ALIBABA SECURITY

Solving The Last Mile Problem Between Machine Learning and Security Operations Xiangyu Liu, Xinyue Shen





Whoami





- Xiangyu Liu
 - Senior Algorithm Engineer @Alibaba Security
 - CUHK PhD (2016)
 - Academic: IEEE S&P, ACM CCS
 - Industry: DEF CON, Black Hat Asia
 - Interests: Machine Learning, Cybersecurity
- Xinyue Shen
 - Algorithm Engineer Intern @Alibaba Security
 - Interests: Cybersecurity, NLP, Knowledge Graph
- Special Thanks
 - Tao Zhou, Quan Lu, Security Operation Team @Alibaba Security



What is Security Operations?

A security operations center (SOC) is a centralized unit that deals with security issues on an organizational and technical level.

--WikiPedia



What is Security Operations ?

What others think I do



Money \$100 Goal \$3620 II •)

What I think I do

What I really do



.......



Why not introduce **Machine Learning** in **SOC**?



Challenges

Partially Observable

Hard to collect all security-related data

	ncertainty
U	noortanity

Depend on attackers and environment

Correlation

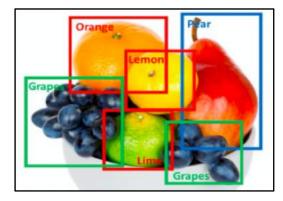
Current decisions affect subsequent

Strong Interpretability

Security needs strong interpretability









Challenges

Partially Observable

Hard to collect all security-related data

	ncertaint	٦V
$\mathbf{\overline{\mathbf{v}}}$		·y

Depend on attackers and environment

Correlation

Current decisions affect subsequent

Strong Interpretability

Security needs strong interpretability

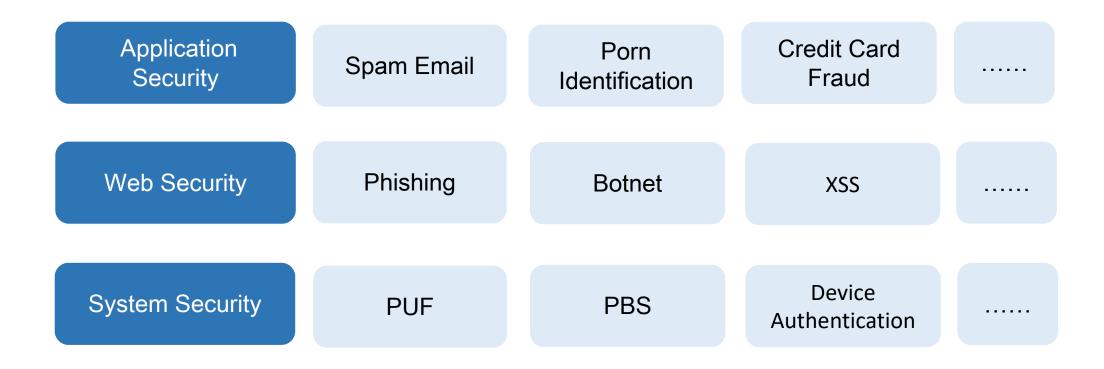






What ML can do in Security

• Data + Close Domain+ Quantitative Expert Experience



Application of Machine Learning in Cyberspace Security Research. Lei Zhang, Yong Cui, Jing Liu, Yong Jiang, Jianping Wu. Chinese Journal of Computers, 2017.



Is there anything wrong when they meet SOC?







"The Accuracy Rate of Our Model is 99.9%!" "Sounds good. But our data scale is enormous. Over 100 million every day."

"So, even the accuracy is high, your model will still produce 100000 alerts every day...."

"Well How many alerts can you handle?"

"only 100 alerts per day!"





Produce **100000** alerts per day



Handle 100 alerts per day

"And this is only one model."





Produce **100000** alerts per day



Handle 100 alerts per day

"How many attack types we may meet in reality?"





