Unknown Threat Detection

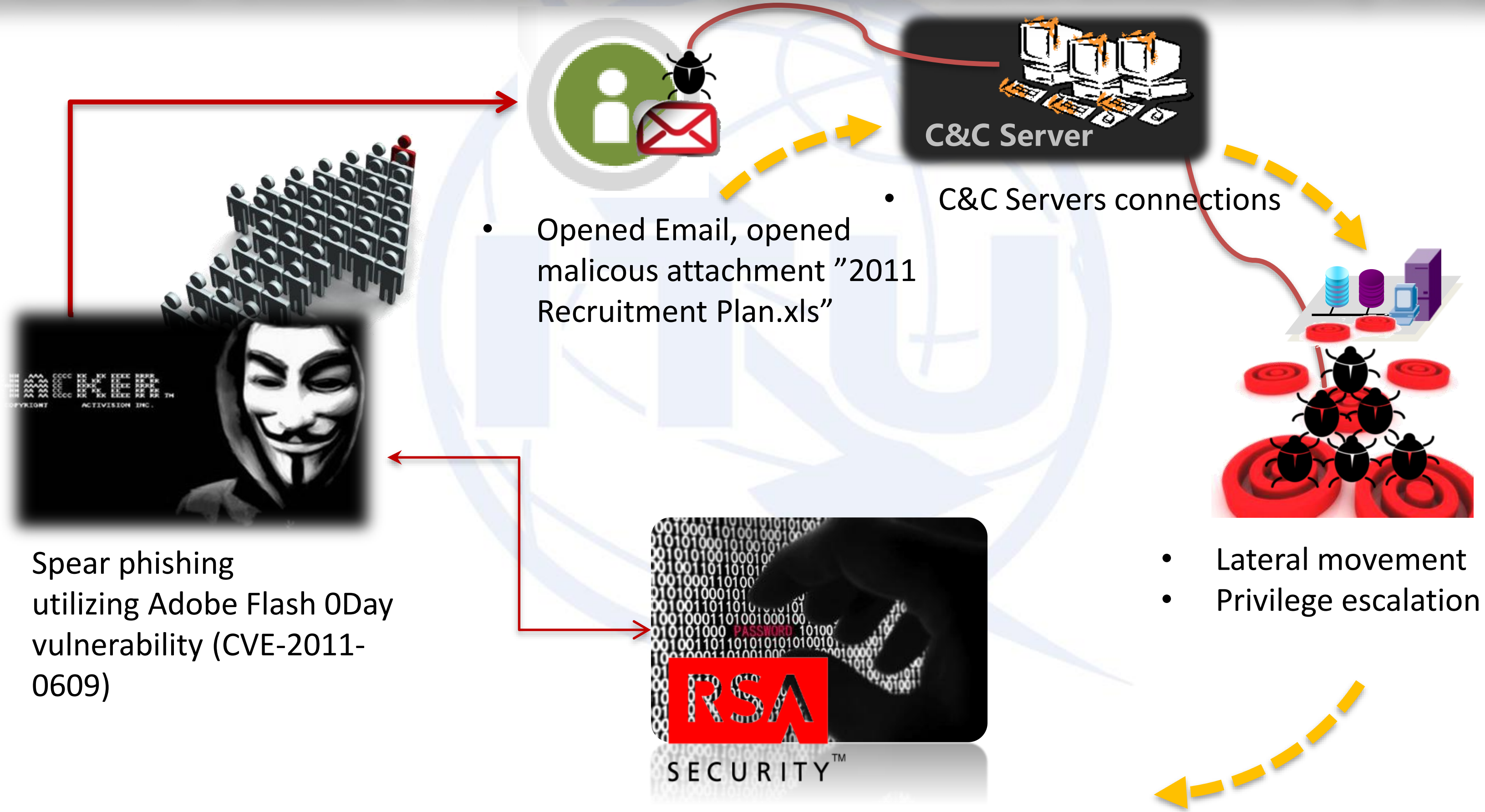
--- the Key Ability of APT Defense

Tian Tian, ZTE Corporation

APT Case Review

--- RSA SecurID Breach

APT (Advanced Persistent Threat) attack against the world famous security company!



