ITL Tuning Guide Overview

ObserveIT Insider Threat Library (ITL) contains ~250 Alerts Rules for Windows/Mac (and an additional ~70 Alerts Rules for Unix/Linux).

To help you use the Alert Rules, ObserveIT carefully researched and determined which Alert Rules bring the highest value to customers. These "top" Alert Rules for Windows/Mac are now active by default. All other Window/Mac rules are deactivated by default.

This guide shows you how to tune the "top" Alert Rules to avoid false positives and includes both basic and advanced tuning instructions.

For a .pdf of this document, click here.

Basic Tuning

To get started tuning alerts, do the following:

1. Validate the prerequisites
    *   Website Categorization module is installed successfully (if required)
    *   LDAP Settings are defined to utilize Active Directory users/groups.

        Select **Configuration** > **User Management** >**LDAP Settings**.
    *   SMTP Settings are defined to receive email notifications on Alerts.

        Select **Configuration** > **Settings** >**SMTP Settings**.

2. Populate User Lists with User Login Names and Activity Directory Groups

    Select **Configuration** > **Alerts** >**Lists**, and add **Users** and **Groups** to the following lists:

    *   **Privileged Users**
    *   **Developers & DevOps**
    *   **Remote Vendors**

    > Note: After adding a user or group to one of the above lists, remember to exclude it from the Everyday Users Group. This way no user or group is associated with more than one list.

3. Populate the General Lists with items that correspond to the alert rule that will trigger

Select Configuration > Lists, and add relevant Items to the following lists:

- **Sensitive files**: keywords (e.g., ".pdf", "salary", "revenues.xlsx") within file names that are sensitive for exfiltration via printing, sending out in email, copying/pasting, viewing, copying text from.
- **Sensitive folders**: keywords within folder names that are sensitive for viewing or exfiltration via copying/pasting.
- **Keywords in file names to trigger alert on uploading**: Keywords to be searched in uploaded file names (and extensions)
- **Keywords to be monitored upon copying them to clipboard**: Keywords to be monitored in case they're copies to the clipboard
- **Sensitive keywords to be detected in Subject of outgoing emails**: Sensitive keywords in the Subject field of and email that trigger an alert
- **Unauthorized black-listed websites**: Site names that are blacklisted and unauthorized for browsing within the organization (e.g., "youtube", "<competitor-name>.com")
- **Sensitive Windows servers**: Names of sensitive windows server in your organization (e.g. Production servers)
- **Sensitive Windows desktops**: Names of sensitive windows desktops in your organization (e.g. the laptops of executives)

4. Clean up the Alerts screen - Remove pre-tuning triggered Alerts

After completing the above tuning, it is recommended that you clean the Alerts screen by deleting all the old alerts (select all Alerts in all pages and click the Delete icon) so you'll be able to start getting only post-tuning alerts.

5. Let ObserveIT run and review high-risk users in the **User Risk Dashboard**

Let the system run for at least a week and as a starting point we recommend to start by reviewing the high-risk users that appear at the top of the User Risk Dashboard. To switch and view all alerts of a high-risk user, in the **User Risk Dashboard** screen, click the **Investigate** button by the relevant high-risk user.

- You can fine-tune false-positive Alerts from the **Tuning** popup by clicking the **Tuning** icon. The **Ongoing Alerts Tuning Options** allow you to easily exclude users or Active Directory Groups from a specific Alert rule.

- Alternatively, you can open an Alert rule directly from the **Tuning** popup for full editing capabilities by clicking **Open this Alert Rule for editing**.

- Delete (or change status) of already triggered false-positive Alerts.

- Fine-tune Lists from the **Configuration** > **Alerts** > **Lists** screen in order to add/remove list items from Lists or add/exclude users and Active Directory Groups from specific User Lists.

More Advanced Tuning

For additional advanced tuning, you can do the following:

1. Populate the rest of the User Lists with relevant users/groups

   - **Executives List**: Managers whose risk is lower than standard employees
   - **Termination List**: Users who are in a watch list because they are currently in a pre-termination period (initiated by employee or organization)
   - **Users in Watch List**: Users who are in a watch-list for reasons other than termination
   - **Disabled Users**: Users who left the company and might still have access to company assets

2. Fine tune irregular working hours in the below Alert Rules (by default, the regular hours are 7:00 am to 7:00 pm, Mon to Fri):

   - **Performing large file or folder copy during irregular hours**
   - **Printing large number of pages during irregular hours**

3. See the table in List of Active Alert Rules that details all active Alert Rules and consider fine tuning the Lists that are marked as optional.

