RSAConference™2023

San Francisco | April 24 – 27 | Moscone Center

Stronger Together

SESSION ID: AIR-M05

Hunting Stealth Adversaries with Graphs & AI

#RSAC

Jess Garcia

Founder of One eSecurity | Senior SANS instructor
@j3ssgarcia

(one) eSecurity SANS GIAC CERTIFICATIONS

Disclaimer

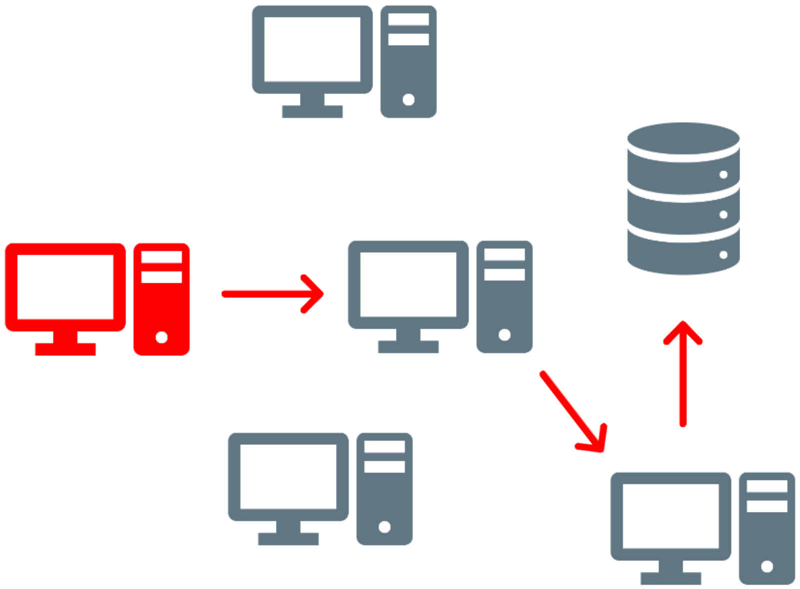
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Our Objective

Would you be able to **Detect a Stealth Adversary** moving through the network?

This is a tough challenge due to the inherent noise of non-malicious activity

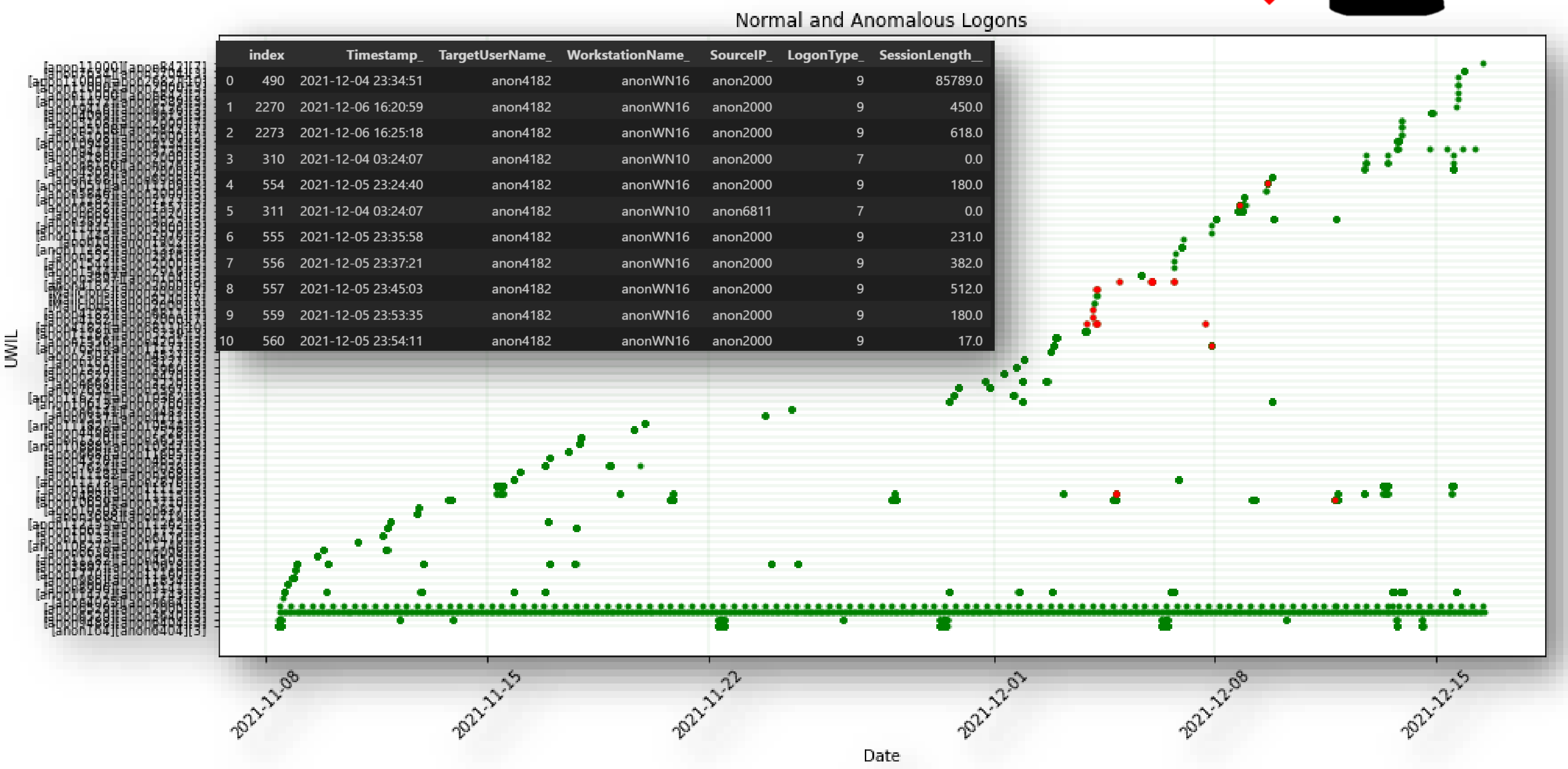


In past RSAC editions …

TOP 100 MALICIOUS EVENTS

We used ML to find anomalous/malicious logons

www.ds4n6.io/rsac22



	index	Timestamp_	TargetUserName_	WorkstationName_	SourceIP_	LogonType_	SessionLength__
0	490	2021-12-04 23:34:51	anon4182	anonWN16	anon2000	9	85789.0
1	2270	2021-12-06 16:20:59	anon4182	anonWN16	anon2000	9	450.0
2	2273	2021-12-06 16:25:18	anon4182	anonWN16	anon2000	9	618.0
3	310	2021-12-04 03:24:07	anon4182	anonWN10	anon2000	7	0.0
4	554	2021-12-05 23:24:40	anon4182	anonWN16	anon2000	9	180.0
5	311	2021-12-04 03:24:07	anon4182	anonWN10	anon6811	7	0.0
6	555	2021-12-05 23:35:58	anon4182	anonWN16	anon2000	9	231.0
7	556	2021-12-05 23:37:21	anon4182	anonWN16	anon2000	9	382.0
8	557	2021-12-05 23:45:03	anon4182	anonWN16	anon2000	9	512.0
9	559	2021-12-05 23:53:35	anon4182	anonWN16	anon2000	9	180.0
10	560	2021-12-05 23:54:11	anon4182	anonWN16	anon2000	9	17.0

Hunt Evil: Lateral Movement

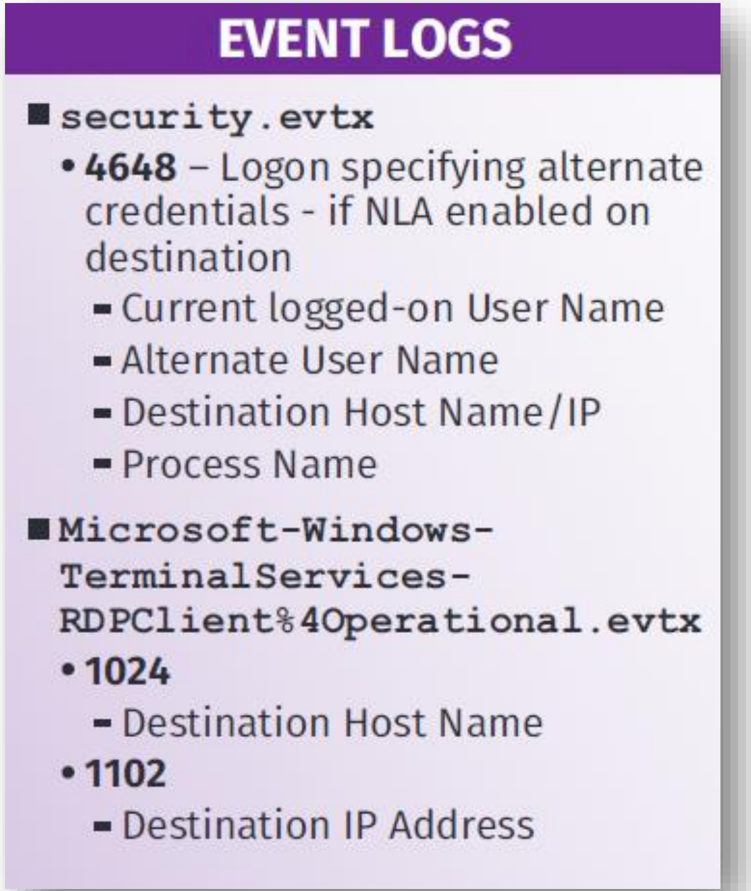
https://www.sans.org/posters/hunt-evil/

- Remote Desktop
- Map Network Shares (net.exe)
- PsExec
- Schedule Tasks
- Services
- WMI/WMIC
- PowerShell Remoting

Hunt Evil: Lateral Movement

Remote Desktop

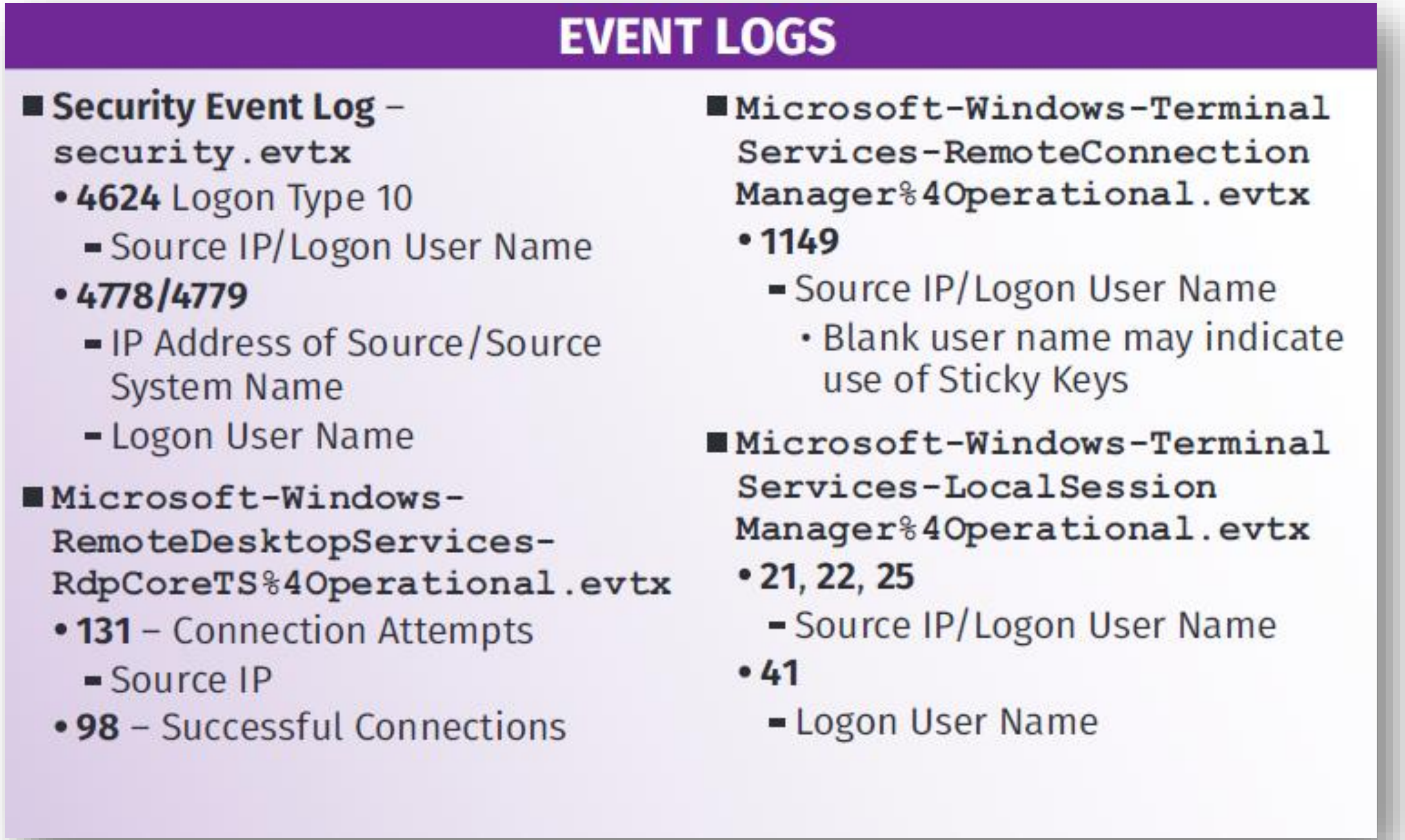
SOURCE



EVENT LOGS

- security.evtx
  - **4648** – Logon specifying alternate credentials - if NLA enabled on destination
    - Current logged-on User Name
    - Alternate User Name
    - Destination Host Name/IP
    - Process Name
- Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx
  - **1024**
    - Destination Host Name
  - **1102**
    - Destination IP Address

