# Hidden in Plain Sight

## Detecting Intrusion in Systems Logs

Content classification: Public

advenica

# Outline

- Advenica
- Intrusion detection
- Data exfiltration
- Operational data

# Advenica

- Encryption
- Network segmentation
- Between networks

# Detecting intrusion

- Attempted intrusion
- Successful intrusion
- Reconnaissance
- Data exfiltration

# Signs of intrusion

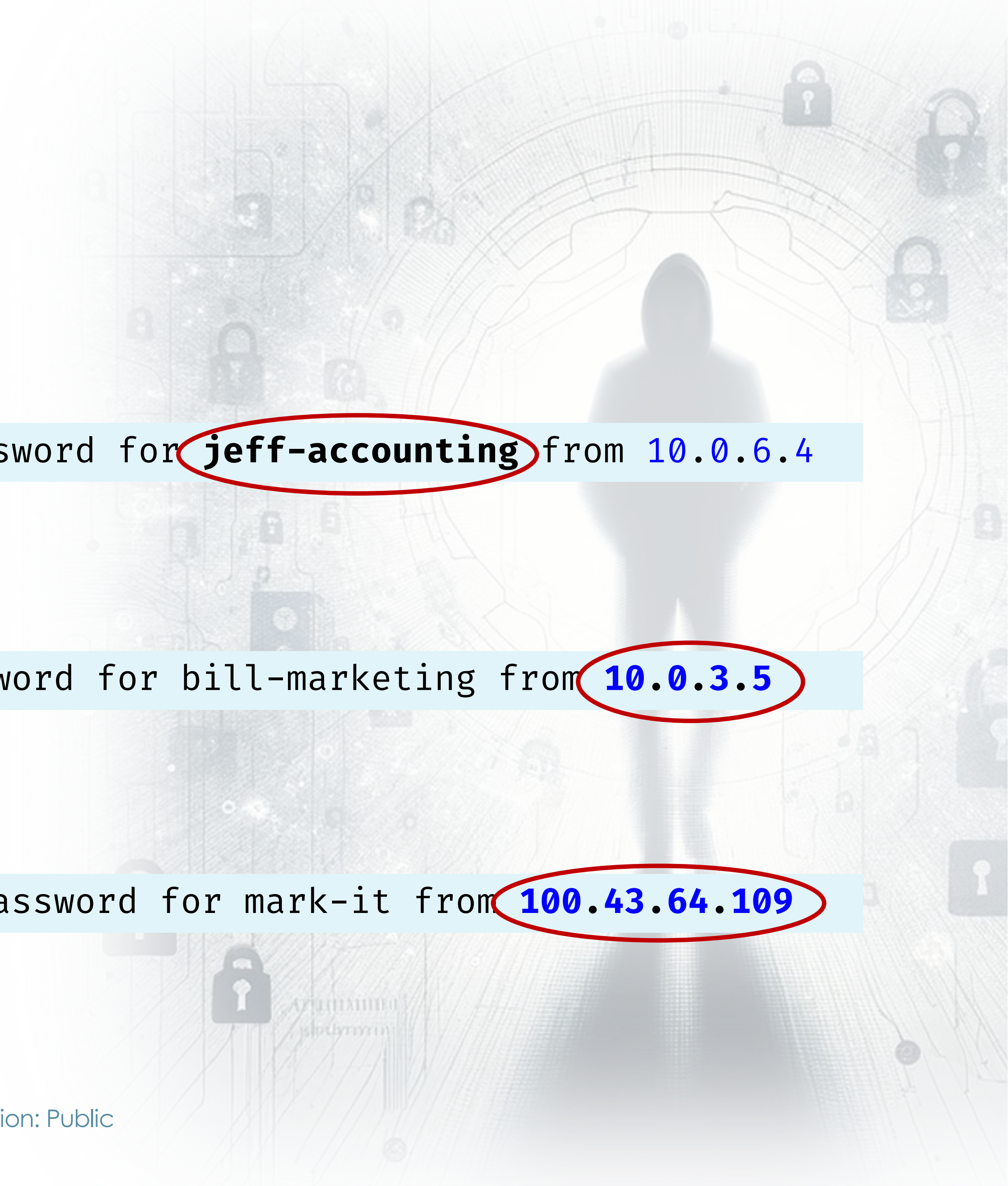
## Multiple failed login attempts

```
sshd[9362]: Failed password for invalid user admin from 100.43.64.2 port 58257 ssh2
sshd[9364]: Failed password for invalid user buffy from 100.43.64.2 port 58212 ssh2
sshd[9366]: Failed password for invalid user mallard from 100.43.64.2 port 58109 ssh2
sshd[9368]: Failed password for manager from 100.43.64.2 port 58030 ssh2
sshd[9370]: Failed password for manager from 100.43.64.2 port 58160 ssh2
sshd[9372]: Failed password for manager from 100.43.64.2 port 58199 ssh2
sshd[9374]: Accepted password for manager from 100.43.64.2 port 58156 ssh2
systemd-logind [9374]: New session 426 of user manager
```

