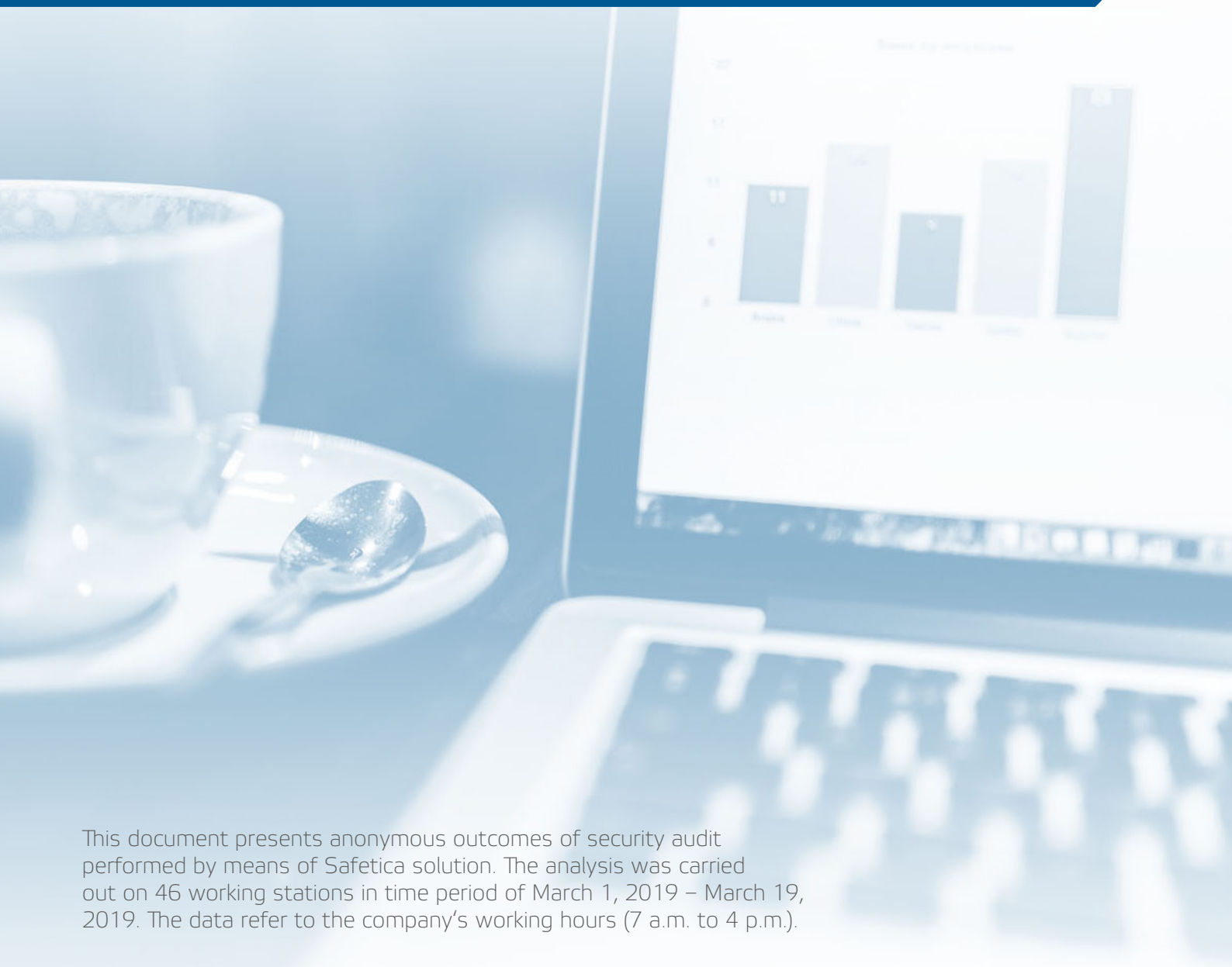
SECURITY AUDIT



This document presents anonymous outcomes of security audit performed by means of Safetica solution. The analysis was carried out on 46 working stations in time period of March 1, 2019 – March 19, 2019. The data refer to the company's working hours (7 a.m. to 4 p.m.).

safetica®

Contents

SCOPE OF AUDIT

The security audit focuses on sensitive files in the company environment, files that leave the company, and how employees use company resources.

The audit is based on monitored files and user activity on the computers where Safetica has been deployed. The security issues and recommended precautions are assessed on which files in Safetica you classified as sensitive, the safest methods you selected for transferring sensitive content, and which risky activities are being carried out by employees.

