safetica

SECURITY AUDIT REPORT

18/12/2023 – 18/01/2024

Contents

Scope of Security Audit 1

Files transferred to USB or other external devices 3

Files sent via email 5

Files sent via webmail 7

Files uploaded to the web 9

Files sent via instant messaging 11

Files transferred to cloud storage 13

Analysis of application usage 15

Analysis of website usage 16

Use of IT resources – printing 18

SCOPE OF SECURITY AUDIT

The Security Audit focuses on sensitive files in the company environment, on files that leave the company, and on how users use company resources.

It is based on audited files and user activity on devices with installed Safetica. The security issues and recommended precautions are based on your settings - on what is considered sensitive in your company, on the safe methods you use for transferring sensitive files, and on risky activities carried out by users.

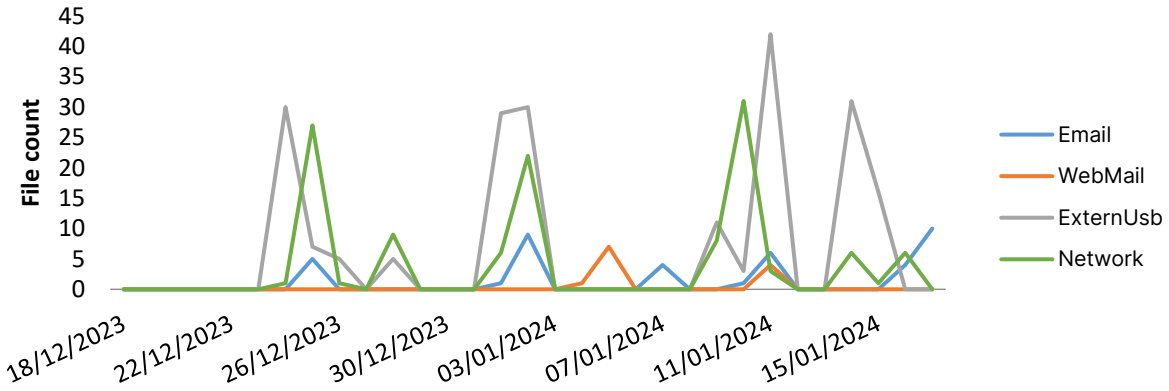
AUDITED DATA

- **4 GB** of data
- **1,012** file operations
- **1,000** files
- **433** outgoing files

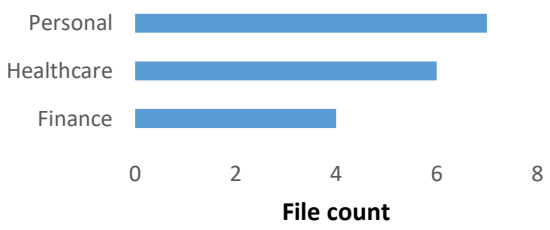
AUDITED ENVIRONMENT

- **179** user accounts
- **0** devices with Safetica
- **28** devices in total
- **76** Safetica admin accounts

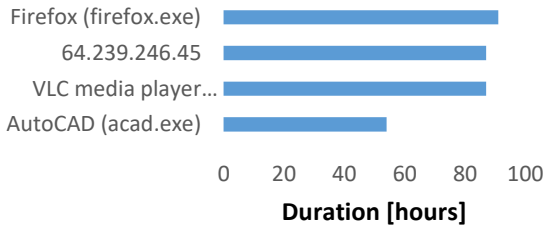
When were sensitive files sent?



What data classifications did files have?



What were the most common / activities?



When an incident occurs, a quick response is important to minimize negative impacts. Real-time alerts sent to the responsible individuals will help you quickly understand where the problem arose.

You don't have any real-time alerts set up for incidents.

Regular inspections of the company's security status are vital to your overall security strategy.

You have set up regular reports on the company's security status.

Without knowing which company data is sensitive, no policies can be applied to prevent data leaks.

