Combining Dynamic and Static Attack Information for Attack Tracing and Event Correlation

Adel Alshamrani, Ankur Chowdhary, Oussama Mjihil, Sowmya Myneni, Dijiang Huang.

Arizona State University

GLOBECOM18

Outline

- Background on APT
- Problem Statement
- Contribution
- Conclusion

What is APT?

- Definition by NIST:*
  - **Advanced**: attackers are usually well-funded with access to advanced tools and methods.
  - **Persistent**: attackers are highly determined and persistent and they do not give up.
  - **Threats**: The threat is usually sensitive data loss or impediment of critical components.

R. S. Ross, "Managing information security risk: Organization, mission, and information system view," Special Publication (NIST SP)-800-39, 2011

What is APT?

- APT Attack Chain:
  1. Reconnaissance
     - Social Engineering
  2. Foothold Establishment
     - Malware, Command & Control (C&C)
  3. Lateral Movement
     - Penetration, scanning, etc
  4. Data Exfiltration
     - Moving data to remote location
  5. Cover up
     - Delete traces

Limitation in Current State of the Art

- Major limitations can be summarized into:
  A. APT related issues
  B. Risk assessment related issues

Limitation in Current State of the Art

A. APT related issues

- Parts of APT threats are considered
  - Focus on detecting specific stage
    - » i.e., C&C connections
- Drawback: lacking the *panoramic view* required to understand the whole attack trace.

Limitation in Current State of the Art

B. Risk assessment related issues

1) Risk assessment on known vulnerabilities
2) Attack graph based limitation

Problem Statement

- **Monitoring Known Vulnerability Exploitation**: Tracking known vulnerabilities and any of their exploitations.
- **Early Detection**: Understanding the attack intentions and prevent future damage.

Contribution

- To Detect & Mitigate APT attacks, we design a framework that involves three phases:
  1. Information Gathering and Coordination
  2. Security Risk Assessment
  3. Countermeasure Selection