## Logins from system users

```
sshd[23410]: Accepted password for nobody from 10.0.2.2 port 48321 ssh2
sshd[23410]: Accepted password for mysql from 10.0.2.2 port 42351 ssh2
```

# Other signs of intrusion



## Unusual access

```
15:19:18 authserver sshd[9364]: Accepted password for jeff-accounting from 10.0.6.4
```

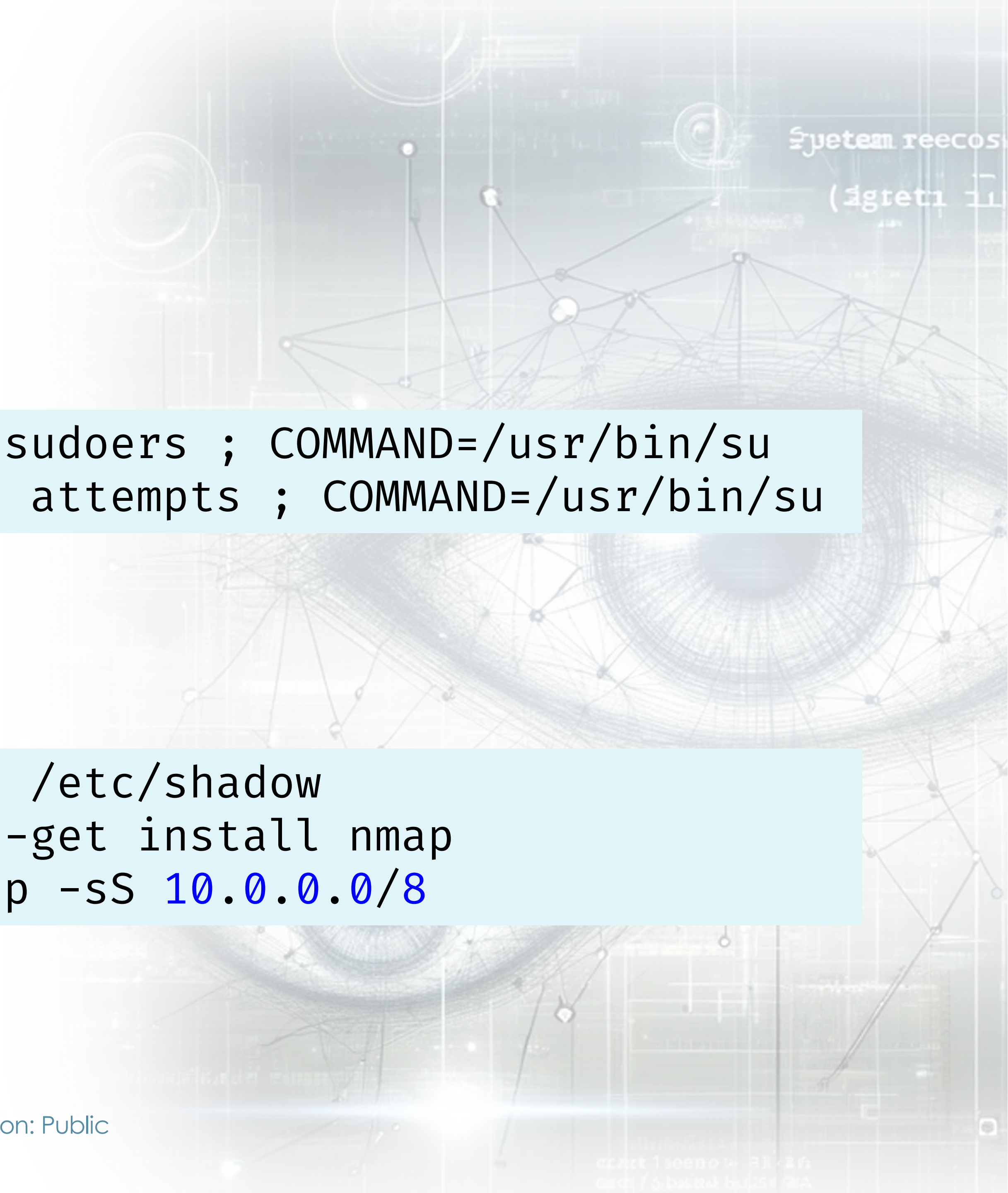
## ... at a strange time

```
02:23:59 vpnserver sshd[9364]: Accepted password for bill-marketing from 10.0.3.5
```