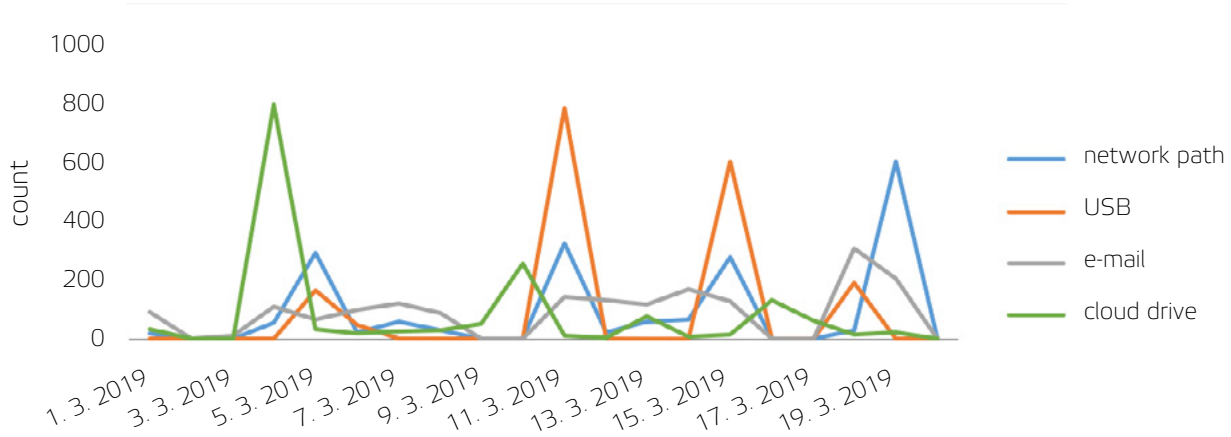
Monitored data:

- **301 GB** of data
- **91.599** file operations
- **33.032** files
- **4.240** outgoing files

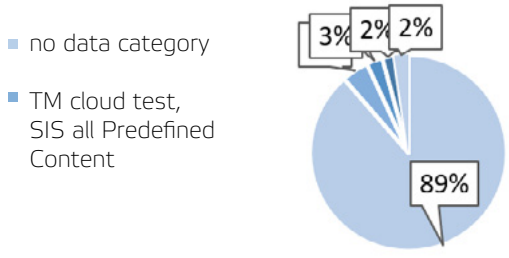
Monitored environment:

- **321** user accounts
- **83** computers with Safetica
- **223** computers in total
- **42** Safetica administrators

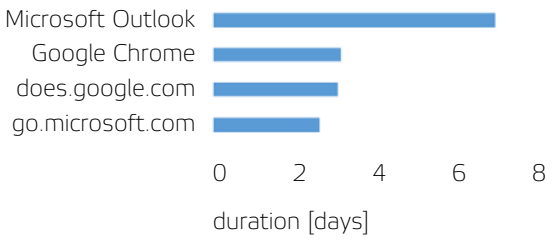
When were files sent?



What data categories did files have?



What were the most common activities?



In the event of a security incident, you will be alerted by instant alerts.

If a security issue occurs, a quick response is important to minimize negative impacts. Instant alerts to the responsible individuals will help you quickly understand where the problem arose.

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

Regular inspection of the company's security status is an vital part of the overall security strategy.

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

Without knowing what sensitive company data are, no security policies can be applied to prevent data leaks.

Recommendations:

- Regularly check that the alerts you set are up to date and are addressed to the person responsible.
- Set regular reports for selected areas.
- Regularly check that the reports you set are up to date and are addressed to the person responsible.
- Regularly check what data your employees are working with and identify sensitive files.
- Categorize files with sensitive data on regular basis.

FILES TRANSFERRED BY USBS OR OTHER EXTERNAL DEVICES

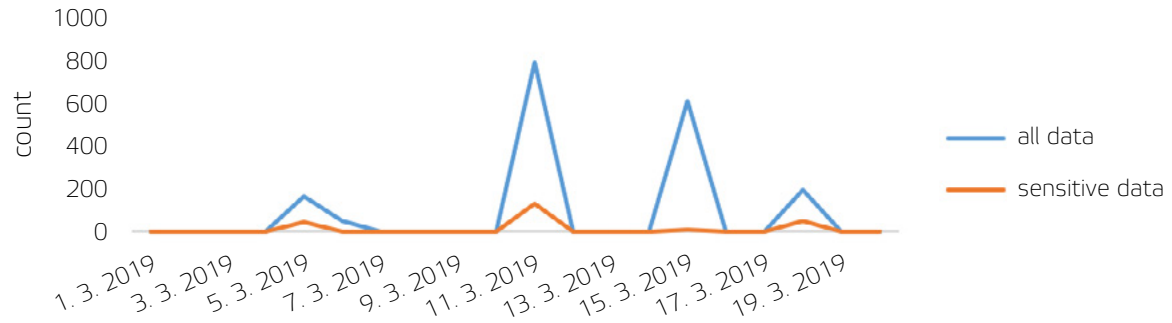
Uploading a large amount of sensitive files to a USB flash drive is a quick and easy way for a company to lose control over its data. If the USB is lost or stolen, critical data can fall into unauthorized hands.