You have identified sensitive company data that needs to be protected.

RECOMMENDATIONS

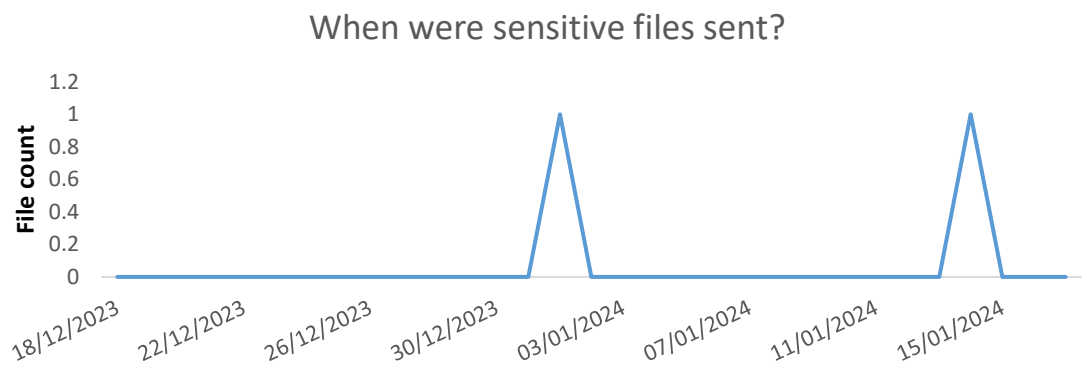
- Set real-time email alerts for all incidents you wish to audit.
- Check that the real-time alerts you set up are up-to-date and are addressed to the person responsible.
- Set automated reports for all relevant areas.
- Check that the reports you set up are up-to-date and are addressed to the person responsible.
- Check which files your users work with and identify sensitive content.
- Regularly classify files with sensitive content.

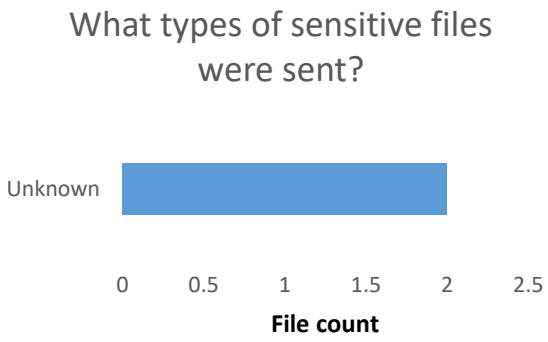
FILES TRANSFERRED TO USB OR OTHER EXTERNAL DEVICES

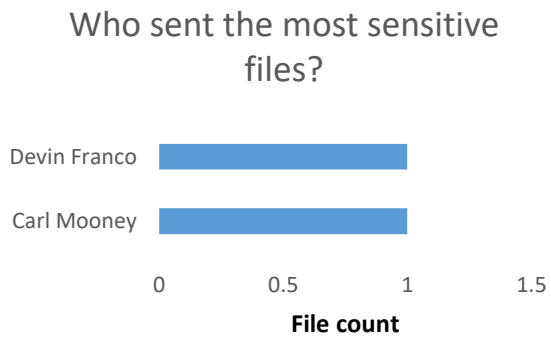
Transferring a large amount of sensitive files to a USB flash drive is a quick and easy way for a company to lose control of its data. If the USB is lost or stolen, critical data can fall into unauthorized hands.

Transferring data out of the company via a USB device is a significant risk. Ensuring that USB devices are secure is a necessary security measure.

2 sensitive files were transferred to USB or other external devices. These files were not controlled by any policy.







Overview of all files transferred to this destination type in the selected period:

Total files not identified as sensitive: 229

- non-blocking policies: 37 files
- blocked by policies: 40 files
- compliant to policies: 152 files

Total sensitive files: 2

- no policy: 2 files

Show detailed records in Safetica.

