

# Online Training for Security Knowledge Graph to fight Cyber attacks

Chinmaya Mishra

Lead Data Scientist , Microsoft (Security & Compliance)

IIIT, Sricity (PhD. Scholar)

lasa global BIL-T 2021



This disclaimer **informs** readers that **the views, thoughts, and opinions expressed in this presentation belong solely to the author, and not necessarily to the author's employer, organization, committee or other group or individual.**



# Discussion Area

Online Training - ML

Knowledge Graph - Data

Cyber attacks - Domain

# AGENDA

---

Motivation

---

Recent Cyber Trends

---

Top 5 questions for Cyber defenders

---

Can Knowledge Graph help ?

---

Applications of KG

---

How to build Security KG for threat prediction ?

---

Define Ontology

---

Data Collection

---

Data Preprocessing For NER model

---

Data Featurization

---

NER Model Building & Validation

---

KG creation

---

KRL embedding for down streaming task

---

KRL Node prediction and validation

---

Challenges in Security KG

---

Online Training for Security KG

---



# MOTIVATION

## Security paradigm Shift

## Increase in Cyber Crime (US FBI)

- 35% increase in Cyber crime from 2014 to 2018 and it is still increasing
- Overall loss > \$2.7 billion

## Sophisticated Attack vector used by Adversaries

- File less execution
- Complex malware type i.e., Metamorphic and Polymorphic
- Signature based detection to behavior-based detection

## Rise of Cyber structured and unstructured data

## Growth of cyber-Knowledge over time

- Difficult to analyze
- No Knowledge Graph/ Knowledge database

## Rapid change in Tools and tactics

- Usage of new tactics across threat actor
- Cross usage of tools

# RECENT CYBER TRENDS

1000 + Blogs Per day

20000 + Words

100 + Cyber entities

Many more .....

## Sopra Steria Ransomware Attack

French IT service giant Sopra Steria was attacked by ransomware on the evening of 20th October, as confirmed by the company. Its fintech business, Sopra Banking Software, identified the virus which is a new version of the Ryuk ransomware and previously unknown to cyber security providers.

REvil ransomware attack against MSPs and its clients around the world | Sec...



[CREATED] 2 DAYS AGO by mohdrennis | Public | TLP: White

FileHash-MD5: 4 | FileHash-SHA1: 4 | FileHash-SHA256: 4

A look at Kaspersky's latest security solutions for businesses, following the discovery of the REvil ransomware gang, which is believed to be responsible for more than 1,000 attacks around the world. revil, reports, andariel, kaspersky, blog, great, global research and analysis team, analysis, security, malware statistics, virus statistics, spam, phishing, cybercrime, raas, ransomware, supply-chain...

## WildPressure APT Emerges With New Malware Targeting Windows and macOS



[CREATED] 18 HOURS AGO by dekaRituraj | Public | TLP: White

FileHash-MD5: 8 | FileHash-SHA1: 6 | FileHash-SHA256: 1 | IPv4: 5 | URL: 10 | Domain: 5 | Hostname: 3

A malicious campaign that has set its sights on industrial-related entities in the Middle East since 2019 has resurfaced with an upgraded malware toolkit to strike both Windows and macOS operating ... milum, vbscript, blackshadow, tandis, wildpressure, c++, kitten, andariel, kaspersky, blog, great, global research and analysis team, analysis, security, malware statistics, virus statistics, spam, ph...

January 20, 2021

## Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop

Microsoft 365 Defender Research Team

Microsoft Threat Intelligence Center (MSTIC)

Microsoft Cyber Defense Operations Center (CDOC)

## TA505 adds GoLang crypter for delivering miners and ServHelper



[CREATED] 4 HOURS AGO by mohdrennis | Public | TLP: White

FileHash-MD5: 2 | FileHash-SHA1: 2 | FileHash-SHA256: 4 | IPv4: 2 | URL: 11 | YARA: 2 | Domain: 37

In a series of blog posts, Jason Reaves and Joshua Platt look at how the GoLang crypter and PowerShell loaders are being used to deliver malware to Bitcoin and Eth users. servhelper, golang, systemroot, waitjob, stopjob, ta505, servicedll, timeout, eqtermervice, rdpwrap, jason, nsis, dropper, bitcoin, close, open

# Top 5 questions for Cyber Defenders

---

Can I keep a track of all adversaries ?

---

Can I observe the temporal behaviour of cyber attacks in nutshell ?