223 sensitive files of total 1793 files have been transferred by USB or other external devices. Your security policies were not restrictive.

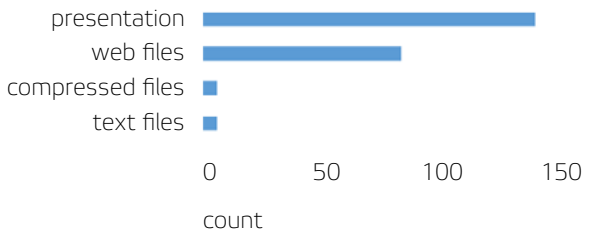
Transferring data out of the company via a USB device is a significant risk. Ensuring that USB devices are secure is a necessary security measure.

15 sensitive files of total 16 files have been transferred by USB or other external devices. These files followed your security policies.

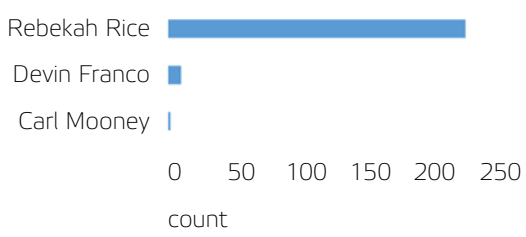
When were files sent?



Which categories of sensitive files were transferred?



Who sent the most sensitive files?



Recommendations:

- Define which USBs and external devices are trusted.

FILES TRANSFERRED BY E-MAIL

E-mail attachments are one of the easiest ways for sensitive data leaks. In most cases, damage to the company is accidental rather than intentional – sending to a wrong recipient or attaching a wrong file.

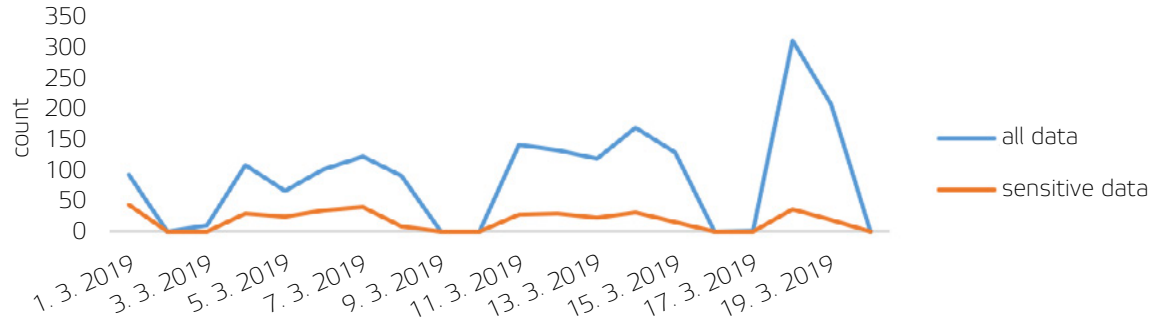
3 sensitive files of total 124 files have been transferred by e-mail. These files were not controlled by any security policy.

E-mails with sensitive files should only be sent to trusted recipients who need to work with the data.

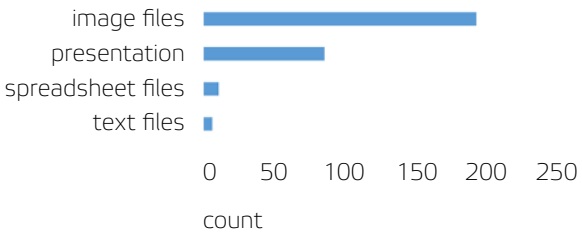
121 sensitive files of total 121 files have been transferred by e-mail. Your security policies were not restrictive.

241 sensitive files of total 1557 files have been transferred by e-mail. These files followed your security policies.

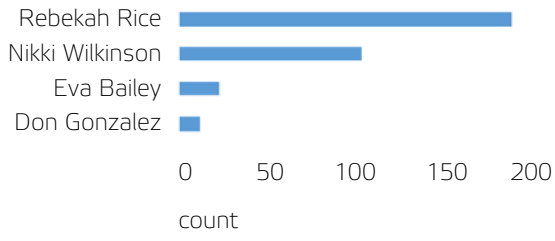
When were files sent?



Which categories of sensitive files were transferred?



Who sent the most sensitive files?