RECOMMENDATIONS

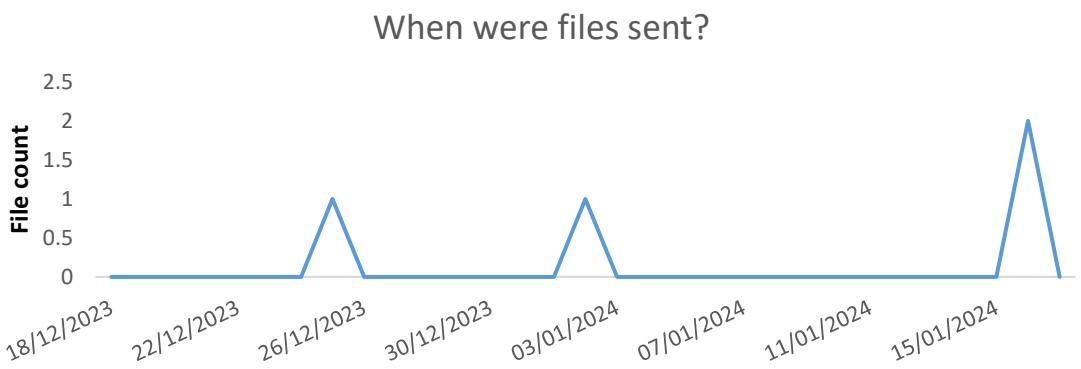
- Define and revise which USBs and other external devices are safe to use.
- Check which files are transferred. Evaluate if these need to be classified as sensitive.
- Make untrusted USBs and other external devices read-only or completely block access to them.
- Set policies for sensitive files transferred to USBs and other external devices.
- Set alerts for when sensitive files are transferred to untrusted USBs.
- Set email alerts for when somebody copies a large number of files to USBs.

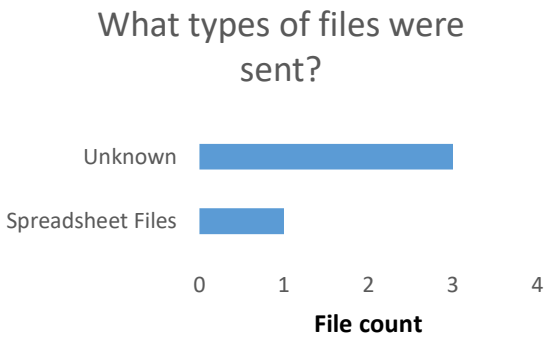
FILES SENT VIA EMAIL

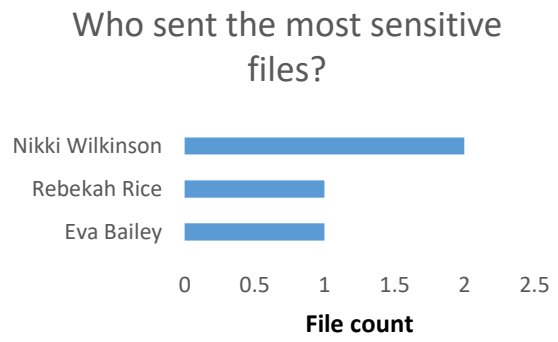
Email attachments are one of the most common ways for sensitive files to leak. In most cases, damage to the company is accidental rather than intentional – sending files to the wrong recipient or attaching a wrong file.

Emails with sensitive files should only be sent to trusted recipients who need to work with them.

4 files not identified as sensitive were transferred to email. Your policies were not blocking.







File samples:

Time	File	User	Destination
17/01/2024 11:06	military-digital-katie-couric-uruguay.xlsm	Eva Bailey	xhwmlkm@example.com
17/01/2024 11:05	right-hearing-20201109-style-moroni-60273581.xlsb	Eva Bailey	xhwmlkm@example.com
25/12/2023 13:57	sudan-books.xlsx	Eva Bailey	eva.bailey@personal.com
17/01/2024 11:04	wellington_military_tanzania.xls	Eva Bailey	xhwmlkm@example.com

Overview of all files transferred to this destination type in the selected period:

Total files not identified as sensitive: 40

- non-blocking policies: 4 files
- blocked by policies: 33 files
- compliant to policies: 3 files

Show detailed records in Safetica.

