Proactive Cyber Defence Solutions

Whoami

✓ Kazem Fallahi

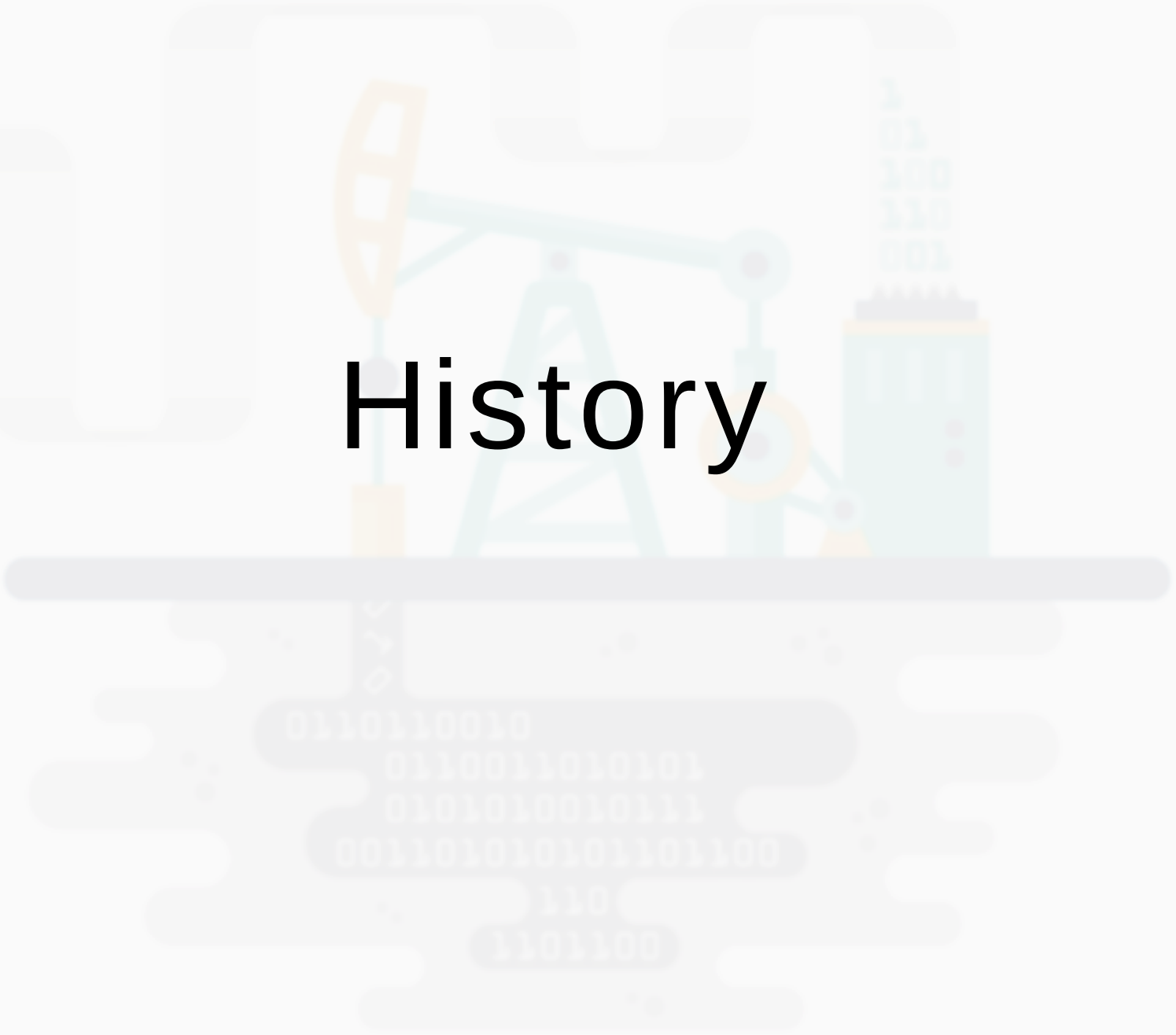
 mk.fallahi@gmail.com

 mk_fallahi

 __MKF__

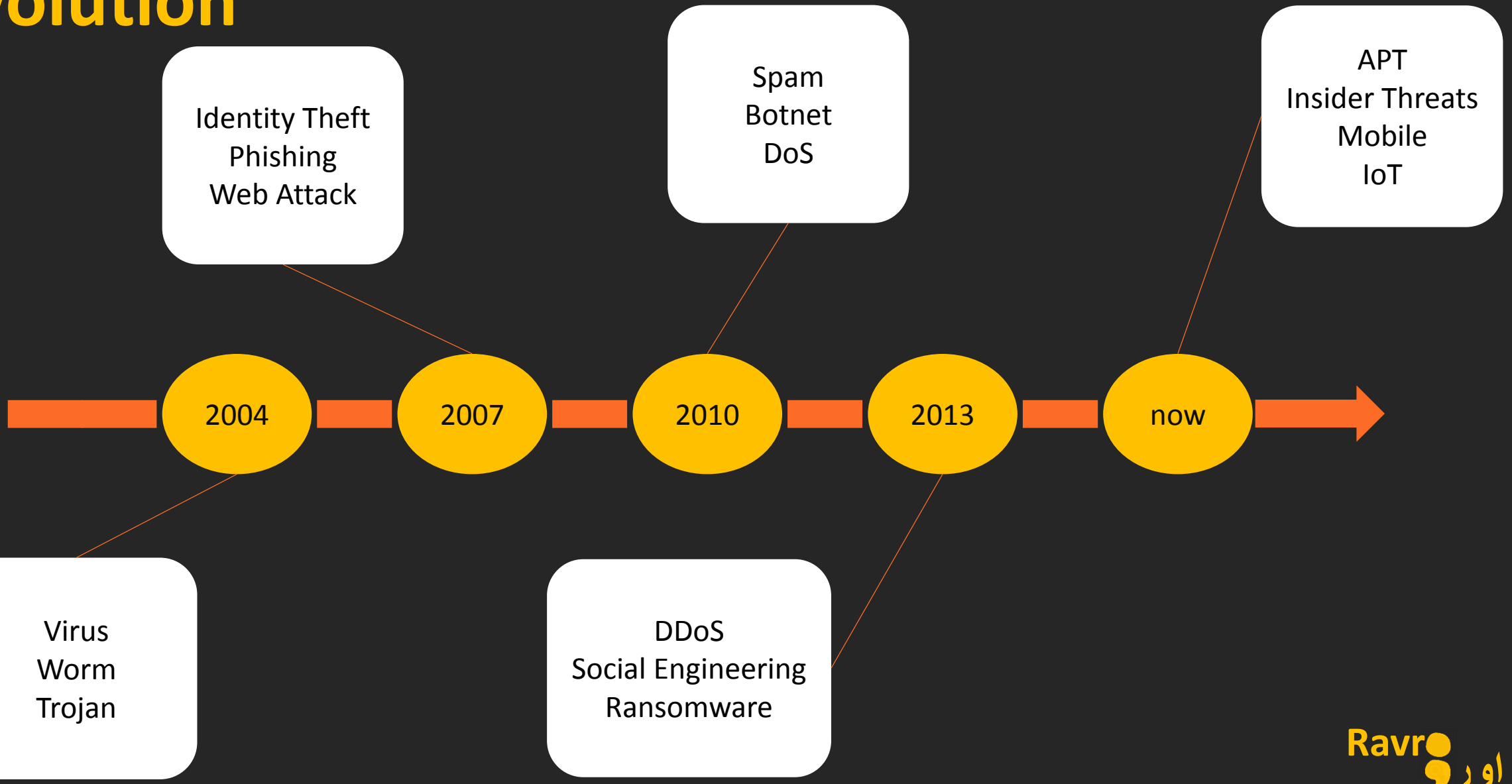
Agenda

- ✓ Attack History
- ✓ Dwell Time
- ✓ Cyber Defence Evolution
- ✓ Threat Hunting
- ✓ Red Teaming



History

Evolution


Identity Theft
Phishing
Web Attack
Spam
Botnet
DoS
APT
Insider Threats
Mobile
IoT
2004
2007
2010
2013
now
Virus
Worm
Trojan
DDoS
Social Engineering
Ransomware

Data is the new oil

APT
Silent but EVIL

APT

- Advanced
- Complex
- Remain in network for long period
- Don’t destroy systems
- Don’t interrunpt normal operation
- Usually sponsored by nations or very large organizations
- Motivation: financial gain or political espionage
- Final Goal: steal government or industrial secrets