DESTINATION



EVENT LOGS

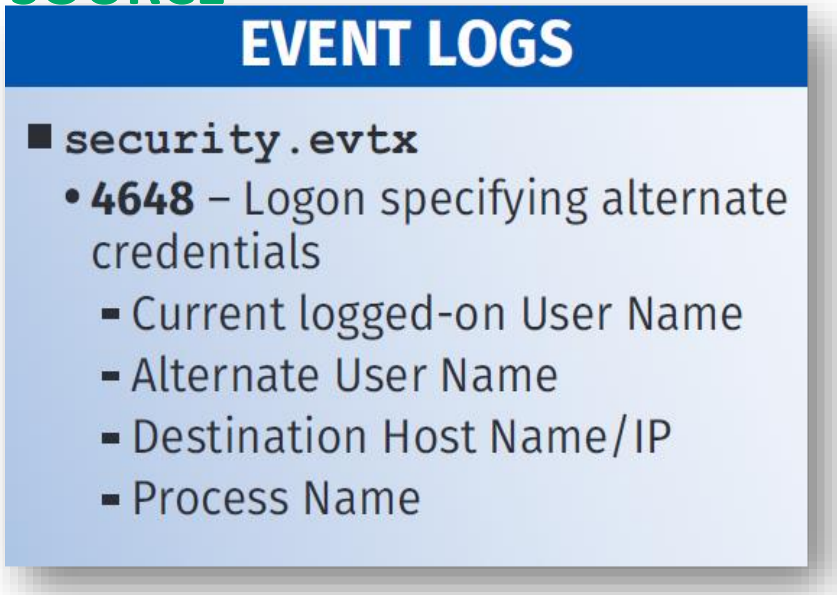
- **Security Event Log** – security.evtx
  - **4624** Logon Type 10
    - Source IP/Logon User Name
  - **4778/4779**
    - IP Address of Source/Source System Name
    - Logon User Name
- Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx
  - **131** – Connection Attempts
    - Source IP
  - **98** – Successful Connections
- Microsoft-Windows-Terminal Services-RemoteConnection Manager%4Operational.evtx
  - **1149**
    - Source IP/Logon User Name
      - Blank user name may indicate use of Sticky Keys
- Microsoft-Windows-Terminal Services-LocalSession Manager%4Operational.evtx
  - **21, 22, 25**
    - Source IP/Logon User Name
  - **41**
    - Logon User Name

Source: SANS DFIR Poster – Hunt Evil (v4.10_02-23)
https://www.sans.org/posters/hunt-evil/

Hunt Evil: Lateral Movement

WMI/WMIC

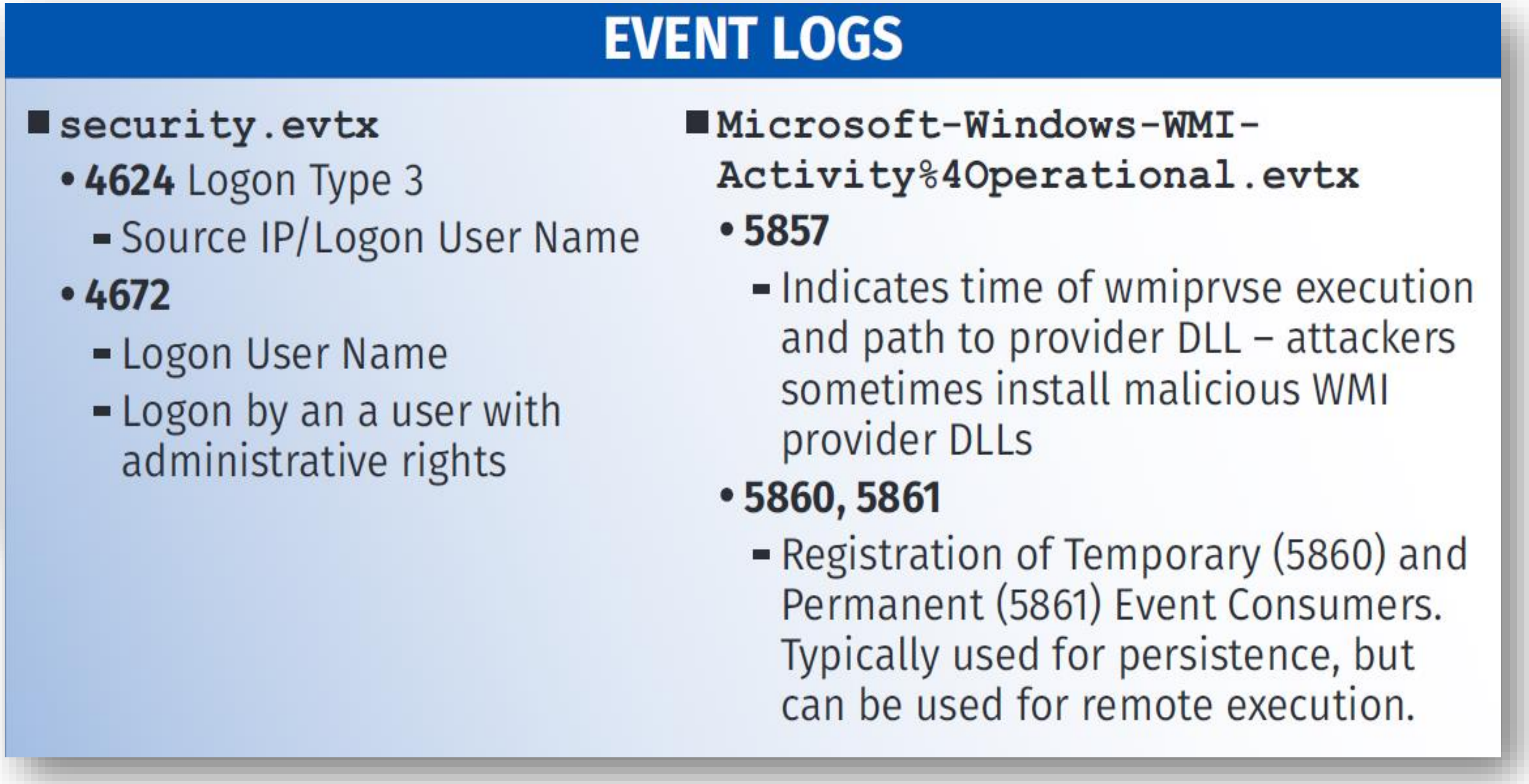
SOURCE



EVENT LOGS

- `security.evtx`
  - **4648** – Logon specifying alternate credentials
    - Current logged-on User Name
    - Alternate User Name
    - Destination Host Name/IP
    - Process Name

DESTINATION



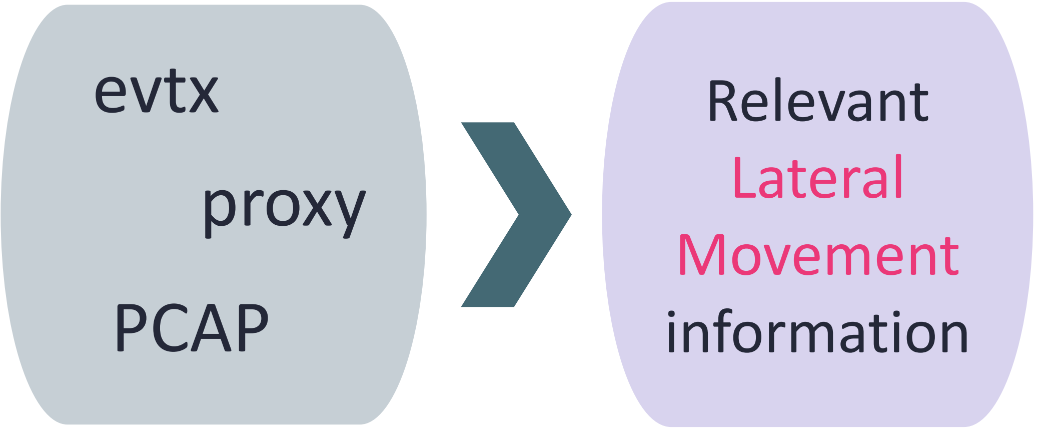
EVENT LOGS

- `security.evtx`
  - **4624** Logon Type 3
    - Source IP/Logon User Name
  - **4672**
    - Logon User Name
    - Logon by an a user with administrative rights
- `Microsoft-Windows-WMI-Activity%4Operational.evtx`
  - **5857**
    - Indicates time of wmiprvse execution and path to provider DLL – attackers sometimes install malicious WMI provider DLLs
  - **5860, 5861**
    - Registration of Temporary (5860) and Permanent (5861) Event Consumers. Typically used for persistence, but can be used for remote execution.

Source: SANS DFIR Poster – Hunt Evil (v4.10_02-23)
https://www.sans.org/posters/hunt-evil/

Sabonis

Digital Forensic and Incident Response **Pivoting Tool**



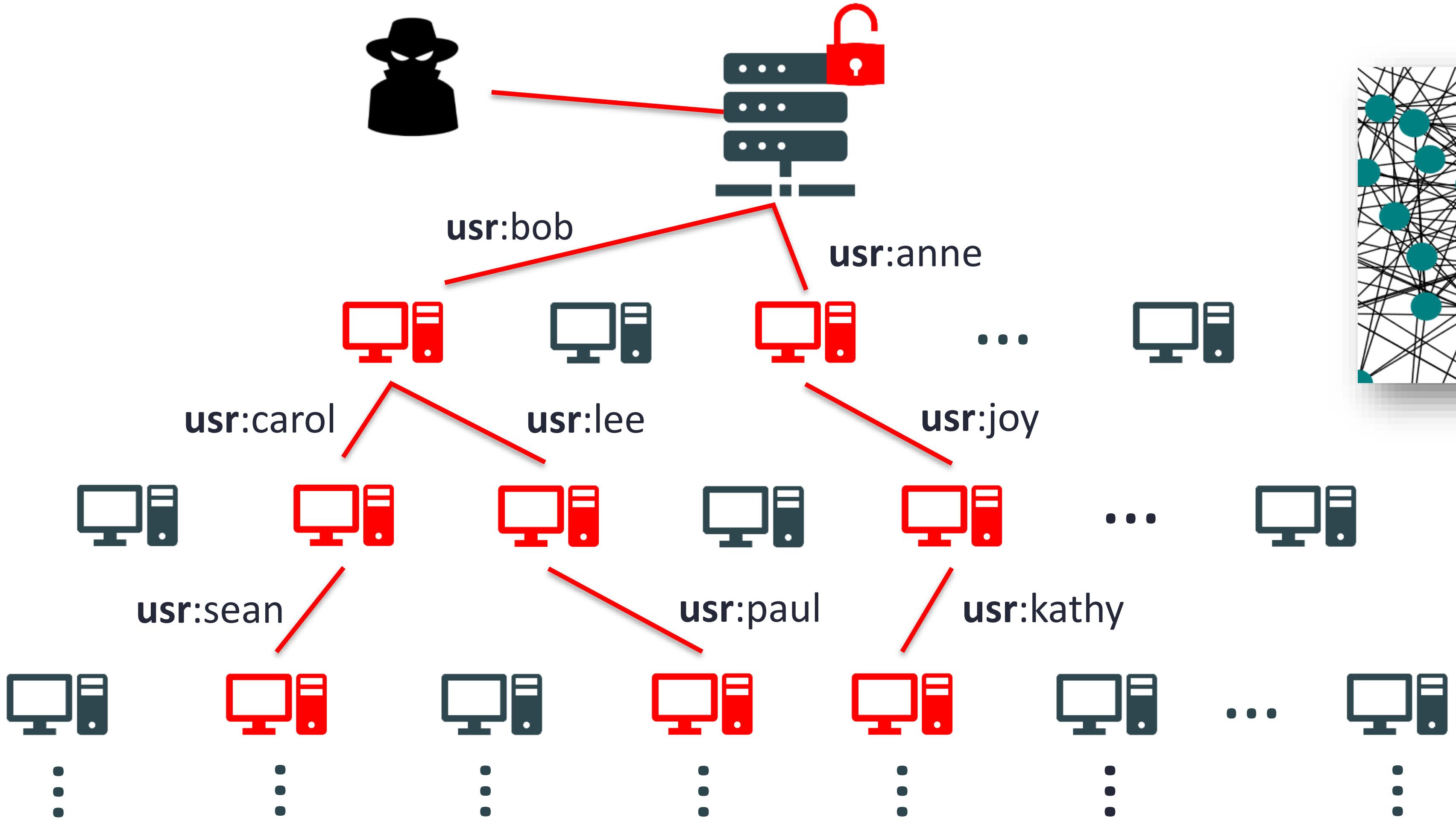
- 🔍 Extracts and merges **LM** from 7 different **EVTX files**
- 🔍 Parses Squid **proxy events**
- 🔍 Extracts all LM from **PCAP files**
- ⚡ Quick and **low memory comsumption**
- 📄 Loads different sources into a **Neo4J database**
- 🔍 Includes a **Cypher Playbook** to make investigations easy

