WHAT'S NEW IN OBSERVEIT 7.0

ObserveIT 7.0 provides a complete approach to identify and eliminate insider threats.

ObserveIT unveils new actionable analytics and the ability to proactively block risky, out-of-policy activities by insiders, giving security and IT teams powerful weapons in their challenge to make their organizations more secure. With the innovations now available, ObserveIT 7.0 continues to enable its customers to ensure that privileged users, vendors, consultants, and business users, do not act in negligent or malicious ways that could put their businesses at risk.

Key new features include real-time detection when someone types sensitive keywords to exfiltrate data, forcibly preventing users who connect to non-allowed computers, stopping user attempts to violate security or compliance policies, and more. Profiling user behaviour allows you to understand normal user behaviour and easily spot any abnormal activities.

OBSERVEIT 7.0 NEW FEATURES AND ENHANCEMENTS

User Activity Profile – Provides smarter detection and faster investigation of risky users:

- ✓ Enables security analysts to understand normal user behavior and see exactly how users are spending their time.
- ✓ Provides visibility into employee or remote vendor productivity by examining how much time they spend in each application, their working days/hours, as well as idle time.
- ✓ Identifies abnormal user activity and reduces investigation time by detecting new security incidents within the context of what users are normally doing.
- ✓ Identifies risky user activity such as applications/websites/Unix commands that are abnormally used, or run on infrequently used computers.

Key Logging Alerts – Provide greater visibility on users with the highest level of access to critical data in your organization and increased awareness of workplace violence terminology, fraud terms, and improper or malicious language use. You can detect:

- ✓ Sensitive keywords and commands typed in desktop applications, websites, and shell command tools
- ✓ Workplace violence terms, fraud terms, and other improper or malicious keywords
- ✓ Data exfiltration attempts by users typing protected keywords in emails or chat applications, social media sites, etc.
- ✓ Commands executed in CLI tools such as Windows CMD, PowerShell, PuTTY or Mac Terminal

Preventive Actions – Enable security and compliance teams to block user activities that breach security or violate company policies, by forcibly locking users out of the system or shutting down sensitive applications or websites.

- ✓ Hard enforcement of company policy.
- ✓ Effective asset protection and potential damage control.
- ✓ Improve Security/IT processes by collecting user feedback before the application is closed or the user is logged-off, and optimizing internal processes accordingly.

Revamped Web Console UI – The ObserveIT Web Console User Interface has been rebranded and refreshed to provide:

- ✓ An enhanced look-and-feel that is consistent across the product.
- ✓ Responsive design with resizable UI to better support high resolution displays and accommodate more data.
- ✓ Improved terminology changes – "Endpoints" (replacing monitored "Servers", "Desktops", "Terminal Servers", etc.) and "Recording Policies".

Managing content Updates: Insider Threat Library – ObserveIT now provides customers with periodic Insider Threat Library updates that are independent of software release cycles, enabling security administrators to keep up-to-date with new insider threat scenarios.

New Insider Threat Library (ITL) Rules – Additional out-of-the-box insider threat scenarios are provided by new system rules for key logging, unauthorized DBA, and Active Directory activity.

New and Improved Reports– New reporting capabilities on websites visited, printed documents, USB storage device connections, file copying, installing and uninstalling applications, and so on, significantly improving security operations and regulatory compliance.