APT Example

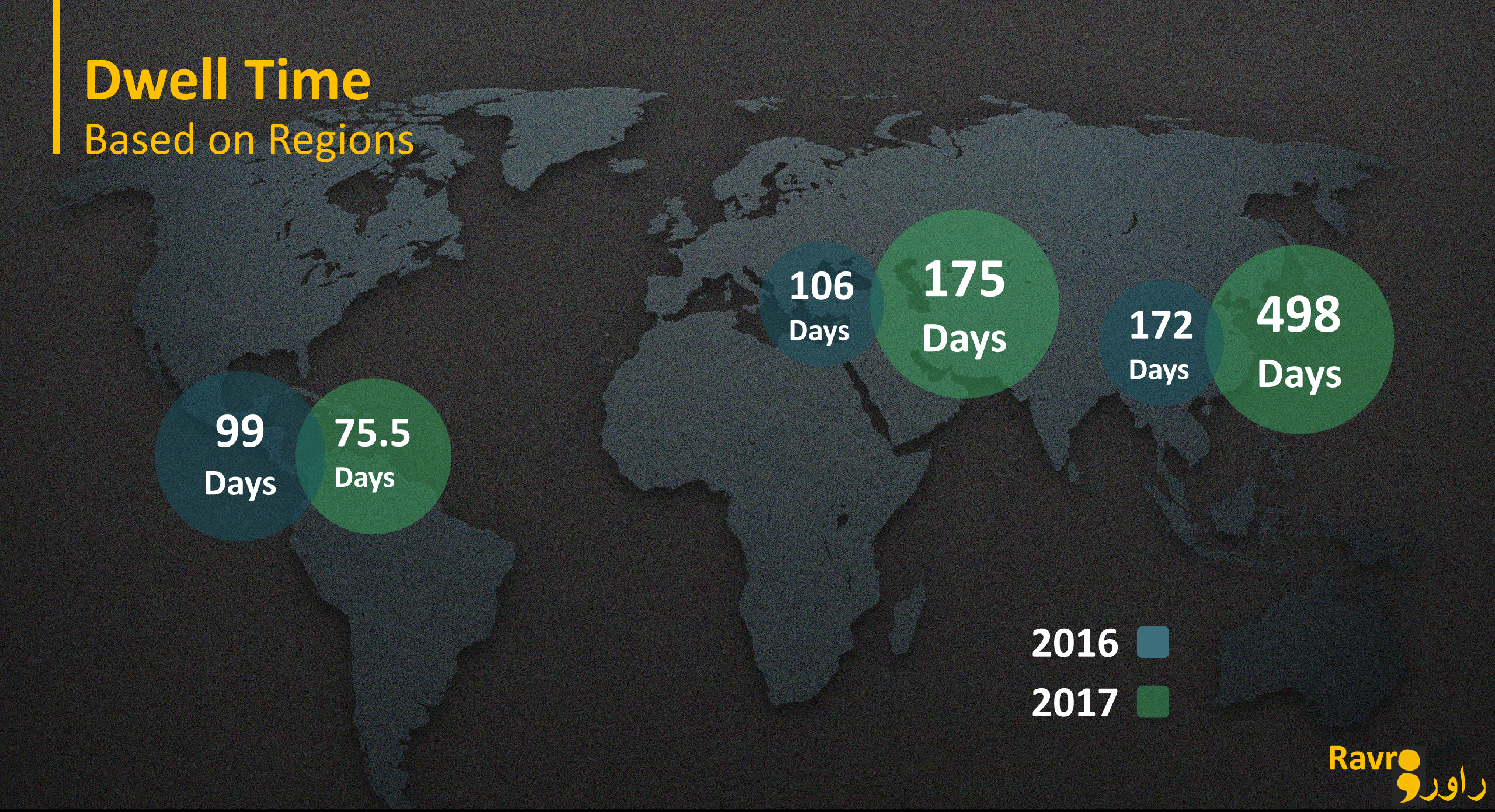
- Cloud Look
- Inception Framework (2014)
- Sykipot (2006)
- GhostNet (2009)
- STUXNET (2010)
- Red October (2012)
- APTs

Adversaries
Are already in your network

Dwell Time

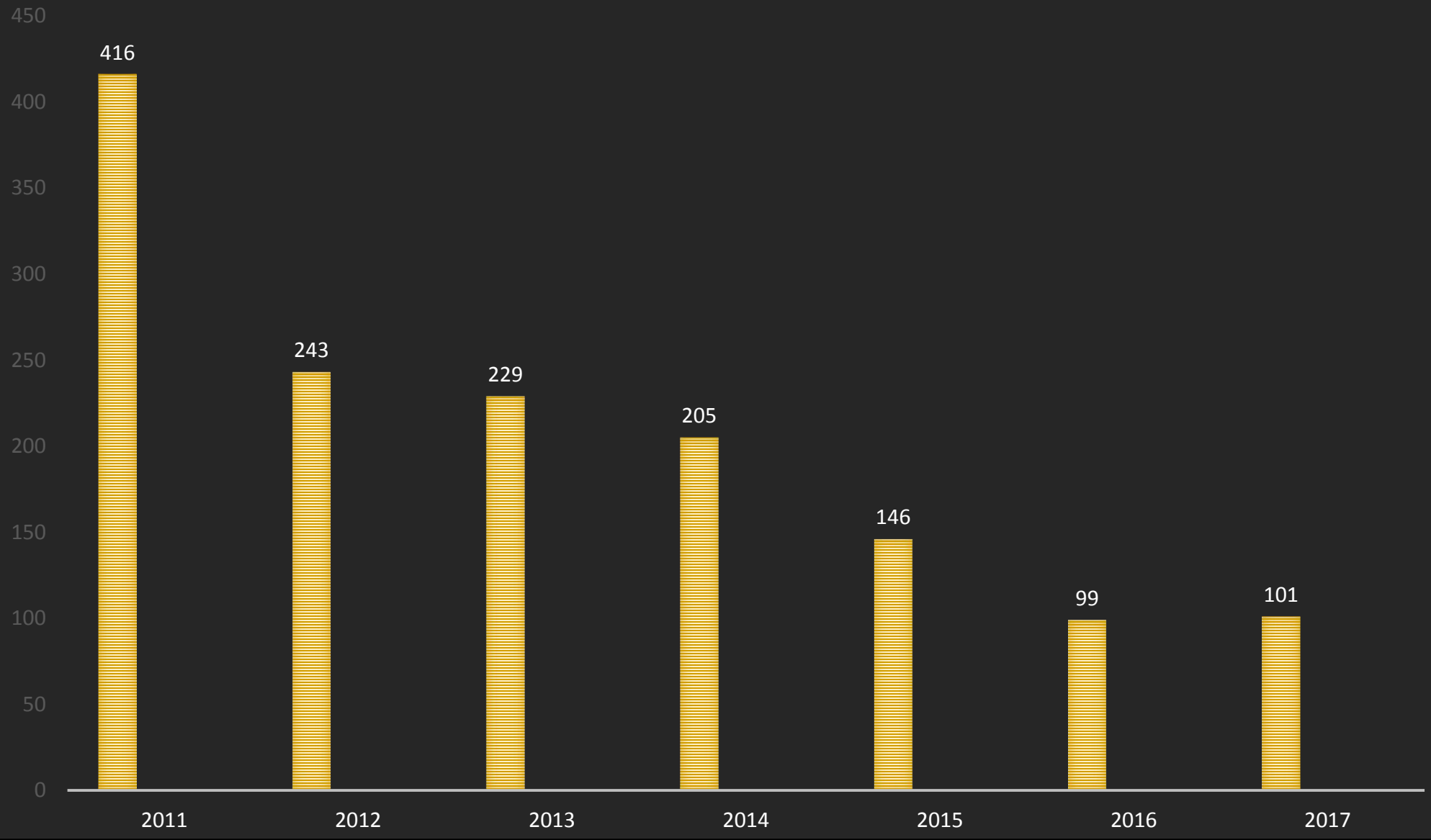
Dwell Time

Based on Regions



Dwell Time In The World

Dwell Time


450
400
350
300
250
200
150
100
50
0
416
243
229
205
146
99
101
2011
2012
2013
2014
2015
2016
2017