---

How can I predict the next attack by looking at all cyber entities ?

---

Risk posture of my organisation is covered ?

---

Who is behind my Organisation ?



# Can Knowledge Graph help ?

- *“KGs provide us a novel aspect to describe the real world, which stores structured relational facts of concrete entities and abstract concepts in the real world. KGs mainly contain two elements, i.e., entities that represent both concrete and abstract concepts, and relations that indicate relationships between entities ~ RDF (resource description framework)”*
- Ex: Beijing is the capital of China. In KGs, we will represent this fact with the triple form as (Beijing, is capital of, China).

(Knowledge Representation Learning: A Quantitative Review Yankai Lina , Xu Hana , Ruobing Xiea , Zhiyuan Liua,\* , Maosong Suna 2018)

<u>Company</u>	<u>KG application</u>
Microsoft	Bing search engine, LinkedIn data
Google	Search engine
Facebook	Networking
eBay	Product catalog





## Applications of KG:

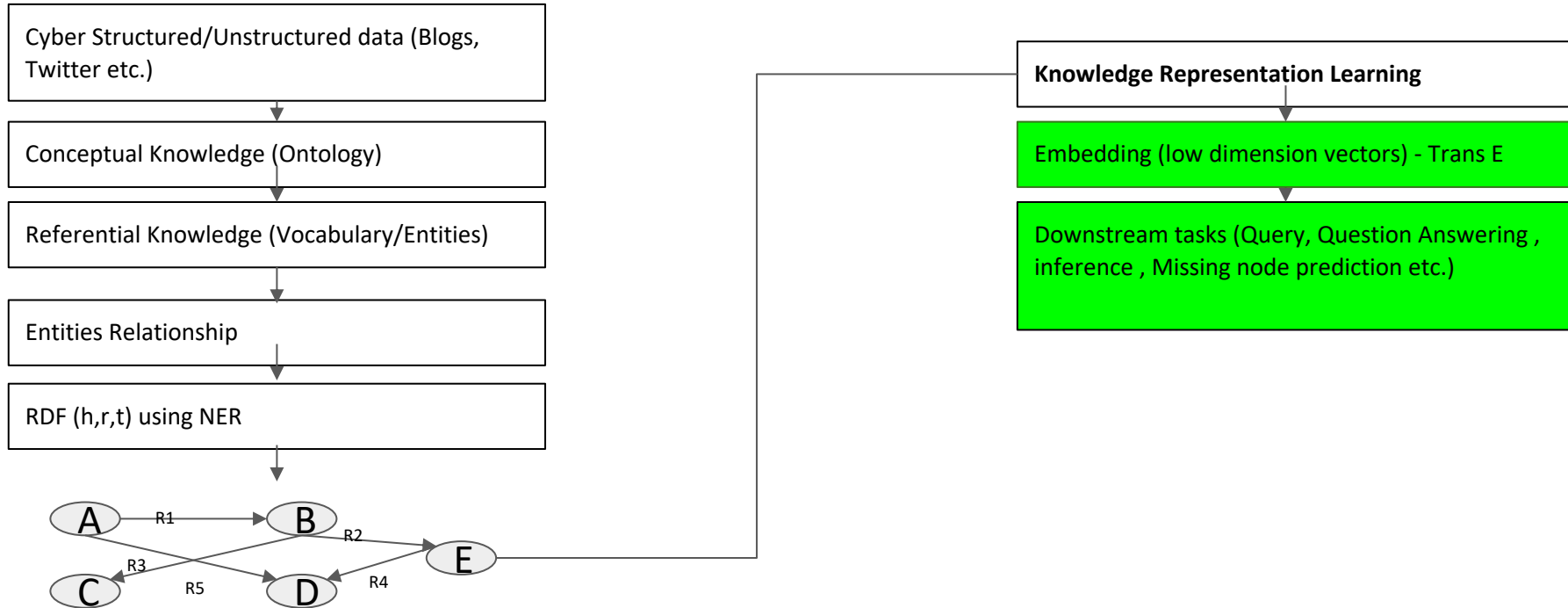
---

- Provide a shared substrate of knowledge within an organization, allowing different products and applications to use similar vocabulary and to reuse definitions and descriptions that others create
- provide a compact formal representation that developers can use to infer new facts and build up the knowledge
- word similarity computation [6]
- word sense disambiguation [7, 8]
- entity disambiguation [9]
- semantic parsing [10, 11]
- text classification [12, 13]
- topic indexing [14]
- document summarization [15]
- document ranking [16]
- information extraction [17, 18]
- question answering [19, 20]

