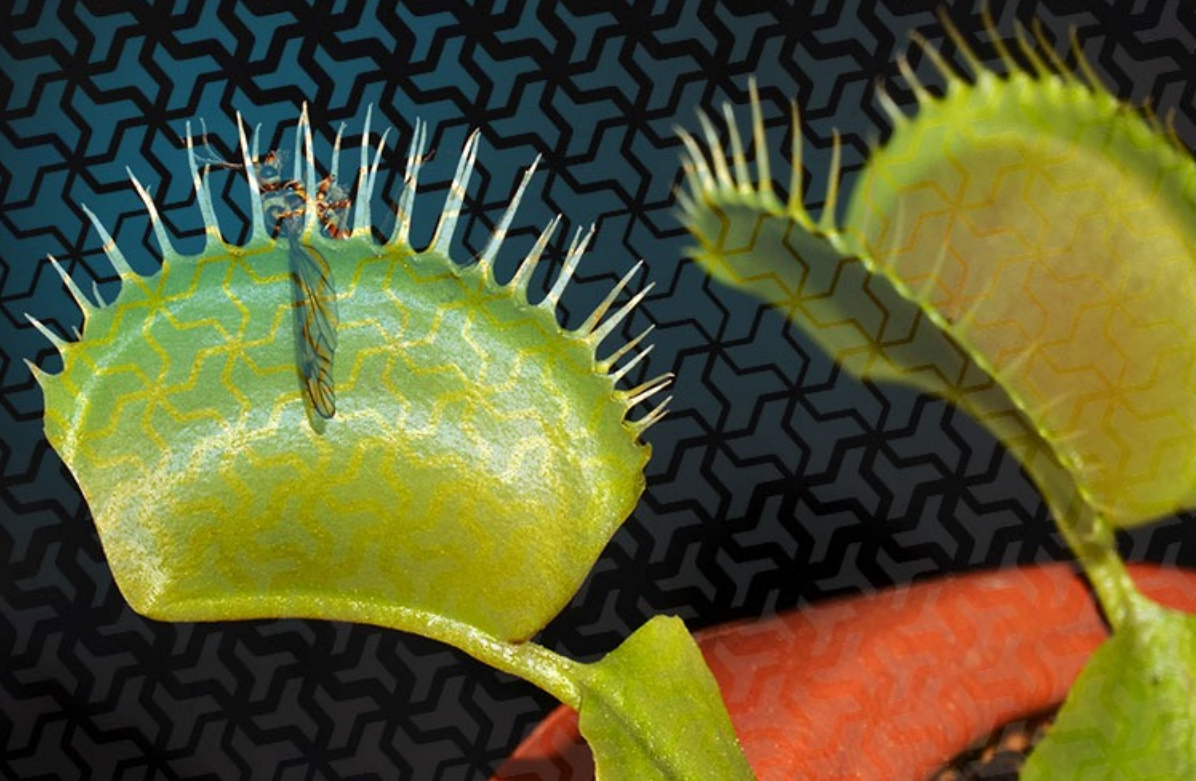
A Game between Adversary and AI Scientist

Satnam, Arunabha, Deepak,
Waseem, Nirmesh, Santosh,
Balamurali, Narayana
Acalvio Technologies

NULLCON
March 3, 2018



Who am I

- At Acalvio from **Day 1**
- 15+ Years in DS, ML, AI
- General Motors, Samsung Research, CA Technologies
- Author- Patents, Tech Pubs and Tech Talks
- Rock Climber

Outline

- Define the Problem
- A possible solution - research work
- Demos
- Under the hood

Problem

Can we play a game with adversary?

Can we engage with adversary?

Is adversary visible to defender?

- Extensive reconnaissance of target and defender

- Using the same tools and techniques as defender

Is he a “Returning” Adversary?

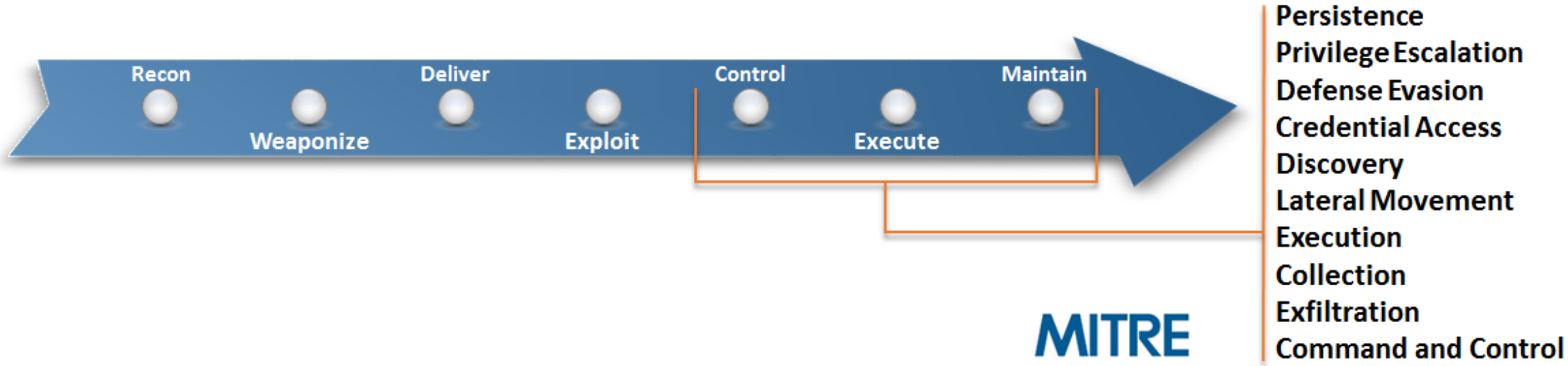
—> Compare Tools, Tactics and Procedures (TTPs)