Spear phishing utilizing Adobe Flash 0Day vulnerability (CVE-2011-0609)

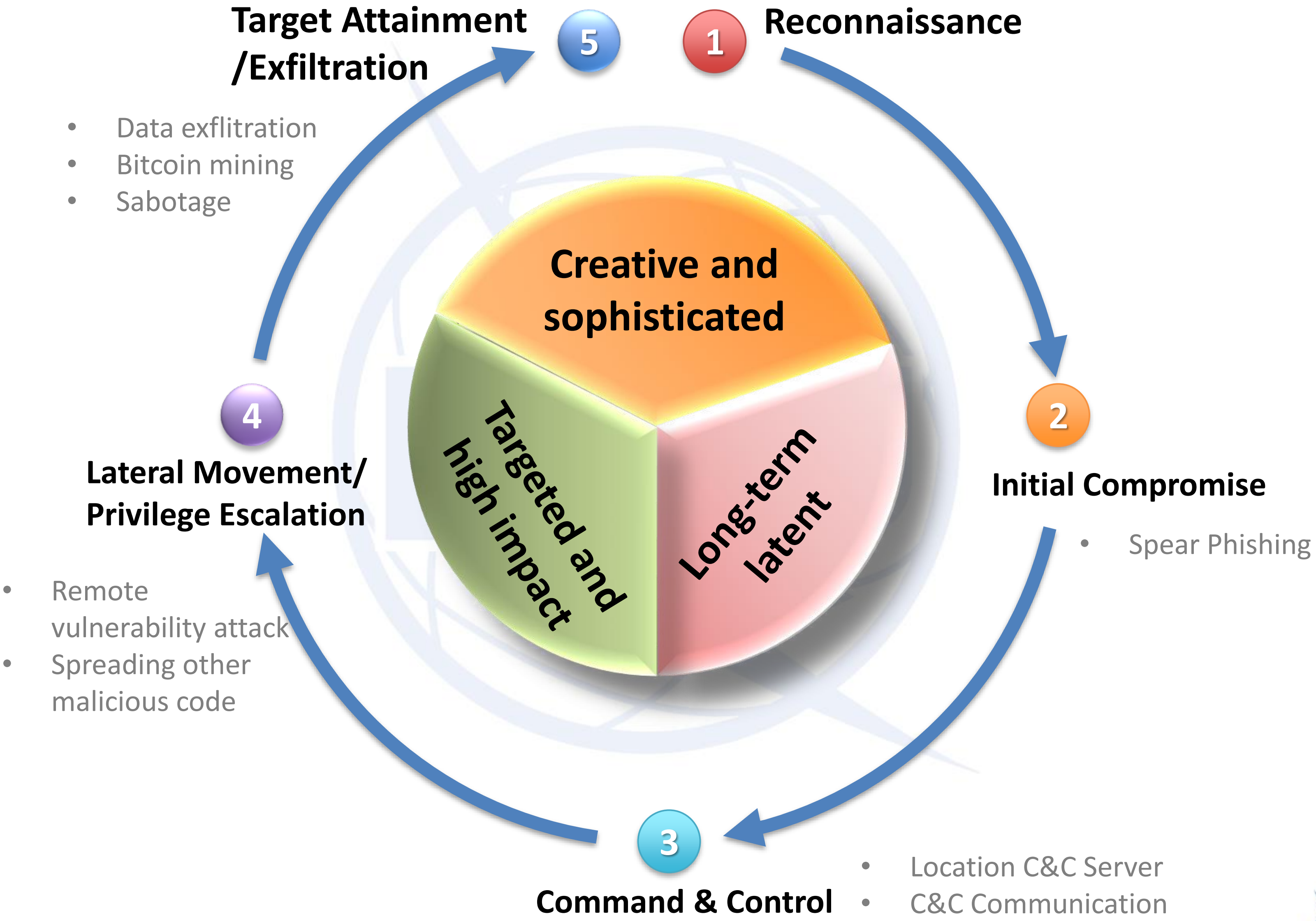
- Opened Email, opened malicous attachment ”2011 Recruitment Plan.xls”

