



# A Visual Guide to Insider Threat Investigations

**AD-HOC INVESTIGATIONS  
VS. OBSERVEIT**

# Getting Practical: Insider Threat Investigations

## What do we mean when we say **Insider Threat**?

The truth is, at times, it can be very abstract. And while there is value in understanding the principles and best practices that underlie a strong security program, it can also be very helpful to see for yourself what a given process actually looks like.

Today, we want to do just that: give you a visual glimpse into a practical security process. We'll walk you through exactly how an insider threat investigation works.

### **In this eBook, we'll cover:**

- The Insider Threat investigation process with security solutions like Security Information and Event Management (SIEMs)
- What an investigation looks like within ObserveIT, a dedicated insider threat management platform, including:
  - **Proactive** threat hunting
  - **Reactive** alert investigations after a known incident



---

# Ad-Hoc Insider Threat Investigations

A Step-by-Step Look

# Step 1 Kicking off an Ad-Hoc Investigation

Without an Insider Threat platform and/or a dedicated program in place, investigations can be piecemeal, messy, and inefficient.

**First, an alert will come in. This can come from one of two places:**

**Inside:** This is the best-case scenario. If an internal alert goes off, it usually comes from a system, like a SIEM platform, which consist of monitoring logs and the security tools that feed into them (such as data loss prevention [DLP] or endpoint detection and response [EDR] tools.)

**Outside:** The worst-case scenario? A customer, regulatory body, or someone else on the outside notices something out of the ordinary and notifies the company that there may have been a security breach.

**Regardless of where the alert comes from, this is what kicks off the investigation.**

# Step 2 Gathering Intel

**The next step is to gather more intel.** While the alert will usually let you know “what” has happened, it won't tell you the whole story. You need to dig around to figure out:

- **Where** did this happen? (In a web app? On the desktop?)
- **What** systems are affected?
- **When** did the potential incident take place?
- **What** other suspicious user activity has taken place within the time frame of the incident? (Important context that will determine the course of action)

As you can imagine—or may know from going through this process yourself—handling an alert in this manner can be very time-consuming. It requires the security team to go through many different tools, often searching through massive amounts of logs under significant time pressure. This alert may be one of hundreds coming in every day, which can make it challenging to identify which ones represent real problems.

## Fast Facts



Source: CA 2018 Insider Threat Report

## Typical security log fed through a SIEM

Event 4648, Microsoft Windows security auditing.

General		Details	
A logon was attempted using explicit credentials.			
Subject:	Security ID:	OBSERVEIT-SYS\lucas.calixto	
	Account Name:	lucas.calixto	
	Account Domain:	OBSERVEIT-SYS	
	Logon ID:	0x126BC132	
	Logon GUID:	{00000000-0000-0000-0000-000000000000}	
Account Whose Credentials Were Used:			
	Account Name:	lucas.calixto	
	Account Domain:	OBSERVEIT-SYS.LOCAL	
	Logon GUID:	{5fcee335-99ef-0bfe-bb97-ced3d1826ef9}	
Target Server:			
	Target Server Name:	fps01	
	Additional Information:	cifs/fps01	
Process Information:			
	Process ID:	0x4	
	Process Name:		
Network Information:			
	Network Address:	10.199.1.14	
	Port:	445	

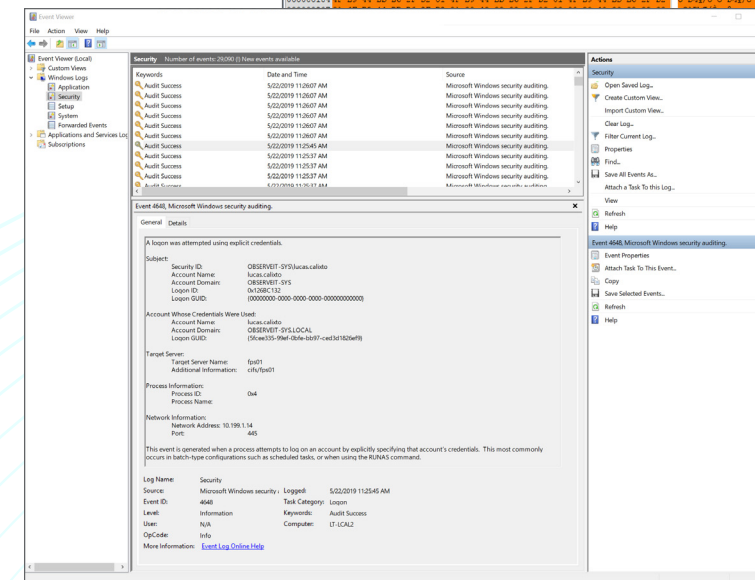
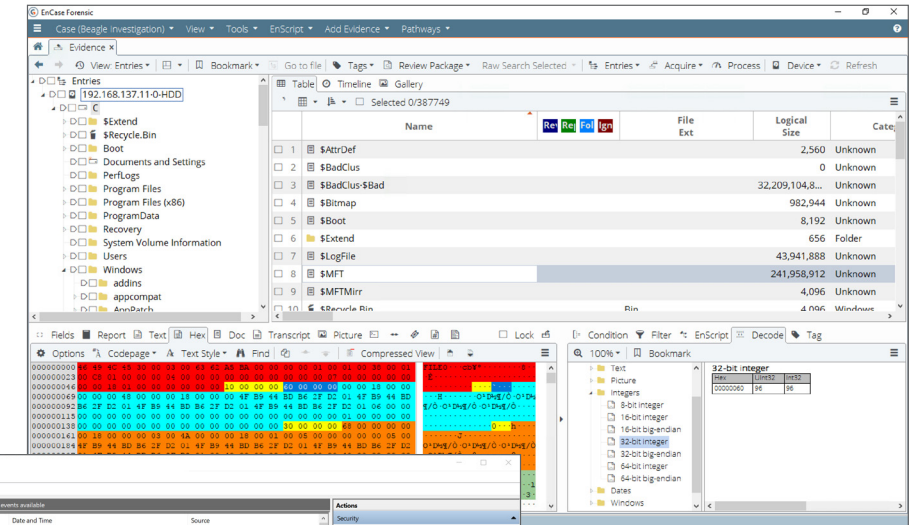
Source: Microsoft Windows Logs

# Step 3 Determining User Actions

Once you have dug up the appropriate logs, you will need to determine what the perpetrator was up to. For example, you will need to figure out whether there is any history around this user that will help you understand what they did and why.