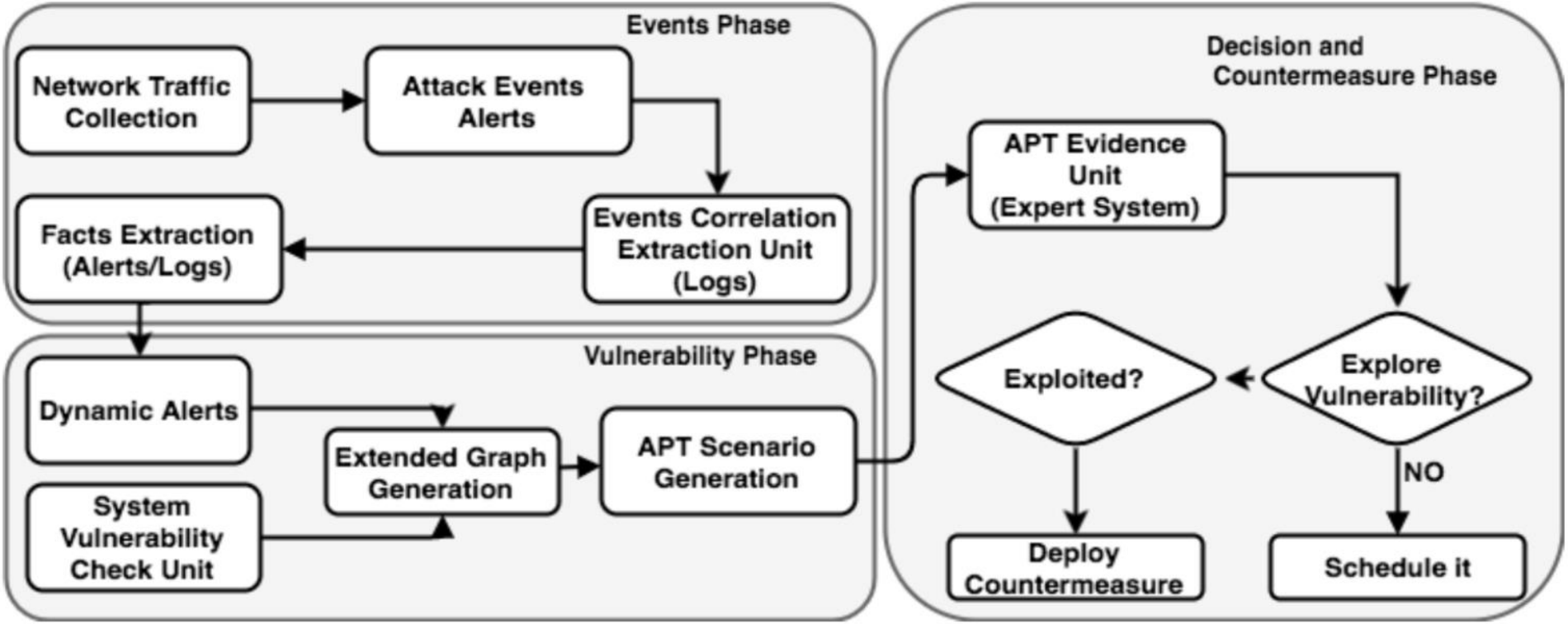
Objective

- Collect evidence from available and valuable data
  - Multiple sources of information
    - Static VS Dynamic
    - Network level VS System level
- Obtain attack evidence and suspicious activities.
- Correlate suspicious activities.
- Draw a conclusion and generate APT-Attack Path.

Static vs Dynamic

- **Static data**:
  - Reveal information about the system.
  - Configuration, vulnerabilities, security policies, and so on.
  - NOT attack related data.
  - Periodically generated, or on ad hoc.
- **Real-time data (dynamic data)**:
  - Reveal information about security incidents (attack events).
  - Vulnerability exploitation, privileges escalation, and so on.
  - Attack related data
  - Continuously monitored.

Approach Process Flow



Algorithm 1 Real-time APT Tracking

Input: Attack graph Info, Attack events
Output: APT attack scenarios

Require:

APTPaths[] ▷ List of possible APT Scenarios
MaxValPath[] ▷ The maximum value of the Path
ValPath[] ▷ The Current value of the Path
function MAXIMUMATTACKPATHVALUE
  for $eachPath : APTPaths$ **do**
    for $each\ e : Path$ **do** ▷ e : Event or Vulnerability
      $MaxValPath_i = MaxValPath_i + e.BS$
    end for
  end for
end function
function REALTIMEATTACKPATHVALUE
  for $each\ event : logFile$ **do**
    For all paths containing the event
    $ValPath_i = ValPath_i + element.BS$
  end for
  $Attack - Progress[Path_i] = \frac{ValPath_i}{MaxValPath_i}$
  if $AttackProgress[Path_i] \leq threshold$ **then**
    $RealTimeAttackPathValue <>$
  else
    $CountermeasureApplication < Path_i >$
  end if
end function
function BENEFIT_FUNCTION(vul)
  $Distance \leftarrow NbrHop * Complexity$
  return $\frac{Degree*BS}{Distance}$
end function
function COUNTERMEASUREAPPLICATION(Path)
  for $all\ vul : Path$ **do**
    $Benefit = benefit\_function < vul >$
    $ROI = \frac{Benefit}{CC+CDC}$
    $\lambda = \max_{ROI}(vul)$
  end for
end function

Base Score

ID	Events	Base Score(BS)
1	login from known host using public key authentication	5
2	download malware from remote host	7.9
3	local buffer overflow	6.3
4	remote user shell login	8.3
5	port scanning	5.3
6	ftp_connect	7.1
7	write to ftp home directory	7.9
8	remote user shell login	8.3
9	local buffer overflow	6.3
10	data exfiltration	10

