OBSERVEIT INSIDER THREAT LIBRARY

FOR INTENTIONAL AND UNINTENTIONAL THREAT DETECTION

Note: This document was written for ObserveIT Enterprise version 7.8.x.

ObserveIT's Insider Threat Library contains hundreds of pre-configured rules that cover common scenarios of risky user activity across operating systems, applications, and different type of users, that might generate alerts.

The Library comes with built-in user lists that have common risk characteristics including Everyday Users, Privileged Users, Remote Vendors, Executives, Developers and DevOps, Disabled Users, 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 you populate these user lists with users and groups based on Active Directory or built-in system groups, the ObserveIT 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.

Table of Contents

Common Alert Scenarios

The following scenarios are some examples of risky user activities that might generate alerts in ObserveIT (click to see alerts that address each scenario):

- ✓ **Exfiltrating (by copying/moving) a downloaded file to a local sync folder of popular cloud storage services (Dropbox, Box, Google Drive, Apple iCloud Drive, Microsoft OneDrive)**
- ✓ **Exporting data from enterprise web application by downloading or exporting a file**
- ✓ **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**
- ✓ **Downloading file from infected/malicious/copyright-violating website that can put the organization at risk**
- ✓ **Downloading software from websites dedicated for downloads (e.g. CNET Download)**
- ✓ **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**
- ✓ **Copying to clipboard any text or text that contains predefined keywords from sensitive desktop or web applications**
- ✓ **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)**
- ✓ **Running TOR browser 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**
- ✓ **Opening AirDrop folder on Mac, potentially to exfiltrate or bring in data**

Alert Rule Categories

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

Categories apply to Windows, Mac, or Unix/Linux systems; some are relevant for all systems.

Note: In addition to the 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 which operating systems they apply to. To see details about the rules that apply to each category, click the relevant √ indication.

CATEGORY	WINDOWS/MAC	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		√

CATEGORY	WINDOWS/MAC	UNIX/LINUX
IT Sabotage		√
Performing Privilege Elevation		√
Identity Theft		√
System Tampering		√
Messing with ObserveIT Components	√	√
GIT Suspicious Activity	√	√
Docker and Containers Suspicious Activity		√

Data Exfiltration (Windows/Mac)

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.
Exporting data from enterprise web application by file downloading	An alert is triggered upon downloading a file from a list of sensitive enterprise web applications.
Copying any text from sensitive web application	An alert is triggered upon copying to the clipboard any text from a predefined sensitive web application.
Copying any text from sensitive desktop application	An alert is triggered upon copying to the clipboard any text from a predefined sensitive desktop application.
Copying predefined keyword from sensitive web application	An alert is triggered upon copying to the clipboard a predefined keyword from a predefined sensitive web application.
Copying predefined keyword from sensitive desktop application	An alert is triggered upon copying to the clipboard a predefined keyword from a predefined sensitive desktop application.
Opening AirDrop sharing folder on Mac	An alert is triggered upon opening a local folder that allows sharing with a remote device. This operation can indicate an early intent to copy sensitive information to other devices to

ALERT RULE	DESCRIPTION
Note: This rule applies specifically on Mac systems.	exfiltrate it from the organization.
Opening cloud storage sync folder on Mac Note: This rule applies specifically on Mac systems.	An alert is triggered upon opening a local folder in which content is always synchronized with a remote cloud storage service. This operation can indicate an early intent to copy sensitive information to this folder to exfiltrate it from the organization.
Running Android File Transfer on Mac Note: This rule applies specifically on Mac systems.	An alert is triggered upon using the Android File Transfer application on Mac. This operation can indicate an early intent to copy sensitive information to a private phone to exfiltrate 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.
Exfiltrating tracked file to a cloud sync folder or any web file	An alert is triggered when any user moves or copies a tracked file (downloaded or exported from the web) to a cloud storage sync folder.
Exfiltrating tracked file to the web by uploading	An alert is triggered when any user uploads a tracked (downloaded or exported from the web) file to any website or web-application.