- Is it a disgruntled former employee attempting to exfiltrate data? (**intentional threat**)
- Or someone who simply slipped up and did something out of policy? (**accidental threat**)

Context is crucial, and it can be very difficult to build on an ad-hoc basis. Pictured on the right are typical log files and security solutions used to investigate insider threats.



Source: <https://blogs.opentext.com>

Source: Microsoft Windows Logs

# Step 4 Building Evidence

**Finally, when it is clear what happened, you will need to build evidence.** You can't simply go to leadership (or the authorities if it is a legal issue) and say, "This is what happened." You need proof, which can be especially hard to provide when all you have to work with is logs.

In case your organization needs to move forward with legal action, you must know what type of digital forensic evidence is admissible to law enforcement. If you suspect that there's a possibility of criminal activity, seek help from outside legal experts early in the process to make these determinations.



# Ad-Hoc Investigations are **Not Ideal**

Conducting Insider Threat investigations on an ad-hoc basis, as you can see, **is not ideal.**

It is:

- **Inefficient**
- **Time-consuming**
- **Lacking in context**
- **Difficult to dig deep enough**
- **High risk**

Ineffective investigational tools can really slow down the entire process, and in the meantime, the threat may continue to evolve and put the business at great risk of reputational damage or cost. According to Deloitte, average remediation costs can exceed \$10 million. This cost is also largely dependent on the size of the organization, the extent of the damage, and required mitigation actions.

**Investing in tools that are purpose-built for Insider Threat Management can increase accuracy and efficiency of investigations.** This is a very common threat source today, and having tools that can quickly provide the appropriate context can protect your organization's reputation and resources.



---

# Insider Threat Investigations with ObserveIT

Proactive Insider Threat Hunting and  
Reactive Incident Investigation



# Scenario 1 Insider Threat Hunting (Proactive Investigation)

Insider Threat hunting means taking a look at your riskiest users' behavior on a regular basis.

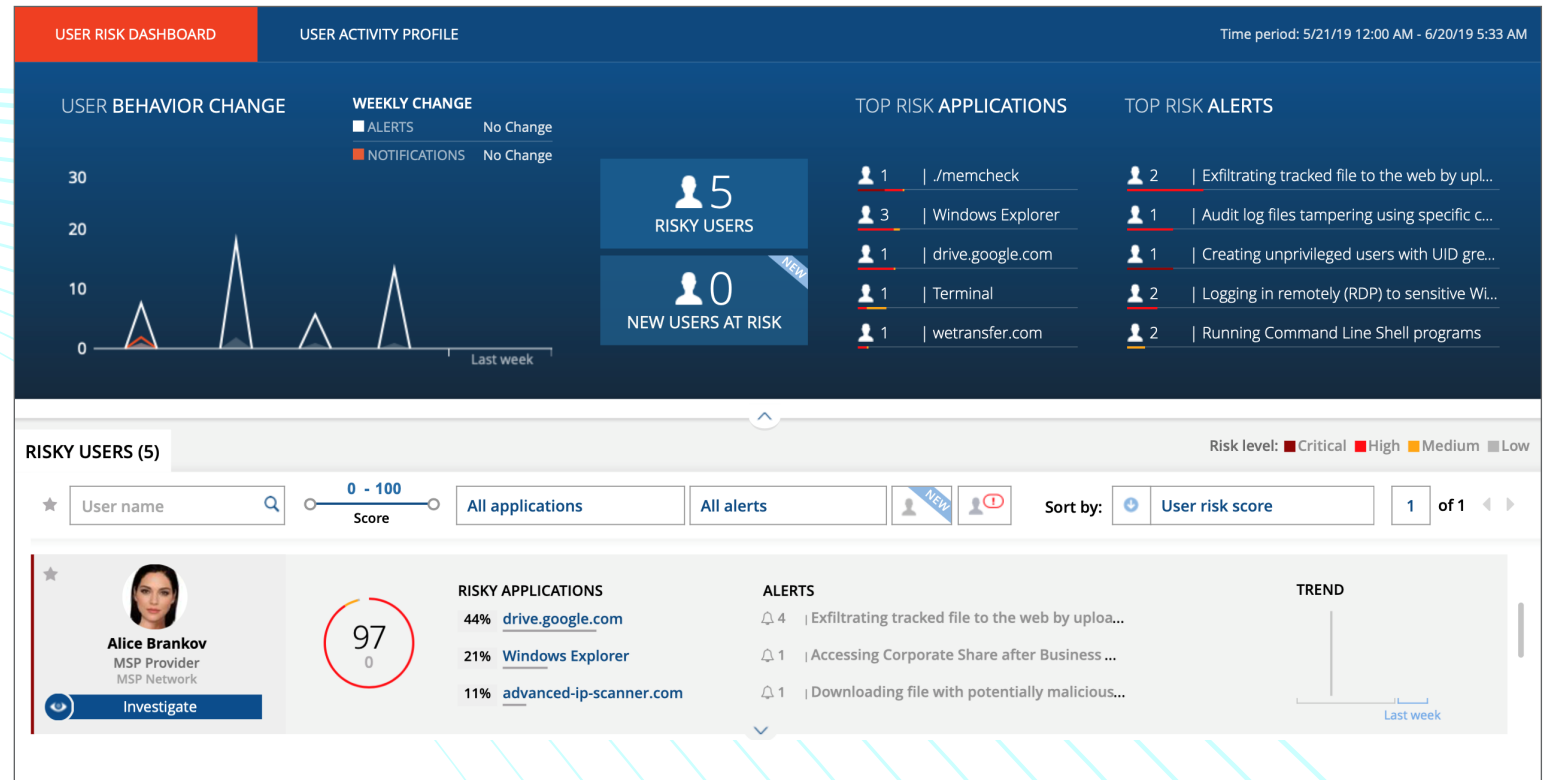
If you spot anomalous behavior during one of these routine checks, you can take a deeper look.