Recommendations:

- Define the company's trusted environments for e-mails.
- Regularly revise trusted e-mail domains.
- Regularly check where e-mails are sent.
- Check if e-mail attachments need to be categorized as sensitive data.

FILES TRANSFERRED BY WEBMAIL

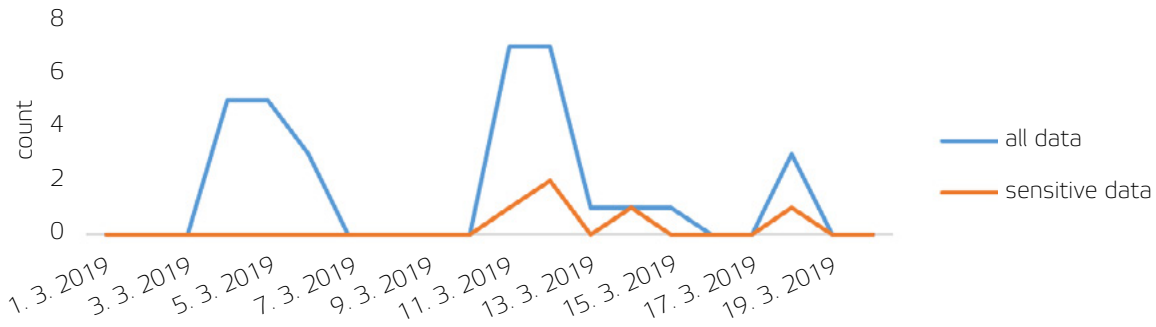
Web e-mail services are popular for communicating and sending sensitive files. At the same time, however, this form of communication is another risk channel that needs to be protected against potential data leaks.

3 sensitive files of total 31 files have been transferred by webmail. Your security policies were not restrictive.

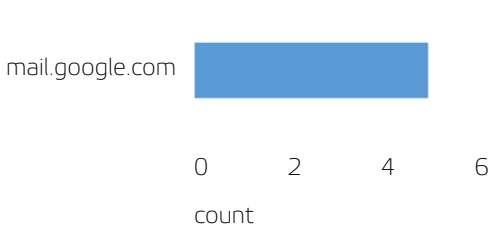
Using webmail services for sending sensitive content is the security issue as it is not possible to control recipients on the endpoint.

2 sensitive files of total 2 files have been transferred by webmail. These files followed your security policies.

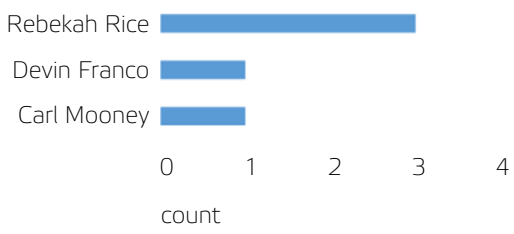
When were files sent?



Where were the sensitive files sent?



Who sent the most sensitive files?



Recommendations:

- Determine which webmail services are trusted.

COMPANY FILES UPLOADED TO THE WEB

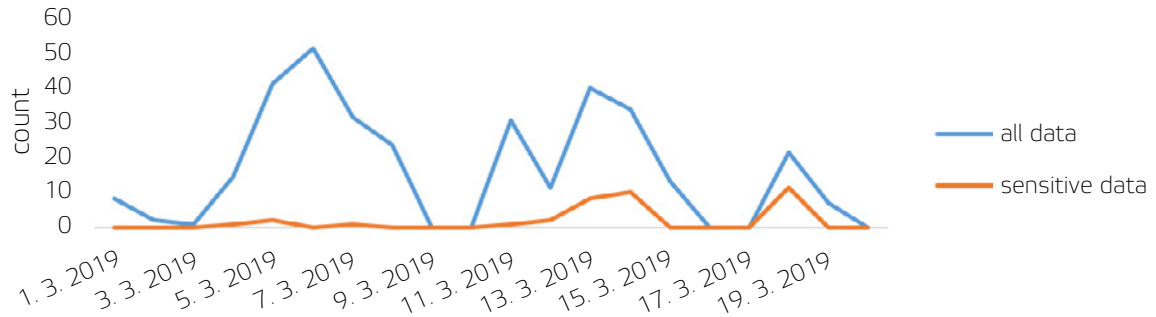
Uploading files to the web is a popular way for employees to share larger files that can't be sent as e-mail attachments. It is therefore important to specify rules for sending files via this channel.

11 sensitive files of total 298 files have been transferred by web upload. Your security policies were not restrictive.