## ... from a strange place

```
15:44:04 backupserver sshd[9364]: Accepted password for mark-it from 100.43.64.109
```

# Hacker reconnaissance



## Looking for sudo

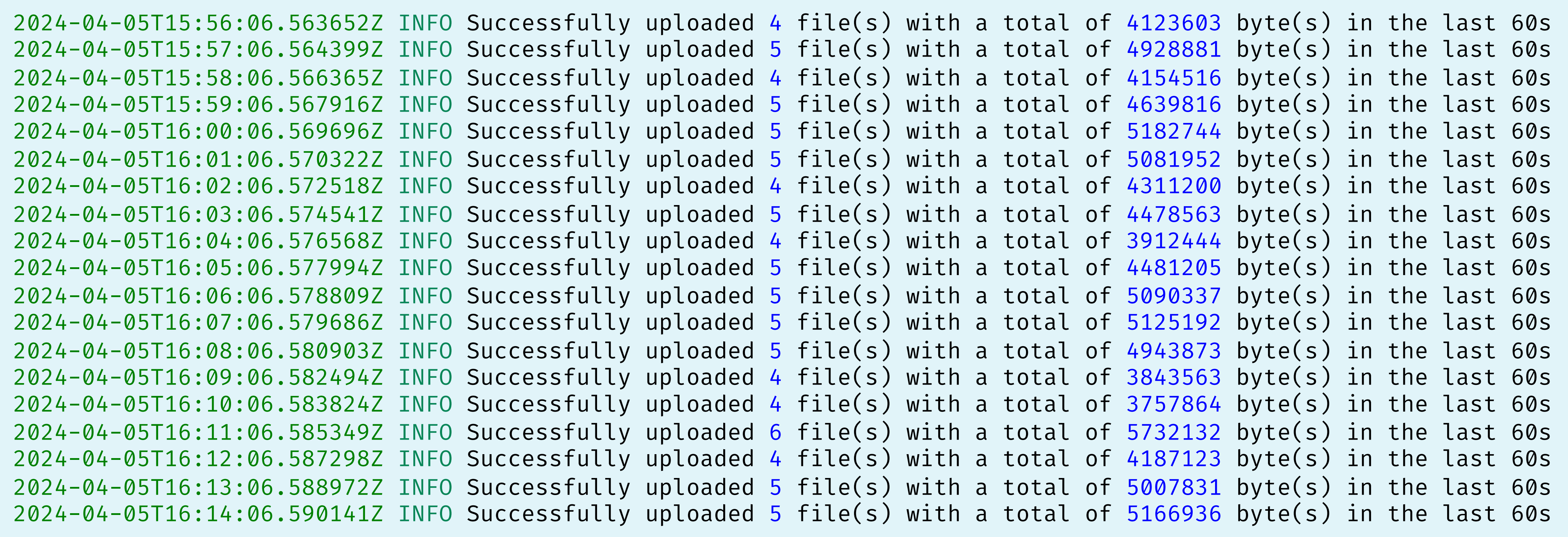
```
sudo: jeff-accounting : user NOT in sudoers ; COMMAND=/usr/bin/su
sudo: mark-it : 3 incorrect password attempts ; COMMAND=/usr/bin/su
```

## ... and finding it

```
sudo: mark-it : COMMAND=/usr/bin/cat /etc/shadow
sudo: mark-it : COMMAND=/usr/bin/apt-get install nmap
sudo: mark-it : COMMAND=/usr/bin/nmap -sS 10.0.0.0/8
```

