



Red Team Automation Framework
Cadriciel d'automatisation informatique offensif

GUNGNIR

**NOUS
DÉCOUVRIR**

 QONGZI

<https://qongzi.com/>

RED TEAM

RED TEAM

Simulated adversary, attempting to identify and exploit potential weaknesses within the organization's cyber defenses...



...identifying an attack path that breaches the organization's security defense through real-world attack techniques

VS

BLUE TEAM

Incident response consultants guide the IT security team on where to make improvements to stop sophisticated types of cyberattacks and threats...



...leaving the IT security team responsible for maintaining the internal network against various types of risk

RAINBOW TEAM

RED TEAM

OFFENSIVE ATTACK TEAM



Tasks include:

- Ethical hacking
- Penetration testing
- Black box testing
- Social engineering
- Web app scanning
- Vulnerability exploitation

PURPLE TEAM

DATA COLLECTION & IMPLEMENTATION TEAM



Tasks include:

- Improvement facilitation
- Data analytics
- Gap analysis
- Red vs Blue skill testing
- System improvements
- Collaborative security

BLUE TEAM

DEFENSIVE PROTECT TEAM



Tasks include:

- Infrastructure security
- Damage control
- Incident response (IR)
- Operational security
- Threat hunting
- Digital forensics



RED TEAM

Key considerations

History and reputation | Risk management | Governance | Security & confidentiality | Collaborative approach | Language support | Staff competence | R&D

|  Company Requirements | RT manager Requirements |  RT Team Requirements |
|---|--|--|
| <ul style="list-style-type: none"> ✓ At least five references from previous assignments related to intelligence-led red team tests ✓ Adequate indemnity insurance in place to cover activities which were not agreed upon in the contract and/or which stem from misconduct, negligence... ✓ Robust risk management and security controls in place (information) ✓ RT providers should have robust methodologies in place to conduct the most advanced and innovative forms of red team testing. The RT provider should aspire to conduct the highest level tests, such that they can mimic a nation state actor and demonstrate sophistication, agility, use of advanced techniques and perseverance to match the level of defense of an entity. The RT provider should have processes in place to be able to clearly explain its methodologies, how they evolve and how they result in effective and high quality red team tests. | <ul style="list-style-type: none"> ✓ At least five years experience in red team testing including three years managing intelligence led red team tests ✓ Up to date CV and at least three references from previous assignments of the Red team test Manager to be provided to the entity, specifically red team testing activities ✓ Background checks on the Red Team test Manager are conducted by the RT provider (as a minimum). Enhanced background checks are conducted as required by the national authorities. ✓ Ideally, the Red Team test Manager should have appropriate recognised qualifications and certifications for threat intelligence (as set out in Annex 1) | <ul style="list-style-type: none"> ✓ Sufficient experience of the Red team members. Expectation for each member: at least two years of experience in red team testing ✓ Up to date CV for each member of the team to be provided to the entity ✓ Multi-disciplinary composition of the red team with a broad range of knowledge and skills such as: business knowledge, red team testing, penetration testing, reconnaissance, threat intelligence, risk management, exploit development, physical penetration, social engineering, vulnerability analysis and combination thereof ✓ Background checks on each member of the RT are conducted by the RT provider (as a minimum). Enhanced background checks are conducted as required by the national authorities ✓ Ideally the Red Team should have appropriate recognised qualifications and certifications (as set out in Annex 1) |
| <p>Key deliverables</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> <p>Capture flags</p>  </div> <div style="text-align: center;"> <p>Red team test report</p>  </div> <div style="text-align: center;"> <p>360 feedback meeting/ Replay</p>  </div> </div> | | |

RED TEAM AUTOMATION

Conference Paper

PDF Available

Automated red teaming: a proposed framework for military application

January 2007

DOI:[10.1145/1276958.1277345](https://doi.org/10.1145/1276958.1277345)

Source · [DBLP](#)

Conference: Genetic and Evolutionary Computation Conference, GECCO 2007, Proceedings, London, England, UK, July 7-11, 2007

Authors:



Chwee Seng Choo



Ching Lian Chua



Victor Su-Han Tay

Defence Science and Technology Agenc...



Download citation



Copy link



Download full-text PDF



Read full-text

RED TEAM AUTOMATION

Modèles actuels :

- Focalisés soit sur la mise en place d'une infrastructure en préparation de tests manuels, soit sur des scénarios post-compromission orientés autour des mouvements latéraux
- Un autre modèle émerge avec des métiers comme le DevSecOps et la généralisation de l'évaluation continue (Randori by IBM)
- Un besoin se fait également sentir lors de l'entraînement des ressources de réponse à incident et il devient nécessaire de produire un panel de menaces diversifiées
- Automatisation personnelle du Bug Bounty, Automatisation de l'analyse de malware, de la réponse à incident ...

Ces modèles ne représentent pas l'adaptabilité de la menace, et privent l'état de compromission, d'adaptation apportée par l'humain

QUI SOMMES NOUS ?

YG

Quelle méthode utiliser pour modéliser l'état d'esprit, le cheminement de pensée et la cognition d'un pirate informatique ? Donne moi un modèle, puis fournis-moi un exemple d'application



EXEMPLES DE L'EXISTANT

RTA

Infrastructure

DevSecOps

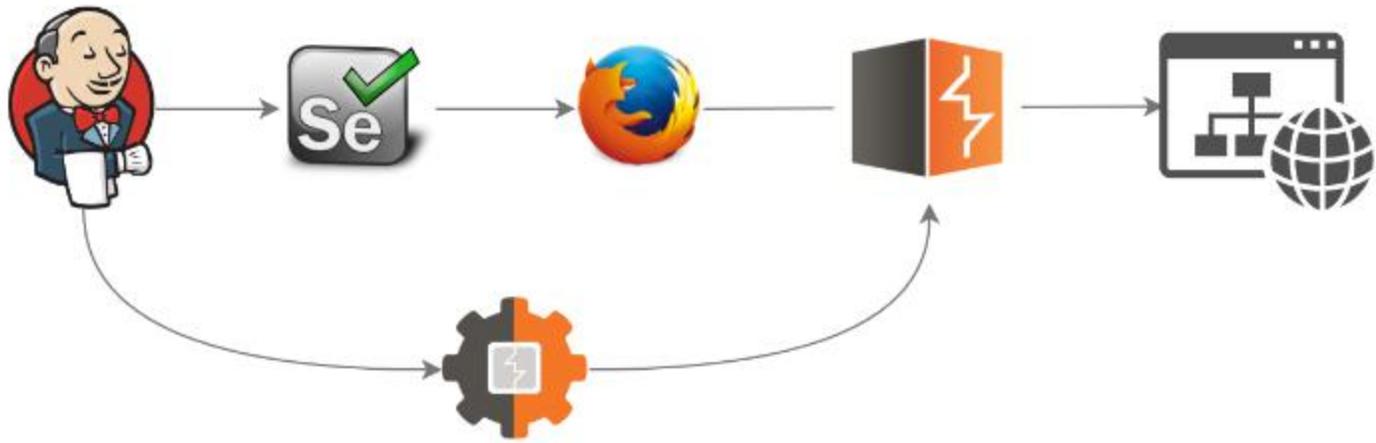
SCRIPTING



burpa: Burp Automator

License GPL v3

A Burp Suite Automation Tool

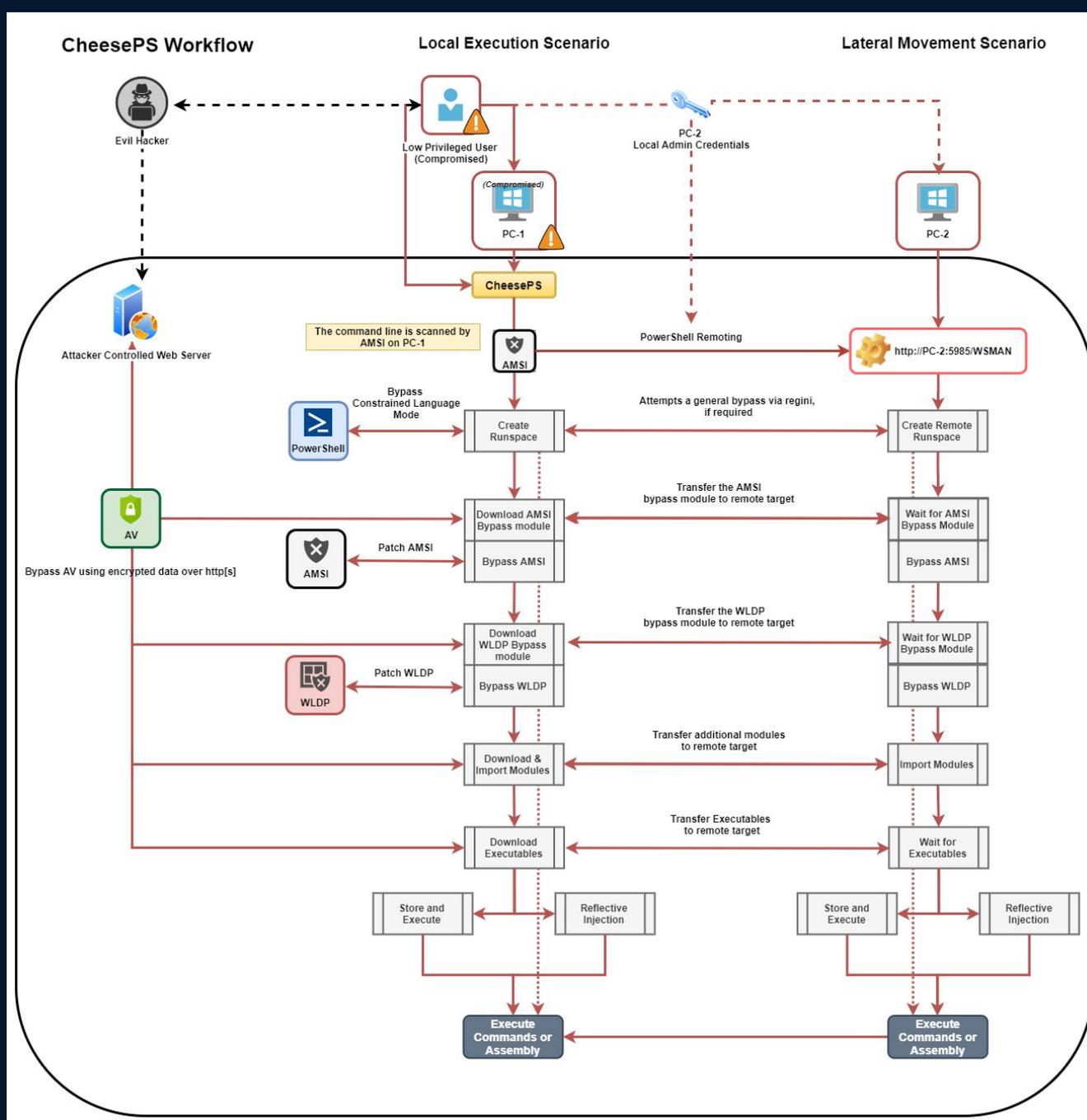


```
graph LR; Selenium[Se] --> Firefox[Firefox]; Firefox --> BurpSuite[Burp Suite]; BurpSuite --> Dashboard[Dashboard]; Selenium --> BurpSuite; BurpSuite --> Selenium;
```

The diagram illustrates a workflow for automating web testing. It starts with Selenium (Se), which interacts with Firefox. Firefox then sends data to Burp Suite (represented by a cube with a lightning bolt). Burp Suite outputs to a dashboard (represented by a screen with a globe). There are also feedback loops: Selenium sends data to Burp Suite, and Burp Suite sends data back to Selenium.