RECOMMENDATIONS

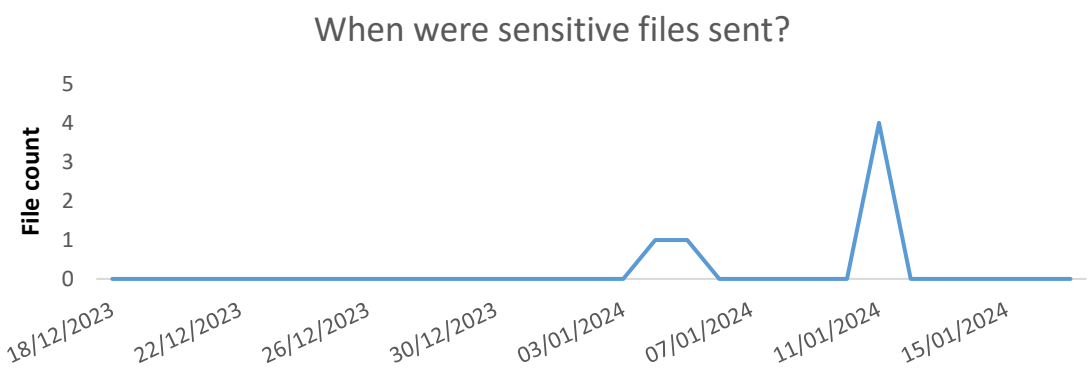
- Define and revise which email domains are considered safe in your company.
- Check which emails were sent with attachments. Evaluate if email attachments need to be classified as sensitive.
- Set policies for sensitive files sent via email.
- Set real-time email alerts for situations when sensitive files are sent to untrusted email domains.

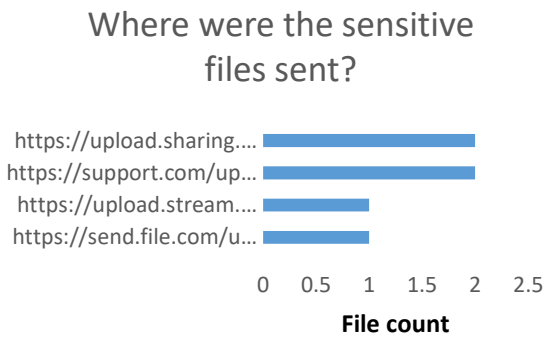
FILES SENT VIA WEBMAIL

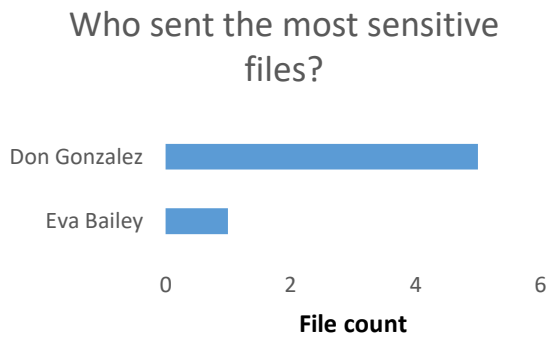
Webmail services are popular for communicating and sending sensitive files. For this reason, they pose a risk and need to be protected against potential data loss.

Using webmail services for sending sensitive files is a security issue as it is not possible to control recipients on the device.

6 sensitive files were transferred to webmail. Your policies were not blocking.







Overview of all files transferred to this destination type in the selected period:

Total files not identified as sensitive: 4

- compliant to policies: 4 files

Total sensitive files: 8

- non-blocking policies: 6 files
- blocked by policies: 1 files
- compliant to policies: 1 files

Show detailed records in Safetica.

