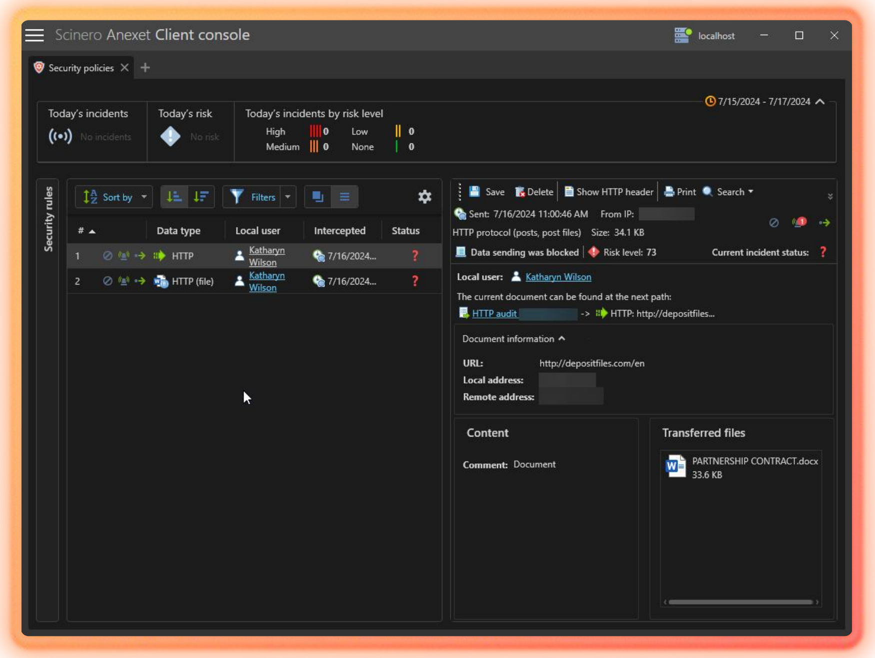
Data Protection and Leak Prevention

The system controls the actions with confidential information, its movement, storage and withdrawal outside the company's perimeter



Today's incidents: No incidents

Today's risk: No risk

Today's incidents by risk level

High	0	Low	0
Medium	0	None	0

7/15/2024 - 7/17/2024

#	Data type	Local user	Intercepted	Status
1	HTTP	Katharyn Wilson	7/16/2024...	?
2	HTTP (file)	Katharyn Wilson	7/16/2024...	?

Sent: 7/16/2024 11:00:46 AM From IP: [redacted]

HTTP protocol (posts, post files) Size: 34.1 KB

Data sending was blocked | Risk level: 73 Current incident status: ?

Local user: Katharyn Wilson

The current document can be found at the next path:

HTTP audit [redacted] -> HTTP: http://depositfiles...

Document information

URL: http://depositfiles.com/en

Local address: [redacted]

Remote address: [redacted]

