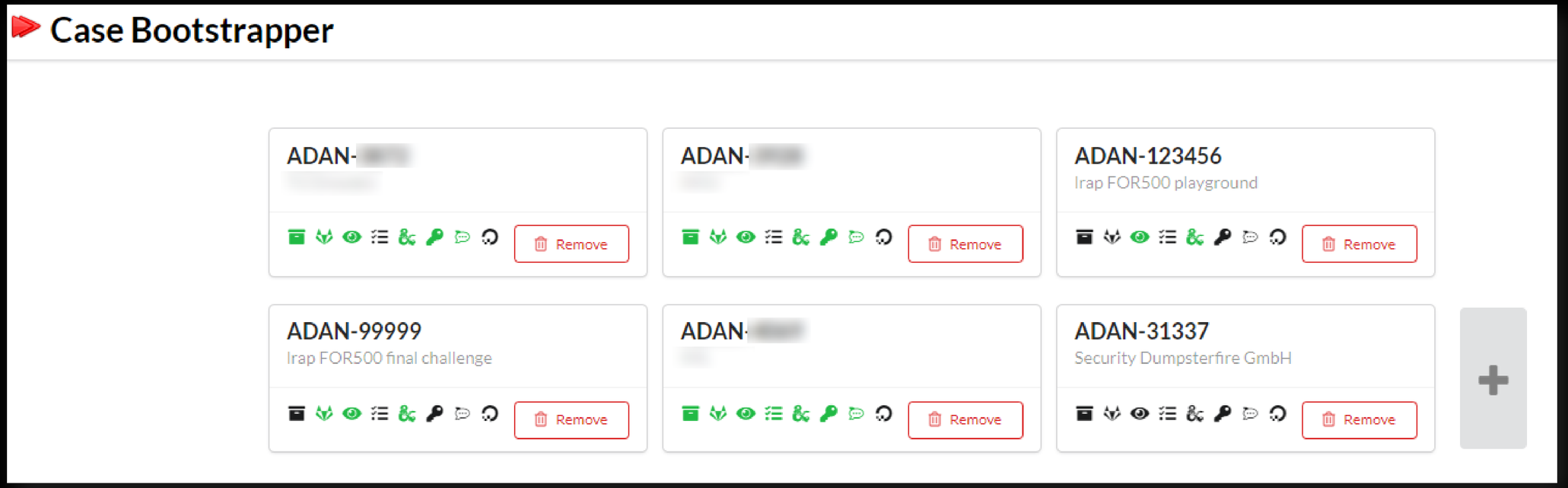
How to do Incident Response – Fast!