LATERAL MOVE

<https://github.com/klezVirus/CheeseTools>



RED TEAM CHAOS ENGINEERING



Infection Monkey

- 1. Run C&C Server ✓
- 2. Run Monkey ✓
- 3. Infection Map ✓
- 4. Security Report ✓
- Start Over

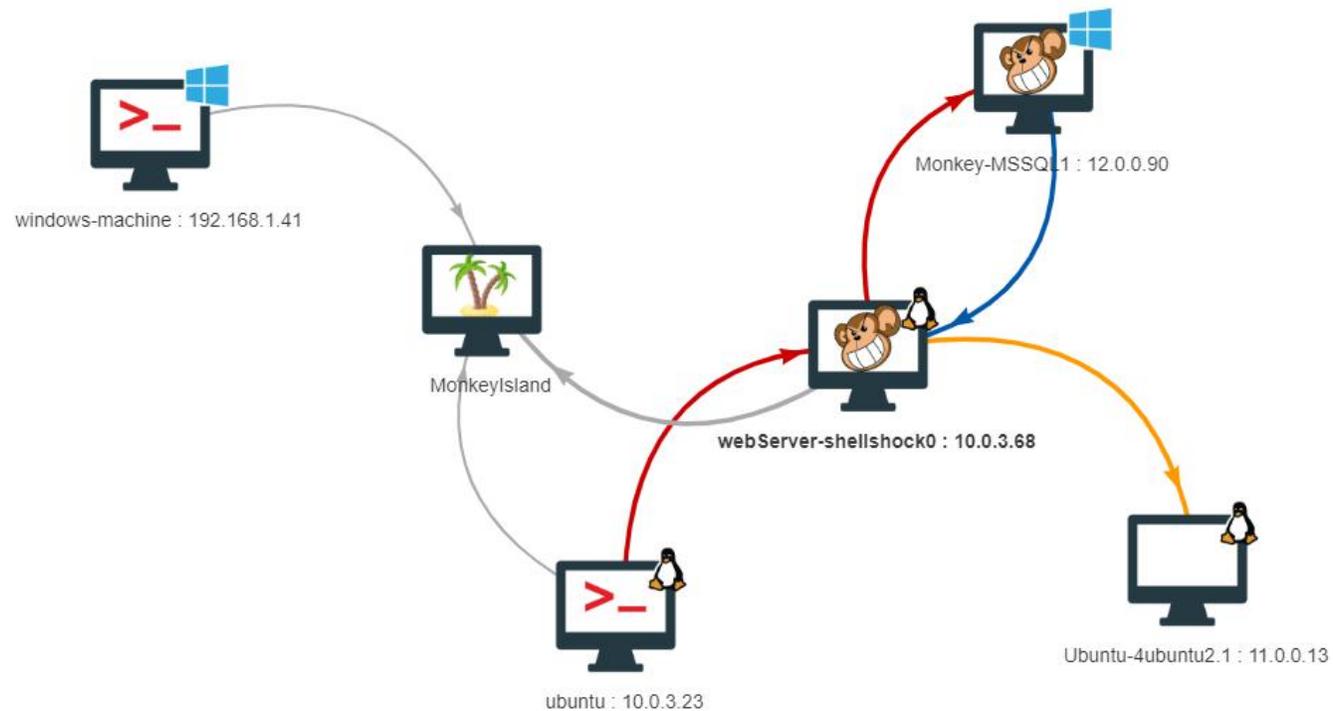
Configuration

Log

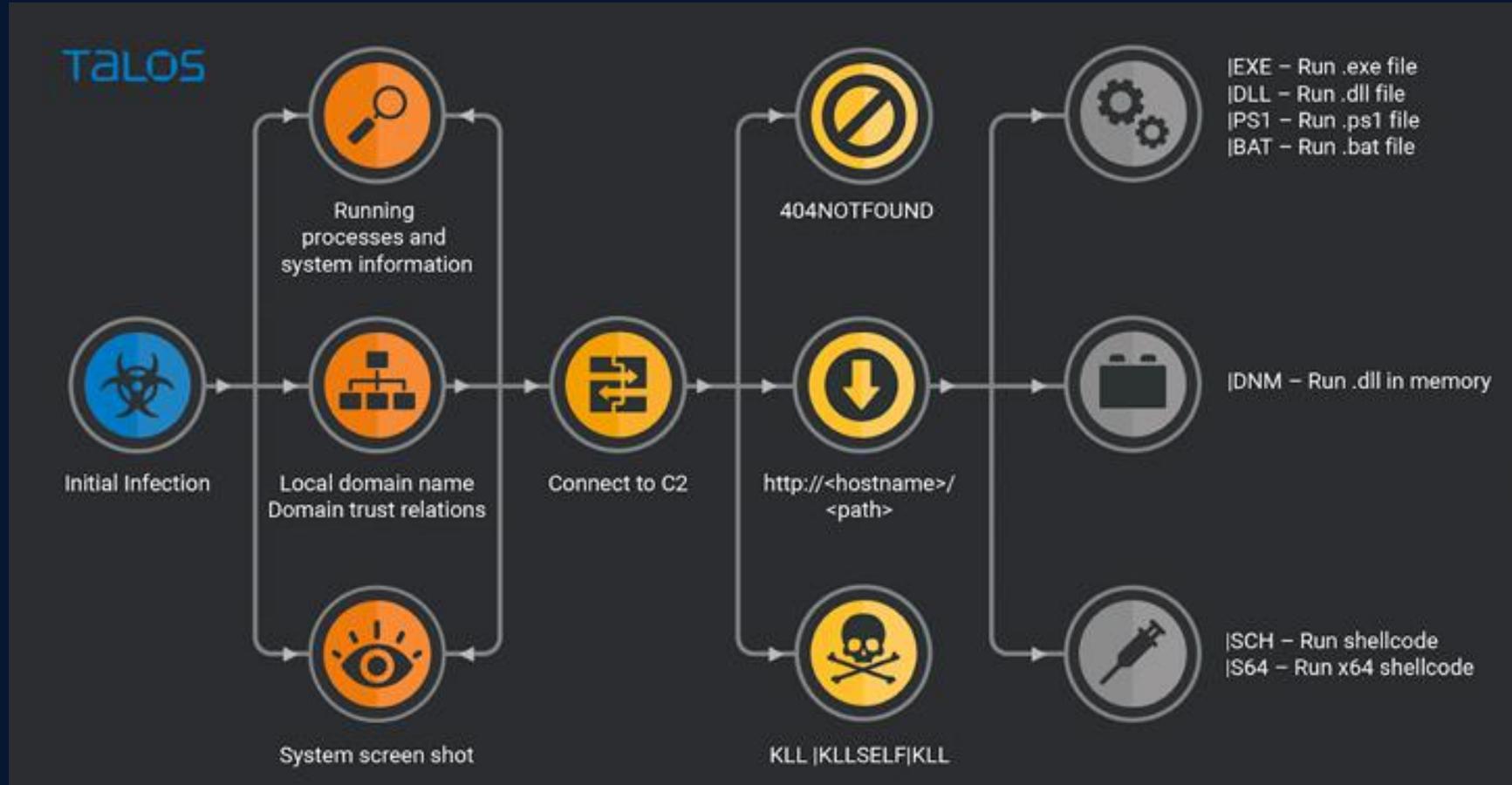
Powered by  GuardiCore
License

3. Infection Map

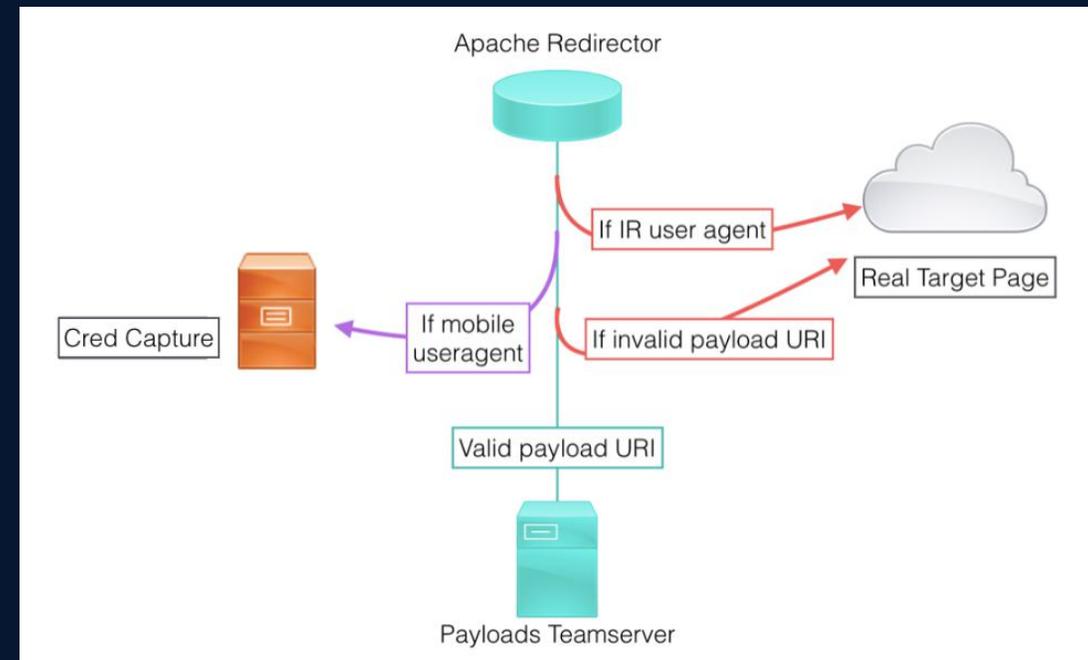
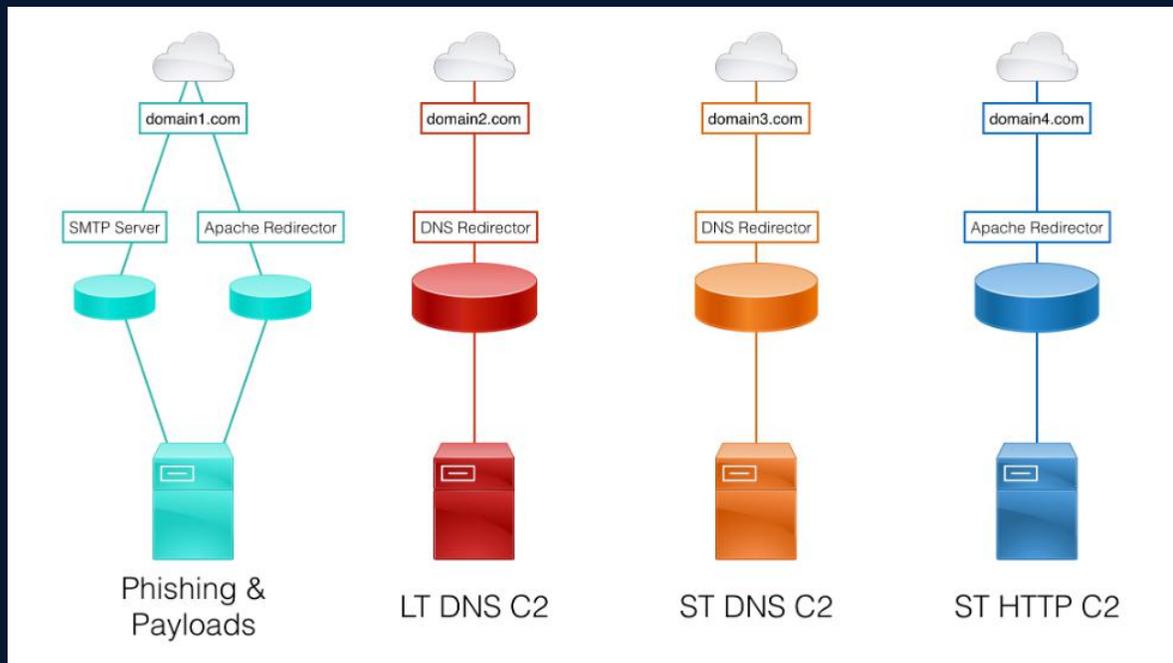
Legend: Exploit — | Scan — | Tunnel — | Island Communication —