ALERT RULE	DESCRIPTION
Exfiltrating a file to the web by uploading	An alert is triggered when any user uploads any file from any origin to any website or web-application.
Copying any text from a sensitive file	An alert is triggered when any user copies text from a file in the list named “Sensitive files”.
Uploading files to a web site using curl on Mac	An alert is triggered when any user on a Mac endpoint attempts to use curl to upload a file to any website.
Browsing for files to be inserted as an attachment in Outlook	An alert is triggered when any user browses for a file to be inserted as an attachment to an Outlook email message.
Copying credit card number to the clipboard	An alert is triggered when a credit card number is copied to the clipboard.
Exfiltrating sensitive data via SFTP, SCP or RSYNC to Amazon	An alert is triggered when any user attempts to exfiltrate sensitive data via SFTP, SCP or RSYNC to Amazon.
Exfiltrating a file to an unlisted USB device	An alert is triggered upon exfiltrating a file (both tracked file and non-tracked file) to an unlisted USB device. Note that this rule will not be triggered for files named in the exclusion list: Excluded file names for alerts on exfiltration.
Connecting unlisted USB device	An alert is triggered upon either insertion of a USB device or detecting an already connected USB device which is not part of the white listed USB devices. Note that this alert is relevant only for agents from version 7.7 onward.
Connecting USB Storage Device (before 7.7)	An alert is triggered upon connecting a USB storage device to the computer with an agent older than version 7.7. This operation can indicate an early intent to either take out sensitive information or to copy files/folders into the organization assets.
Connecting white listed or ignored USB device	An alert is triggered upon either insertion of a USB device or detecting an already connected USB device which is either white listed or exists in the ignored list.
Taking screenshot using keyboard shortcut	An alert is triggered upon taking screenshots on Windows or Mac via the relevant keyboard shortcuts in each operating system.
Pasting files copied from sensitive folders	An alert is triggered upon pasting files or folders that were originally copied from a folder that appears in the list of sensitive folders.
Pasting sensitive files or folders	An alert is triggered upon pasting files or folders that are part of the list of sensitive files or the list of sensitive folders.
Pasting text into sensitive web application	An alert is triggered upon performing paste of text into a web application (by site name) that is part of the list of sensitive web applications for pasting text into them.
Pasting text into sensitive desktop application	An alert it triggered upon performing paste of text into application (by Process Name) that is part of the list of sensitive desktop applications for pasting text into them.
Pasting text that contains predefined sensitive keywords	An alert is triggered upon pasting text that contains keywords that are part of the list of sensitive keywords to be monitored for copy & paste.

ALERT RULE	DESCRIPTION
Pasting text that contains predefined sensitive keywords	An alert is triggered upon pasting text that contains keywords that are part of the list of sensitive keywords to be monitored for copy & paste.
Pasting screenshot or image into sensitive web application	An alert is triggered upon performing paste of screenshot or image into web application (by site name) that is part of the list of sensitive web applications for pasting text or images into them.
Pasting screenshot or image into sensitive desktop application	An alert is triggered upon performing paste of screenshot or image into desktop application (Accessing cloud services for upload and sharing by Process Name) that is part of the list of sensitive desktop applications for pasting text or images into them.
Accessing upload and sharing cloud 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 can indicate an intent to remove sensitive information from the organization.
Sending email with sensitive keywords in Subject to untrusted domain	This alert will be triggered upon sending out email that contains in the Subject a sensitive keyword (that appears in a dedicated list), and where the list of recipients includes at least one recipient in an untrusted domain.
Sending email with large file attachment to untrusted domain	This alert will be triggered upon sending out email to at least one untrusted domain with file attachment which is larger than predefined value (5MB by default).
Sending email with sensitive file attachment to untrusted domain	This alert will be triggered upon sending out email with file attachment whose name is within the predefined list of sensitive files, and where at least one of the recipients is within untrusted domain.
Saving email file attachment to a local sync folder	This alert will be triggered upon saving a file attachment from email client directly to one of the supported local sync folders.
Saving email file attachment to a USB storage device	This alert will be triggered upon saving a file attachment from email client directly to a USB storage device.

Data Exfiltration (Unix/Linux)

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

ALERT RULE	DESCRIPTION
Prevent exfiltration of SSH or SSHD configuration files or keys via SFTP	An alert is triggered when SSH or SSHD configuration files or keys are exfiltrated via SFTP.
Prevent exfiltration of Passwd, Group, Shadow, Profile files via SFTP	An alert is triggered when Passwd, Group, Shadow or Profile files are exfiltrated via SFTP.
Potential backdoor data exfiltration using ICMP	An alert is triggered when a user attempts to exfiltrate system information using PING.
Exfiltrating data via email using TELNET	An alert is triggered upon running TELNET to send out an email from the server.