4. See the full ITL Alert Rules to review the entire library of rules and see if you want to active more Alert Rules.

List of Active Alert Rules

Alert Rule Name	Required Tuning (Mandatoryand Optional)
DATA EXFILTRATION	
Performing large file or folder copy during irregular hours	1. Optional: Irregular Hours/Days within the Alert Rule
Exporting data from enterprise web application by file downloading	1. Optional: List - Enterprise web applications to detect download from 2. Optional: List - File extensions to detect their exporting from enterprise apps
Accessing upload and sharing cloud services	-
Exfiltrating tracked file to the web by uploading	1. **Mandatory: List - Keywords in file names to trigger alert on uploading** 2. Optional: List - Excluded file names from alerts on exfiltration
Performing large file or folder copy	-
Exfiltrating a file to an unlisted USB device	1. Optional: List – White listed USB devices 2. Optional: List - Excluded file names from alerts on exfiltration
Connecting unlisted USB device	1. Optional: List – White listed USB devices 2. Optional: List - Excluded vendors/models from alert on detecting connected USB
Exfiltrating a file to the web by uploading	1. **Mandatory: List - Keywords in file names to trigger alert on uploading** 2. Optional: List - Excluded file names from alerts on exfiltration
Exfiltrating a file that was tagged with a sensitive MIP label	1. **Mandatory: List - Sensitive MIP labels**
Exfiltrating tracked file to a cloud sync folder	1. Optional: List - Excluded file names from alerts on exfiltration
Printing sensitive documents	1. **Mandatory: List – Sensitive files**
Printing large number of pages during irregular hours	1. Optional: Irregular Hours/Days within the Alert Rule
Sending email with sensitive keywords in Subject to untrusted domain	1. **Mandatory: List - Sensitive keywords to be detected in Subject of outgoing emails**
Sending email with large file attachment to untrusted domain	1. Optional: File size threshold (5000 KB by default)
Sending email with sensitive file attachment to untrus-	1. **Mandatory: List – Sensitive files**

ted domain	
Saving email file attachment to a local sync folder	-
Saving email file attachment to a USB storage device	-
Pasting files copied from sensitive folders	1. **Mandatory: List - Sensitive folders**
Pasting text that contains predefined sensitive keywords	1. **Mandatory: List - Keywords to be monitored upon copying them to clipboard**
DATA INFILTRATION	
Browsing harmful, risky or contaminating sites	-
Downloading file from a site dedicated to downloads	-
Downloading file from a cloud storage service site	1. Optional: List - Excluded site names from alert on download from cloud services
Downloading file with potentially malicious extension	1. Optional: List - File extensions to detect malicious file download
Downloading file from infected or malicious site	-
CARELESS BEHAVIOR	
Running software to enable sharing and access from remote machine	-
Opening a clear text file that potentially stores passwords	-
BYPASSING SECURITY CONTROLS	
Running TOR browser	-
Downloading the MIMIKATZ utility	-
Browsing to website related to MIMIKATZ utility	-
Running VPN, Proxy or Tunneling tools	-
HIDING INFORMATION AND COVERING TRACKS	
Clearing browsing history in Google Chrome	-
Clearing browsing history in IE or Firefox	-
Running steganography tools	-
RUNNING MALICIOUS SOFTWARE	
Running password and license cracking tools	-
Running hacking or spoofing tools	-
Running command-line-based hacking tool	-
Running port scanning tools	-
UNACCEPTABLE USE	
Running computer anti-sleep software	-

Browsing Illegal activities, violence or hate sites	-
Browsing unauthorized predefined sites	1. **Mandatory: List - Unauthorized black-listed web-sites**
Browsing Adult sites	-
Browsing Gambling sites	-
Browsing Illegal drugs sites	-
UNAUTHORIZED DATA ACCESS	
Accessing sensitive folder	1. **Mandatory: List - Sensitive folders**
UNAUTHORIZED MACHINE ACCESS	
Logging in remotely (RDP) to sensitive Windows Server from unauthorized client	1. **Mandatory: List - Sensitive Windows servers** 2. Optional: List - Authorized addresses for login from
Logging in to any machine by disabled users (ex-employees)	-
Logging in Remotely (RDP) to sensitive Windows Desktop by unauthorized user	1. **Mandatory: List - Sensitive Windows desktops**
SEARCHING FOR INFORMATION	
Searching data on password cracking	-
Searching data on steganography	-
Searching data on monitoring or sniffing	1. Optional: List - Monitoring/sniffing keywords
Searching data on Remote Access and Desktop Sharing	1. Optional: List - Remote access and desktop sharing keywords
Running advanced monitoring or sniffing	1. Optional: List - Monitoring/sniffing keywords
Searching data on hacking or spoofing	1. Optional: List - Hacking/Spoofing keywords
Searching data on file transfer (FTP or SFTP)	1. Optional: List - FTP keywords
Searching data on Dynamic-DNS	1. Optional: List - Dynamic-DNS keywords
Searching data on Darknet TOR (The Onion Router)	1. Optional: List - TOR (Darkweb) keywords
Searching data on VPN, Proxy or Tunneling	1. Optional: List - VPN/Proxy/Tunneling keywords
PERFORMING UNAUTHORIZED ADMIN TASKS	
Running PowerShell-specific dangerous command	1. Optional: List - PowerShell dangerous commands
MESSING WITH OBSERVEIT COMPONENTS	
Trying to kill ObserveIT processes on Windows	1. Optional: List - Command line tools 2. Optional: List - ObserveIT services on Windows 3. Optional: List - Kill commands on Windows
Trying to Kill ObserveIT processes on Mac	1. Optional: List - Command line tools

	2. Optional: List - ObserveIT services on MAC
	3. Optional: List - Kill commands on Mac and Unix/Linux
Opening ObserveIT Agent folder	-
INSTALLING/UNINSTALLING QUESTIONABLE SOFTWARE	
Installing hacking or spoofing tools	1. Optional: List - Hacking/Spoofing keywords
	2. Optional: List - Reserved keyword used in Window Title of OIT virtual screenshots
COPYRIGHT INFRINGEMENT	
Downloading file from copyright-violating or P2P site	-
Browsing copyright-violating sites	-
CREATING BACKDOOR	
Adding a local Windows User	-