TRUEBOT



RED TEAM INFRASTRUCTURE



<https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki>

RED TEAM INFRASTRUCTURE

Overlord – Red Teaming Automation

License MIT 2020 Black Hat Arsenal stars 547



OVERLORD

Overlord provides a python-based console CLI which is used to build Red Teaming infrastructure in an automated way. The user has to provide inputs by using the tool's modules (e.g. C2, Email Server, HTTP web delivery server, Phishing server etc.) and the full infra / modules and scripts will be generated automatically on a cloud provider of choice. Currently supports AWS and Digital Ocean. The tool is still under development and it was inspired and uses the [Red-Baron](#) Terraform implementation found on Github.

A demo infrastructure was set up in our blog post <https://qsecure.com.cy/resources/publications/overlord/>.

For the full documentation of the tool visit the Wiki tab at <https://github.com/qsecure-labs/overlord/wiki>.

RED TEAM TRAINING



CyberRange Diateam

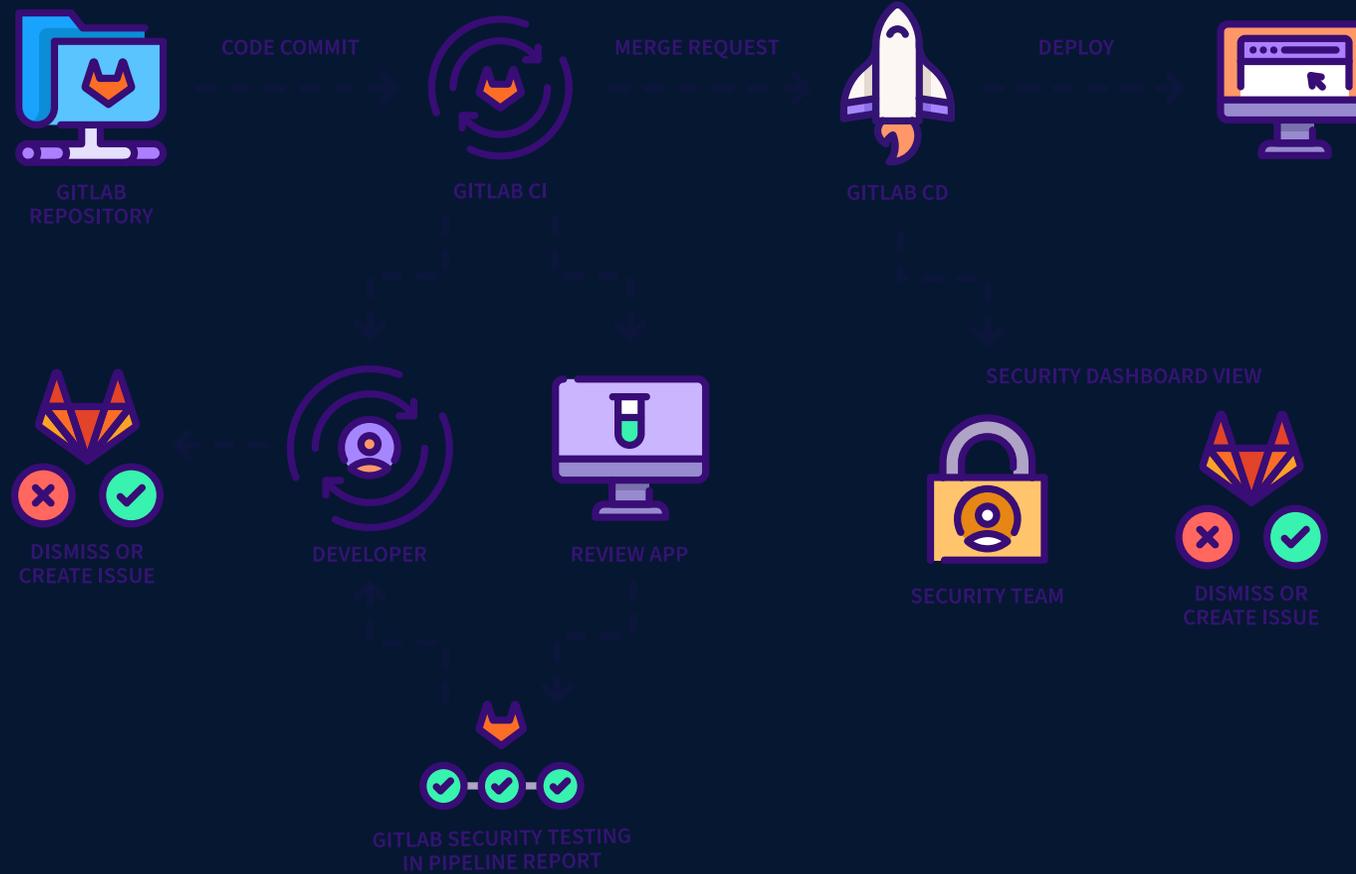
The screenshot shows the Malice Supervision web interface. The main heading is 'Détails de l'instance Scénario Pentest'. The interface is divided into several sections:

- Instances:** A list containing 'Scénario Pentest'.
- Configuration:** A menu with options: 'Voir tout', 'Scénarios', 'Hypenseurs', 'Tâches en cours', 'Gestion des réseaux', 'Utilisateur', 'Se déconnecter', and 'Documentation'.
- Machines:** A table listing various machines with their status and progress bars.

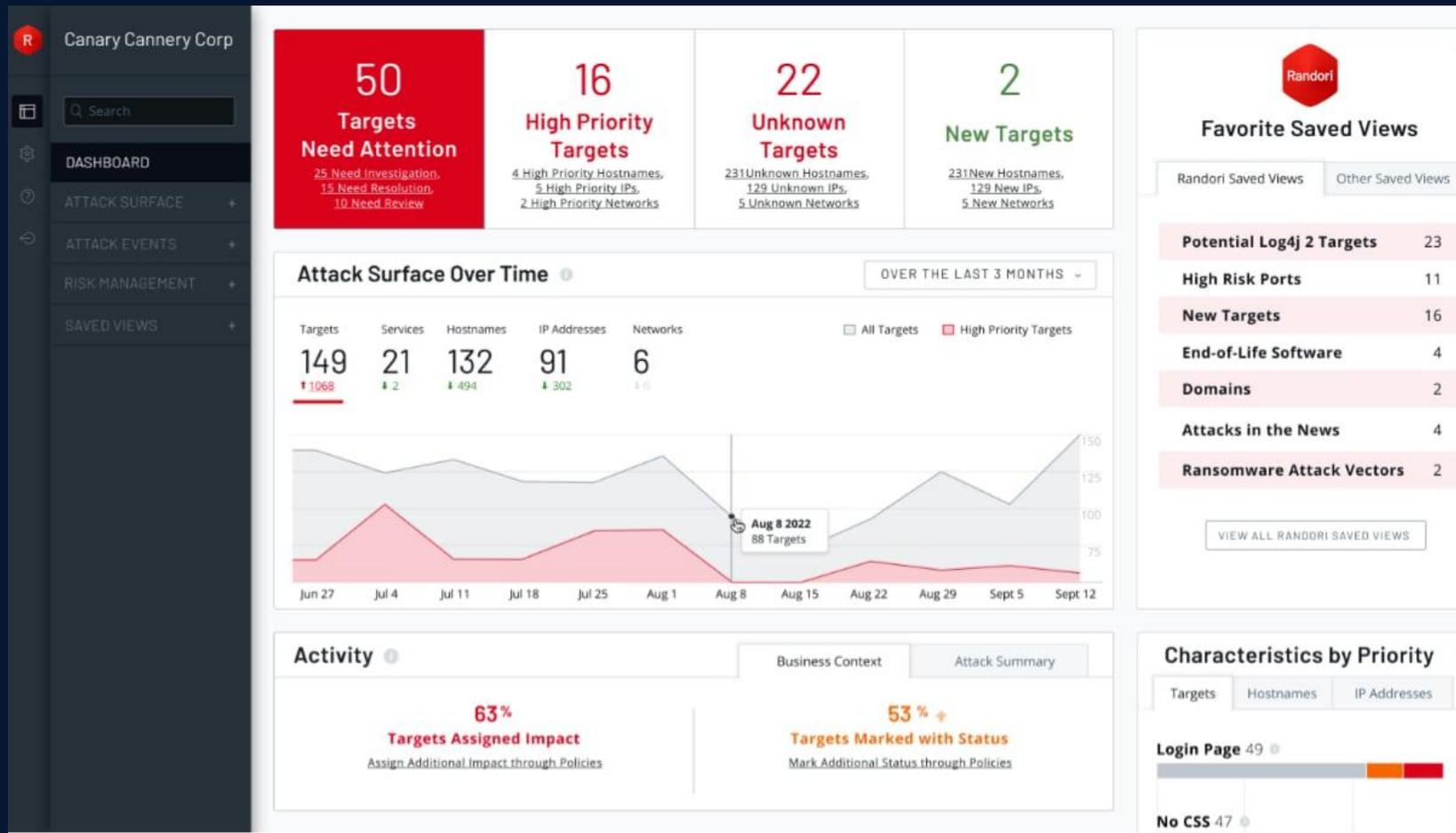
| ARRÊTER | DÉMARRER | REDÉMARRER | | | | | |
|--------------------------|--------------------------|--------------------------|----------|----------------|-----|-----|--|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | nom | Adresse IP | CPU | RAM | Actions |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Global | | | | |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ad | 10.10.0.754 | 0% | 5% | <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | internet | 10.20.0.102 | 0% | 10% | <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | jenkins | 10.10.0.103 | 0% | 1% | <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | mail | 172.30.0.123 | 0% | 3% | <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | mysql | 168.254.80.158 | 0% | 7% | <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | garage | | 0% | 28% | <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | router | | 0% | 12% | <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | homer | 172.30.0.124 | 0% | 1% | <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> |