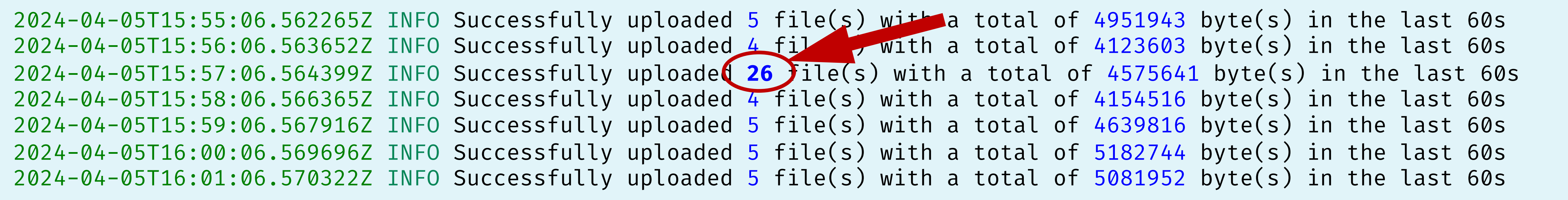
# Data exfiltration

## File transfer service sample log

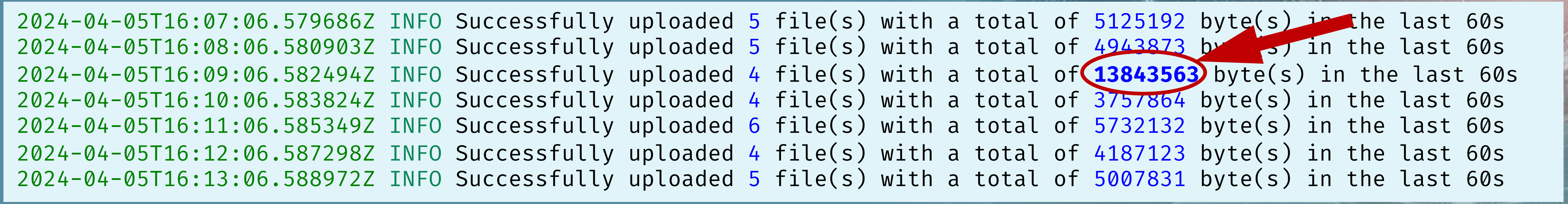


```
2024-04-05T15:56:06.563652Z INFO Successfully uploaded 4 file(s) with a total of 4123603 byte(s) in the last 60s
2024-04-05T15:57:06.564399Z INFO Successfully uploaded 5 file(s) with a total of 4928881 byte(s) in the last 60s
2024-04-05T15:58:06.566365Z INFO Successfully uploaded 4 file(s) with a total of 4154516 byte(s) in the last 60s
2024-04-05T15:59:06.567916Z INFO Successfully uploaded 5 file(s) with a total of 4639816 byte(s) in the last 60s
2024-04-05T16:00:06.569696Z INFO Successfully uploaded 5 file(s) with a total of 5182744 byte(s) in the last 60s
2024-04-05T16:01:06.570322Z INFO Successfully uploaded 5 file(s) with a total of 5081952 byte(s) in the last 60s
2024-04-05T16:02:06.572518Z INFO Successfully uploaded 4 file(s) with a total of 4311200 byte(s) in the last 60s
2024-04-05T16:03:06.574541Z INFO Successfully uploaded 5 file(s) with a total of 4478563 byte(s) in the last 60s
2024-04-05T16:04:06.576568Z INFO Successfully uploaded 4 file(s) with a total of 3912444 byte(s) in the last 60s
2024-04-05T16:05:06.577994Z INFO Successfully uploaded 5 file(s) with a total of 4481205 byte(s) in the last 60s
2024-04-05T16:06:06.578809Z INFO Successfully uploaded 5 file(s) with a total of 5090337 byte(s) in the last 60s
2024-04-05T16:07:06.579686Z INFO Successfully uploaded 5 file(s) with a total of 5125192 byte(s) in the last 60s
2024-04-05T16:08:06.580903Z INFO Successfully uploaded 5 file(s) with a total of 4943873 byte(s) in the last 60s
2024-04-05T16:09:06.582494Z INFO Successfully uploaded 4 file(s) with a total of 3843563 byte(s) in the last 60s
2024-04-05T16:10:06.583824Z INFO Successfully uploaded 4 file(s) with a total of 3757864 byte(s) in the last 60s
2024-04-05T16:11:06.585349Z INFO Successfully uploaded 6 file(s) with a total of 5732132 byte(s) in the last 60s
2024-04-05T16:12:06.587298Z INFO Successfully uploaded 4 file(s) with a total of 4187123 byte(s) in the last 60s
2024-04-05T16:13:06.588972Z INFO Successfully uploaded 5 file(s) with a total of 5007831 byte(s) in the last 60s
2024-04-05T16:14:06.590141Z INFO Successfully uploaded 5 file(s) with a total of 5166936 byte(s) in the last 60s
```