Countermeasure Selection

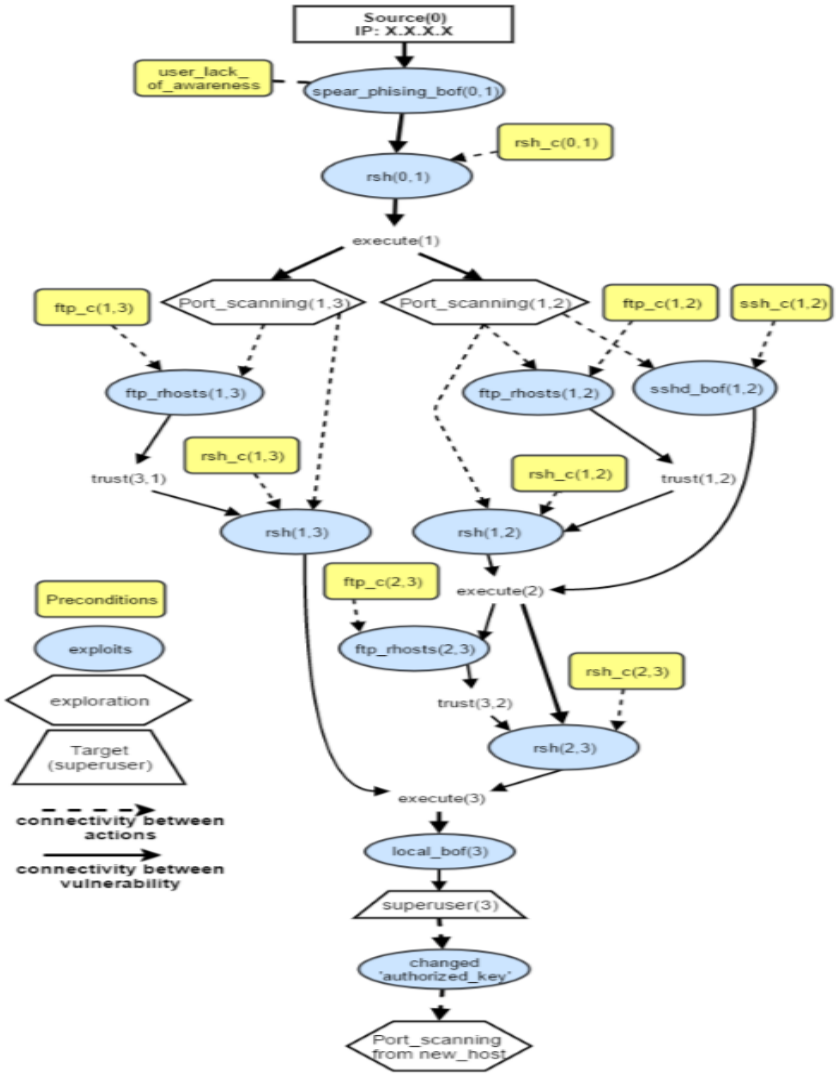
- **Definition 1: Countermeasure Cost (CC)** is evaluated by the defender based on the countermeasure application and its consequences.
- This involves the cost of the resources:
  - training, skills, personnel, network resources,
- With the aforementioned factors, we consider the cost to range from greater than 0 to 10 ($CC \in (0, 10]$).