Jasper Bongertz
Head of CSIRT
G Data Advanced Analytics

Leonard Rapp
Security Engineer
G Data Advanced Analytics

G DATA
advanced analytics

G DATA
advanced analytics



G DATA
advanced analytics

Velociraptor

Triage

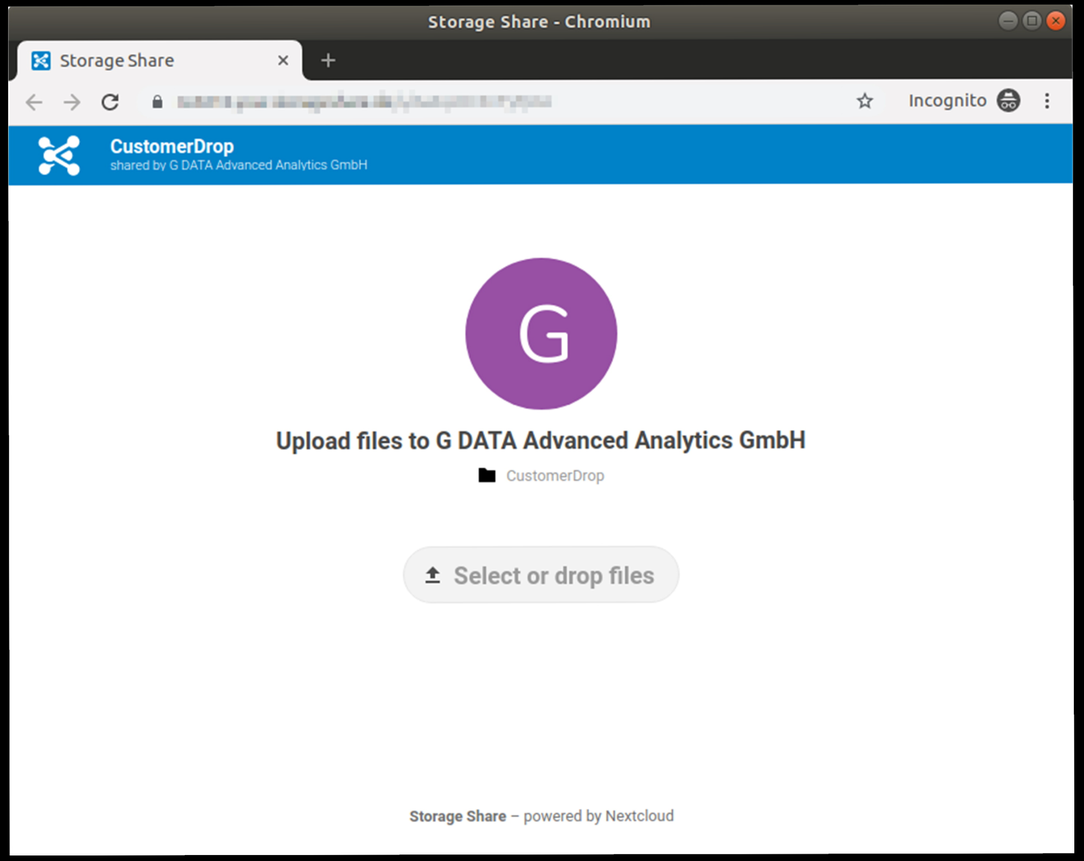
```
autoexec:
  argv: ["artifacts", "collect", "-v", "AcquireAndUploadToNextCloud"]
  artifact_definitions:
    - name: AcquireAndUploadToNextCloud
      parameters:
         - name: webdav_url
           default: "https:/[redacted]webdav/"
         - name: share_key
           default: CHANGEME

      sources:
         - queries:
              - LET hostname <= SELECT Hostname FROM info()
              - LET filename <= format(format="Collection_%s_%d.zip", args=[get(item=hostname, member="0.Hostname"), now()])
              - SELECT upload_webdav(
                  file=Container,
                  url=webdav_url,
                  basic_auth_user=share_key,
                  name=filename
                  ) AS Uploaded
                FROM collect(
                  artifacts=["Windows.KapeFiles.Targets"],
                  args=dict(`Windows.KapeFiles.Targets`=dict(
                    Amcache="Y",
                    Antivirus="Y",
                    EventLogs="Y",
                    FileSystem="Y",
                    LnkFilesAndJumpLists="Y",
                    PowerShellConsole="Y",
                    Prefetch="Y",
                    RemoteAdmin="Y",
                    RecentFileCache="Y",
                    RegistryHives="Y",
                    ScheduledTasks="Y",
                    VSSAnalysis="Y",
                    SRUM="Y",
                    WindowsTimeline="Y"
                  )),
                  output=filename,
                  level=5)
```