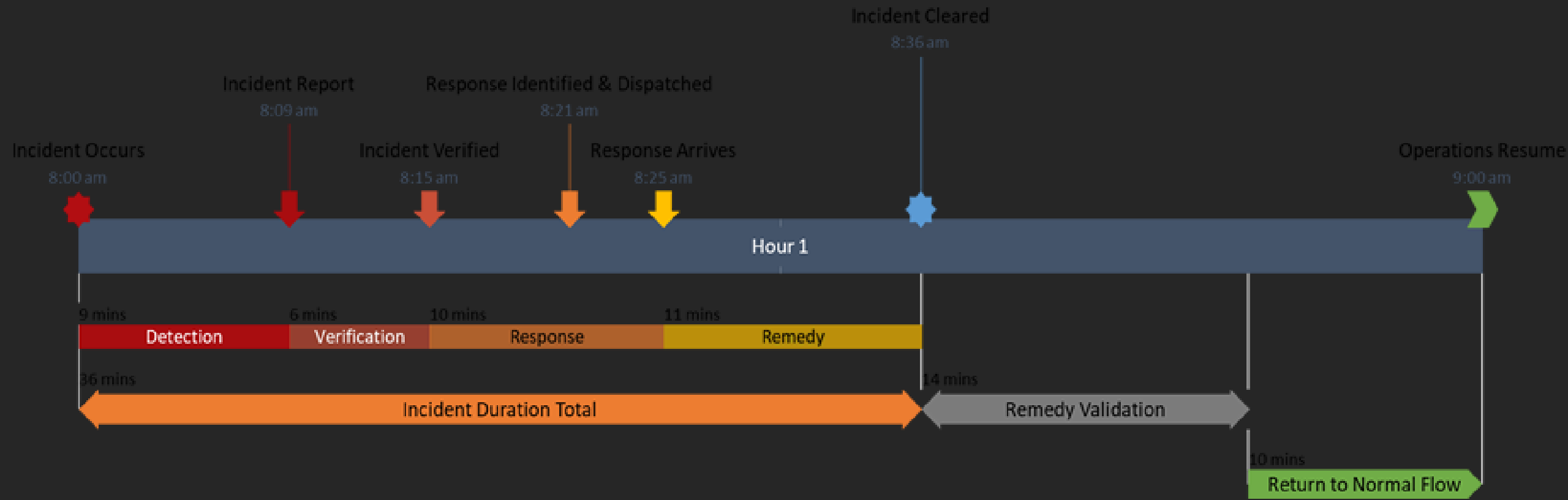
Incident Response Timeline

66
Days
Occurrencr to Discovery

3
Days
Discovery to Containment

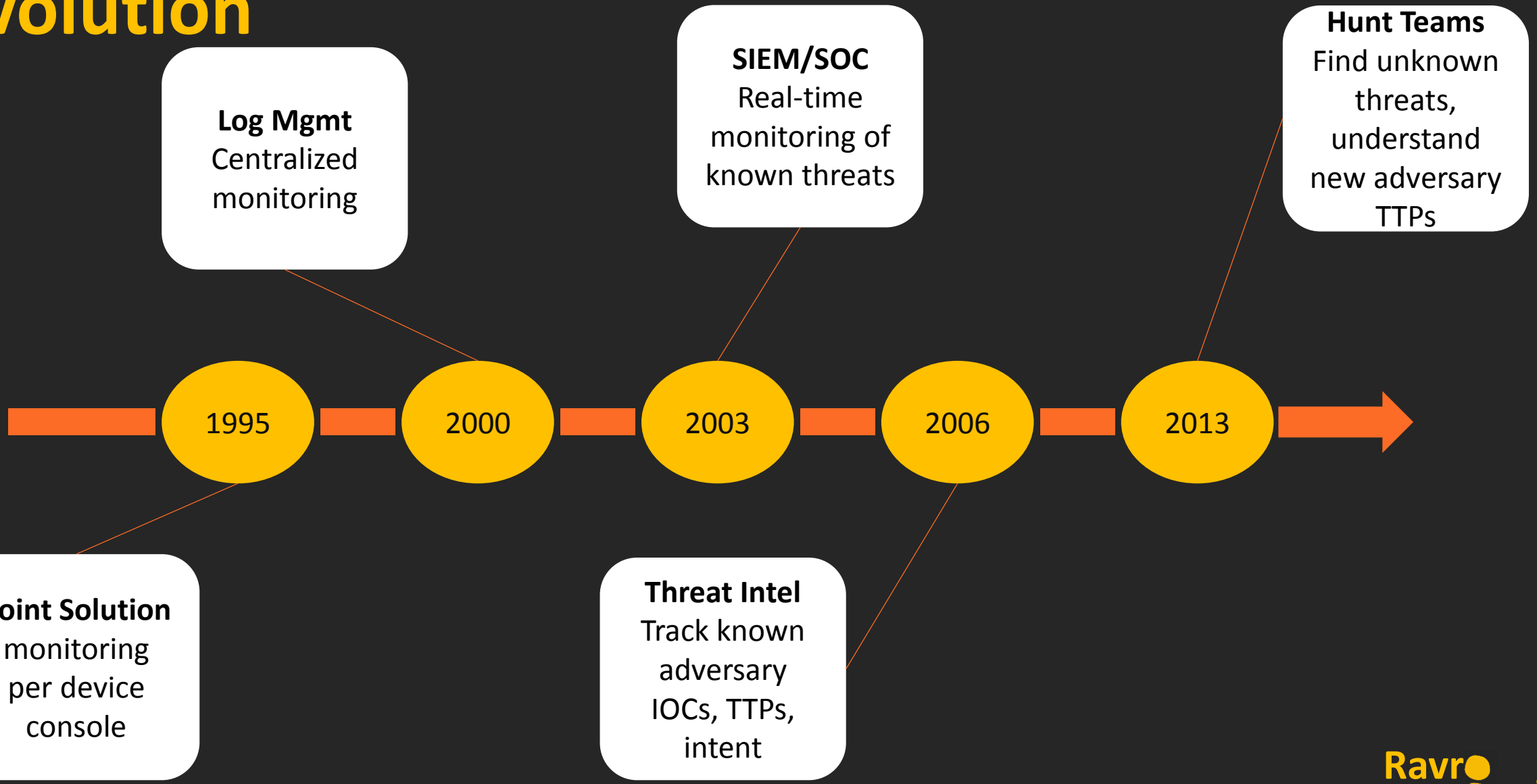
36
Days
Time to Complete Forensic Investigation

38
Days
Discovery to Notification



Cyber Defence Evolution

Evolution

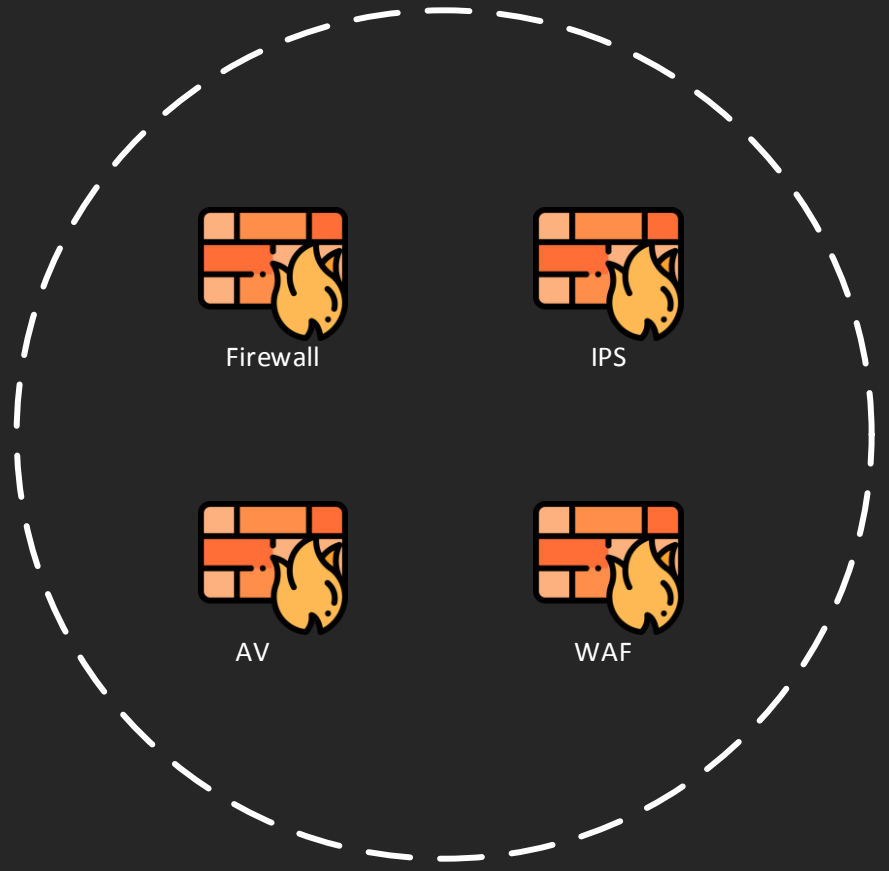

Log Mgmt
Centralized monitoring
SIEM/SOC
Real-time monitoring of known threats
Hunt Teams
Find unknown threats, understand new adversary TTPs
1995
2000
2003
2006
2013
Point Solution
monitoring per device console
Threat Intel
Track known adversary IOCs, TTPs, intent

Goal

- Prevent Attackers From Achieving Their Goal
- Reduce Attack Dwell Time
- Change Mindset

