SECURITY SUMMIT

14-15-16 marzo 2023

Security Summit

Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

Nuove evoluzioni dell'automazione di attività offensive: il Breach & Attack Simulation

Daniel Bertoni, Co-founder, Pikered srl

Diego Lorenzi, Co-founder, Pikered srl

14 marzo 2023 16.30-17.10

Daniel Bertoni

HEAD OF CYBERSECURITY

Diego Lorenzi

HEAD OF DATA SCIENCE

Cyber Attack Kill Chain

4. **Exploitation**
Esecuzione del Payload sulla macchina remota

3. **Delivery**
Invio del Payload alla vittima

5. **Installation**
Installazione di una backdoor per instaurare un meccanismo di persistenza

2. **Weaponization**
Confezionamento del Payload per eludere I meccanismi di difesa

6. **Command & Control**
Canale sicuro che permette all'attaccante di muoversi nella rete interna dell'organizzazione

1. **Reconnaissance**
Ricerca, identificazione e selezione dei target

7. **Actions on Objectives / Exfiltration**
Raggiungimento dell'obiettivo: esfiltrazione di dati, deploy di un ransomware ecc..

Automazione della Cyber Attack Kill Chain

	Vulnerability Scan	Penetration Test	Breach & Attack Simulation
Reconnaissance	🟢	🟢	🟡
Weaponization	🟠	🟡	🟢
Delivery	🟠	🟡	🟢
Exploitation	🟠	🟢	🟢
Installation	🟠	🟡	🟢
Command & Control	🟠	🟡	🟢
Exfiltration	🟠	🔴	🟢

I limiti delle soluzioni automatizzate tradizionali

01

Simulazione non reale e in condizioni di partenza differenti rispetto ai reali attacchi informatici.

02

Copertura parziale della Cyber Attack Kill Chain.

03

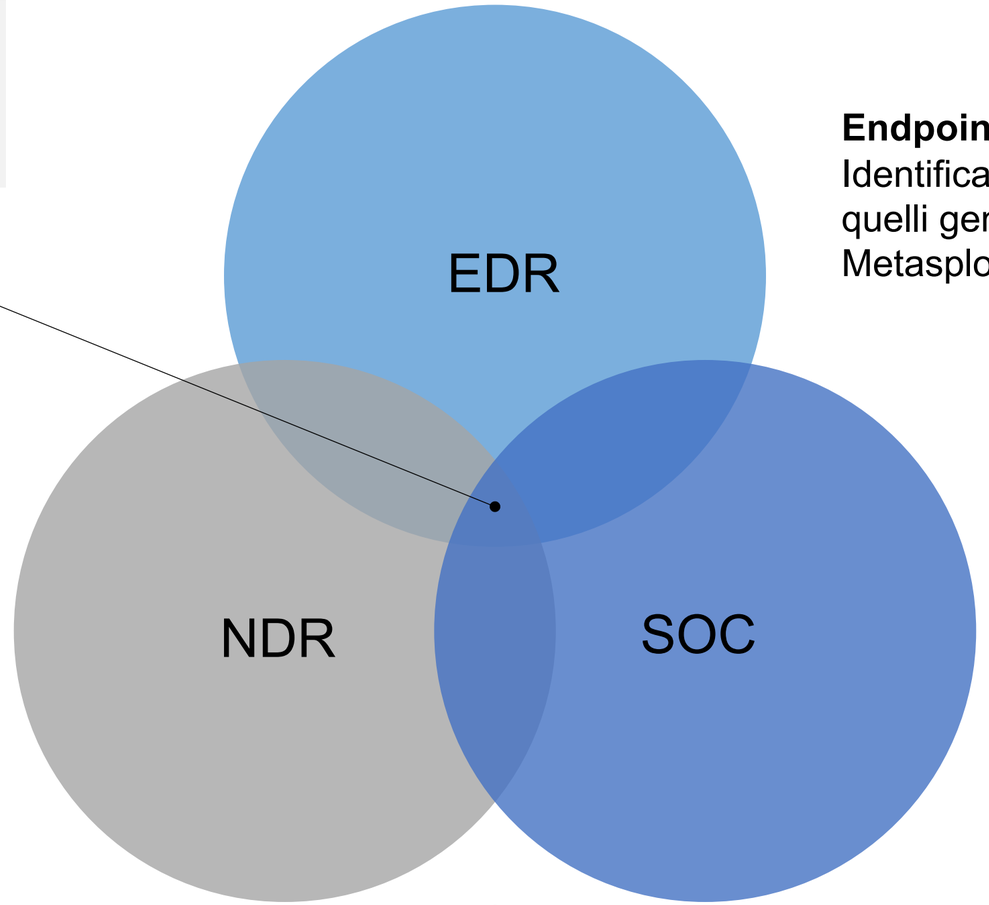
Tecniche impiegate obsolete e che non rispecchiano i vettori d’attacco sempre più complessi utilizzati dai criminali.

04

Obiettivi diversi e non in linea con le reali esigenze della sicurezza.

Obiettivi

Soluzione che validi tutte le linee di difesa implementate all'interno e sul perimetro della rete



Endpoint Detection & Response
Identificare payloads diversi da quelli generati da Cobalt Strike, Metasploit, Empire, Covenant ecc…

Network Detection & Response
Identificare connessioni di "Beaconing" o connessioni anomale nella rete interna

SIEM / SOC / Blue Team

Allenare il Blue Team a riconoscere vettori d'attacco più moderni e complessi

Assumed Breach

Il modello Assumed Breach presume che la compromissione sia già avvenuta e ci permette di lavorare immediatamente sulle capacità di Detection & Response nell'attività di Post-Exploitation

Phishing	Il vettore d'attacco per l'accesso iniziale ancora più utilizzato: Documenti di Microsoft Office malevoli, pagine per la cattura di credenziali.
Insider Threat	Una persona interna che intenzionalmente o inconsciamente compromette degli asset interni all'organizzazione.
0-day Exploits	La cronaca recente ci ha mostrato anche che prodotti di fascia alta non sono esenti da Exploit 0-day: Microsoft Exchange, VPN…
Compromissione già avvenuta	Presuppone che la compromissione sia già in atto e che qualcuno si stia già muovendo all'interno della rete sottraendo informazioni sensibili.

