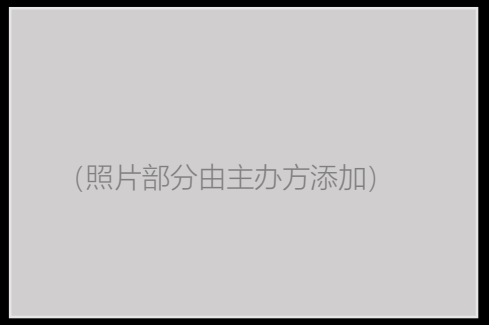


部分可观下APT攻击行为捕获：马尔可夫决策助力AI模型

孟雷　　斗象科技高级机器学习专家

CIS 网络安全创新大会
Cyber Security Innovation Summit

Agenda

APT威胁严峻

AI模型助力APT检测

马尔可夫决策助力AI模型

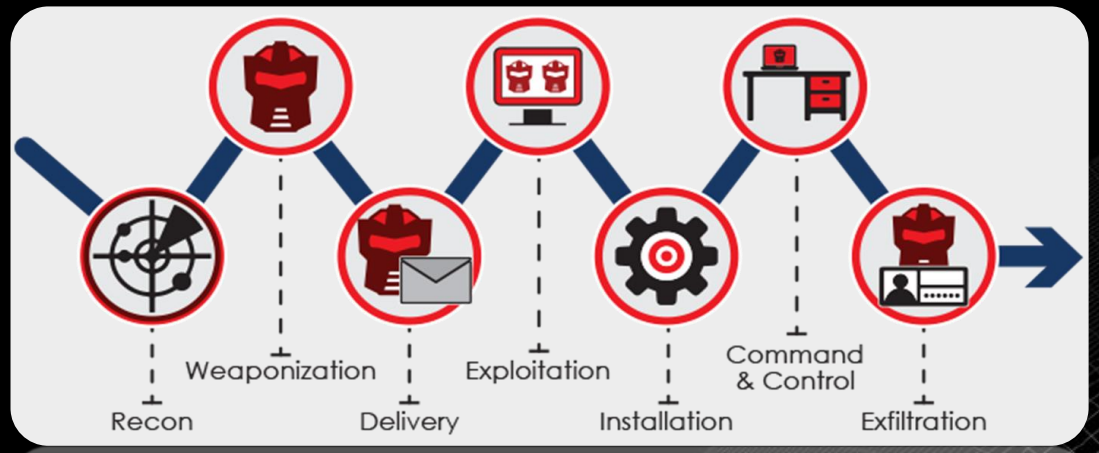
Data Exfiltration 检测与防御

总结

高级持续威胁（APT）
以精确打击要害及核心信息窃取为主要目，
对企业网络安全，信息资产安全构成严重威胁。

攻击行为挖掘 | Cyber Kill Chain and ATT&CK

网络安全创新大会
Cyber Security Innovation Summit



Social Engineering

Spear phishing

0-Day Exploits

Custom Malware

Malware Variants
metamorphism & packer

Convert/Encrypted Tunnel

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Audio Capture	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Automated Collection	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Clipboard Data	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data Staged	Data Transfer Size Limits	Connection Proxy
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	Custom Command and Control Protocol
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery	Logon Scripts	Graphical User Interface	Data from Network Shared Drive		
Path Interception		Disabling Security Tools	Input Capture		Pass the Hash	InstallUtil		Exfiltration Over Command and Control Channel	Custom Cryptographic Protocol
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Ticket	MSBuild	Data from Removable Media		Data Encoding
File System Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception	Network Service Scanning	Remote Desktop Protocol	PowerShell	Email Collection	Exfiltration Over Other Network Medium	Data Obfuscation
Service Registry Permissions Weakness				Peripheral Device Discovery	Remote File Copy	Process Hollowing	Input Capture		Fallback Channels
Web Shell		Indicator Blocking			Remote Services	Regsvcs/Regasm	Screen Capture	Exfiltration Over Physical Medium	Multi-Stage Channels
Authentication Package	Exploitation of Vulnerability			Permission Groups Discovery	Replication Through Removable Media	Regsvr32	Video Capture		Multiband Communication
Bootkit	Bypass User Account Control					Rundll32		Scheduled Transfer	
Component Object Model Hijacking	DLL Injection	Component Object Model Hijacking		Process Discovery	Shared Webroot	Scheduled Task			Multilayer Encryption
Basic Input/Output System		Indicator Removal from Tools		Query Registry	Taint Shared Content	Scripting			Remote File Copy
Change Default File Association		Indicator Removal on Host		Remote System Discovery	Windows Admin Shares	Service Execution			Standard Application Layer Protocol
Component Firmware		Install Root Certificate		Security Software Discovery		Windows Management Instrumentation			Standard Cryptographic Protocol
External Remote Services		InstallUtil		System Information Discovery					Standard Non-Application Layer Protocol
Hypervisor		Masquerading		System Owner/User Discovery					Uncommonly Used Port
Logon Scripts		Modify Registry		System Service Discovery					Web Service
Modify Existing Service		MSBuild		System Time Discovery					
Netsh Helper DLL		Network Share Removal							
Redundant Access		NTFS Extended Attributes							
Registry Run Keys / Start Folder		Obfuscated Files or Information							
Security Support Provider		Process Hollowing							
Shortcut Modification		Redundant Access							
Windows Management Instrumentation Event Subscription		Regsvcs/Regasm							
Winlogon Helper DLL		Regsvr32							
		Rootkit							
		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							