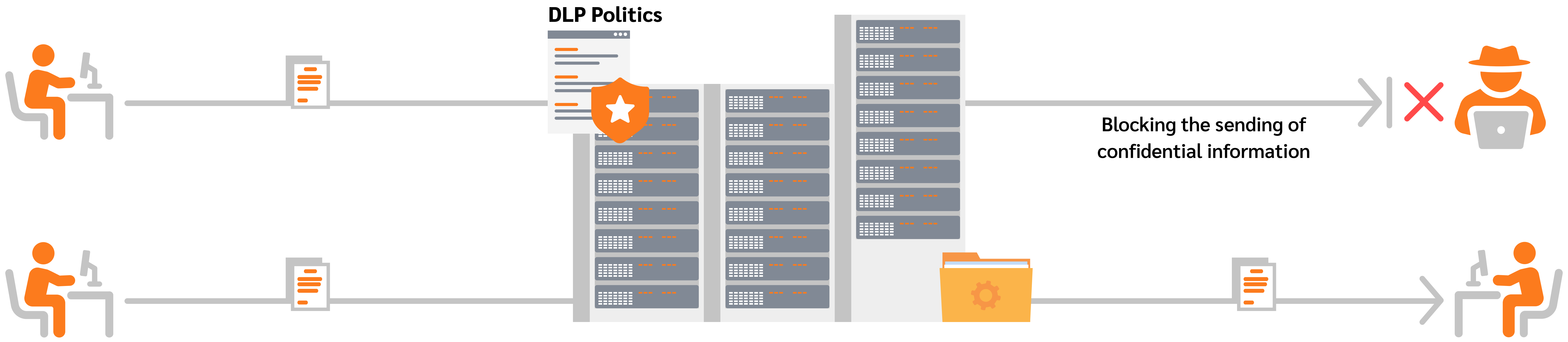
Content

Comment: Document

Transferred files

PARTNERSHIP CONTRACT.docx 33.6 KB

- Control information transmission on various channels, including messengers, email services, cloud storages, etc
- Detect information leaks through external devices. If data is copied or transferred through such devices, you'll get notified
- Create policy rules. The system can be configured to protect the necessary kind of data
- Manage risks. Detect potentially dangerous employees and capture their actions at the workstation

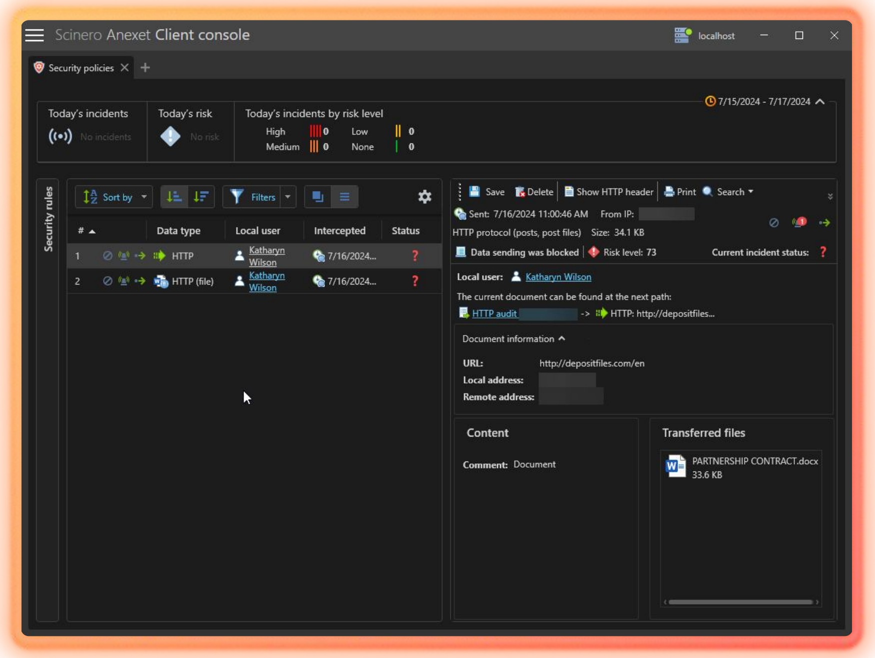


Anexet Servers

The Fight Against Corruption

The complex monitors employee communication, which allows you to identify conflicts of interest, cases of blackmail, attempts to receive bribes and other corporate fraud

- Control communication chains. It is possible to control all the ways of corporate communication to see potential threats
- Find unloyal workers, who are looking for a new job or trying to contact the third parties
- DLP finds unusual connections and employees behavior patterns in communication
- Detect insiders. Only chosen employees will have the access to the sensitive data



7/15/2024 - 7/17/2024

Today's incidents: No incidents

Today's risk: No risk

Today's incidents by risk level: High 0, Medium 0, Low 0, None 0

#	Data type	Local user	Intercepted	Status
1	HTTP	Katharyn Wilson	7/16/2024...	?
2	HTTP (file)	Katharyn Wilson	7/16/2024...	?