Linee di difesa implementate dagli EDR/XDR

YARA Scans

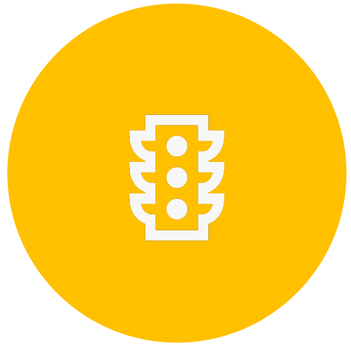
Malicious strings and Opcodes, Signatures…

Userland Hooks

Windows API Hooking, PEB Hooking…

Telemetria Avanzata

Event Tracing for Windows Threat Intelligence (EtwTi), Kernel Callbacks



“Malicious Score”

Determina se il processo contenga o stia eseguendo codice malevolo

YARA Scans - Evasion

Encoding, Encryption
Mascheramento dello shellcode tramite encoding o encryption, Self-Decryption routines, Sleep-Obfuscation

API Hashing, Function Call Obfuscation
Risoluzione “on-the-fly” delle API necessarie alle successive operazioni offensive.

Binary Signature
I file firmati sono tendenzialmente sottoposti a meno controlli.

Uncommon Data Sections
Alcune sezioni dei file PE sono completamente ignorate dagli EDR.

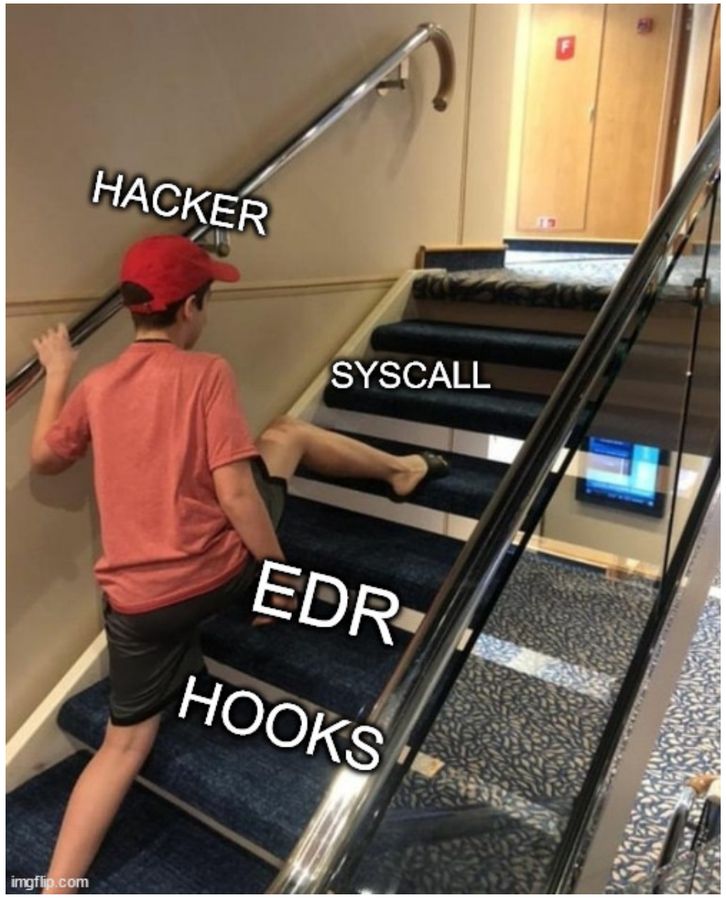
Hooking - Evasion

“Classic” API Unhooking
Sostituire la DLL in memoria con una copia pulita letta dal disco.

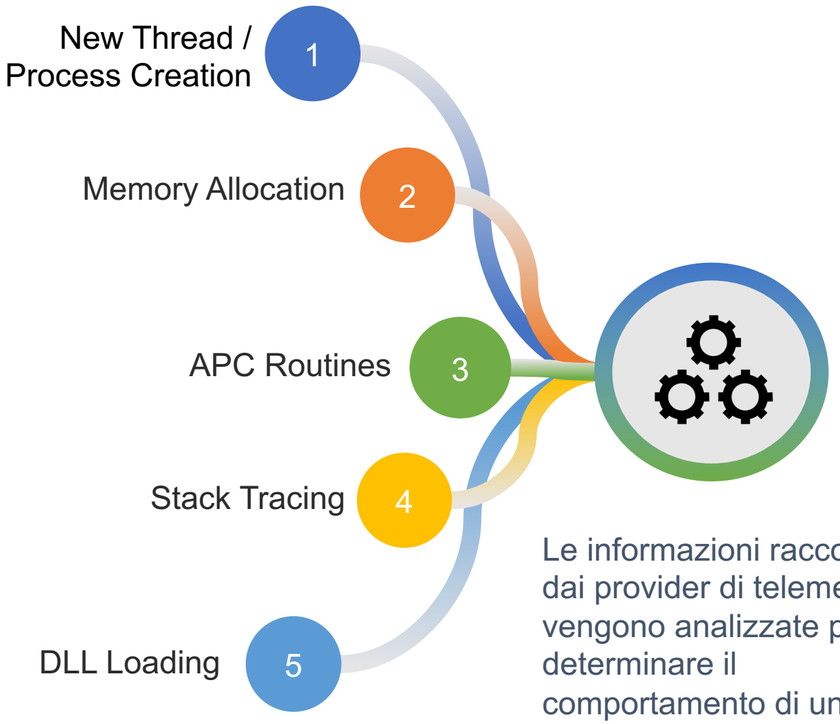
Direct / Indirect Syscall
Invocazione diretta o indiretta della Syscall bypassando l’Hook dell’EDR.

