories with WRITE/EXECUTE permissions in preparation for an attack (on Linux/Unix)**
- ✓ **Performing IT sabotage by deleting local users or files in sensitive directories (on Linux/Unix)**
- ✓ **Creating backdoors by adding users/groups to be used later un-innocently**
- ✓ **Installing questionable or unauthorized software such as hacking/spoofing tools on either desktops or sensitive servers**
- ✓ **Accessing sensitive administration tools or configurations, such as Registry Editor, Microsoft Management Console, PowerShell, Firewall settings, etc.**
- ✓ **Adding new credential on SQL Server Management Studio that can be used later as a backdoor**

Alert Rule Categories

ObserveIT's library of rule scenarios are grouped by security categories to help navigation and facilitate their operation and maintenance.

Some categories are relevant specifically for Windows or Unix/Linux systems, and some are relevant for both systems.

Note: In addition to 26 built-in categories, you can create new security categories. You can also unassign rules from categories, and reassign them.

The following table lists the alert rule categories with an indication of whether they apply to Windows, Unix/Linux, or Windows and Unix/Linux systems. To see details about the rules that apply to each category, click the relevant √ indication.

CATEGORY	WINDOWS	UNIX/LINUX
Data Exfiltration	√	√
Data Infiltration (Bringing in Troubles)	√	
Hiding Information and Covering Tracks	√	√
Unauthorized Machine Access	√	√
Unauthorized Data Access	√	
Bypassing Security Controls	√	
Unacceptable Use	√	
Careless Behavior	√	√
Creating Backdoor	√	√
Time Fraud	√	
Unauthorized Activity on Servers	√	
Running Malicious Software	√	√
Performing Unauthorized Admin Tasks	√	√
Copyright Infringement	√	
Searching for Information	√	
Using Unauthorized Communication Tools	√	
Installing/Uninstalling Questionable Software	√	
Unauthorized Active Directory Activity	√	
Unauthorized DBA Activity	√	
Shell Attack		√
Preparation for Attack		√
Unauthorized Shell Opening		√
IT Sabotage		√
Performing Privilege Elevation		√
Identity Theft		√
System Tampering		√

Data Exfiltration (Windows)

The following out-of-the-box alert rules are assigned to the (Windows) Category: DATA EXFILTRATION

ALERT RULE	DESCRIPTION
Copying sensitive file	An alert is triggered upon copying to the clipboard files that are predefined as sensitive. This operation could indicate an intent to steal sensitive information from the organization.
Copying sensitive folder	An alert is triggered upon copying to the clipboard folders that are predefined as sensitive. This operation could indicate an intent to steal sensitive information from the organization.
Synchronizing MS-Office document with another Microsoft account	An alert is triggered upon opening the Switch Account window in Microsoft Office applications. This action could indicate an intent to send the currently opened document out of the organization to a private account.
Opening cloud storage sync folder	An alert is triggered upon opening a local folder whose content is always synchronized with a remote cloud storage service. This operation could indicate an intent to copy sensitive information to this folder in order to steal it from the organization.
Typing sensitive intellectual property related words in web mail, Chat, IM, Social Media sites	An alert is triggered upon browsing to web mail, Chat, IM or Social Media sites and typing words that are confidential from intellectual property aspects.
Performing large file or folder copy	An alert is triggered upon copying to clipboard either a large number of files/folders or files/folders whose total size exceeds the thresholds defined in Server Policy. This action could indicate an intent to steal information from the organization.
Performing large file or folder copy during irregular hours	An alert is triggered upon copying to clipboard during irregular working hours either a large number of files/folders or files/folders whose total size exceeds the thresholds defined in a Server Policy. This could indicate an intent to steal information.
Printing large number of pages during irregular hours	An alert is triggered upon sending large number of pages to a printer during irregular working hours. This action could indicate that the user is stealing information from the organization.
Printing sensitive documents	An alert is triggered upon sending to a printer one of the predefined sensitive documents. This action could indicate that the user is stealing sensitive information from the organization.
Running a cloud backup application	An alert is triggered upon running a cloud backup software that can copy files/folders to a remote location. This action could indicate an intent to steal sensitive information from the organization.

Running CD or DVD burning tools	An alert is triggered upon running a CD/DVD burning software. This operation could indicate an intent to steal sensitive information from the organization.
Uploading or sharing files via cloud storage services	An alert is triggered upon browsing to websites that offer cloud transfer or storage services, in order to potentially upload a file and share it with another person. This action could indicate an intent to steal sensitive information from the organization.

Data Exfiltration (Unix/Linux)

The following out-of-the-box alert rules are assigned to the (Unix/Linux) Category: DATA EXFILTRATION

ALERT RULE	DESCRIPTION
Retrieving configuration files via SFTP or SCP	An alert is triggered upon running the GET command of SFTP or SCP in order to retrieve files from a remote configuration directory. Note: SFTP recording always sends the full path of files even if a specific file name is provided.
Running RSYNC command on sensitive configuration directories	An alert is triggered upon running the RSYNC command within sensitive configuration directories. This command can be used to make a copy of sensitive configuration.