			AT	TBCK Matri	x for Én	erprise				
-			-	Briese Tradie	E	-	-	-	-	interest and interest into the local distance of the local distanc
Oracia Disportan	-	lash, processo Sarlar	no bak Tukun	Access States Margarithme	Anneal Technicise	Annual Passant	Service.	Autor Datase	Animated Sufficiency	and the
		Accession in the second	Annes Annes Annes Annes Annes	811.1m	-	-	lamon lamon lamon	Annual	ina Second	Transfer of the local division of the local
Webser ombros	increasing a sector	accord Names	Approved The lay	-	-	trane Tables	Sergiar Pergeset Real Mod	represent them	-	Terretal Terretal Terretal Terretal Terretal Terretal
Tradition Tradition Tradition	Compare within Ma	-		Name on Arrive	Consta Scotta	the per Manager Manager	Addal Experiment of National Sections	-	Tanta Tanta ka	Dates Designing
State Association Association	Second Second	earer Rise	And the second	-	Antonio e A		im.			turn Derekter Dete Natur Natur Dete Typopie Dete
Texperiores 144	Anenejata Istorg	-	Spectra Second	The local division	-	Street.	Pare Pro	doporteur COM Remen Manual Manual Manual Manual Manual	Seture Det	tan Ine-ing
								-	and Germal	-
-minuted	Receipted.	Perkeya	tion of the second seco	Ten fart 6	Ramme Artest Artes	the state	Page Page Table	Summer's Street	Lotan Dellar Dellar Male	fan Minneller
Sang Proving distances Sangage Com- transport that	lanat Bargalatan Tat	atlate	111 41	Symphec Mult. The	freed interested	Terretal Status Decemp	H		Andrew Color Reduct	No Sinata Integ Integ Integ Done Done
7.44 Automatic	Laketer-tr Statistics	holt		Composed.		Support Support Support	Name of Street		Torontal Land	tataak Haaraa
Anne .	ingend time	Press. Sciences		Service of Sales Scale (Sales)	Test Carton	Terrar Ornet Shirter	Name Josephere	Caston		Mittitude Discrete
	indut :	Ellerge Miller File-Annesigner		Daniel Parel Mary	Ingel Printer		National Sec. Concept Second Ma	March (Fr Strength		
	1000 1000	Company of					-	Street.		NAMES OF
		Kanggonat Periodes Konggonat Stead kangi Reading	Traja Par Galacter Galacter Galacter	No. Income lines Highering	-	Annes April 10	1	una Sancer		Margane Despilat
	und ett.	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	(Annual Content	**.10.000	Constructs No receiving	Anne Anne Anne Anne Anne Anne Anne Anne	Internet in the second			Additional for the second seco
1	-	Ris. Second Contex Reporting	netwoor.	Section 2010	antes antes	Same	(Marrison) Schwart			terration of the local division of the local
	Person	ta hereisete Herity	19.300	(Institution) Tests	Salash Bolta Salashi Salashi		Annes Maria			Amount for Total
	-	Name of Street, or	-	Supreme to average (second	-					Name of Street, or other street, or othe
	Report.	Inter Standard Franklingson Ministerio Franklingson Franklingson Franklingson	N 1	Table Birghter Ministry Spinister	Sector Manage Include Automotion Automotion					Second Patianets
	(14440)	Inclusion in the state	=	the barrow	Inclusion Andrewson	Same				Income State
-	-	-	-	De Personne		Dataset Sature (see				Liger Property
	-	-	Conception 1	mana anna an a						Station of Lot o
	Anna Benden Agen (Bene) Agen (Bene) Agen (Bene) Anna Agen (Bene) Anna Agen (Bene) Agen Agen Agen Agen Agen Agen Agen Agen	Anna in Anna in Anna interne Anna interne Anna interne Anna interne Anna interne Anna interne Anna interne		De Geregens Regiones Para ante espise Oficial						
	Squ(Bury	Auris Matter	Table 1 and	-						
	Appendix and	10.000.010		Street of Concession, Name						
_	(marine	12100	Auto Techniqu	The second diverse						
	Secondar.			tion finite						
	1 Annual V	Appendiane and		Strengt for Descent of Spinster, Spi						
		Laurenter oger	that (feat)	ARTINENE Anna Anna Anna						
_	and a second	analary .		Pade Tana						
-	the land	transmission in the second		Naga Arman Sa San Canad Daylor						
_	Name And States States and States			Salation						
_	Phone the set	Maria Second		Cardinas						
-	The second	fore room 111		-						
		Mungelumini 2004								
		Part - market								
				many						
		Personal Victoria		Street liter						
-		An and the		Construction Process						
				-						
		Realises for two -		Performing						
		Handonman Harmony Harmony Landson Harmony Harm		Here Harris Here						
		Residences		Termination of						
		Rearing Sugar		-						
				-						
		Robert and Balant		14-2						
		Balant Balanta		Nara Maria						
		The system		Roatti D'and Train Provider Typelley,						
		Tre Paulies								
		-		Appendition (Proc.) Appendition (Proc.)						
		And the second		Super-Linguistics Encourse						
		Normal Normal Normal Normalise		San Performance						
		Lineson .		-						
		10								
				front second second						