RECOMMENDATIONS

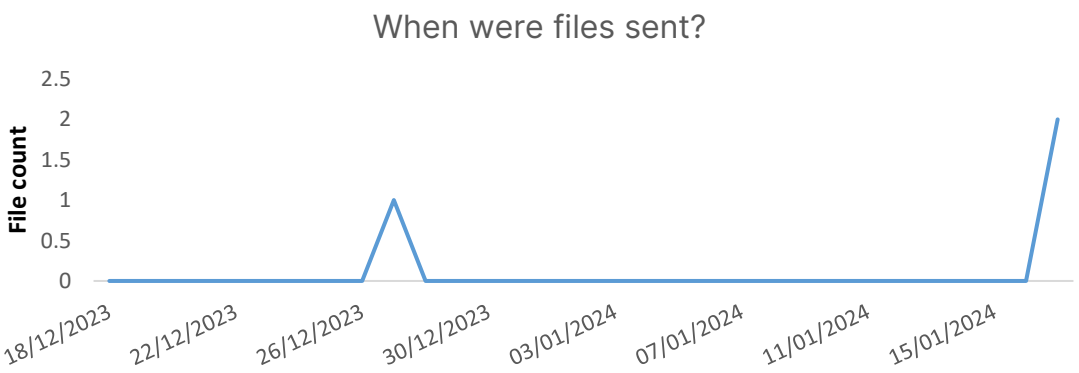
- Define and revise webmail domains that are considered safe by the company.
- Check which files are sent. Evaluate if these need to be classified as sensitive.
- Set policies for sensitive files sent via webmail domains.
- Set alerts for when sensitive files are sent via untrusted webmail domains.

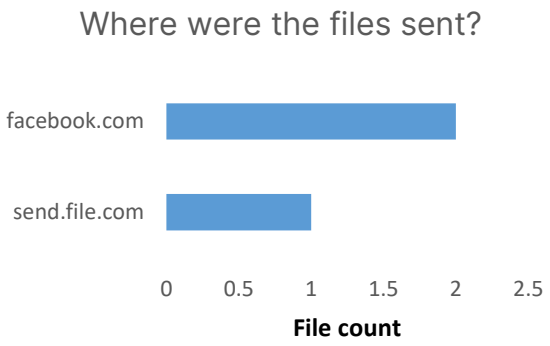
FILES UPLOADED TO THE WEB

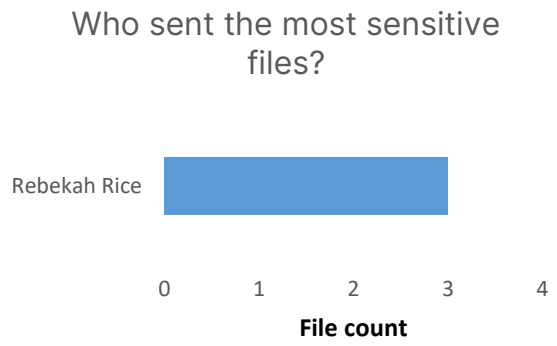
Uploading files to the web is a popular way for users to share larger files that can't be sent as email attachments. It is, therefore, important to create policies for web upload.

Company files uploaded to public websites can be instantly downloaded by strangers and thus you may lose control of them.

There was an attempt to transfer 3 files not identified as sensitive to web upload. Your policies blocked these file transfers.







File samples:

Time	File	User	Destination
27/12/2023 08:20	5535496-popup-chad.ai	Rebekah Rice	send.file.com
17/01/2024 11:49	malta_roof_don-drysdale_construction.woff2	Rebekah Rice	facebook.com
17/01/2024 11:49	mark-hamill_astana_style.wad	Rebekah Rice	facebook.com

Overview of all files transferred to this destination type in the selected period:

Total files not identified as sensitive: 9

- blocked by policies: 3 files
- compliant to policies: 6 files

Show detailed records in Safetica.