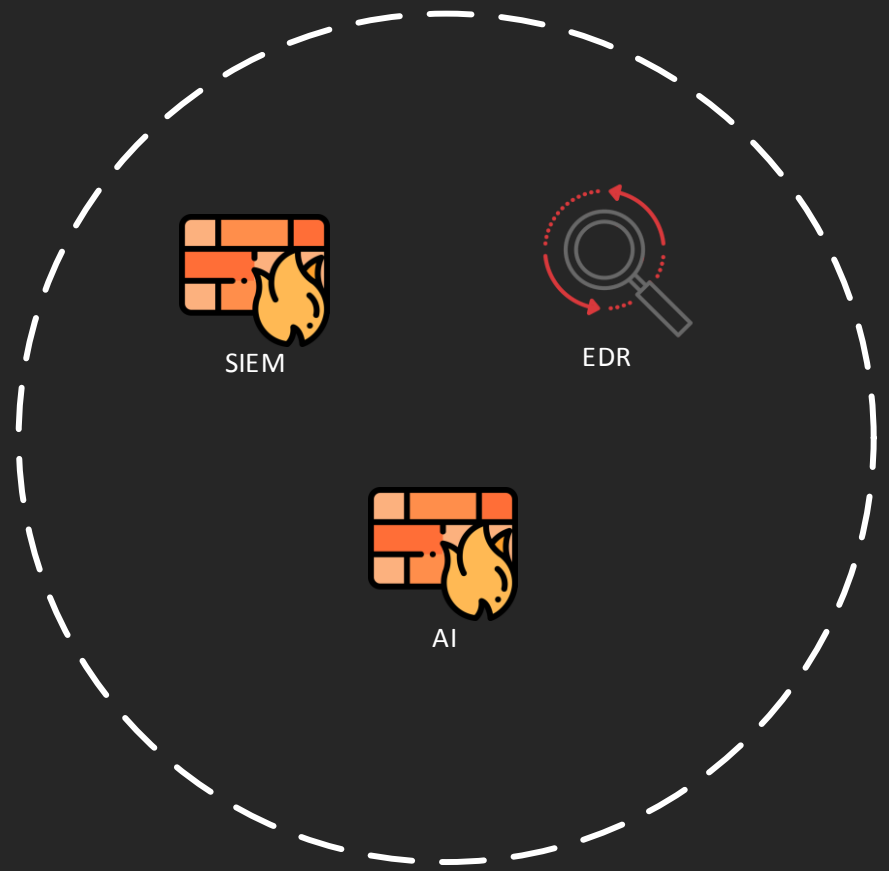
NG Cyber Security Solutions

Old solutions



Focused on threat prevention

Next generation solutions



Focused on threat Hunting

Ravro راور

Reactive Security VS Proactive Cyber Defence

Ravro راور

Traditional vs Modern Defense

Traditional Defense

- Prevention is Core
- Perimeter Focused
- Mainly Reactive

Modern Defense

- Prevention is ideal but Detection & Response is Crucial
- Everywhere is your Perimeter
- **Proactive Threat Hunting**

SIEM is Dead!

John Linkous 2012

Why Traditional Solution Can’t Stop Hackers

- Government support from hacking teams
- Hacking as a full-time job
- Government hackers have a high degree of expertise
- Hacking teams have high financial support

Focus Area To Reduce Dwell Time

- Fundamental security controls
- Granular visibility and correlated intelligence
- Continuous endpoint monitoring
- Actionable prediction of human behavior
- User awareness (user behavior analysis)

Threat Hunting

Why Hunting

- one of the hot topics at RSA 2018
- Rather than waiting for the inevitable data breach to happen, **proactively** scout around for and hunt down bad actors and malicious activity on your networks.
- Threat hunting combines the use of threat intelligence, analytics, and automated security tools with human smarts.
- Hunting consists of manual or machine-assisted techniques
- as opposed to relying only on automated systems like SIEMs

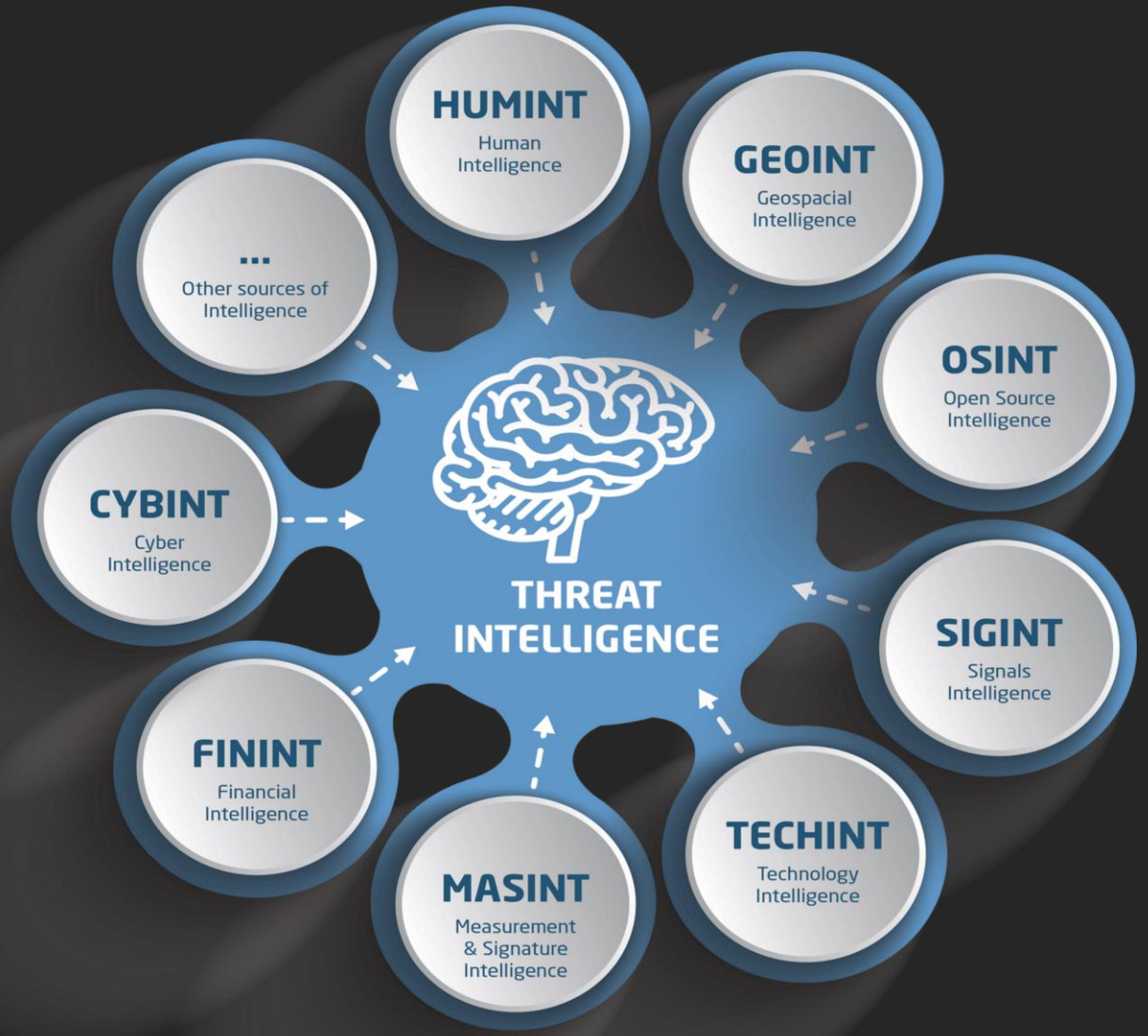
Ravro راور

Goals of Threat Hunting

- Gaining better visibility into the organization’s weaknesses
- Provide early and accurate detection
- Control and reduce impact and damage with faster response
- Improve defenses to make successful attacks increasingly difficult
- Tracking activity and looking for anomalies

Definition

Threat Hunting refers to **proactively and iteratively** searching through networks or datasets to detect and respond to advanced threats that evade traditional rule or signature-based security solutions.