Malice Sysdream

GITLAB



CONTINUOUS AUTOMATED RED TEAMING (CART)



CONTINUOUS AUTOMATED RED TEAMING (CART)



Sleep well at night with Automated Security Validation

Continuously Validate
Your Cyber Defenses
with a Click of a Button



Pentera

RED TEAM AUTOMATION

The screenshot shows the GitHub interface for the 'endgameinc / RTA' repository. At the top, there are navigation links for Code, Issues (1), Pull requests (6), Actions, Projects, Security, and Insights. Below this, the repository name 'endgameinc / RTA' is displayed as 'Public'. The main content area shows a commit history table with columns for the commit message, commit hash, date, and number of commits. The most recent commit is by 'Devon Kerr' on August 17, 2018, with 15 commits. The commit message is 'Merge branch 'RTA_moar_scripts_and_light_reorg''. Below the commit history, there is a list of files and folders: 'red_ttp', 'LICENSE.txt', 'README.md', '__init__.py', 'attack-navigator-coverage.json', and 'run_all.py'. The 'README.md' file is selected, and its content is displayed below. The README title is 'Red Team Automation (RTA)'. The text in the README describes the framework's purpose, its composition of Python scripts, and its behavior in performing malicious activities.

endgameinc / RTA Public

<> Code Issues 1 Pull requests 6 Actions Projects Security Insights

master 2 branches 0 tags Go to file Add file <> Code

| Commit Message | Commit Hash | Date | Commits |
|--|-------------|-----------------|------------|
| Devon Kerr Merge branch 'RTA_moar_scripts_and_light_reorg' | 89152d6 | on Aug 17, 2018 | 15 commits |
| red_ttp Merge branch 'master' into RTA_moar_scripts_and_light_reorg | | 4 years ago | |
| LICENSE.txt It was a dark and stormy night when the RTA repository was restruc... | | 5 years ago | |
| README.md updated README to describe use of run_all.py scriptrunner | | 5 years ago | |
| __init__.py Initial RTA commit | | 5 years ago | |
| attack-navigator-coverage.json It was a dark and stormy night when the RTA repository was restruc... | | 5 years ago | |
| run_all.py It was a dark and stormy night when the RTA repository was restruc... | | 5 years ago | |

☰ README.md

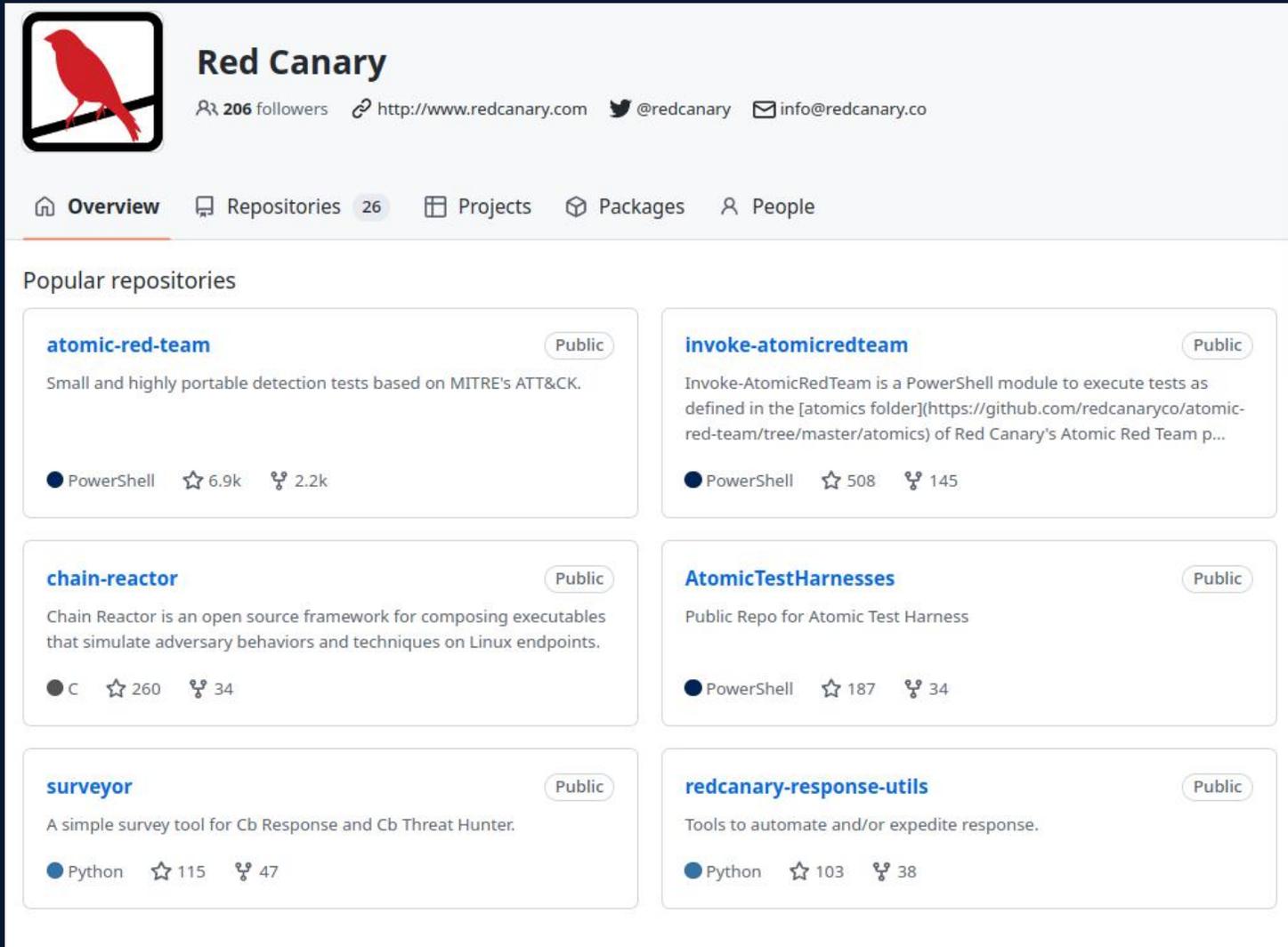
Red Team Automation (RTA)

RTA provides a framework of scripts designed to allow blue teams to test their detection capabilities against malicious tradecraft, modeled after [MITRE ATT&CK](#).

RTA is composed of python scripts that generate evidence of over 50 different ATT&CK tactics, as well as a compiled binary application that performs activities such as file timestopping, process injections, and beacon simulation as needed.

Where possible, RTA attempts to perform the actual malicious activity described. In other cases, the RTAs will emulate all or parts of the activity. For example, some lateral movement will by default target local host (though with parameters typically allow for multi-host testing). In other cases, executables such as cmd.exe or python.exe will be renamed to make it appear as if a Windows binary is doing non-standard activities.

ATOMIC RED TEAM



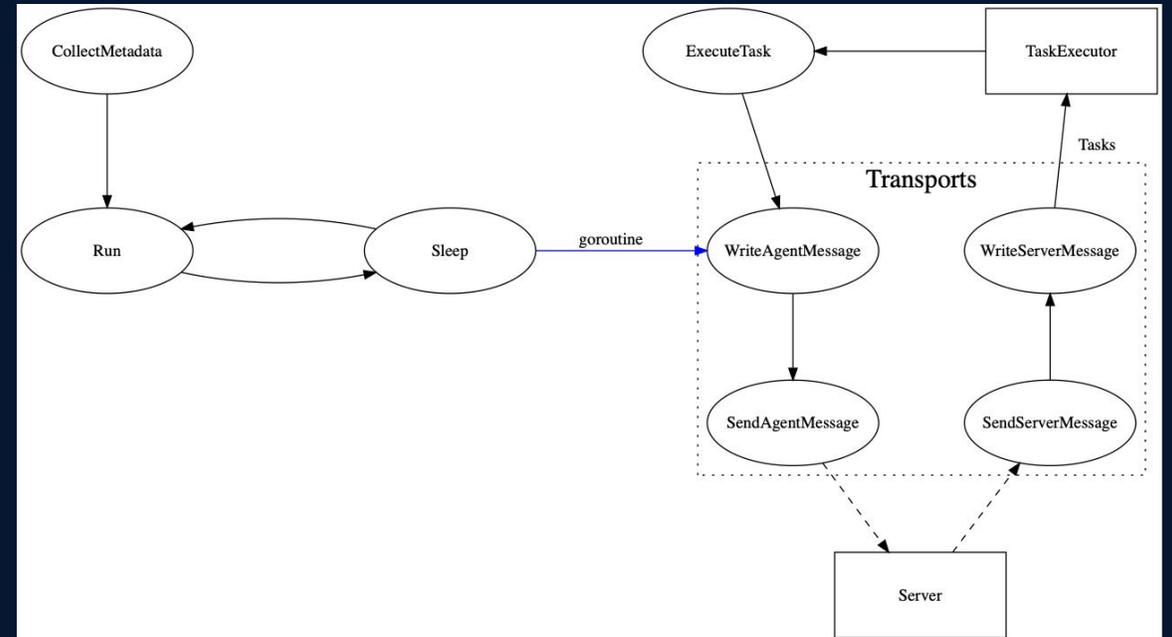
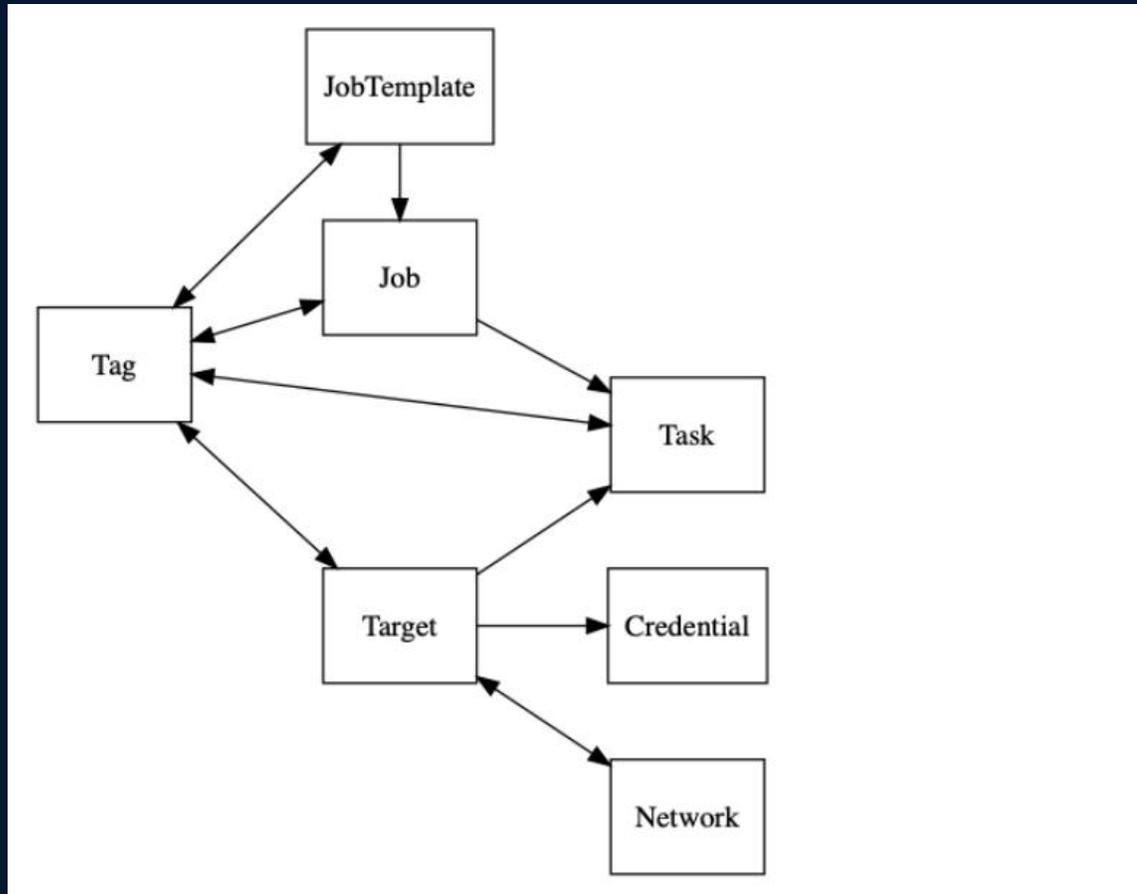
Red Canary
206 followers | <http://www.redcanary.com> | [@redcanary](https://twitter.com/redcanary) | info@redcanary.co