Sent: 7/16/2024 11:00:46 AM From IP: [redacted]

HTTP protocol (posts, post files) Size: 34.1 KB

Data sending was blocked | Risk level: 73 Current incident status: ?

Local user: Katharyn Wilson

The current document can be found at the next path:

HTTP audit [redacted] -> HTTP: http://depositfiles...

Document information

URL: http://depositfiles.com/en

Local address: [redacted]

Remote address: [redacted]

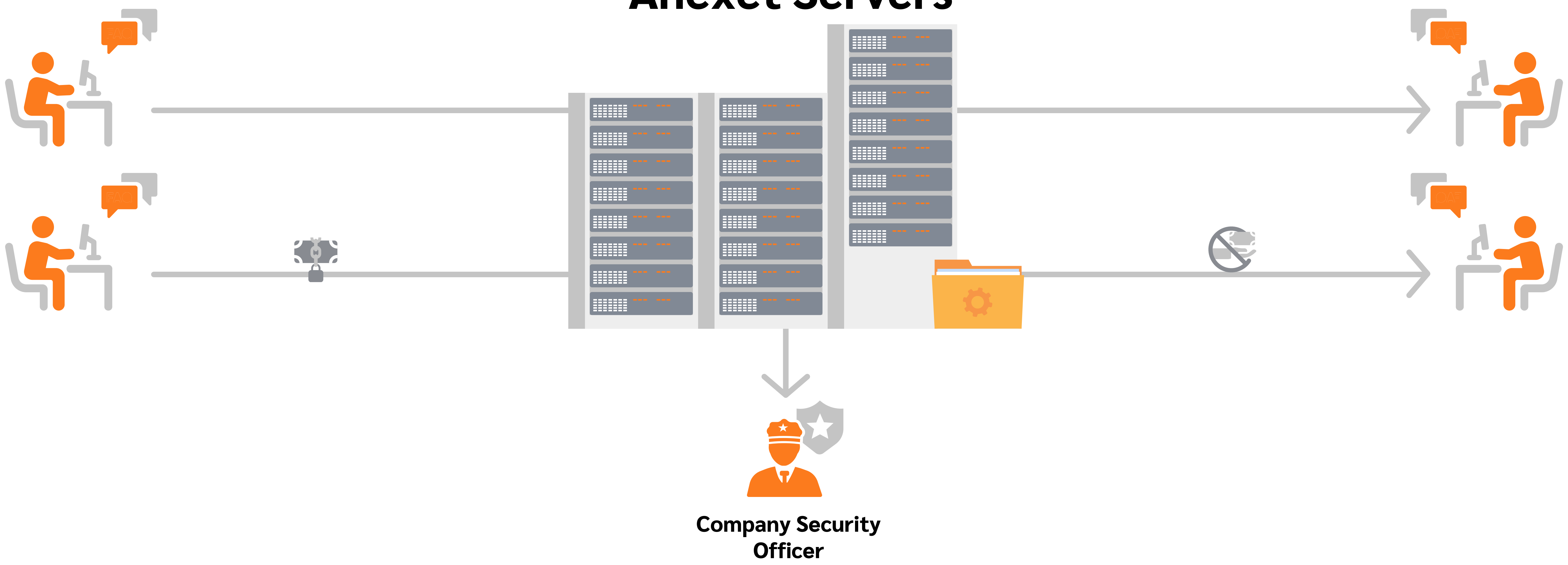
Content

Comment: Document

Transferred files

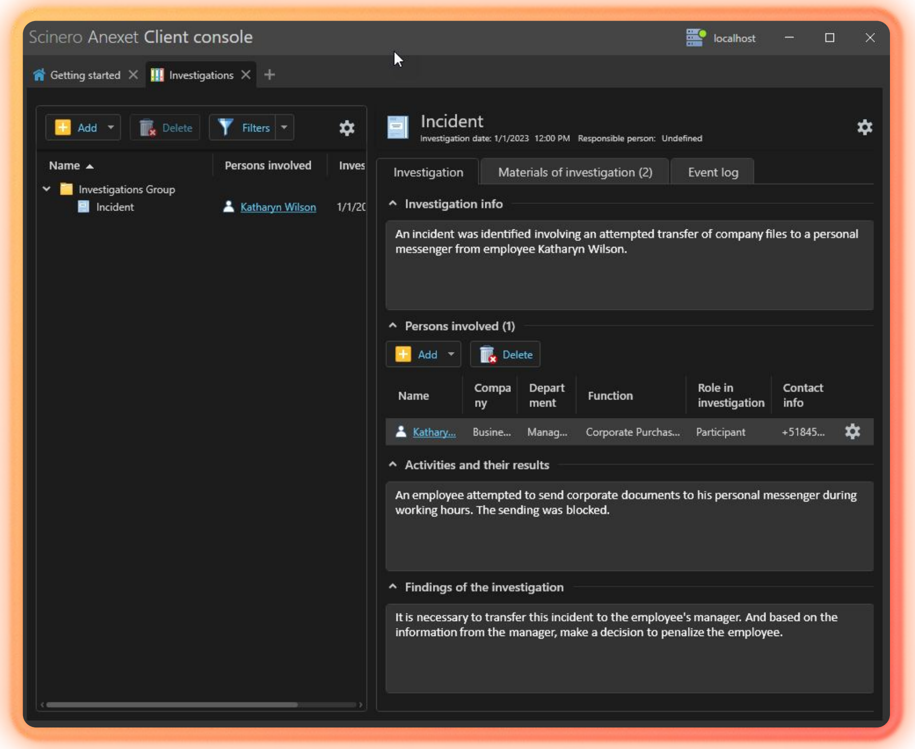
PARTNERSHIP CONTRACT.docx 33.6 KB

Anexet Servers



Investigation of Incidents

The software records all the actions of employees, which allows you to retrospectively establish the details of what happened, conduct an investigation and identify those involved



Name	Persons involved	Inves
Investigations Group		
Incident	Katharyn Wilson	1/1/20

Incident

Investigation date: 1/1/2023 12:00 PM Responsible person: Undefined

Investigation info

An incident was identified involving an attempted transfer of company files to a personal messenger from employee Katharyn Wilson.

Persons involved (1)

Name	Company	Department	Function	Role in investigation	Contact info
Kathary...	Busine...	Manag...	Corporate Purchas...	Participant	+51845...