Data Infiltration (Bringing in Troubles)

The following out-of-the-box alert rules are assigned to the (Windows) Category: DATA INFILTRATION

ALERT RULE	DESCRIPTION
Browsing harmful, risky or contaminating sites	An alert is triggered upon browsing to websites that are categorized as risky from various security aspects.
Browsing software download sites	An alert is triggered upon browsing of websites that are dedicated for downloading software, potentially to download and then install it.
Connecting USB Storage Device	An alert is triggered upon connecting a USB storage device to the computer. This operation can indicate an intent to either steal sensitive information or to copy files/folders into the organization's assets.
Using FTP or SFTP protocol in browser	An alert is triggered upon browsing FTP/SFTP site via the browser, by using the FTP/SFTP protocol in the URL address field, potentially in order to download files/folders.

Hiding Information and Covering Tracks (Windows)

The following out-of-the-box alert rules are assigned to the (Windows) Category: HIDING INFORMATION AND COVERING TRACKS

ALERT RULE	DESCRIPTION
Clearing browsing history	An alert is triggered upon opening the settings window of Internet Explorer, Google Chrome or Firefox in order to clear the browser history data. This action could indicate that the user has something to hide.
Copying Windows event log files	An alert is triggered upon copying to the clipboard Windows event log files. This action could indicate that the user plans to overwrite event log files in order to hide his actions that are documented in these log files.
Exporting Windows Registry data	An alert is triggered upon opening Windows Registry and invoking the Export command. This action could indicate that the user plans to manipulate Windows Registry data.
Importing Windows Registry data	An alert is triggered upon opening Windows Registry and invoking the Import command. This action could indicate that the user plans to manipulate Windows Registry data.
Password protecting Excel file	An alert is triggered upon opening the General Options screen in Microsoft Excel to potentially set a password protection upon saving a file. This action could indicate that the user has something to hide.
Password protecting PowerPoint file	An alert is triggered upon opening the General Options screen in Microsoft PowerPoint to potentially set a password protection upon saving a file. This action could indicate that the user has something to hide.
Password protecting Word file	An alert is triggered upon opening the General Options screen in Microsoft Word to potentially set a password protection upon saving a file. This action could indicate that the user has something to hide.
Running secured or encrypted email client	An alert is triggered upon running a secured or encrypted email client which could be used to bring in or send out information that cannot be monitored. This action could indicate that the user behind it has something to hide.
Running steganography tools	An alert is triggered upon running one of the predefined stenography tools that are usually used to conceal text information within images, and by that to block data ex-filtration tools to detect this data leak.
Zipping file with password	An alert is triggered upon running a compression solution and setting a password protection for the compressed file. This action could indicate that the user has something to hide.

Hiding Information and Covering Tracks (Unix/Linux)

The following out-of-the-box alert rules are assigned to the (Unix/Linux) Category: HIDING INFORMATION AND COVERING TRACKS

ALERT RULE	DESCRIPTION
Audit log files tampering using almost any command	An alert is triggered upon running almost any commands (except for TAIL/CAT/SUDO) on audit log files which might prevent SIEM products from tracing hidden activity on this machine.
Audit log files tampering using specific commands	An alert is triggered upon running specific view/edit/delete/copy commands on audit log files which might prevent SIEM products from tracing hidden activity on this machine.
Editing audit log files using SUDO	An alert is triggered upon accessing audit log files using SUDO not for viewing purposes. An interactive user is allowed to access audit log files only for viewing them and not for editing.
Misusing SUDO-authorized text editor to run shell commands	An alert is triggered upon breaking out of a text editor executed via the SUDO command, by executing external commands.
Running the steganography tool CLOAKIFY	An alert is triggered upon executing CLOAKIFY.PY which is a text-based steganography tool that can be used to hide information from data leak scanning tools using list-based ciphers.

Unauthorized Machine Access (Windows)

The following out-of-the-box alert rules are assigned to the (Windows) Category: UNAUTHORIZED MACHINE ACCESS

ALERT RULE	DESCRIPTION
Logging in locally to sensitive Windows Server by unauthorized user	ACTION REQUIRED: Add users black/white list (authorized/unauthorized) in the WHO statement. An alert is triggered upon local login (accessing the machine physically) to a predefined sensitive Windows server, by an unauthorized user.
Logging in locally to sensitive Windows Desktop by unauthorized user	An alert is triggered upon local login (accessing the machine physically) to a predefined sensitive Windows desktop, by a user not included in the authorized users list for these sensitive machines.
Logging in remotely (RDP) to sensitive Windows Server during irregular hours	An alert is triggered upon remote login (via RDP session) to a predefined sensitive Windows server during irregular hours (before the beginning or after the end of a working weekday, or during weekend).
Logging in remotely (RDP) to sensitive Windows Server from unauthorized client	An alert is triggered upon remote login (via RDP session) to a predefined sensitive Windows server from a client not included in the list of authorized client IPs or client names for these sensitive machines.
Logging in remotely (RDP) to sensitive Windows Desktop by unauthorized user	ACTION REQUIRED: Add users black/white list (Authorized/Unauthorized) in the WHO statement. An alert is triggered upon remote login (via RDP session) to a predefined sensitive Windows desktop by a user not included in the predefined list.
Logging in remotely (RDP) to sensitive Windows Desktop from unauthorized client	An alert is triggered upon remote login (via RDP session) to a predefined sensitive Windows desktop from a client not included in the list of authorized client IPs or client names for these sensitive machines.
Logging in remotely (RDP) to sensitive Windows Server by unauthorized user	ACTION REQUIRED: Add users black/white list (authorized/unauthorized) in the WHO statement. An alert is triggered upon remote login (via RDP session) to a predefined sensitive Windows server by an unauthorized user.
Logging in to sensitive machine using a shared account	An alert is triggered when Secondary Authentication mode was used while the user was logged in to this machine, indicating that the primary user name was probably a shared account (e.g., Administrator).
Running a remote PC access tool	An alert is triggered upon running a remote login utility in order to take control over a remote machine, or to open a telnet/SSH session on a remote machine.