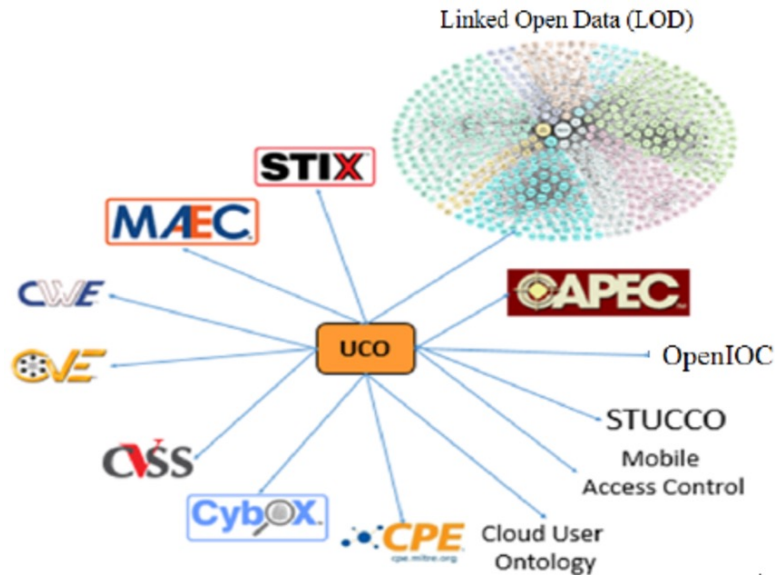


**Security Knowledge Graph is the Key ?**

# How to build Security KG for threat prediction



# Ontology



## Nodes:

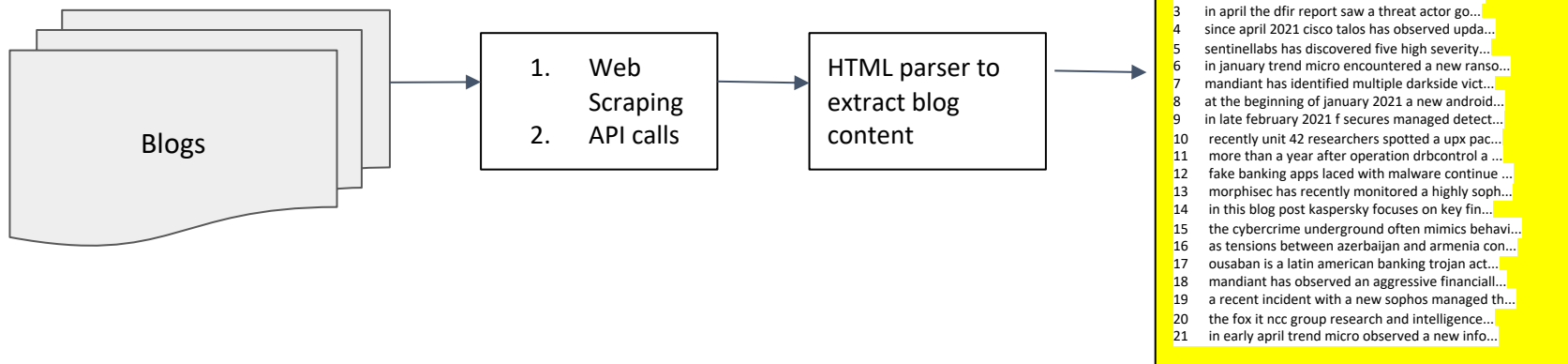
- **Software/Malware/Tool** : An entity that relates to a piece of code usually used as tool such as Office or Unix operating system. An entity that refers to malicious code and/or software which is inserted into a system.
- **OS** : An entity that defines the operating system.
- **Attack-pattern/Technique** : An entity that refers to steps that could result in an active attack on an individual or group of users.
- **Group/Actor** : An entity that refers to grouping of activities that could lead to a malicious attack

## Relationship :

- **uses** : Relationship where the subject entity belongs to a campaign or malware class and object entity belongs to a tool or software class, wherein subject entity aims to leverage object entity to carry on an attack. (Malware , Uses , OS) & (Actors , uses , Techniques)
- **attributed-to** : Relationship where the subject entity belongs to campaign or intrusion-set class and object entity belongs to threat actor class wherein subject entity is attributed to object entity. (Malware , attributed-to , Actor)