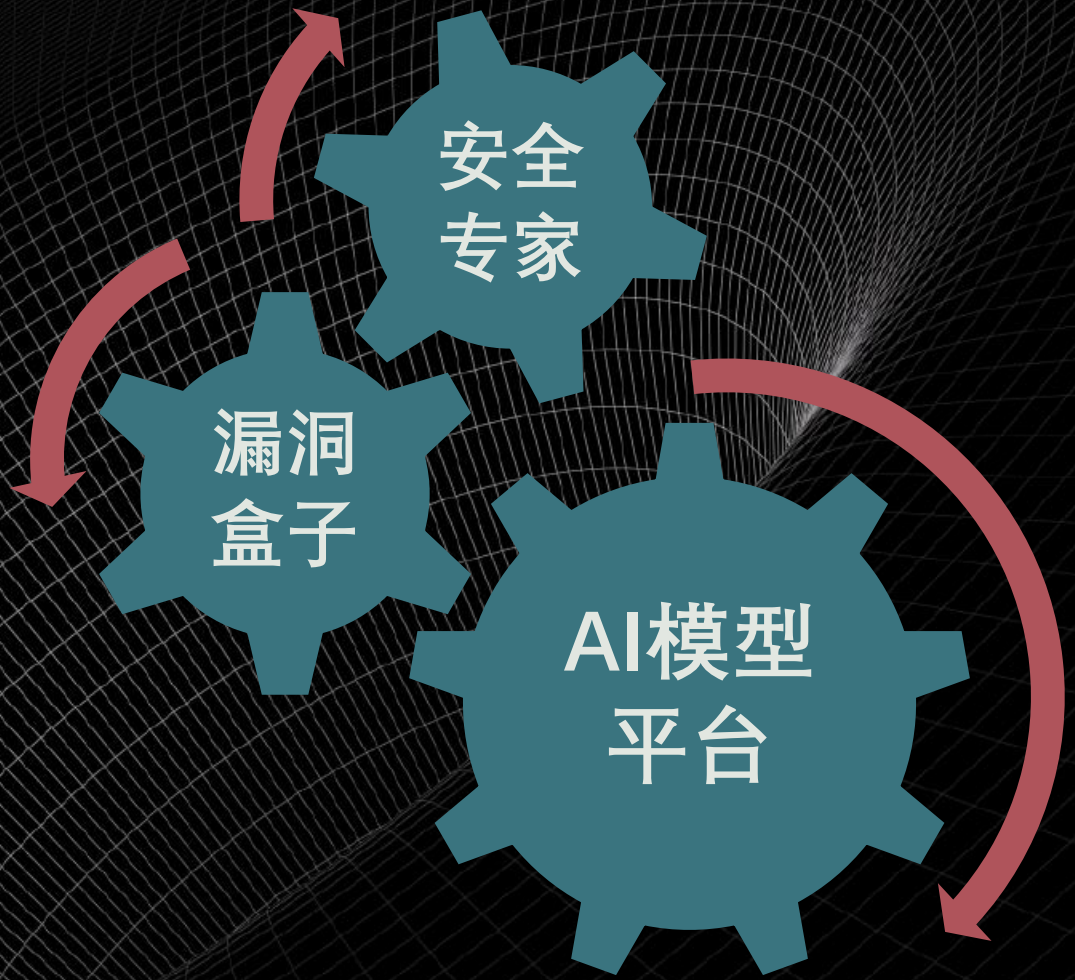
Legend	
APT 28	50
Deep Panda	29
Both	17

网络流量分析

- C&C 连接
- 内部异常访问
- 异常数据传输

文件分析

- 邮件附件
- Web页面下载文件
- 其它文件



监督学习

- DGA检测模型
- DNS隧道检测模型
- 恶意加密流量检测
- ……

非监督学习

- Webshell检测模型
- 异常流量检测模型
- ICMP隧道检测
- ……

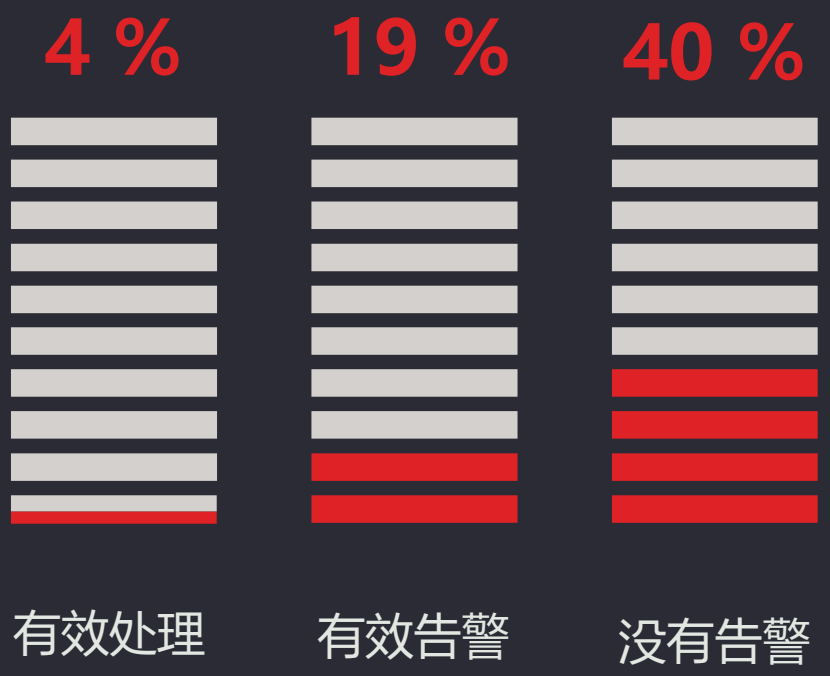
深度学习

- 恶意文件检测模型
- 僵尸网络检测
- 恶意文件家族检测
- ……

困境 | 未知的威胁严峻，防御是与时间赛跑

网络安全创新大会
Cyber Security Innovation Summit

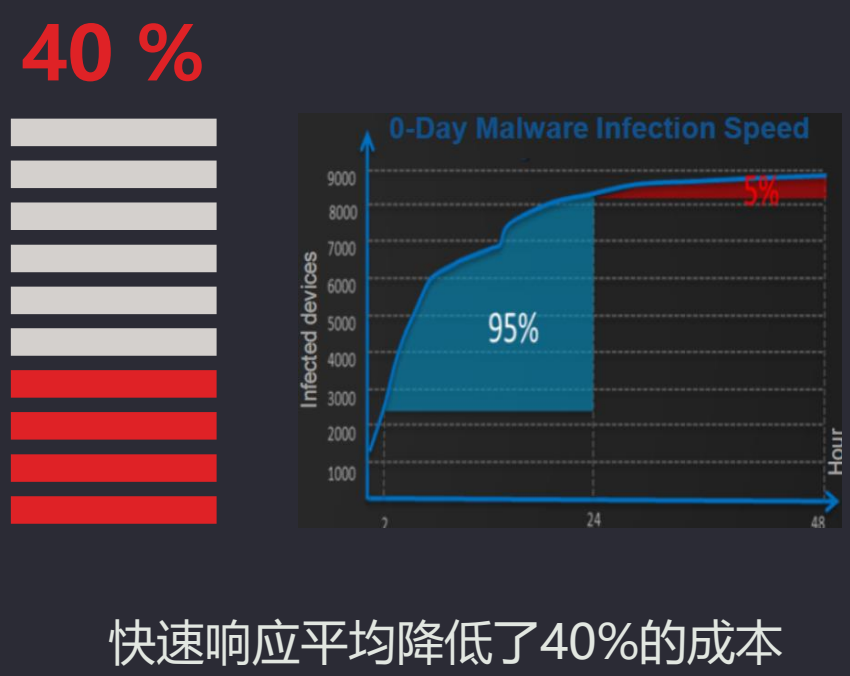
误报造成的平均损失: 每年130万美元



新型攻击：隐蔽 伪装

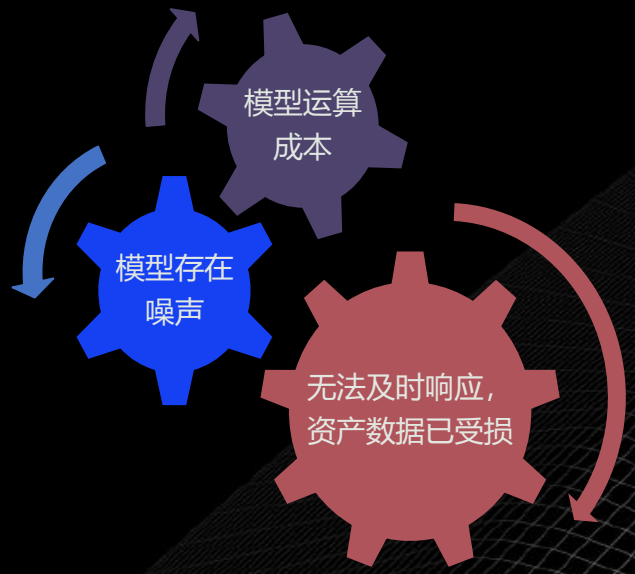
APT 0day 渗透入侵无处不在

反应慢造成的损失: 成本增加40%

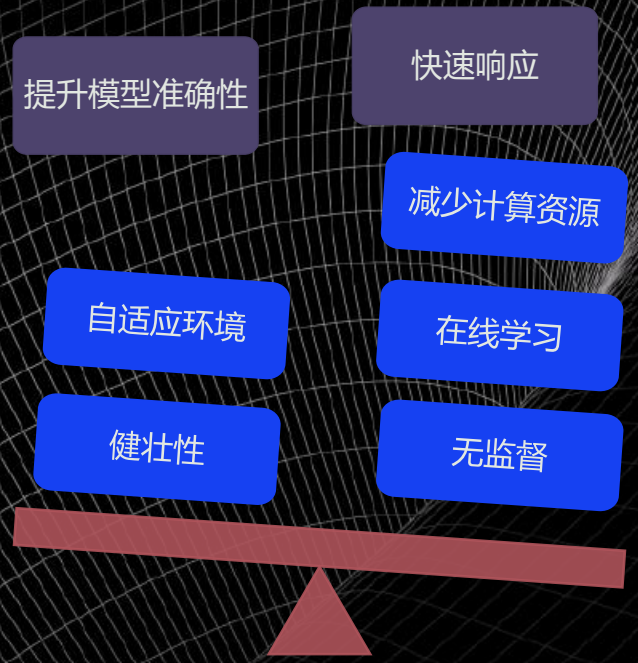


快速响应平均降低了40%的成本

弱智能体



强智能体



部分可观环境

（检测模型存在噪声）

DGA模型 | Webshell模型 | Mysql模型 | 加密流量模型

恶意文件模型 | DNS隧道模型 | ICMP隧道模型

含噪音的AI模型集

计算资源、算力、分析损耗

Observation

Reward

Action

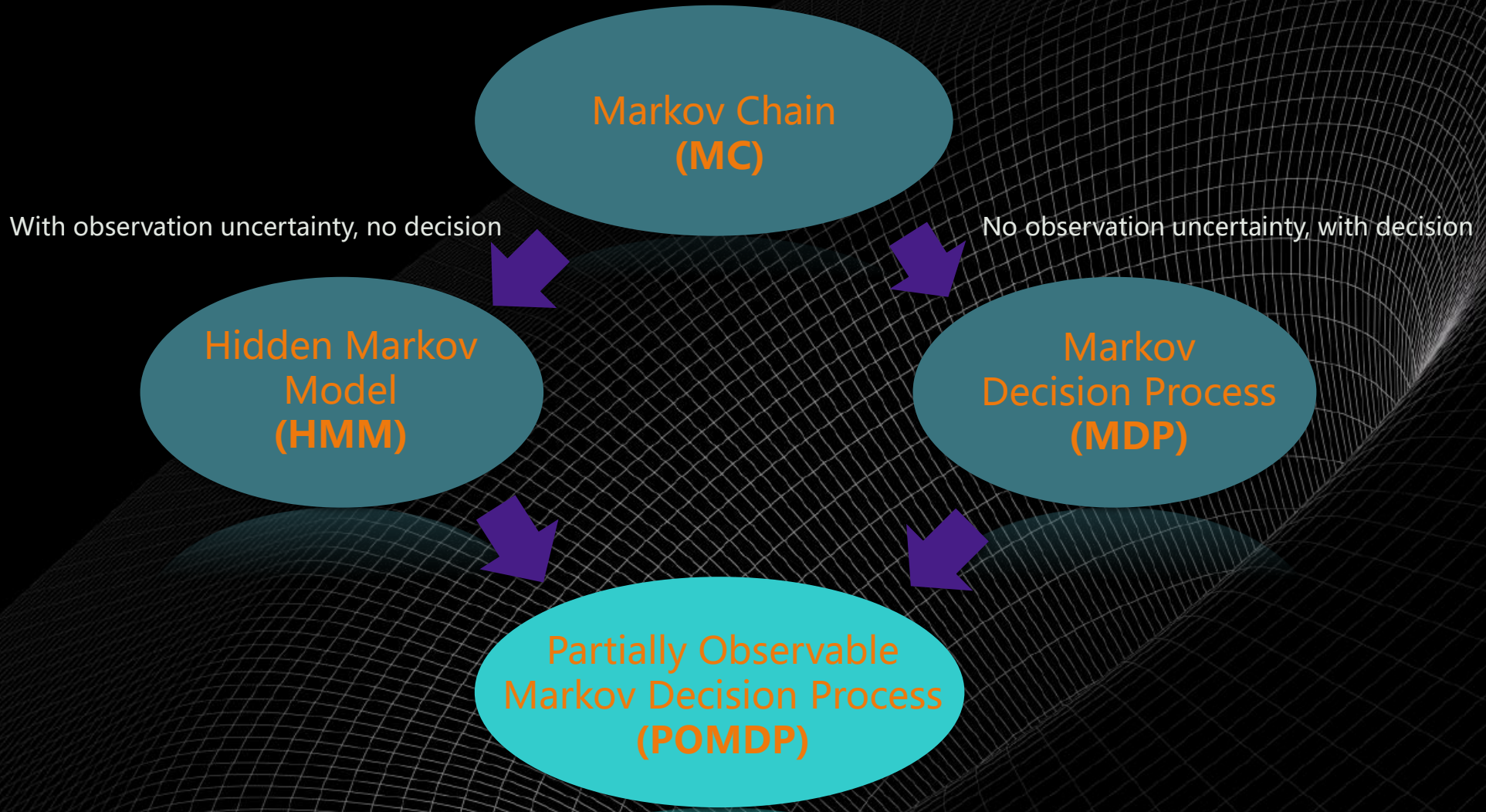
{normal，anomaly}

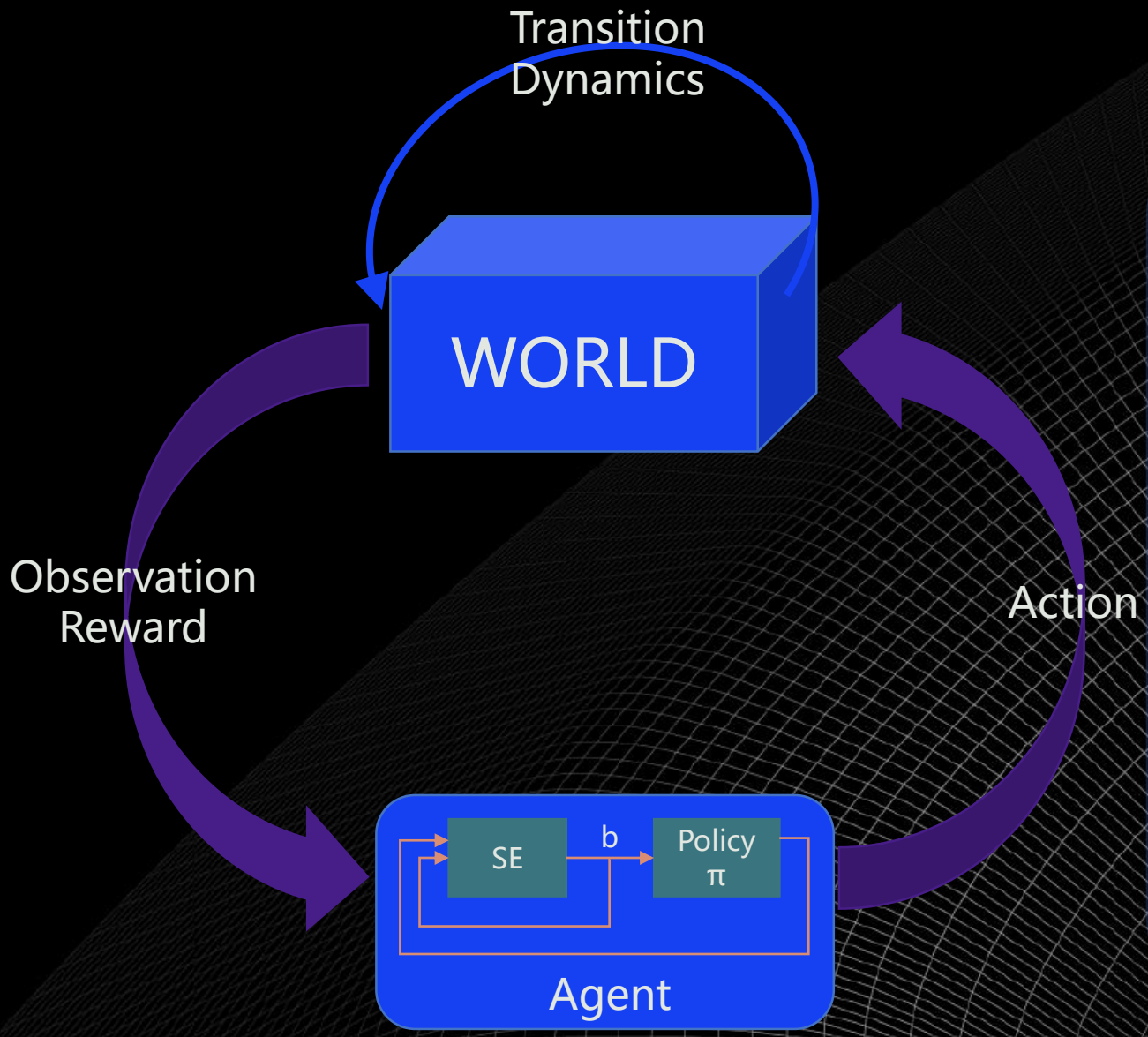