# Gathering Intel

## Insider Threat Intelligence Screen

It all starts with a proactive threat analyst looking at the riskiest users on a regular basis. If the analyst sees some risky behavior, they will proceed to investigate the user behind it.



Source: ObserveIT Insider Threat Management Platform

# Diving Into Specific Alerts

## Alerts Screen

Next, the analyst will want to get more context around the “who, what, where, when and why” on this specific alert. A timeline view correlates intelligence about the user, application, file, critical system, and the user’s actions and presents it in an easy-to-understand format.

In these examples within the ObserveIT platform, you can see that the user, Derek F, opened a root shell using a non-standard command, and hid files by moving them to a hidden directory. In the Alerts view, it becomes evident that this user has been abusing his privileges, and is up to something suspicious.

The image displays two screenshots of the ObserveIT Alerts screen, showing detailed information for specific alerts.

**Alert 1: Exfiltrating tracked file to the web by uploading**

- Who?** observeitdemo.com\Brian.c
- Did What?**
  - File operation trigger: Upload
  - Exfiltrated file name: Hey\_ya.mp3 [View File History](#)
  - Original file name: Client-Profiles-2017.xlsx
  - To website/web-application: uploadfiles.io
  - To website/web-application: https://uploadfiles.io
  - To website category: Storage
  - Originated from website: observeit.my.salesforce.com
  - Originated from website: https://observeit.my.salesforce.com/sfc/#version?selectedDocumentId=069w00000056vak
  - Originated from website category: Computing & Internet
- On Which Computer?** WIN-DESKLAB01 | 10.0.2.83
- From Which Client?** LT-MGORDY (192.168.1.236)
- When?** Monday, 7/8/2019 8:35 AM (Server time: 10:35 PM)

**Alert 2: Accessing unauthorized upload and sharing cloud services**

- Who?** observeitdemo.com\Brian.c
- Did What?**
  - Visited url: **https://uploadfiles.io**
  - Visited url categorized: Storage
- On Which Computer?** WIN-DESKLAB01 | 10.0.2.83
- From Which Client?** LT-MGORDY (192.168.1.236)
- When?** Monday, 7/8/2019 8:35 AM (Server time: 10:35 PM)







































Source: ObserveIT Insider Threat Management Platform

# Gathering Context

## Timeline View

Next, the analyst will want to get more context around the “who, what, where, when and why” of this specific alert. TA timeline view brings together user and application data, including details on the user’s actions and the file system in question.

Once they have this context, they will want to examine whether the information explains the validity of the user action that lead to the alert (case closed). Or, on the other hand, does the information illuminate an actual insider threat action?

11:32:39 AM	www.advanced-ip-scanner.com	<a href="#">Downloaded/exported file "Advanced_IP_Scanner_2.5.3850.exe" from www.advanced-ip-scanner.com to C:\Users\oit-serviceaccount\Downloads\</a>	 
11:32:53 AM	Setup/Uninstall	Select Setup Language	 
11:32:56 AM		Setup - Advanced IP Scanner 2.5	 
11:33:04 AM	advanced_ip_scanner	Advanced IP Scanner	
11:34:32 AM	Windows Explorer	\\10.0.2.226\Corporate Share Folder	 
11:34:38 AM		\\10.0.2.226\Corporate Share Folder\Data Sets 2017	 
11:35:33 AM	LibreOffice	Patient Records.xlsx (read-only) - LibreOffice Calc	
11:35:51 AM	Search and Cortana application	Search	
11:35:56 AM	Windows PowerShell	Windows PowerShell	 
11:36:22 AM		Select Administrator: Windows PowerShell	 
11:36:27 AM		Administrator: Windows PowerShell	 
11:36:46 AM	LibreOffice	Patient Records.xlsx (read-only) - LibreOffice Calc	
11:37:53 AM	Windows Explorer	\\10.0.2.226\Corporate Share Folder\Data Sets 2017	
11:38:02 AM		FILECOPY (4, 0.342MB) - [FOUO] Declared Statements.doc, HR_Records.pdf, Patient Records.xlsx, Payment_Information.pdf, origin=...26\Corporate Share Folder\Data Sets 2017	 
11:38:03 AM	 advanced-ip-scanner.com	Advanced IP Scanner - Download Free Network Scanner. - Google Chrome	
11:38:05 AM	 drive.google.com	Google Drive - Google Chrome	 
11:38:10 AM		My Drive - Google Drive - Google Chrome	 
11:38:16 AM		<a href="#">Uploaded file "Payment_Information.pdf" to drive.google.com from \\Device\Mup\10.0.2.226\Corporate Share Folder\Data Sets 2017\</a>	 
11:38:16 AM		<a href="#">Uploaded file "Patient Records.xlsx" to drive.google.com from \\Device\Mup\10.0.2.226\Corporate Share Folder\Data Sets 2017\</a>	 
11:38:16 AM		<a href="#">Uploaded file "[FOUO] Declared Statements.doc" to drive.google.com from \\Device\Mup\10.0.2.226\Corporate Share Folder\Data Sets 2017\</a>	 
11:38:16 AM		<a href="#">Uploaded file "HR_Records.pdf" to drive.google.com from \\Device\Mup\10.0.2.226\Corporate Share Folder\Data Sets 2017\</a>	 

Source: ObserveIT Insider Threat Management Platform

# Building Evidence

## Diary Screens

If this incident is considered “out of policy” and egregious enough, then the analyst will need to leverage User, File, Email and Endpoint diaries to understand exactly what happened. Using ObserveIT, they can navigate Endpoint diaries if a critical system is in question, or User, File or Email diaries for all other reasons

In this example, the analyst is viewing the Email Diary to gather more evidence about the suspicious activity taken by user.