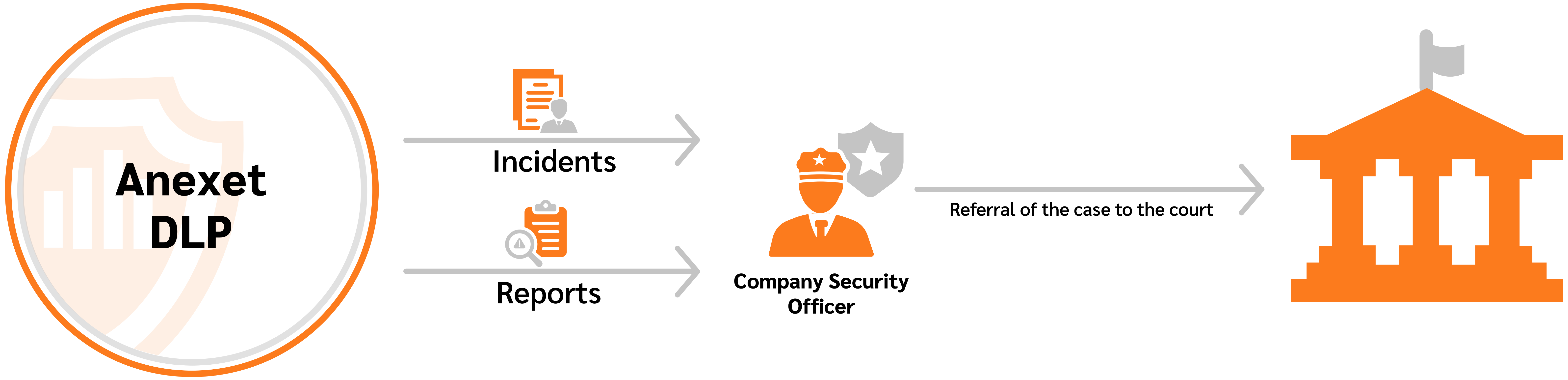
Activities and their results

An employee attempted to send corporate documents to his personal messenger during working hours. The sending was blocked.

Findings of the investigation

It is necessary to transfer this incident to the employee's manager. And based on the information from the manager, make a decision to penalize the employee.

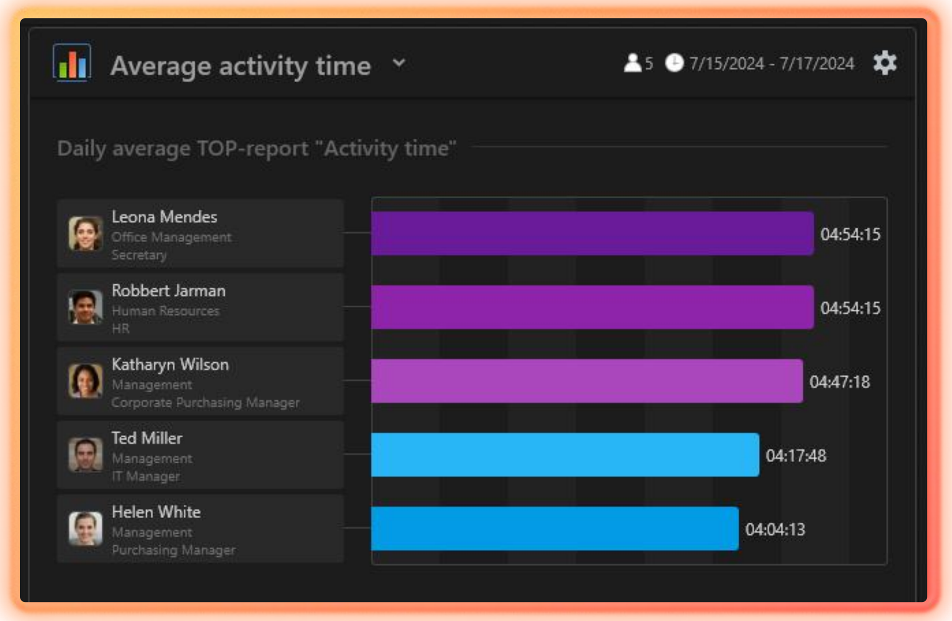
- Organize information handling within the framework of security incident investigations
- In the case of incident, the system will help to track the start of breach and find perpetrators
- Create reports. Helps to find the reason and vulnerabilities in protection, and take prevention measures
- Use reports in court. In the case of trial, the company can use objective data from the investigation



Control of Employees’ Working Hours

It allows you to track the activity of employees, including time spent at work, their actions and the use of computer resources

- See how employees use the worktime: what do they do on the work place, what websites do they visit, etc
- Take screenshots from employees’ monitors. Set triggers on events: launching an application, transferring an archive, etc
- Record audio through the microphone and video from the webcameras
- Visualize connections between workers. Observe communication chains and conversation topics