Unauthorized Machine Access (Unix/Linux)

The following out-of-the-box alert rules are assigned to the (Unix/Linux) Category: UNAUTHORIZED MACHINE ACCESS

ALERT RULE	DESCRIPTION
Leapfrogging with identity change 1	An alert is triggered upon opening a new SSH session with an identity change which could indicate an account misuse. Note: This is rule 1 out of 2 rules for this scenario.
Leapfrogging with identity change 2	An alert is triggered upon opening a new SSH session with an identity change which could indicate an account misuse. Note: This is rule 2 out of 2 rules for this scenario.
Logging in remotely to sensitive Unix or Linux machine from unauthorized client	An alert is triggered upon detecting a new login to a sensitive machine from a remote unauthorized client IP. The alert applies when the agent is installed on the machine that is being controlled (i.e., not on the controlling machine).

Unauthorized Data Access

The following out-of-the-box alert rules are assigned to the (Windows) Category: UNAUTHORIZED DATA ACCESS

ALERT RULE	DESCRIPTION
Accessing Social Media Sites from Server	An alert is triggered upon browsing to Social Media Sites on a machine that functions as a server. This action could indicate an intent to steal sensitive information from the server, or to download files/folders to this server.
Invoking Mac authentication service dialog	An alert is triggered upon performing an action on Mac that requires administrative privileges to be set via the authentication service dialog.
Accessing unauthorized folder	An alert is triggered upon opening in Windows Explorer a folder which is included in black-listed unauthorized folders.
Trying to access a system that requires credentials	An alert is triggered whenever the Windows Security popup that prompts for entering credentials is displayed to the user. This happens upon trying to access a web-based system or a folder that requires credentials.

Bypassing Security Controls

The following out-of-the-box alert rules are assigned to the (Windows) Category: BYPASSING SECURITY CONTROLS

ALERT RULE	DESCRIPTION
Accessing the Darknet using TOR (The Onion Router)	An alert is triggered upon running TOR (The Onion Ring) browser in order to access the TOR network (the Dark Web). Such an operation could indicate that a user wants to hide his identity while performing illegal activity.
Adding Windows Firewall Rules	An alert is triggered upon opening the built-in Windows Add New Rule screen in Firewall settings to define a new rule.
Changing computer data or time	An alert is triggered upon opening the built-in Windows date and time settings screen potentially to change the time or data, in order to manipulate the documentation of user actions or to avoid expiration of time-limited software license.
Configuring Windows Firewall Status	An alert is triggered upon opening the built-in Windows Firewall settings screen, potentially to turn off the settings before performing incoming or outgoing networking that is usually blocked by Firewall.
Configuring Windows LAN or Proxy Settings	An alert is triggered upon opening the built-in Windows LAN/Proxy settings screen, potentially to configure internet access through a 3rd party in order to hide the IP or identity of the user.
Configuring Windows VPN Connection	An alert is triggered upon opening the built-in Windows VPN settings screen, potentially to configure access to a private network that would not be available otherwise.
Creating a new virtual machine instance	An alert is triggered upon creating a new virtual machine instance in one of the predefined virtualization solutions.
Logging in with local user account	An alert is triggered upon performing login with a domain name which is not included in predefined domains. Such a login is usually a local user login in which the domain name is the machine name (typical to laptops disconnected from an organization's network).
Running VPN, Proxy or Tunneling tools	An alert is triggered upon running advanced networking tools either to enable access to private networks or to hide the user identity.

Unacceptable Use

The following out-of-the-box alert rules are assigned to the (Windows) Category: UNACCEPTABLE USE

ALERT RULE	DESCRIPTION
Typing workplace violence words	An alert is triggered upon typing a sensitive word that is included in a list of workplace violence words.
Browsing Adult sites	An alert is triggered upon browsing to websites with adult content.
Browsing Dynamic DNS sites	An alert is triggered upon browsing to websites offering Dynamic DNS services, that automatically update DNS servers with the frequently changing IP associated with a specific domain name. This action could indicate that the user is trying to hide his IP.
Browsing Gambling sites	An alert is triggered upon browsing to gambling websites, which can affect employee productivity and also indicate an employee with addiction issues or financial debt.
Browsing hacking, key loggers or password-cracking sites	An alert is triggered upon browsing to websites related to hacking tools, key loggers, or password cracking tools. This action could indicate that the user has plans to obtain access to sensitive information.
Browsing Illegal activities, violence or hate sites	An alert is triggered upon browsing to websites related to illegal activities, violence, hate, terrorism and weapons.
Browsing Illegal drugs sites	An alert is triggered upon browsing to websites related to illegal drugs.
Browsing remote proxies' sites	An alert is triggered upon browsing to websites related to remote proxies. This action could indicate that the user is trying to make indirect network connections to other network services while changing his real identity.
Running Bitcoin mining tools	An alert is triggered upon running various tools for Bitcoin mining. As this is a digital payment system and a currency, a high computing power is required for this resource-intensive process. This action indicates usage of IT resources for private needs.