ALERT RULE	DESCRIPTION
Running SFTP, SCP or RSYNC on SSH or SSHD configuration files	An alert is triggered upon running the SFTP/SCP or RSYNC command to exfiltrate an SSH or SSHD configuration file from a server.
Retrieving the Passwd, Group, Shadow or Profile files via SFTP, SCP or RSYNC	An alert is triggered upon running the GET command via SFTP/SCP or RSYNC to retrieve sensitive files (Passwd, Group, Shadow or Profile) from a remote configuration directory.
Exfiltrating data from the server via Unix email tools	An alert is triggered upon running Unix email tools (such as MAILX, SSMTP, MAIL, SENDMAIL, MUTT) to transfer data out of the server.
Exfiltrating SSL certificates and associated private keys via SFTP, SCP or RSYNC	An alert is triggered when a user attempts to exfiltrate an SSL certificate using SFTP, SCP or RSYNC.
Exfiltrating sensitive system files via SFTP, SCP or RSYNC	An alert is triggered upon running an SFTP/SCP or RSYNC command in order to exfiltrate a file from a sensitive directory.
Uploading files to a web site using curl on Unix or Linux	An alert is triggered when any user on a Unix or Linux endpoint attempts to use curl to upload a file to any website.

Data Infiltration (Bringing in Troubles) (Windows/Mac)

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

ALERT RULE	DESCRIPTION
Downloading file from cloud storage service site	An alert is triggered upon downloading a file from a website that is categorized as a Storage site.
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.
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.
Downloading file with potentially malicious extension	An alert is triggered upon downloading a file whose extensions is part of the list of potentially malicious file extensions.
Downloading file from a site dedicated to downloads	An alert is triggered upon downloading a file from website that is categorized as a download website.
Downloading file from infected or malicious site	An alert is triggered upon downloading a file from website that is categorized as infected or a malicious website.

Data Infiltration (Bringing in Troubles) (Unix/Linux)

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

ALERT RULE	DESCRIPTION
Copying files from remote servers to sensitive system folders via SFTP	An alert is triggered when a file from a remote server is copied to a sensitive system folder via SFTP.

ALERT RULE	DESCRIPTION
Prevent the copying of files from remote servers to sensitive system folders via SFTP (inactive)	An alert is triggered when a file from a remote server is copied to a sensitive system folder via SFTP. Note that this rule is inactive by default as it contains a preventive action.

Hiding Information and Covering Tracks (Windows/Mac)

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 in IE or Firefox	An alert is triggered upon opening the settings window of Internet Explorer or Firefox 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 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.
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 steganography 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.
Password protecting a file in UltraEdit text editor	An alert is triggered when a file in the UltraEdit text editor has been password protected.
Hiding files by moving them into hidden directory	An alert is triggered when any file is moved into a hidden directory.

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.

ALERT RULE	DESCRIPTION
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/Mac)

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

ALERT RULE	DESCRIPTION
Taking control on remote machine from Mac Note: This rule applies specifically on Mac systems.	An alert is triggered upon opening a Terminal application on Mac and running SSH to take control over a remote machine.
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.,

ALERT RULE	DESCRIPTION
	Administrator).
Running a remote PC access tool to access a remote machine	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.
Logging in to any machine by disabled users (ex-employees)	This alert will be triggered upon login to any type of machine (Win, Mac, Unix, Linux) of users who are part of the list Disabled Users (ex-employees whose account in Active Directory should have been disabled).
Connecting to a sensitive server using FTP applications	An alert is triggered upon using an FTP client on Windows or Mac and connecting to a remote server that is part of the Sensitive Remote Servers list.
Connecting to a new FTP or SFTP server using FTP application	An alert is triggered upon using an FTP application and connecting to a remote FTP or SFTP server.
Connecting to a sensitive Mac machine using Screen Sharing	An alert is triggered upon trying to connect to a sensitive remote Mac machine using Mac's built-in Screen Sharing mechanism.
Connecting to a sensitive server using Finder on Mac	An alert is triggered upon trying to connect to a remote server that is part of the Sensitive Remote Servers list using Finder on Mac (the equivalent to Windows Explorer on Windows).
Connecting to a sensitive Windows server from Mac	An alert is triggered upon trying to connect to Windows server that is part of a Sensitive Remote Servers list, while doing it from Mac using Microsoft Remote Desktop application.
Connecting to a sensitive VMWare VsPhere client	An alert is triggered upon trying to type the name or IP of sensitive machine in order to connect to a VMWare VsPhere Client.
Logging in with the default built-in privileged account to sensitive servers	An alert is triggered upon logging in to sensitive remote servers with the default privileged accounts of Administrator or root.
Interacting with remote machines using PowerShell commands	An alert is triggered upon opening PowerShell and invoking specific commands that are used for interacting with remote machines.