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public- Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command	Data Encoding

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

——MITRE



.....

......



Produce **100000** alerts per day



Handle 100 alerts per day

"So actually the number of alerts is 100000 × 300 + per day..."









Can we bridge the gap and solve this awkward thing?





- Behavior analysis
- Feature based sorting
- Ensemble risks
- Knowledge graph
- White list
- ...



Best Practices: Large-Scale Data



Porn Identification

- Labeling is easy
- Labeling is relatively cheap
- Lots of samples



Intrusion detection

- Depend on experience and time consuming
- Security experts are expensive
- Few samples

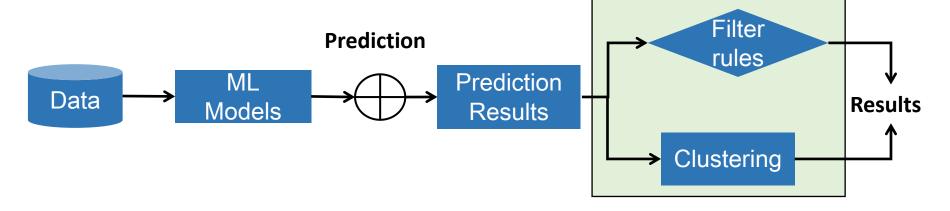




Best Practices: Behavior Analysis

- A cyber-security problem can be taken as consisting of several subproblems
 - Machine learning can be applied in some part
 - The malicious behaviors can be distinguished by rules or can be clustered
- Our Approach



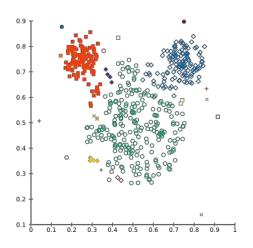




Best Practices: Behavior Analysis

- Example
 - Domain generating algorithm (DGA) detection
 - A DGA is a program that provides malware with new domains
 - Mistakes: Using ML to detect DGAs directly
- Approach
 - ML is used to detect the randomness of domains
 - LSTM, Ngram, and etc.
 - Filter rules
 - IP relationship, number of requests, number of subdomains, and etc.
 - Clustering
 - The features described above, and/or embedding techniques

earnestnessbiophysicalohax.com kwtoestnessbiophysicalohax.com rvcxestnessbiophysicalohax.com hjbtestnessbiophysicalohax.com txmoestnessbiophysicalohax.com dbzwestnessbiophysicalohax.com sgjxestnessbiophysicalohax.com

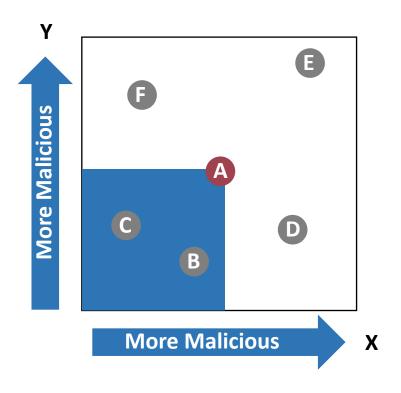


.