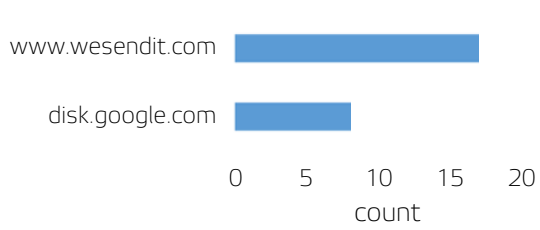
Company files that are uploaded to public sites can be instantly downloaded by a stranger and thus you may lose control of them.

25 sensitive files of total 25 files have been transferred by web upload. These files followed your security policies.

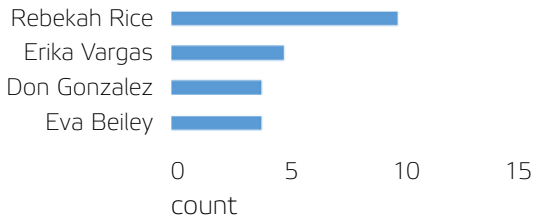
When were files sent?



Where were the sensitive files sent?



Who sent the most sensitive files?



Recommendations:

- Define trusted websites for the company environment.

FILES TRANSFERRED BY INSTANT MESSAGING APPS

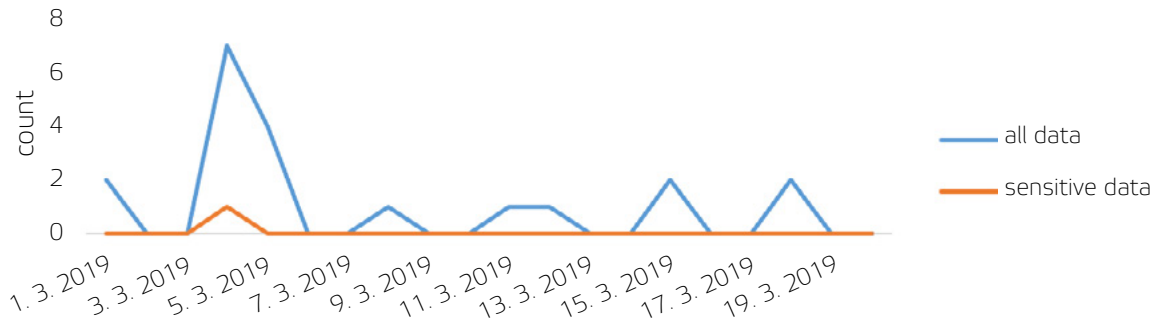
Instant messaging applications are a communication tool for working with colleagues and partners around the world. While sending files is limited to a small circle of recipients, instant messaging poses a threat to companies that do not monitor and control the use of these applications.

18 files have been transferred by instant messaging. Your security policies were not restrictive.

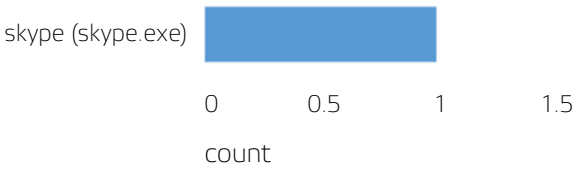
Sending company files without any restrictions by instant messaging applications puts company data in danger.

1 sensitive files of total 2 files have been transferred by instant messaging. These files followed your security policies.

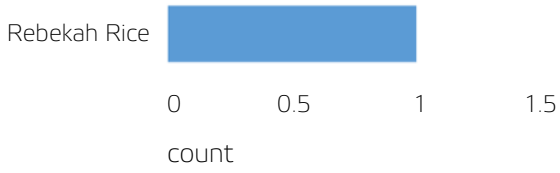
When were files sent?



Where were the sensitive files sent?



Who sent the most sensitive files?



Recommendations:

- Define trusted instant messaging applications for the business environment.

FILES TRANSFERRED BY CLOUD STORAGE SERVICES

Company files can leak when data are transferred to personal cloud storage with insufficient security settings.

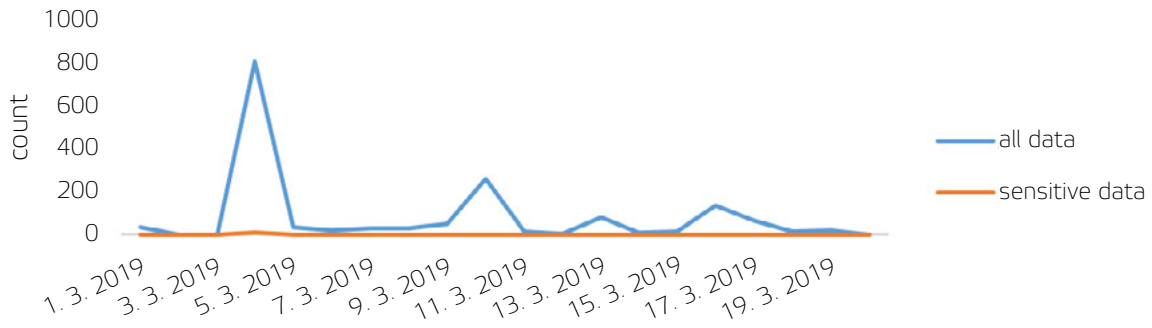
18 files have been transferred by cloud storage service. These files were not controlled by any security policy.