RECOMMENDATIONS

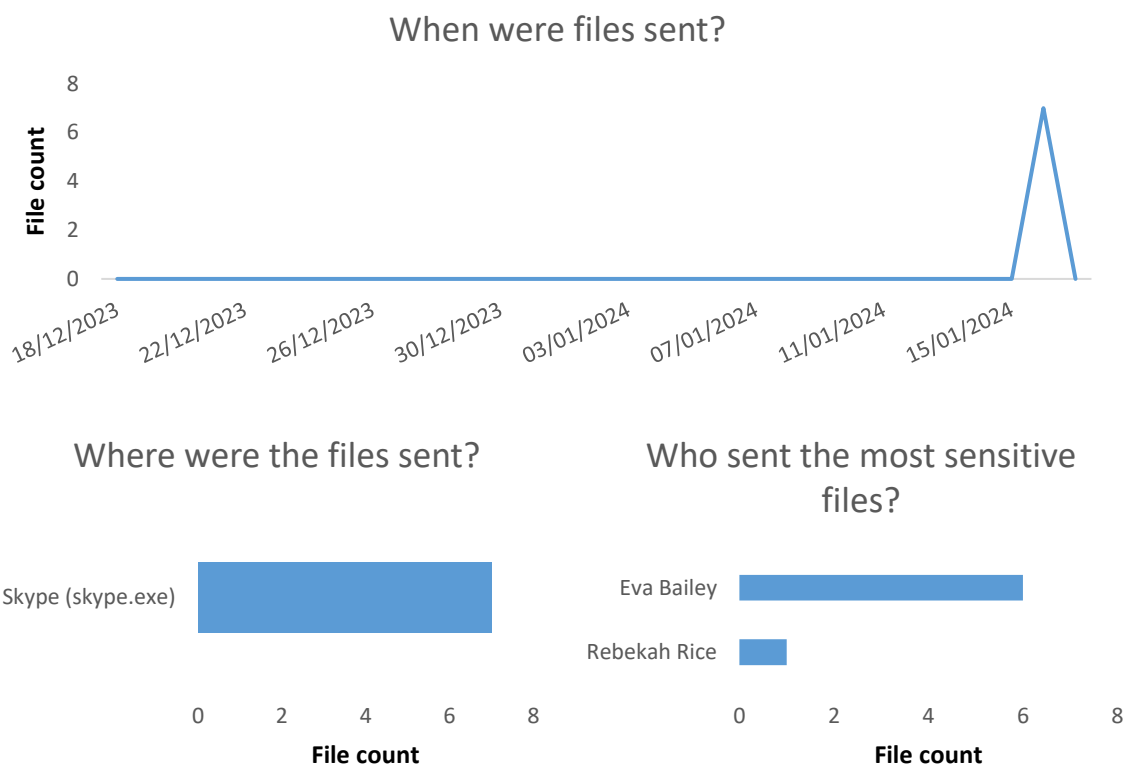
- Define and revise which websites are considered safe by the company.
- Check which files are uploaded. Evaluate if these need to be classified as sensitive.
- Set policies for sensitive files uploaded to websites.
- Set alerts for when sensitive files are uploaded to untrusted websites.

FILES SENT VIA INSTANT MESSAGING

Instant messaging applications are a communication tool for working with colleagues and partners around the world. While sending files is limited to a small circle of recipients, instant messaging poses a threat to companies that do not audit and control the use of these apps.

Uncontrolled sending of company files via instant messaging apps puts company data in danger.

There was an attempt to transfer 7 files not identified as sensitive to instant messaging. Your policies blocked these file transfers.



File samples:

Time	File	User	Destination
16/01/2024 23:59	malta_roof_don-drysdale_construction.woff2	Eva Bailey	Skype (skype.exe)
16/01/2024 23:59	malta_roof_don-drysdale_construction.woff2	Eva Bailey	Skype (skype.exe)
16/01/2024 23:59	malta_roof_don-drysdale_construction.woff2	Eva Bailey	Skype (skype.exe)

Overview of all files transferred to this destination type in the selected period:

Total files not identified as sensitive: 11

- blocked by policies: 7 files
- compliant to policies: 4 files

Show detailed records in Safetica.