{analyze，block，pass}

State : {blocking，passing}

部分可观马尔可夫决策

马尔可夫模型 | MC HMM MDP POMDP





POMDP 通过六元组（S，A，T，R，Z，O）表示一个序贯决策过程。相对于MDP，智能体并无法直接观察目前状态，必须根据部分区域观测结果推断状态的分布。

- S是有限集，其中s∈S代表一个状态
- A是有限集，其中a∈A代表一个行动
- T：S×A→Π(S)称为状态转移函数，用T(s, a, s’)表示在状态s上执行a达到s’的概率P(s’|s, a)
- R：S×A→R称为回报函数，R(s, a)表示在s上执行行动a所得即时回报
- Z是一个有限集，z∈Z代表一个观察
- O：S×A→Π(Ω)称为观察函数，O(s’，a, z)表示执行a达到s’观察到z的概率P(z|s’，a)

Agent通过维持一个信度状态b来对其历史进行总结，b_0代表初始信度状态。

$$b_t(s) = \Pr(s_t = s | z_t, a_{t-1}, z_{t-1}, \ldots a_0, b_0)$$

$$B(s) = \{b(s_0), b(s_1), b(s_2), \ldots, b(s_n), b(s_p)\}$$

对于一个给定策略，在初始信念状态下，按策略π执行动作得到累计代价值为：

$$V_\pi(b) = R(b, a(\pi)) + \gamma \sum_{z \in Z} P(z|b, a(\pi)) V_{\pi(z)}(b_a^z)$$

其中，

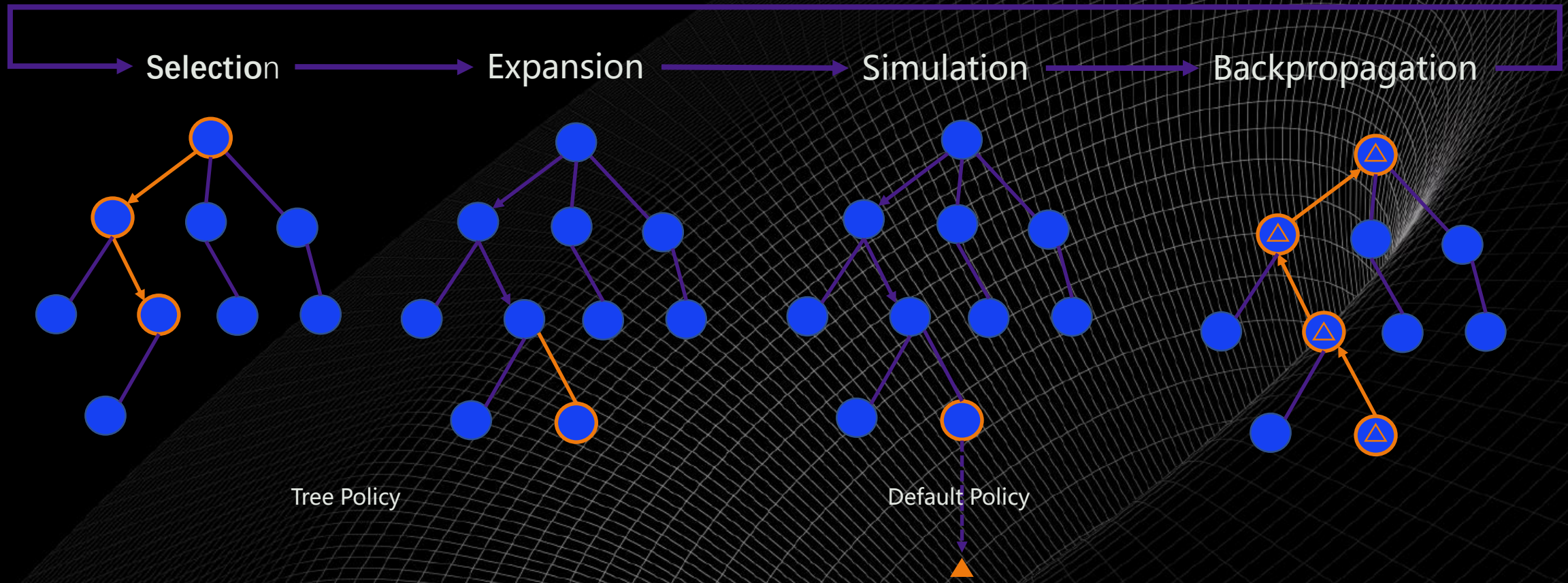
$$R(b, a(\pi)) = \sum_{s \in S} b(s) R(s, a(\pi)) \qquad P(z|b, a(\pi)) = \sum_{s \in S} b(s) \sum_{s' \in S} b(s) T(s', s, a(\pi))\, O(z, a(\pi), s')$$