Threat Hunting

- Known Bad
- Suspicious Behavior
- Unknown Bad

Keys to Successful Hunt

Planing, preparing, proccesing

skill, experience, efficiency

Tools, procedures, tech

Huntrs Skillsets

Cyber Security

- Intrusion Analysis
- Malware Analysis
- Threat Intelligence

Data Science

- Data Management
- Data Visualization
- Statistics
- Programming

Mindset

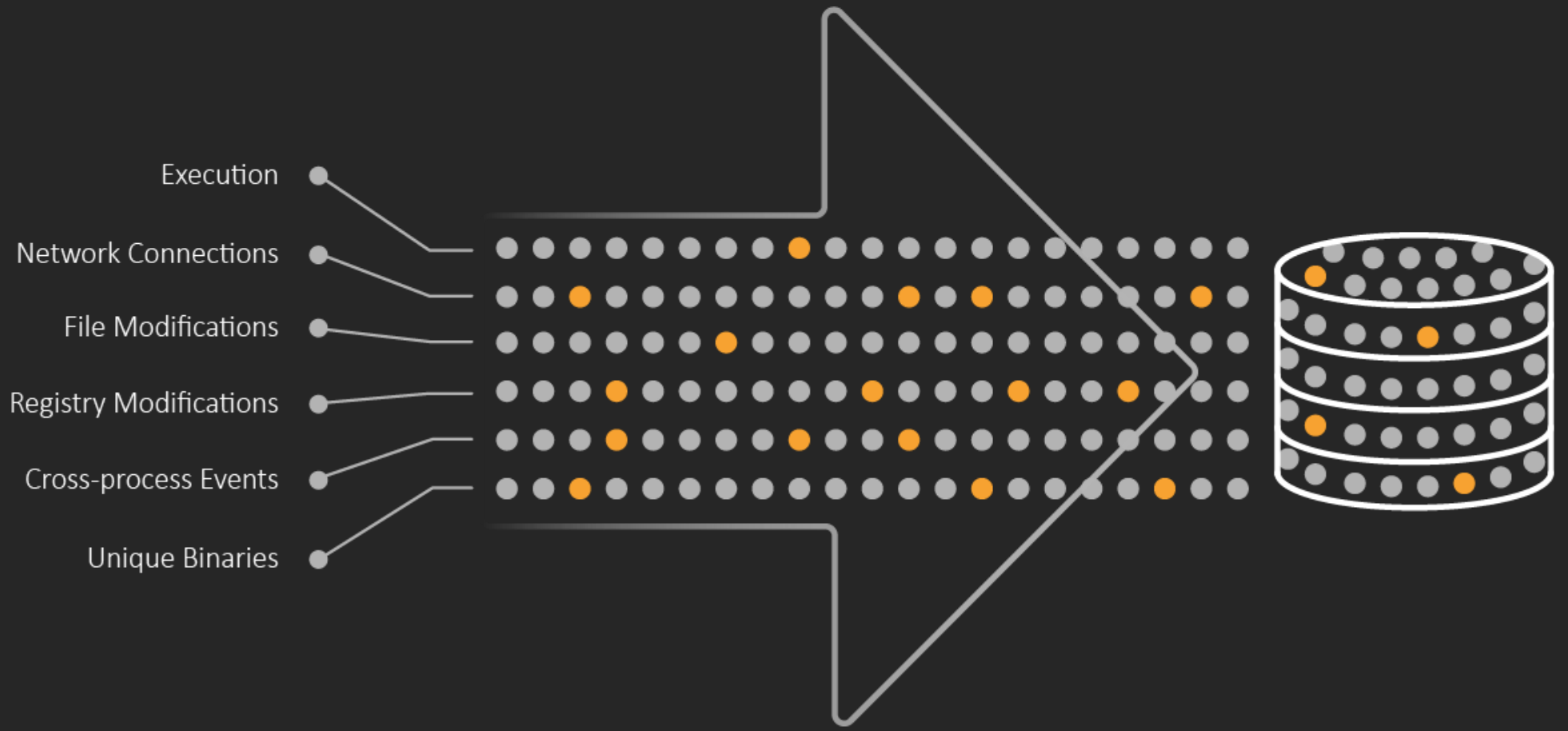
- Desire to learn
- Creative
- Analytical
- Red team

Ravro راورو

Threat Hunting Activities

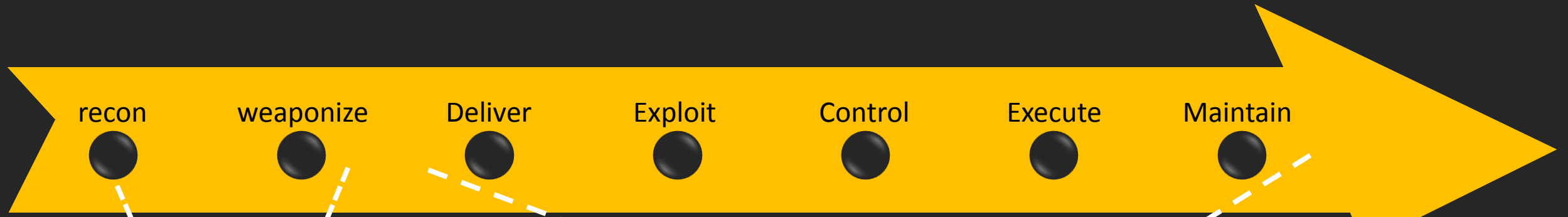
- Understanding the threats
- Identifying critical data and business processes utilizing that data
- Intuition, hunches and hypotheses
- Behavioral analytics
- Complete Situational Awareness
- Analyzing all data
- Looking for anomalies

Data Collection & Analysis



Cyber Kill Chain
The Seven Phases of a Cyber Attack

- Reconnaissance
  Harvesting email addresses, conference information, ...
- Weaponization
  Coupling exploit with backdoor into deliverable payload
- Delivery
  Delivering weaponized bundle to the victim via email, web, USB, ...
- Exploitation
  Exploiting avulnerability to execute code on vitim's system
- Installation
  Installing malware on the asset
- COMMAND & CONTROL
  Command channel for the remote manipulation of victim
- Actions & Objectives
  Intruders accomplish their original goals



PRE-ATT&CK

Priority Definition
Planing,Direction
Target Selection
Information Gathering
Technical, People, Organizational
Weakness Identification
Technical, People, Organizational
Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Biuld Capabilities
Test Capabilities
Stage Capabilities

Enterprise ATT&CK

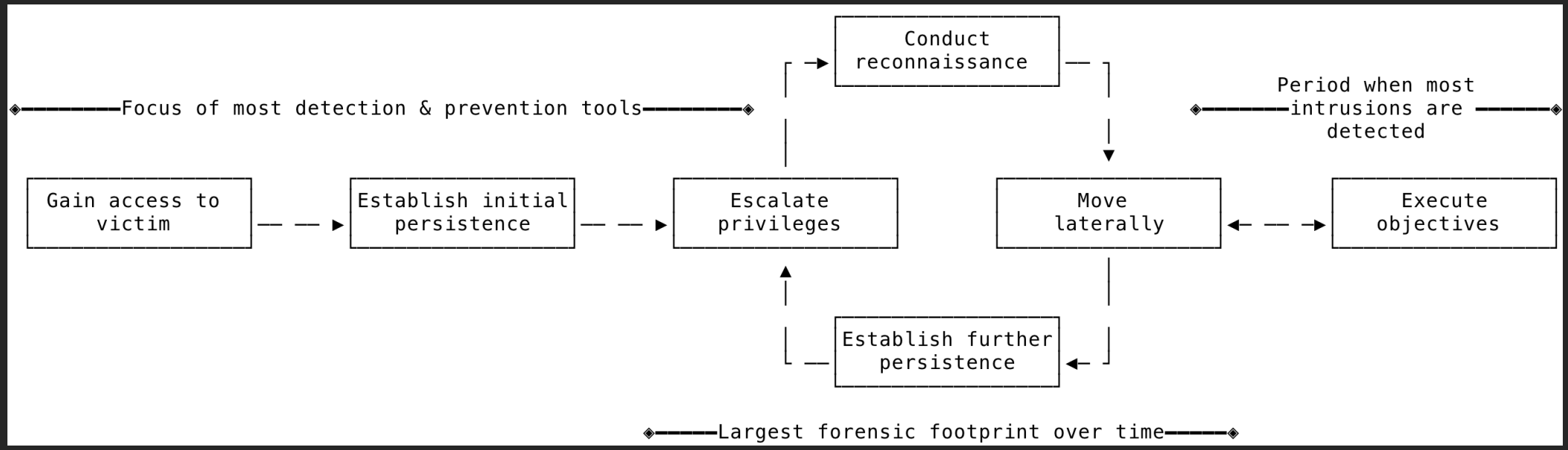
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Comand & Control