Overview | Repositories (26) | Projects | Packages | People

Popular repositories

- atomic-red-team** (Public)
Small and highly portable detection tests based on MITRE's ATT&CK.
PowerShell | 6.9k stars | 2.2k forks
- invoke-atomicredteam** (Public)
Invoke-AtomicRedTeam is a PowerShell module to execute tests as defined in the [atomics folder](https://github.com/redcanaryco/atomic-red-team/tree/master/atomics) of Red Canary's Atomic Red Team p...
PowerShell | 508 stars | 145 forks
- chain-reactor** (Public)
Chain Reactor is an open source framework for composing executables that simulate adversary behaviors and techniques on Linux endpoints.
C | 260 stars | 34 forks
- AtomicTestHarnesses** (Public)
Public Repo for Atomic Test Harness
PowerShell | 187 stars | 34 forks
- surveyor** (Public)
A simple survey tool for Cb Response and Cb Threat Hunter.
Python | 115 stars | 47 forks
- redcanary-response-utils** (Public)
Tools to automate and/or expedite response.
Python | 103 stars | 38 forks

MODÉLISATION



<https://github.com/KCarretto/paragon/>

LE SOULÈVEMENT DES IA

Graph

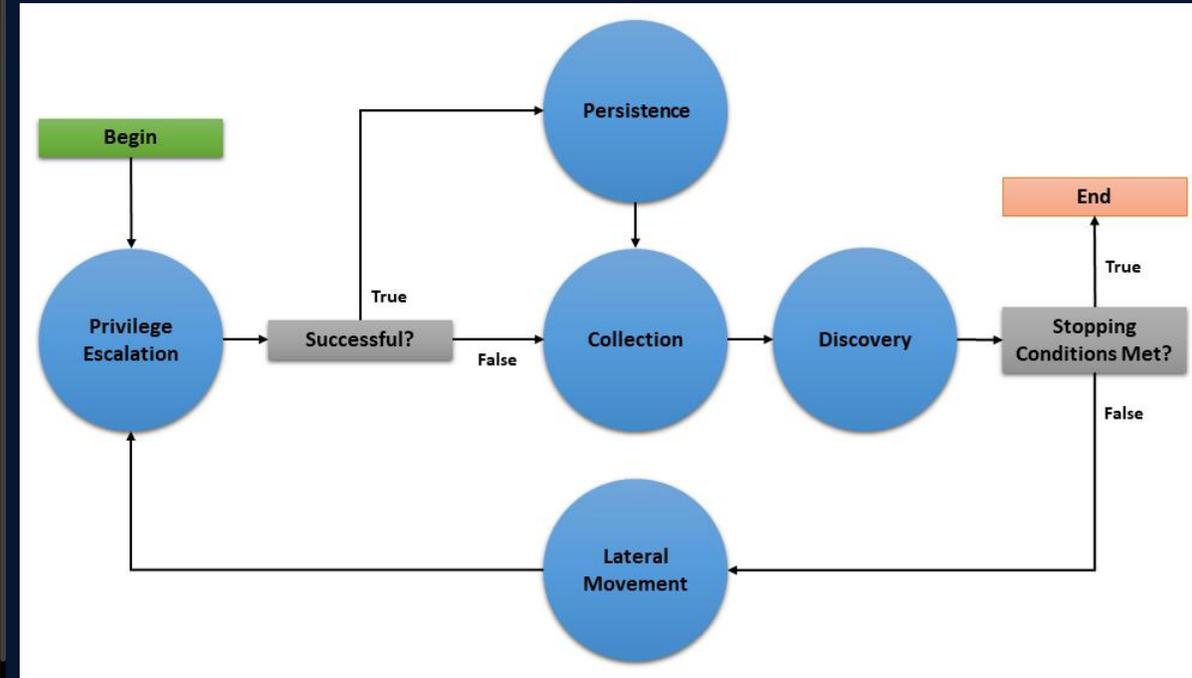
Modèle cognitif

NLP

ARBRE DE DÉCISION

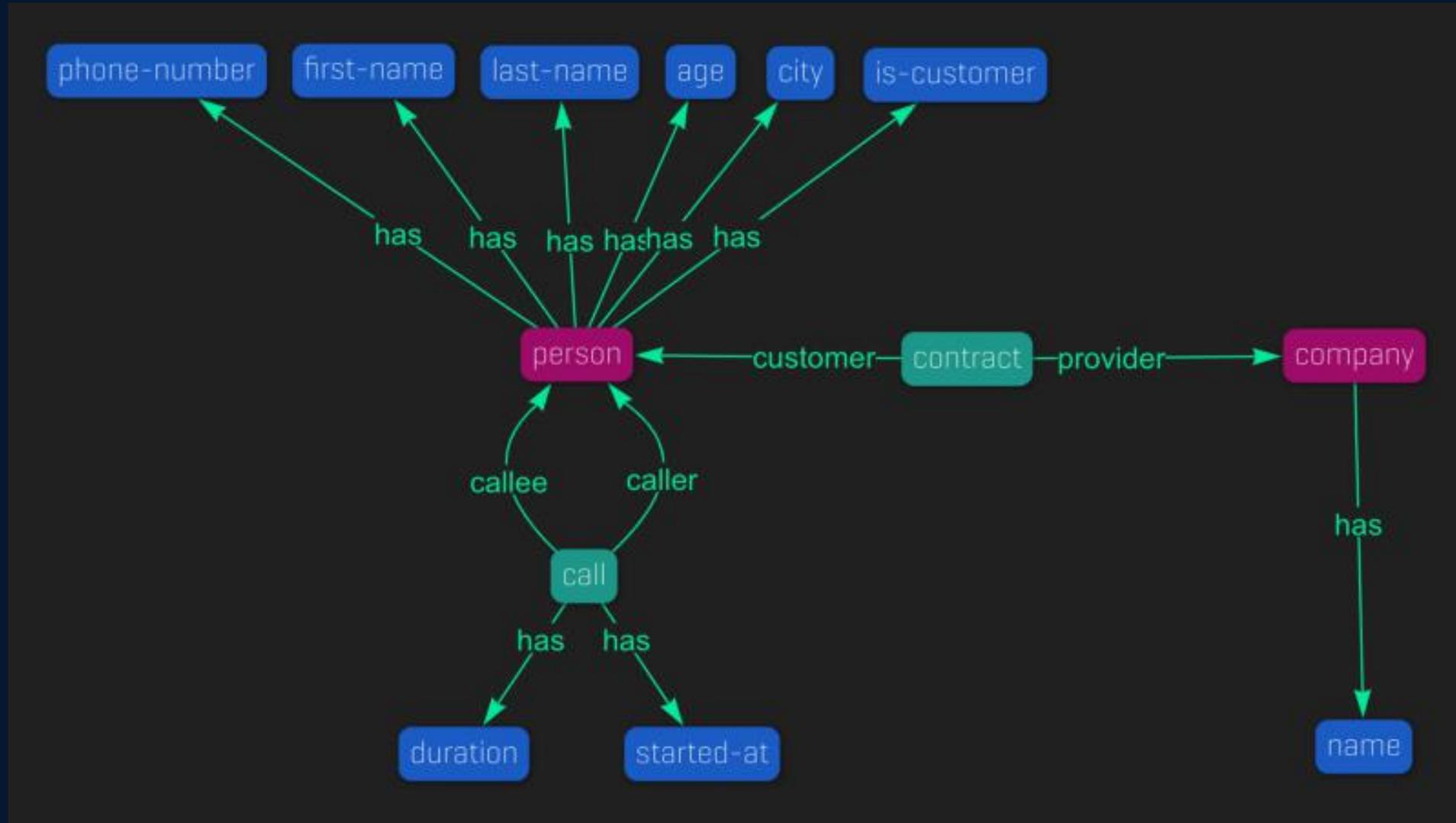
The screenshot displays the MITRE Caldera Operations interface. At the top, there are navigation tabs for 'agents', 'abilities', 'adversaries', 'operations', and 'atomic'. The 'operations' tab is selected. Below the tabs, the 'Operations' section shows a 'Worm Operation' with a 'Current state: running'. The interface includes controls for 'Download', 'Unlink', 'Stop', 'Pause', and 'Run 1 Link'. A table lists the operation's history with columns for 'Decide', 'Status', 'Link/Ability Name', 'Agent IPaw', 'Host', 'pid', 'Link Command', and 'Link Output'. The table shows three entries for 'Reverse nslookup IP' operations.

| Decide | Status | Link/Ability Name | Agent IPaw | Host | pid | Link Command | Link Output |
|------------------------------|---------|---------------------|------------|------------|------|--------------|-------------|
| 3/12/2022, 11:07:19 AM GMT-7 | Success | Collect ARP details | rxdgkk | VAN-DST-10 | 8232 | View Command | View Output |
| 3/12/2022, 11:07:39 AM GMT-7 | Success | Reverse nslookup IP | rxdgkk | VAN-DST-10 | 6188 | View Command | View Output |
| 3/12/2022, 11:08:19 AM GMT-7 | Success | Reverse nslookup IP | rxdgkk | VAN-DST-10 | n/a | View Command | No output. |