InfoSec Game: Assumptions

- Unlike Chess, cyber game has infinite state space

—> Use Mitre ATT@CK model to define the state space

Adversary Tactics



Mitre ATT@CK Model

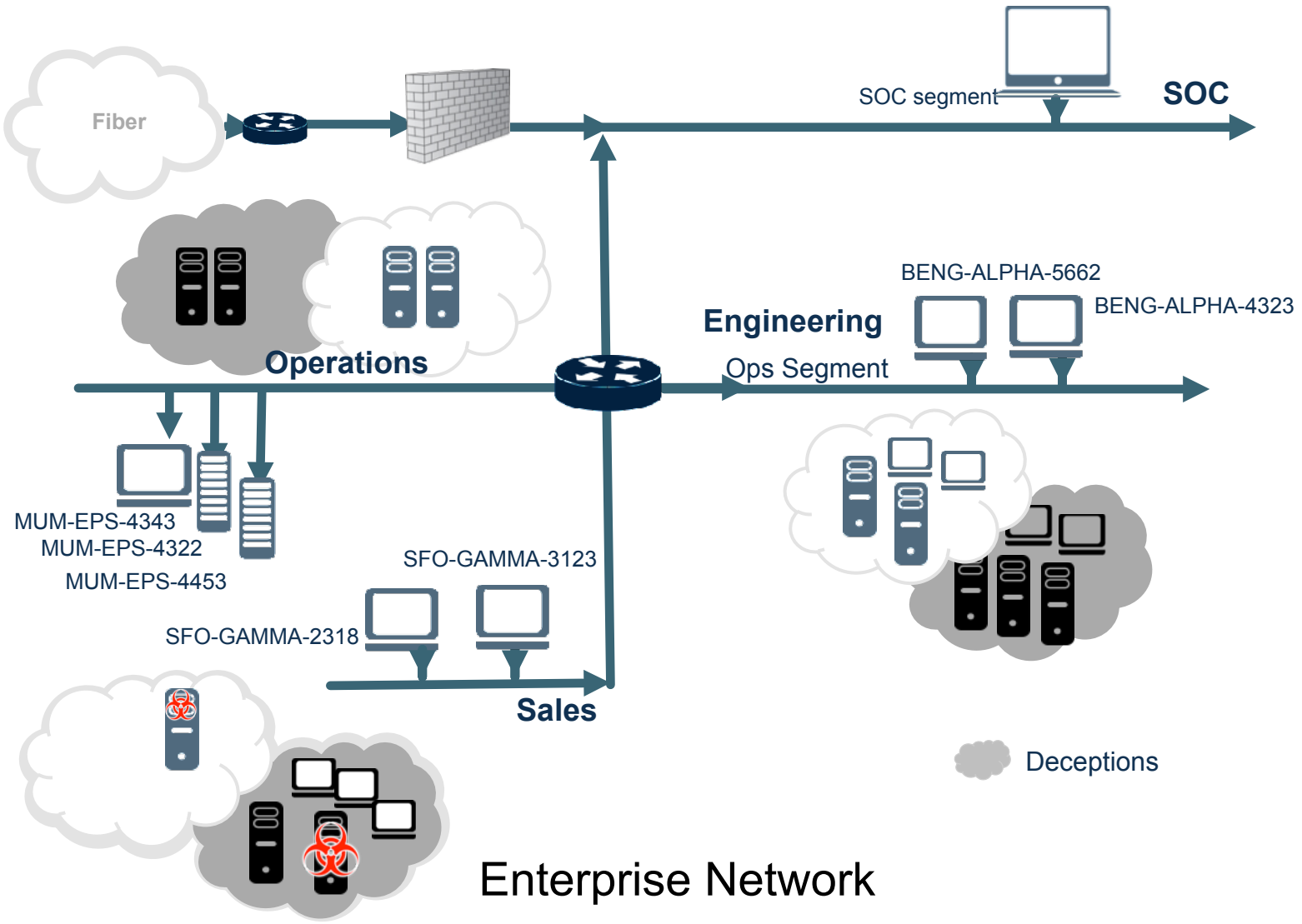
APT 1
APT 18
APT 28
APT 29
APT 30

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Legitimate Credentials			Credential Dumping	Account enumeration	Application deployment software	Command Line	Commonly used port	Automated or scripted exfiltration
Accessibility Features		Binary Padding	Credentials in Files	File system enumeration	Exploitation of Vulnerability	File Access	Comm through removable media	Data compressed
AddMonitor		DLL Side-Loading	Network Sniffing	Group permission enumeration	Logon scripts	PowerShell	Custom application layer protocol	Data encrypted
DLL Search Order Hijack		Disabling Security Tools	User Interaction	Local network connection enumeration	Pass the hash	Process Hollowing	Custom encryption cipher	Data size limits
Edit Default File Handlers		File System Logical Offsets		Local networking enumeration	Pass the ticket	Registry	Data obfuscation	Data staged
New Service		Process Hollowing		Operating system enumeration	Peer connections	Rundll32	Fallback channels	Exfil over C2 channel
Path Interception		Bypass UAC		Owner/User enumeration	Remote Desktop Protocol	Scheduled Task	Multiband comm	Exfil over alternate channel to C2 network