The screenshot displays the ObserveIT Email Diary interface. The top navigation bar includes: ENDPOINT DIARY, USER DIARY, FILE DIARY, EMAIL DIARY (highlighted), DBA ACTIVITY, ALERTS, CONFIGURATION, SEARCH, and REPORTS. The left sidebar contains: Email Activity (highlighted), Latest Sessions (listing users like John.m, Derek F, brian.c, alice.b, antonio.l), Quick Help (User Guide, Configuration Guide), and a search bar.

The main content area shows the Email Activity filter section with fields for Period (Last 1 Months), Subject, From, Recipient, Recipient domains (All selected), Attachment name, Attachment existence (Any), Endpoint (All), User Login (All), and Recipients domains type (Any). A 'Show' button and 'Reset' link are present.

Below the filters is a table of email activity with columns: Time, Subject, From, Recipients, Attachments, Login, Endpoint Name, IP, and Session. The table shows 5 items, with the first one expanded to show details.

Time	Subject	From	Recipients	Attachments	Login	Endpoint Name	IP	Session
7/08/2019								
08:33 AM	Your favorite song	oituser888@gmail.com	tim.armstrong@obs...	Hey_ya.mp3 (219 KB)	Brian.c	WIN-DESKLAB01		
7/02/2019								
08:54 AM		oituser888@gmail.com	oituser888@gmail.com	Rebel_Rebel.mp3 (219 KB)	brian.c	WIN-DESKLAB01		
08:53 AM	Song you like	oituser888@gmail.com	Kevin.donovan@obs...	Rebel_Rebel.mp3 (219 KB)	brian.c	WIN-DESKLAB01		
6/27/2019								
02:30 PM	The file you requested	oituser888@gmail.com	Kevin.donovan@obs...	Client-Profiles-2... (219 KB)	brian.c	WIN-DESKLAB01		

The expanded email details show:

- Subject: The file you requested
- From: oituser888@gmail.com
- To: Kevin.donovan@observeit.com
- Bcc: oituser888@gmail.com
- Attached files: Client-Profiles-2017.xlsx (219 KB)

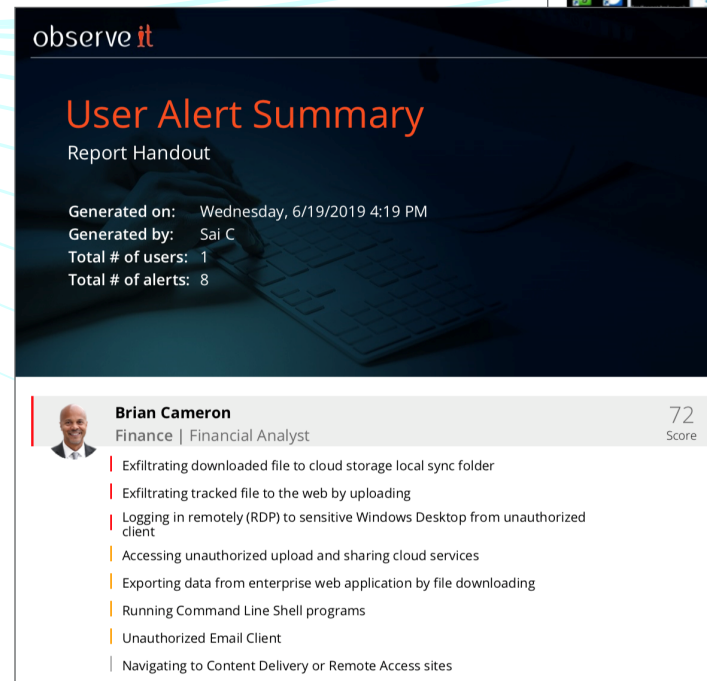
Source: ObserveIT Insider Threat Management Platform

# Confirming and Sharing Evidence

## ObserveIT Reports

At the end of the evidence-gathering stage, the analyst can use ObserveIT's screen recording features to confirm their suspicion. Visual activity replays can back up the metadata evidence gathered from the Diaries screen.

Once the evidence is confirmed, the analyst can share the screen recording and metadata as an easy-to-understand report for Legal, HR and other stakeholders on the incident response team for decision-making purposes.



The screenshot shows a 'User Alert Summary' report for Brian Cameron. It includes a 'Report Handout' section with the following statistics: Generated on: Wednesday, 6/19/2019 4:19 PM; Generated by: Sai C; Total # of users: 1; Total # of alerts: 8. Below this is a list of alert details for Brian Cameron, including actions like 'Exfiltrating downloaded file to cloud storage local sync folder' and 'Exfiltrating tracked file to the web by uploading'.