# DATA COLLECTION

OTX Pulse Blogs Via API



1. Alienvault otx pulse: (Dataset - 3286 , Major Columns : Adversaries , Malwares , Description about the blog, File and IP indicators and so on)

<https://otx.alienvault.com/>

\* Under permissible API



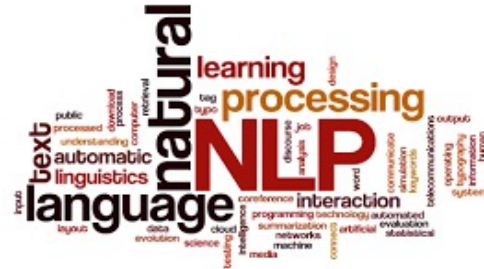
# Data Preprocessing for NER model

0 recently obtained technical evidence now allow...  
1 transparent tribe also known as apt36 and myth...  
2 internal alien labs research has identified ne...  
3 in april the dfir report saw a threat actor go...  
4 since april 2021 cisco talos has observed upda...  
5 sentinellabs has discovered five high severity...  
6 in january trend micro encountered a new ranso...  
7 mandiant has identified multiple darkside vict...  
8 at the beginning of january 2021 a new android...  
9 in late february 2021 f secures managed detect...  
10 recently unit 42 researchers spotted a upx pac...  
11 more than a year after operation drbcontrol a ...  
12 fake banking apps laced with malware continue ...  
13 morphisec has recently monitored a highly soph...  
14 in this blog post kaspersky focuses on key fin...  
15 the cybercrime underground often mimics behavi...  
16 as tensions between azerbaijan and armenia con...  
17 ousaban is a latin american banking trojan act...  
18 mandiant has observed an aggressive financial...  
19 a recent incident with a new sophos managed th...  
20 the fox it ncc group research and intelligence...  
21 in early april trend micro observed a new info...

## LEXICAL FEATURES

1. Remove punctuation
2. Removing multiple line breaks
3. Make all lowercase
4. Create phrases instead of tag words
5. Missing Value treatment
6. Lemmatization and stemming

0 recently obtained technical evidence now allow...  
1 transparent tribe also known as apt36 and myth...  
2 internal alien labs research has identified ne...  
3 in april the dfir report saw a threat actor go...  
4 since april 2021 cisco talos has observed upda...  
5 sentinellabs has discovered five high severity...  
6 in january trend micro encountered a new ranso...  
7 mandiant has identified multiple darkside vict...  
8 at the beginning of january 2021 a new android...  
9 in late february 2021 f secures managed detect...  
10 recently unit 42 researchers spotted a upx pac...  
11 more than a year after operation drbcontrol a ...  
12 fake banking apps laced with malware continue ...  
13 morphisec has recently monitored a highly soph...  
14 in this blog post kaspersky focuses on key fin...  
15 the cybercrime underground often mimics behavi...  
16 as tensions between azerbaijan and armenia con...  
17 ousaban is a latin american banking trojan act...  
18 mandiant has observed an aggressive financial...  
19 a recent incident with a new sophos managed th...  
20 the fox it ncc group research and intelligence...  
21 in early april trend micro observed a new info...



# DATA FEATURIZATION 1

## Syntactic Features

1. POS Tagging
2. Orthographic Features (ismixcaps, ispunction, isothersymbol, isAlpunct and contains apt)

## Semantic Features

1. W2Vec embedding trained on cyber corpus (Size - 50)

X array

```
[158]: {'word': 'technical',
       'lemma': 'technic',
       'pos': 'Adj',
       'orthotag': 'LOWERCASE',
       'wordtype': 'WORD',
       'pword': 'obtained',
       'plemma': 'obtain',
       'ppos': 'Verb',
       'porthotag': 'LOWERCASE',
       'pwordtype': 'WORD',
       'nword': 'evidence',
       'nlemma': 'evid',
       'npos': 'Noun',
       'northotag': 'LOWERCASE',
       'nwordtype': 'WORD',
       'em0': 0.38242462,
       'em1': -1.8959522,
       'em2': -0.81171393,
       'em3': -2.1022105,
       'em4': 2.8834286,
       'em5': 3.3092175,
       'em6': -1.9517027,
       'em7': -0.045751214,
       'em8': 0.5125661,
       'em9': -0.87238455,
       'em10': -0.4837797,
       'em11': -3.820923,
       'em12': -2.4346275,
       'em13': 0.5136932,
       'em14': -2.0492282,
       'em15': 0.9053825,
       'em16': -2.6824055,
       'em17': 2.8443503,
       'em18': -1.201635,
       'em19': 1.124606,
       'em20': -2.1868472,
       'em21': 1.5428668,
       'em22': 5.9842634,
       'em23': -2.106654,
       'em24': 1.3416728,
       'em25': -2.7744014,
       'em26': -2.0945942}
```