Dynamic SSN Resolution
Risoluzione “on-the-fly” del System Service Number.

Hardware Breakpoints
Manomettere i parametri della syscall dopo aver forzato l’EDR a ritenere “innocua” l’operazione.



EtwTi, Kernel Callbacks - Evasion

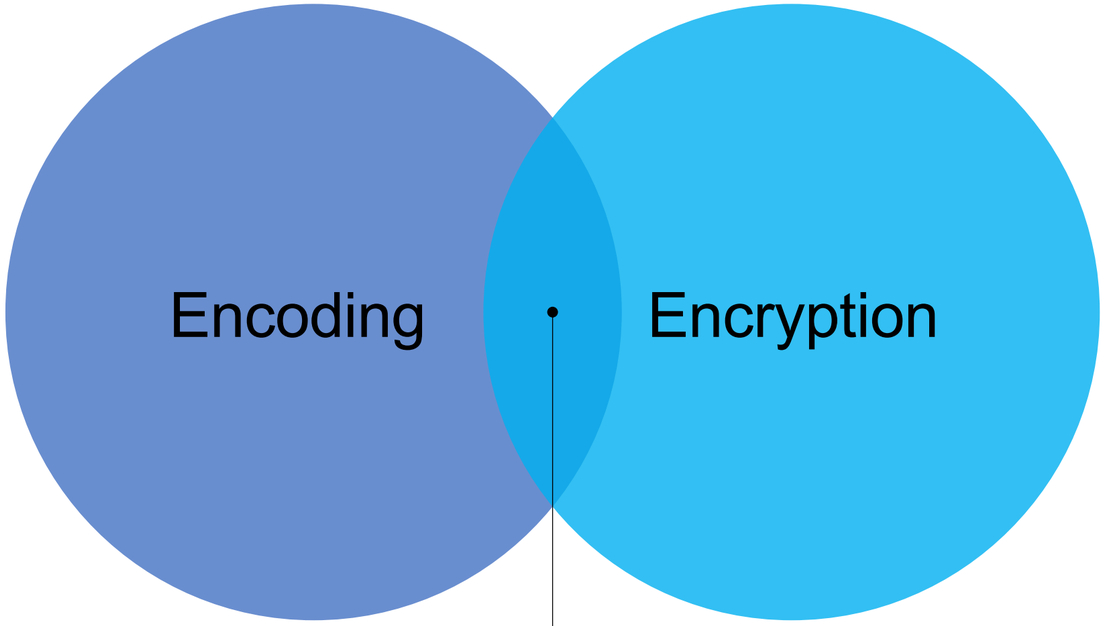


Le informazioni raccolte dai provider di telemetria vengono analizzate per determinare il comportamento di un processo, anche tramite l'ausilio dell'intelligenza artificiale.

01	Thread Stack Spoofing
02	ROP Chains
03	CMDLine Spoofing
04	"Normalizzare" il comportamento del malware

Encoding vs Encryption

BASE64
Trasformare il dato con un algoritmo conosciuto in modo che sia facilmente usufruibile a diversi tipi di sistemi.



AES, RC4, XOR

Trasformare il dato con un algoritmo conosciuto e una secret-key in modo che solo il reale destinatario possa usufruire del dato originale.

Nascondere il payload agli occhi dei motori AV che possono identificarlo tamite binary-matching o pattern facilmente riconoscibili.

XOR: implementazione classica

```
VOID XOR(PCHAR data, SIZE_T data_len, PCHAR key, SIZE_T key_len) {
    INT j = 0;

    for (INT i = 0; i < data_len; i++) {
        if (j == key_len - 1)
            j = 0;

        data[i] = data[i] ^ key[j];
        j++;
    }
}
```