G DATA advanced analytics

Velociraptor

Triage

Nextcloud & TFT



G DATA advanced analytics

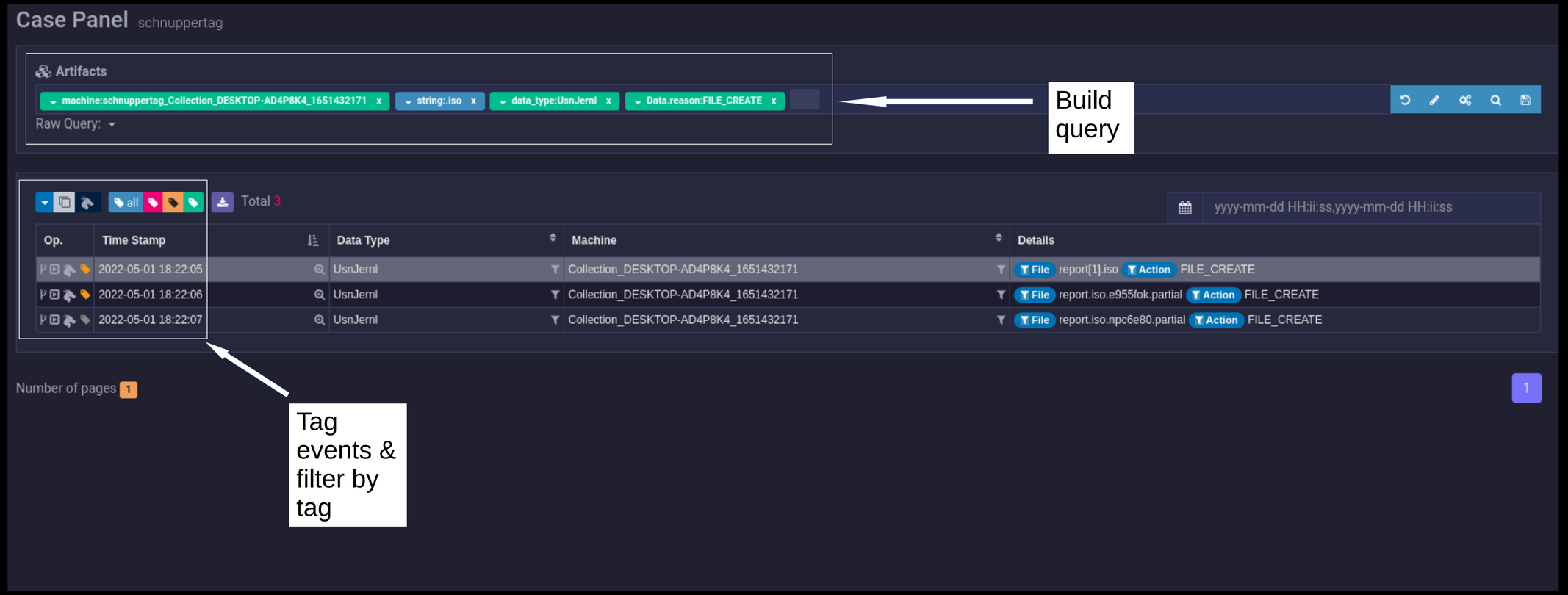
Velociraptor

Triage

Nextcloud & TFT

DFIR Kuiper

Parsing & Analyse



G DATA advanced analytics

Velociraptor

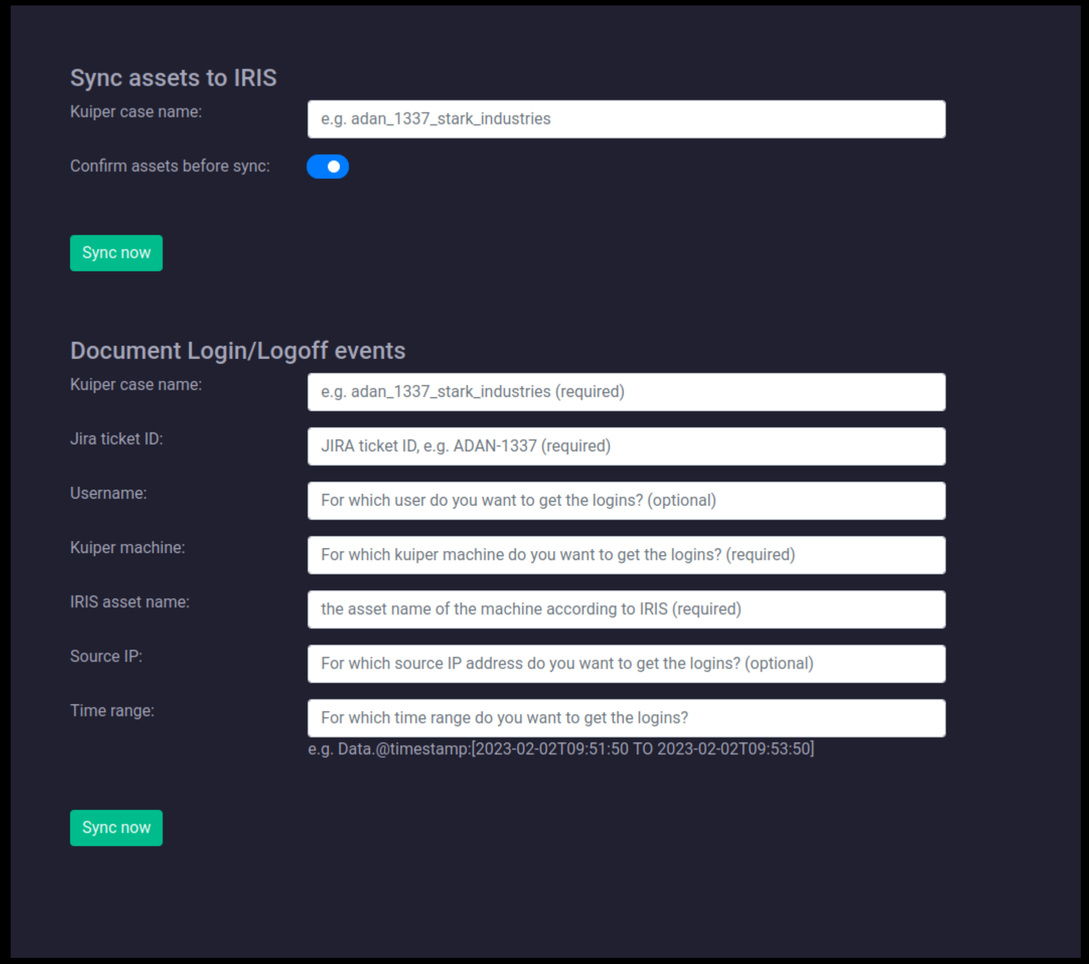