**MITRE** | **ATT&CK™**

0 recently obtained technical evidence now allow  
1 transparent tribz also known as apt36 and myth  
2 internal alien labs research has identified ne  
3 in april the dir report said the threat actor  
4 since april 2021 cisco talos has observed u  
5 sentinellabs has discovered five high severity  
6 in january trend micro encountered a new ransom  
7 mandiant has identified multiple darkside vici  
8 at the beginning of january 2021 a new android  
9 in late february 2021 f secures managed detec  
10 recently unit 42 researchers spotted a uxp pac  
11 more than a year after operation dbcontrol a  
12 fake banking apps laced with malware continue  
13 morphic has recently monitored a highly sp  
14 in this blog post kaspersky focuses on key be  
15 the cybercrime underground often mimics fin  
16 as tensions between azerbaijan and armenia con  
17 ousban is a latin american banking trojan co  
18 mandiant has observed an aggressive frame  
19 a recent incident with a new sophos managed th  
20 the fox it ncc group research and intelligence  
21 in early april trend micro observed a new info...

MITRE list of **Actor**,  
**Malware**, **Technique**

Operating System (**OS**)  
list

1. Attackcti python API
2. Tag **BIO** for each document

Goblin Panda APT is the  
B | | O O

**Y array**

```
[161]: ['0',  
        '0',  
        '0',  
        '0',  
        '0',  
        '0',  
        '0',  
        '0',  
        '0',  
        '0',  
        '0',  
        '0',  
        '0',  
        '0',  
        '0',  
        '0',  
        '0',  
        '0',  
        '0',  
        'B-TECHNIQUE',  
        '0',  
        '0']
```

# Rules

```
if x=='Malware' and y=='os':  
    relation='uses'  
elif x=='BActor' and y=='Technique':  
    relation='uses'
```

```
if x=='Malware' and y=='os':
    relation='uses'
elif x=='BActor' and y=='Technique':
    relation='uses'
```

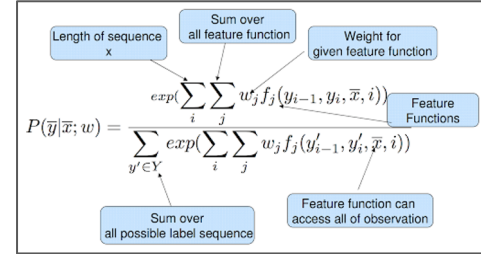
# MODEL BUILDING & VALIDATION

1. Conditions Random Field with hyper parameter tuning
2. Saving model object in 'pkl' format

## CRF Model output

```
Fitting 3 folds for each of 3 candidates, totalling 9 fits
[Parallel(n_jobs=1)]: Using backend SequentialBackend with 1 concurrent workers.
[Parallel(n_jobs=1)]: Done 9 out of 9 | elapsed: 3.5min finished
best params: {'c1': 0.4236969007987103, 'c2': 0.0012612104343276205}
best CV score: 0.9944841688620059
model size: 0.19M
Predict the test set
[[965  0  0  0  1  0  0]
 [  0 264  0  0  0  0  0]
 [  0  0 194  0  0  0  0]
 [  0  0  0 130  0  0  0]
 [  0  0  0  0  45  0  0]
 [  0  0  0  0  0  28  0]
 [  0  0  0  0  0  0 21]]
```

- Model performed really well with an overall CV score of 99%.