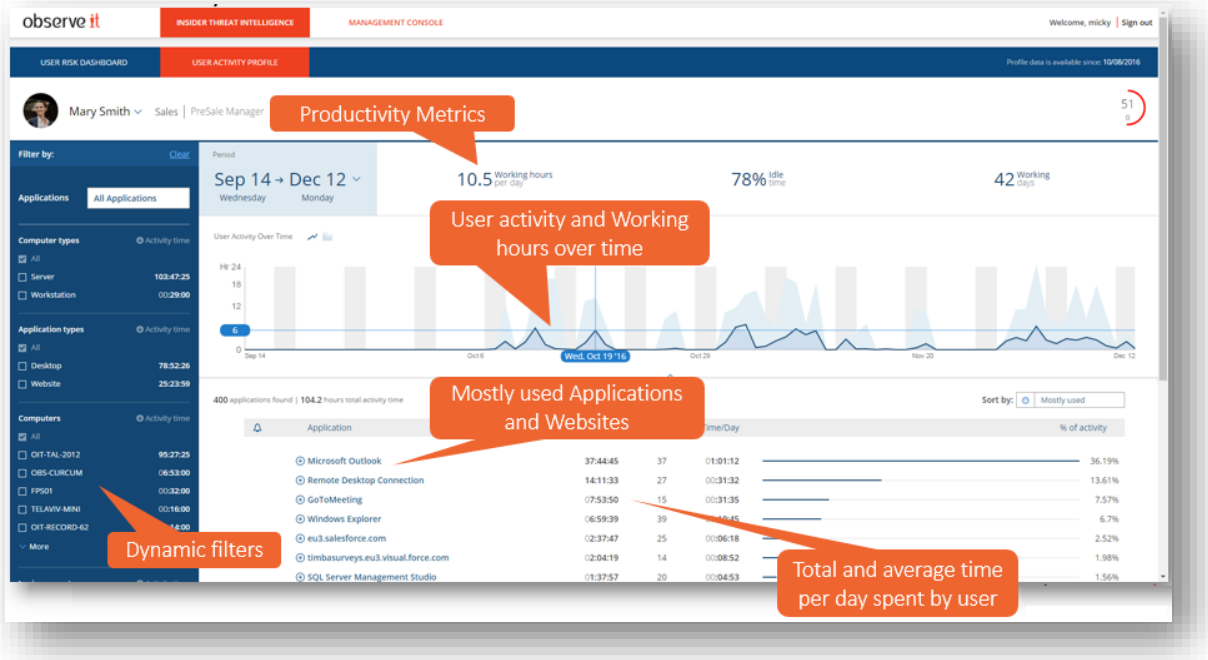
USER ACTIVITY PROFILE

The Insider Threat Intelligence platform provides access to the profiles of users to investigate employee or remote vendor activity, in order to determine:

- Where users spend most of their time?
- Which applications do they use?
- How much time do users spend in applications?
- How much time during working hours is the user idle?
- Which computers are used to work on or to connect from?
- Which shared accounts are being used?
- Is anything abnormal about the user's behavior?

By viewing the normal behavior of a user or comparing it with the user's peers, investigators can quickly determine if the activity that is being investigated is indeed risky.

Dynamic filtering capabilities enable you to focus your investigation on specific applications, endpoints, login accounts, and/or remote client machines. An overall view of user activity during the specified profile period is displayed in a User Activity Over Time graph.



Viewing a User's Activity Profile

From the Applications list, you can drill down to view the relevant sessions with details and watch the video recordings.

To protect the privacy of recorded users, ObserveIT enables you to "anonymize" all personal user information that could identify users. In Anonymization mode, all personal user information in the Web Console is encoded – so there is no way to tell the name of the user, the role or department, or see the user's personal photo. In addition, computers that are accessed and login accounts that are in use are anonymized. This information remains hidden in the ObserveIT Web Console unless specifically requested and approved to be exposed.

Note that in Anonymization mode, a Security Analyst or an Investigator using the system can still get detailed visibility to the risky users including their alerts and activity, but without their personal identity, names of computers accessed, or login accounts, being exposed.