Ravro راورو

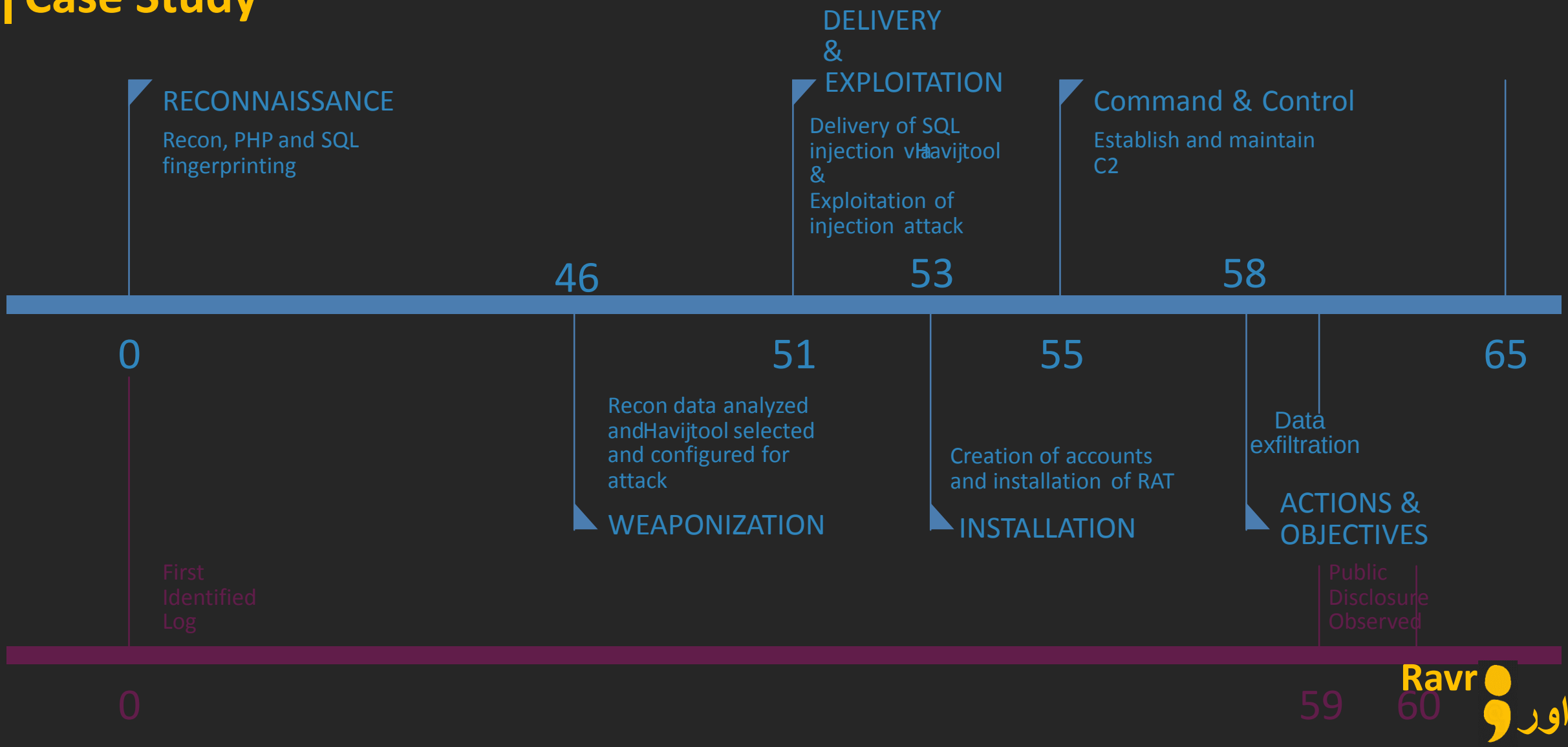
MITRE Enterprise ATT&CK™ Framework

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Image File Execution Options Injection	Image File Execution Options Injection	Process Doppelgänging	Forced Authentication	Network Share Discovery	AppleScript	AppleScript	Man in the Browser	Exfiltration Over Physical Medium	Multi-hop Proxy
Plist Modification	Plist Modification	Mshta	Hooking	System Time Discovery	Third-party Software	Third-party Software	Browser Extensions	Exfiltration Over Command and Control Channel	Domain Fronting
Valid Accounts	Valid Accounts	Hidden Files and Directories	Password Filter DLL	Peripheral Device Discovery	Windows Remote Management	Windows Remote Management	Video Capture	Scheduled Transfer	Data Encoding
DLL Search Order Hijacking	DLL Search Order Hijacking	Launchctl	LLMNR/NBT-NS Poisoning	Account Discovery	SSH Hijacking	LSASS Driver	Audio Capture	Data Encrypted	Remote File Copy
AppCert DLLs	AppCert DLLs	Space after Filename	Securityd Memory	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Automated Collection	Automated Exfiltration	Multi-Stage Channels
Hooking	Hooking	LC_MAIN Hijacking	Private Keys	System Information Discovery	Pass the Ticket	Mshta	Clipboard Data	Exfiltration Over Other Network Medium	Web Service
Startup Items	Startup Items	HISTCONTROL	Keychain	Security Software Discovery	Replication Through Removable Media	Local Job Scheduling	Email Collection	Exfiltration Over Alternative Protocol	Standard Non-Application Layer Protocol
Launch Daemon	Launch Daemon	Hidden Users	Input Prompt	System Network Connections Discovery	Windows Admin Shares	Trap	Screen Capture	Data Transfer Size Limits	Communication Through Removable Media
Dylib Hijacking	Dylib Hijacking	Clear Command History	Bash History	System Owner/User Discovery	Remote Desktop Protocol	Source	Data Staged	Data Compressed	Multilayer Encryption
Application Shimming	Application Shimming	Gatekeeper Bypass	Two-Factor Authentication Interception	System Network Configuration Discovery	Pass the Hash	Launchctl	Input Capture		Standard Application Layer Protocol
AppInit DLLs	AppInit DLLs	Hidden Window	Account Manipulation	Application Window Discovery	Exploitation of Vulnerability	Space after Filename	Data from Network Shared Drive		Commonly Used Port
Web Shell	Web Shell	Deobfuscate/Decode Files or Information	Replication Through Removable Media	Network Service Scanning	Shared Webroot	Execution through Module Load	Data from Local System		Standard Cryptographic Protocol
Service Registry Permissions Weakness	Service Registry Permissions Weakness	Trusted Developer Utilities	Input Capture	Query Registry	Logon Scripts	Regsvcs/Regasm	Data from Removable Media		Custom Cryptographic Protocol
Scheduled Task	Scheduled Task	Regsvcs/Regasm	Network Sniffing	Remote System Discovery	Remote Services	InstallUtil			Data Obfuscation
New Service	New Service	Exploitation of Vulnerability	Credential Dumping	Permission Groups Discovery	Application Deployment Software	Regsvr32			Custom Command and Control Protocol
File System Permissions Weakness	File System Permissions Weakness	Extra Window Memory Injection	Brute Force	Process Discovery	Remote File Copy	Execution through API			Connection Proxy
Path Interception	Path Interception	Access Token Manipulation	Credentials in Files	System Service Discovery	Taint Shared Content	PowerShell			Uncommonly Used Port
Accessibility Features	Accessibility Features	Bypass User Account Control				Rundll32			Multiband Communication
Port Monitors	Port Monitors	Process Injection				Scripting			Fallback Channels
Screensaver	Screensaver	SID-History Injection				Graphical User Interface			
LSASS Driver	LSASS Driver	Sudo				Command-Line Interface			
Browser Extensions	Browser Extensions	Setuid and Setgid				Scheduled Task			
Local Job Scheduling	Local Job Scheduling	Component Object Model Hijacking				Windows Management Instrumentation			
Re-opened Applications	Re-opened Applications	InstallUtil				Trusted Developer Utilities			
Rc.common	Rc.common	Regsvr32				Service Execution			
Login Item	Login Item	Code Signing							
LC_LOAD_DYLIB Addition	LC_LOAD_DYLIB Addition	Modify Registry							
Launch Agent	Launch Agent	Component Firmware							
Hidden Files and Directories	Hidden Files and Directories	Redundant Access							
.bash_profile and .bashrc	.bash_profile and .bashrc	File Deletion							
Trap	Trap	Timestomp							
Launchctl	Launchctl	NTFS Extended Attributes							
Office Application Startup	Office Application Startup	Process Hollowing							
Create Account	Create Account	Disabling Security Tools							
External Remote Services	External Remote Services	Rundll32							
Authentication Package	Authentication Package	DLL Side-Loading							
Netsh Helper DLL	Netsh Helper DLL	Indicator Removal on Host							
Component Object Model Hijacking	Component Object Model Hijacking	Indicator Removal from Tools							
Redundant Access	Redundant Access	Indicator Blocking							
Security Support Provider	Security Support Provider	Software Packing							
Windows Management Instrumentation Event Subscription	Windows Management Instrumentation Event Subscription	Masquerading							
Registry Run Keys / Start Folder	Registry Run Keys / Start Folder	Obfuscated Files or Information							
Change Default File Association	Change Default File Association	Binary Padding							
Component Firmware	Component Firmware	Install Root Certificate							
Bootkit	Bootkit	Network Share Connection Removal							
Hypervisor	Hypervisor	Bootkit							
Logon Scripts	Logon Scripts								