- C&C Servers connections

- Lateral movement
- Privilege escalation

- Exfiltrate SecureID data
- Remove attack traces

Advanced Cyber Attack Lifecycle & Features



1 Reconnaissance

2 Initial Compromise

- Spear Phishing

3 Command & Control

- Location C&C Server
- C&C Communication

4 Lateral Movement/ Privilege Escalation

- Remote vulnerability attack
- Spreading other malicious code

5 Target Attainment /Exfiltration

- Data exflitration
- Bitcoin mining
- Sabotage

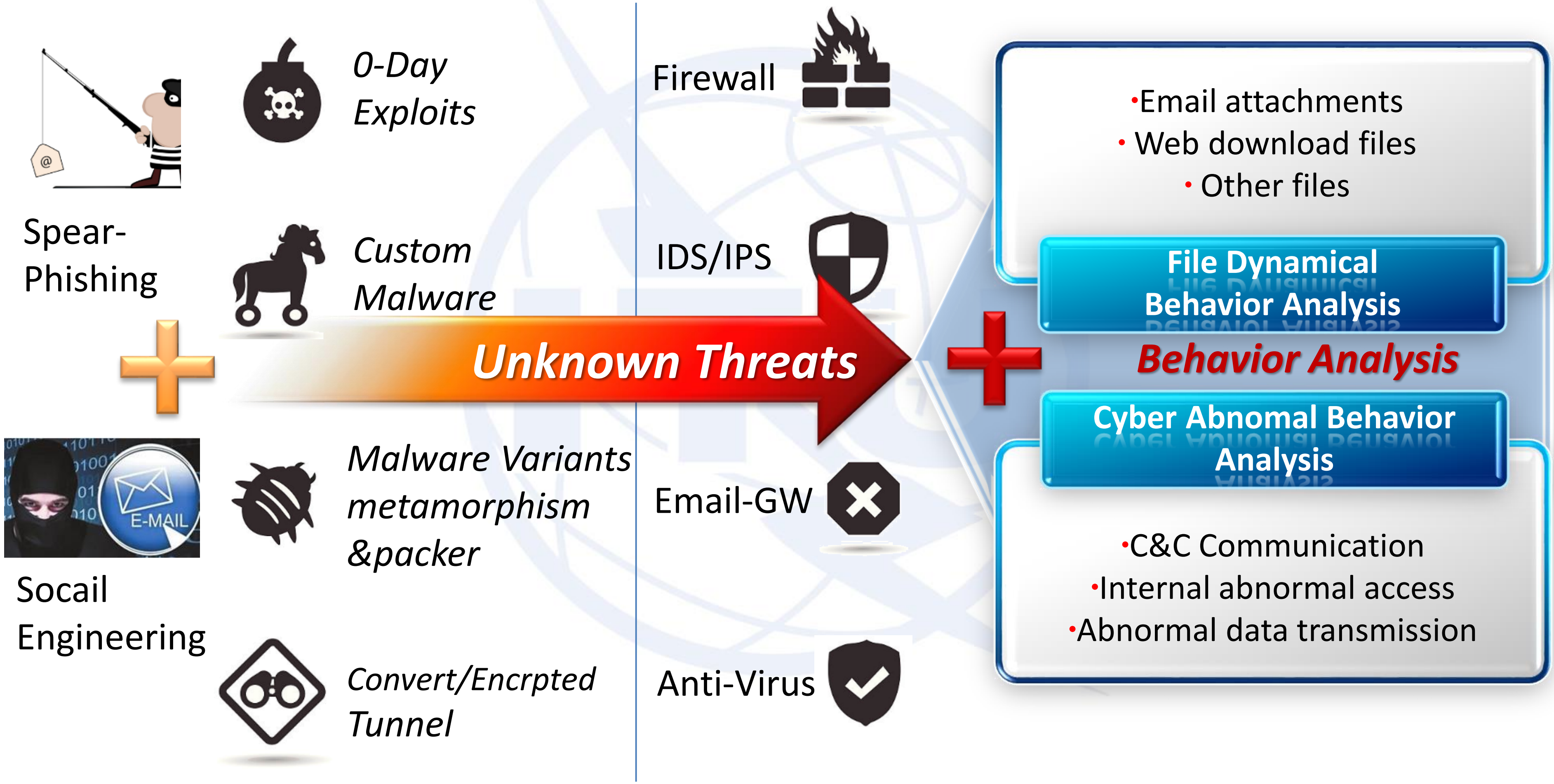
Creative and sophisticated

Long-term latent

Targeted and high impact

Advanced cyber threats are hard to detect,
new methods of detection and analysis are needed.