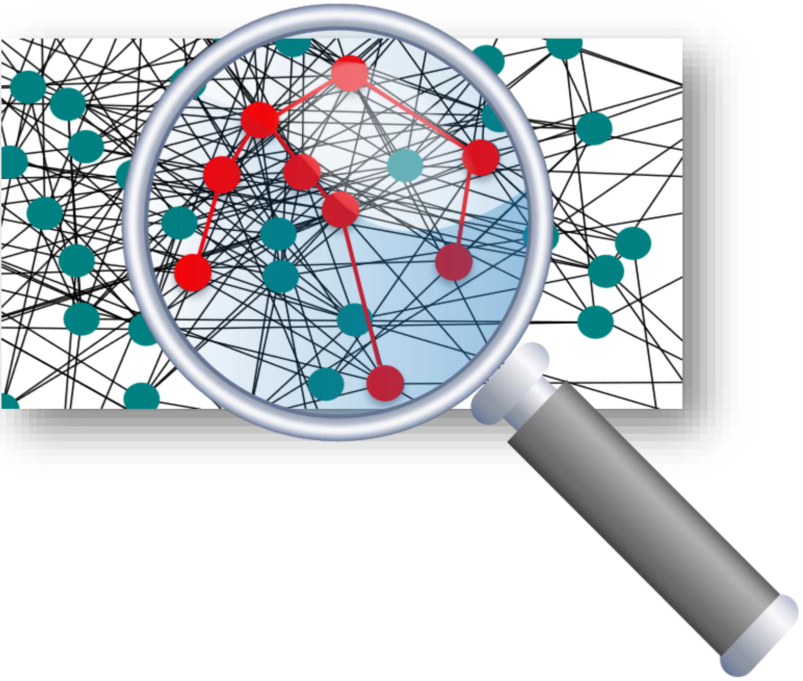
https://github.com/jupyterj0nes/sabonis

The New Challenge

- How to detect **Anomalies at Scale**?
- How to detect **Lateral Movement** in a network with hundreds or thousands of nodes?

Threat Actor: Lateral Movement



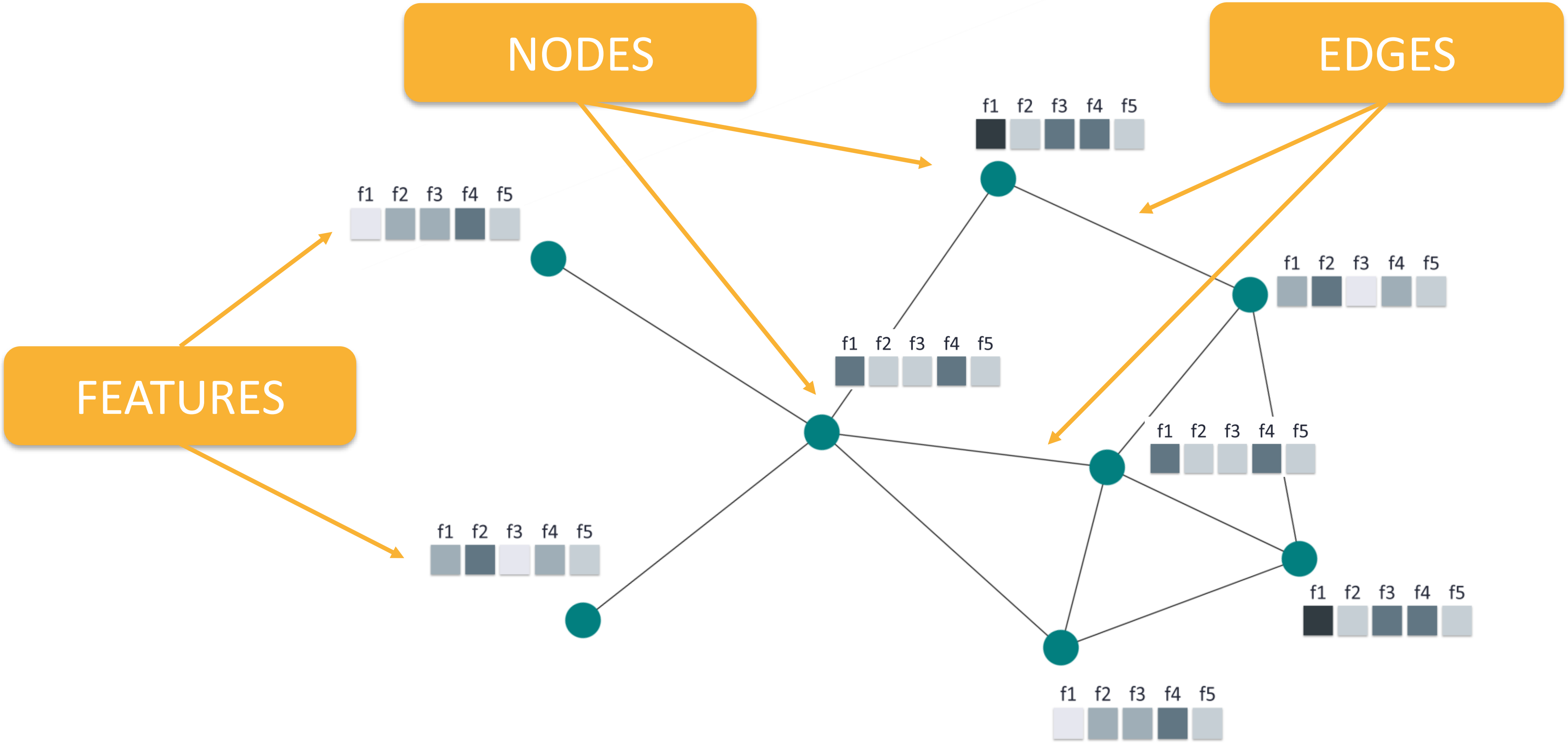


Stronger Together

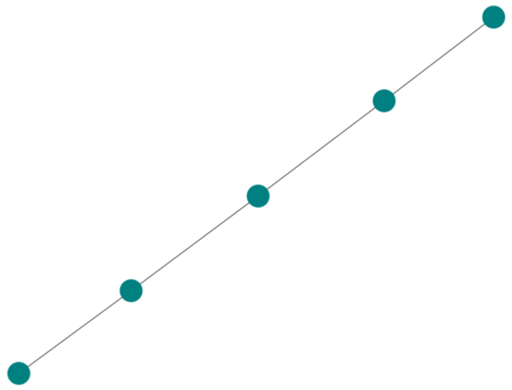
THE POWER OF GRAPHS

All you need are graphs

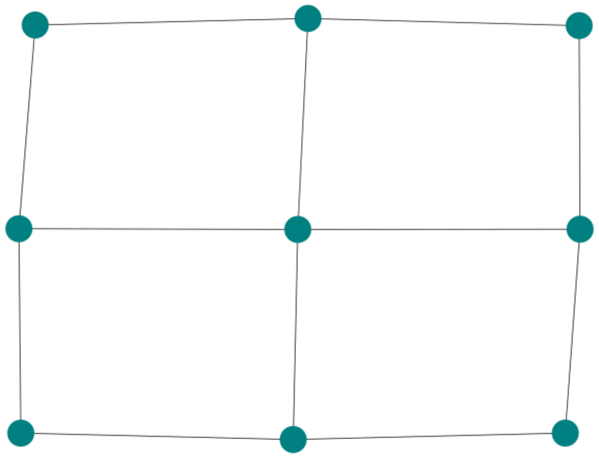
What is a graph?



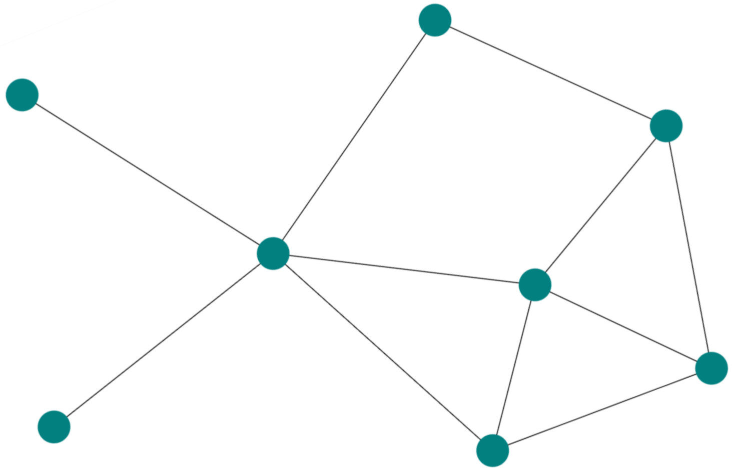
What are graphs for?