Careless Behavior (Windows)

The following out-of-the-box alert rules are assigned to the (Windows) Category: CARELESS BEHAVIOR

ALERT RULE	DESCRIPTION
Browsing Phishing sites	An alert is triggered upon browsing to websites that have been analyzed and detected as Phishing websites that try to steal the credentials of users by presenting an imitation of legitimate websites.
Enabling Windows Remote Assistance	An alert is triggered upon opening the Windows Remote Assistance dialog that is built in to the Windows Operating System. This action could indicate that the user plans to grant access to this machine to a remote user.
Running program with invalid digital signature	An alert is triggered whenever Windows Operating System detects opening a file with an invalid digital signature. This usually happens upon running either files downloaded from Internet or files executed directly from a remote machine (using UNC).
Running software to enable sharing and remote access	An alert is triggered upon running applications that enable desktop sharing with remote computers or applications that allow remote computers to access and control the computer.
Storing passwords in clear text	An alert is triggered upon detecting a potential user that stores passwords in a file that is named using the word PASSWORD (or its variants). As a bad security practice, such file names are searched for by malicious codes for password harvesting.

Careless Behavior (Unix/Linux)

The following out-of-the-box alert rule is assigned to the (Unix/Linux) Category: CARELESS BEHAVIOR

ALERT RULE	DESCRIPTION
Getting content from remote location	An alert is triggered upon downloading or getting content/files from a remote location using a WGET/CURL/SFTP/SCP command. Such files can be risky as they could include commands that can run without proper verification.

Creating Backdoor (Windows)

The following out-of-the-box alert rules are assigned to the (Windows) Category: CREATING BACKDOOR

ALERT RULE	DESCRIPTION
Adding a local Windows User or Group	An alert is triggered upon opening the Local Users and Groups screen potentially in order to add a local user. Such an operation could indicate a potential security backdoor to be exploited at a later date.
Enabling unauthorized access via Network Policy Server	An alert is triggered upon invoking Windows Network Policy Server which can be used to enable unauthorized access to or from a specific machine.
Changing user password from Windows MMC	An alert is triggered upon opening the Reset Password built-in Windows screen in order to change a password. Such an operation can be exploited by a user who can physically access another user's machine to change the user password.
Resetting the password of an Active Directory user	An alert is triggered upon opening the Reset Password dialog of Active Directory in order to reset a user's password. This action could indicate an intent to exploit a potential security backdoor by logging in to systems using the credentials of another user.
Creating a new user in Active Directory	An alert is triggered upon opening the Active Directory screen that is used for creating a new user. This action could indicate a potential security backdoor to be exploited at a later date.

Creating Backdoor (Unix/Linux)

The following out-of-the-box alert rules are assigned to the (Unix/Linux) Category: CREATING BACKDOOR

ALERT RULE	DESCRIPTION
Adding a local user	An alert is triggered upon running the USERADD command to add a regular or power user locally on a machine. Such a local user is not exposed at the network level as are other users, and could pose a risk to system security.
Adding a local user with a duplicated user ID	An alert is triggered upon adding a new user (via USERADD command) with the user ID (UID) of another user that already exists on the system. The new user can log in using his own password and perform actions as if they were performed by another user.
Changing a program to a SETUID program	An alert is triggered upon trying to change a program to be a SETUID program (via CHMOD command) which can provide root permissions.
Modifying root cron job	An alert is triggered upon using the CRONTAB command with the -e option with root permissions, in order to modify cron jobs. This could enable potential backdoor user activity.

Time Fraud

The following out-of-the-box alert rules are assigned to the (Windows) Category: TIME FRAUD

ALERT RULE	DESCRIPTION
Browsing Chat (IRC) sites	An alert is triggered upon browsing to Chat (IRC) websites which can affect employee productivity and also be used to send out sensitive information.
Browsing competitor sites	An alert is triggered upon browsing to the organization's competitors' websites. This action could indicate that the user is looking for a position outside the organization.
Browsing Gaming sites	An alert is triggered upon browsing to gaming websites as this can affect employee productivity.
Browsing IM sites	An alert is triggered upon browsing to Instant Messaging websites, which can affect employee productivity and also be used to send out sensitive information.
Browsing Job Searching sites	An alert is triggered upon browsing to websites dedicated to job searching, including employment agencies, recruitment consultancies, head hunters, CV and career advice. This action could indicate that the user plans to leave the organization.
Browsing Music sites	An alert is triggered upon browsing to music websites as this can affect employee productivity.
Browsing News sites	An alert is triggered upon browsing to news websites as this can affect employee productivity.
Browsing Shopping sites	An alert is triggered upon browsing to shopping websites as this can affect employee productivity.
Browsing Social Media sites	An alert is triggered upon browsing to social media websites as this can seriously affect employee productivity.
Browsing Sports sites	An alert is triggered upon browsing to sports websites as this can affect employee productivity.
Browsing Streaming media sites	An alert is triggered upon browsing to streaming media websites as this can affect employee productivity.
Browsing counter-productivity sites	An alert is triggered upon browsing to various counter-productivity websites (such as dating, travelling, dining, horoscope, fashion, and more) as this can affect employee productivity.