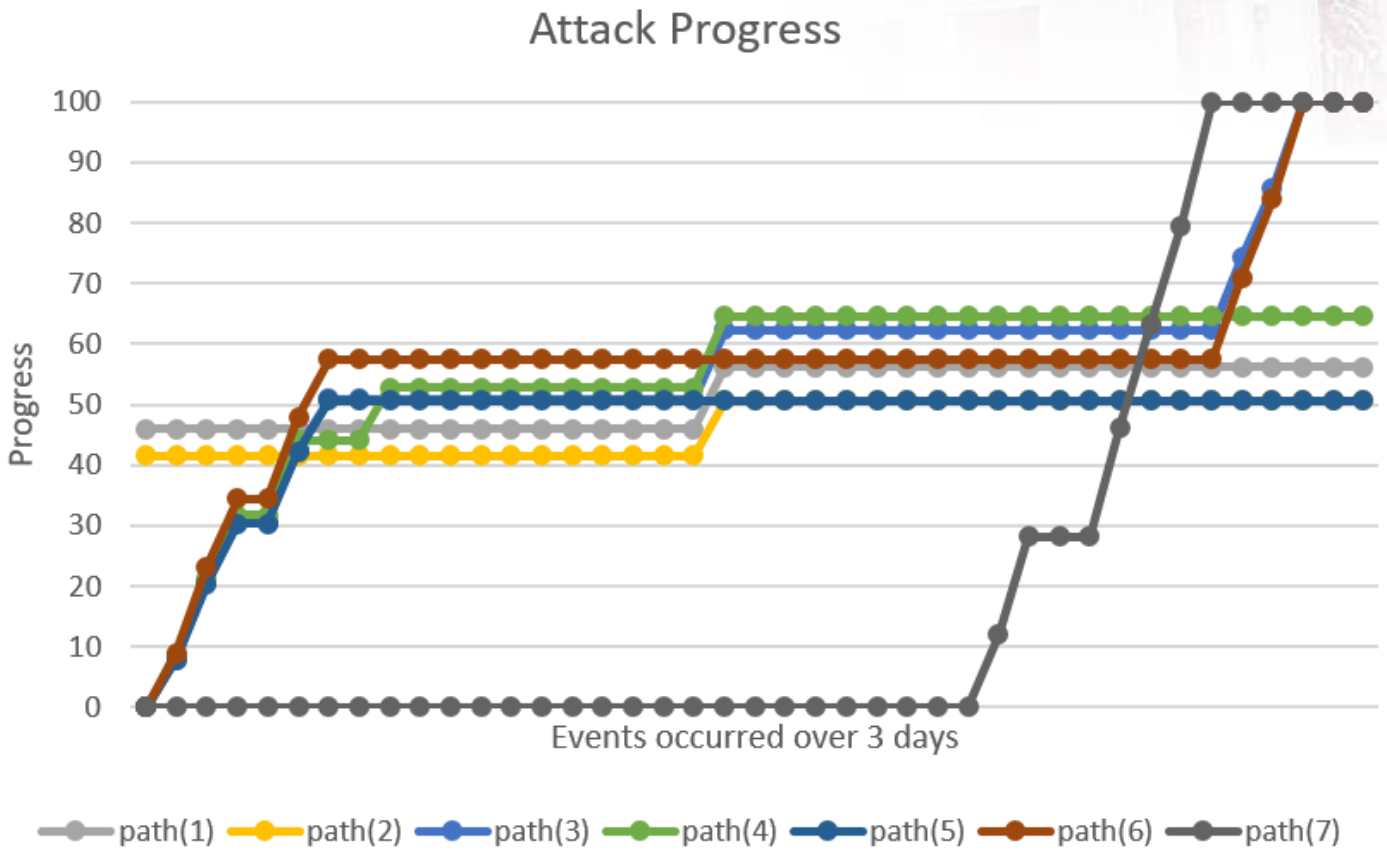
Optimal Countermeasure Selection

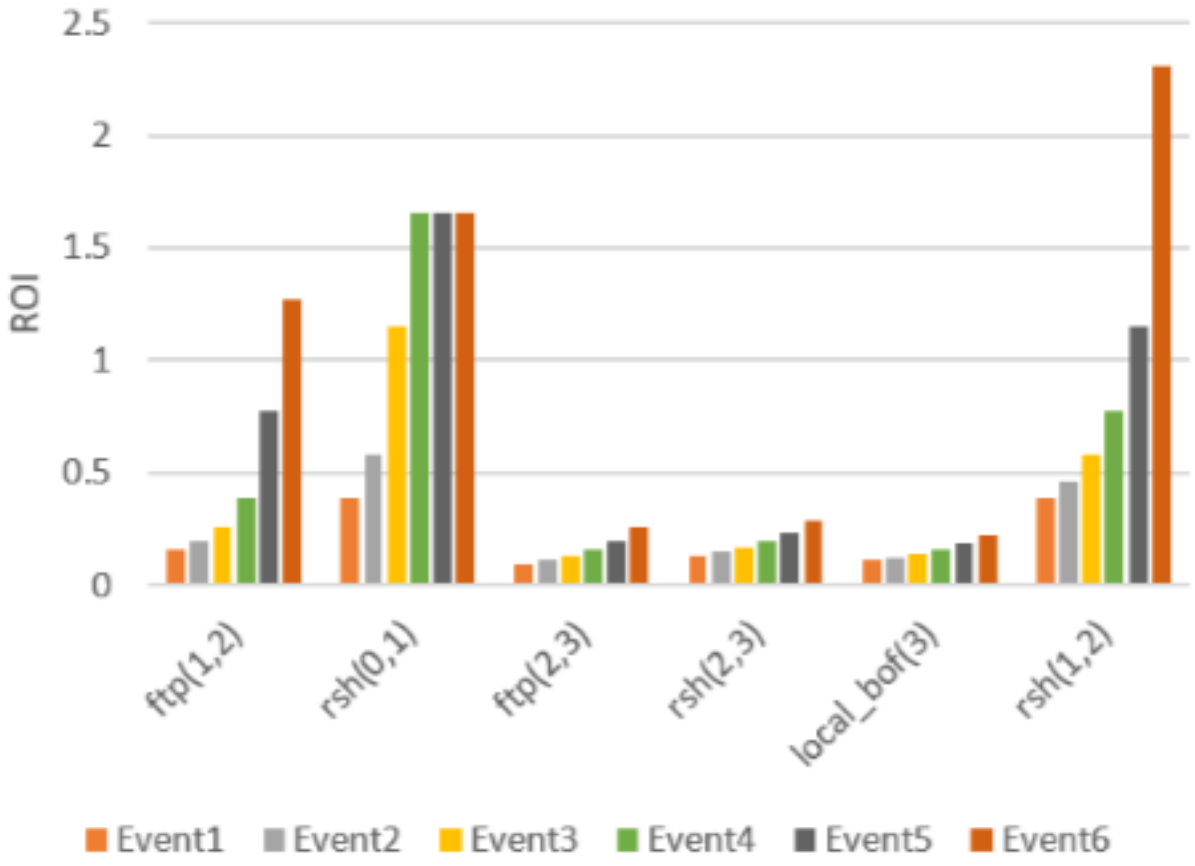
- **Definition 2: Countermeasure Deployment Complexity (CDC)** is the effort required from the defender to apply the countermeasure which depends on the amount of components that are involved in the application of a specific countermeasure.
- With the aforementioned factors, we consider the cost to range from greater than 0 to 10 (CDC $\in$ (0, 10]).