Time series

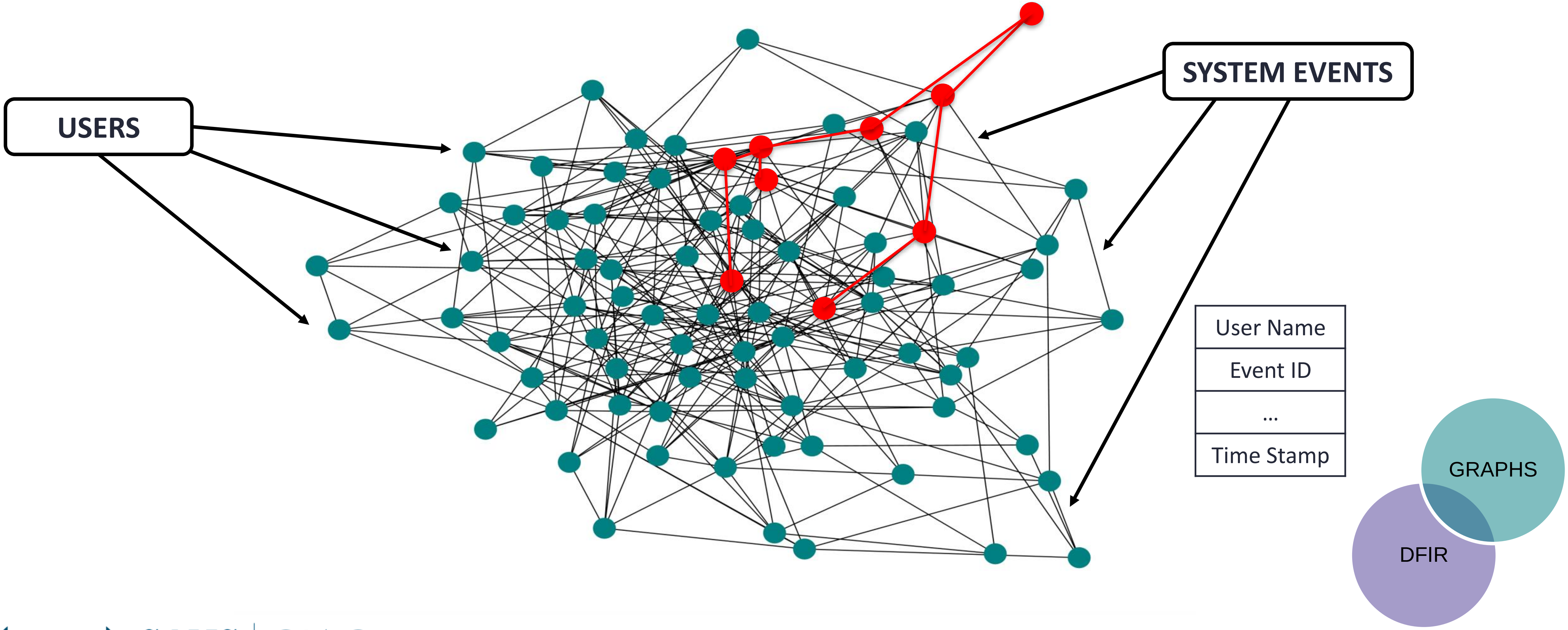


Images



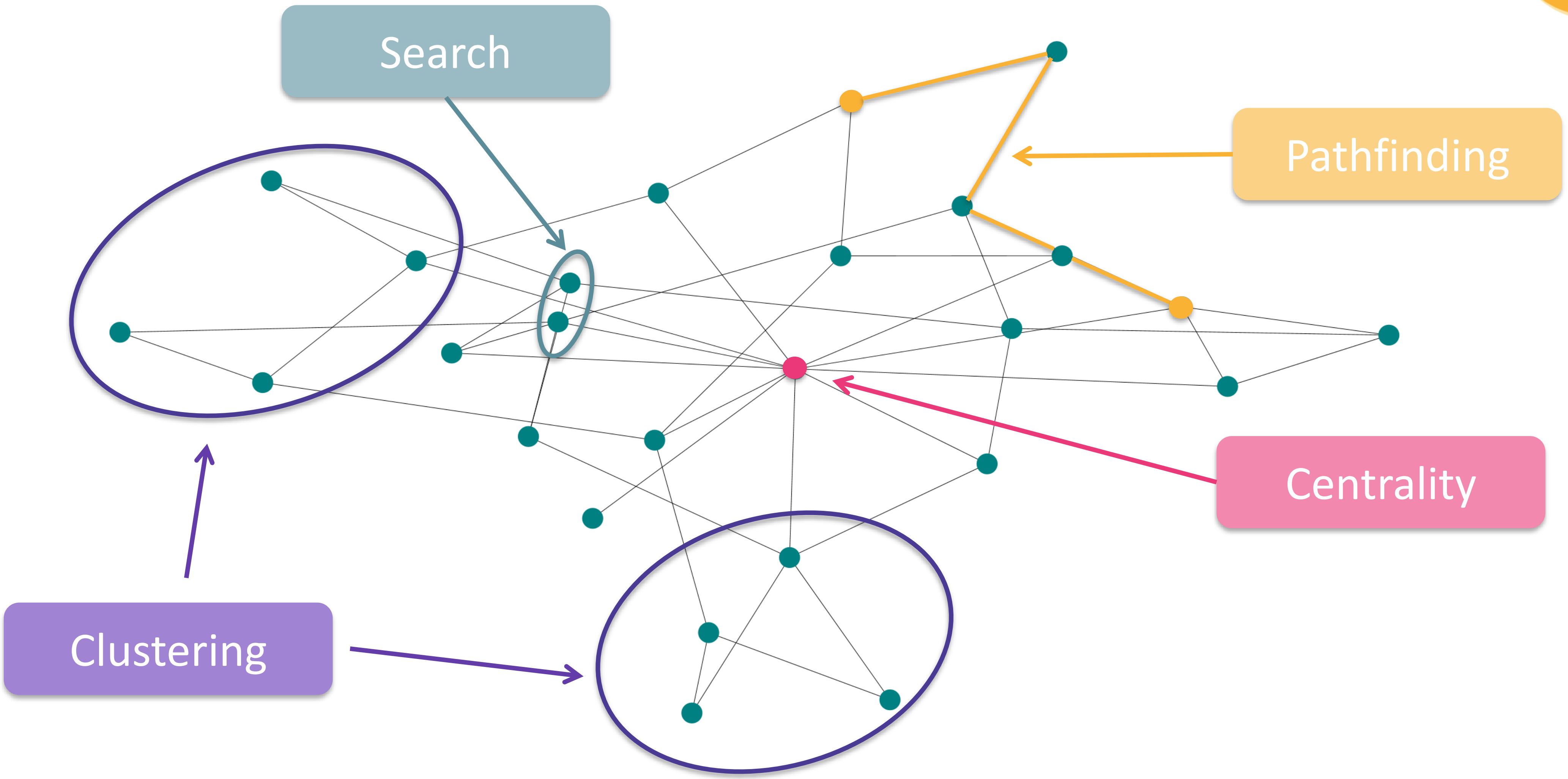
Networks

Lateral Movement on Graphs



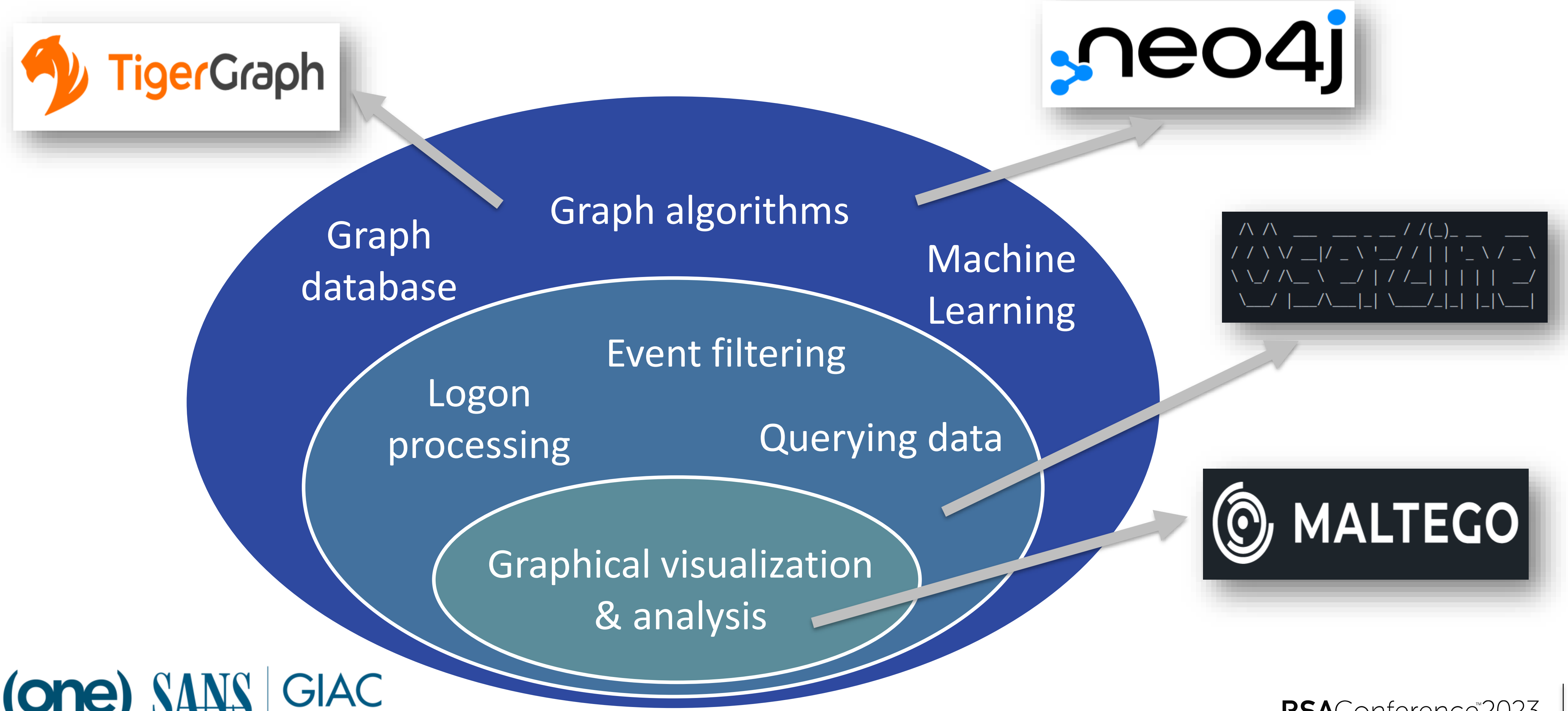
User Name
Event ID
…
Time Stamp

Graph Algorithms



https://www.oreilly.com/library/view/graph-algorithms/9781492047674/

Graph Tools



Graph database

Graph algorithms

Machine Learning

Event filtering

Logon processing

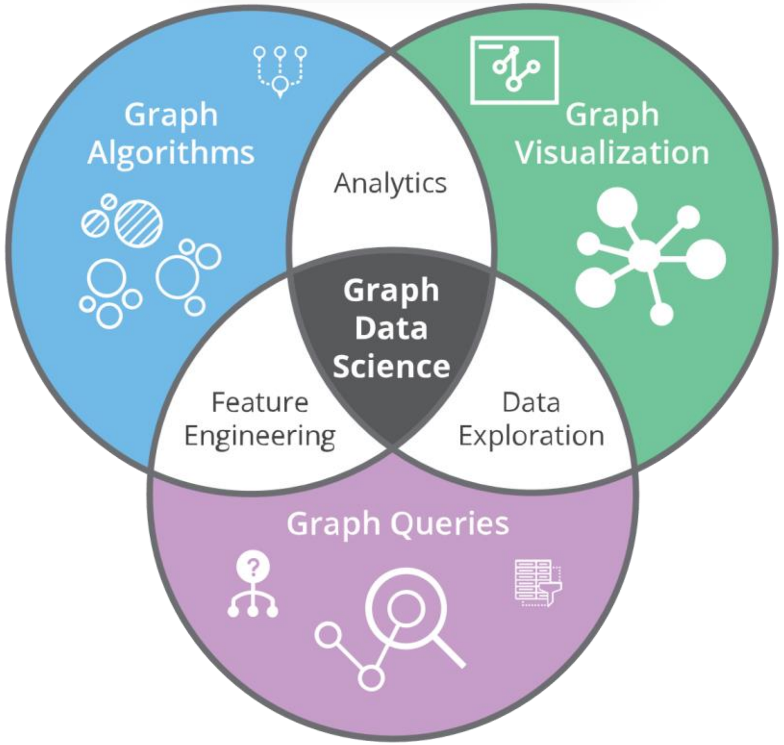
Querying data

Graphical visualization & analysis

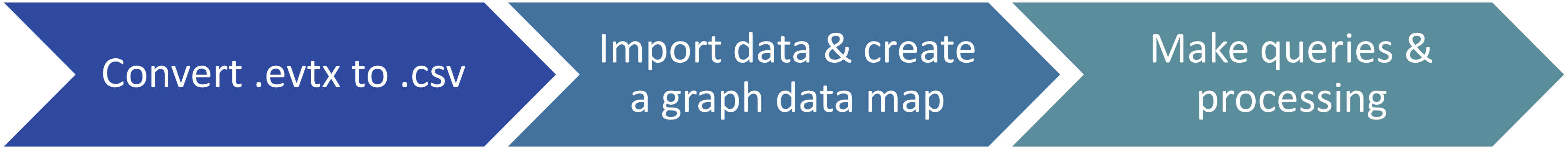
Neo4j

- Graph Data Base Management System
- Graph Visualization Platform
- Graph Data Queries
- Graph Algorithm Catalogue
- ML for Graphs