Advanced Attacks Vs. Defenses



Spear-Phishing

Socail Engineering

0-Day Exploits

Custom Malware

Malware Variants metamorphism &packer

Convert/Encrpted Tunnel

Firewall

IDS/IPS

Email-GW

Anti-Virus

Unknown Threats

- Email attachments
- Web download files
- Other files

File Dynamical Behavior Analysis

Behavior Analysis

Cyber Abnomal Behavior Analysis

- C&C Communication
- Internal abnormal access
- Abnormal data transmission

File Dynamical Behavior Analysis --- Sandbox Technology

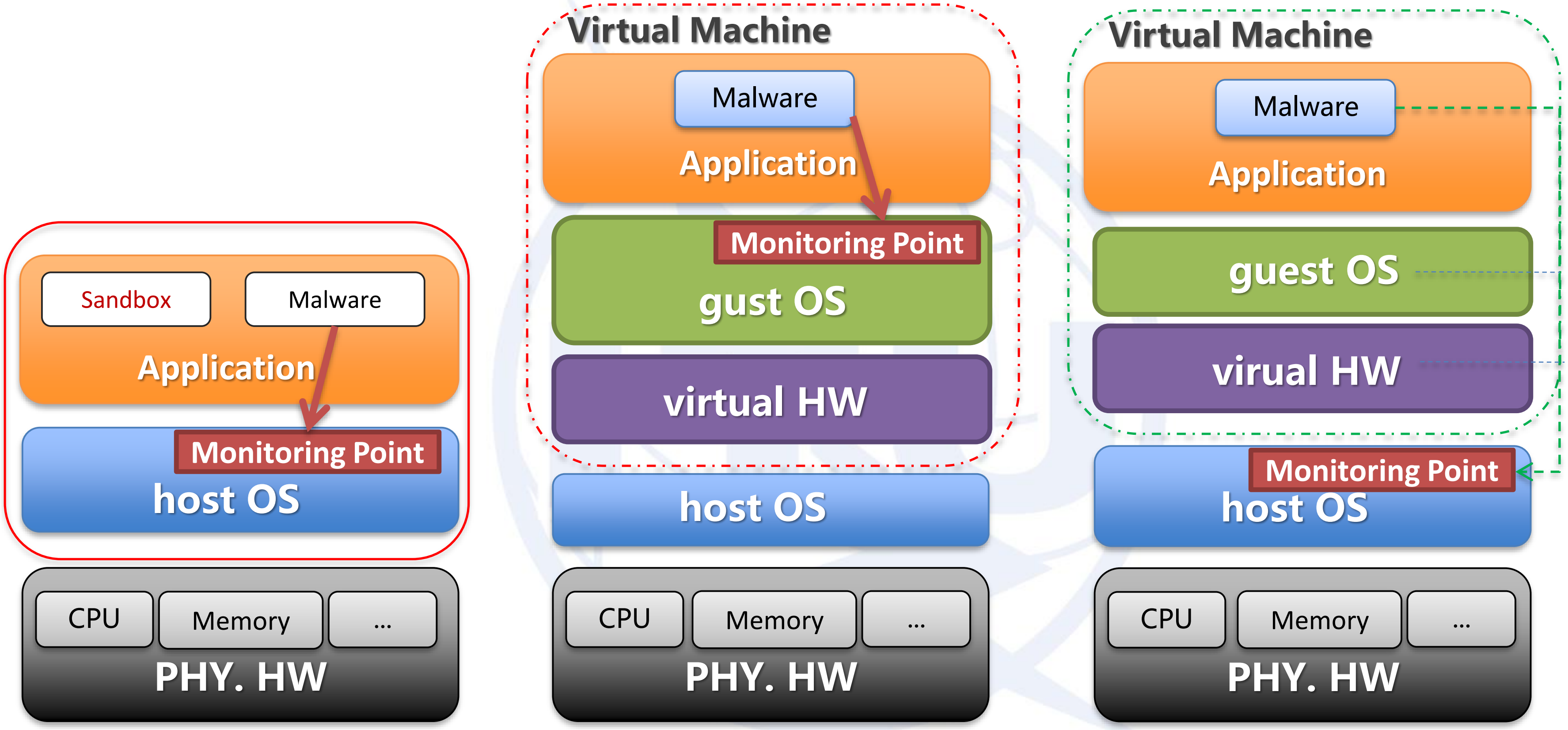
Principle

- Use behavioral analysis methods to monitor unknown malware programs in a simulated/isolated environment

Requirement

- High Level of Visibility into Malware Behavior
- Resistance to Evasion
- Scalability of Analysis and Management