Triage

Nextcloud & TFT

DFIR Kuiper

Parsing & Analyse

Analyst & k2i



G DATA advanced analytics

Velociraptor

Triage

Nextcloud & TFT

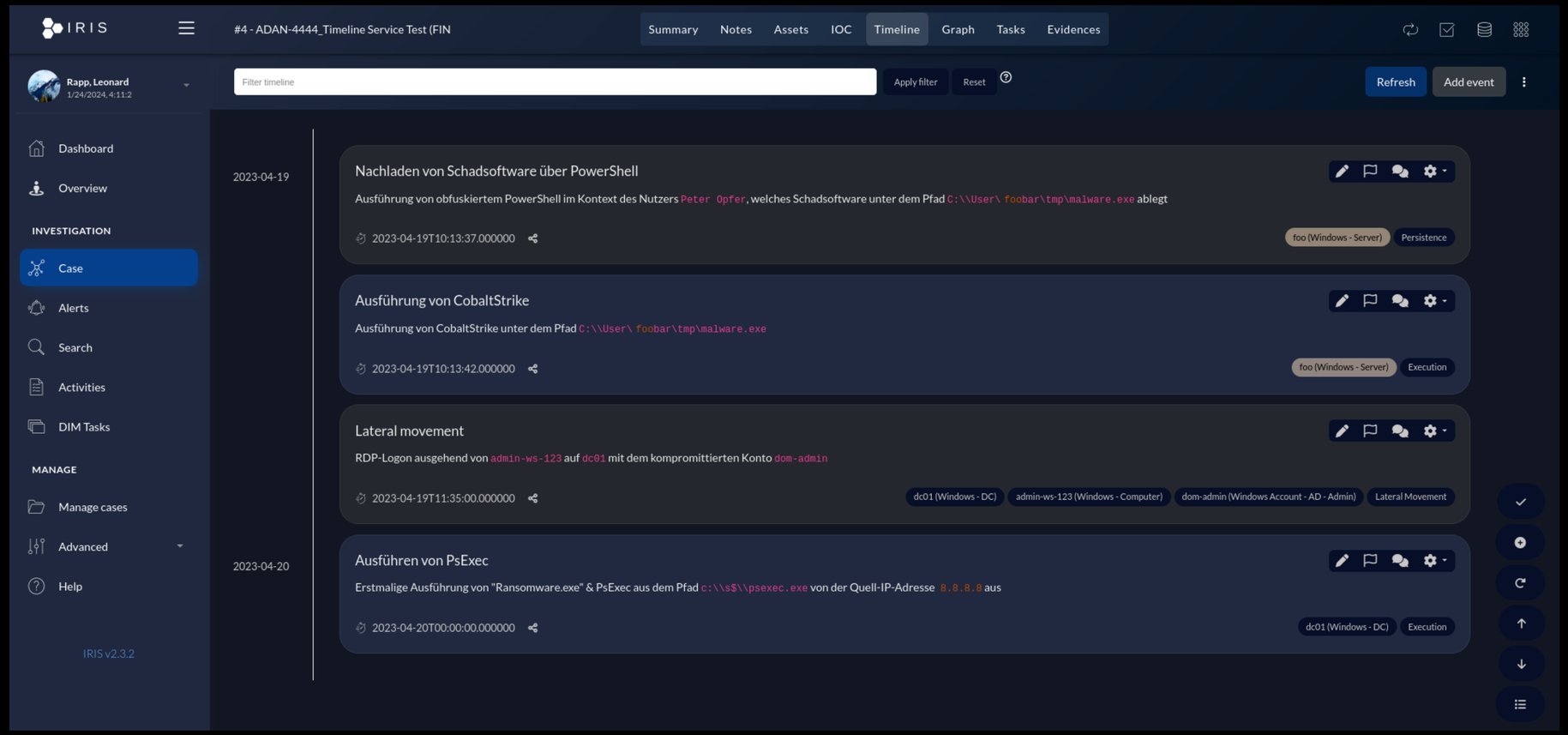
DFIR Kuiper

Parsing & Analyse

Analyst & k2i

DFIR IRIS

Dokumentation



G DATA advanced analytics

Active Cases:

#2 - ADAN-9898_Timeline IRIS Test Case	#24 - ADAN-4199	#32 - ADAN-4398	#35 - ADAN-4539	#34 - ADAN-4540
Timeline / IOCs / Systems	Timeline / IOCs / Systems	Timeline / IOCs / Systems	Timeline / IOCs / Systems	Timeline / IOCs / Systems