https://neo4j.com/product/neo4j-graph-database/

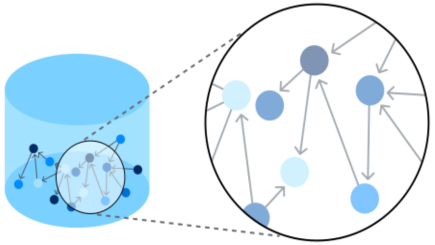


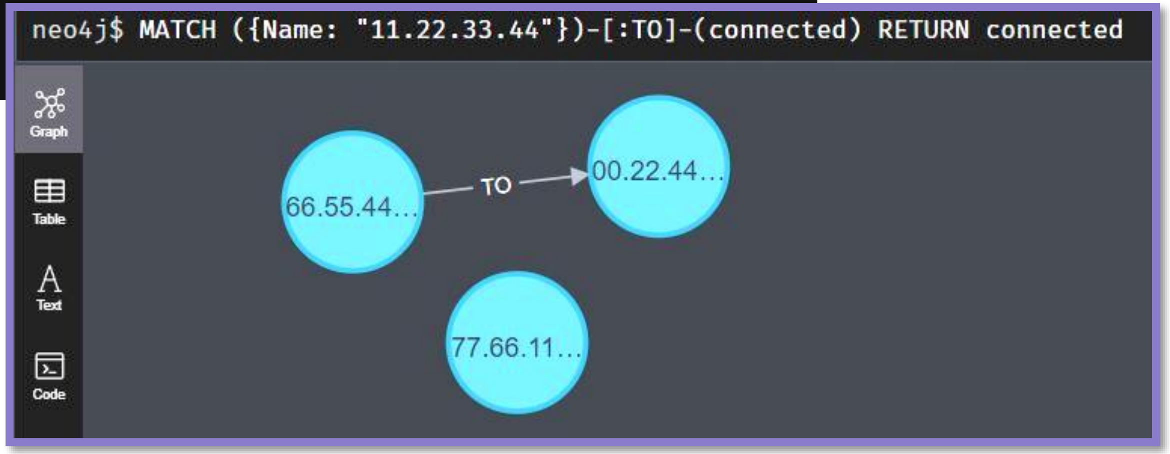
Neo4j: Data Loading


Convert .evtx to .csv
Import data & create a graph data map
Make queries & processing

```
LOAD CSV WITH HEADERS FROM "file:///evtx.csv" AS evtx
MERGE  (src:Host {Name: evtx.source})
MERGE  (dst:Host {Name: evtx.destination})
CREATE (src)-[l:link {date: date(evtx.time)}]->(dst)
MATCH  ({Name: "11.22.33.44"})-[:link]-(connected) RETURN connected


```

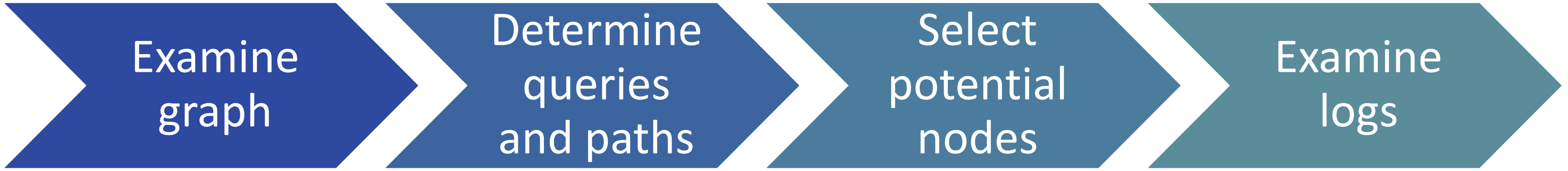


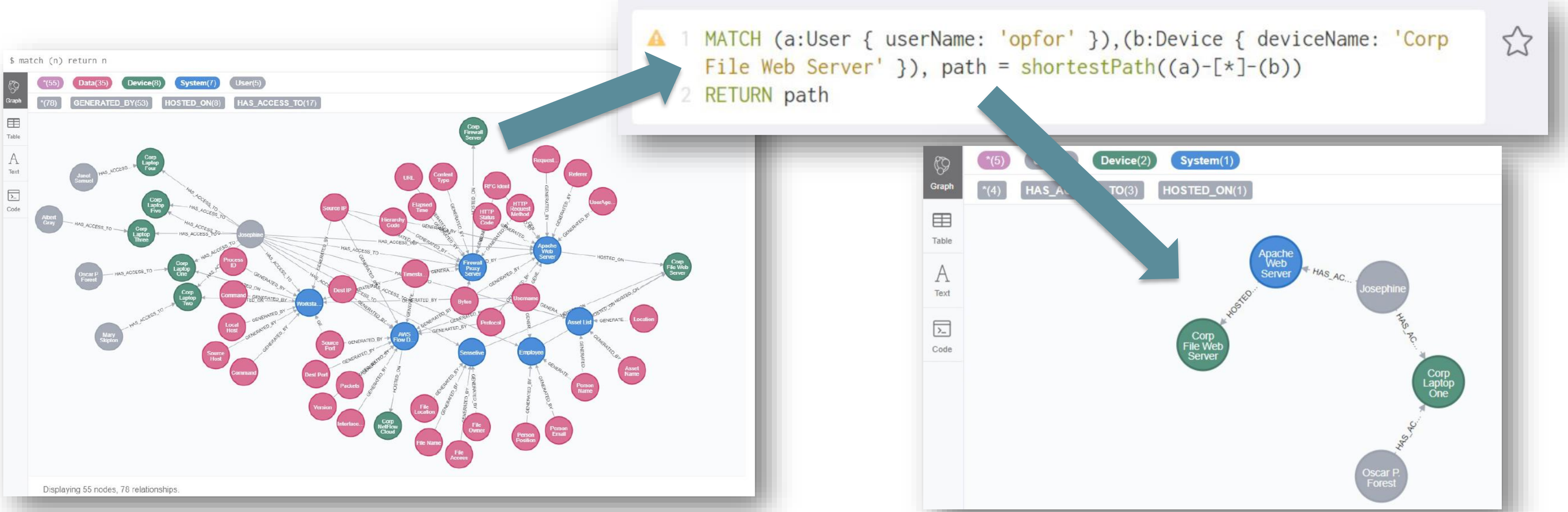


```
neo4j$ MATCH ({Name: "11.22.33.44"})-[:TO]-(connected) RETURN connected
```

https://www.oreilly.com/library/view/hands-on-graph-analytics/9781839212611/

Neo4j: Lateral Movement Analysis





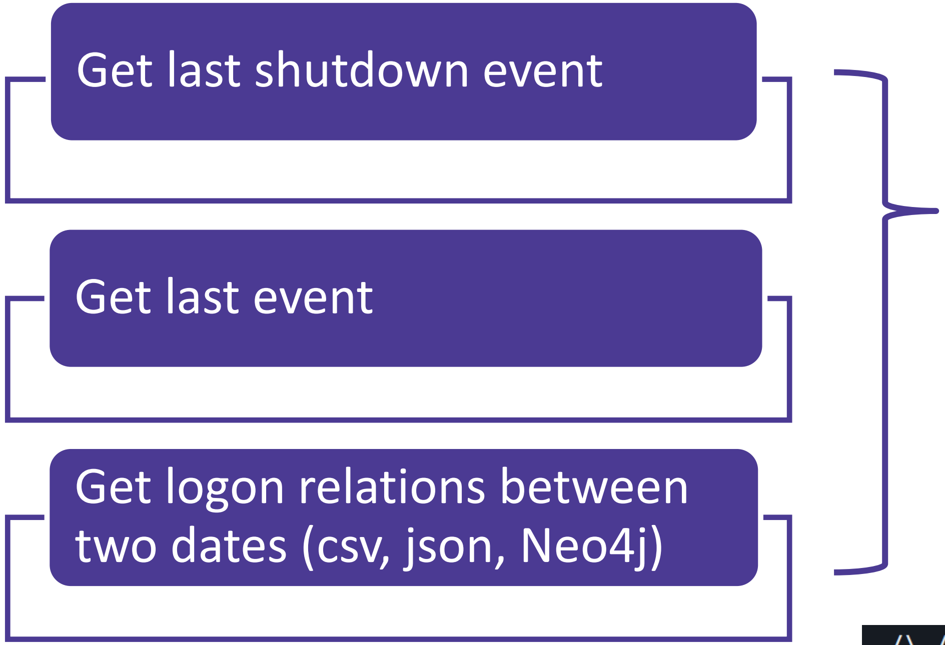
```
$ match (n) return n
```

Displaying 55 nodes, 78 relationships.

```
MATCH (a:User { userName: 'opfor' }),(b:Device { deviceName: 'Corp
File Web Server' }), path = shortestPath((a)-[*]-(b))
RETURN path
```

https://www.sans.org/white-papers/39030/

UserLine



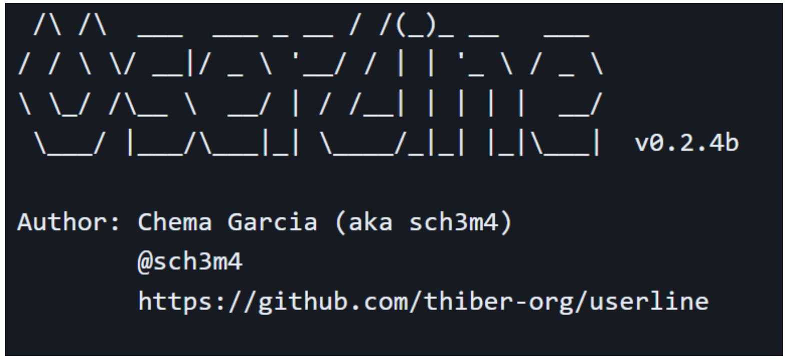
Logon Events

- WORKSTATION_UNLOCKED=4801
- SCREENSAVER_DIMISSED=4803
- LOGON=4624
- LOGON_EXPLICIT=4648
- SESSION_RECONNECTED=4778

Logoff Events

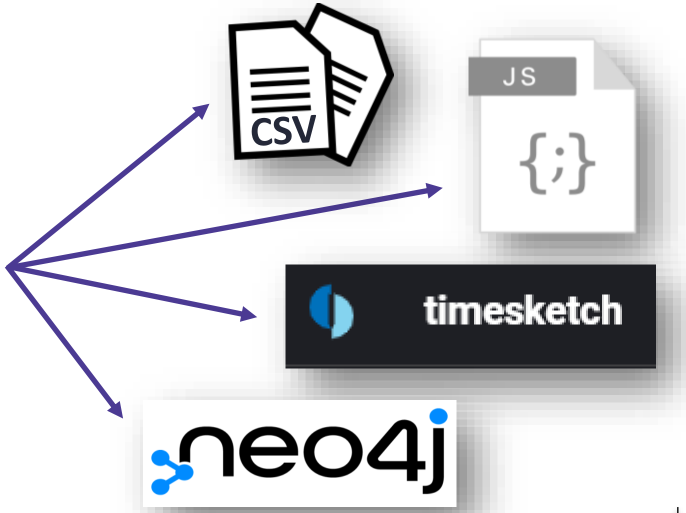
- WORKSTATION_LOCKED=4800
- SCREENSAVER_INVOKED=4802
- SHUTDOWN=4609
- LOGOFF=4634
- SESSION_DISSCONECTED=4779
- LOGOFF_INITIATED=4647

https://github.com/THIBER-ORG/userline



```
 /\ /\  ___  ___ _ __ / /(_)_ __   ___
/ / \ \/ __|/ _ \ '__/ / | | '_ \ / _ \
\ \_/ /\__ \  __/ | / /__| | | | |  __/
 \___/ |___/\___|_| \____/_|_| |_|\___|  v0.2.4b

Author: Chema Garcia (aka sch3m4)
        @sch3m4
        https://github.com/thiber-org/userline
```