POMDP模型目标是求解使累计代价值最小的最优策略π*，即∀b，∀π有下式成立：

$$V_{n+1}^*(b) \le V_{n+1}^\pi(b)$$

求出POMDP决策模型为：

$$V_{n+1}(b) = \min_{a \in A} \left\{ \sum_{s \in S} b(s) R(s, a) + \gamma \sum_{z \in Z} \sum_{s \in S} b(s) \sum_{s' \in S} b(s) T(s', s, a) O(z, a, s') V_n(b') \right\}$$


Selection
Expansion
Simulation
Backpropagation
Tree Policy
Default Policy

攻击行为

Internet

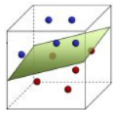
- 通过邮件附件、漏洞利用、植入后门等方式感染主机
- 与远端C&C服务器连接获取控制命令
- 窃取凭证，提升系统权限，感染其他主机
- 数据收集
- 数据传递

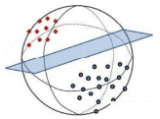
日志

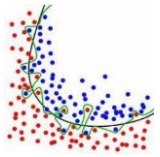
协议

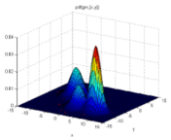
沙箱

情报









检测模型（弱AI）

渗透

- Webshell模型
- 恶意文件模型

C&C连接

- DGA模型
- C2服务端模型

横移感染

- 横移检测模型
- UEBA

命令执行

- 隐蔽隧道检测
- 僵尸网络模型

传输

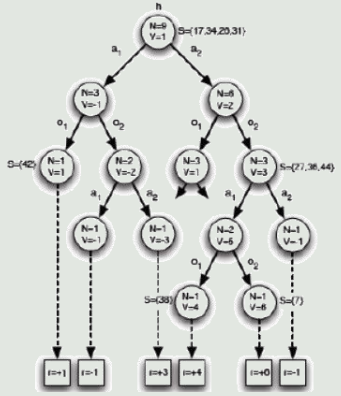
- 恶意加密流量模型

POMDP（强AI）

World
(S, A, T, R, Z, O)