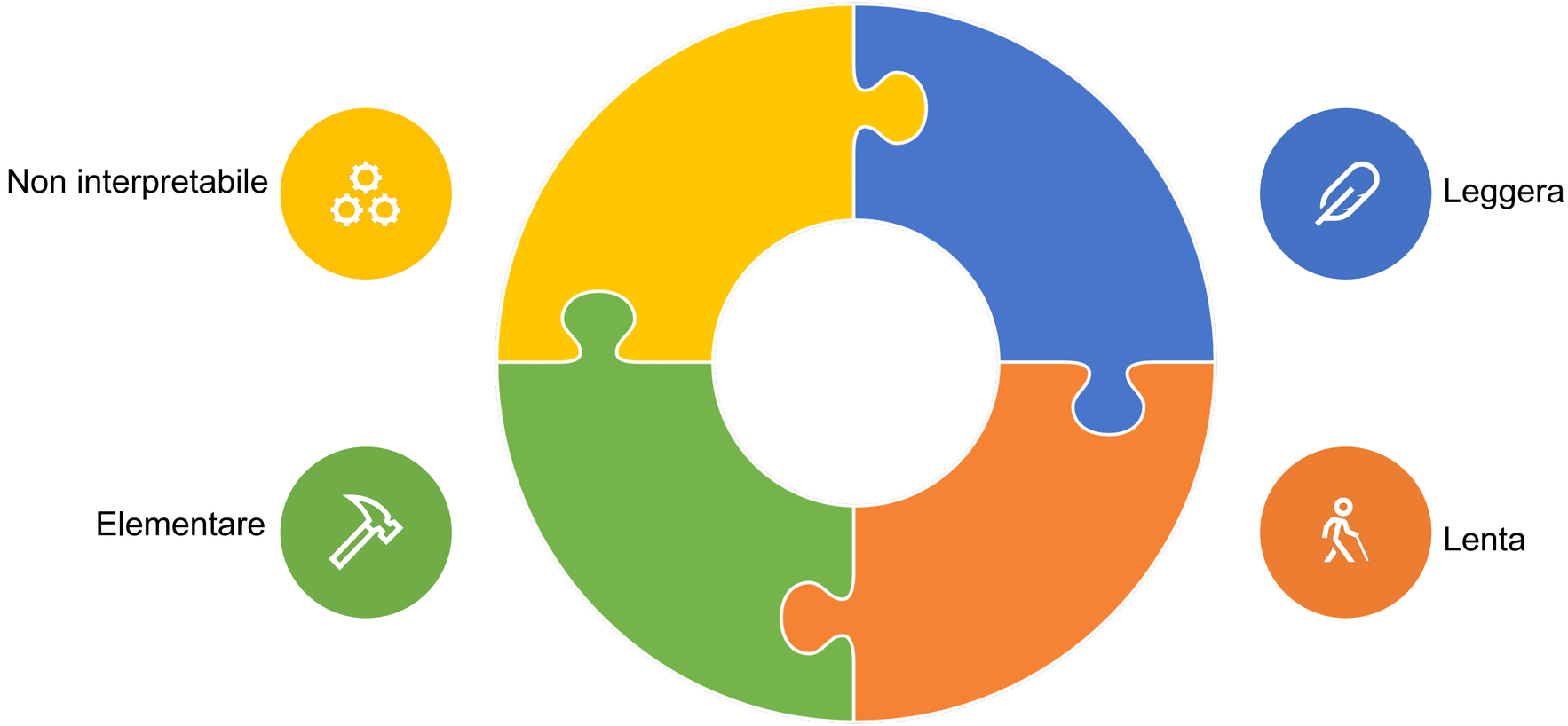
```
C:\Users\pikered\Desktop\dev>ThreatCheck.exe -f xor.exe
[+] Target file size: 125440 bytes
[+] Analyzing...
[!] Identified end of bad bytes at offset 0x453
```

Classica implementazione in C della crittografia XOR con chiave multi-byte

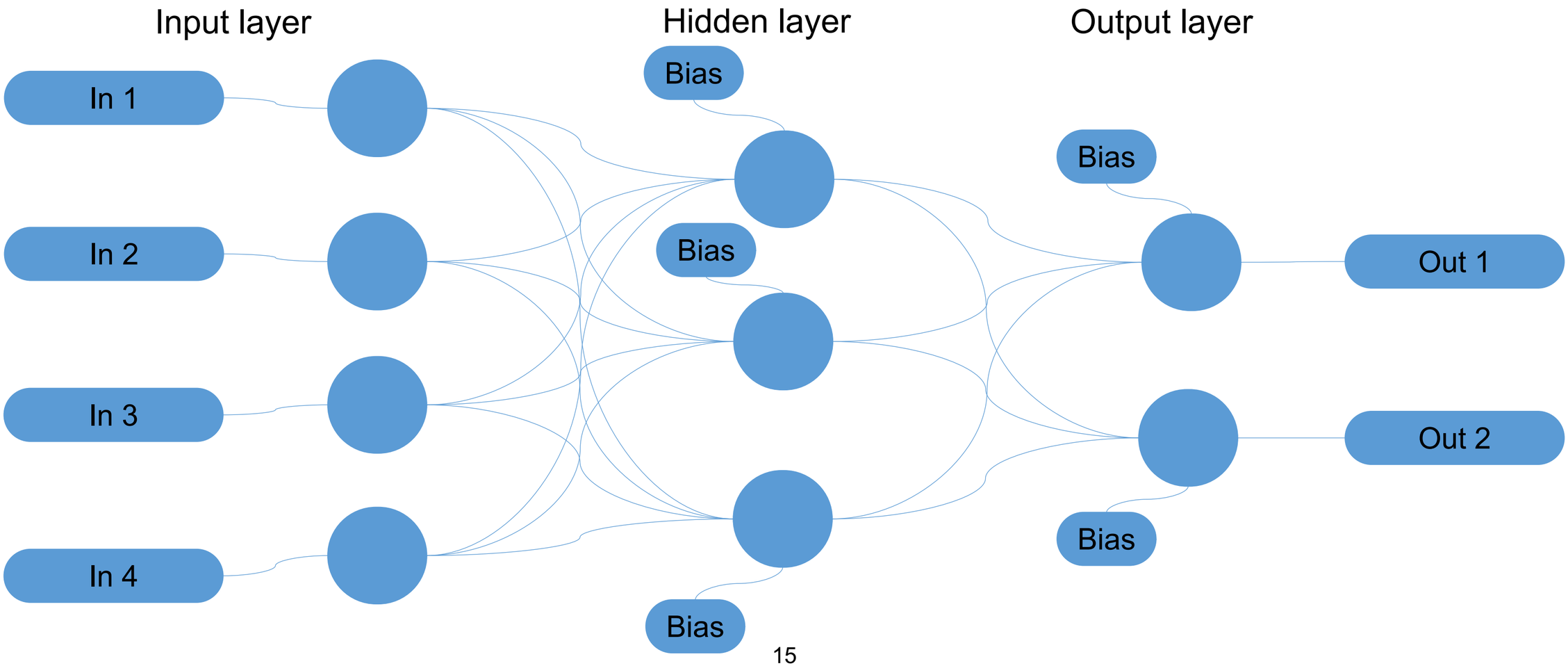
Set di istruzioni considerate come sospette in corrispondenza della routine di decryption

```
.text:000000014000100B loc_14000100B:                          ; DATA XREF: .rdata:000000014001BAB8↓o
.text:000000014000100B                                         ; .rdata:000000014001BAC8↓o ...
.text:000000014000100B                 mov     [rsp+8+arg_0], rsi
.text:0000000140001010                 xor     r10d, r10d
.text:0000000140001013                 xor     esi, esi
.text:0000000140001015                 xor     ebx, ebx
.text:0000000140001017                 dec     r9
.text:000000014000101A                 mov     rdi, rdx
.text:000000014000101D                 mov     r11, rcx
.text:0000000140001020
.text:0000000140001020 loc_140001020:                          ; CODE XREF: sub_140001000+52↓j
.text:0000000140001020                 xor     ecx, ecx
.text:0000000140001022                 movsxd  rdx, r10d
.text:0000000140001025                 cmp     rdx, r9
.text:0000000140001028                 lea     r11, [r11+1]
.text:000000014000102C                 cmovnz  rcx, rsi
.text:0000000140001030                 movzx   eax, byte ptr [rcx+r8]
.text:0000000140001035                 lea     rsi, [rcx+1]
.text:0000000140001039                 xor     [r11-1], al
.text:000000014000103D                 xor     eax, eax
.text:000000014000103F                 cmp     rdx, r9
.text:0000000140001042                 cmovnz  eax, r10d
.text:0000000140001046                 inc     ebx
.text:0000000140001048                 lea     r10d, [rax+1]
.text:000000014000104C                 movsxd  rax, ebx
.text:000000014000104F                 cmp     rax, rdi
.text:0000000140001052                 jb      short loc_140001020
.text:0000000140001054                 mov     rsi, [rsp+8+arg_0]
.text:0000000140001059                 mov     rbx, [rsp+8+arg_8]
.text:000000014000105E                 pop     rdi
.text:000000014000105F
```