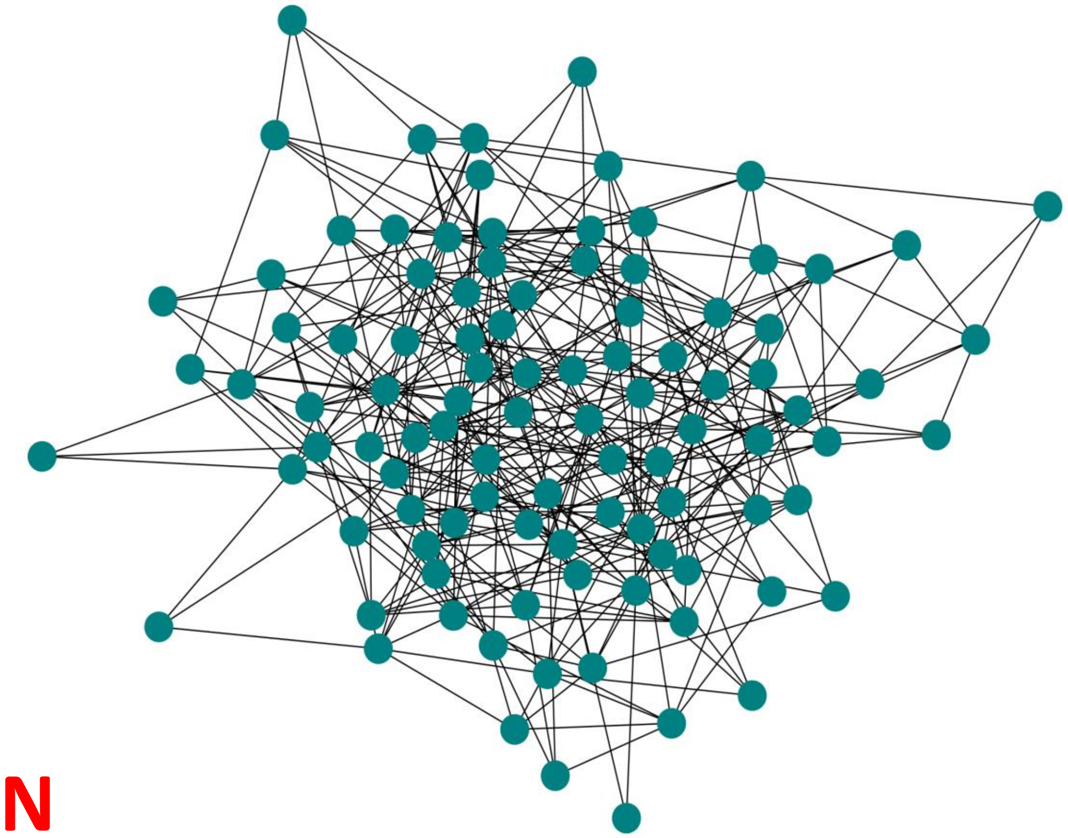


Initial Problem

Would we be able to detect **Lateral Movement** in complex networks?

For large amounts of data, visual analysis may **NOT** be effective.

WE NEED AUTOMATIZATION



Initial Problem

Would AI / ML help in this intense and time-consuming task?

RSAConference™2023

Stronger Together

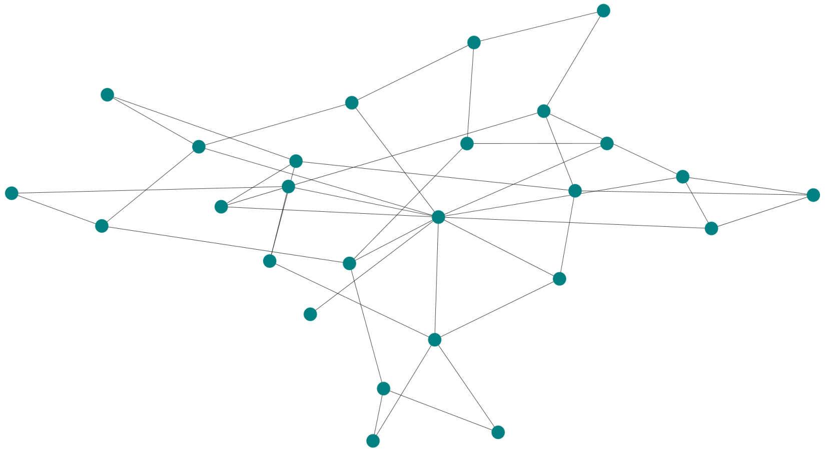
MACHINE LEARNING FOR GRAPHS

Stronger Together

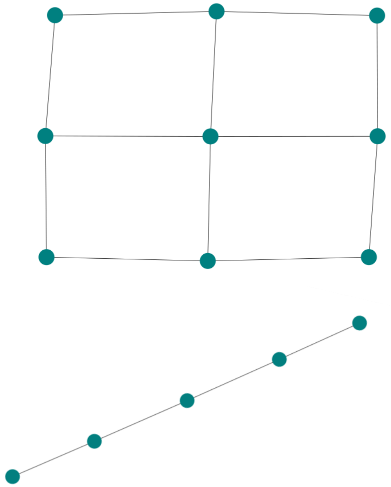
(one) eSecurity SANS | GIAC CERTIFICATIONS

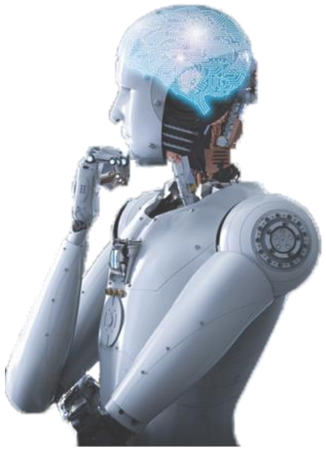
The Challenge

Most of the existing ML algorithms are specialized in simple data types

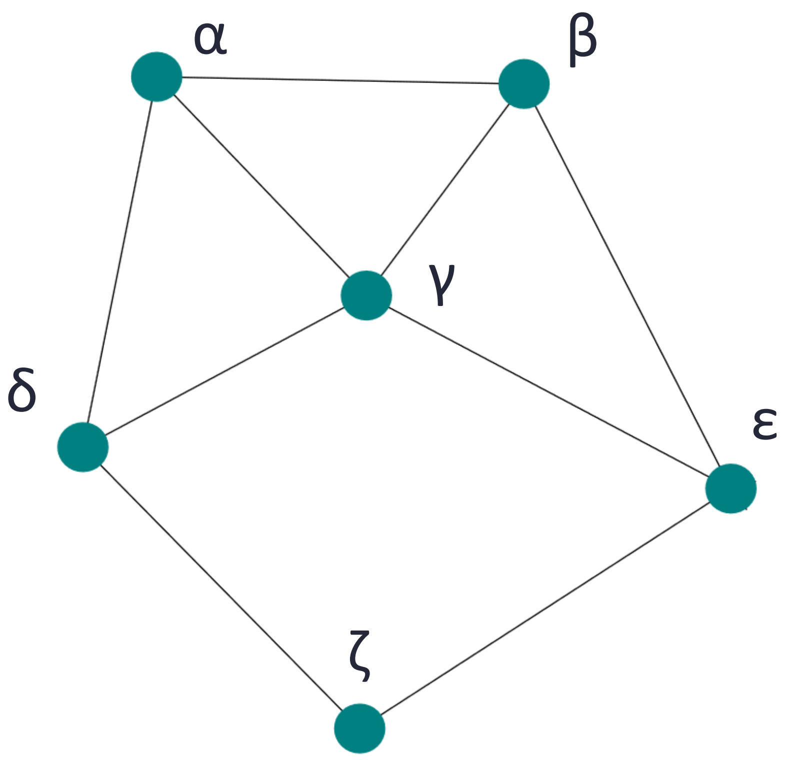


VS





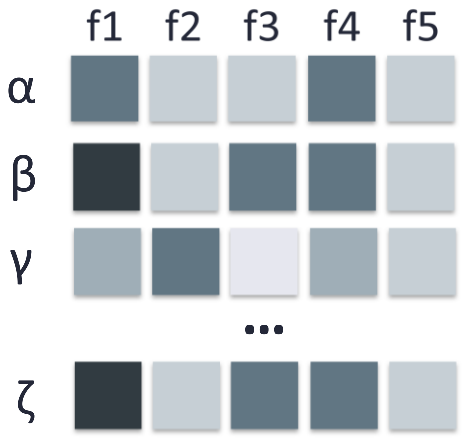
Graph Data



$$
A = \begin{array}{c|cccccc}
 & \alpha & \beta & \gamma & \delta & \varepsilon & \zeta \\
\hline
\alpha & 0 & 1 & 1 & 1 & 0 & 0 \\
\beta & 1 & 0 & 1 & 0 & 1 & 0 \\
\gamma & 1 & 1 & 0 & 1 & 1 & 0 \\
\delta & 1 & 0 & 1 & 0 & 0 & 1 \\
\varepsilon & 0 & 1 & 1 & 0 & 0 & 1 \\
\zeta & 0 & 0 & 0 & 1 & 1 & 0
\end{array}
$$

Adjacency Matrix

X =

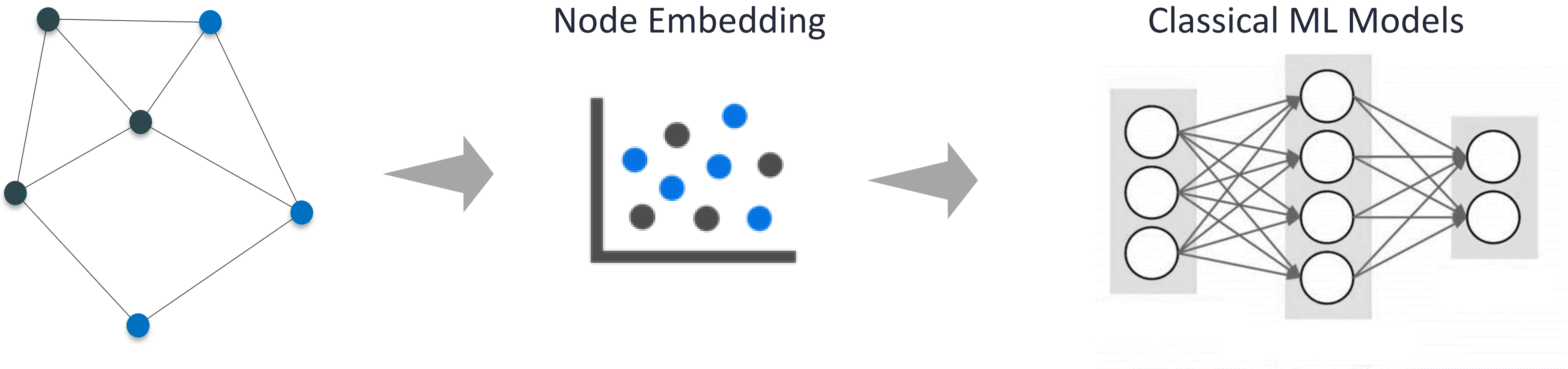


Feature Matrix

https://www.khanacademy.org/computing/computer-science/algorithms/graph-representation/a/representing-graphs

Node Embedding

Map **nodes** in a graph to **numerical features**



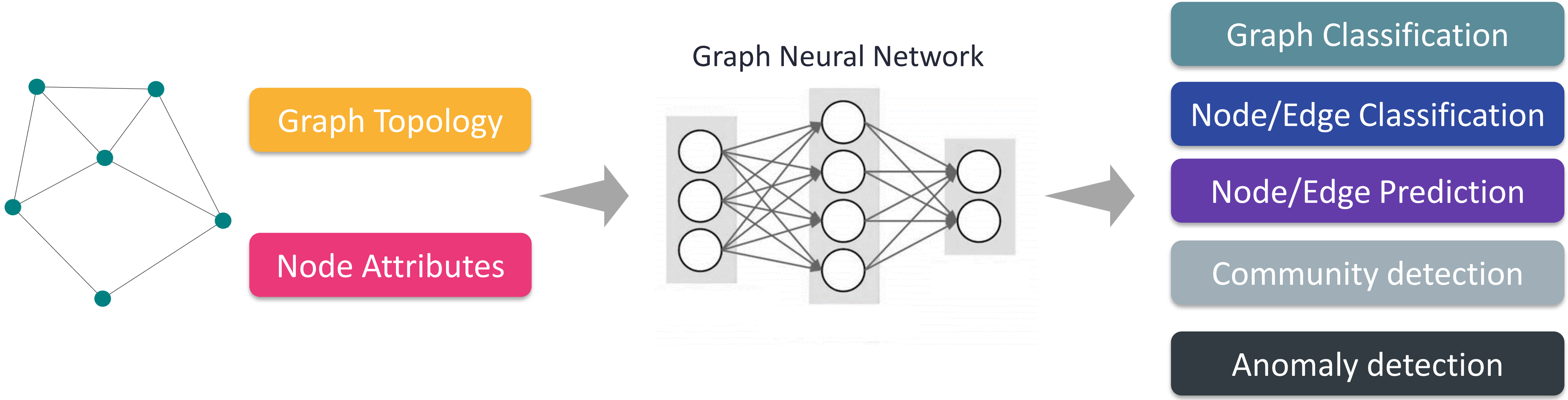
Node Embedding

Classical ML Models

https://towardsdatascience.com/graph-embeddings-how-nodes-get-mapped-to-vectors-2e12549457ed