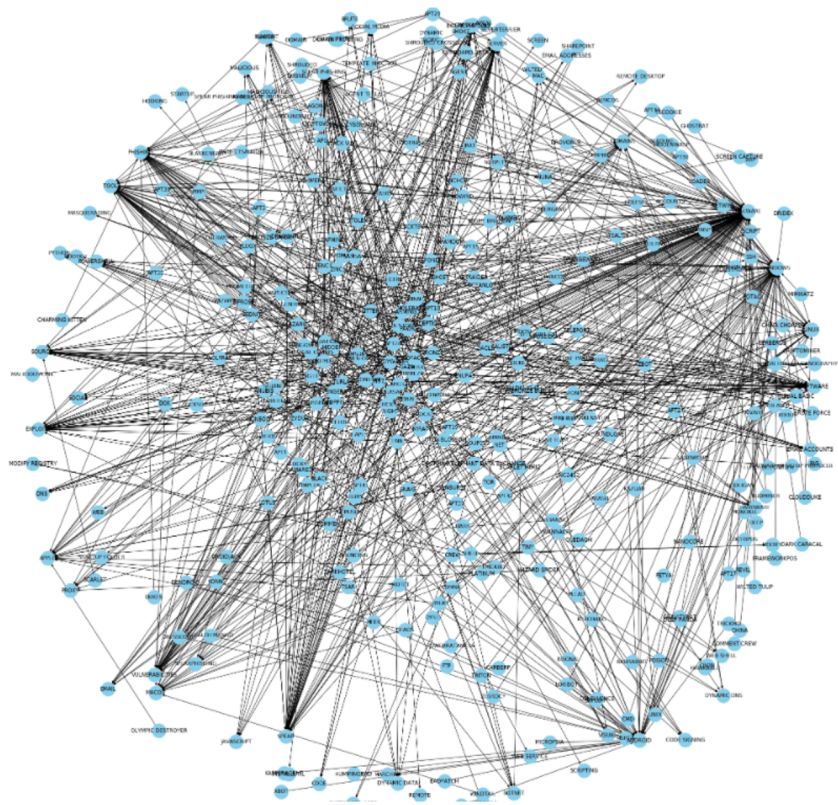
## 2.5 NER model Validation

```
# class-wise scores on validation data
sorted_labels = sorted(
    labels,
    key=lambda name: (name[1:], name[0])
)
met=metrics.flat_classification_report(test['YArray'], y_pred, labels=sorted_labels, digits=3)
print(met)
```

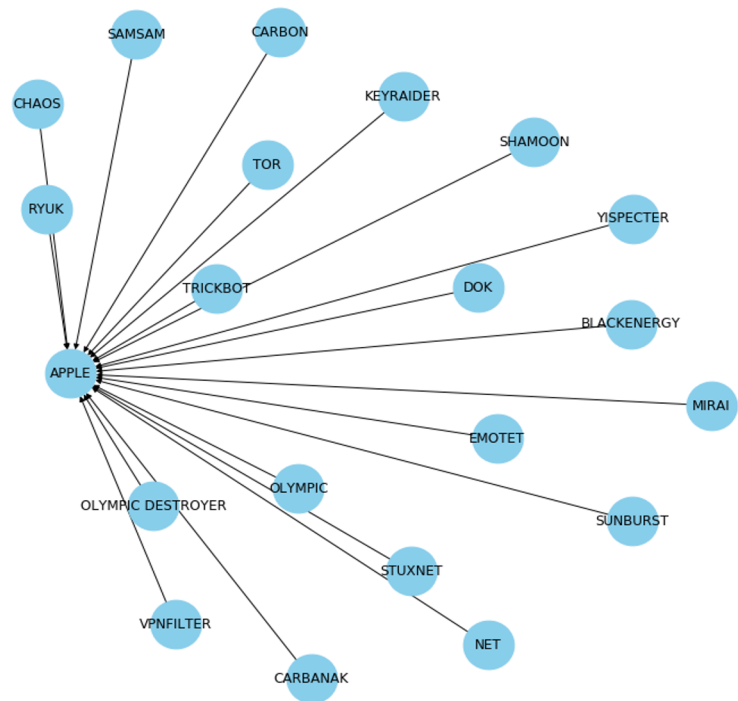
	precision	recall	f1-score	support
B-BADACTOR	1.000	0.870	0.930	223
I-BADACTOR	1.000	0.757	0.862	37
B-MALWARE	1.000	0.802	0.890	329
I-MALWARE	1.000	0.840	0.913	25
B-OS	1.000	1.000	1.000	130
B-TECHNIQUE	0.999	0.983	0.991	982
I-TECHNIQUE	0.957	0.726	0.826	62
micro avg	0.998	0.921	0.958	1788
macro avg	0.994	0.854	0.916	1788
weighted avg	0.998	0.921	0.956	1788



# SECURITY KG



## Tail - APPLE (Malware , Uses , OS)



# KRL EMBEDDING FOR DOWN STREAMING TASK

KRL (Knowledge Representation Learning) usually wants to encode the semantic meaning of entities and relations with their corresponding low-dimensional vectors.