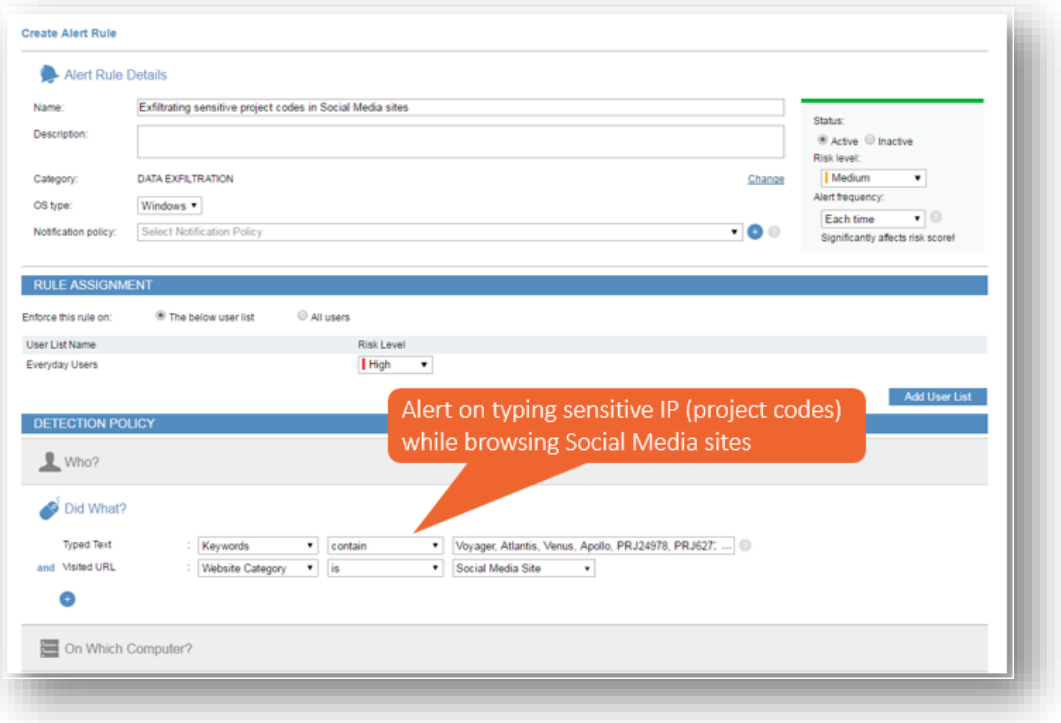
KEY LOGGING ALERTS

ObserveIT Key Logging enables the detection and alerting on sensitive keywords and commands typed in desktop applications, websites, and shell command tools. Real-time alerts can also be generated on workplace violence terms, fraud terms, and other improper or malicious keywords that users typed.

Data exfiltration attempts can be detected if users type protected keywords in emails or chat applications, social media sites, and so on.

Captured key logging data can generate alerts that identify when a user types blacklisted commands in CLI tools such as Windows CMD, Powershell, Putty, or Terminal (Mac), blacklisted phrases in an email, or sensitive words while browsing social media websites. Following are some examples:

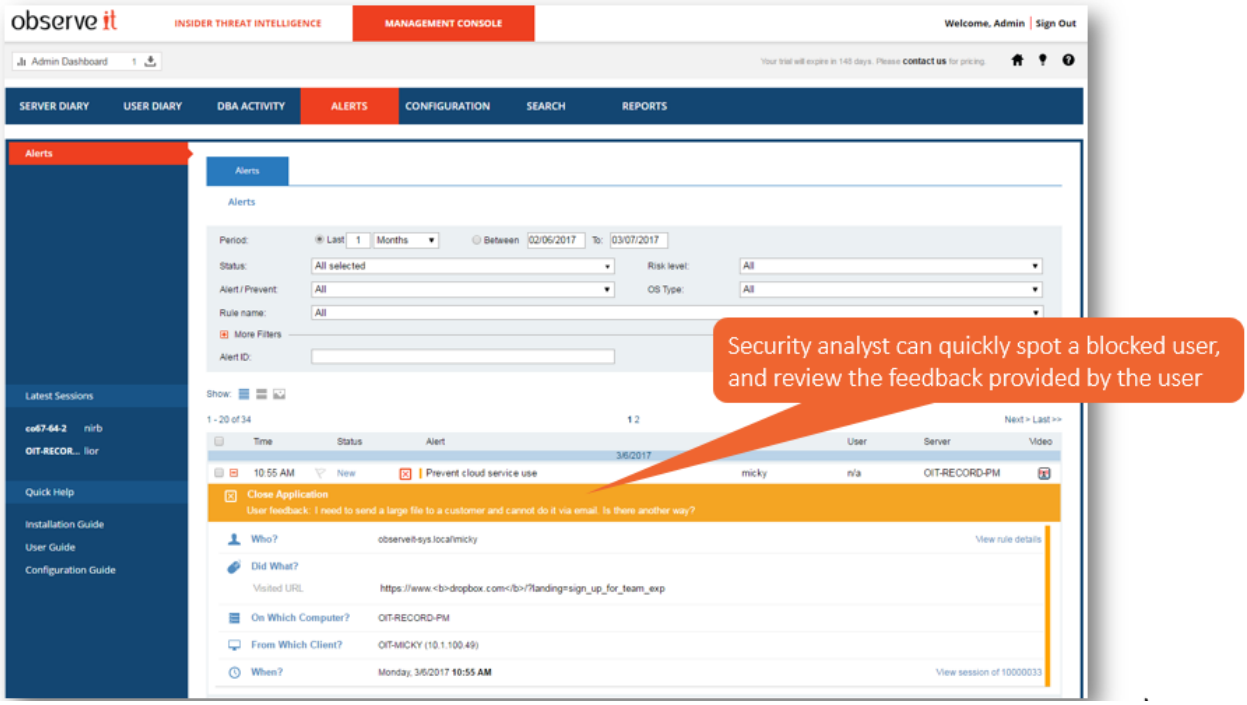
- When a user types within CMD or PowerShell windows the command "netstat" that is included in a list of blacklisted commands specified in the List **Network Sniffing**.
- When a user creates an email or replies to an email using blacklisted phrases or improper language specified in the List **Work violence words/phrases.**
- When a user types sensitive words such as the company name while browsing within websites categorized as **Instant Messaging**, **Chats** or a **Social Media Site**. Sensitive keywords are specified in a list.