Scheduled Task		DLL Injection		Process enumeration	Windows management instrumentation	Service Manipulation	Multilayer encryption	Exfil over other network medium
Service File Permission Weakness		Indicator blocking on host		Security software enumeration	Windows remote management	Third Party Software	Peer connections	Exfil over physical medium
Shortcut Modification		Indicator removal from tools		Service enumeration	Remote Services		Standard app layer protocol	From local system
BIOS	Exploitation of Vulnerability	Indicator removal from host		Window enumeration	Replication through removable media		Standard non-app layer protocol	From network resource
Hypervisor Rootkit		Masquerad-ing			Shared webroot		Standard encryption cipher	From removable media
Logon Scripts		NTFS Extended Attributes			Taint shared content		Uncommonly used port	Scheduled transfer
Master Boot Record		Obfuscated Payload			Windows admin shares			
Mod. Exist'g Service		Rootkit						
Registry Run Keys		Rundll32						
Serv. Reg. Perm. Weakness		Scripting						
Windows Mgmt Instr. Event Subsc.		Software Packing						
Winlogon Helper DLL								

Defender’s Tools are at Perimeter

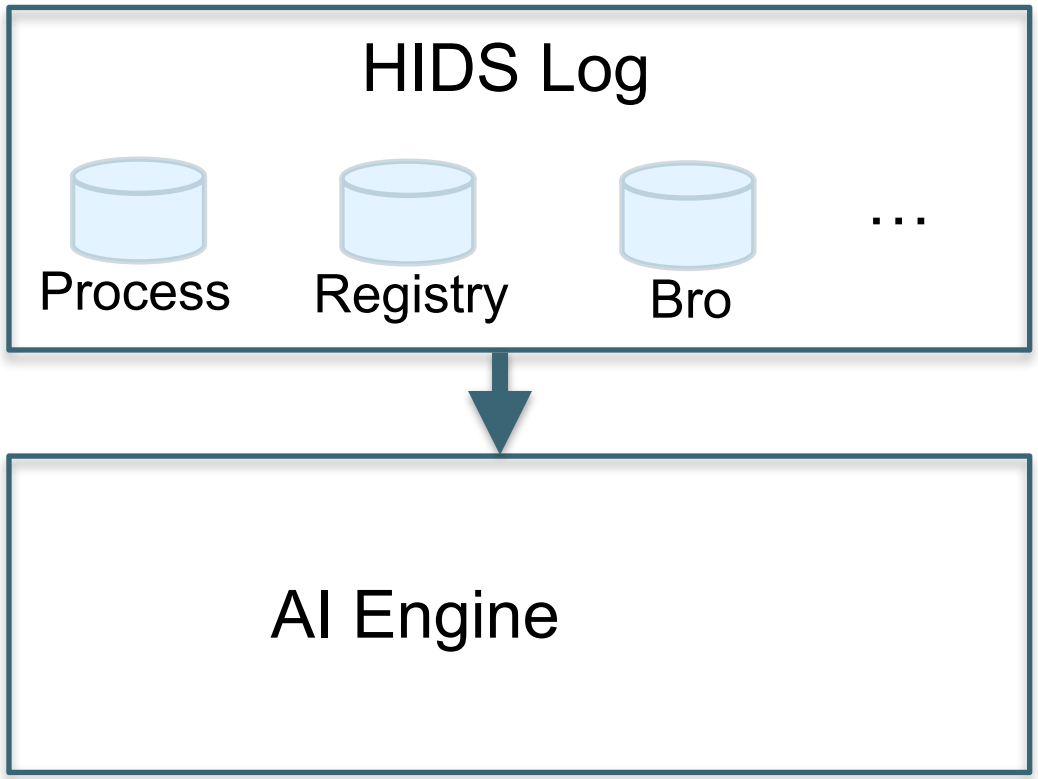
Need new tools to detect adversary INSIDE the NETWORK

Deceptions in Enterprise



- **Deceptions (D)**
- Emulations of Hosts, Applications, Database Servers, etc.
- Real VM Hosts, Applications, etc.
- Browser Cookies, Registry entries, etc.
- Vulnerability in OS/ Application, Shares, etc.