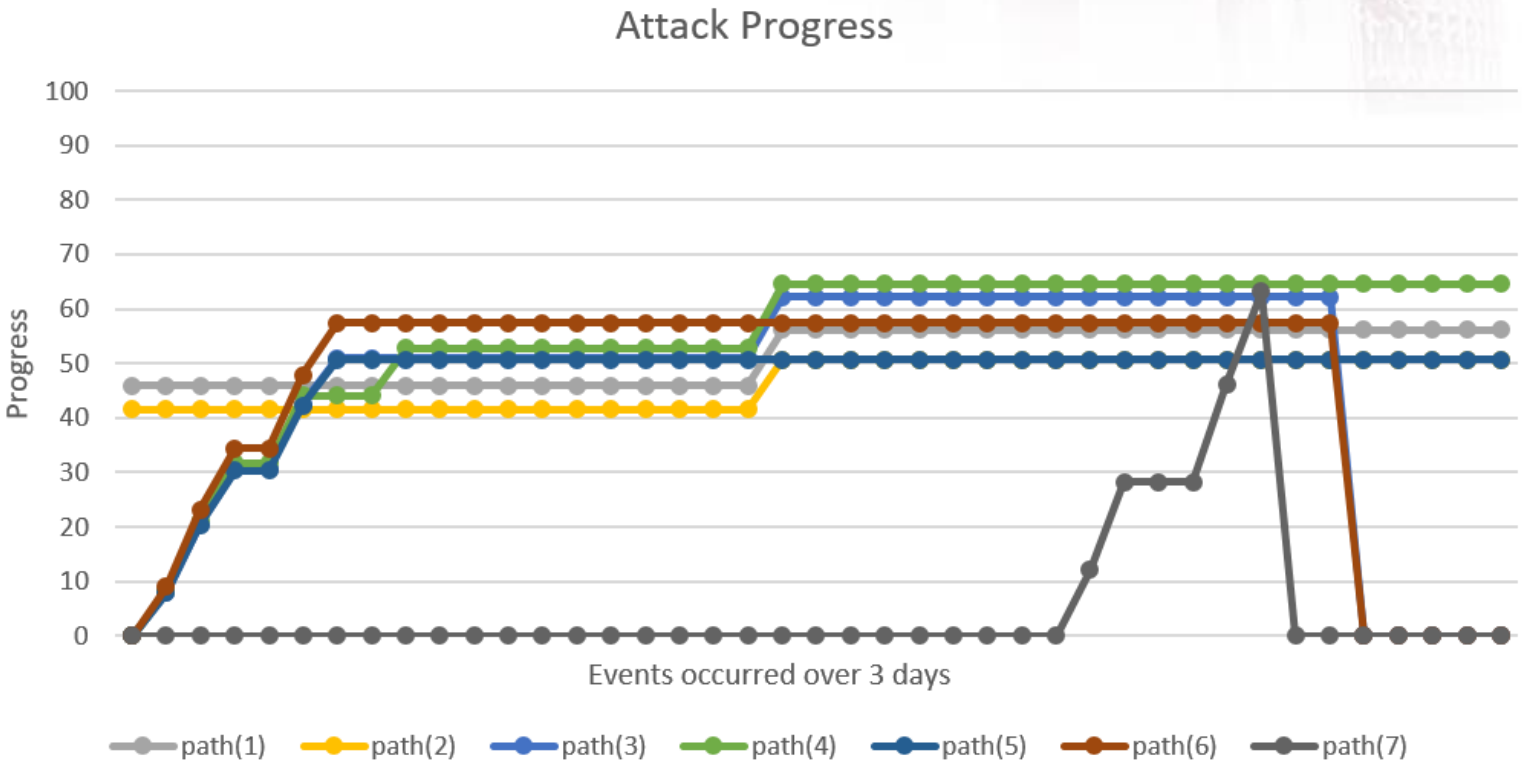
Optimal Countermeasure Selection

No.	Countermeasure	CC	CDC
1	Traffic redirection	6	7
2	Traffic isolation	3	2
3	Block port	4	1
4	Software patch	7	6
5	Network reconfiguration	7	9
6	Service migration	6	8


Source(0)
IP: X.X.X.X
user_lack_of_awareness
spear_phising_bof(0,1)
rsh_c(0,1)
rsh(0,1)
execute(1)
ftp_c(1,3)
Port_scanning(1,3)
Port_scanning(1,2)
ftp_c(1,2)
ssh_c(1,2)
ftp_rhosts(1,3)
ftp_rhosts(1,2)
sshd_bof(1,2)
rsh_c(1,3)
trust(3,1)
rsh_c(1,2)
trust(1,2)
rsh(1,3)
rsh(1,2)
ftp_c(2,3)
execute(2)
Preconditions
exploits
exploration
Target (superuser)
ftp_rhosts(2,3)
rsh_c(2,3)
trust(3,2)
rsh(2,3)
execute(3)
connectivity between actions
connectivity between vulnerability
local_bof(3)
superuser(3)
changed 'authorized_key'
Port_scanning from new_host
.....


Attack Progress
Progress
100
90
80
70
60
50
40
30
20
10
0
Events occurred over 3 days
path(1)
path(2)
path(3)
path(4)
path(5)
path(6)
path(7)


2.5
2
1.5
1
0.5
0
ROI
ftp(1,2)
rsh(0,1)
ftp(2,3)
rsh(2,3)
local_bof(3)
rsh(1,2)
Event1
Event2
Event3
Event4
Event5
Event6


Attack Progress
100
90
80
70
60
50
40
30
20
10
0
Progress
Events occurred over 3 days
path(1)
path(2)
path(3)
path(4)
path(5)
path(6)
path(7)

Conclusion & Future Work

- We proposed three phases:
    - Advanced Persistent Threats.
        1. Information Gathering and Coordination
        2. Security Risk Assessment
        3. Optimal Countermeasure Selection
- In the future work, we plan to collect more system data over long time and perform multiple scenarios of APTs.


THANK
YOU