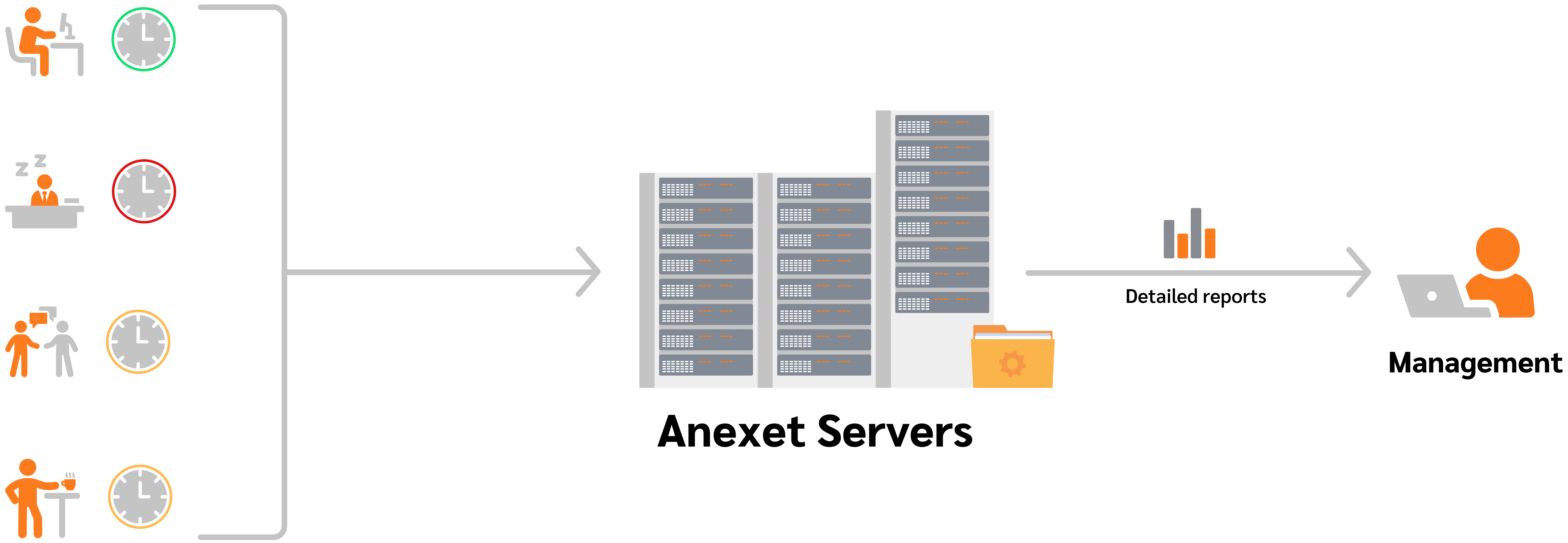


Average activity time

5 7/15/2024 - 7/17/2024

Daily average TOP-report "Activity time"

Leona Mendes Office Management Secretary	04:54:15
Robbert Jarman Human Resources HR	04:54:15
Katharyn Wilson Management Corporate Purchasing Manager	04:47:18
Ted Miller Management IT Manager	04:17:48
Helen White Management Purchasing Manager	04:04:13



