#### **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



#### What I think I do

#### Money \$100 Goal \$3620 Exit Level: 47 II (\*)

#### What I really do



..... ...... ...... ..... ..... ..... . . . . . ....... ...... . . . . . . ...... ....... ...... . . . . . . . .



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

0000 000 000 0.... . . . . 000 000 . . . . . . 0.0.0 0.0.0 0.0.0.0 0 0 0 0.000 0.000 0 0.00000 0.00000000 ............ .....



# Challenges

Partially Observable

Hard to collect all security-related data

U	Incertainty
	in containing

Depend on attackers and environment

#### Correlation

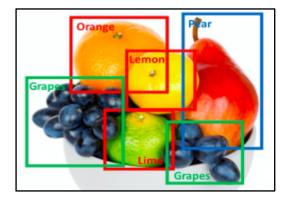
Current decisions affect subsequent

#### Strong Interpretability

Security needs strong interpretability









# Challenges

Partially Observable

Hard to collect all security-related data

	1	•
	Incerta	Intv
$\mathbf{\overline{\mathbf{v}}}$		·····y

Depend on attackers and environment

#### Correlation

Current decisions affect subsequent

#### Strong Interpretability

Security needs strong interpretability

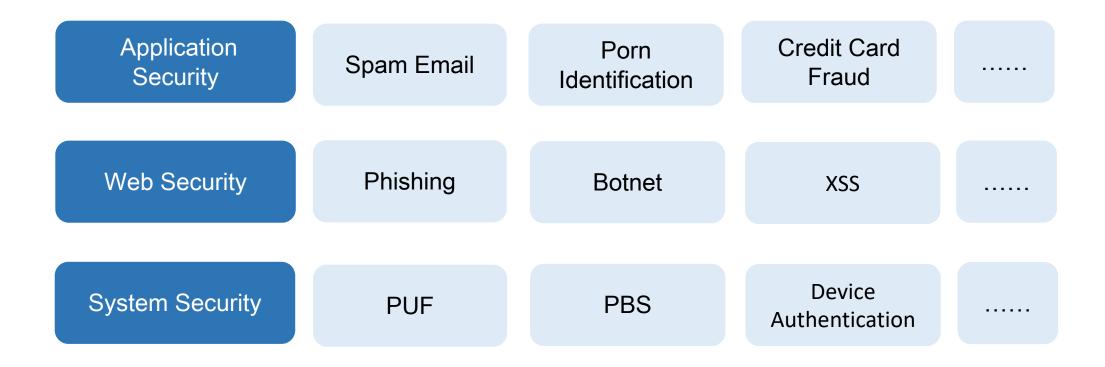






## What ML can do in Security

• 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	T&CK Matri	x for Ent	terprise				
Initial Access	Dentation	Persistence	Privilege Exceletion	Defense Dession	Credential	Discovery	Laberal Movement	Collection	Editoria	Command and Control
Drive-by Compromise	AppleBorpt	Jash, profile and Jassilvs	Access Tokan Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Appedicipe	Audio Capture	Automated Exfituation	Conveniently Used Part
Exploit Public Facing Application Hardware Additions	CMETP	Accessibility Features	Accessibility Features	875.304	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Duta Compressed	Communication Through Bennousbie Media Connection Proxy Countors Control Protocol Control Protocol Control Protocol
Hardware Additions	Command Line Interface	Account Manipulation	AppCent DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Deta Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert OLLS	Appinit DLLs	Bypess User Account Corrol	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Ceta Transfer Size Limite	Custom Command and Control Protocol
Spearphishing Attactoriant	Control Panel Items	Appinit DLLs	Application Shinning	CMETP	Credentials in Files	Network Service Scanning		Data from information Repositories	Exfiltration Over Atternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynemic Oata Exchange	Application Shimming	Bypass User Account Cantrol	Clear Command History	Credentials in Files Credentials in Registry	Network Service Scanning Network Share Discovery	Logon Scripts Pass the Hash	Data from Information Repositories Data from Local System	Editorsion Over Ahmatele Protocol Editorsion Over Command and Control Channel Editorsion Over Ober Network Medium	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Noteork	Channel Exhibution Over Other	Data Obfuscation
Supply Chain Compromise	Execution through Madule Load	875.384	DLL Search Order Hijecking Dyth Hijecking	Compiled HTML File	Forted Authentication	Metwork Solfing Passeed Nairy Discovery Discovery Permission Discovery Process Discovery Process Discovery Process Discovery Passes Discovery Passes Discovery Proces Discovery Process Discover Process Discover Discover Discover Discover Discover	Remote Desktop	Data hom Alsteoti Dhared Drive Data Asin Amovable Media Email Collection Pout Copture Douser Screen Copture Screen Copture	Medium Exhibition Over	Domain Pronting
Supply Chain Compromise Trusted Relationship	Exploitation for Client Execution		Exploitation for Privilege Escalation	Component Formware	Forsed Authentication	Petpheral Device	Remote File Copy	Email Collection	Medium Scheduled Transfer	Falback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Wedow Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Renate Services	Input Capture		Multi-Stage Channels