Unauthorized Activity on Servers

The following out-of-the-box alert rules are assigned to the (Windows) Category: UNAUTHORIZED ACTIVITY ON SERVERS

ALERT RULE	DESCRIPTION
Accessing Social Media Sites from Server	An alert is triggered upon browsing to Social Media Sites on a machine that functions as a server. This action could indicate an intent to steal sensitive information from the server or to download files/folders to this server.
Installing software on Server	An alert is triggered upon running software installations on a machine that functions as a server. Usually servers are installed only with applications that are critical for performing their business tasks.
Running unauthorized email or webmail on Server	An alert is triggered upon running either a desktop email client or webmail (via a browser) on a machine that functions as a server. This operation could indicate an intent to take out sensitive information from the server or to download files.
Running unauthorized Instant Messaging application on Server	An alert is triggered upon running an Instant Messaging application on a machine that functions as a server. This operation could indicate an intent to steal sensitive information from the server or to download files/folders to this server.

Running Malicious Software (Windows)

The following out-of-the-box alert rules are assigned to the (Windows) Category: RUNNING MALICIOUS SOFTWARE

ALERT RULE	DESCRIPTION
Running hacking or spoofing tools	An alert is triggered upon running one of the predefined hacking or spoofing tools on a Windows system that can be used to gain access to restricted areas or to create damage to the organization's assets.
Running password cracking tools	An alert is triggered upon running one of the predefined password cracking tools that can be used to try and break a password-protected file with potentially sensitive information.
Running port scanning tools	An alert is triggered upon running one of the predefined port scanning tools that can be used as a port scanning attack to gain knowledge about which services are running on a specific machine, and what is the installed OS.

Running Malicious Software (Unix/Linux)

The following out-of-the-box alert rules are assigned to the (Unix/Linux) Category: RUNNING MALICIOUS SOFTWARE

ALERT RULE	DESCRIPTION
Running a malicious command	An alert is triggered upon running a predefined malicious command. (It is suggested that you periodically review the malicious commands list.)
Running hacking or spoofing tools on Linux	An alert is triggered upon running one of the predefined hacking or spoofing tools on a Linux system that can be used to gain access to restricted areas or to create damage to the organization assets.
Running a non-standard SETUID program	An alert is triggered upon detecting the execution of a SETUID program which is not included in the standard SETUID programs.
Running the NC (netcat) utility	An alert is triggered upon running the NC utility (netcat) that can be used to perform advanced networking actions, such as opening TCP connections, sending UDP packets, and scanning ports.

Performing Unauthorized Admin Tasks (Windows)

The following out-of-the-box alert rules are assigned to the (Windows) Category: PERFORMING UNAUTHORIZED ADMIN TASKS

(See also Bypassing Security Controls for some similar alert rules)

ALERT RULE	DESCRIPTION
Editing Registry Editor entry	An alert is triggered upon opening various edit dialogs of the Windows Registry Editor. This action could indicate that the user plans to make changes in a Registry key which usually should not be done by a non-Administrator user.
Editing User Account Control (UAC) Settings	An alert is triggered upon opening the User Account Control settings screen potentially to change the settings (i.e., when to get notifications from the operating system on programs that are about to make changes on a machine).
Granting full access to Office 365 mailbox	An alert is triggered upon using Office 365 web interface, opening the access settings window and granting full access to a user for a specific Outlook mailbox. This action should not be done by non-Administrators.
Opening Registry Editor	An alert is triggered upon invoking the Windows Registry Editor which usually should not be used by a non-Administrator user due to its sensitivity to changes.
Running Command Line Shell programs	An alert is triggered upon running one of the command line shell programs (CMD, PowerShell) which are powerful utilities to make changes in the system.
Running Command Line Shell programs as Administrator (See also Performing Privilege Elevation for similar alert rules)	An alert is triggered upon running one of the command line shell programs (CMD, PowerShell) as an Administrator, as these are very powerful utilities for making changes in the system when launched with Administrator privileges.
Running DBA tools	An alert is triggered upon running one of the predefined DBA tools that can be used to read sensitive information, to make changes, or to delete it.
Running Windows management tools	An alert is triggered upon running one of the predefined Windows built-in management tools (such as MMC and MSCONFIG). This action could indicate that the user plans to make changes to the system settings.
Running unauthorized command by admin in command line tools	An alert is triggered upon running a command line tool and invoking a command which should not be executed by privileged users.
Running unauthorized command by non-admin user in command line tools	An alert is triggered upon running a command line tool and invoking a command which should not be executed by non-admin users.