观察值/奖惩

动作



Agent

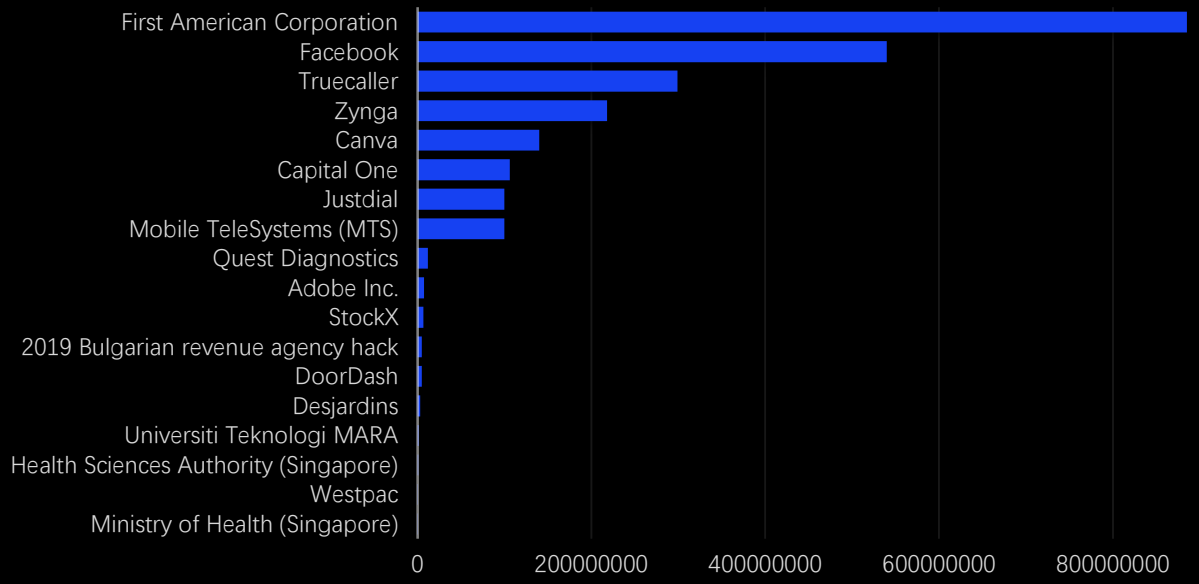
案例介绍

Data Exfiltration 检测和抵御

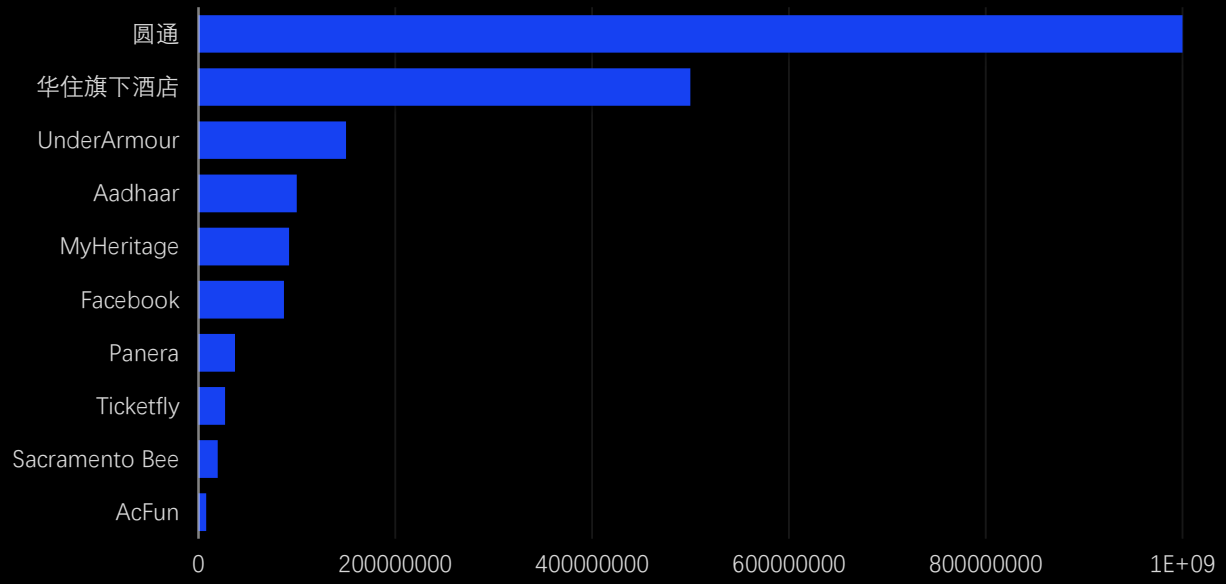
近几年数据泄露事件

网络安全创新大会
Cyber Security Innovation Summit

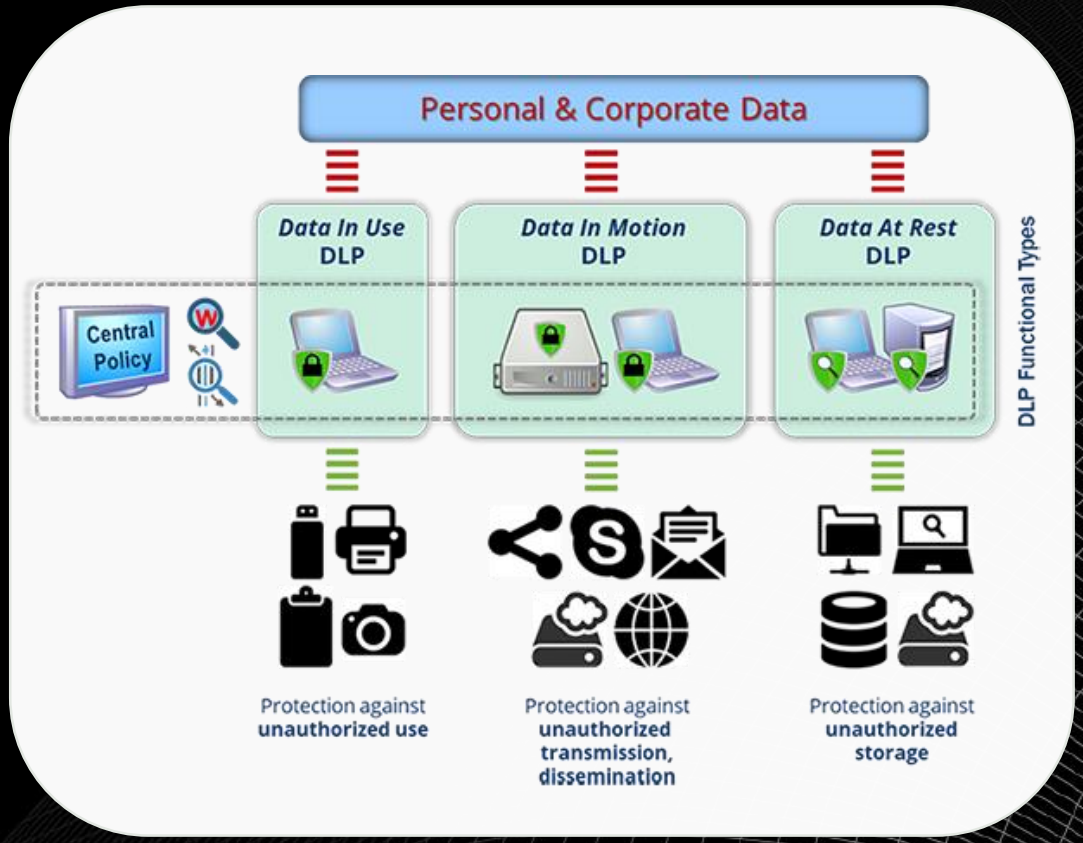
2019年 企业数据泄露统计



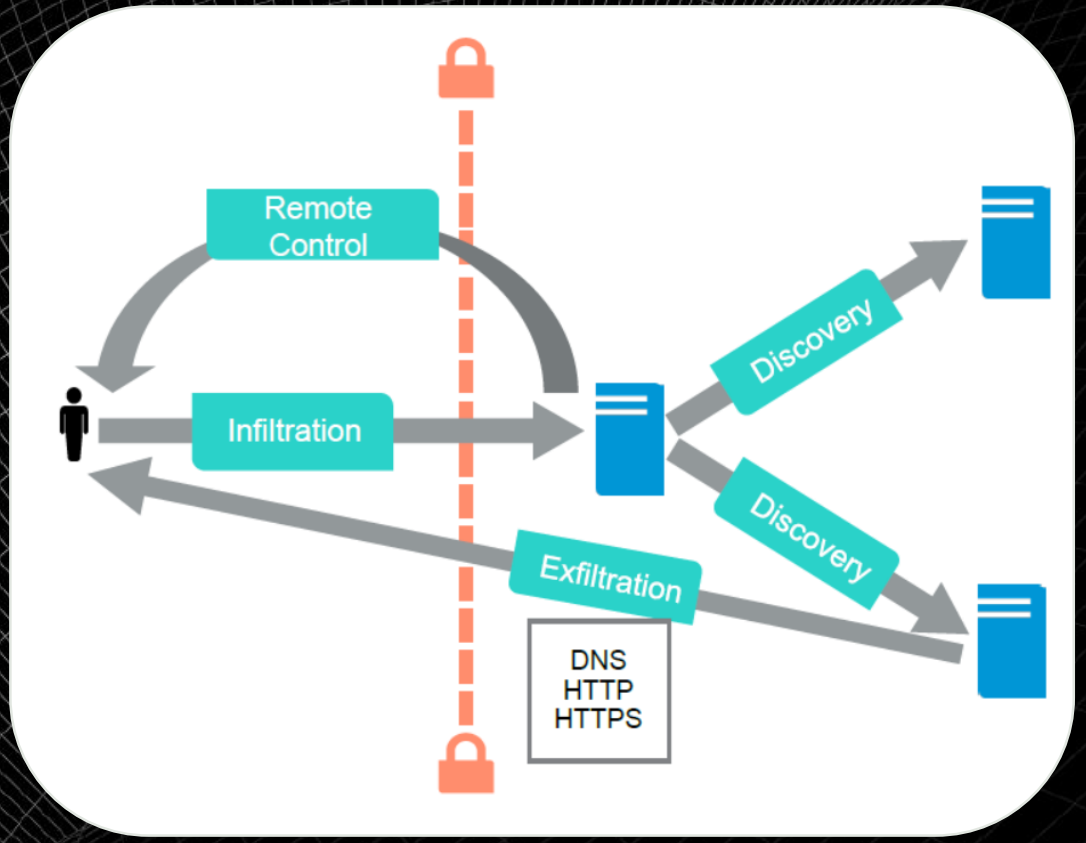
2018年 企业数据泄露统计



以前


Personal & Corporate Data
Data In Use DLP
Data In Motion DLP
Data At Rest DLP
Central Policy
DLP Functional Types
Protection against unauthorized use
Protection against unauthorized transmission, dissemination
Protection against unauthorized storage

现在


Remote Control
Infiltration
Discovery
Discovery
Exfiltration
DNS
HTTP
HTTPS

Data Exfiltration | Hidden Tunnel

Command and Control
External Remote Access
Hidden DNS Tunnel
Hidden HTTP/S Tunnel
Suspicious Relay
Suspect Domain Activity
Malware Update
Peer-to-Peer
Pulling Instructions
Suspicious HTTP
Stealth HTTP Post
TOR Activity
Threat Intel Match

Reconnaissance
Internal Darknet Scan
Port Scan
Port Sweep
SMB Account Scan