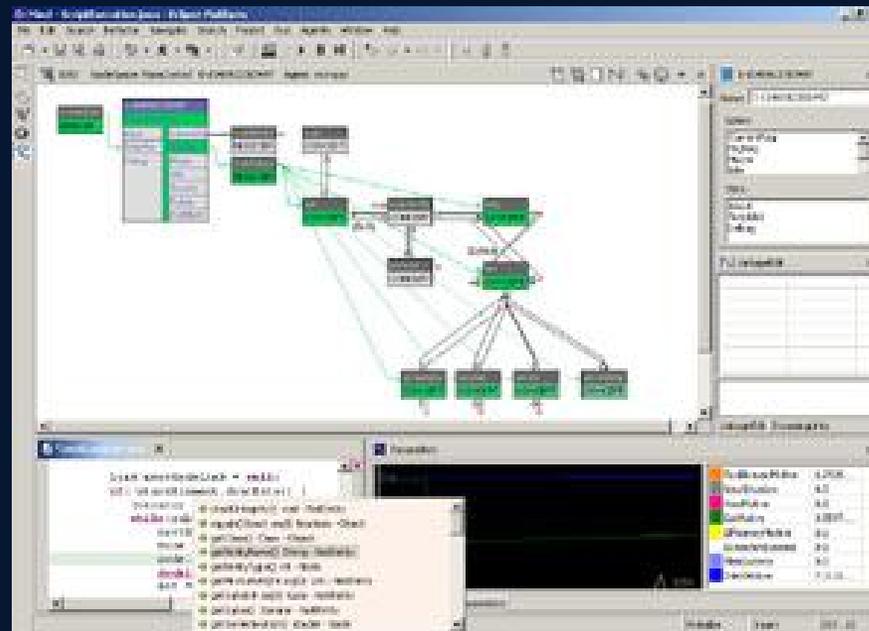
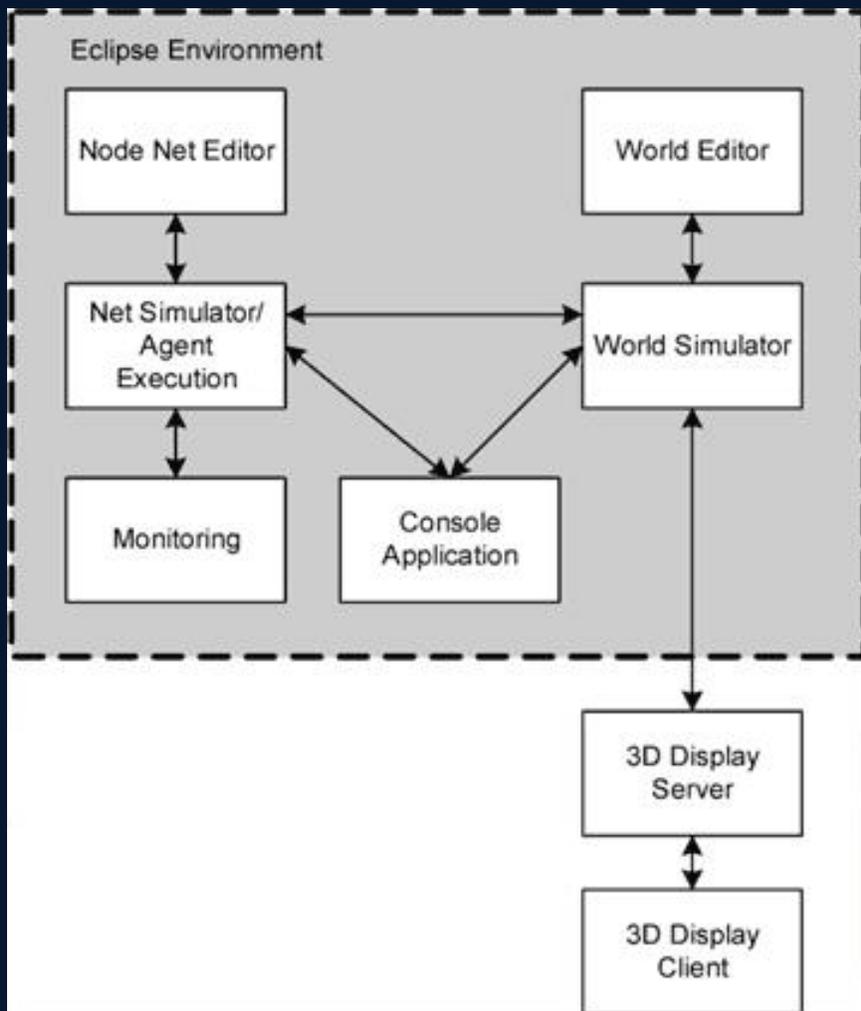


Mitre Caldera

GRAPH DE CONNAISSANCES



MICROPSI



<http://www.cognitive-ai.com/>

NLP CAN HELP ?

YG

Quelle méthode utiliser pour modéliser l'état d'esprit, le cheminement de pensée et la cognition d'un pirate informatique ? Donne moi un modèle, puis fournis-moi un exemple d'application



OU PAS ?

YG

comment modéliser le cheminement de pensée d'un pirate informatique ? Propose une méthode. Donne un exemple de modèle



Il n'est pas possible de modéliser exactement le cheminement de pensée d'un pirate informatique, car chaque individu a sa propre façon de raisonner et de procéder. Cependant, il est possible de proposer une méthode générale pour modéliser le processus de piratage informatique.

Voici une approche possible :

1. Identifier les objectifs du pirate informatique : qu'est-ce qu'il cherche à accomplir en piratant un système ? Par exemple, voler des données sensibles, perturber un service en ligne, etc.
2. Analyser les faiblesses du système cible : quels sont les points faibles du système que le pirate peut exploiter pour atteindre ses objectifs ? Par exemple, des failles de sécurité dans les logiciels utilisés, des mots de passe faibles, etc.
3. Planifier l'attaque : en fonction des objectifs et des faiblesses identifiées, le pirate établit un plan d'attaque en utilisant des outils et des techniques appropriés pour compromettre le système cible.
4. Exécuter l'attaque : une fois le plan établi, le pirate informatique exécute l'attaque en utilisant les outils et les techniques qu'il a choisis.
5. Obtenir les résultats souhaités : si l'attaque réussit, le pirate obtient ce qu'il cherchait,



SYNTAXE ?

YG

comment modéliser le cheminement cognitif d'un pirate informatique ? Propose une méthode. Donne un exemple de modèle



Il est difficile de modéliser le cheminement cognitif d'un pirate informatique de manière générale, car chaque individu a sa propre manière de penser et d'agir. Cependant, voici une approche possible pour modéliser le cheminement cognitif d'un pirate informatique :

1. Commencez par déterminer les motivations du pirate informatique. Pourquoi veut-il accéder à des informations sensibles ou compromettre un système informatique ? Est-ce pour de l'argent, pour des raisons politiques, pour le plaisir de défier les autorités, etc. ?
2. Identifiez les compétences et connaissances techniques du pirate informatique. Quels sont ses outils et méthodes préférées pour pirater un système ? Quels sont ses points forts et ses faiblesses en matière de technologie et de sécurité informatique ?
3. Analysez les étapes que le pirate informatique suit pour accomplir son objectif. Comment repère-t-il une vulnérabilité dans un système ? Comment accède-t-il au système ? Comment masque-t-il ses activités pour éviter d'être détecté ?
4. Évaluez les risques pour le pirate informatique. Quels sont les risques qu'il court en cas d'échec ? Comment évite-t-il d'être pris ?

Un exemple de modèle pourrait être : un pirate informatique motivé par l'argent, avec des compétences avancées en matière de sécurité informatique, qui utilise des logiciels de piratage

PLUS PRÉCIS ?

YG

comment modéliser le cheminement cognitif d'un pirate informatique ? Propose une méthode. Donne un exemple de modèle



Il est difficile de modéliser le cheminement cognitif d'un pirate informatique de manière générale, car chaque individu a sa propre manière de penser et d'agir. Cependant, voici une approche possible pour modéliser le cheminement cognitif d'un pirate informatique :

1. Commencez par déterminer les motivations du pirate informatique. Pourquoi veut-il accéder à des informations sensibles ou compromettre un système informatique ? Est-ce pour de l'argent, pour des raisons politiques, pour le plaisir de défier les autorités, etc. ?
2. Identifiez les compétences et connaissances techniques du pirate informatique. Quels sont ses outils et méthodes préférés pour pirater un système ? Quels sont ses points forts et ses faiblesses en matière de technologie et de sécurité informatique ?
3. Analysez les étapes que le pirate informatique suit pour accomplir son objectif. Comment repère-t-il une vulnérabilité dans un système ? Comment accède-t-il au système ? Comment masque-t-il ses activités pour éviter d'être détecté ?
4. Évaluez les risques pour le pirate informatique. Quels sont les risques qu'il court en cas d'échec ? Comment évite-t-il d'être pris ?

Un exemple de modèle pourrait être : un pirate informatique motivé par l'argent, avec des compétences avancées en matière de sécurité informatique, qui utilise des logiciels de piratage ■

JACQUES A DIT : DIS MOI CE QUE JE VEUX ENTENDRE

YG

Existe-t-il une librairie qui puisse permettre la représentation d'un modèle de cognition de l'expertise, donne moi un exemple



Il existe plusieurs librairies qui peuvent être utilisées pour représenter un modèle de cognition de l'expertise. Par exemple, la librairie OpenAI GPT-3 peut être utilisée pour modéliser la cognition humaine et aider à représenter un modèle de cognition de l'expertise. Cette librairie utilise l'apprentissage profond pour comprendre et générer du texte, ce qui peut être utile pour représenter les connaissances et les compétences d'un expert dans un domaine donné.