Performing Unauthorized Admin Tasks (Unix/Linux)

The following out-of-the-box alert rules are assigned to the (Unix/Linux) Category: PERFORMING UNAUTHORIZED ADMIN TASKS

ALERT RULE	DESCRIPTION
Editing the SUDOERS file	An alert is triggered upon trying to edit the SUDOERS file which can grant unauthorized root permissions for users (as the SUDOERS file grants root permissions to run specific commands).
Running IPTABLES command	An alert is triggered upon running the IPTABLES command that can be used to setup, maintain, or inspect the tables of IPv4 packet filter rules in the kernel.
Running management commands on system services	An alert is triggered upon using the SERVICE or CHKCONFIG commands to view or change system services.
Viewing cron job content	An alert is triggered upon trying to view the content of cron jobs using CRONTAB.

Copyright Infringement

The following out-of-the-box alert rules are assigned to the (Windows) Category: COPYRIGHT INFRINGEMENT

ALERT RULE	DESCRIPTION
Browsing copyright-violating sites	An alert is triggered upon browsing websites that support violation of copyrighted content such as movies and music.
Running license cracking or license key generator tool	An alert is triggered upon running license cracking tools or key generator tools in order to activate software without purchasing a valid license. This operation can expose an organization to actions against copyright-violation.
Running P2P tools to get or share copyrighted media	An alert is triggered upon running P2P (Peer to Peer) tools to either share or consume content that can be copyrighted and can expose organizations to actions against copyright-violation.

Searching for Information

The following out-of-the-box alert rules are assigned to the (Windows) Category: SEARCHING FOR INFORMATION

ALERT RULE	DESCRIPTION
Searching sensitive files or folders	An alert is triggered upon invoking the built-in search of Windows Explorer on a predefined sensitive file or folder name.
Searching data on hacking or spoofing	An alert is triggered upon searching predefined keywords (including the name of tools) related to hacking or spoofing tools in web search engines.
Searching data on monitoring or sniffing	An alert is triggered upon searching predefined keywords (including the name of tools) related to monitoring or sniffing tools in web search engines.
Searching data on VPN, Proxy or Tunneling	An alert is triggered upon searching predefined keywords (including the name of tools) related to VPN, proxy, or tunneling tools in web search engines.
Searching data on Dynamic-DNS	An alert is triggered upon searching predefined keywords (including the name of tools) related to Dynamic-DNS tools in web search engines.
Searching data on password cracking	An alert is triggered upon searching predefined keywords (including the name of tools) related to password cracking tools in web search engines.
Searching data on Darknet's TOR (The Onion Router)	An alert is triggered upon searching predefined keywords (including the name of tools) related to TOR (The Onion Router) which is included in the Darknet in web search engines.
Searching data on file transfer (FTP or SFTP)	An alert is triggered upon searching predefined keywords including the name of tools) related to FTP/SFTP tools in web search engines.
Searching data on Remote Access and Desktop Sharing	An alert is triggered upon searching predefined keywords (including the name of tools) related to remote access and desktop sharing tools in web search engines.
Running advanced monitoring or sniffing	An alert is triggered upon running a monitoring or sniffing tool which is part of a predefined list. The usage of such tools could indicate a user attempt to obtain information which might be sensitive.
Searching for technical information on the ObserveIT monitoring solution	An alert is triggered upon browsing to the ObserveIT website, the official ObserveIT documentation, or upon opening the folder in which the product is installed. Any of these actions could potentially indicate an attempt to tamper with the monitoring solution.

Searching data on steganography	An alert is triggered upon searching predefined keywords (including the name of tools) related to steganography tools in web search engines. Such tools are usually used to conceal text information within images, and by doing this block data exfiltration tools to detect the data leak.
Browsing information outlets (WikiLeaks-like)	An alert is triggered upon browsing to information-leak websites such as WikiLeaks in order to either publish or read sensitive information.

Using Unauthorized Communication Tools

The following out-of-the-box alert rules are assigned to the (Windows) Category: USING UNAUTHORIZED COMUNICATION TOOLS

ALERT RULE	DESCRIPTION
Accessing unauthorized Social Networks	An alert is triggered upon browsing to blacklisted social networks.
Running unauthorized IM tools	An alert is triggered upon running blacklisted Instant Messaging tools.
Running unauthorized email or webmail	An alert is triggered either upon running blacklisted email clients or browsing to blacklisted webmail services.

Installing/Uninstalling Questionable Software

The following out-of-the-box alert rules are assigned to the (Windows) Category: INSTALLING/UNINSTALLING QUESTIONABLE SOFTWARE

ALERT RULE	DESCRIPTION
Installing advanced monitoring tools	An alert is triggered upon running the installation file of a predefined advanced monitoring tool in order to reveal information that could be sensitive.
Installing Dynamic-DNS tools	An alert is triggered upon running the installation file of a predefined Dynamic-DNS tool in order to hide an identity.
Installing file transfer applications	An alert is triggered upon running the installation file of an FTP/SFTP desktop application that can be used to transfer files/folders.
Installing hacking or spoofing tools	An alert is triggered upon running the installation file of a predefined hacking or spoofing tool that can be used to gain access to a restricted area or cause damage to an organization's assets.
Installing non-standard software	An alert is triggered upon running an installation file which is not included in the permitted software for installation.