Kerberos Account Scan
File Share Enum
Suspicious LDAP Query
RDP Recon
RPC Recon

Lateral Movement
Suspicious Remote Exec
Suspicious Remote Desktop
Suspicious Admin
Shell Knocker
Automated Replication
Brute-Force Attack
SMB Brute-Force
Kerberos Brute Force
Suspicious Kerberos Client
Suspicious Kerberos Account
Kerberos Server Activity
Ransomware File Activity
SQL Injection Activity

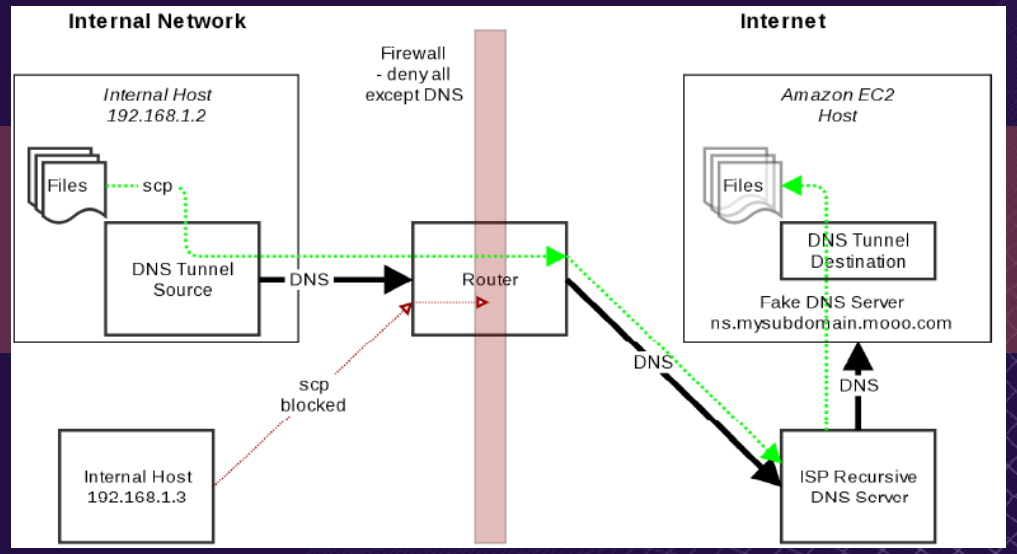
Exfiltration
Data Smuggler
Smash and Grab
Hidden DNS Tunnel
Hidden HTTP/S Tunnel

Botnet Monetization
Abnomal Web or Ad Activity
Cryptocurrency Mining
Brute-Foce Attack
Outbound DoS
Outbound Port Sweep
Outbound Spam

AI模型 | 基于机器学习的DNS隐蔽隧道检测模型

网络安全创新大会 Cyber Security Innovation Summit

通过DNS隧道攻击

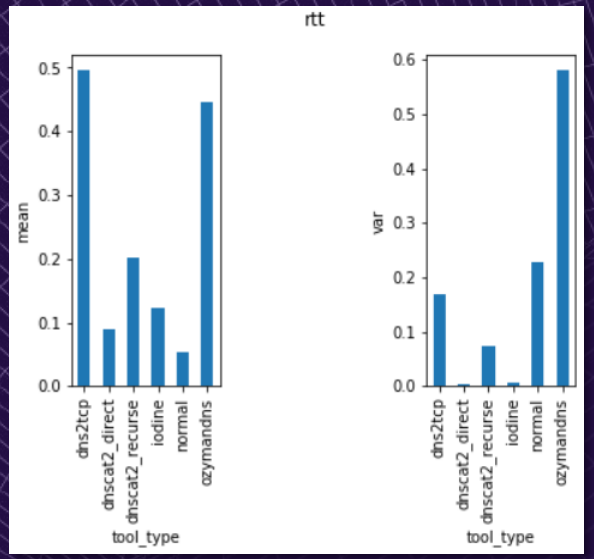


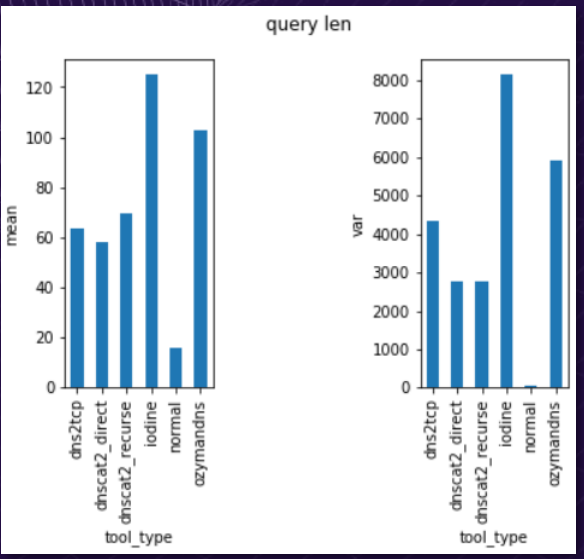
查询域名举例：

0ufb582¾xgcxýaabacuqa4xzÒabagdvó¿asfsicÞykîa
wrÐfßêÚÀxçÞdahixça.aaqigu×mÒdëàecflÉrupÁÔÊ
ÇciÕkhÏnyryÔfðÅ7dëlÃÄk6pvcÇlqvïdzh.2hÕsÐíøëe
mßét÷üÙëÅaah3å÷àw÷ß2ròa.log.riskivy.info