	Graphical User Interface	Rooskit Dowser Extensions Change Oefault File Association Component Premare Component Object Noel Hjacking	File System Permissions Weakness	Cortrol Parel Items	Input Prompt	Process Discovery	Replication Through Removable	Manin the Browser		Multi-top-Provy
	LSASS Driver	Component	Hocking	DCShadow	Ketenasting	Query	Media 55H	Screen		Mitbard
-	LEADS Driver	Component Object Wodel	Image File Execution	Coreol Panel Items DCShadow DLL Search Order Highting	Kerberseeting	Remote System	shared Webroot	Udeo Cepture		Multileyer Encryption
		Hjacking Create Account	Options Injection	OLL Side Loading	LLMNUNET-	Security	Tairt Shared			Port Knocking
	Local Job Scheduling Mohta	DLL Search Order Hjacking	File System Permasiona Weakvess Floaking Image File Dascular Dascention Launch Caemos New Service Path Interception	Deobhuscate/Decode Files or Information	Network	Security Software Discovery System Information Discovery	Third-party follows			Remote Access
-	PowerShell	Hjacking Dyth Hijacking	Path	Ples or information Disabiling Security Tools	Password	Information Discovery System Network Configuration	Wedges			Remote File
	Reports/Repairs			Tools Exploitation for Defense Eventor	LLANKUNET, NS Polasning Network Solfing Pasewand Film D.L. Proste Keys Securited Memory Two Factor Antheriostion	-tensvork Configuration Discovery System	Pese Per Thole Pesebe Dealboy Renoted Renote Fe Renoted Renotes Renote			Desi Delacación Denan Paranta Esthact Charosh Malt-Departura Malt-Angel Malt-
	Berne 11	Services	Flet Modification Part Monthors Pipetion Dipetion Dipetion Dipetion Dipetion Dipetion Distance Distanc		Second	Discovery System Network Connections Discovery System Owner/User Discovery	Renote Management			Application Layer Protocol
-	Registrat	Permissions Weakness	Monitors	Extra Window Memory Injection File Deletion	Menory	Owner/User Discovery				Cryptographic Protocol
_		Directories	injection		Authentication Interception	Discovery System Service Discovery System Time Discovery				Standard Non- Application Layer Protocol
-	Scheduled Task	Hooking	SD-Hatory Injection	File Permissions Modification		System Time Discovery				Uncommonly Used Port
	Service	Image File	Task Service	File Permissions Modification File System Logical Offsets Gatekeeper Bypass						WHO SERVER
	Execution	Execution Options injection	Registry Permissions Weakness							
	Signed Binary Proxy Execution Signed Script	Karnel Modules and Extensions	Setuid and Setupid	HISTCONTROL						
	Proxy Execution Source	Addition LSASS Driver	Barns Sudo	Directories Hidden Users						
	Space after Filename	Launch Agent	Sudo	Hidden Window						
	Third-party Software	Launch Deemon	Valid Accounts	Image File Execution Options Injection						
	Trap Transed	Launchedl Local Jab	Web Shell	Indicator Blocking						
	Utilities User Execution	Login Item		Indicator Removal on						
	Papers/Harm	Logon Scripts		Handbard Same and an ann an ann an ann an ann an ann an						
	Windows Remote Management	Modify Existing Service		Install Root Certificate						
	XSL Script Processing	Netsh Helper DLL		InstallUS						
-		New Service Office Application Startup		LC, MAN Hjacking Launched						
		Path Interception		Masquerading						
		Part Knocking		Mahta						
-		Part Monitors Recommon		NTFS File Attributes Network Share						
		Respond		Obfuscated Files or Information						
		Redundant		Plat Modification						
		Registry Run Keys / Startup Folder SIP and Trust		Port Knocking Process						
		Provider Hjacking		Dependplinging						
		Scheduled Task Scheensaver		Process Hollowing Process Injection						
_		Security Support Provider		Redundant Access						
		Permissions Weakness		Record 22						
		Shortcut Modification		Rootkit						
		Startup Items System Firmware		Rundl02 SIP and Trust						
		Time Providers		source Hipsking Scripting						
_		Trap		Signed Binary Proxy Execution						
		Web Shell		Signed Script Proxy Execution Software Packing						
		Stansard        Stansard <t< td=""><td></td><td>Space after Filename</td><td></td><td></td><td></td><td></td><td></td><td></td></t<>		Space after Filename						
		Minispen Helper DLL		Template Injection						
				Timestorip Trusted Developer						