Installing P2P file sharing tools	An alert is triggered upon running the installation file of a peer-to-peer (P2P) application that can be used to share/use content that might be copyrighted, insert malicious content, or steal sensitive information.
Installing password cracking tools	An alert is triggered upon running an installation file of a predefined password cracking tool, in order to try and break a password-protected file with potentially sensitive information.
Installing Remote Access and Sharing Desktop tools	An alert is triggered upon running an installation file of a remote PC access or other desktop sharing application that could be used to take control of a machine remotely or take control of another remote machine.
Installing secured or encrypted email client	An alert is triggered upon running an installation file of a secured or encrypted email client which could be used to transfer information that cannot be monitored. This action could indicate that the user has something to hide.
Installing TOR (The Onion Router) tools	An alert is triggered upon running an installation file of a predefined TOR tool such as TOR browser in order access the Dark Web. This action could indicate that a user wants to hide his identity while performing illegal activity.
Installing unauthorized cloud backup applications	An alert is triggered upon running an installation file of a blacklisted cloud backup application that could be used to insert malicious software or steal sensitive information.
Installing unauthorized cloud transfer applications	An alert is triggered upon running an installation file of a blacklisted cloud transfer application that could be used to insert malicious software or steal sensitive information.
Installing unauthorized email client or Instant Messenger	An alert is triggered upon running an installation file of an email client or Instant Messaging application that is not authorized.
Installing virtualization solution	An alert is triggered upon running an installation file of various predefined virtualization solutions. This action could indicate that the user is trying to perform activity on a virtual machine that will be destroyed later leaving no traces.
Installing VPN, Proxy or Tunneling tools	An alert is triggered upon running an installation file of a predefined VPN/Proxy/Tunneling tool that can be used to gain access to a restricted area or hide the real identity of a user.
Uninstalling a program on Windows Desktop	An alert is triggered upon running the uninstallation of any software on a machine that functions as a desktop.
Uninstalling a program on Windows Server	An alert is triggered upon running the uninstallation of any software on a machine that functions as a server.

Unauthorized Active Directory Activity

The following out-of-the-box alert rules are assigned to the (Windows) Category: UNAUTHORIZED ACTIVE DIRECTORY ACTIVITY

ALERT RULE	DESCRIPTION
Adding new Group object in Active Directory	An alert is triggered upon adding new object from type Group in Active Directory.
Adding new InetOrgPerson object in Active Directory	An alert is triggered upon adding new object from type InetOrgPerson in Active Directory.
Adding new msDS-ResourcePropertyList object in Active Directory	An alert is triggered upon adding new object from type msDS-ResourcePropertyList in Active Directory.
Adding new msImaging-PSPs object in Active Directory	An alert is triggered upon adding new object from type msImaging-PSPs in Active Directory.
Adding new msMQ-Custom-Recipient object in Active Directory	An alert is triggered upon adding new object from type msMQ-Custom-Recipient in Active Directory.
Adding new Printer object in Active Directory	An alert is triggered upon adding new object from type Printer in Active Directory.
Adding new Shared Folder object in Active Directory	An alert is triggered upon adding new object from type Shared Folder in Active Directory.
Adding group membership to Active Directory user	An alert is triggered upon clicking the **Add** button in the **Member Of** tab within the properties dialog of an Active Directory user, in order to add groups in which the user will be a member.
Adding members to Active Directory group	An alert is triggered upon clicking the **Add** button in the **Members** tab in the properties dialog of an Active Directory group, in order to add users, contacts, computers, service accounts and groups.
Opening Active Directory object properties for viewing or changing	An alert is triggered upon opening the properties dialog of an Active Directory object in order to view or change its properties.

Unauthorized DBA Activity

The following out-of-the-box alert rules are assigned to the (Windows) Category: UNAUTHORIZED DBA ACTIVITY

ALERT RULE	DESCRIPTION
Executing SQL update command	An alert is triggered upon executing SQL command that includes the keyword update. This operation is highly sensitive, as it changes content within database tables.
Opening Server Properties window on SQL Server Management Studio	An alert is triggered upon opening the Server Properties window on SQL Server Management Studio.
Adding new Login ID on SQL Server Management Studio	An alert is triggered upon opening the New Login window on SQL Server Management Studio.
Deleting object on SQL Server Management Studio	An alert is triggered upon opening the Delete Object window on SQL Server Management Studio.
Detaching database on SQL Server Management Studio	An alert is triggered upon opening the Detach Database window on SQL Server Management Studio.
Backing up database on SQL Server Management Studio	An alert is triggered upon opening the Back Up Database window on SQL Server Management Studio.
Copying database on SQL Server Management Studio	An alert is triggered upon opening the Copy Database window on SQL Server Management Studio.
Exporting database or tables on SQL Server Management Studio	An alert is triggered upon invoking exporting functions on SQL Server Management Studio.
Adding new Server Role on SQL Server Management Studio	An alert is triggered upon opening the New Server Role window on SQL Server Management Studio.
Adding new Credential on SQL Server Management Studio	An alert is triggered upon opening the New Credential window on SQL Server Management Studio.