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

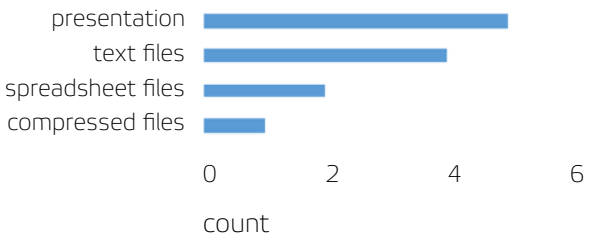
10 sensitive files of total 673 files have been transferred by cloud storage service. Your security policies were not restrictive.

2 sensitive files of total 1072 files have been transferred by cloud storage service. These files followed your security policies.

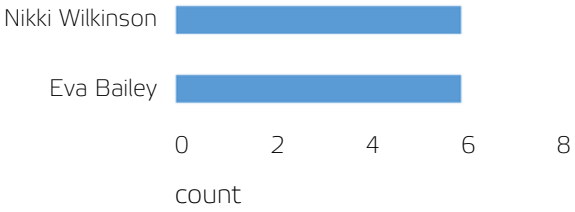
When were files sent?



Which categories of sensitive files were transferred?



Who sent the most sensitive files?



Recommendations:

- Define a trusted business environment for cloud storage services.

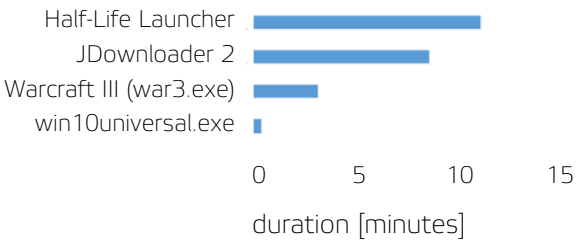
ANALYSIS OF HOW APPLICATIONS ARE USED

Understanding which applications employees use helps companies discover where there are security risks, how expensive licenses are used, and where productivity can be improved.

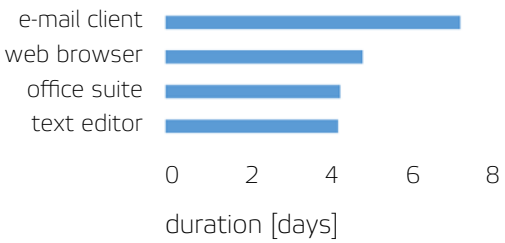
You have restricted risky applications which cannot be used by employees.

Clearly defined rules for using applications increase company security.

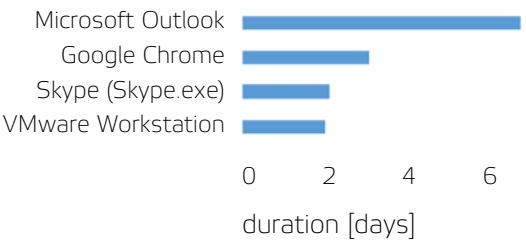
What were the most common risky activities?



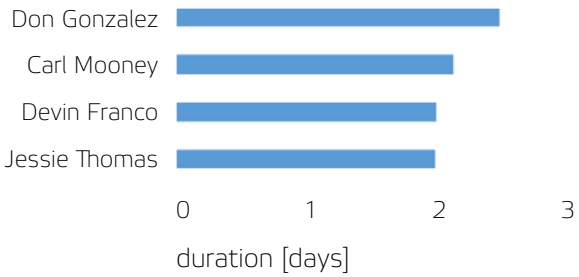
How did employees use their work time?



What were the most common activities?



Who sent the most active?



Recommendations:

- Periodically categorize monitored applications.

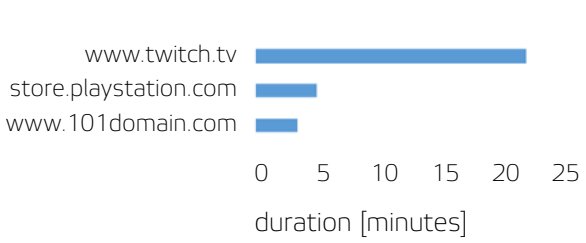
ANALYSIS OF WEB USAGE

Understanding which websites employees visit helps companies discover where security risks are or where productivity can be improved.