AI Engine



Game: Demos

1: Recon - nmap

Adversary

- Adversary performs recon and nmap to find out to the neighbourhood

Defender

- Defender detects it and provides a few RDP credentials on the endpoints

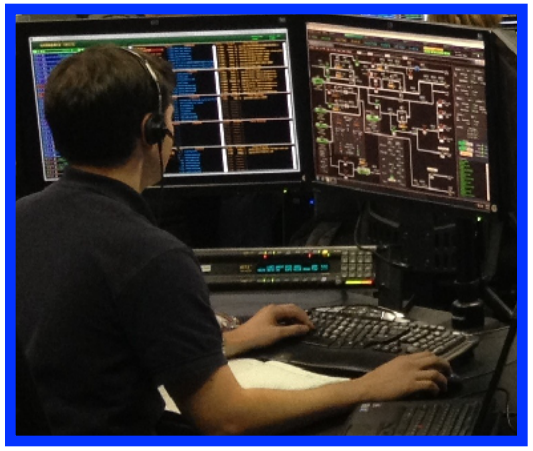
Demo>>

2: Obfuscated PowerShell Script

Adversary

- Adversary obfuscates PowerShell attack and executes in another host

Defender



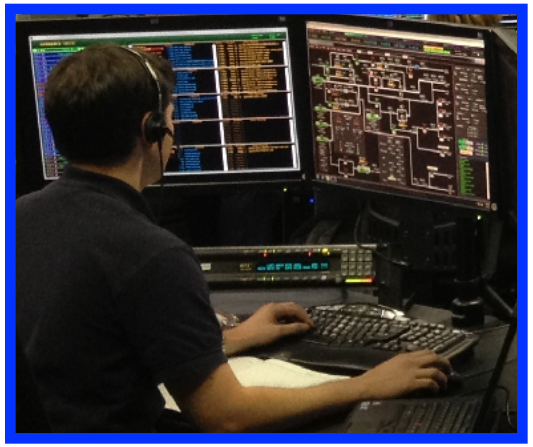
- Defender detects obfuscated PowerShell commands