#### 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
- ...

0000 0.0 0000 000 000 0.... 0 0 0 0 0 0000 . . ...... . . . . ...... 
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
... ......



#### Best Practices: Large-Scale Data



#### Porn Identification

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



#### Intrusion detection

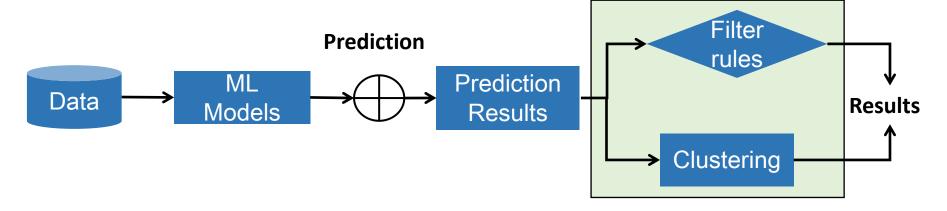
- Depend on experience and time consuming
- Security experts are expensive
- Few samples



#### 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



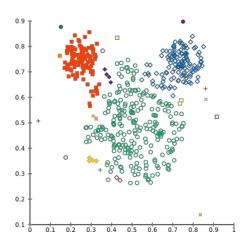




## **Best Practices: Behavior Analysis**

- 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

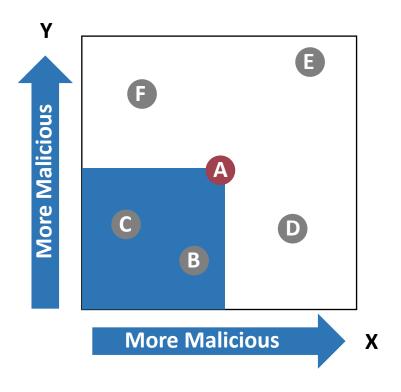


. . . . . .



## **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



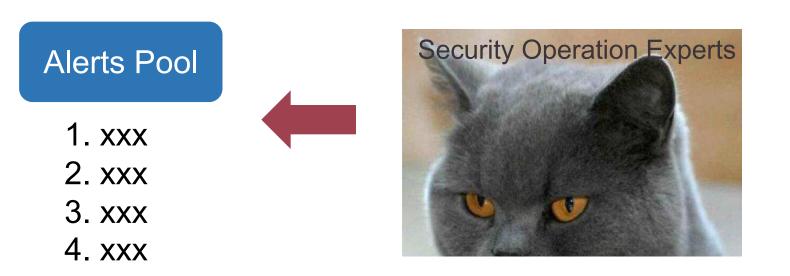


## **Best Practices: Feature Based Sorting**

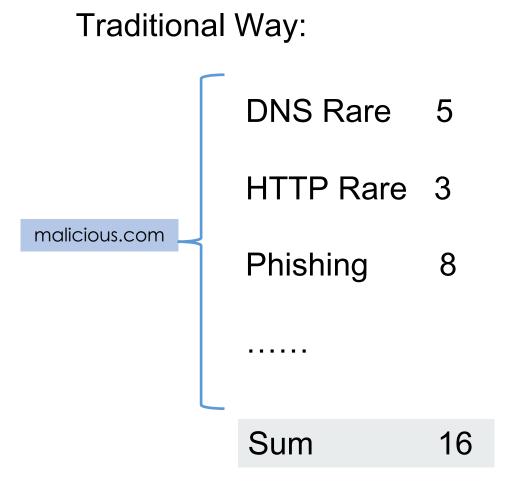
- Compare with historical data
  - Extract features per day/hour/...
  - Sort the data in a longer time window, e.g. one week
- Application
  - Phishing detection, Usenix Security'17
  - UEBA
  - ...
- Limitations
  - At the expense of recall
  - What features to extract is very hard to determine