**observe it**

### User Alert Summary

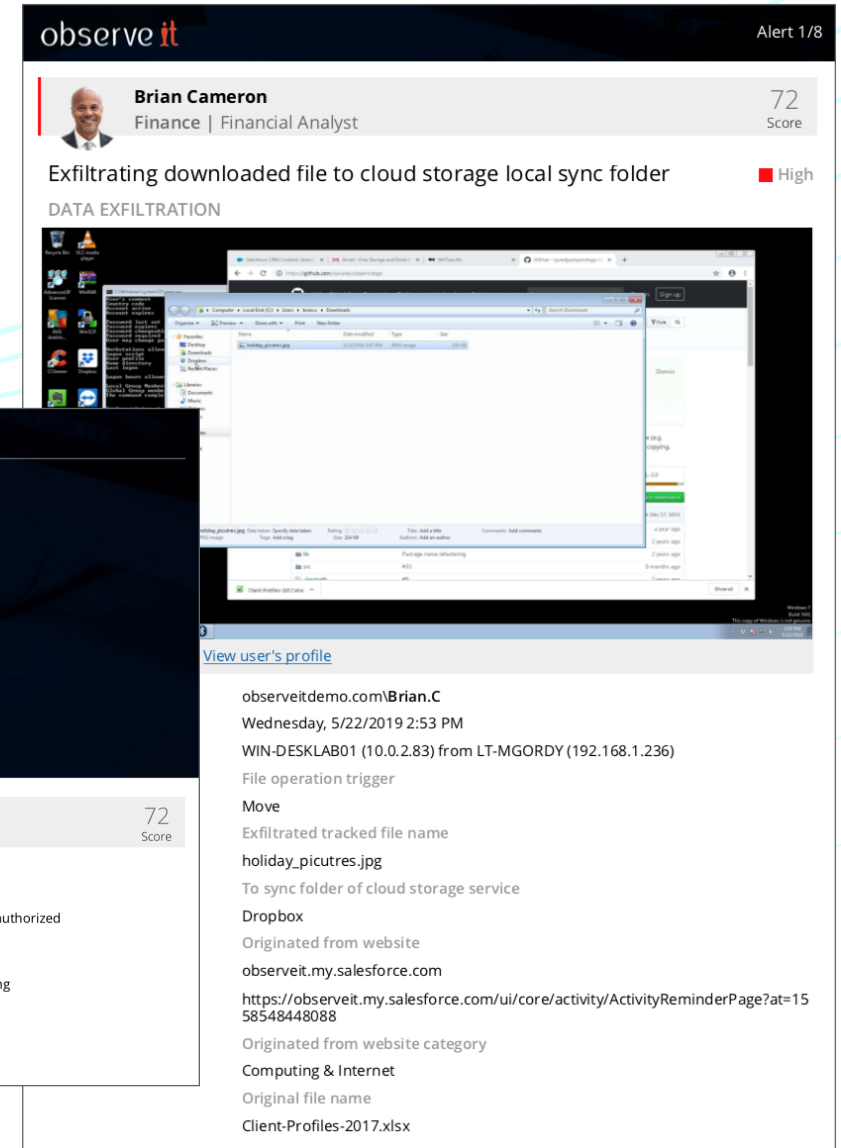
Report Handout

Generated on: Wednesday, 6/19/2019 4:19 PM  
Generated by: Sai C  
Total # of users: 1  
Total # of alerts: 8

**Brian Cameron** | Finance | Financial Analyst | 72 Score

- Exfiltrating downloaded file to cloud storage local sync folder
- Exfiltrating tracked file to the web by uploading
- Logging in remotely (RDP) to sensitive Windows Desktop from unauthorized client
- Accessing unauthorized upload and sharing cloud services
- Exporting data from enterprise web application by file downloading
- Running Command Line Shell programs
- Unauthorized Email Client
- Navigating to Content Delivery or Remote Access sites

Source: ObserveIT Insider Threat Management Platform



The screenshot displays an ObserveIT alert for Brian Cameron with a score of 72. The alert title is 'Exfiltrating downloaded file to cloud storage local sync folder' with a 'High' severity. It includes a 'DATA EXFILTRATION' section with a screenshot of a Windows file explorer window showing a file named 'holiday\_pictures.jpg' being moved to a cloud storage sync folder. Below this is a 'View user's profile' section with detailed metadata: observeitdemo.com\Brian.C, Wednesday, 5/22/2019 2:53 PM, WIN-DESKLAB01 (10.0.0.2.83) from LT-MGORDY (192.168.1.236), File operation trigger, Move, Exfiltrated tracked file name, holiday\_pictures.jpg, To sync folder of cloud storage service, Dropbox, Originated from website, observeit.my.salesforce.com, https://observeit.my.salesforce.com/ui/core/activity/ActivityReminderPage?at=1558548448088, Originated from website category, Computing & Internet, Original file name, Client-Profiles-2017.xlsx.

**observe it** | Alert 1/8

**Brian Cameron** | Finance | Financial Analyst | 72 Score

Exfiltrating downloaded file to cloud storage local sync folder ■ High

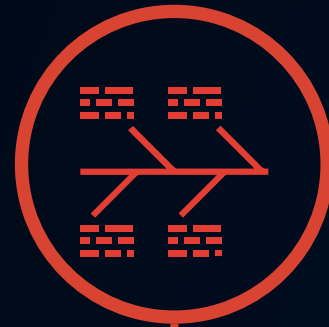
DATA EXFILTRATION

View user's profile

observeitdemo.com\Brian.C  
Wednesday, 5/22/2019 2:53 PM  
WIN-DESKLAB01 (10.0.0.2.83) from LT-MGORDY (192.168.1.236)  
File operation trigger  
Move  
Exfiltrated tracked file name  
holiday\_pictures.jpg  
To sync folder of cloud storage service  
Dropbox  
Originated from website  
observeit.my.salesforce.com  
https://observeit.my.salesforce.com/ui/core/activity/ActivityReminderPage?at=1558548448088  
Originated from website category  
Computing & Internet  
Original file name  
Client-Profiles-2017.xlsx

Source: ObserveIT Insider Threat Management Platform

# Scenario 2 Reactive Incident Investigation



1

An **ALERT**  
is triggered

2

**SEARCH  
SCREEN**  
provides a  
microscope

3

**TIMELINE**  
view gives  
context

4

**DIARY SCREENS**  
illuminate  
details

5

**REPORTS**  
confirm  
evidence



# An Alert is Triggered

In the **Alerts Screen**, the analyst can get a real-time view of all suspicious user activity at any given time, and dig in to learn more about a potential insider threat incident. Or, if an alert is triggered from an external security solution, an analyst can gather further detail into user activity within ObserveIT. In these examples, you can see that the user is accessing an unauthorized cloud storage website and uploading seemingly sensitive data to unknown websites. These look like out of policy violations, which need further investigation.