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 sensitive 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.
Accessing system folders	An alert is triggered upon opening in Windows Explorer one of the system folders as defined in external list.
Viewing or editing sensitive documents on Mac	An alert is triggered upon viewing or editing sensitive documents on Mac via document editing tools. It builds on the [CMD-P] for the Print event but combines it with the application for editing documents - either Numbers or Microsoft Word (can be added)

Bypassing Security Controls

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

ALERT RULE	DESCRIPTION
Opening ObserveIT Agent folder	An alert is triggered upon opening the folder in which the ObserveIT Agent is installed, potentially for tampering or covering tracks.
Running TOR browser	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.
Changing Internet security settings	An alert is triggered upon customizing the security level in Internet Properties. The operation can indicate an early intent to bypass security controls in Internet and bring in dangers.
Running a partially monitored browser	This alert will be triggered upon using Opera browser, which is only partially monitored by ObserveIT (no URL capturing). This operation can indicate an early intent to hide information and cover tracks from the organization.
Browsing to website related to MIMIKATZ utility	An alert is triggered upon downloading a file related to the MIMIKATZ utility which allows playing with Windows security.
Downloading the MIMIKATZ utility	An alert is triggered upon browsing or searching website related to the MIMIKATZ utility which allows playing with Windows security.

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 unauthorized predefined sites	An alert is triggered upon browsing to a predefined blacklisted website.
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.
Downloading computer anti-sleep software	An alert is triggered upon downloading an installation file or ZIP file that is a member of the Computer Anti-sleep Software list that can be used by employees to make it appear as they're working, while they're actually not.
Running computer anti-sleep software	An alert is triggered upon running an executable file that is part of the Computer Anti-sleep Software list that can be used by employees to make it appear as they're working, while they're actually not.

Careless Behavior (Windows/Mac)

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

ALERT RULE	DESCRIPTION
Opening sharing settings on Mac Note: This rule applies specifically on Mac systems.	An alert is triggered upon opening the Sharing settings in System Preferences on Mac, potentially to enable sharing and so allow remote access to the Mac.
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 access from remote machine	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.
Opening a clear text file that potentially stores passwords	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.
Accessing file or folder sharing settings	An alert is triggered upon accessing Windows dialog for file sharing settings or folder sharing settings.
Enabling Windows Remote Assistance from System Properties	An alert is triggered upon opening the Remote tab within the System Properties dialog to enable Remote Assitance. This action can indicate that the user plans to grant access to this machine to a remote user.

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 a Backdoor (Windows/Mac)

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

ALERT RULE	DESCRIPTION
Adding a local Windows User	An alert is triggered upon opening the Local Users and Groups screen potentially to add a local user. Such an operation could indicate a potential security backdoor to be exploited later.
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.
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 later.
Setting up a VPN server	This alert will be triggered upon creating a new incoming connection by changing network adapter settings. The new incoming connections allows other people to access the computer and network.
Opening Users and Groups Preferences on Mac	An alert is triggered upon opening the Users and Groups dialog which is part of the Preferences screens on Mac.

Creating a Backdoor (Unix/Linux)

The following out-of-the-box alert rules are assigned to the (Unix/Linux) Category: CREATING A 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, to modify `cron` jobs. This could enable potential backdoor user activity.
Editing PASSWD, GROUP, SHADOW, PROFILE files	An alert is triggered when a PASSWD, GROUP, SHADOW or PROFILE file is edited.
Setting up a VPN server	This alert will be triggered upon creating a new incoming connection by changing network adapter settings. The new incoming connections allows other people to access the computer and network.

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/Mac)

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

ALERT RULE	DESCRIPTION
Running command-line-based hacking tool	An alert is triggered upon running a hacking tool in the form of a script or executable in command line tools.
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/Mac)

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
Adding or modifying Roles and Features in IIS Manager	An alert is triggered upon opening the Microsoft IIS settings wizard to add roles or features.
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 PowerShell-specific dangerous command	An alert is triggered upon running a predefined PowerShell command that is risky or can cause damage.
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.