Best Practices: Feature Based Sorting

- Focus on precision
- Feature extraction
 - Assume we have only two features: X and Y
- Scoring:
 - if *A* is more malicious than *B* in every dimension, Increment *A*'s score by one
 - Can be customized
- Sorting:
 - Let N denote all the elements, K as the budget of SOC
 - Sort *N* by each element's score, and select top K elements



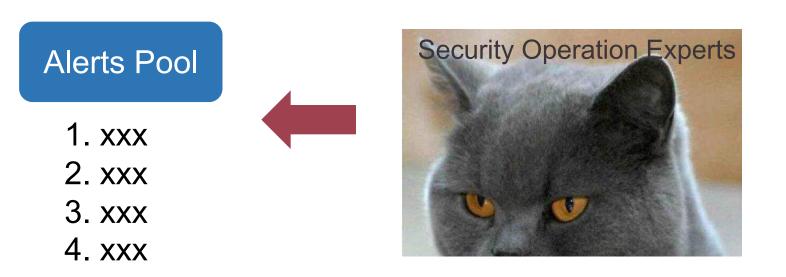


Best Practices: Feature Based Sorting

- Compare with historical data
 - Extract features per day/hour/...
 - Sort the data in a longer time window, e.g. one week
- Application
 - Phishing detection, Usenix Security'17
 - UEBA
 - ...
- Limitations
 - At the expense of recall
 - What features to extract is very hard to determine

Ho, G., Javed, A. S. M., Paxson, V., & Wagner, D. (2017). Detecting Credential Spearphishing Attacks in Enterprise Settings. USENIX Security'17







.

.......

.....

......

.......

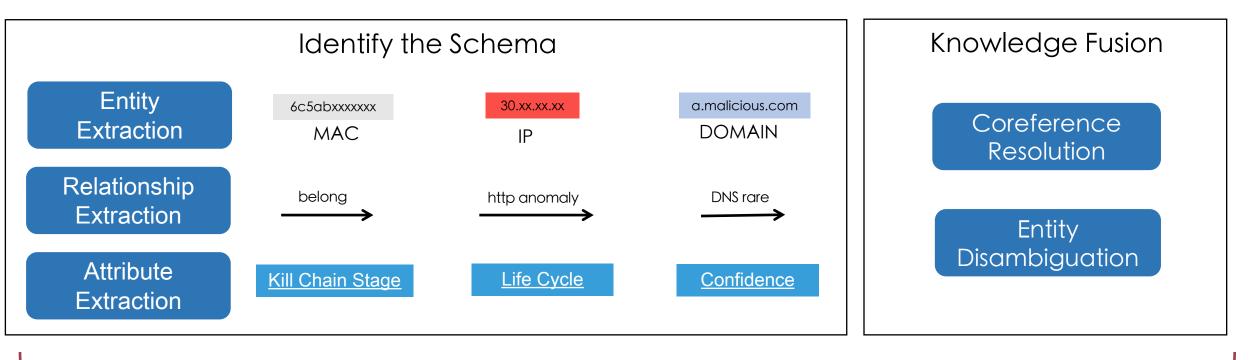
Traditional Way: DNS Rare 5 HTTP Rare 3 malicious.com Phishing 8 Sum 16 Problems behind it:

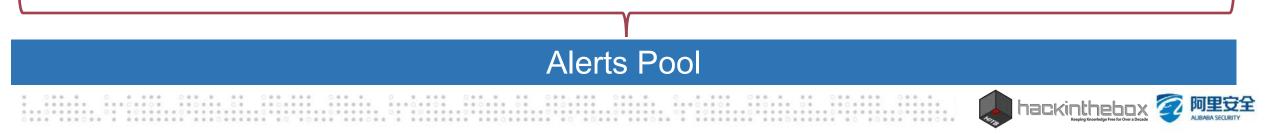
- 1. Not all related alerts can be produced.
- 2. Lateral movement is common.