Key Logging – Detecting the typing of sensitive keywords

PREVENTIVE ACTIONS

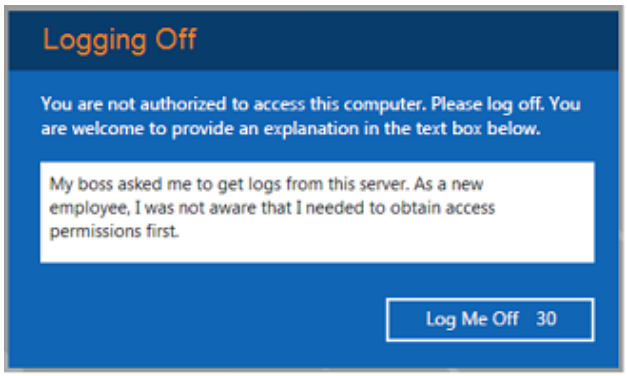
To prevent users from breaching security or violating policies, ObserveIT enables you to force users to log-off when connecting to unauthorized computers, and close applications or websites that are involved in unauthorized activity. Before an application is closed or the user is logged-off, users have an option to provide an explanation for their activities. This user feedback, which is invaluable for understanding the reason for the alleged violation, can be viewed in the Alerts page of the Web Console, together with the alert details.



Alert details showing user feedback for an application that was forcibly closed

The **Log Off** action blocks the user's screen with a message asking them to log off or they will be automatically logged off within a specified period of time. Users have an option to provide an explanation for their activity before they are forcibly logged-off.

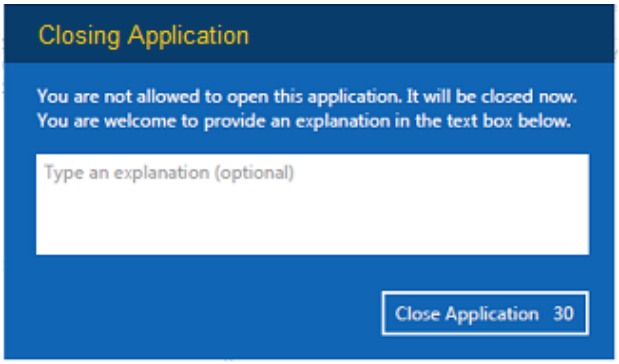
Following is an example of a forced Log Off message to a remote vendor who is trying to connect to an unauthorized server. In this example, the user provided feedback.



Log Off message example

The **Close Application** action blocks the user's screen with a message asking them to close the application or it will be automatically closed within a specified period of time. Users have an option to provide an explanation for their activity before the application is closed.