XOR: implementazione alternativa



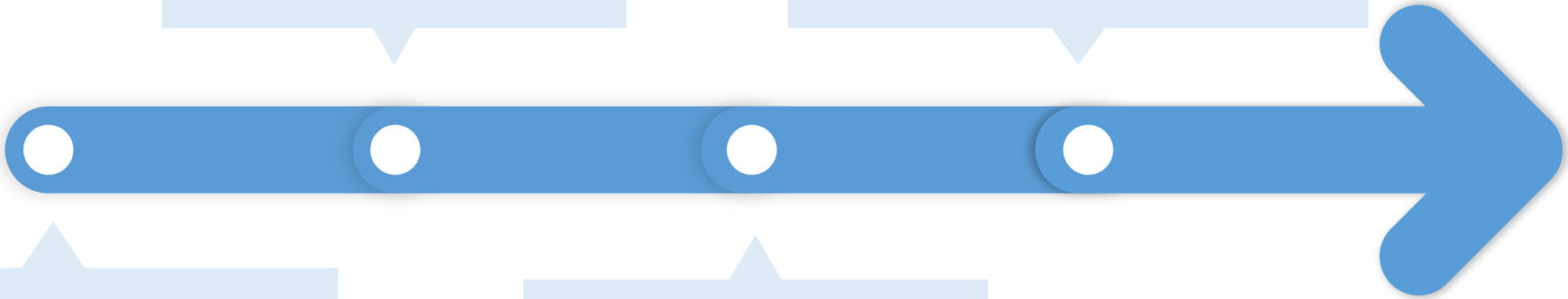
Reti neurali



Rete neurale da 0

$$e^x = \sum_{i=1}^{n} \frac{x^i}{i!} + o(x^n)$$

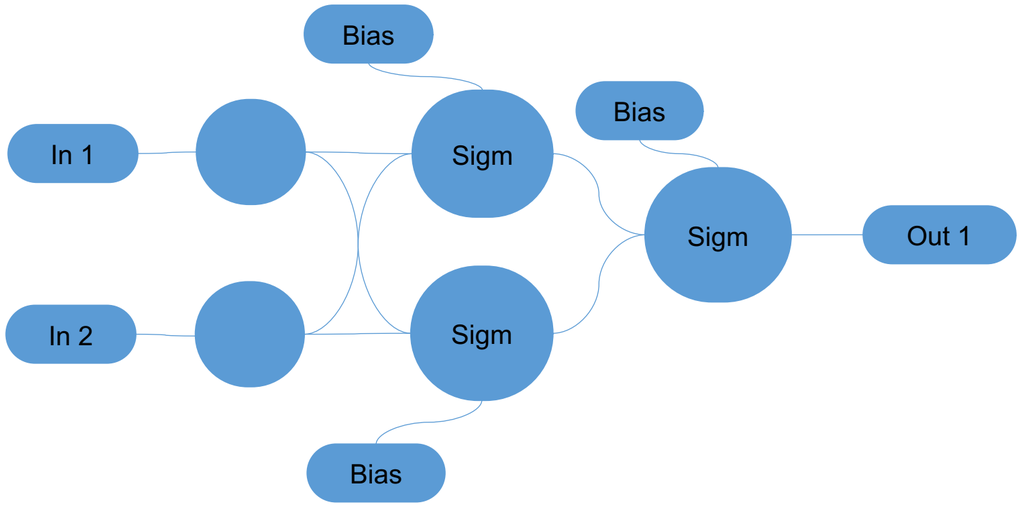
$$f\left(bias + \sum_i weight_i * input_i\right)$$