Best Practices: Knowledge Graph

Alerts Pool Construction





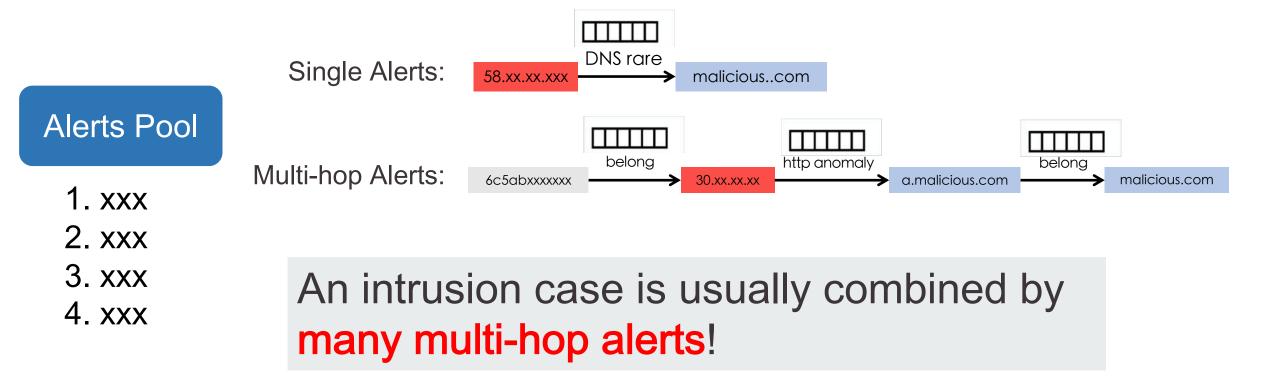
Some attributes

- Kill chain stage
- Life cycle

.

Confidence

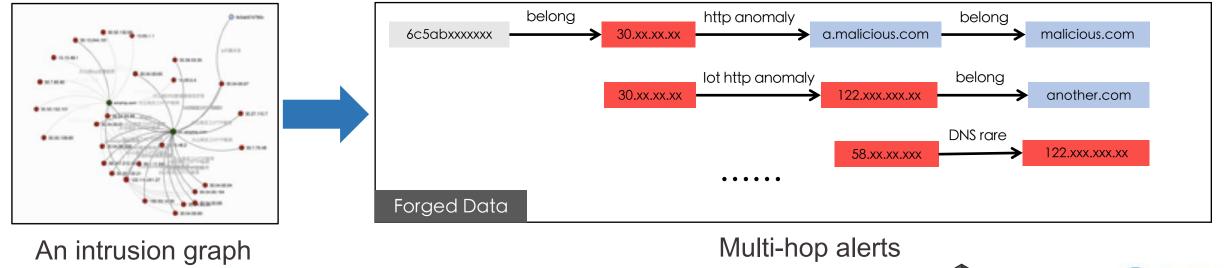
After identify the Schema, every alert is a Triple(entity-relationship-entity).





An intrusion case is usually combined by many multi-hop alerts!