Demo>>

3: Credentials Dump using PowerSploit and Mimikatz

Adversary

Defender



- Attacker dumps credentials using PowerSpoit and Mimikartz

- Defender detects PowerSploit and Mimikartz activities

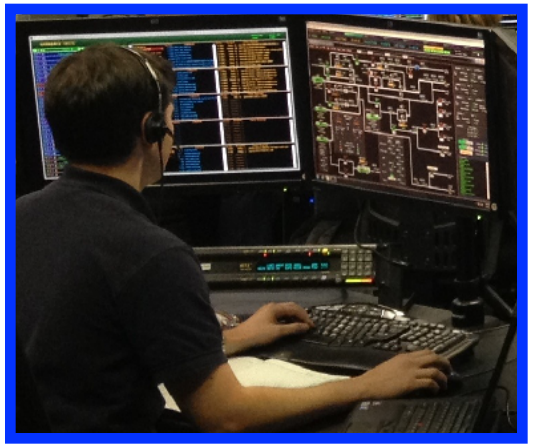
Demo>>

4: Data Exfilteration via DNS Tunnel

Adversary

- Adversary uses DNS Tunnel using DNSCat2 to exfiltrate the credentials

Defender

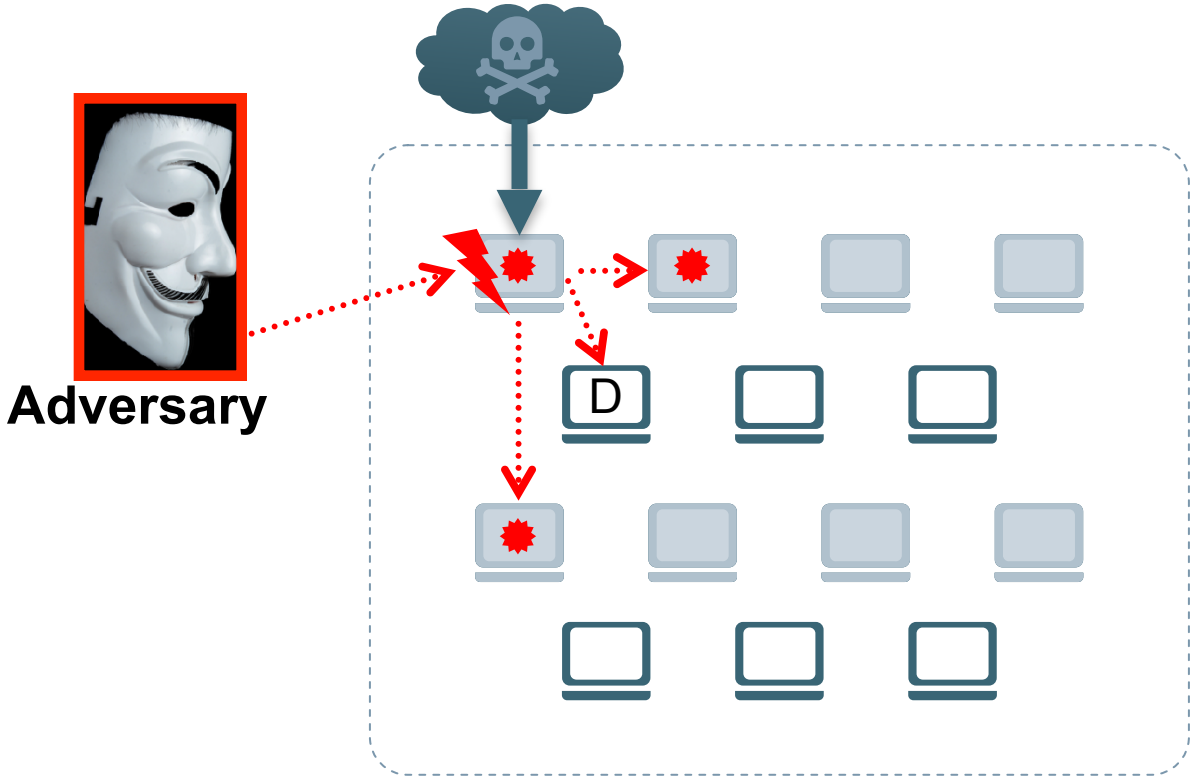


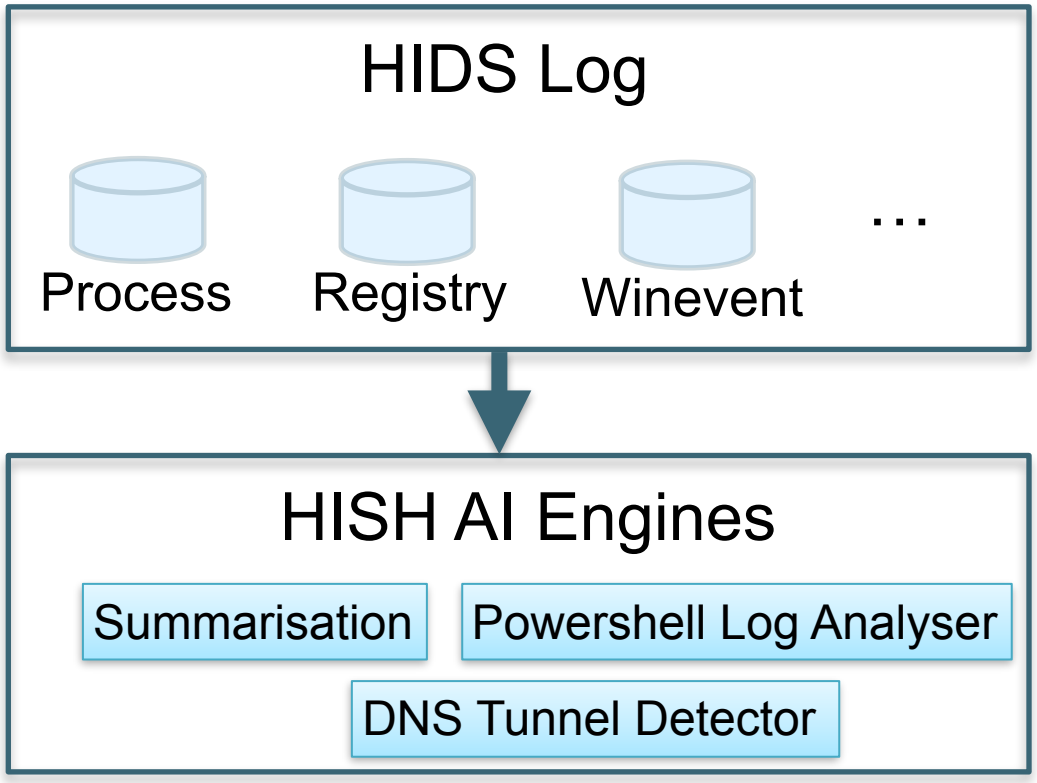
- Defender detects the DNS tunnel using AI