The image displays two screenshots of the ObserveIT Alerts screen. The top screenshot shows an alert titled "Exfiltrating tracked file to the web by uploading". The bottom screenshot shows an alert titled "Accessing unauthorized upload and sharing cloud services". Both alerts are for user "Brian.c" on computer "WIN-DESKLAB01".

Alert Title	Who?	Did What?	On Which Computer?	From Which Client?	When?
Exfiltrating tracked file to the web by uploading	observeitdemo.com\Brian.c	File operation trigger: Upload Exfiltrated file name: Hey_ya.mp3 Original file name: Client-Profiles-2017.xlsx To website/web-application: uploadfiles.io To website category: Storage Originated from website: observeit.my.salesforce.com Originated from website category: Computing & Internet	WIN-DESKLAB01   10.0.2.83	LT-MGORDY (192.168.1.236)	Monday, 7/8/2019 8:35 AM (Server time: 10:35 PM)
Accessing unauthorized upload and sharing cloud services	observeitdemo.com\Brian.c	Visited url: https://uploadfiles.io Visited url categorized: Storage	WIN-DESKLAB01   10.0.2.83	LT-MGORDY (192.168.1.236)	Monday, 7/8/2019 8:35 AM (Server time: 10:35 PM)

Source: ObserveIT Insider Threat Management Platform

# Search Screen Provides a Microscope

Using the **Search Screen**, the analyst can learn more about any activity related to the search term of interest. In this case, you can see various instances “gmail” came up, across users, user sessions, applications and endpoints.

The session history can be viewed as a summary or timeline, or the analyst can choose to view a video playback of the potential incident.

With ObserveIT, analysts can search many different forms of metadata, including username, machine type, application used, file name, and more.

The screenshot displays the ObserveIT Search interface. At the top, there is a search bar with the term 'gmail' entered. To the right, a dropdown menu is set to 'All common fields'. Below the search bar, a filter indicates 'Limit search to: Last 3 Months'. A 'Search' button and a 'Reset' link are visible on the right. The results section shows '6 Sessions' for the date '7/8/2019'. A table lists the search results with columns for Time, Endpoint Name, Client Name, Name, and Video. The first row shows a login event at 10:25:14 PM from endpoint WIN-DESKLAB01. Subsequent rows show Outlook and Chrome sessions, with one Chrome session displaying a Google search for 'gmail'. The final row shows an Outlook session with an email activity log for an email sent from oituser888@gmail.com to tim.armstrong@observeit.com.

Time	Endpoint Name	Client Name	Name	Video
7/8/2019				
10:25:14 PM	WIN-DESKLAB01	LT-MGORDY	observeitdemo.com\Brian.c (login)	<a href="#">View session</a>
10:26:21 PM	Microsoft Outlook		Window title: Inbox - oituser888@gmail.com - Outlook	<a href="#">▶</a>
10:31:38 PM	Google Chrome		URL: https://www.google.com/search?q=gmail&rlz=1C1GCEU_enUS823US823&oq=gmail&aqs=chrome..69i57j0l5.1299j0j7&so	<a href="#">▶</a>
10:31:40 PM	Google Chrome		Window title: gmail - Google Search - Google Chrome	<a href="#">▶</a>
10:31:51 PM	Google Chrome		Window title: Inbox (285) - oituser888@gmail.com - Gmail - Google Chrome	<a href="#">▶</a>
10:33:10 PM	Microsoft Outlook		Email Activity: Email sent using an email client Subject: Your favorite song Email From: oituser888@gmail.com Email To: tim.armstrong@observeit.com Email BCC: oituser888@gmail.com Attached files: 'Hey_ya.mp3' (0.210MB)	<a href="#">▶</a>

Source: ObserveIT Insider Threat Management Platform

# Timeline View Gives Context

The analyst can then click into a specific user's timeline to investigate the user's activity further.

From the timeline view, the analyst can see who did what, on which computer, from which client, and when.

They can then view a video playback of a user's session to confirm their suspicions.

USER ACTIVITY (WINDOW TITLES)		
Time ^	Application/Website	Activity Details
8:33:10 AM	Microsoft Outlook	Sent email including file(s) "Hey_ya.mp3" From: oituser888@gmail.com Recipients (Untrusted recipient domains): tim.armstrong@observeit.com, oituser888@gm... Subject: Your favorite song
10:25:42 PM	Windows Explorer	Start
10:26:08 PM	Windows Explorer	Program Manager
10:26:10 PM	Windows Explorer	Start menu
10:26:21 PM	Microsoft Outlook	Inbox - oituser888@gmail.com - Outlook
10:26:25 PM	Windows Explorer	Program Manager
10:26:44 PM	Google Chrome	
10:26:54 PM	salesforce.com	Salesforce.com: The Customer Success Platform To Grow Your Business - Google Chrome
10:26:56 PM	login.salesforce.com	Login   Salesforce - Google Chrome
10:26:57 PM		Paste of text (encrypted data) in Login   Salesforce - Google Chrome
10:27:06 PM	observeit.my.salesforce.com	Salesforce - Enterprise Edition - Google Chrome
10:27:10 PM		Salesforce CRM Content: Search Content - Google Chrome
10:27:18 PM		Salesforce CRM Content: Client-Profiles-2017 - Google Chrome
10:27:19 PM		Downloaded/exported file "Client-Profiles-2017.xlsx" from observeit.my.salesforce.com to C:\Users\brian.c\Downloads
10:28:43 PM	Microsoft Excel	Client-Profiles-2017.xlsx - Protected View - Excel
10:30:11 PM		Client-Profiles-2017.xlsx - Excel
10:30:20 PM		LARGEPRINTJOB - document=[Client-Profiles-2017.xlsx], printer=[Send To OneNote 2016], num-of-pages=[15]
10:30:25 PM		Client-Profiles-2017.xlsx - Excel
10:30:43 PM	Microsoft Corporation	Client-Profiles-2017.xlsx - Excel
10:30:45 PM	Microsoft Outlook	Inbox - oituser888@gmail.com - Outlook
10:30:47 PM		Untitled - Message (HTML)
10:31:03 PM		Paste of the image in Untitled - Message (HTML)