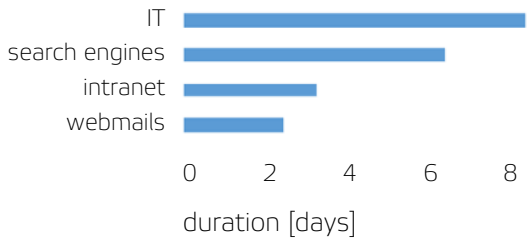
You have restricted risky websites which cannot be visited by employees.

Clearly defined rules for visiting websites increase the security of the company.

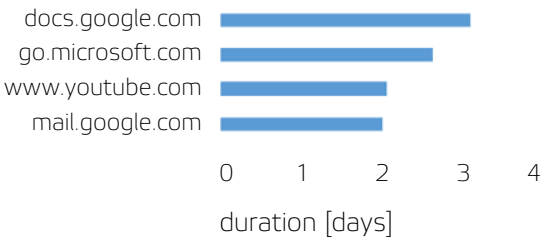
What were the most common risky activities?



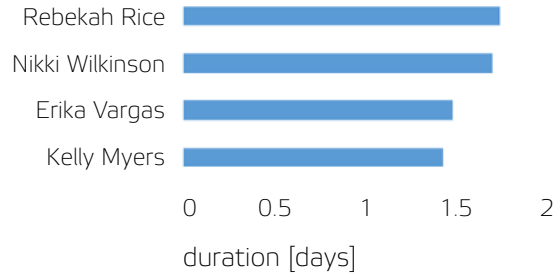
How did employees use their work time?



What were the most common activities?



Who sent the most active?



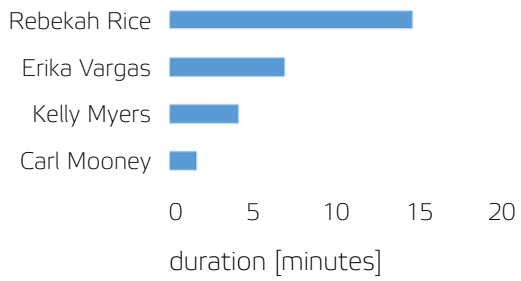
Recommendations:

- Regularly categorize monitored websites.

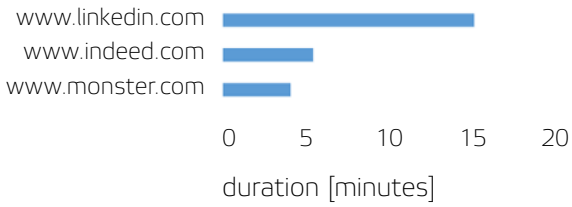
ANALYSIS OF JOB SEARCH WEBSITE USAGE

Employees who choose to leave the company pose a significant security risk. If they enter a new job, with a competitor for example, and take important documents with them, the damage to your company can be substantial.

What were the most common risky activities?



How did employees use their work time?

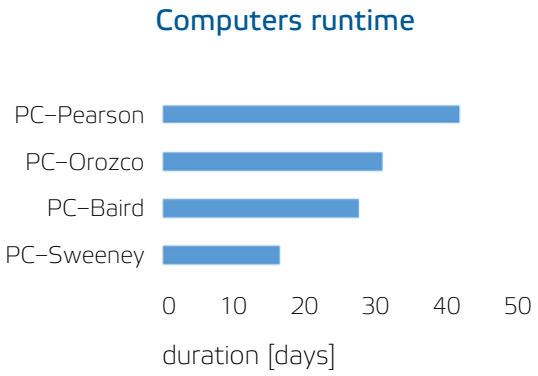


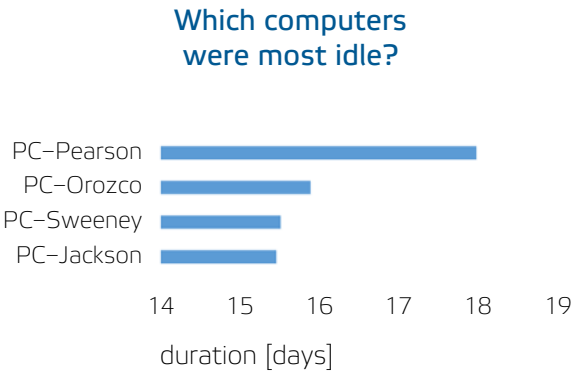
Recommendations:

- Regularly categorize monitored job search websites.