$$\ln(x) = 2\sum_{i=1}^{n} \frac{1}{2i-1}\left(\frac{x-1}{x+1}\right)^{2i-1} + o(x^n)$$

$$sigmoid(x) = \frac{1}{1+e^{-x}}$$

XOR: implementazione con rete neurale

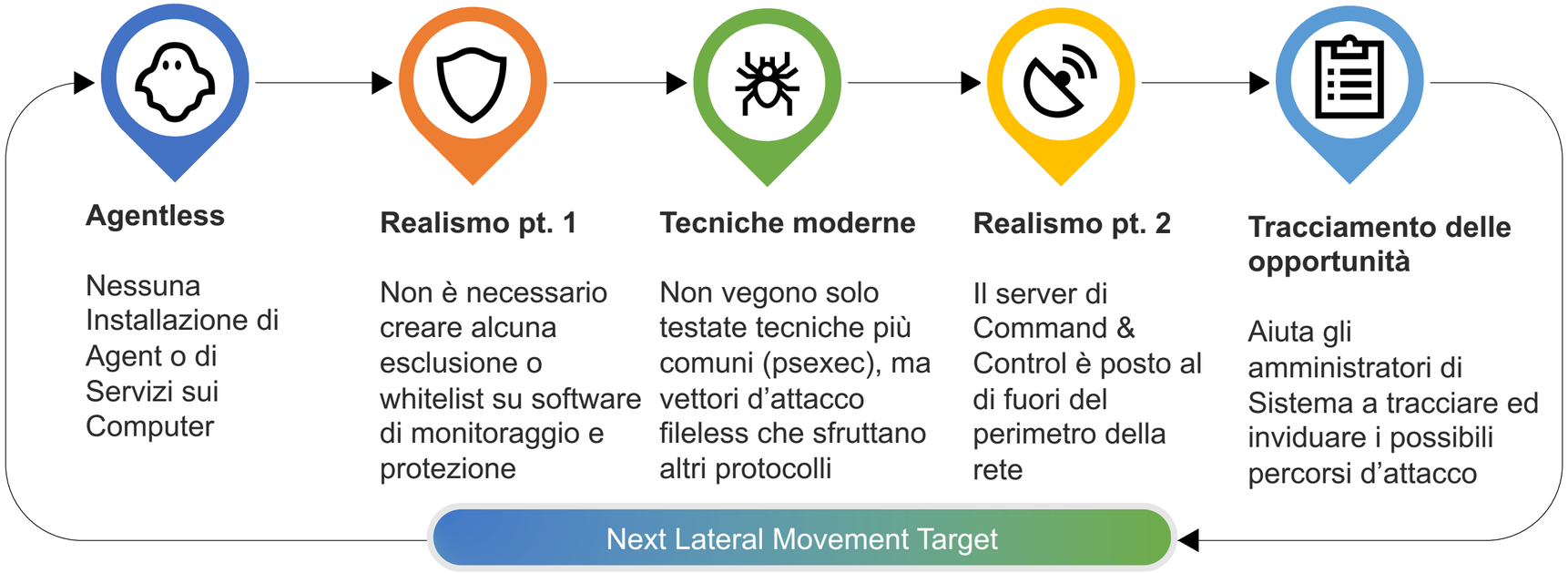


A	B	A⊕B
0	0	0
1	0	1
0	1	1
1	1	0

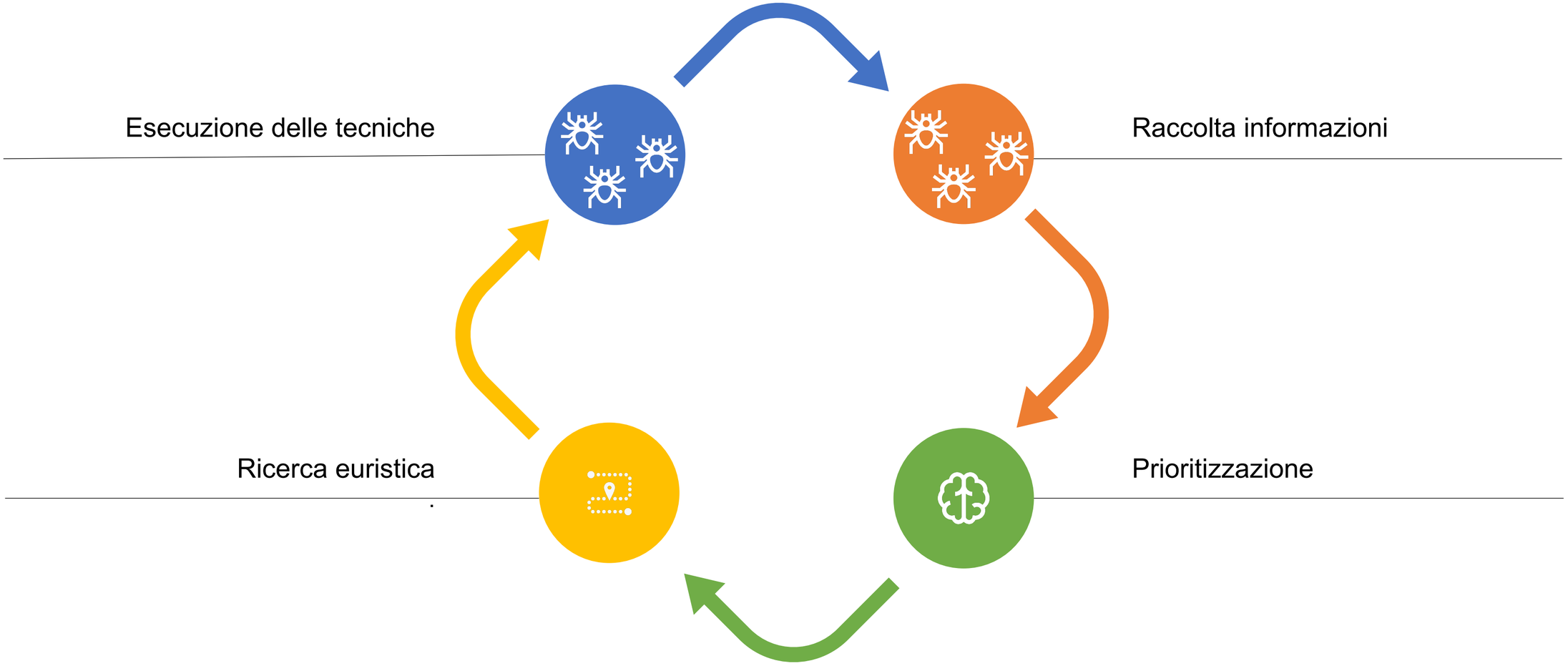
```
C:\Users\pikered\Desktop\dev>ThreatCheck.exe -f xor_neural.exe
[+] No threat found!
```