Source: ObserveIT Insider Threat Management Platform

# Diary Screens Illuminate Details

Once the analyst finds the user at fault, they'll go to **User, Email, File or Endpoint diaries** to quickly add more evidence before, during and after incident(s) in question. Pictured here is an Email Diary in ObserveIT

The screenshot displays the ObserveIT Email Diary interface. The top navigation bar includes: ENDPOINT DIARY, USER DIARY, FILE DIARY, EMAIL DIARY (highlighted), DBA ACTIVITY, ALERTS, CONFIGURATION, SEARCH, and REPORTS. The left sidebar contains: Email Activity (highlighted), Latest Sessions (listing users like john.m, Derek F, brian.c, alice.b, antonio.l), Quick Help (User Guide, Configuration Guide), and a footer with User Guide and Configuration Guide.

The main content area is titled "Email Activity" and features a filter section with the following options:

- Period: Last 1 Months (selected), Between 06/12/2019 to 07/12/2019
- Subject: [Text Input]
- From: [Text Input]
- Recipient: [Text Input]
- Recipient domains: All selected
- Attachment name: [Text Input]
- Attachment existence: Any
- Endpoint: All
- User Login: All
- Recipients domains type: Any

Buttons for "Show" and "Reset" are located at the bottom right of the filter section. Below the filters, a table displays email activity with columns: Time, Subject, From, Recipients, Attachments, Login, Endpoint Name, IP, and Session. The table shows 5 items, with the first item expanded to show details.

Time	Subject	From	Recipients	Attachments	Login	Endpoint Name	IP	Session
<b>7/08/2019</b>								
08:33 AM	Your favorite song	oituser888@gmail.com	tim.armstrong@obs...	Hey_ya.mp3 (219 KB)	Brian.c	WIN-DESKLAB01		
<b>7/02/2019</b>								
08:54 AM		oituser888@gmail.com	oituser888@gmail.com	Rebel_Rebel.mp3 (219 KB)	brian.c	WIN-DESKLAB01		
08:53 AM	Song you like	oituser888@gmail.com	Kevin.donovan@obs...	Rebel_Rebel.mp3 (219 KB)	brian.c	WIN-DESKLAB01		
<b>6/27/2019</b>								
02:30 PM	The file you requested	oituser888@gmail.com	Kevin.donovan@obs...	Client-Profiles-2... (219 KB)	brian.c	WIN-DESKLAB01		

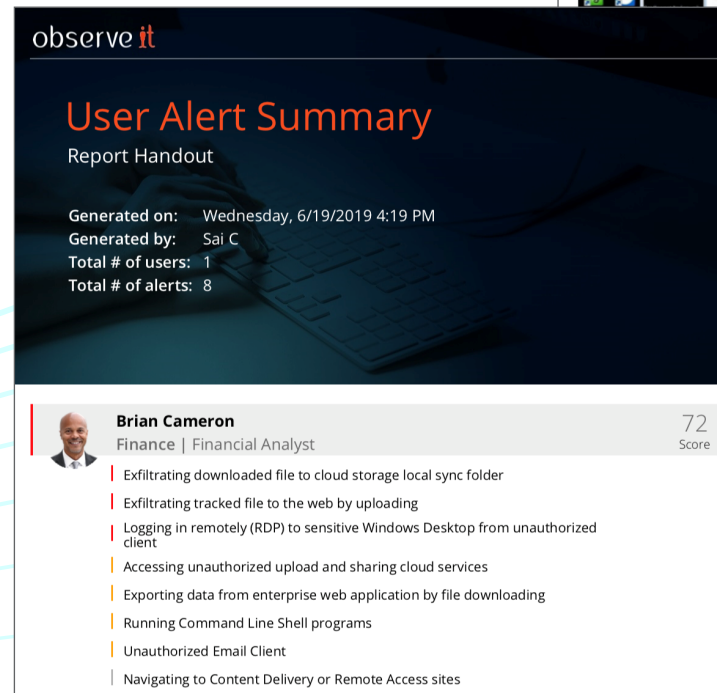
Expanded email details for the selected item:

- Subject: The file you requested
- From: oituser888@gmail.com
- To: Kevin.donovan@observeit.com
- Bcc: oituser888@gmail.com
- Attached files: Client-Profiles-2017.xlsx (219 KB)

Source: ObserveIT Insider Threat Management Platform

# Reports Confirm Evidence

Once the analyst collects relevant information, they can export it into easy-to-understand **User Alert Summaries** and **ObserveIT Reports** to send to Legal, HR or other stakeholders in the incident response chain of command.