监督学习方式
DNS隧道数据流量316268对
正常数据流量320677对
使用随机森林算法，检测准确度>95%

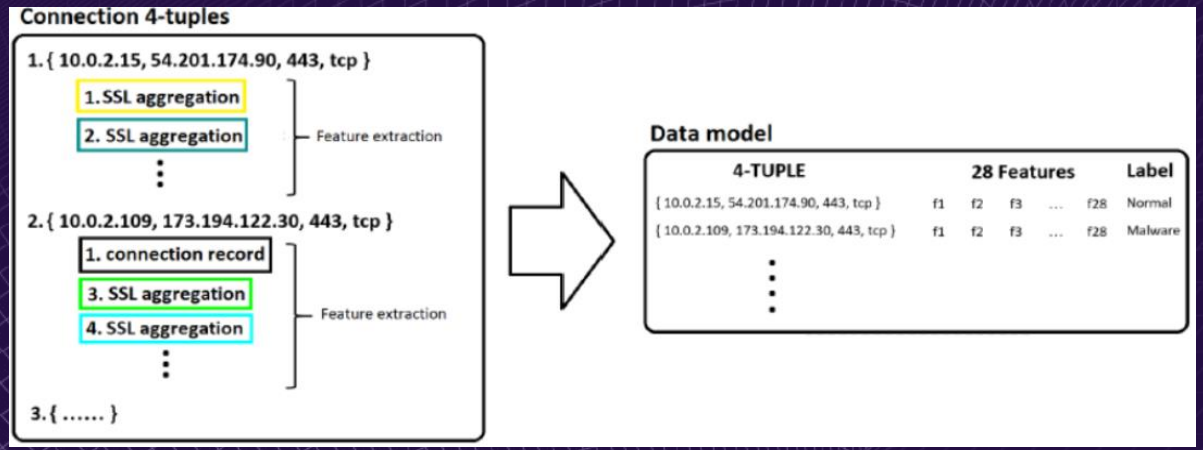
特征：响应时间间隔平均值和方差；查询域名长度平均值和方差；应答段长度平均值和方差；查询子域名各字符信息熵平均值和方差；查询类型频率



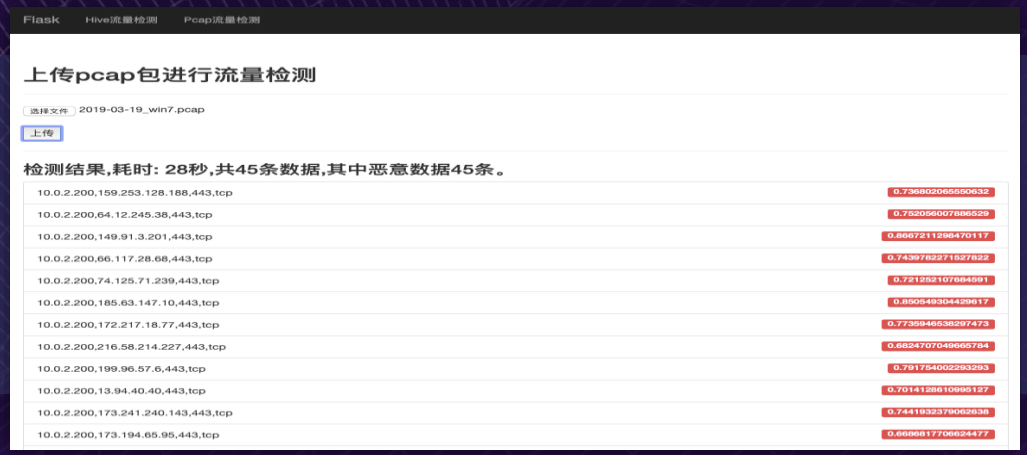


AI模型 | 基于机器学习的恶意HTTPS流量检测模型

网络安全创新大会
Cyber Security Innovation Summit



- 解析流量生成，conn.log、ssl.log、x509.log
- 连接四元组（SrcIP，DstIP，DstPort，协议）
- SSL聚合（一个连接记录、一个SSL记录、一个证书记录）
- 连接记录是非ssl的Connection .log中的连接记录
- 包含28特征（SSL聚合和连接记录的数量、持续时间均值...）



POMDP模型 | 针对 Data Exfiltration 设计

Data Exfiltration POMPD模型是一个具有状态空间S、动作空间A、状态转移T、观测空间Z、观测概率O和报酬函数R的元组（S，A，T，Z，O，R）

- 状态空间定义

$S = \{S_{blocking}, S_{passing}\}$ 阻止态、放行态

- 动作空间定义

$A = \{A_{analyze}, A_{block}, A_{pass}\}$ AI模型分析、阻止、放行

- 观察空间定义

$Z = \{Z_{regular}, Z_{tunnel}\}$ 合法流量、隧道流量

POMDP模型 | 针对 Data Exfiltration 设计

Data Exfiltration POMPD模型是一个具有状态空间S、动作空间A、状态转移T、观测空间Z、观测概率O和报酬函数R的元组（S，A，T，Z，O，R）

- 状态转移函数定义

$$T(s',a)=\begin{cases}1, & s' \in S, a = A_{analyze} \\ \frac{1}{|S|}, & s' \in S, a = A_{pass} \\ \frac{1}{|S|}, & s' \in S, a = A_{block}\end{cases}$$

当前状态下，执行动作a，转移到s’概率

- 观察概率函数定义

$$O(z|s,a)=\begin{cases}Q, & z = Z_{regular}|s = S_{passing} a = A_{analyze} \\ 1-Q, & z = Z_{regular}|s = S_{passing} a = A_{analyze} \\ Q, & z = Z_{regular}|s = S_{blocking} a = A_{analyze} \\ 1-Q, & z = Z_{tunnel}|s = S_{blocking} a = A_{analyze} \\ \frac{1}{|Z|}, & otherwise\end{cases}$$

状态s下，执行动作a，获得观察值z概率

Q指代AI模型准确率

POMDP模型 | 针对 Data Exfiltration 设计

Data Exfiltration POMPD模型是一个具有状态空间S、动作空间A、状态转移T、观测空间Z、观测概率O和报酬函数R的元组（S，A，T，Z，O，R）

- 报酬函数定义

$$R(s,a)=\begin{cases} L, & s=S_{passing}, a=A_{pass} \\ L, & s=S_{blocking}, a=A_{block} \\ 1-L, & s=S_{blocking}, a=A_{pass} \\ L-1, & s=S_{passing}, a=A_{block} \\ \frac{L}{C}, & s\in S, a=A_{analyze} \end{cases}$$