Lateral Movement

Come il BAS simula la propagazione di un’infezione all’interno della rete e può aiutarci a bloccarla



IA per un’automazione realistica

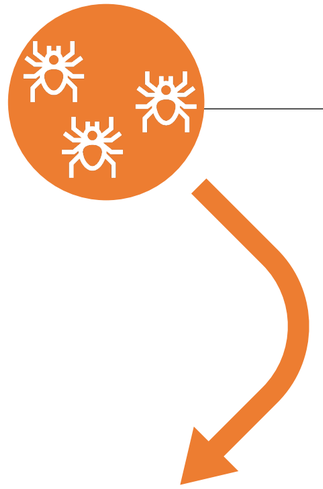


IA per un’automazione realistica

Gli implant catturano informazioni sugli oggetti nella rete e sulle tecniche eseguite

Esfiltrazione stealth

Conoscenza limitata della rete, apprendimento online



Raccolta informazioni

IA per un’automazione realistica

Il motore di elaborazione individua le tecniche eseguibili e assegna ad esse delle priorità

Diversi gradi di importanza degli obiettivi

Diversi gradi di rischio ed efficacia delle tecniche

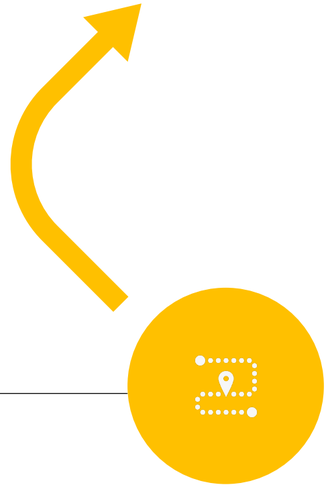
Prioritizzazione

IA per un’automazione realistica

Il motore di elaborazione calcola un piano d’attacco multi-agente con orizzonte temporale variabile

Emulazione di un Red Team

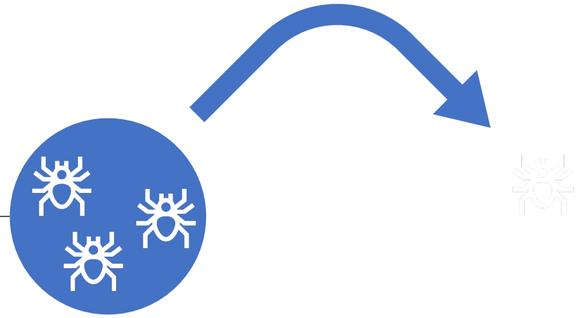
Raggiungimento degli obiettivi ed espansione nella rete