ALERT RULE	DESCRIPTION
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.
Removing roles or features in IIS Manager	This alert will be triggered upon opening the Remove Role and Features Wizard window in IIS Manager. This operation indicates an early intent to cause damage to the organization network.
Changing Internet protocol properties	This alert will be triggered upon opening the Internet Protocol Properties window. The operation can indicate an intent to change connected DNS servers and IP addresses.
Connecting to Amazon FTP server on Mac	An alert is triggered upon trying to connect the Amazon EC2 (with the default user account), potentially in order to transfer data to it.
Mounting file system using the mount command on Mac	An alert is triggered upon using manually the mount command on Mac in order to mount a file system. Usually it is expected to be done using the UI, and doing via command line is worth reviewing.
Accessing system libraries on Mac	An alert is triggered upon accessing via Finder directories of system libraries on Mac.
Trying to change computer name or domain	An alert is triggered upon opening the Computer Name/Domain Changes dialog, potentially in order to change the computer name or the domain name membership.
Changing the state of a Windows service	An alert is triggered upon changing the state of a Windows service (e.g. starting or stopping) from the Services screen.
Changing Windows startup configuration	An alert is triggered upon opening Windows System Configuration utility, potentially in order to make changes in the flow of the startup process of the machine.
Connecting to a remote Registry on Windows	An alert is triggered upon opening Registry Editor and trying to connect to a remote computer in order view of modify Registry keys.
Opening Startup and Recovery dialog	An alert will be triggered upon opening the Startup and Recovery dialog, potentially to make changes on local computer.
Opening Windows system certificates screen	An alert is triggered upon opening the certificates screen within Microsoft Management Console (MMC).
Renaming computer via command line tools	An alert is triggered upon trying to change a computer name via command line tools.

ALERT RULE	DESCRIPTION
Accessing Windows Environment Variables screen	An alert is triggered upon accessing the Environment Variables screen on Windows, potentially to make changes in internal Windows settings.
Creating or modifying scheduled tasks in command line tools	An alert is triggered upon creating or modifying scheduled tasks via command line tools.
Viewing network connections and network adapters settings	An alert is triggered upon opening the Network Connection screen on Windows.
Opening Windows Services screen	An alert is triggered upon opening the Services screen on Windows, potentially in order to stop or start one of the Windows Services.

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).
Editing the SUDOERS file using VISUDO	An alert is triggered upon trying to edit the SUDOERS file using VISUDO. This file can grant unauthorized 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
Downloading file from copyright-violating or P2P site	An alert is triggered upon downloading a file from a website that is categorized as a copyright-sensitive or P2P site.
Browsing copyright-violating sites	An alert is triggered upon browsing websites that support violation of copyrighted content such as movies and music.
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 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 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, 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.

ALERT RULE	DESCRIPTION
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.
Accessing Programs and Features screen on Windows	An alert is triggered upon opening Windows Programs and Features screen, potentially in order to uninstall a program.

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.

ALERT RULE	DESCRIPTION
Opening Active Directory object properties for viewing or changing	An alert is triggered upon opening the properties dialog of an Active Directory object to view or change its properties.
Running Active Directory management tools on an unauthorized workstation	An alert is triggered upon opening built-in MMC utility to manage Active Directory on workstations that are not part of the authorized workstations to do it.
Using Active Directory diagnostic tool to manage Active Directory	An alert is triggered upon opening NTDSUTIL which is a diagnostic tool for Active Directory.

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 ALTER command	An alert is triggered upon executing SQL command that includes the keyword ALTER. This operation is highly sensitive, as it changes the structure of objects 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.
Connecting to a sensitive DB server from SQL Server Management Studio	An alert is triggered upon typing the name or IP of a sensitive database server in order to connect to it from within Microsoft SQL Server Management Studio.
Modifying database records by using command line tools	An alert is triggered upon using command line tools to executing SQL command that modifies DB records. This operation is highly sensitive, as it changes content of tables within database tables.
Modifying database records by executing SQL command via DBA tools	An alert is triggered upon executing SQL command that modifies DB records. This operation is highly sensitive, as it changes content of tables within database tables.

ALERT RULE	DESCRIPTION
Logging in to SQL Server Management Studio using too generic credentials	An alert is triggered upon opening SSMS and trying to login using credentials that are too generic (not secured enough).
Running database management tools on an unauthorized workstation	An alert is triggered upon opening an SQL tool on workstations that are not part of the authorized workstations to do it.
Deleting database table by executing SQL command	An alert is triggered upon executing either the TRUNCATE TABLE or DROP TABLE commands that entirely deleted tables from database.