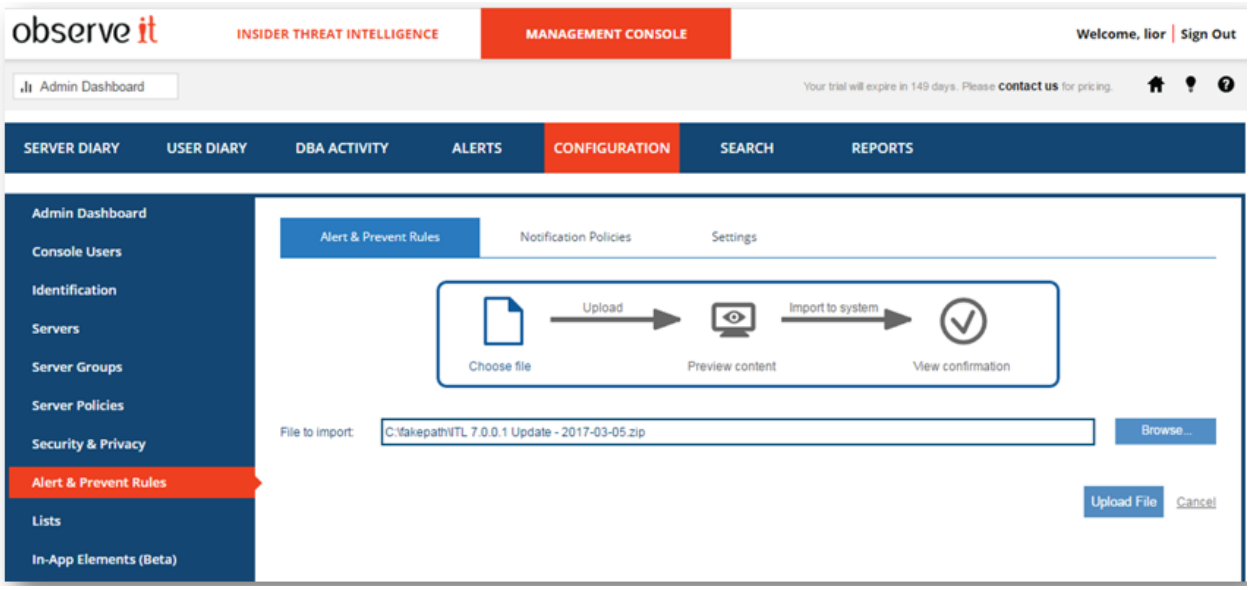
Following is an example of a blocking message that an everyday user might receive when opening the Registry Editor. The application will be forcibly closed within the specified time.



Close Application message example

MANAGING CONTENT UPDATES: INSIDER THREAT LIBRARY

The Insider Threat Library (ITL) is maintained by a Content Manager and can be released as a ZIP file containing System Rules which customers can import using the Import Wizard. System rules are exported with their current User List assignments.



Importing System Rules that were exported from the Insider Threat Library

NEW INSIDER THREAT LIBRARY (ITL) RULES

In this version of ObserveIT, new system rules provide additional out-of-the-box insider threat scenarios for key logging, unauthorized DBA activity, and unauthorized Active Directory activity.

Key Logging

- Typing workplace violence words
- Typing sensitive intellectual property related words in web mail, Chat, IM, Social Media sites
- Running unauthorized command by admin in command line tools
- Running unauthorized command by non-admin user in command line tools

Unauthorized DBA Activity

- Executing SQL update command
- Opening Server Properties window on SQL Server Management Studio
- Adding new Login ID on SQL Server Management Studio
- Deleting object on SQL Server Management Studio
- Detaching database on SQL Server Management Studio
- Backing up database on SQL Server Management Studio
- Copying database on SQL Server Management Studio
- Exporting database or tables on SQL Server Management Studio
- Adding new Server Role on SQL Server Management Studio
- Adding new Credential on SQL Server Management Studio

Unauthorized Active Directory Activity

- Adding new Group object in Active Directory
- Adding new InetOrgPerson object in Active Directory
- Adding new msDS-ResourcePropertyList object in Active Directory
- Adding new msImaging-PSPs object in Active Directory
- Adding new msMQ-Custom-Recipient object in Active Directory
- Adding new Printer object in Active Directory
- Adding new Shared Folder object in Active Directory
- Adding group membership to Active Directory user
- Adding members to Active Directory group
- Opening Active Directory object properties for viewing or changing

NEW AND IMPROVED REPORTS

10 new customizable reports were added in this release:

- Remote connection utilities used over the past 2 weeks
- Websites visited by website name and by user over the past week
- Websites visited by user and by website name over the past week
- Printed documents over the past 2 weeks
- Connecting USB storage device over the past 2 weeks
- Large file copy over the past 2 weeks
- Alerts triggered over the past 2 weeks
- Google, Bing, and Yahoo searches over the past 2 weeks
- Application installations over the past 3 months (PCI requirements)
- Application Uninstallations over the past 3 months (PCI requirements)

NEW SUPPORTED PLATFORMS

- ✓ RHEL/CentOS 7.3 x86_64
- ✓ Oracle Linux 7.3 i386/x86_64
- ✓ Solaris 10 with OpenSSL version 1.0.1
- ✓ Windows Server 2016 on the Server-side (Application Server and Web Console)
- ✓ Microsoft SQL Server 2016