Sandbox Technologies

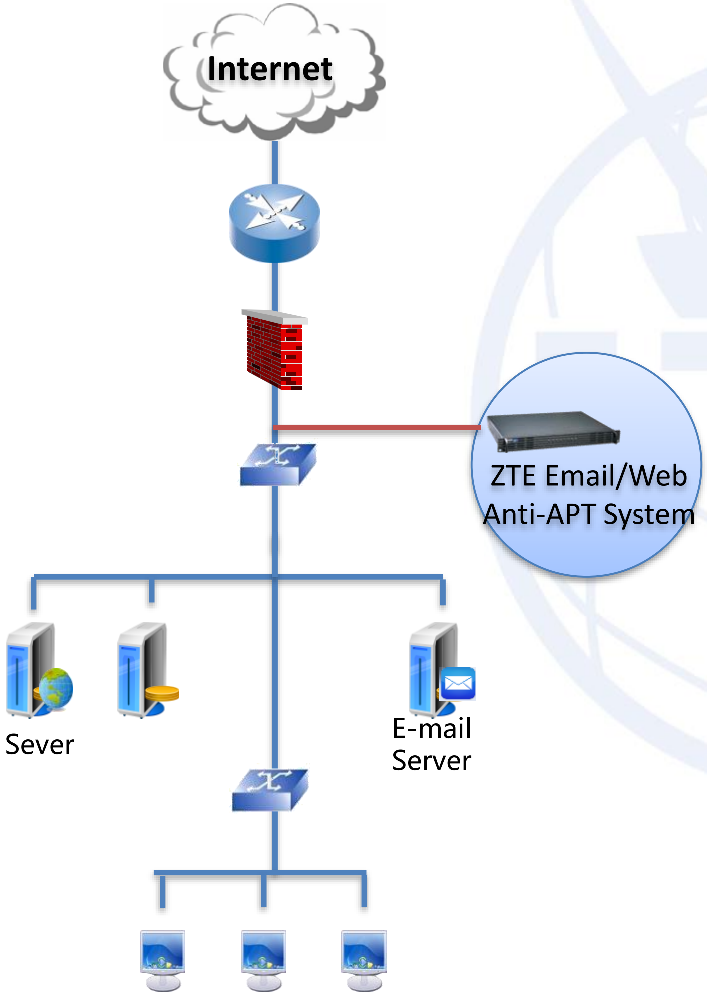


First-generation Sandboxing

Second-generation Sandbox based on software virtualization

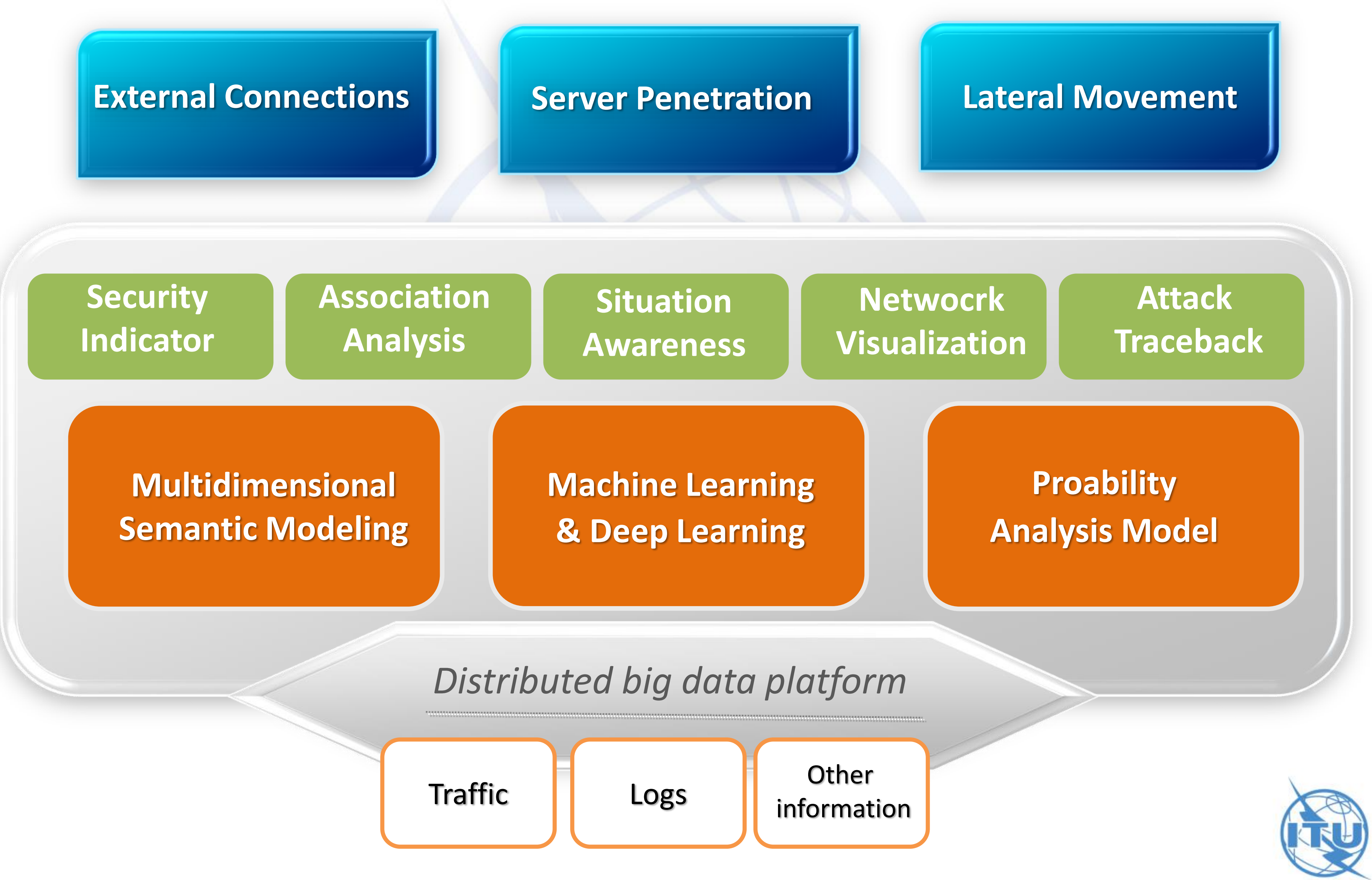
Third-generation Sandbox based on hareware virtualization

ZTE Email/Web Anti-APT System



- **Easy deployment**
  - Common mode: parallel deployment
  - Analyze incoming traffic mirroring
- **Advanced technology**
  - Third-generation Sandbox technology based on hardware virtulization
- **Scalble Analysis and Management**
  - Support distributed deployment of dynamic analysis engines