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.

ALERT RULE	DESCRIPTION
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 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 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.

ALERT RULE	DESCRIPTION
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 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.
Editing network configuration files	An alert is triggered upon trying to edit network configuration files.
Editing the SSH or SSHD configuration files	An alert is triggered when an SSH or SSHD configuration file is edited.

Messing with ObserveIT Components

The following out-of-the-box alert rules are assigned to the category: MESSING WITH OBSERVEIT COMPONENTS

ALERT RULE	DESCRIPTION
Logging in to ObserveIT Web Console using a sensitive account	An alert is triggered upon logging in ObserveIT web console using an administrative or sensitive account. The accounts are not supposed to be used in logging in by individuals. This operation can indicate an early intent to hide identities.
Looking for ObserveIT processes using Activity Monitor on Mac	An alert is triggered upon looking for ObserveIT processes within Activity Monitor utility on Mac, potentially in order to kill them and stop being monitored by ObserveIT.
Looking for ObserveIT processes using Terminal on Mac	An alert is triggered upon looking for ObserveIT processes using commands within Terminal on Mac, potentially in order to kill them and stop being monitored by ObserveIT.

ALERT RULE	DESCRIPTION
Looking for ObserveIT libraries using Terminal on Mac	An alert is triggered upon looking for ObserveIT libraries using commands within Terminal on Mac, potentially in order to stop being monitored by ObserveIT.
Trying to Kill ObserveIT processes on Mac	An alert is triggered upon trying to kill one of the ObserveIT processes running on Mac, potentially in order to stop being monitored by ObserveIT.
Trying to Kill ObserveIT processes on Unix or Linux	An alert is triggered upon trying to kill one of the ObserveIT processes running on Unix or Linux, potentially in order to stop being monitored by ObserveIT.
Trying to Kill ObserveIT processes on Windows	An alert is triggered upon trying to kill one of the ObserveIT processes running on Windows, potentially in order to stop being monitored by ObserveIT.
Trying to stop ObserveIT service on Unix or Linux	An alert is triggered upon trying to execute a command that stops ObserveIT service on Unix or Linux, potentially in order to stop being monitored by ObserveIT.
Trying to stop ObserveIT service on Unix or Linux using INIT	An alert is triggered upon trying to execute a command that stops ObserveIT service on Unix or Linux, potentially in order to stop being monitored by ObserveIT.
Accessing ObserveIT libraries on Linux	An alert is triggered upon executing commands involving ObserveIT libraries. Such activity can indicate an intent to detect if one is being monitored, or to remove or harm libraries while trying to hide activity.
Changing ObserveIT Image Security settings	An alert is triggered upon browsing to the web page in which Image Security settings can be changed on ObserveIT Application Server.
Changing ObserveIT Installation Security settings	An alert is triggered upon browsing to the web page in which Installation Security settings can be changed on ObserveIT Application Server.
Logging in to ObserveIT Web Console on an unauthorized machine	An alert is triggered upon trying to browsing to ObserveIT Web Console login page in order to login from a machine which is not in the list of legitimate machines to do it from.

GIT Suspicious Activity

The following out-of-the-box alert rules are assigned to the category: GIT SUSPICIOUS ACTIVITY

ALERT RULE	DESCRIPTION
Creating a remote pointing to a GIT repository	An alert is triggered upon creating a remote pointing to a Git source-code repository via command line.
Cloning GIT content to a remote repository on Unix or Linux	An alert is triggered upon executing a cloning command in Unix or Linux, usually in order to contribute to a project that already exist.
Cloning GIT content to remote repository on Mac	An alert is triggered upon executing a cloning command in command line tools on Mac, usually in order to contribute to a project that already exist.

Docker and Containers Suspicious Activity

The following out-of-the-box alert rules are assigned to the category: DOCKER AND CONTAINERS SUSPICIOUS ACTIVITY

ALERT RULE	DESCRIPTION
Accessing unauthorized containers in interactive mode	An alert is triggered upon accessing unauthorized container in interactive mode.
Running unauthorized container	An alert is triggered upon running container which is not in the authorized containers list.
Executing commands to run inside containers	An alert is triggered upon executing a command within a container.
Executing a sensitive docker command	An alert is triggered upon executing a sensitive command which is part of a list.
Opening a shell inside an unauthorized container	An alert is triggered upon opening a shell inside a container which is not part of the authorized containers.