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









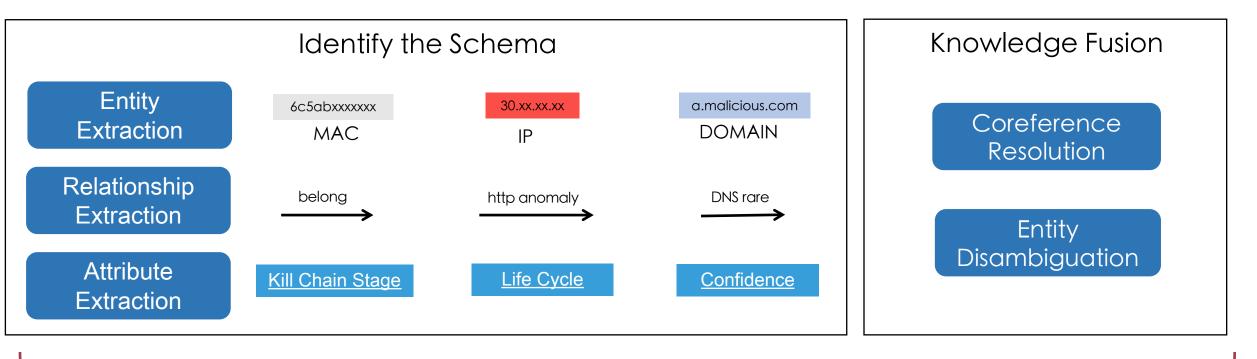
Problems behind it:

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



#### Best Practices: Knowledge Graph

#### Alerts Pool Construction





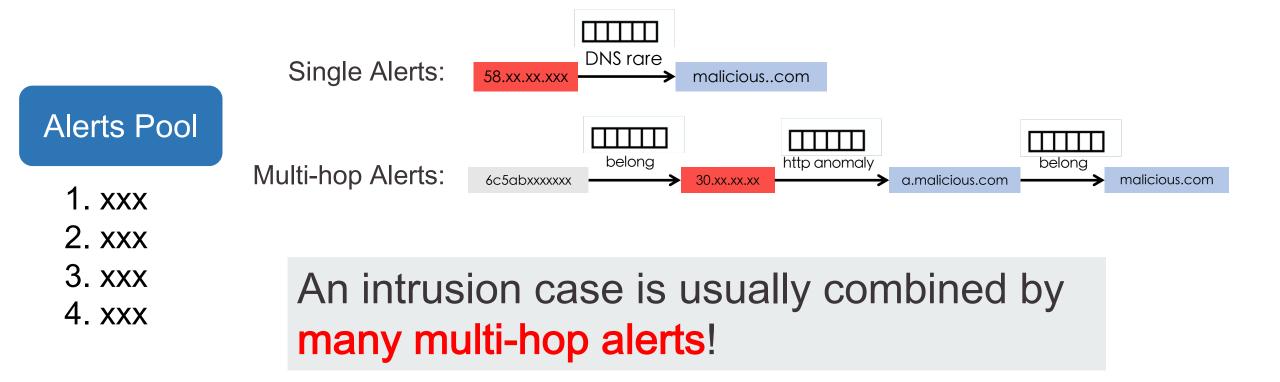
Some attributes

- Kill chain stage
- Life cycle

. . . . . .

Confidence

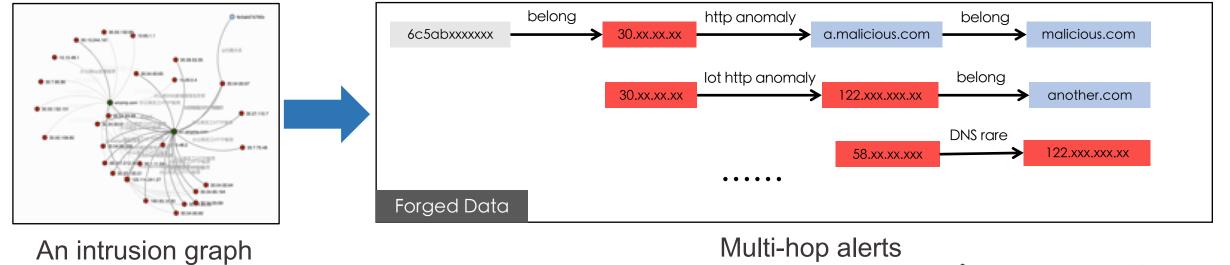
After identify the Schema, every alert is a Triple(entity-relationship-entity).