# Data exfiltration



```
2024-04-05T15:55:06.562265Z INFO Successfully uploaded 5 file(s) with a total of 4951943 byte(s) in the last 60s
2024-04-05T15:56:06.563652Z INFO Successfully uploaded 4 file(s) with a total of 4123603 byte(s) in the last 60s
2024-04-05T15:57:06.564399Z INFO Successfully uploaded 26 file(s) with a total of 4575641 byte(s) in the last 60s
2024-04-05T15:58:06.566365Z INFO Successfully uploaded 4 file(s) with a total of 4154516 byte(s) in the last 60s
2024-04-05T15:59:06.567916Z INFO Successfully uploaded 5 file(s) with a total of 4639816 byte(s) in the last 60s
2024-04-05T16:00:06.569696Z INFO Successfully uploaded 5 file(s) with a total of 5182744 byte(s) in the last 60s
2024-04-05T16:01:06.570322Z INFO Successfully uploaded 5 file(s) with a total of 5081952 byte(s) in the last 60s
```

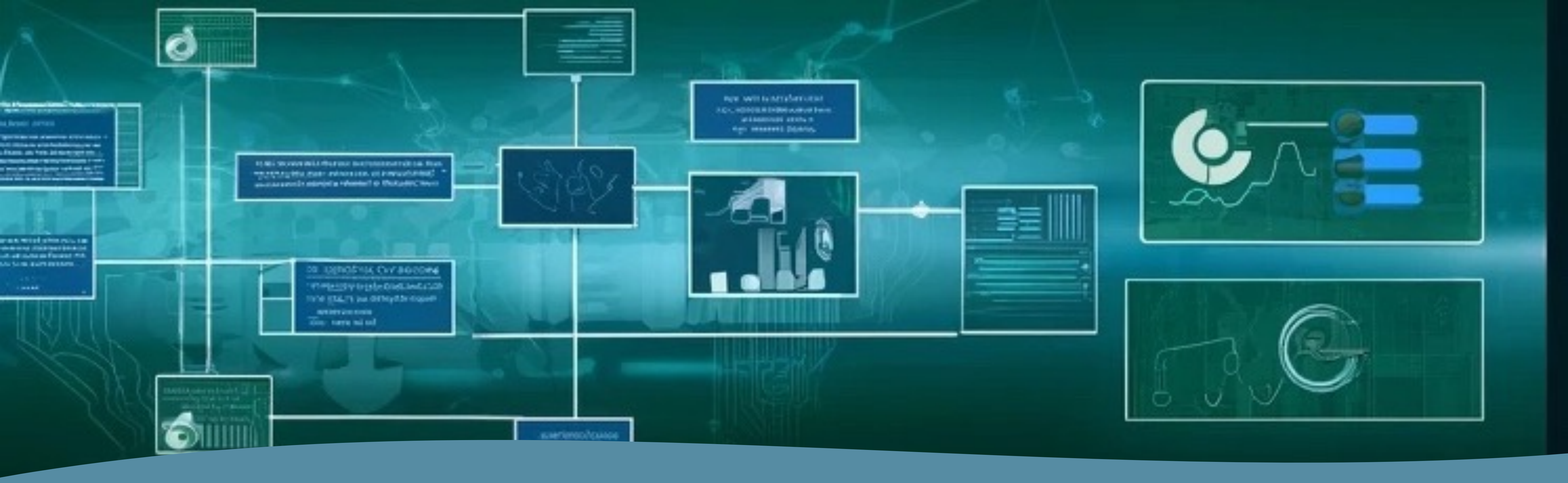


```
2024-04-05T16:07:06.579686Z INFO Successfully uploaded 5 file(s) with a total of 5125192 byte(s) in the last 60s
2024-04-05T16:08:06.580903Z INFO Successfully uploaded 5 file(s) with a total of 4943873 byte(s) in the last 60s
2024-04-05T16:09:06.582494Z INFO Successfully uploaded 4 file(s) with a total of 13843563 byte(s) in the last 60s
2024-04-05T16:10:06.583824Z INFO Successfully uploaded 4 file(s) with a total of 3757864 byte(s) in the last 60s
2024-04-05T16:11:06.585349Z INFO Successfully uploaded 6 file(s) with a total of 5732132 byte(s) in the last 60s
2024-04-05T16:12:06.587298Z INFO Successfully uploaded 4 file(s) with a total of 4187123 byte(s) in the last 60s
2024-04-05T16:13:06.588972Z INFO Successfully uploaded 5 file(s) with a total of 5007831 byte(s) in the last 60s
```

# Operational data

- Confidential
- Highly sensitive
- Difficult to access
  - Physically
  - Legally

Content classification: Public



# Operational data

## Federated learning

- Data stays on device.
- Information leakage?
- Additional overhead?

## Synthetic data

- Unlimited amounts.
- What is realistic?
- How to validate?

advenica

# Questions?

Content classification: Public