Demo>>

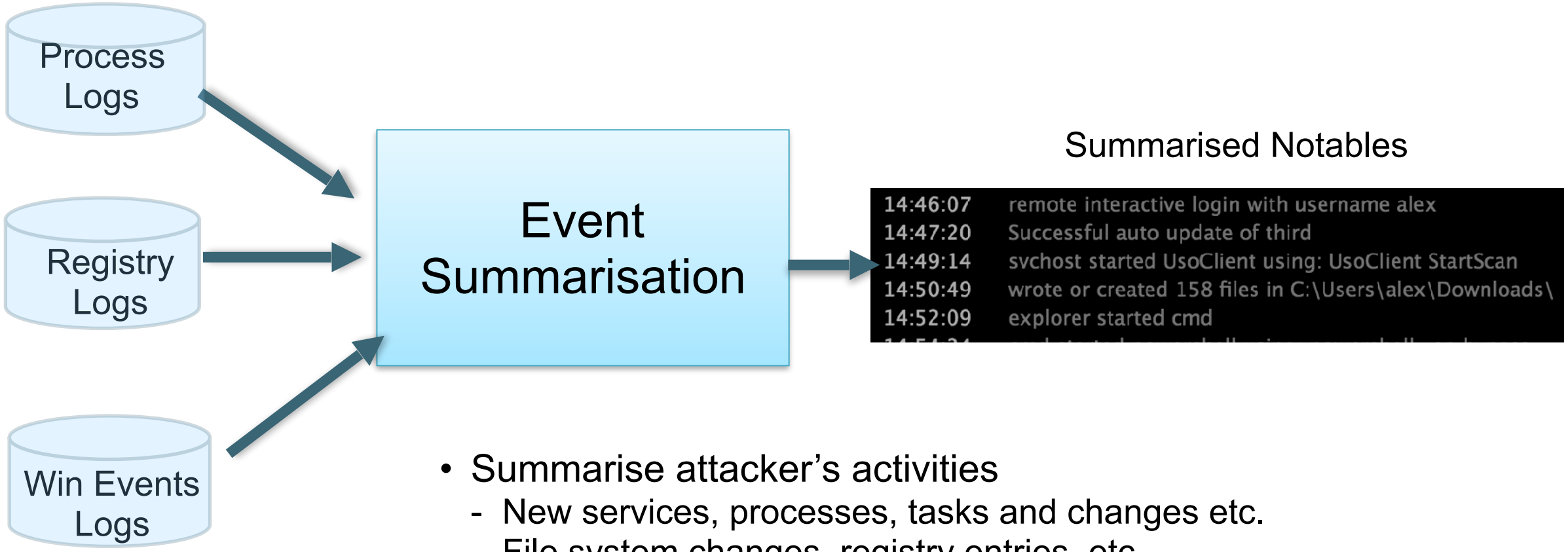
Under the Hood

High Interaction AI Engine



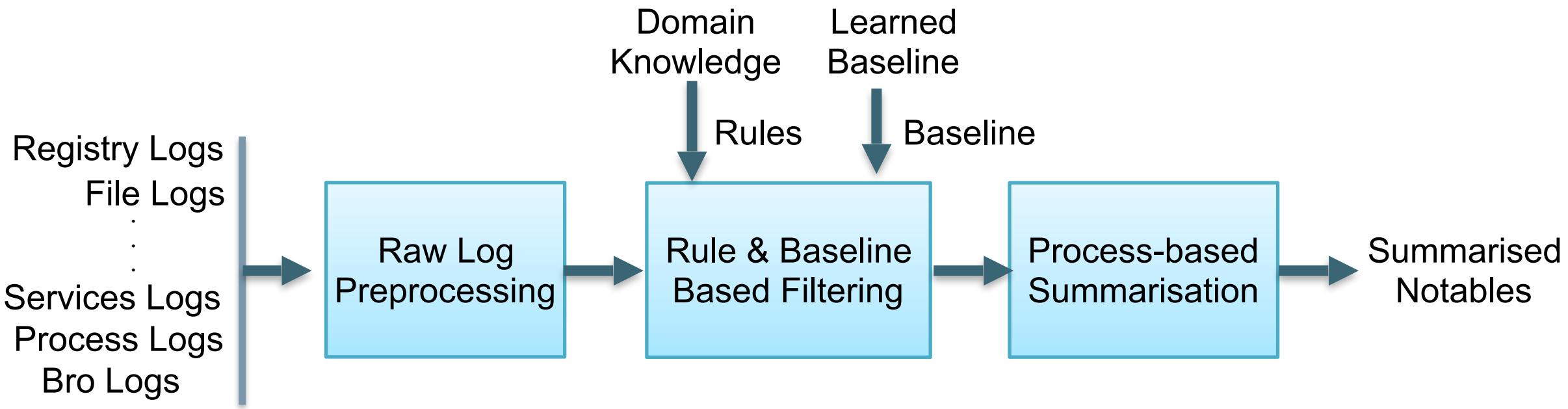


HISH AI: HIDS Log Summarisation



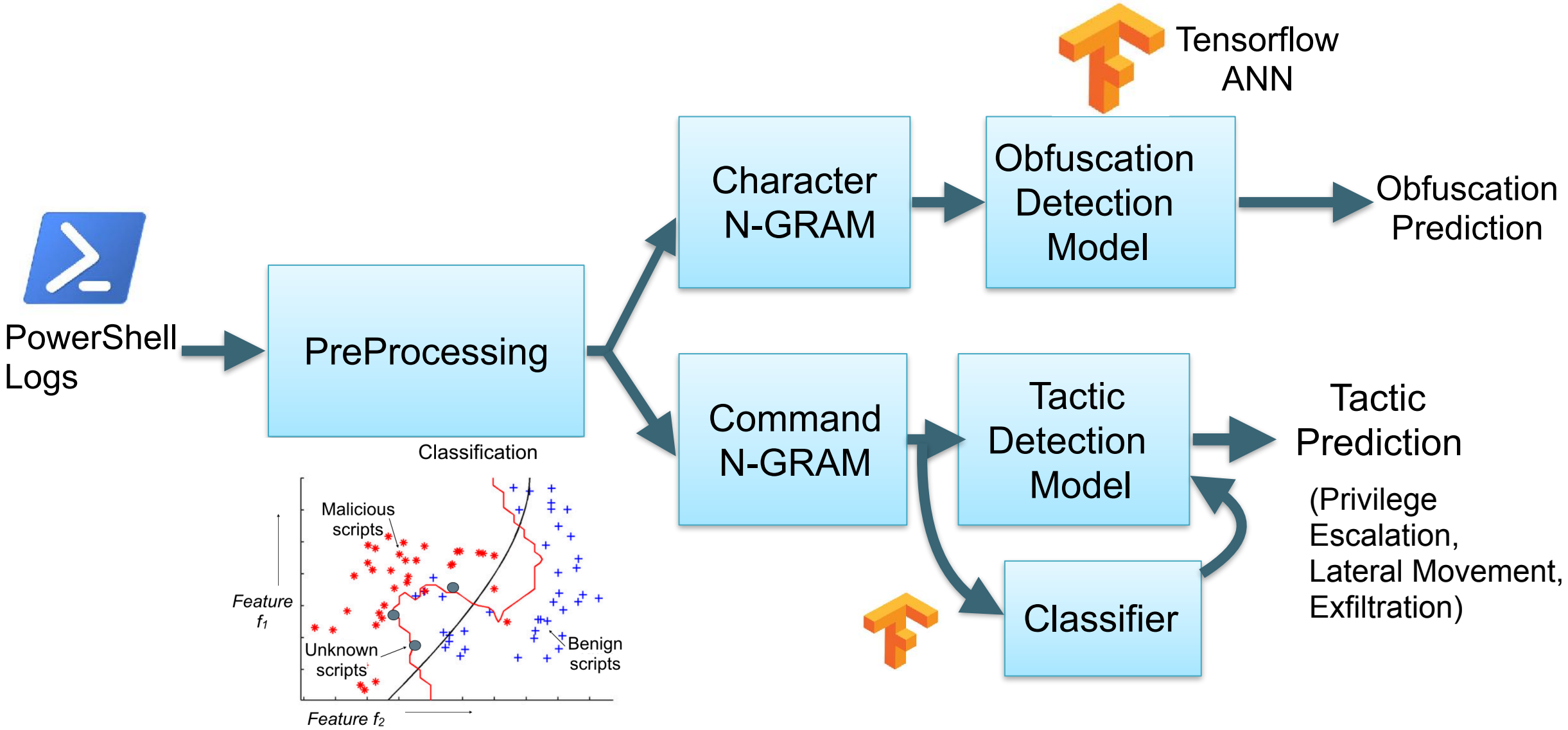
- Summarise attacker's activities
  - New services, processes, tasks and changes etc.