状态s下，执行动作a，获得的即刻回报

L指代网络安全等级，C指代模型计算开销

- 在线求解

部分可观的蒙特卡洛搜索树算法

POMCP

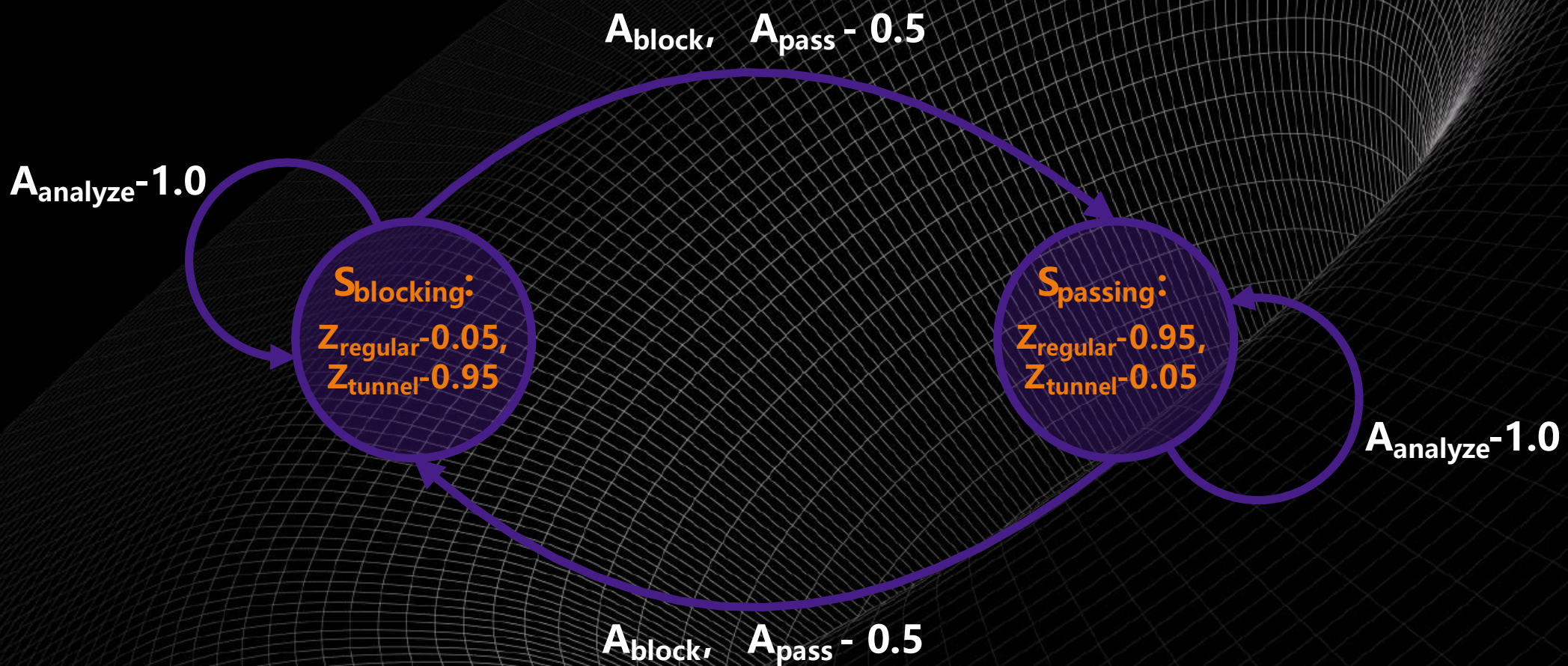
网络安全创新大会
Cyber Security Innovation Summit

DNS隧道检测

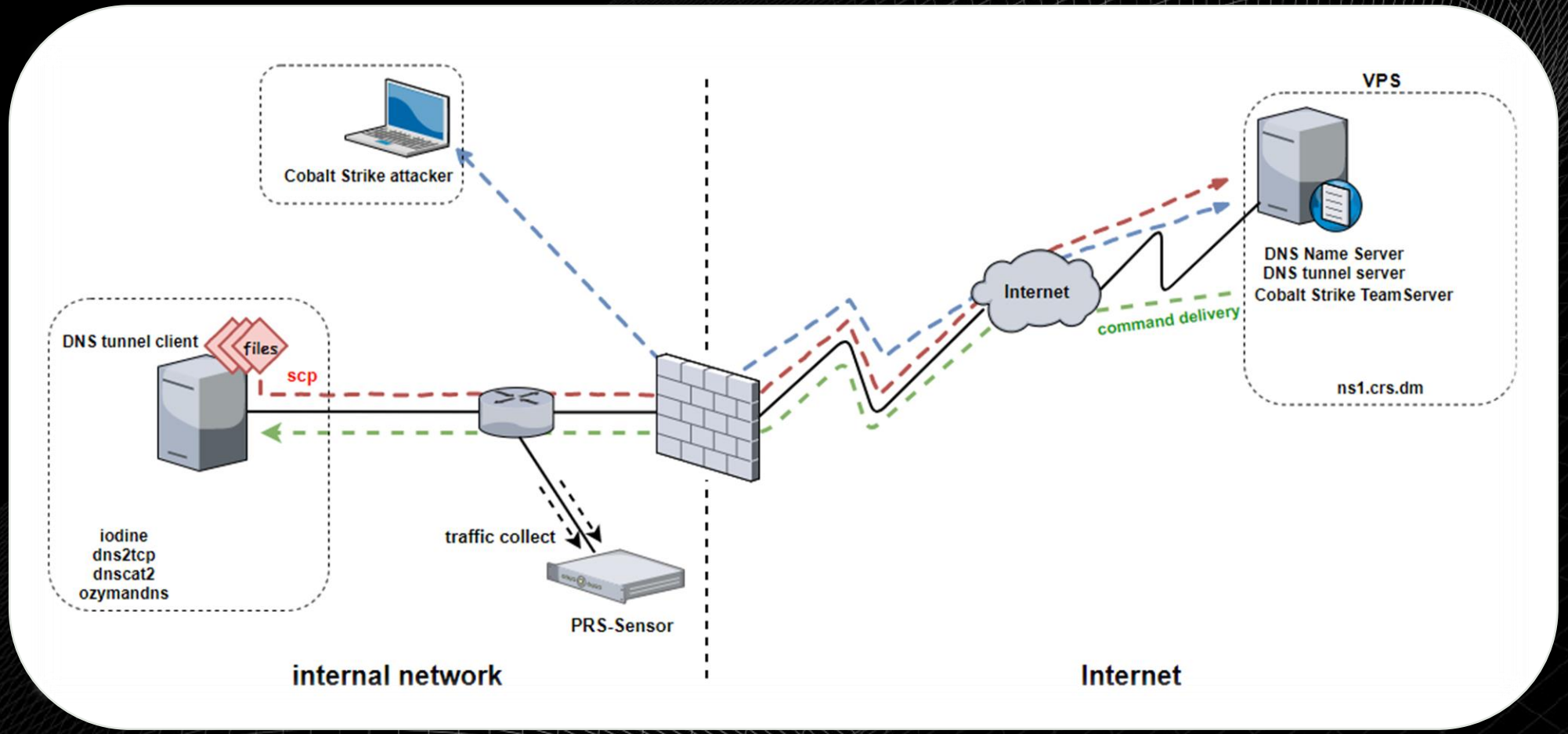
基于POMDP决策强化

超参数设置：

- 基于ML的DNS隧道检测器准确率Q=0.95
- 模型计算开销C=1.28



内网搭建攻击环境，使用多种工具（iodine、dns2tcp、dnscat2、ozymandns）模拟攻击过程



问题：传统基于ML的APT攻击检测模型存在噪音、处理响应慢、耗费资源等

手段：部分可观马尔可夫决策 + 蒙特卡洛搜索树

结果：模拟实验，验证方法可行

CIS 网络安全创新大会
Cyber Security Innovation Summit

THANKS

孟雷

斗象科技高级机器学习专家