RECOMMENDATIONS

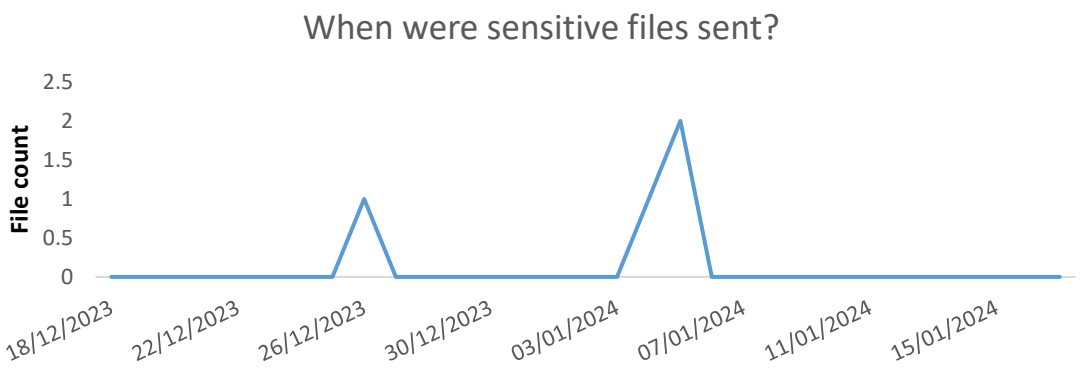
- Check which files are sent. Evaluate if these need to be classified as sensitive.
- Set policies for sensitive files sent via instant messaging apps.

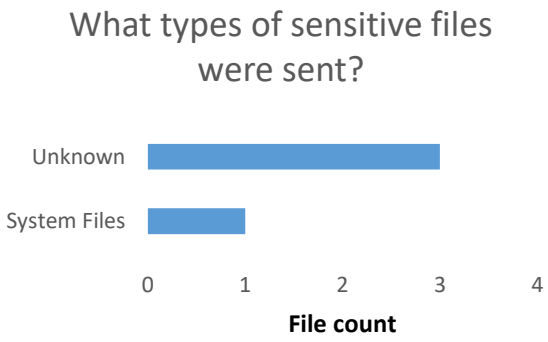
FILES TRANSFERRED TO CLOUD STORAGE

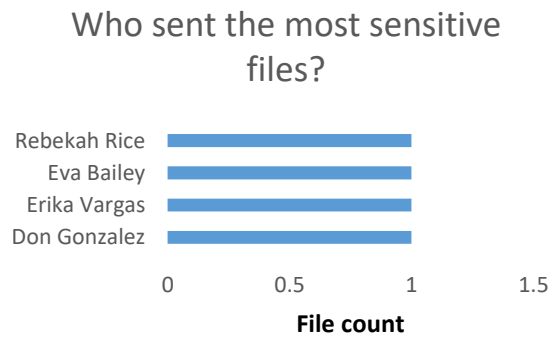
Company files can leak for example after they are transferred to personal cloud storage, and because of insufficient security settings, they are accessible to third parties.

Using personal or unauthorized cloud storage services presents a security risk to sensitive company files.

4 sensitive files were transferred to cloud storage service. Your policies were not blocking.







Overview of all files transferred to this destination type in the selected period:

Total files not identified as sensitive: 8

- non-blocking policies: 4 files
- blocked by policies: 2 files
- compliant to policies: 2 files

Total sensitive files: 8

- non-blocking policies: 4 files
- compliant to policies: 4 files

Show detailed records in Safetica.