  - File system changes, registry entries, etc.
  - Shell commands, Windows event and authentication logs etc.

HISH-AI: Summarisation Engine

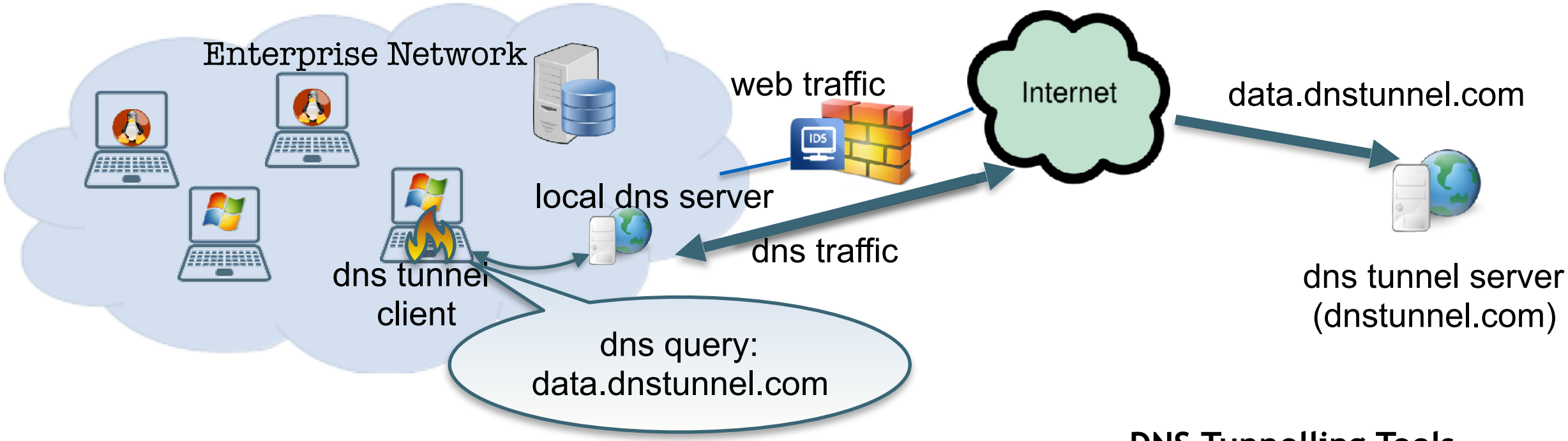


Attack Scenarios	Input Logs	Output Notables
Incident 1	60K	16
Incident 2	6K	5
Incident 3	70K	6