G DATA advanced analytics

Velociraptor

Triage

Nextcloud & TFT

DFIR Kuiper

Parsing & Analyse

Analyst & k2i

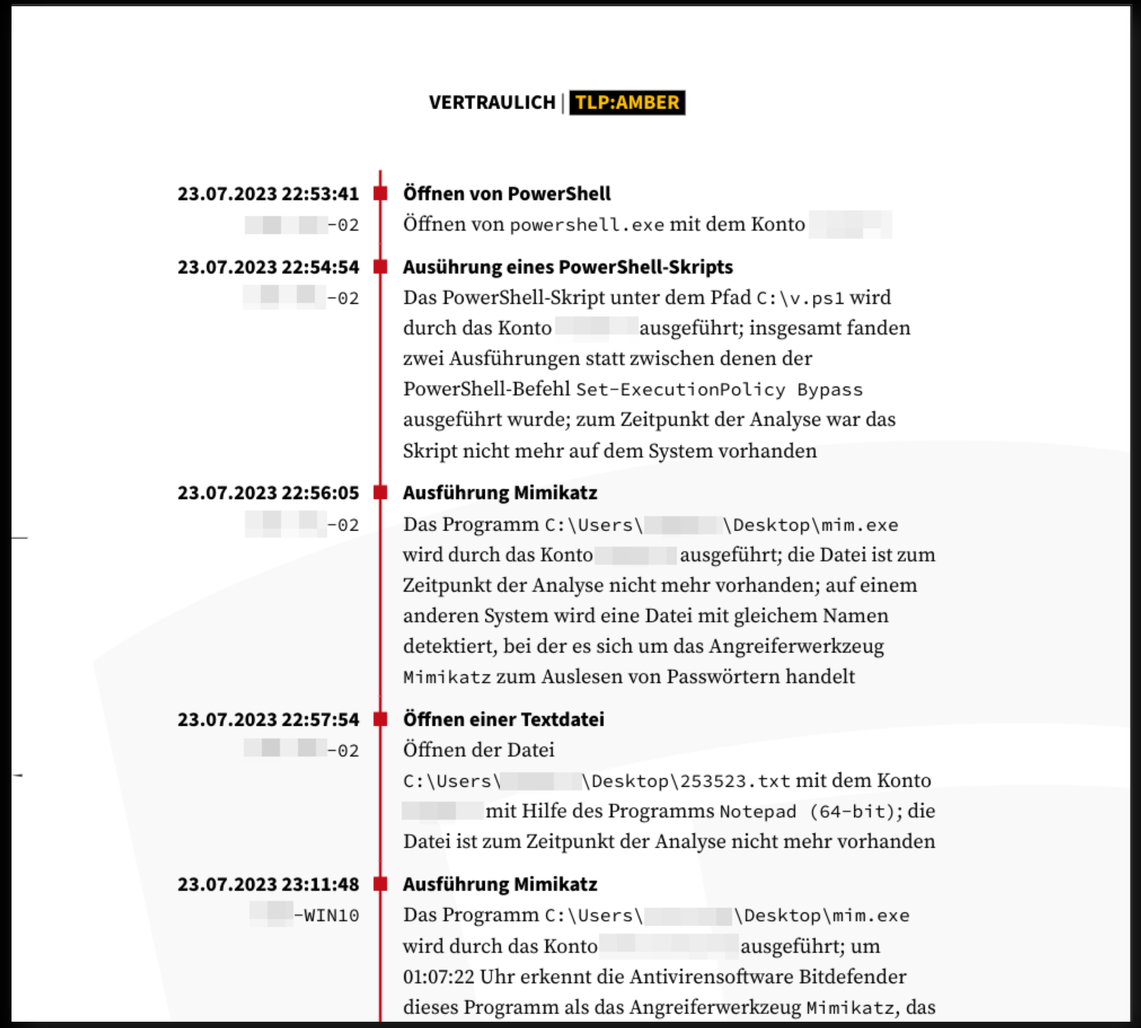
DFIR IRIS

Dokumentation

Timeline Service

LaTeX / PDF

Timeline & Report



VERTRAULICH | TLP:AMBER

23.07.2023 22:53:41 -02
Öffnen von PowerShell
Öffnen von `powershell.exe` mit dem Konto

23.07.2023 22:54:54 -02
Ausührung eines PowerShell-Skripts
Das PowerShell-Skript unter dem Pfad `C:\v.ps1` wird durch das Konto ausgeführt; insgesamt fanden zwei Ausführungen statt zwischen denen der PowerShell-Befehl `Set-ExecutionPolicy Bypass` ausgeführt wurde; zum Zeitpunkt der Analyse war das Skript nicht mehr auf dem System vorhanden

23.07.2023 22:56:05 -02
Ausführung Mimikatz
Das Programm `C:\Users\ \Desktop\mim.exe` wird durch das Konto ausgeführt; die Datei ist zum Zeitpunkt der Analyse nicht mehr vorhanden; auf einem anderen System wird eine Datei mit gleichem Namen detektiert, bei der es sich um das Angreiferwerkzeug `Mimikatz` zum Auslesen von Passwörtern handelt

23.07.2023 22:57:54 -02
Öffnen einer Textdatei
Öffnen der Datei `C:\Users\ \Desktop\253523.txt` mit dem Konto mit Hilfe des Programms `Notepad (64-bit)`; die Datei ist zum Zeitpunkt der Analyse nicht mehr vorhanden

23.07.2023 23:11:48 -WIN10
Ausführung Mimikatz
Das Programm `C:\Users\ \Desktop\mim.exe` wird durch das Konto ausgeführt; um 01:07:22 Uhr erkennt die Antivirensoftware Bitdefender dieses Programm als das Angreiferwerkzeug `Mimikatz`, das

G DATA advanced analytics

Fragen?