Preparation for Attack

The following out-of-the-box alert rules are assigned to the (Unix/Linux) Category: PREPARATION FOR ATTACK

ALERT RULE	DESCRIPTION
Building a software package on production servers	An alert is triggered upon running build commands using GCC/GMAKE on servers in the Production environment, which might indicate an intent for attack.
Changing root password by regular user	An alert is triggered upon trying to change the root password by a regular user using the PASSWD command.
Changing root password by root user	An alert is triggered upon trying to change the root password by a root user using the PASSWD command.
Searching files with advanced permissions	An alert is triggered upon searching (using the FIND command) files with advanced permissions such as sticky bits, SUID, and GUID.
Searching for directories with WRITE or EXECUTE permissions	An alert is triggered upon searching (using the FIND command) directories with WRITE and EXECUTE permissions, to potentially copy to them malicious utilities and then execute them.
Searching for installed network tools	An alert is triggered upon searching (using the FIND command) utilities that can be used to download content from remote networks.
Searching for programming languages	An alert is triggered upon searching (using the FIND command) for programming languages such as C/Perl/Python/Java that are already installed on the machine.
Viewing scheduled cron job tasks	An alert is triggered upon trying to view cron configuration files.

Shell Attack

The following out-of-the-box alert rules are assigned to the (Unix/Linux) Category: SHELL ATTACK

ALERT RULE	DESCRIPTION
Opening a reverse shell	An alert is triggered upon detecting a login of an application (such as a web server) that does not normally perform login tasks. It can indicate a potential attack.
Opening root shell by a non-standard command	An alert is triggered upon detecting the opening of a root shell by a non-authorized command.
Opening root shell using SUDO command from script	An alert is triggered upon executing the SUDO command from within a script, which allows executing programs with security privileges of regular users or super users.

Unauthorized Shell Opening

The following out-of-the-box alert rules are assigned to the (Unix/Linux) Category: UNAUTHORIZED SHELL OPENING

ALERT RULE	DESCRIPTION
Opening a shell by unauthorized application user	An alert is triggered upon detecting a login of an unauthorized application user such as apache web server (that is authorized to run a web server but not to open a shell).
Opening an interactive shell by Apache	An alert is triggered upon detecting an interactive shell that is opened by Apache web server. This rule is an example of a Prevent Rule on login (by catching any executed command). This rule will not trigger any alert until it is activated.
Opening root shell using SUDO command	An alert is triggered upon executing the SUDO command which allows executing programs with security privileges of regular users or super users.

IT Sabotage

The following out-of-the-box alert rules are assigned to the (Unix/Linux) Category: IT SABOTAGE

ALERT RULE	DESCRIPTION
Deleting a local user	An alert is triggered upon deleting a local user, which is either a regular user or super user, using the USERDEL command.
Deleting files from sensitive directory	An alert is triggered upon trying to delete (via the RM command) files from within a sensitive directory which could jeopardize system stability or result in data loss.
Overwriting files using SFTP or SCP in sensitive configuration directories	An alert is triggered upon running the PUT command of SFTP or SCP in order to copy files to a remote sensitive configuration directory.

Performing Privilege Elevation

The following out-of-the-box alert rules are assigned to the (Unix/Linux) Category: PERFORMING PRIVILEGE ELEVATION

ALERT RULE	DESCRIPTION
Changing permission to super user	An alert is triggered upon trying to change permissions using SU or SUDO commands to super user permissions in order to access sensitive information and perform sensitive actions.
Running SU command by non-admin user	An alert is triggered upon running the SU command by a user who is not a member of the unix_admins group. This rule is an example of a Prevent Rule that results in blocking the command. This rule will not trigger any alert until it is activated.
Running SU command to open root shell without root password	An alert is triggered upon running the command SUDO SU in order to open a root shell without being asked for the root password.
Using internal SUDO command suspiciously	An alert is triggered upon running a command from within another unauthorized command executed by SUDO. This rule is an example of an Alert Rule that pops up a Warning Notification to the end user. This rule will not trigger any alert until it is activated.

Identity Theft

The following out-of-the-box alert rules are assigned to the (Unix/Linux) Category: IDENTITY THEFT

ALERT RULE	DESCRIPTION
Changing own password by currently logged in user	An alert is triggered upon trying to change the password of the currently logged-in user (using the PASSWD command) potentially to steal his identity.
Copying or viewing SSH keys	An alert is triggered upon detecting the copying or viewing of SSH keys files of another user in order to steal the identity of a user.

System Tampering

The following out-of-the-box alert rules are assigned to the (Unix/Linux) Category: SYSTEM TAMPERING

ALERT RULE	DESCRIPTION
Editing sensitive system configuration files	An alert is triggered upon running editing tools in order to view or modify sensitive configuration files located under the /ETC directory.
Prevent access to ObserveIT protection policy files	An alert is triggered upon trying to manipulate (READ/WRITE) ObserveIT internal protection policy files. This rule is an example of a Prevent Rule on executing a command with specific arguments. This rule will not trigger any alert until it is activated.