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

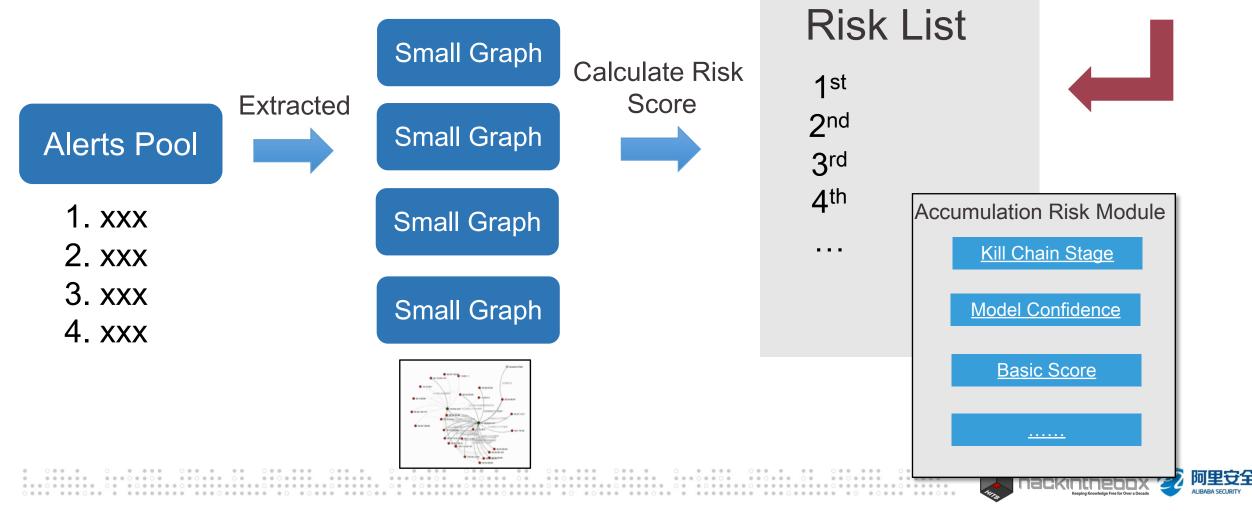
Eg.



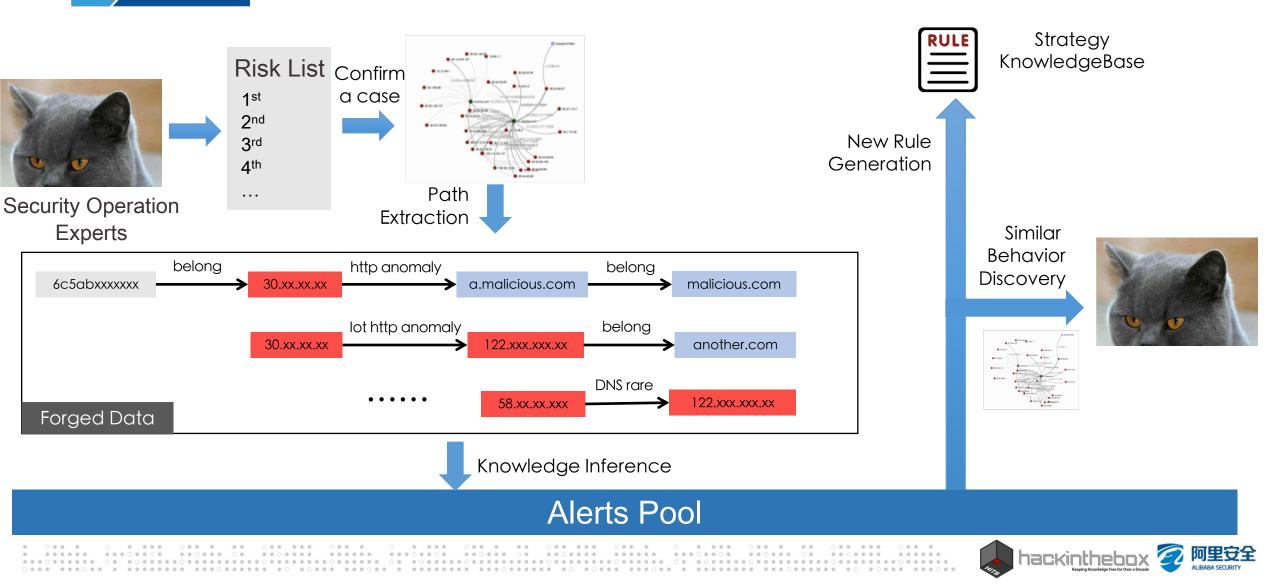


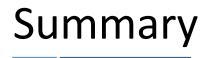


Security Operation Experts



#### 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