Graph Neural Networks

GNN are a type of Neural Network capable of working with **graph data structures**



Graph Topology

Node Attributes

Graph Neural Network

Graph Classification

Node/Edge Classification

Node/Edge Prediction

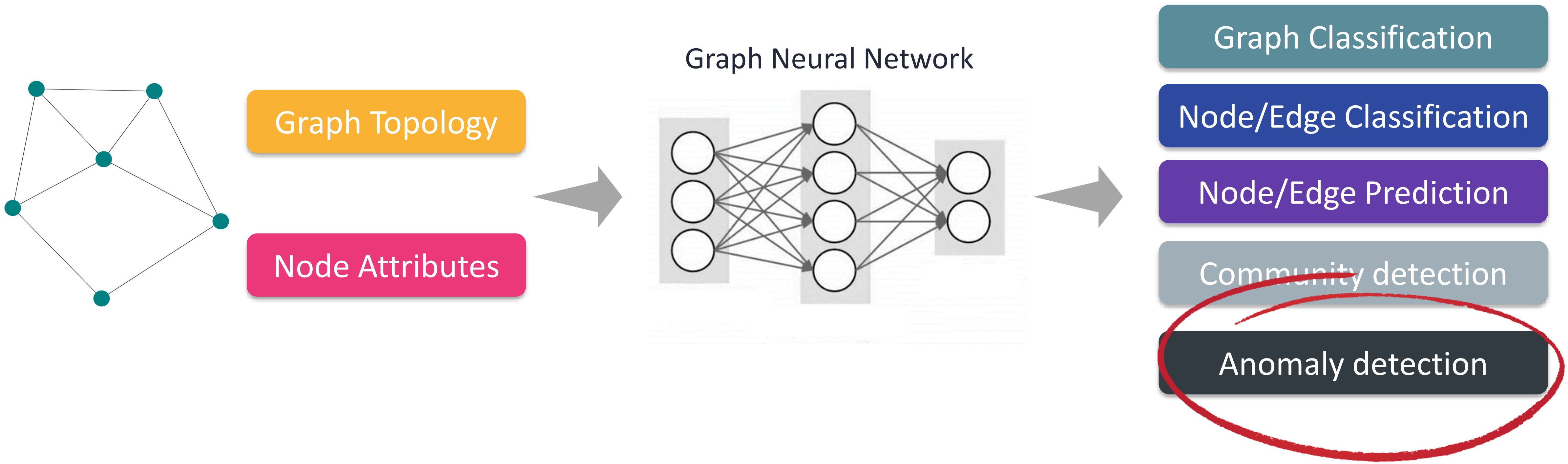
Community detection

Anomaly detection

https://medium.com/@rtsrumi07/understanding-graph-neural-network-with-hands-on-example-part-1-6e35d7fe2777

Graph Neural Networks

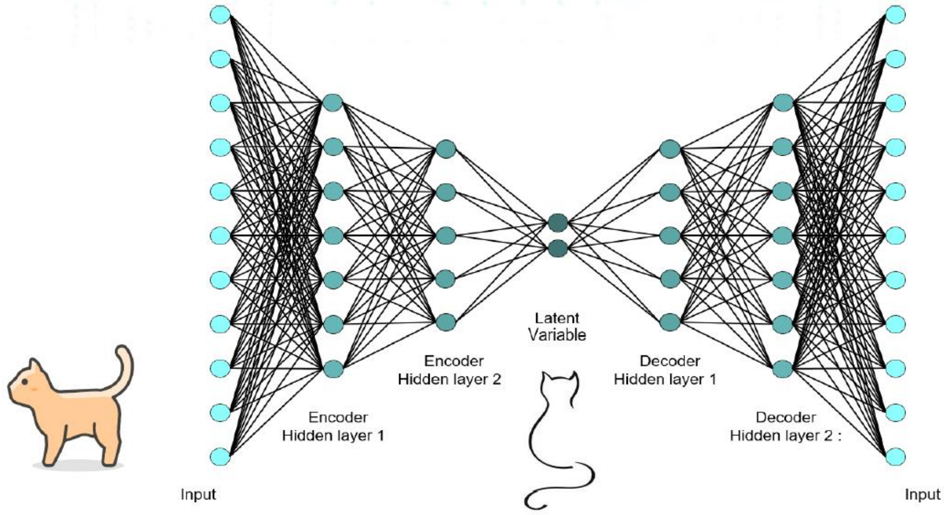
GNN are a type of Neural Network capable of working with **graph data structures**



https://medium.com/@rtsrumi07/understanding-graph-neural-network-with-hands-on-example-part-1-6e35d7fe2777

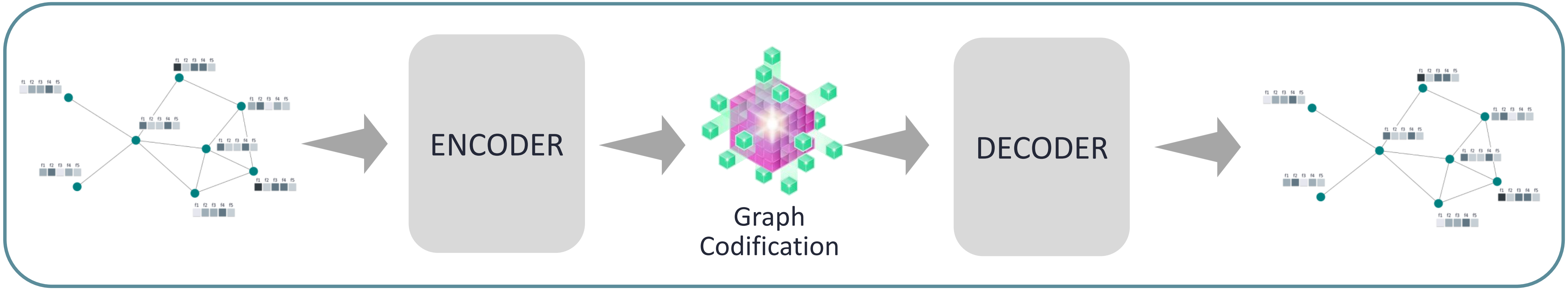
Graph ML for Anomaly Detection

How well are we able to rebuild the input?



Anomaly detection based on the reconstruction error
www.ds4n6.io/rsac21

GRAPH AUTO-ENCODER



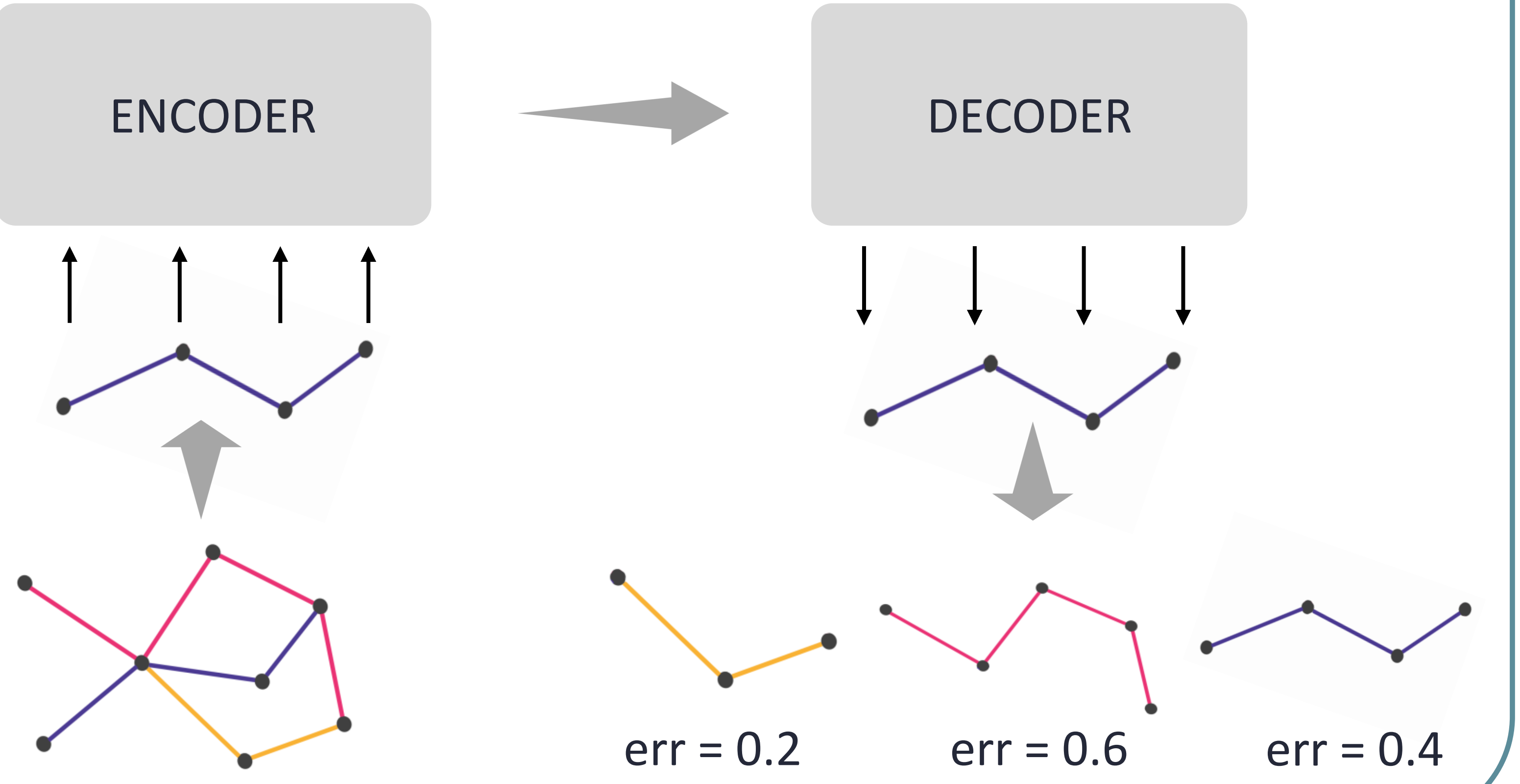
Seq2seq ML Models

LSTM

TRANSFORMERS

ChatGPT

Seq2seq AUTO-ENCODER



Tools for Graph Neural Networks

Take your data to **CHRYSALIS** and use the power of **AI** in your investigations.

PyTorch Spektral PyG TensorFlow

http://www.ds4n6.io/tools/chrysalis

DS4N6 Project

ds4n6.io

Our Mission: Bring **Data Science** & **Artificial Intelligence** to the fingerprints of the average **Forensicator** and promote advances in the field.

Presented in …

THE CYBERSECURITY INDUSTRY COMES TOGETHER FOR RSA CONFERENCE.