KRL models - Linear Models (Structural embedding -> Semantic matching energy -> Latent factor model -> Distmult -> Analogy -> Neural Model -> Translation Model  $C(\text{king}) - C(\text{queen}) \approx C(\text{man}) - C(\text{woman})$ , --> Holographic Models -> Complex Embedding (Eigen vector)

Examples:

**TransH**

**TransR/CTransR**

**TransD**

**Transparse**

**TransA**

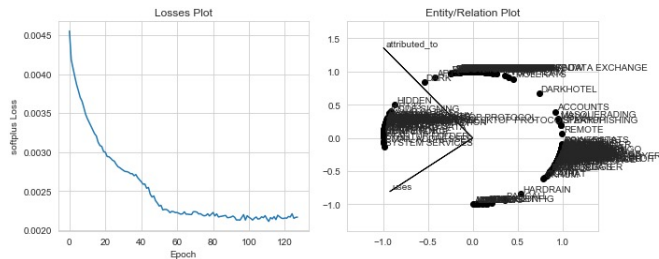
**TransG**

**KG2E**

**TransE**

# KRL EMBEDDING USING TRANS E

- Trans E Algo with hyperparameter tuning
- Loss function – Softplus
- Model performed well with loss gradually decreasing and converging



**TransE** is an energy-based model that produces knowledge base embeddings. It models relationships by interpreting them as translations operating on the low-dimensional embeddings of the entities. Relationships are represented as translations in the embedding space: if  $(h, l, t)$  holds, the embedding of the tail entity  $t$  should be close to the embedding of the head entity  $h$  plus some vector that depends on the relationship  $l$ .

# KRL NODE PREDICTION (Test set)

- Tail Prediction:  
(NANOCORE, uses, ?)

- Relationship Prediction:  
(NANOCORE, ?, WINDOWS)

- Head Prediction:  
(?, uses, WINDOWS)

- Node prediction is 100% correct with high probability nodes are in the higher rank

```
#model inferencing for Link prediction (Train/Test)
model = results.model
# Predict tails
predicted_tails_df = model.get_tail_prediction_df('NANOCORE', 'uses')
print("\nPredict tail\n", predicted_tails_df[predicted_tails_df.in_training==True])
# Predict relations
predicted_relations_df = model.get_relation_prediction_df('NANOCORE', 'WINDOWS')
print("\npredict relation\n", predicted_relations_df[predicted_relations_df.in_training==True])
# Predict heads
predicted_heads_df = model.get_head_prediction_df('uses', 'WINDOWS')
print("\npredict head\n", predicted_heads_df[predicted_heads_df.in_training==True])
```

Predict tail

tail_id	tail_label	score	in_training
338	WINDOWS	-0.09724	True

WARNING:pykeen.models.base:Calculations will fall back to using the score\_hrt method, since this is necessary.

predict relation

relation_id	relation_label	score	in_training
1	uses	-0.09724	True

predict head

head_id	head_label	score	in_training
195	MIMIKATZ	-0.029884	True
54	CHAOS	-0.031167	True
52	CARBON	-0.035084	True
177	LOKIBOT	-0.039147	True
316	TOR	-0.039876	True
269	RYUK	-0.039949	True
198	MIRAI	-0.040036	True
220	OCTOPUS	-0.047773	True
265	RIG	-0.048133	True
33	BISONAL	-0.050959	True
120	EMPIRE	-0.051496	True
66	COMNIE	-0.050946	True
306	STUXNET	-0.060866	True
169	KOMPLEX	-0.060959	True
134	FTP	-0.062889	True
51	CARBERP	-0.063199	True
74	CRYPTOMINER	-0.063564	True
102	DUALTOY	-0.064205	True
230	PETYA	-0.066768	True
321	TSCOOKIE	-0.071656	True
317	TRICKBOT	-0.077464	True
346	XBASH	-0.086364	True
262	RESPONDER	-0.093707	True
150	TRINITYSERVER	-0.094976	True



# KRL NODE PREDICTION (unseen set)

- Tail Prediction:  
(ELDERWOOD,uses, ?)
- Relationship Prediction:  
(ELDERWOOD,?,EXPLOITS)
- Head Prediction:  
(?, uses,EXPLOITS)