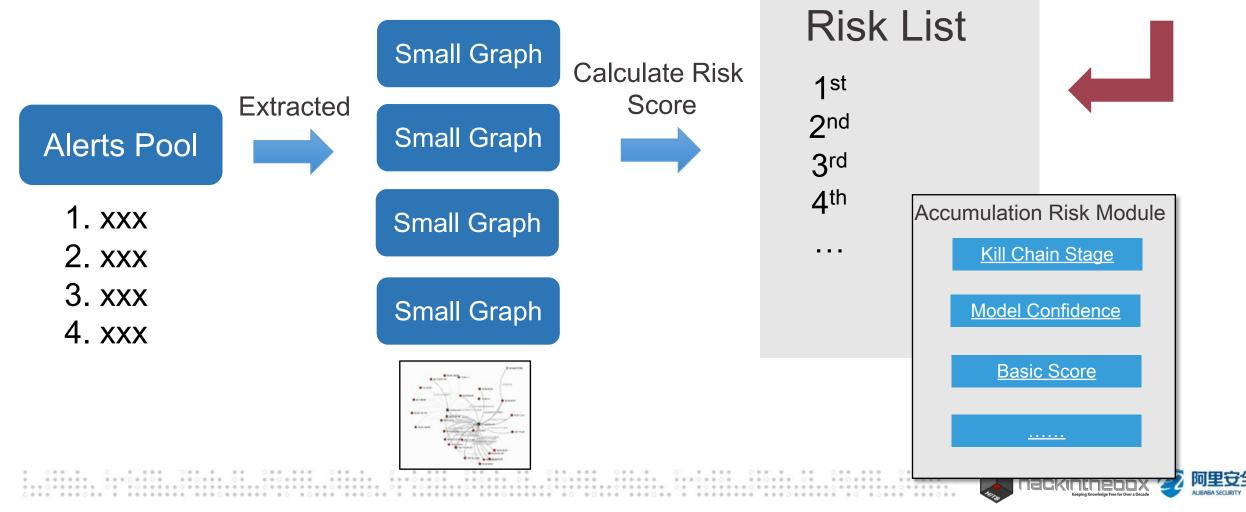
Eg.



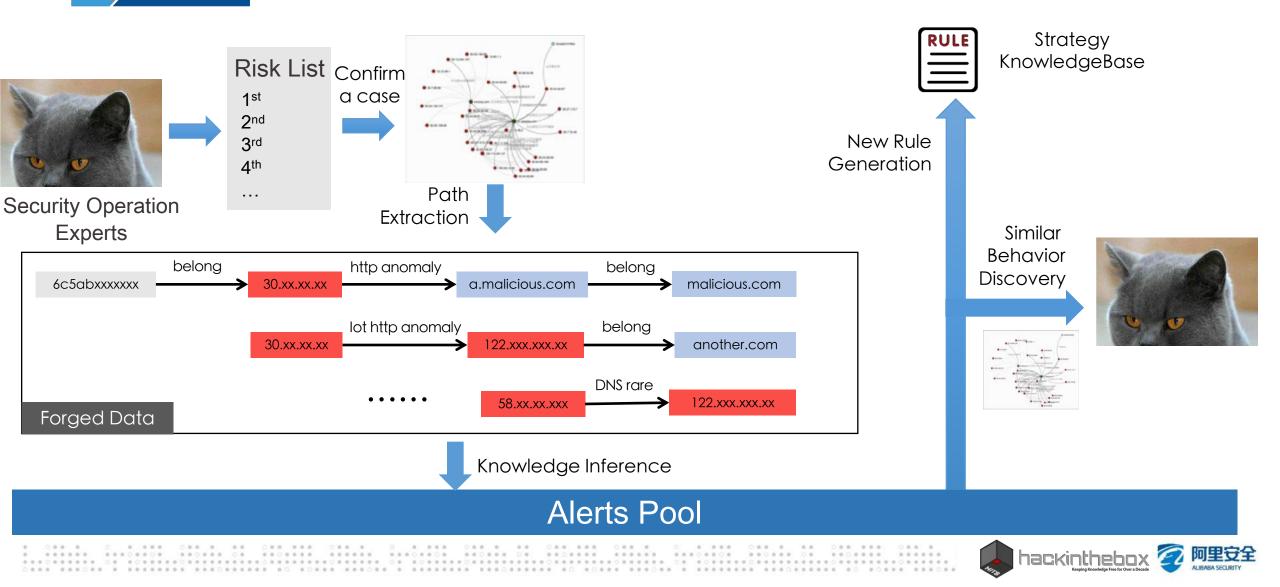


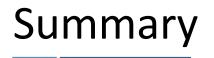


Security Operation Experts



Best Practices: Knowledge Graph





- An in-depth analysis on state-of-the-art security operations and machine learning techniques, reveals the gap between them.
- Several strategies are proposed to solve the last mile problem.
- As showcases, we demonstrate how to implement these approaches in practice.



THANKS