I LOOK FORWARD TO SHARING INSIGHTS WITH YOU WHEN I PRESENT AT

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

RSA Conference 2021

RESILIENCE

Digital Forensics & Incident Response

Summit & Training

Live Online

SANS DFIR

ODSC WEST RECONNECT

Conference & Expo

Nov 16th – 18th, 2021

Threat Hunting

Summit & Training

Live Online

FREE SUMMIT: Oct 7–8

TRAINING: Oct 11–16

SANS DFIR

(one) eSecurity SANS GIAC CERTIFICATIONS

DS4N6.io

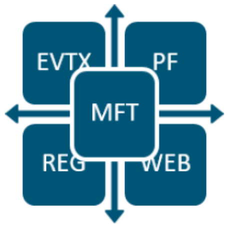
DS4N6

Data Science & ML for DFIR Analysts

http://www.ds4n6.io

CHRYSALIS

D4ML



HAM

ADversAry eMulator

Daisy VM

CHRYSALIS

CHRYSALIS

Python framework that provides high-level DS/ML functions to support incident response tasks

More information in:
ds4n6.io/chrysalis

With only 7 functions take your forensic analysis to the next level

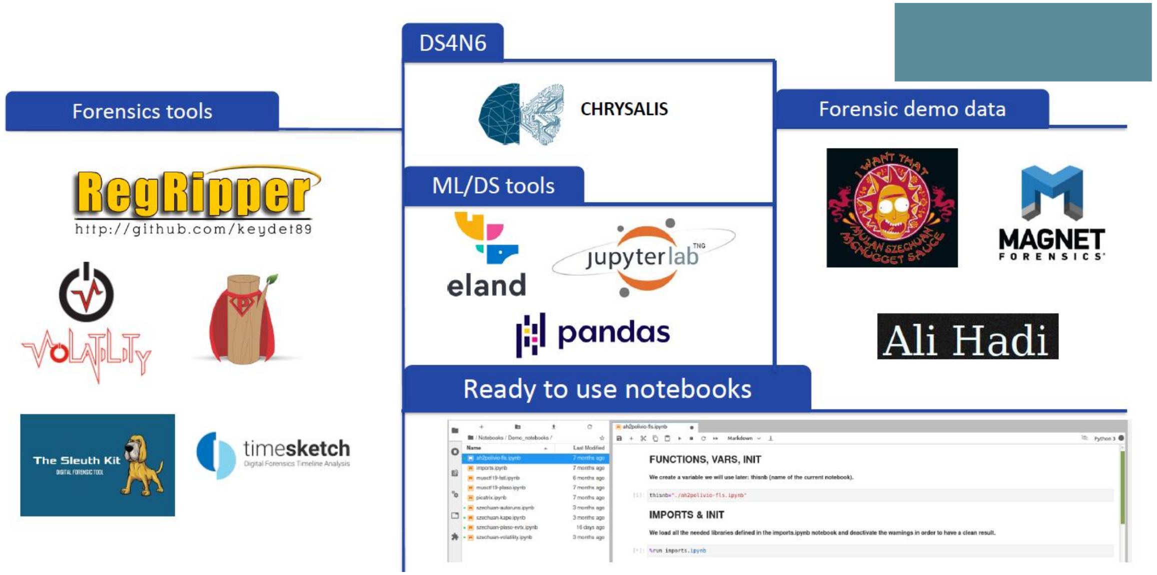
whatis()	Identifies the forensic data type of an object (DataFrame –df– or DataFrame Collection –dfs–).
xread()	Reads tool output data (e.g. Plaso output) and stores it in a df/dfs.
xmenu()	Selects a df from dfs, or a column from a df, displaying the selected data allowing manual analysis.
xanalysis()	Displays a mane with the advanced analysis functions available for the given data type (i.e. forensic artifact).
xdisplay()	Used to select the display settings for the df that will be displayed (max. rows, max. columns, etc.).
simple()	Simplifies forensic output (df) showing only the most interesting columns for analysis.
xgrep()	UNIX-like grep for the df world. Allows the user to search for a regular expression in a df column or full df.

DAISY

Daisy VM

Ready to use DS Virtual Machine designed to carry out Data Science and Machine/Deep Learning Analysis on DFIR data

More information in:
ds4n6.io/daisy



/ Notebooks / Demo_notebooks /

Name	Last Modified
ah2polivio-fls.ipynb	7 months ago
imports.ipynb	7 months ago
musctf19-fstl.ipynb	6 months ago
musctf19-plaso.ipynb	7 months ago
picatrix.ipynb	7 months ago
szechuan-autoruns.ipynb	3 months ago
szechuan-kape.ipynb	3 months ago
szechuan-plaso-evtx.ipynb	16 days ago
szechuan-volatility.ipynb	3 months ago

ah2polivio-fls.ipynb

FUNCTIONS, VARS, INIT

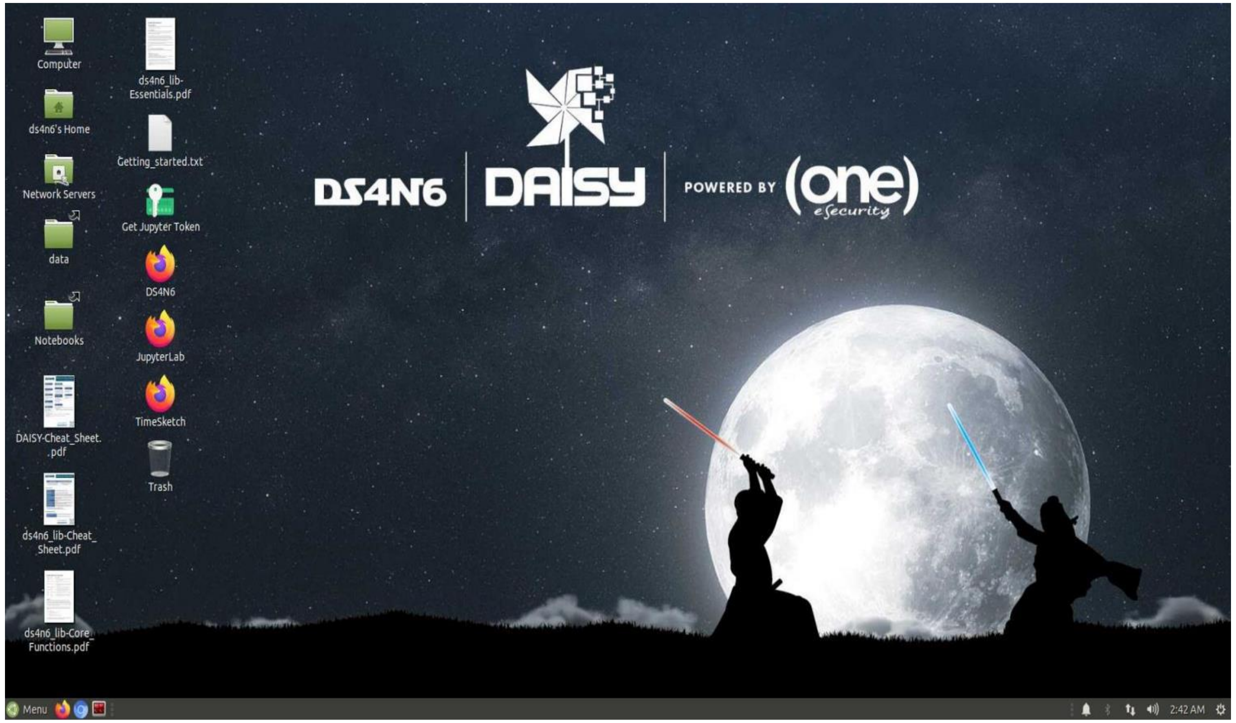
We create a variable we will use later: thisnb (name of the current notebook).

```
[1]: thisnb="./ah2polivio-fls.ipynb"
```

IMPORTS & INIT

We load all the needed libraries defined in the imports.ipynb notebook and deactivate the warnings in order to have a clean result.

```
[*]: %run imports.ipynb
```



(one) eSecurity SANS GIAC CERTIFICATIONS

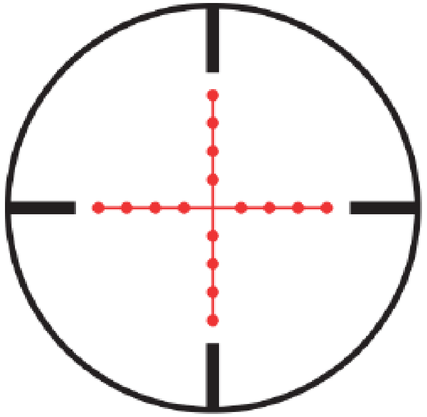
Demo: Real Incident Data – Ransomware Attack

Global Company

The attack could spread

CONTI

TOP Threat Actor from Russia using Cobalt Strike



Worldwide Scope

5k Servers + 350 DCs + 12k Laptops

Demo Data

+100 servers

+10K users

EVTX

+200K events

CONTI

Intrusion + **Ransomware** deployment

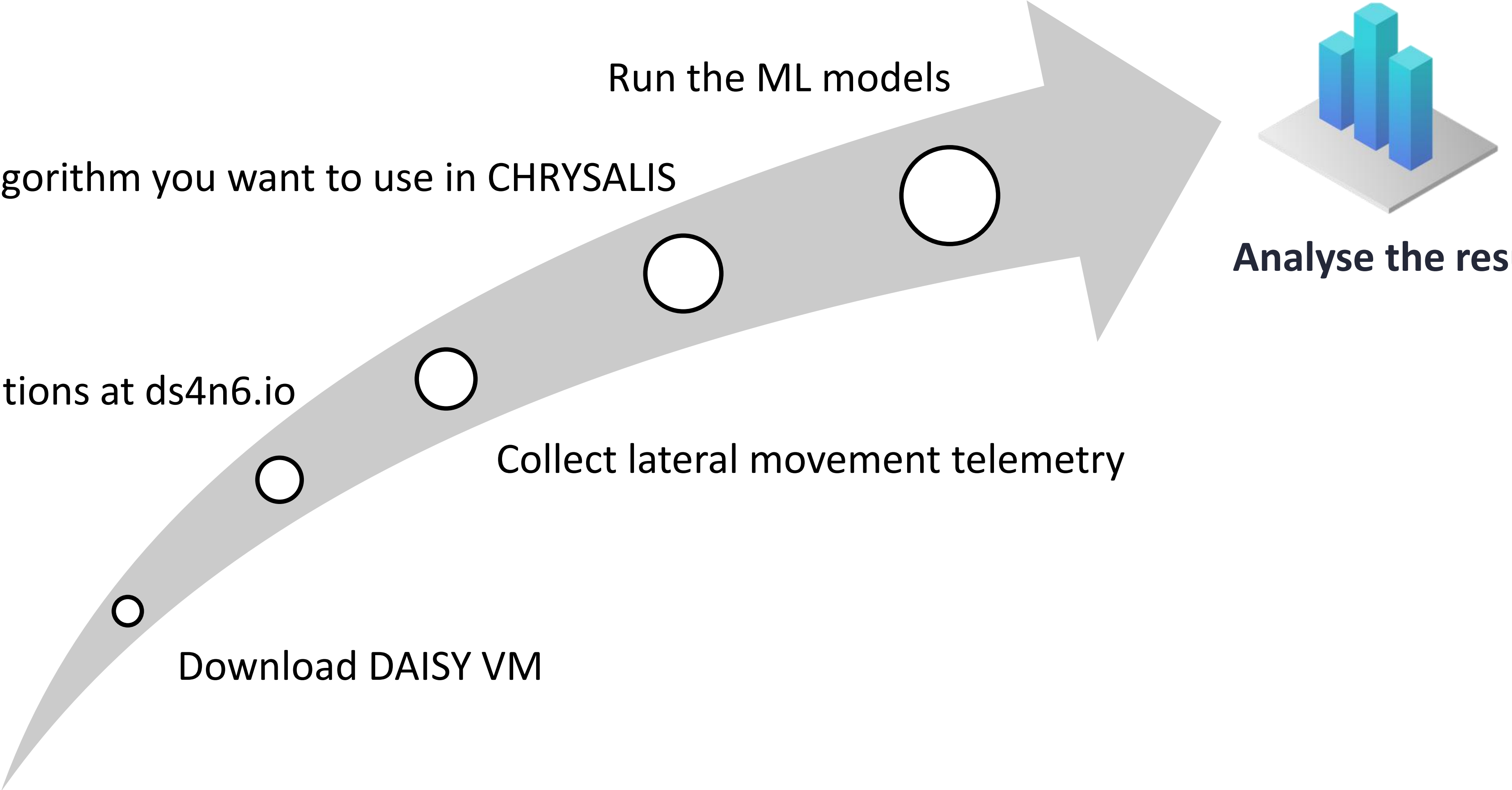
ML analysis performed with CHRYSALIS

DEMO
TIME
(one) eSecurity

Summary

- Graph analysis is a powerful tool to detect patterns of anomalous activity
- Machine Learning applied in Graphs automates the analysis and detection of anomalies
- There are not many open source tools using ML in DFIR
- DS4N6 is an open source project to bring the power of DS and ML to the community: CHRYSALIS, DAISY, etc.
- The presented analysis shows how CHRYSALIS has been effective tool in real world incidents with FORTUNE 500 customers

Apply



Download DAISY VM

Review DS/AI foundations at ds4n6.io

Collect lateral movement telemetry

Select the type of algorithm you want to use in CHRYSALIS

Run the ML models

Analyse the results

All the details about this talk:

ds4n6.io/rsac23

THANKS!!

DS4N6

ds4n6.io

@ds4n6_io

DS4N6

Jess Garcia

@j3ssgarcia

ONE/DS4N6 Research Team:

Mario Perez

Francisco Cortes - Beatriz Padilla

(one) eSecurity

one-esecurity.com

@One_eSecurity

one-esecurity

(one) eSecurity SANS GIAC CERTIFICATIONS