attack.mitre.org

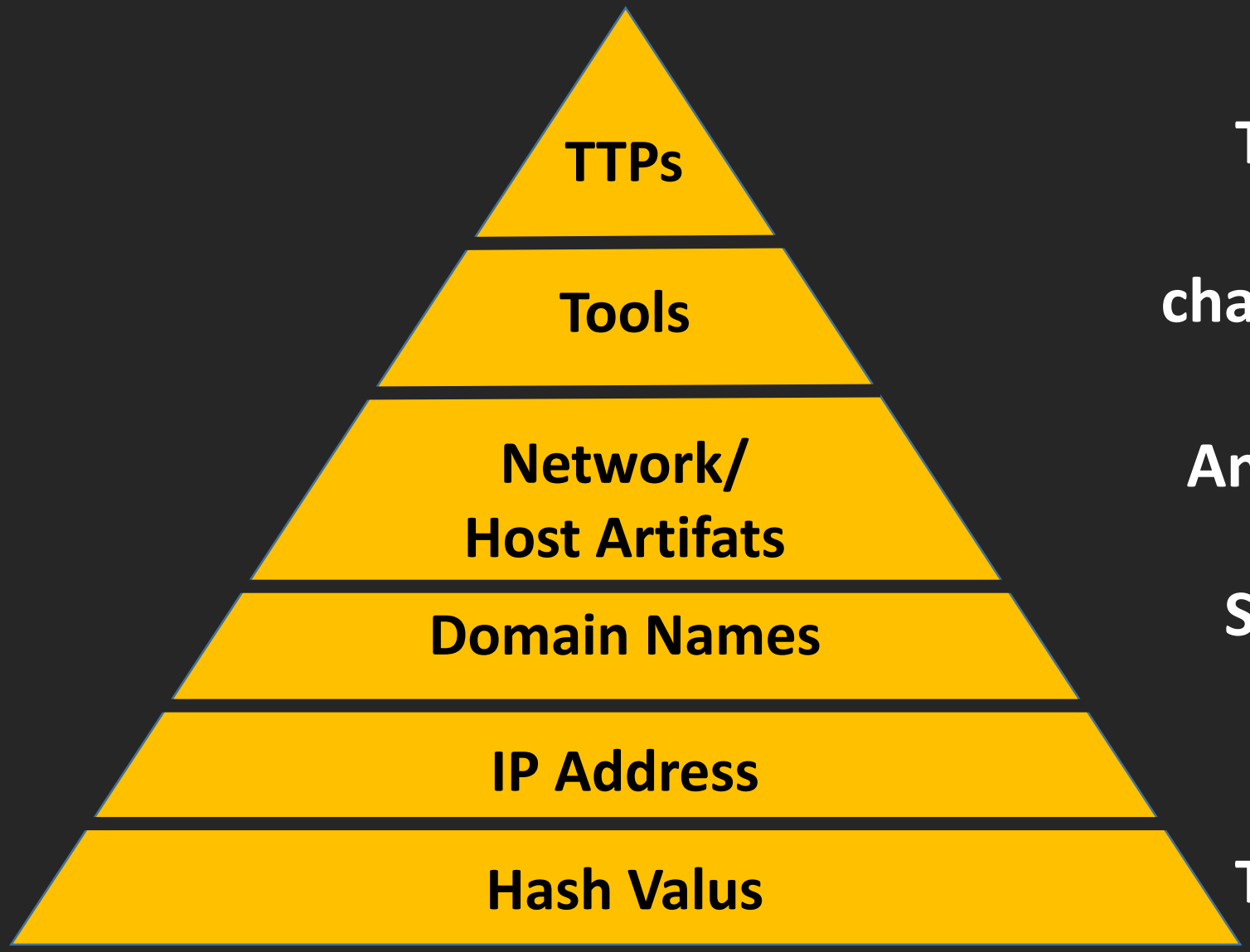

Conduct reconnaissance
Focus of most detection & prevention tools
Period when most intrusions are detected
Gain access to victim
Establish initial persistence
Escalate privileges
Move laterally
Execute objectives
Establish further persistence
Largest forensic footprint over time