USE OF IT RESOURCES – COMPUTERS

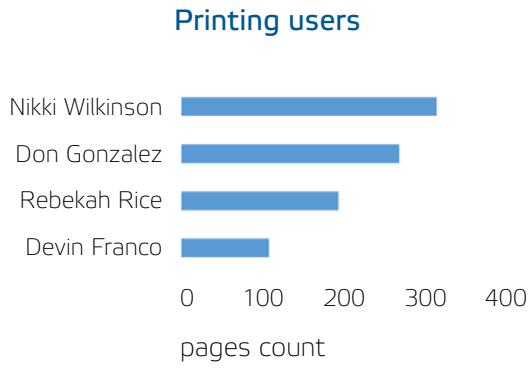
Efficient use of company computers is important for understanding where savings can be made.

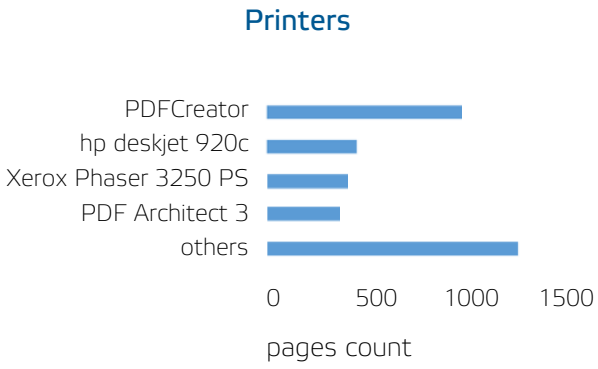




USE OF IT RESOURCES – PRINTING

A print usage report will help you understand if the printed documents pose a security risk or unnecessary cost to the company.

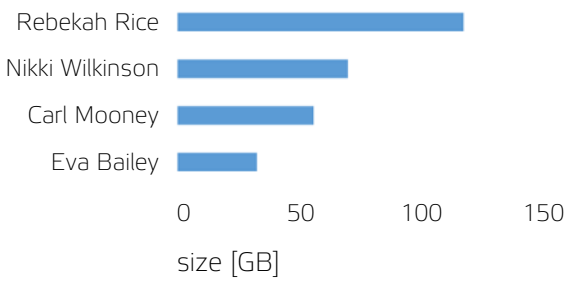




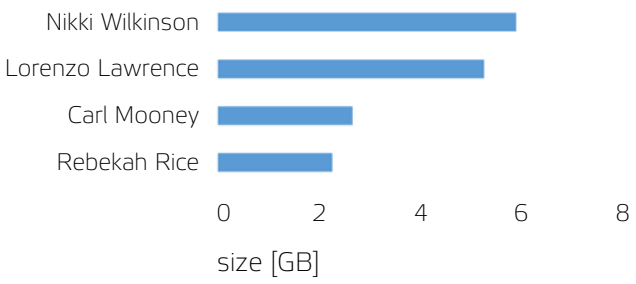
USE OF IT RESOURCES – NETWORK TRAFFIC

Overloading or sending large amounts of data over the network may pose a security risk to the company or reduce the productivity of other employees' work.

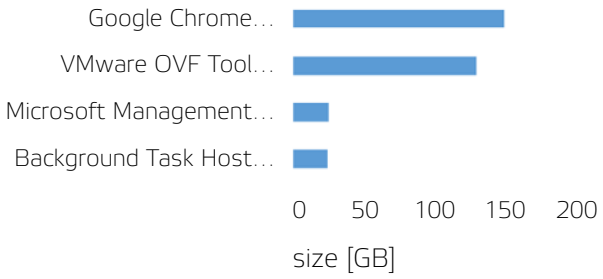
Users download



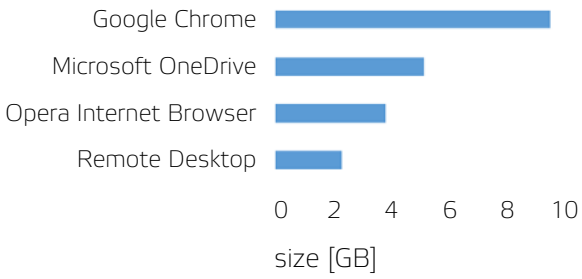
Users upload



Applications download



Applications upload



ABOUT SAFETICA TECHNOLOGIES

Safetica Technologies is a Czech software company that provides data loss prevention solution to companies of all shapes and sizes. Because in Safetica we believe that every company deserves to know that their data is secure.

170,000+ protected devices

1,400+ customers

95+ countries

70+ security experts

TECHNOLOGY ALLIANCES

ESET ENJOY SAFER TECHNOLOGY™

Microsoft

FORTINET Fabric-Ready

AWARDS & ACHIEVEMENTS

Gartner

RED HERRING WINNER 100 EUROPE

SC MAGAZINE AWARDS WINNER Honored in the U.S.

CYBER SECURITY EXCELLENCE AWARDS WINNER 2019

Info Security Products Guide 2019 GLOBAL EXCELLENCE BRONZE

And what about your data?

Try Safetica demo now!

safetica®