HISH-AI: PowerShell Log Engine

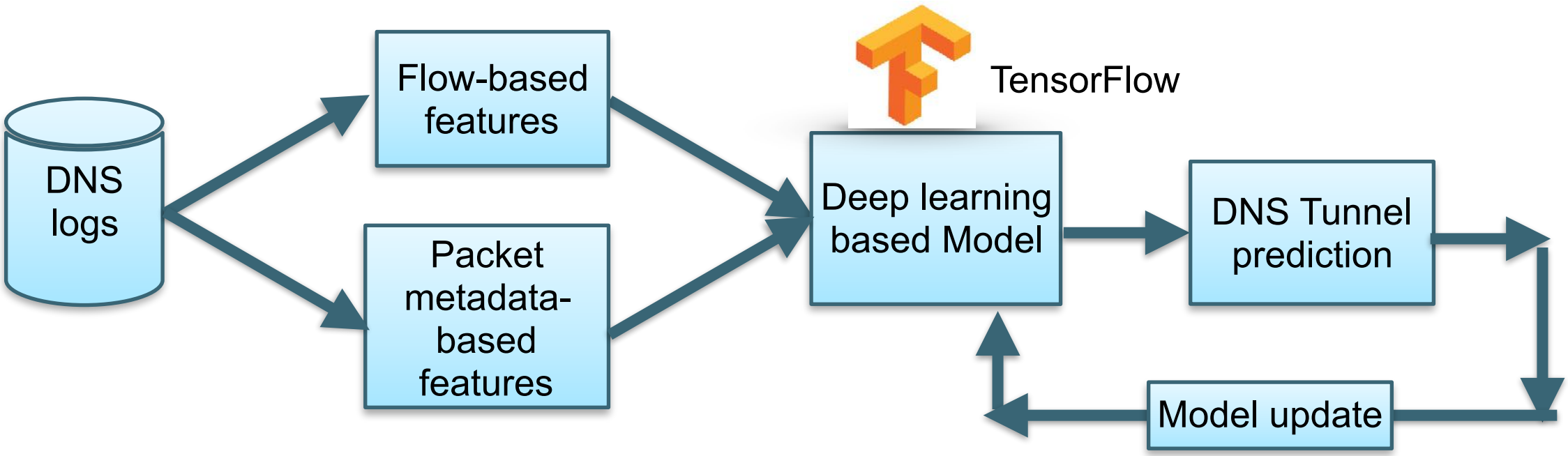


HISH-AI:Data exfiltration using DNS Tunnel



DNS Tunnelling Tools
Iodine, dnscat2, Ozyman

HISH-AI: DNS Tunnel Detection



DNS tunnel detection output:

- IP and domain of tunnelling server: dnstunnel.com
- tunnel start time: 26-02-2018 19:43:37
- tunnel end time: 26-02-2018 19:53:37

Game Theory

Formally Defining A Game

Defining Game - The Normal Form

Finite 2-person normal form game: **<N,A,u>**:

- Players: $N=\{Adversary, Defender\}$ is a finite set of 2 players, indexed by i

- Action set for player i — A_i

  $a=\{a_1,...,a_n\}$

- Utility function or Payoff function for player i: u_i

  $u=(u_1,...,u_n)$ is a profile of utility functions

InfoSec Game

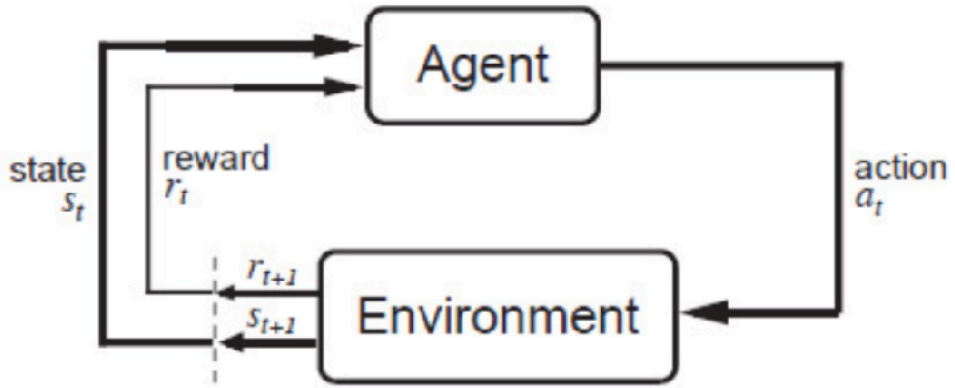
Adversary

Defender		**Carry out attack**	**Quit**
	Allow the attack	1,2	2,1
	Block the adversary	2,2	2,0

- "Row" player is Defender, "column" player is Adversary

- Too simplistic
- How to scale it for the real world?
- How do we learn in real time?

Model as Reinforcement Learning Problem



AlphaGo

- Break the problem into Subproblems and learn in real-time
- Model it as Reinforcement Learning Problem

Summary

- Playing a game needs “Visibility” of the adversary
- Need to surface signal in low SNR
- Fusion of Deception+AI gives a way to engage with the adversary

Questions?

@satnam74s