- Node prediction is not correct and needs improvement.

```
Predict tail
      tail_id tail_label      score in_training
186      186    MALWARE -0.306212         True
WARNING:pykeen.models.base:Calculations will fall back to
essary.
predict relation
Empty DataFrame
Columns: [relation_id, relation_label, score, in_training]
Index: []

predict head
      head_id      head_label      score in_training
62          62          COBALT -0.013204         True
289         289          SOFACY -0.015743         True
172         172    LEAFMINER -0.018116         True
322         322          TURLA -0.018433         True
129         129          FIN7  -0.020163         True
98          98    DROPPING  -0.041235         True
218         218    OCEANLOTUS -0.044938         True
171         171    LAZARUS  -0.052478         True
248         248    QUASAR  -0.058865         True
266         266    ROCKE  -0.071136         True
202         202    MONSOON  -0.072003         True
254         254    REAPER  -0.074957         True
99          99  DROPPING ELEPHANT -0.079163         True
157         157    INCEPTION -0.084219         True
34          34        BLACK  -0.163121         True
```

Can Online training solve the dynamic changing KG ?

## CHALLENGES IN SECURITY KG & KRL

- data sparsity and growing computational inefficiency
- Complex Relation Modeling -1-to-n, n- to-1 and n-to-n relations
- **Low Quality of KGs ~ conflict of error**
- **Large Volume of KGs**
- **Endless Changing of KGs**
- Entity disambiguation and managing identity
- Knowledge extraction from multiple structured and unstructured sources
- Managing operations at scale
- Knowledge inference and verification
- **Federation of global, domain-specific, and customer-specific knowledge**
- Security and privacy for personalized, on-device knowledge graphs



\* Sources are given in Reference section

The background of the slide features a complex, abstract design. It consists of numerous concentric circles and rings, some of which are filled with various digital patterns, including binary code (0s and 1s) and pixelated textures. The color palette is primarily dark blue and black, with highlights of light blue and white. The overall effect is a sense of depth and technological sophistication.

















## Online Training for KRL ?

---

*“In computer science, **online machine learning** is a method of machine **learning** in which data becomes available in a sequential order and is used to update the best predictor for future data at each step, as opposed to batch **learning** techniques which generate the best predictor by **learning** on the entire **training** data set.”*

[https://en.wikipedia.org/wiki/Online\\_machine\\_learning](https://en.wikipedia.org/wiki/Online_machine_learning)

# REFERENCES

Title	Creator	Year	Publisher	Publication
>  Extracting Cybersecurity Related Linked Data from Text	Joshi et al.	2013		2013 IEEE Seventh Inte...
>  Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies	Burger et al.	2014	ACM Press	Proceedings of the 20...
>  Developing an Ontology for Cyber Security Knowledge Graphs	Iannacone et al.	2015		
>  Towards a Knowledge Graph for Science	Auer et al.	2018	ACM	Proceedings of the 8th...
>  Knowledge Representation Learning: A Quantitative Review	Lin et al.	2018		arXiv:1812.10901 [cs]
>  A Practical Approach to Constructing a Knowledge Graph for Cybersecurity	Qi et al.	2018		Engineering
>  Open Research Knowledge Graph: Next Generation Infrastructure for Semantic Scholarly Knowledge	Jaradeh et al.	2019	ACM	Proceedings of the 10t...
>  RelExt: Relation Extraction using Deep Learning approaches for Cybersecurity Knowledge Graph Improvement	Pingle et al.	2019		arXiv:1905.02497 [cs]
>  Knowledge graph exploration: where are we and where are we going?	Lissandrini et al.	2020		ACM SIGWEB Newslet...
>  Knowledge Graphs	Hogan et al.	2021		arXiv:2003.02320 [cs]
>  A Survey on Knowledge Graphs: Representation, Acquisition and Applications	Ji et al.	2021		arXiv:2002.00388 [cs]
>  Machine Knowledge: Creation and Curation of Comprehensive Knowledge Bases	Weikum et al.	2021		arXiv:2009.11564 [cs]
>  A System for Automated Open-Source Threat Intelligence Gathering and Management	Gao et al.			
>  Developing an Ontology of the Cyber Security Domain	Obrst et al.			
>  Industry-Scale Knowledge Graphs: Lessons and Challenges	Taylor			
 1074100.pdf				

THANK YOU