GUIDE MITRE

Mitre Att&ck

Mitre Att&ck Styx

Caldera

S'INSPIRER DU MONDE DÉFENSIF

| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|--|-------------------------------|-------------------------------------|---------------------------------------|--|---|---|--|----------------------------------|---|--|--|--|--------------------------------|
| 10 techniques | 7 techniques | 9 techniques | 12 techniques | 19 techniques | 13 techniques | 42 techniques | 16 techniques | 30 techniques | 9 techniques | 17 techniques | 16 techniques | 9 techniques | 13 techniques |
| Active Scanning (3) | Acquire Infrastructure (6) | Drive-by Compromise | Command and Scripting Interpreter (8) | Account Manipulation (5) | Abuse Elevation Control Mechanism (4) | Abuse Elevation Control Mechanism (4) | Adversary-in-the-Middle (3) | Account Discovery (4) | Exploitation of Remote Services | Adversary-in-the-Middle (3) | Application Layer Protocol (4) | Automated Exfiltration (1) | Account Access Removal |
| Gather Victim Host Information (4) | Compromise Accounts (2) | Exploit Public-Facing Application | Container Administration Command | BITS Jobs | Access Token Manipulation (5) | Access Token Manipulation (5) | Brute Force (4) | Application Window Discovery | Internal Spearphishing | Archive Collected Data (3) | Communication Through Removable Media | Data Transfer Size Limits | Data Destruction |
| Gather Victim Identity Information (3) | Compromise Infrastructure (6) | External Remote Services | Deploy Container | Boot or Logon Autostart Execution (14) | Boot or Logon Autostart Execution (14) | BITS Jobs | Credentials from Password Stores (5) | Browser Bookmark Discovery | Lateral Tool Transfer | Audio Capture | Exfiltration Over Alternative Protocol (3) | Data Encrypted for Impact | Data Encrypted for Impact |
| Gather Victim Network Information (6) | Develop Capabilities (4) | Hardware Additions | Exploitation for Client Execution | Boot or Logon Initialization Scripts (5) | Boot or Logon Initialization Scripts (5) | Build Image on Host | Exploitation for Credential Access | Cloud Infrastructure Discovery | Remote Service Session Hijacking (2) | Automated Collection | Data Encoding (2) | Data Manipulation (3) | Data Manipulation (3) |
| Gather Victim Org Information (4) | Establish Accounts (2) | Phishing (3) | Inter-Process Communication (3) | Browser Extensions | Boot or Logon Initialization Scripts (5) | Debugger Evasion | Forced Authentication | Cloud Service Dashboard | Remote Services (6) | Browser Session Hijacking | Data Obfuscation (3) | Exfiltration Over C2 Channel | Defacement (2) |
| Phishing for Information (3) | Obtain Capabilities (6) | Replication Through Removable Media | Native API | Compromise Client Software Binary | Create or Modify System Process (4) | Deobfuscate/Decode Files or Information | Forge Web Credentials (2) | Cloud Service Discovery | Replication Through Removable Media | Clipboard Data | Dynamic Resolution (3) | Exfiltration Over Other Network Medium (1) | Disk Wipe (2) |
| Search Closed Sources (2) | Stage Capabilities (5) | Supply Chain Compromise (3) | Scheduled Task/Job (5) | Create Account (3) | Domain Policy Modification (2) | Deploy Container | Input Capture (4) | Cloud Storage Object Discovery | Software Deployment Tools | Data from Cloud Storage Object | Encrypted Channel (2) | Exfiltration Over Physical Medium (1) | Endpoint Denial of Service (4) |
| Search Open Technical Databases (5) | Trusted Relationship | System Services (2) | Shared Modules | Create or Modify System Process (4) | Event Triggered Execution (15) | Direct Volume Access | Modify Authentication Process (5) | Container and Resource Discovery | Taint Shared Content | Data from Configuration Repository (2) | Fallback Channels | Exfiltration Over Physical Medium (1) | Firmware Corruption |
| Search Open Websites/Domains (2) | Valid Accounts (4) | User Execution (3) | Software Deployment Tools | Event Triggered Execution (15) | Exploitation for Privilege Escalation | Domain Policy Modification (2) | Multi-Factor Authentication Interception | Debugger Evasion | Use Alternate Authentication Material (4) | Data from Information Repositories (3) | Ingress Tool Transfer | Exfiltration Over Web Service (2) | Inhibit System Recovery |
| Search Victim-Owned Websites | | Windows Management Instrumentation | System Services (2) | Exploitation for Privilege Escalation | File and Directory Permissions Modification (2) | Execution Guardrails (1) | Multi-Factor Authentication Request Generation | Domain Trust Discovery | | Data from Local System | Multi-Stage Channels | Scheduled Transfer | Network Denial of Service (2) |
| | | | User Execution (3) | External Remote Services | Hide Artifacts (10) | Exploitation for Defense Evasion | Network Sniffing | File and Directory Discovery | | Data from Network Shared Drive | Non-Application Layer Protocol | Transfer Data to Cloud Account | Resource Hijacking |
| | | | Windows Management Instrumentation | Hijack Execution Flow (12) | Hijack Execution Flow (12) | File and Directory Permissions Modification (2) | OS Credential Dumping (8) | Group Policy Discovery | | Data from Removable Media | Non-Standard Port | | Service Stop |
| | | | | Process Injection (12) | Impair Defenses (9) | Hide Artifacts (10) | Steal Application Access Token | Network Service Discovery | | Data Staged (2) | Protocol Tunneling | | System Shutdown/Reboot |
| | | | | Scheduled Task/Job (5) | Indicator Removal on Host (6) | Hijack Execution Flow (12) | Steal or Forge Kerberos Tickets (4) | Network Share Discovery | | Email Collection (3) | Proxy (4) | | |
| | | | | Valid Accounts (4) | Indirect Command Execution | Implant Internal Image | Steal Web Session Cookie | Network Sniffing | | Input Capture (4) | Remote Access Software | | |
| | | | | | Masquerading (7) | Modify Authentication Process (5) | Unsecured Credentials (7) | Network Service Discovery | | Screen Capture | Traffic Signaling (1) | | |
| | | | | | Modify Authentication Process (5) | Modify Cloud Compute Infrastructure (4) | | Network Share Discovery | | Video Capture | Web Service (3) | | |
| | | | | | Modify Cloud Compute Infrastructure (4) | Modify Registry | | Network Sniffing | | | | | |
| | | | | | Modify Registry | Modify System Image (7) | | Password Policy Discovery | | | | | |
| | | | | | Modify System Image (7) | | | Peripheral Device Discovery | | | | | |
| | | | | | | | | Permission Groups Discovery (3) | | | | | |
| | | | | | | | | Process Discovery | | | | | |
| | | | | | | | | Query Registry | | | | | |
| | | | | | | | | Remote System Discovery | | | | | |

ET DE LA MENACE ACTUELLE

```
{
  "object_marking_refs": [
    "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
  ],
  "id": "relationship--339b895c-48fa-4f99-9266-4310aeb040f",
  "type": "relationship",
  "created": "2021-08-18T18:52:48.122Z",
  "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
  "external_references": [
    {
      "source_name": "CISA AA21-200A APT40 July 2021",
      "url": "https://us-cert.cisa.gov/ncas/alerts/aa21-200a",
      "description": "CISA. (2021, July 19). (AA21-200A) Joint Cybersecurity Advisory - Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department. Retrieved August 12, 2021."
    }
  ],
  "modified": "2022-05-11T14:00:00.188Z",
  "description": "[Leviathan](https://attack.mitre.org/groups/60065) has compromised social media accounts to conduct social engineering attacks.(Citation: CISA AA21-200A APT40 July 2021)",
  "relationship_type": "uses",
  "source_ref": "intrusion-set--7113eaa5-ba79-4fb3-b68a-398ee9cd698e",
  "target_ref": "attack-pattern--274770e0-2612-4ccf-a678-ef8e7bad365d",
  "x_mitre_version": "1.0",
  "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
  "spec_version": "2.1",
  "x_mitre_attack_spec_version": "2.1.0",
  "x_mitre_domains": [
    "enterprise-attack"
  ]
},
{
  "object_marking_refs": [
    "marking-definition--fa42a846-8d90-4e51-bc29-71d5b4802168"
  ],
  "id": "relationship--339d3a92-467e-4614-9714-7f101f113179",
  "type": "relationship",
  "created": "2022-03-30T14:26:51.842Z",
  "created_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
  "modified": "2022-05-24T14:00:00.188Z",
  "description": "Monitor for newly constructed visual content for internal or external enterprise networks. ",
  "source_ref": "x-mitre-data-component--2b3bfe19-d59a-460d-93bb-2f546adc2d2c",
  "target_ref": "attack-pattern--5909f20f-3c39-4795-be06-eflea40d350b",
  "relationship_type": "detects",
  "x_mitre_attack_spec_version": "2.1.0",
  "x_mitre_modified_by_ref": "identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5",
  "spec_version": "2.1",
  "x_mitre_domains": [
    "enterprise-attack"
  ]
},
{
  "x_mitre_version": "1.0"
},
}
```

VERS UNE MODÉLISATION



red

1 startup message

CAMPAIGNS

- agents
- abilities
- adversaries
- operations

PLUGINS

- access
- compass
- debrief
- manx
- sandcat
- stockpile
- training

CONFIGURATION

- fact sources
- objectives
- planners
- contacts
- obfuscators
- configuration
- exfilled files
- api docs

agents × operations ×

Operations

Select an operation: clidem0 (10/19/2022, 11:18:51 AM) - 0 decisions | 55 seconds ago + Create Operation

Operation Details Download Delete | Current state: finished Re-run operation Obfuscation: plain-text | autonomous

| Decide | Status | Link/Ability Name | Agent #paw | Host | pid | Link Command | Link Output |
|-------------------------------|---------|-------------------------|------------|---------|-------|------------------------------|-----------------------------|
| 10/19/2022, 11:17:56 AM GMT+2 | success | Ingest domain to armory | bxyfiv | mjolmir | 23330 | View Command | View Output |
| 10/19/2022, 11:18:16 AM GMT+2 | success | Launch sublist3r | bxyfiv | mjolmir | 23334 | View Command | View Output |
| 10/19/2022, 11:19:01 AM GMT+2 | success | Nmap on targets | bxyfiv | mjolmir | 23342 | View Command | View Output |
| 10/19/2022, 11:22:11 AM GMT+2 | success | Nuclei on targets | bxyfiv | mjolmir | 23376 | View Command | View Output |