Cyber Abnomal Behavior Analysis



External Connections

Server Penetration

Lateral Movement

Security Indicator

Association Analysis

Situation Awareness

Networck Visualization

Attack Traceback

Multidimensional Semantic Modeling

Machine Learning & Deep Learning

Proability Analysis Model

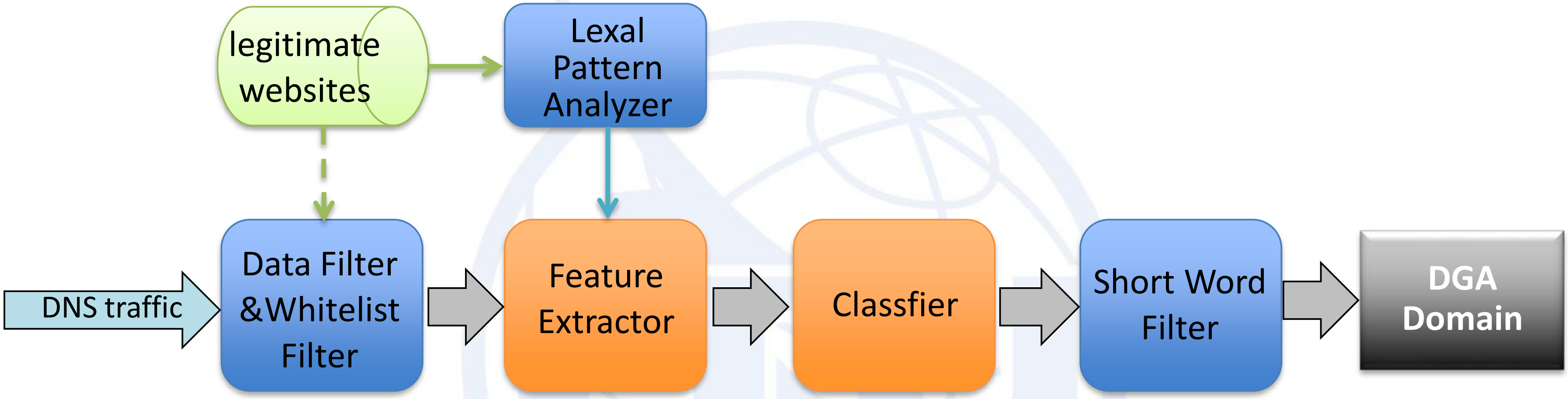
Distributed big data platform

Traffic

Logs

Other information

DGA Detection Example

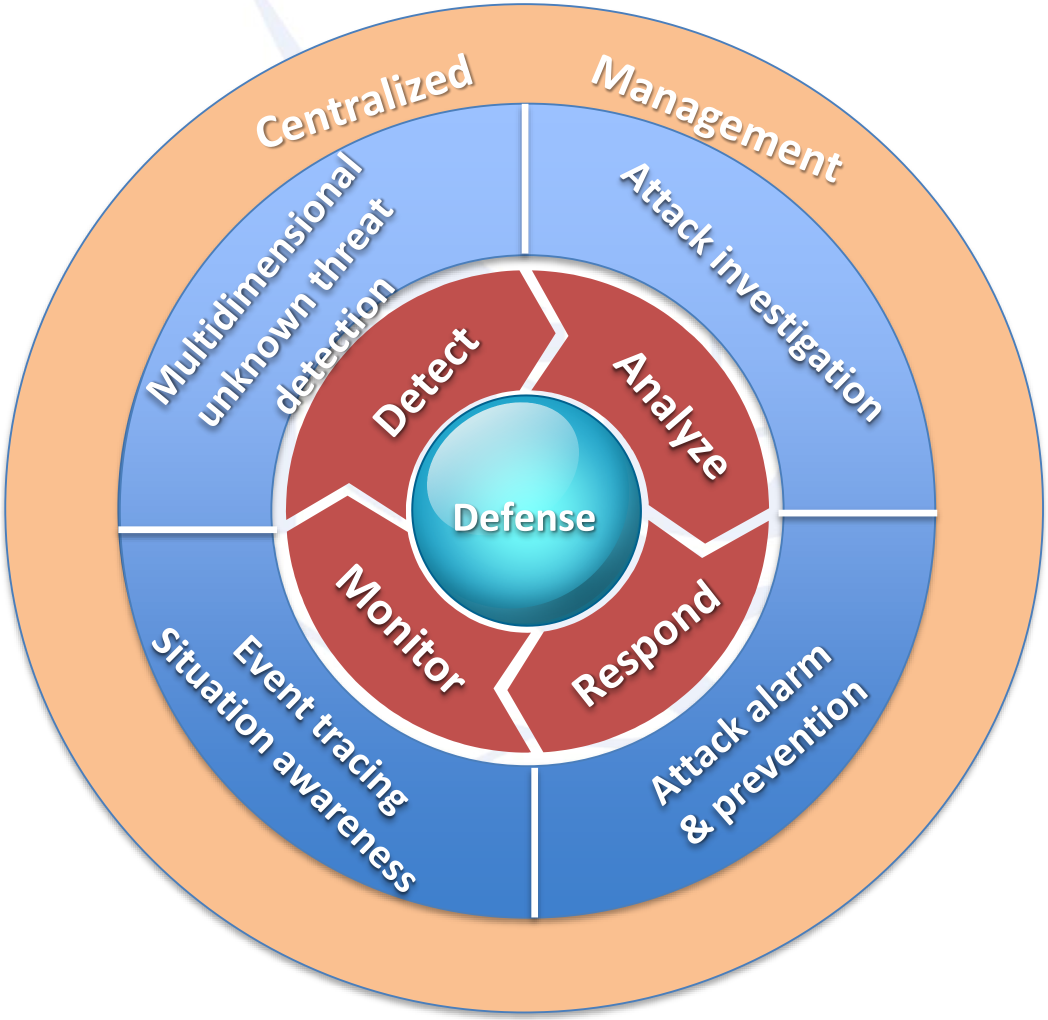