**observe it**

## User Alert Summary

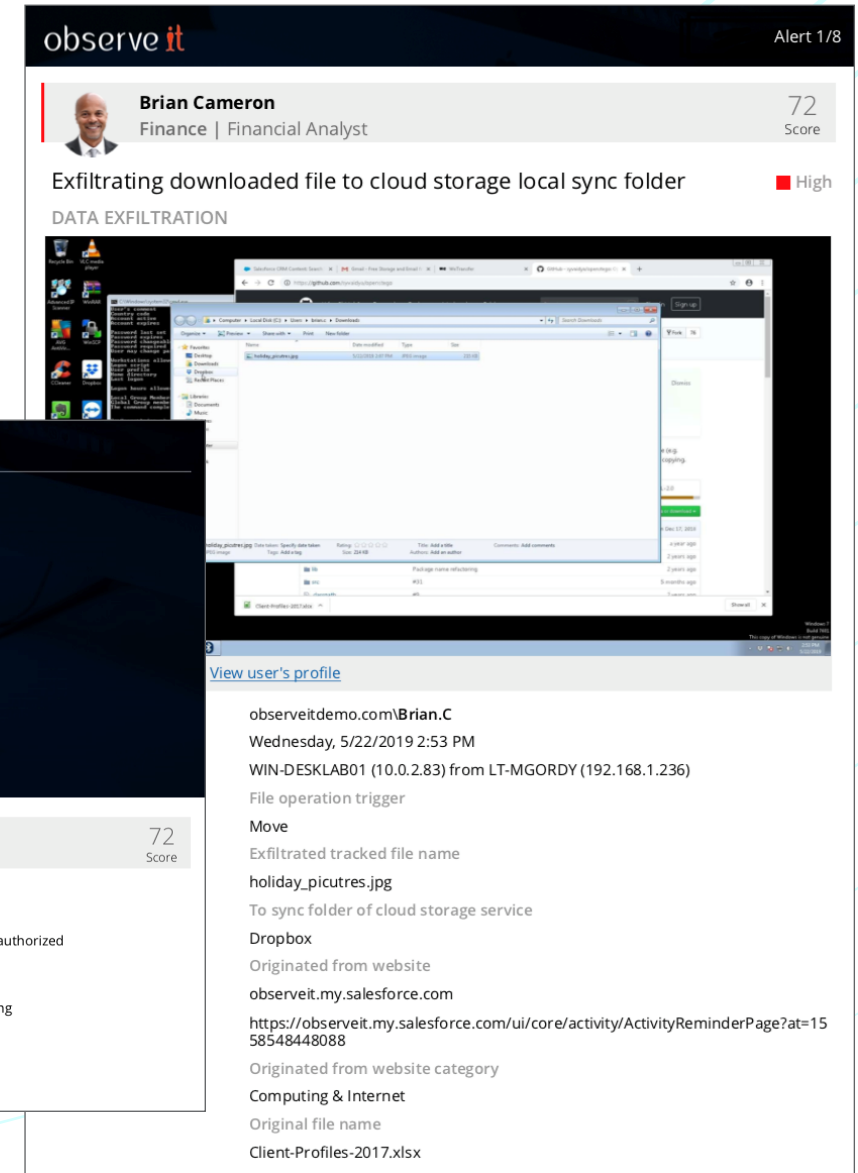
Report Handout

Generated on: Wednesday, 6/19/2019 4:19 PM  
Generated by: Sai C  
Total # of users: 1  
Total # of alerts: 8

**Brian Cameron**  
Finance | Financial Analyst  
72 Score

- Exfiltrating downloaded file to cloud storage local sync folder
- Exfiltrating tracked file to the web by uploading
- Logging in remotely (RDP) to sensitive Windows Desktop from unauthorized client
- Accessing unauthorized upload and sharing cloud services
- Exporting data from enterprise web application by file downloading
- Running Command Line Shell programs
- Unauthorized Email Client
- Navigating to Content Delivery or Remote Access sites

Source: ObserveIT Insider Threat Management Platform

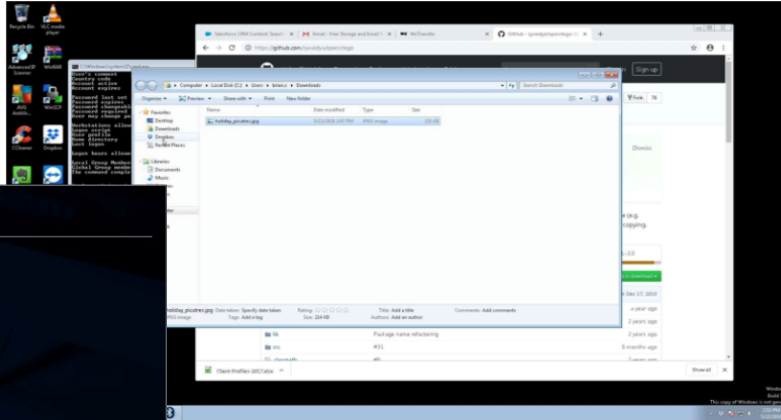


**observe it** Alert 1/8

**Brian Cameron**  
Finance | Financial Analyst  
72 Score

Exfiltrating downloaded file to cloud storage local sync folder ■ High

DATA EXFILTRATION



[View user's profile](#)

observeitdemo.com\Brian.C  
Wednesday, 5/22/2019 2:53 PM  
WIN-DESKLAB01 (10.0.2.83) from LT-MGORDY (192.168.1.236)  
File operation trigger  
Move  
Exfiltrated tracked file name  
holiday\_pictures.jpg  
To sync folder of cloud storage service  
Dropbox  
Originated from website  
observeit.my.salesforce.com  
https://observeit.my.salesforce.com/ui/core/activity/ActivityReminderPage?at=1558548448088  
Originated from website category  
Computing & Internet  
Original file name  
Client-Profiles-2017.xlsx

Source: ObserveIT Insider Threat Management Platform

# Context is Always King

As you can see, ObserveIT's timeline, search function, user diary, and other features make it much easier to gather the necessary context around an insider threat incident—whether it is discovered reactively or proactively. Having a purpose-built insider threat management solution makes it possible to build a case in a time-sensitive fashion and take appropriate action to protect the organization and mitigate further risks.

---

Want to see how ObserveIT could work for your organization?  
[Request a demo](#) of ObserveIT today.

observe **it**

©2019, ObserveIT. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for information purposes only.