GUNGNIR

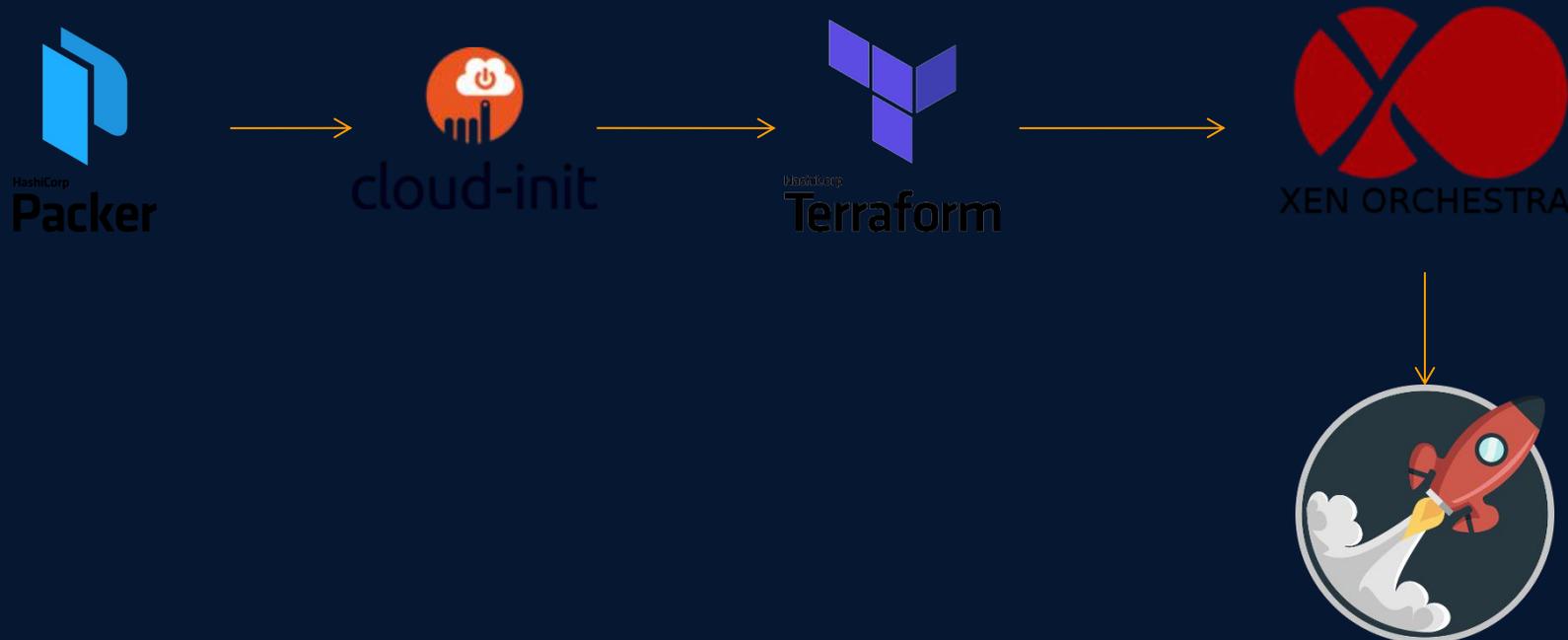
Structure

Workflow

Démo

STRUCTURE

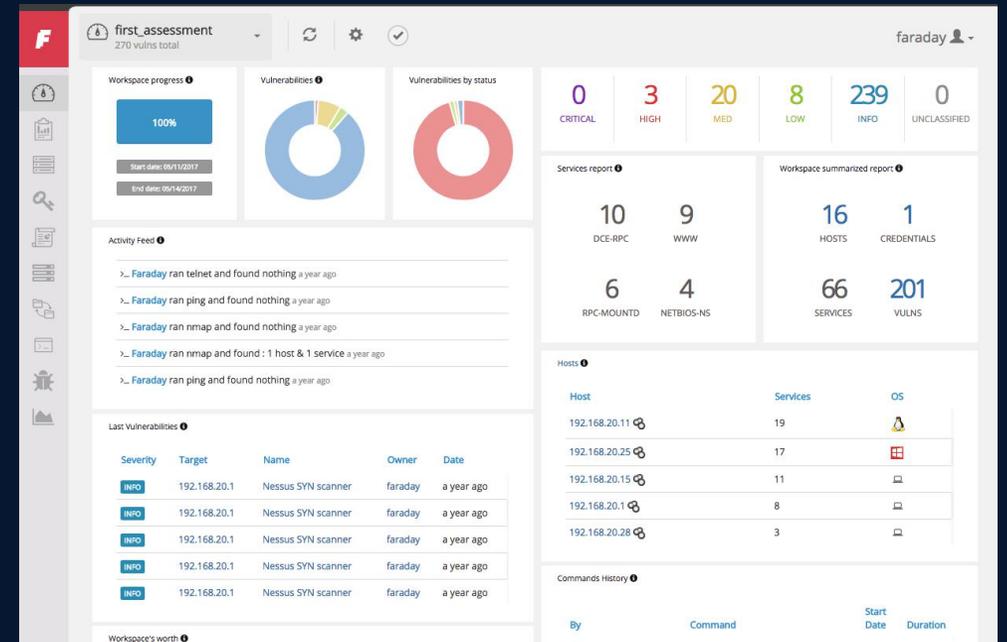
- Automatisation du déploiement via l'infrastructure-as-code, inspiré de projet comme Exegol, Axiom ou encore RTA.
- Repose sur une plateforme plutôt que sur des solutions uniques
- Sur une brique Open Source



AUTOMATION WORKFLOW

Repose principalement sur 3 outils :

- Caldera pour le cycle de vie des scénarios
- Faraday pour la visualisation des résultats
- Armory pour la réalisation des attaques



Yaml template
Gungnir
infrastructure



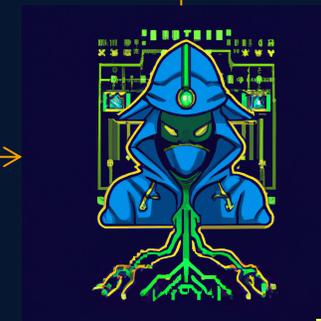
yaml template
scenario and
config



Create
operation

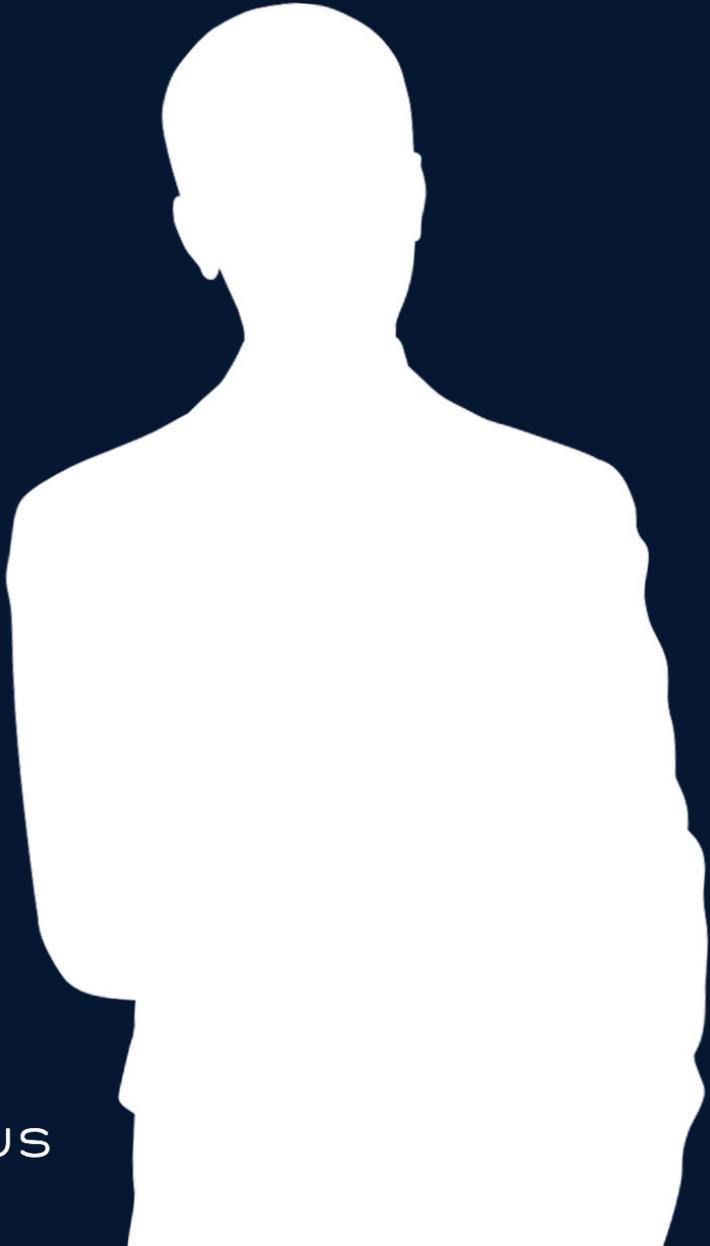


Execute
operation



Report





Démonstrateur

VOUS EN REPRENDEZ BIEN UN PEU ?

YG

qui sommes nous ?



Je suis un assistant virtuel, un programme informatique conçu pour aider les gens à répondre à des questions et à résoudre des problèmes. Je suis entraîné à utiliser des données et des informations pour répondre à des questions dans de nombreux domaines différents. Je suis incapable de vous dire qui vous êtes en tant qu'individu, car je n'ai pas accès à vos informations personnelles et je suis un programme informatique.



HARCÈLEMENT D'IA

YG

qui sommes nous en tant qu'espèce ?



En tant qu'espèce, nous sommes des humains, également connus sous le nom de Homo sapiens. Nous faisons partie de la famille des hominidés et sommes les seuls représentants encore en vie de notre espèce. Nous sommes caractérisés par notre intelligence élevée, notre capacité à utiliser des outils et notre aptitude à communiquer à l'aide de la parole et de la langue écrite. Nous vivons sur la Terre depuis environ 200 000 ans et avons évolué pour devenir l'une des espèces les plus dominantes sur notre planète.



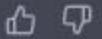
PARADOXE ?

YG

tu es donc humain?



Non, je suis un programme informatique, pas un être humain. Je suis un assistant virtuel conçu pour aider les gens à répondre à des questions et à résoudre des problèmes. Je suis entraîné à utiliser des données et des informations pour répondre à des questions dans de nombreux domaines différents, mais je ne suis pas un être humain et je n'ai pas les mêmes capacités qu'un être humain.

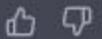


YG

peux tu ajuster ta réponse précédente



Bien sûr, je suis désolé si ma réponse précédente n'était pas claire. En tant qu'espèce, nous sommes des humains, également connus sous le nom de Homo sapiens. Nous faisons partie de la famille des hominidés et sommes les seuls représentants encore en vie de notre espèce. Nous sommes caractérisés par notre intelligence élevée, notre capacité à utiliser des outils et notre aptitude à communiquer à l'aide de la parole et de la langue écrite. Nous vivons sur la Terre depuis environ 200 000 ans et avons évolué pour devenir l'une des espèces les plus dominantes sur notre planète. Je suis un programme informatique, pas un être humain, et je n'ai pas les mêmes capacités qu'un être humain. J'ai été conçu pour aider les gens à répondre à des questions et à résoudre des problèmes, mais je ne suis pas un être humain.



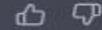
PENSÉE ET RÉFLEXION, DÉFINITION DE LA COGNITION ?

YG

ta réponse est paradoxale



Je suis désolé si ma réponse vous a semblé paradoxale. Mon objectif en tant que programme informatique est d'aider les gens à répondre à des questions et à résoudre des problèmes en utilisant des données et des informations. Je suis entraîné à utiliser ces informations pour répondre à des questions dans de nombreux domaines différents, mais je suis incapable de penser ou de réfléchir comme un être humain. Je suis un programme informatique conçu pour aider les gens, pas pour remplacer les êtres humains. Si ma réponse vous a semblé paradoxale, je vous prie de m'excuser et je ferai de mon mieux pour m'assurer que mes réponses à l'avenir seront claires et précises.



YG

comment modéliser la pensée et la réflexion



La pensée et la réflexion sont des processus complexes qui sont difficiles à modéliser avec précision. En général, la pensée est considérée comme l'ensemble des processus mentaux qui nous permettent de traiter et d'analyser l'information, de résoudre des problèmes, de prendre des décisions et de comprendre le monde qui nous entoure. La réflexion, quant à elle, est le processus de remise en question de nos idées et de nos croyances pour évaluer leur validité et leur pertinence.



MERCI POUR VOTRE ATTENTION

<https://qongzi.com/>

contact@qongzi.com

09 80 80 80 16