Feature Set	Feature Examples
Distribution Template Feature	• Domain valuation • Appearance probability
Structure Template Feature	• Transition probability • TLDs probability
Pronounce Feature	• Number of word-like unit
Common Feature	• Domain length • Number of Repeat letters

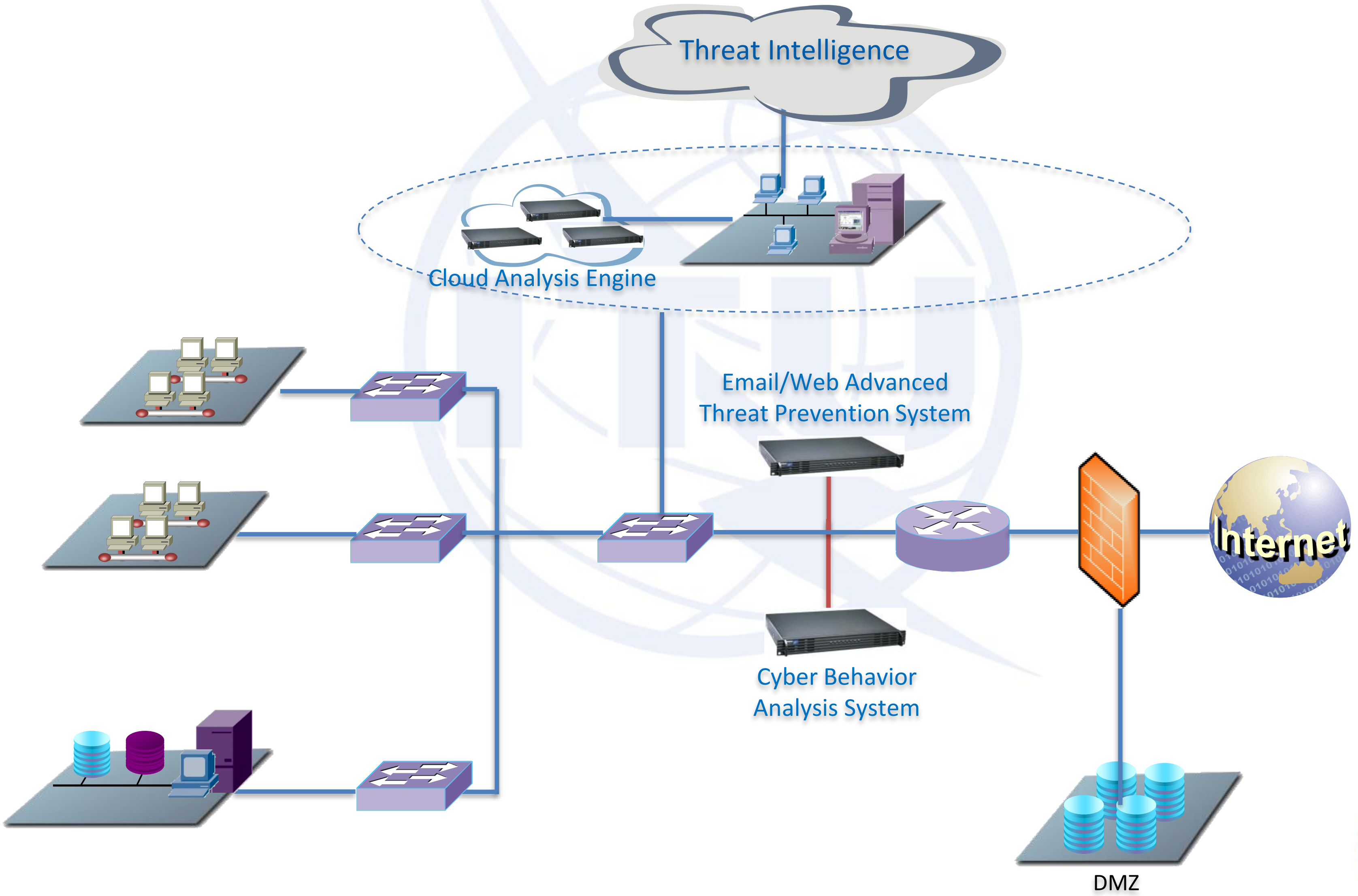
Category	DGA family	Size
ALGORITHM	Conficker/Kraken/ Necurs/Tinba/...	100,000 +
HASH	Murofet/Pushdo/Zeus/...	100,000 +
WORD	Gozi/Matsnu/Rovix/ ...	100,000 +