RECOMMENDATIONS

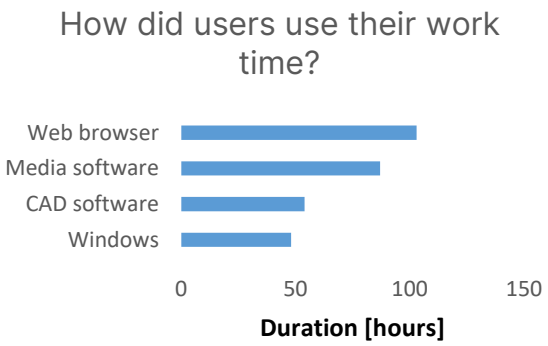
- Check which files are sent. Evaluate if these need to be classified as sensitive.
- Set policies for sensitive files transferred to cloud storage.
- Block the use of cloud storage services that are not essential to your company.

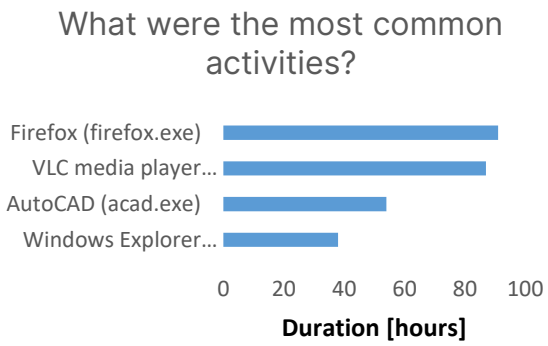
ANALYSIS OF APPLICATION USAGE

Understanding which applications users use helps companies discover where there are security risks and how expensive licenses are used.

Clearly defined rules for using applications increase company security.

You have blocked risky applications so that they cannot be used by users.





Show detailed records in Safetica.

RECOMMENDATIONS

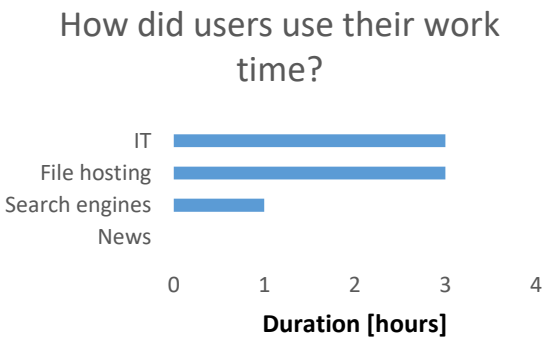
- Check which applications are used. Evaluate if application categories need to be modified.
- Set application policies to prevent the use of risky or harmful applications.
- Set regular automated reports about how applications are used.

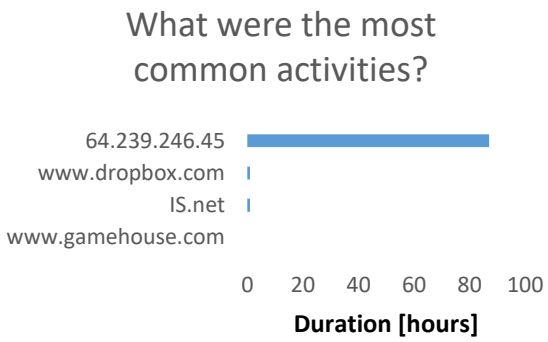
ANALYSIS OF WEBSITE USAGE

Understanding which websites users visit helps companies discover where security risks are.

Clearly defined rules for visiting websites increase company security.

You have blocked risky websites so that they cannot be visited by users.





Show detailed records in Safetica.

RECOMMENDATIONS

- Check which websites are visited. Evaluate if website categories need to be modified.
- Set website policies to prevent visiting risky and harmful websites.
- Set regular automated reports about what websites are visited.

USE OF IT RESOURCES – PRINTING

The print usage overview will help you understand if printed documents pose a security risk or are an unnecessary cost for your company.

Printer users (no activity)

Printers (no activity)

Show detailed records in Safetica.

safetica