Cyber Kill Chain
Case Study



Ravr راور

The Pyramid of Pain



Tough

challenging

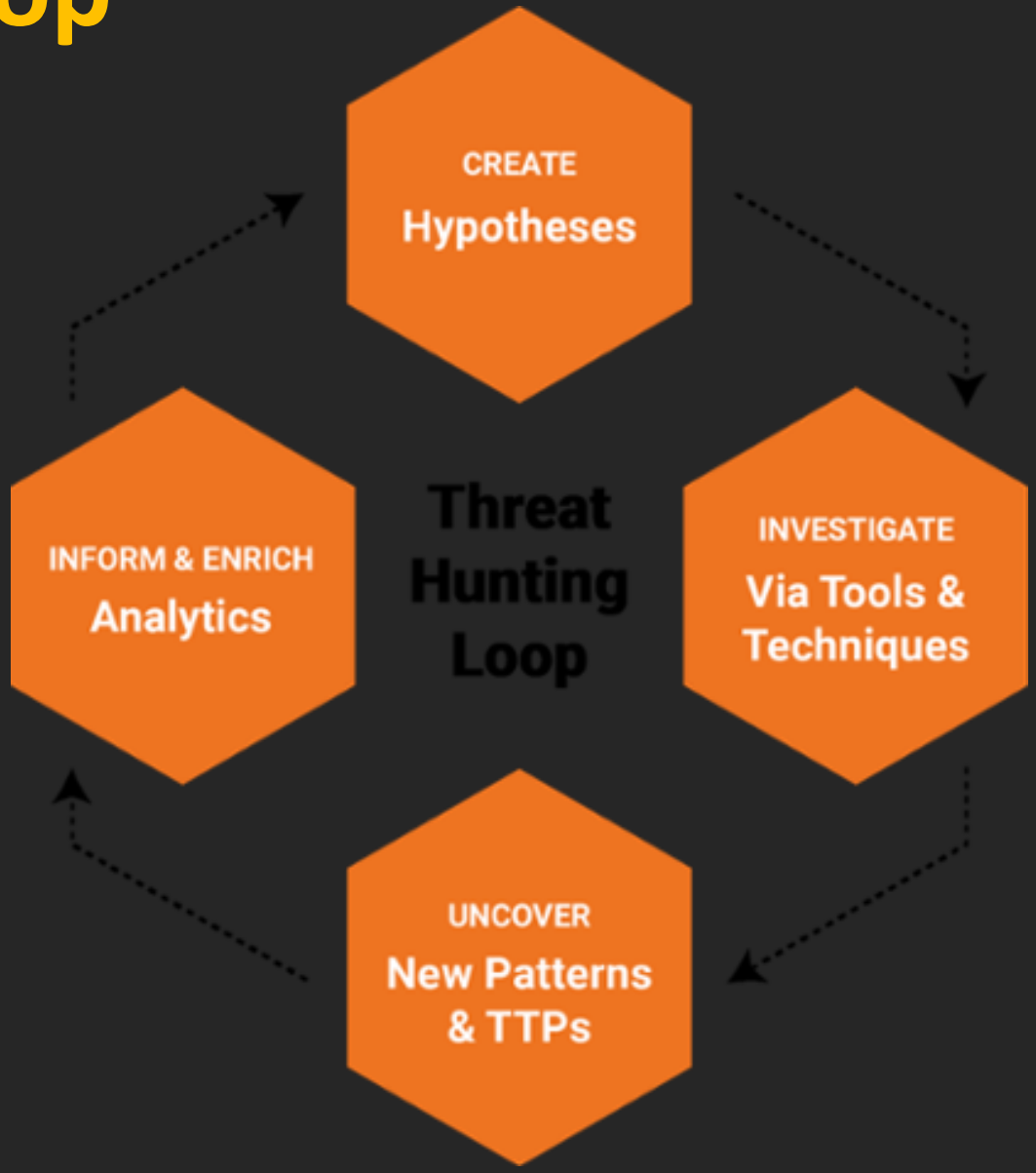
Annoying

Simple

Easy

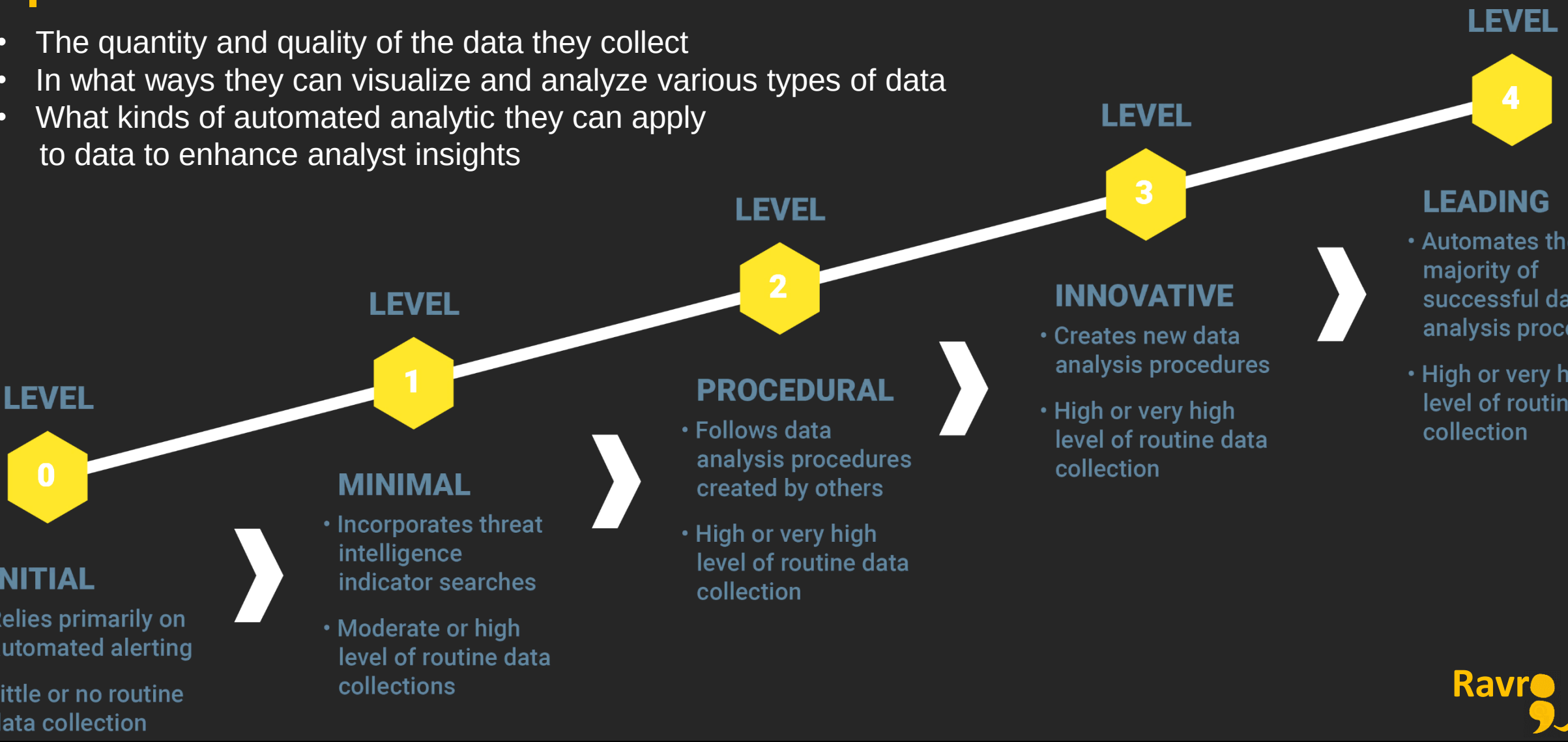
Trivial

The Hunting Loop



The Hunting Maturity Model

- The quantity and quality of the data they collect
- In what ways they can visualize and analyze various types of data
- What kinds of automated analytic they can apply to data to enhance analyst insights



Why Hunting is difficult

- Incidents are non-linear
- adversaries continue to change their patterns
- Targeted intrusions often begin with opportunistic compromises
- Attackers can be erratic & unpredictable
- Evidence is often incomplete or insufficient

- Adapt to changes in behaviors
- learn how the adversary works
- Watch all behaviors of the adversary

Large environments = more noise = more false positives

Ravro راور

Sharing

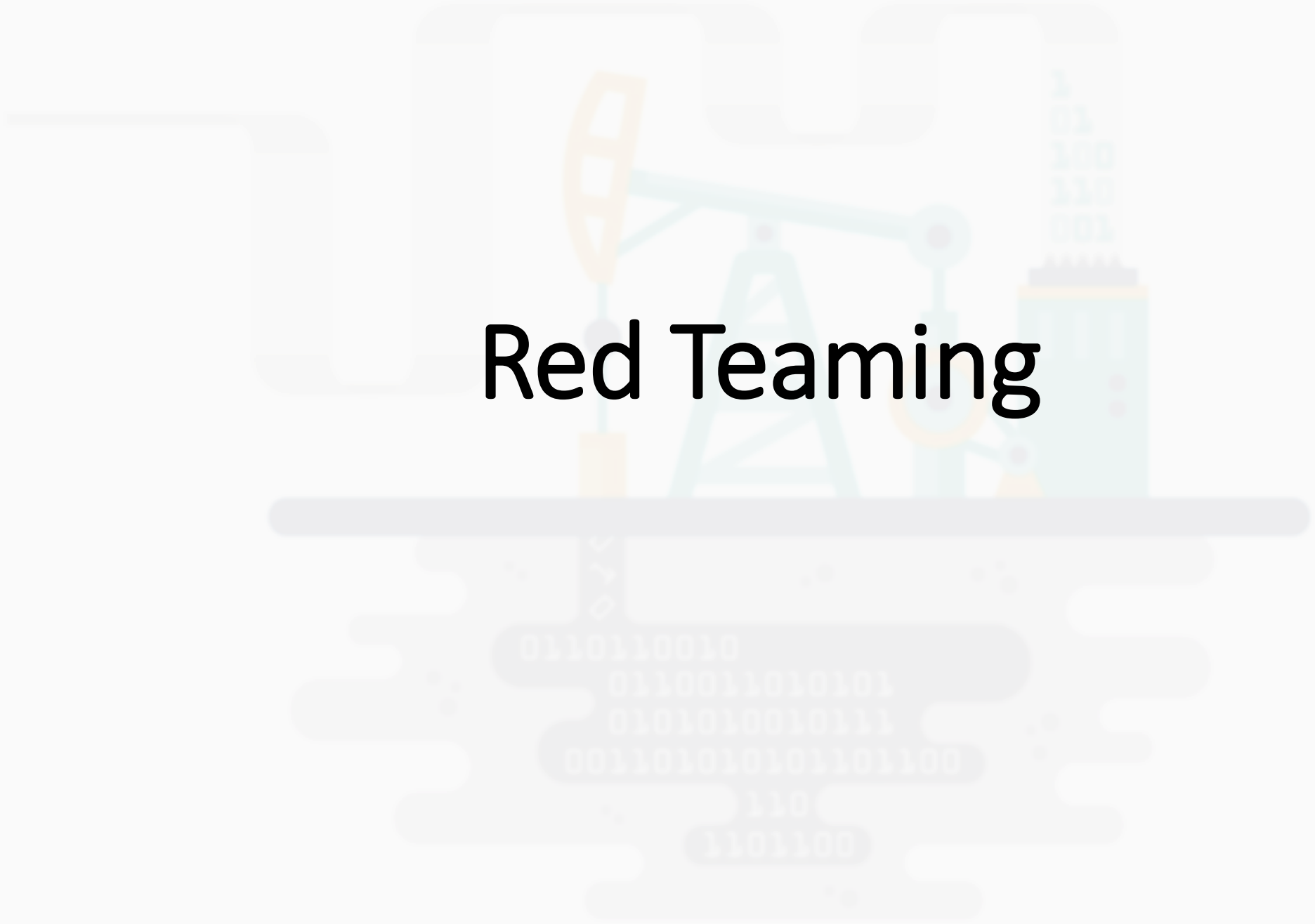
My detection becomes your prevention

- We need to close the gap between sharing speed and attack speed
- 75% of attacks spread from Victim 0 to Victim 1 within one day (24 hours).

Threat Intelligence
Evolving Security From Reaction To Prediction

Ravro راور

Demo



Red Teaming

Red Teaming

- Provides more value than a Penetration Test
- Should be implemented into a regular schedule
- Helps train security personnel
- Helps make sure your boxes are tuned
- Using Weaknesses to find what is most valuable
- Goal Oriented
- Review attack
- Test how teams use services and how they are managed

Red Teaming Goals

- Model recent threats and trends
- Longer term
- Highlight Gaps in Security Controls, detection,…
- Escape and Evade for Persistence

Blue Teaming Goals

- Detect Attack
- Respond and Recover
- Produce Actionable Intelligence
- Identify Gaps and investment needs

Tools

Ravro راور

Team Members

Kazem Fallahi

mk.fallahi@gmail.com
@__mkf__

Omid Palvayeh

O.Palvayeh@gmail.com
@OmidPalvayeh

MohammadAmin Kariman

kariman.mohammadamin@gmail.com
@Ma_kariman

Ravro راورو