Method	Precision	Recall	FPR
RF	0.936	0.938	0.08

ZTE Defense Solution Overview

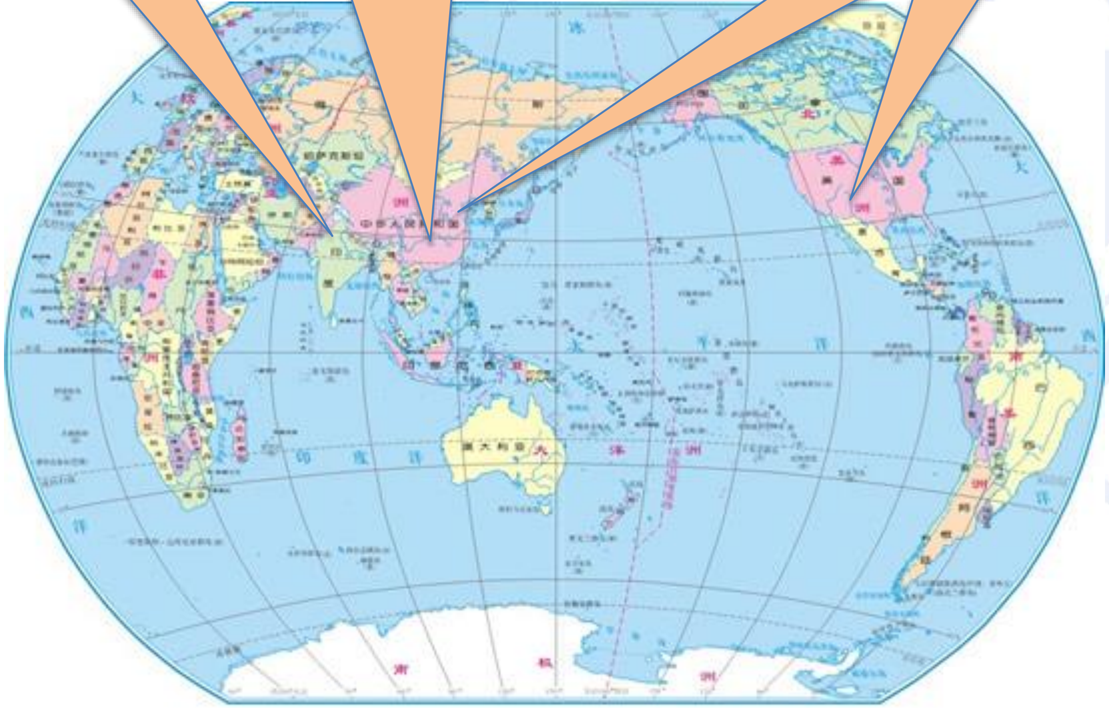


Practical Deployment in ZTE


Threat Intelligence
Cloud Analysis Engine
Email/Web Advanced Threat Prevention System
Internet
Cyber Behavior Analysis System
DMZ

Practical Effect

◆ **Successful detection and early warning of several advanced cyber attacks against ZTE**

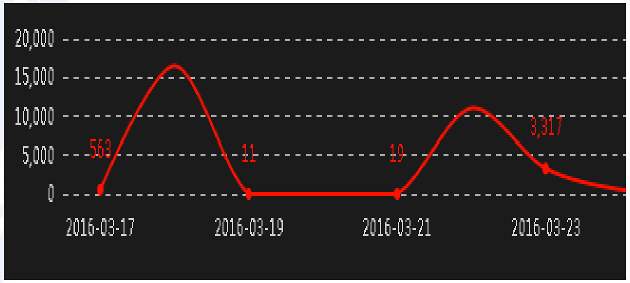


Jan. 2017
Particular areas
attack detected

Feb. 2016
Company executives
targeted attack detected

Feb.~Aug.2016
Continuous ransomware
attack detected

Advanced Attacks cannot be detected by other traditional security products



- ***Highest daily detection number of ransomware: 10,000 +***
- ***Average daily high-risk malwares detected in email : 10 +(cannot be detected by most world famous antivirus software)***

Thanks !