Ricerca euristica

IA per un’automazione realistica

Esecuzione delle tecniche

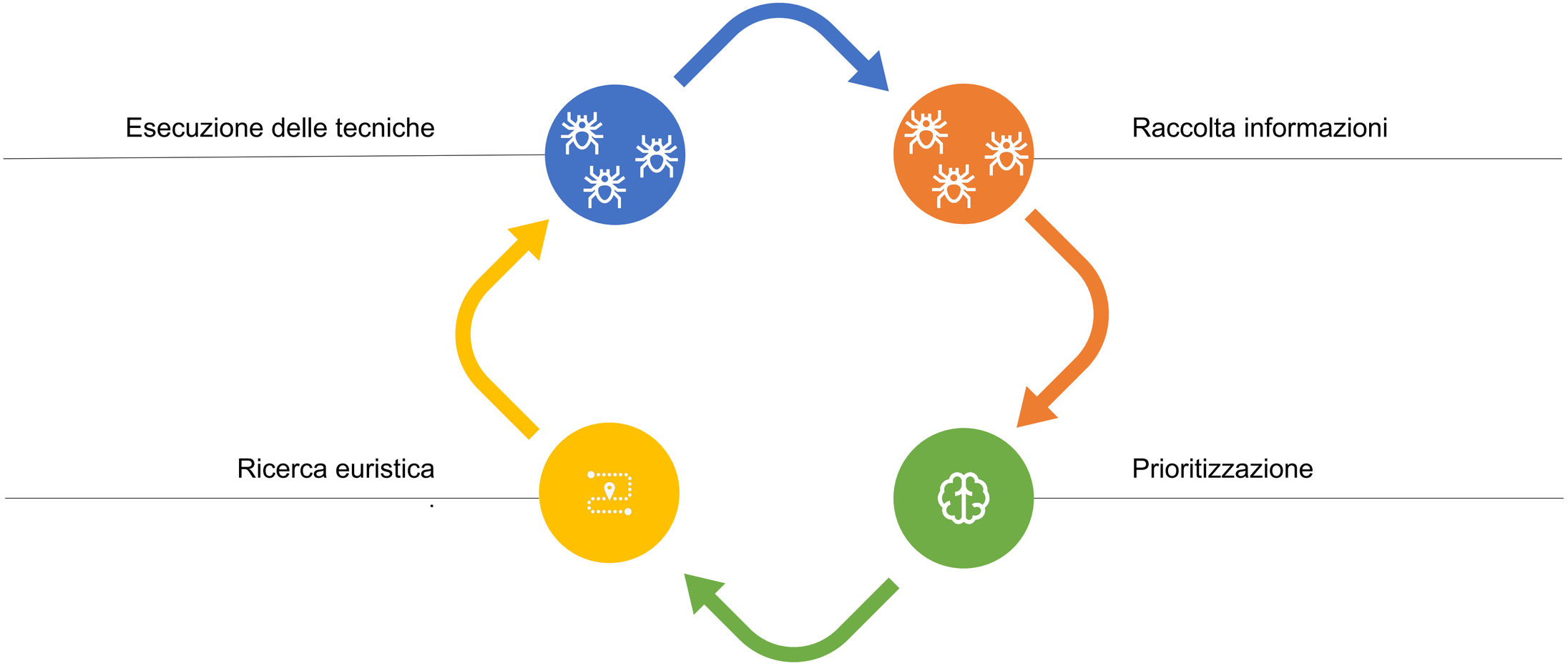


Il motore di elaborazione assegna le tecniche individuate agli implant, che le eseguono in parallelo

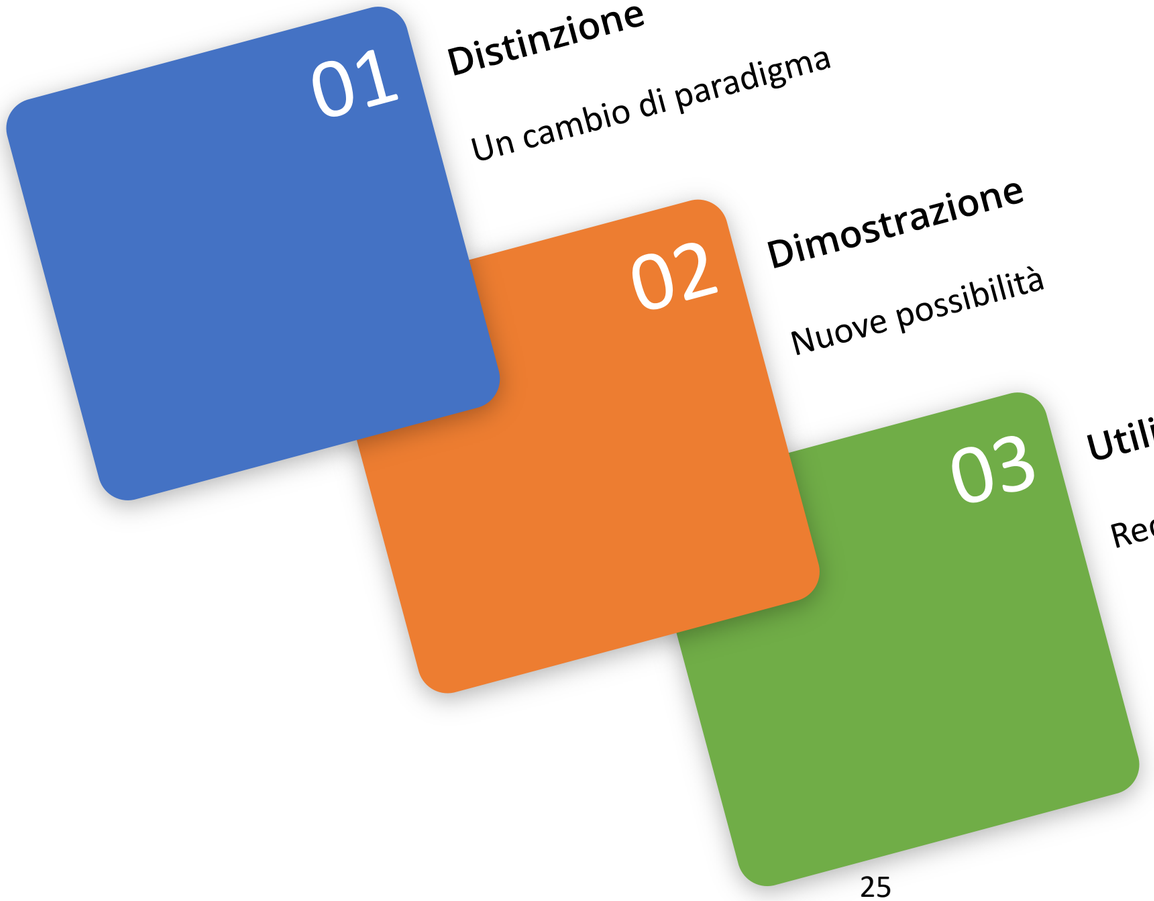
Effettiva compromissione degli host

Creazione di nuovi implant

IA per un’automazione realistica



Concludendo



Distinzione

Un cambio di paradigma

Dimostrazione

Nuove possibilità

Utilizzo

Red Teaming come attività di routine

Q&A

pikered

VIENI A TROVARCI AL NOSTRO STAND!

LinkedIn

www.pikered.com