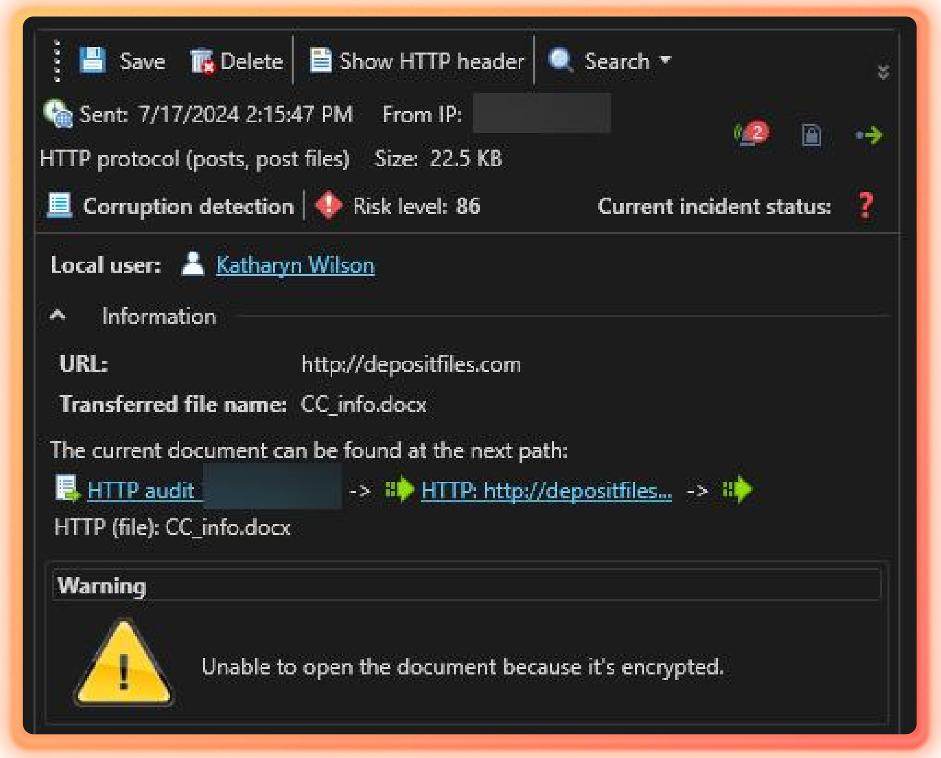
Detailed reports

Anexet Servers

Management

Document Control on Devices

Identify deviation from documents stored in violation of the organization's security policy



Sent: 7/17/2024 2:15:47 PM From IP: [redacted]

HTTP protocol (posts, post files) Size: 22.5 KB

Corruption detection | Risk level: 86 Current incident status: ?

Local user: Katharyn Wilson

Information

URL: http://depositfiles.com

Transferred file name: CC_info.docx

The current document can be found at the next path:

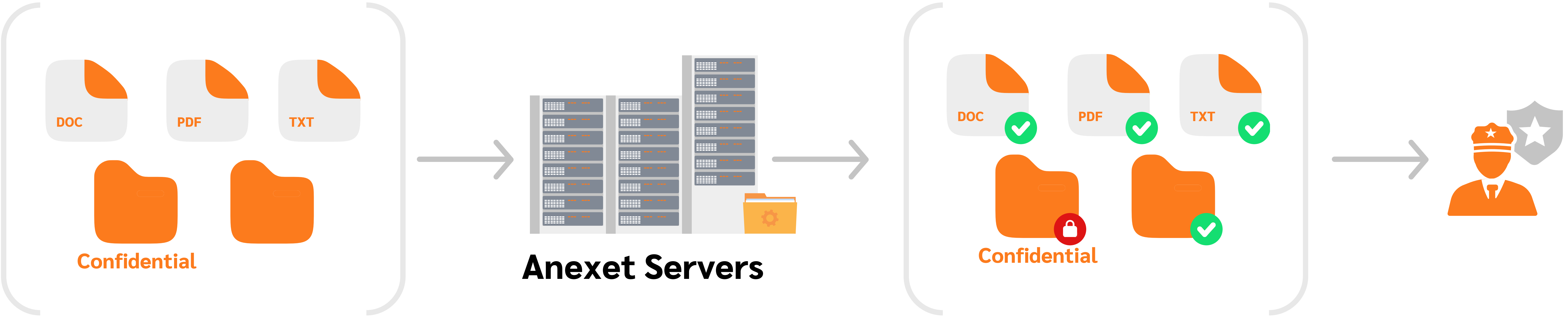
HTTP audit [redacted] -> HTTP: http://depositfiles... ->

HTTP (file): CC_info.docx

Warning

Unable to open the document because it's encrypted.

- Prevent forgery. If an attempt to falsify a document is made, security officer receives a notification
- Decrypt images and audio. The system can transcript images into text and convert audio messages into text
- Detect certain words, phrases, word combinations. It helps identify malicious intentions from the very beginning
- Track document transmission. If the employee tries to send a document or change it, the system will prevent these actions



DOC
PDF
TXT
Confidential
Anexet Servers
DOC
PDF
TXT
Confidential