Defense Evasion with Veil

Jurriën Kol
CYBER SECURITY SPECIALIST
@Ag0sSec


VEIL

Creators: Will Schroeder, Christoffer Truncer & Michael Wright

The Veil-Framework is a collection of red team security tools that implement various attack methods focused on evading detection.

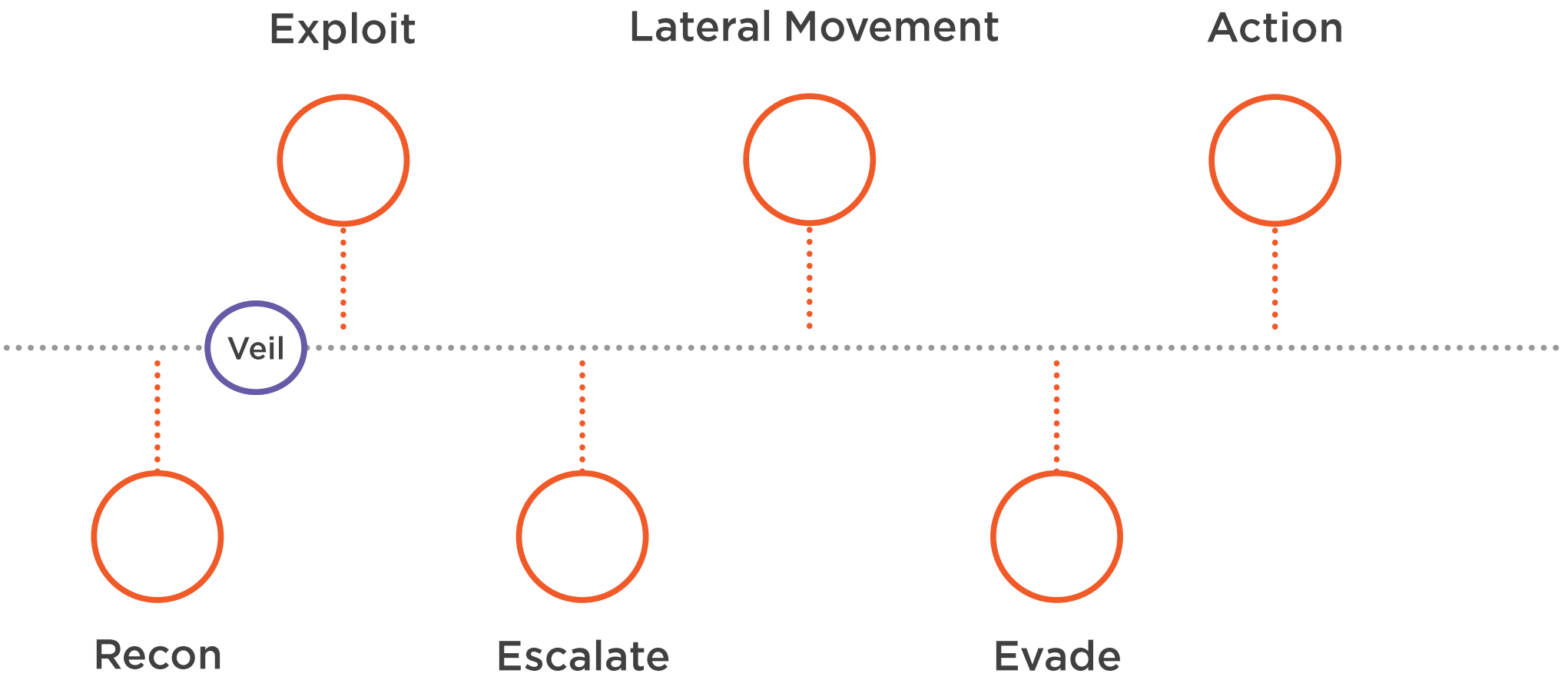
Long description of tool, using most of the creator's own words. How is it described on the GitHub wiki? Why was it made? What problem did

Opensource payload generation and obfuscation framework written in Python

Available at github.com/Veil-Framework/Veil/ for download and through Linux package managers

Allows use of custom or preexisting shellcode and leverages several obfuscation and evasion techniques to create payloads with a unique signature

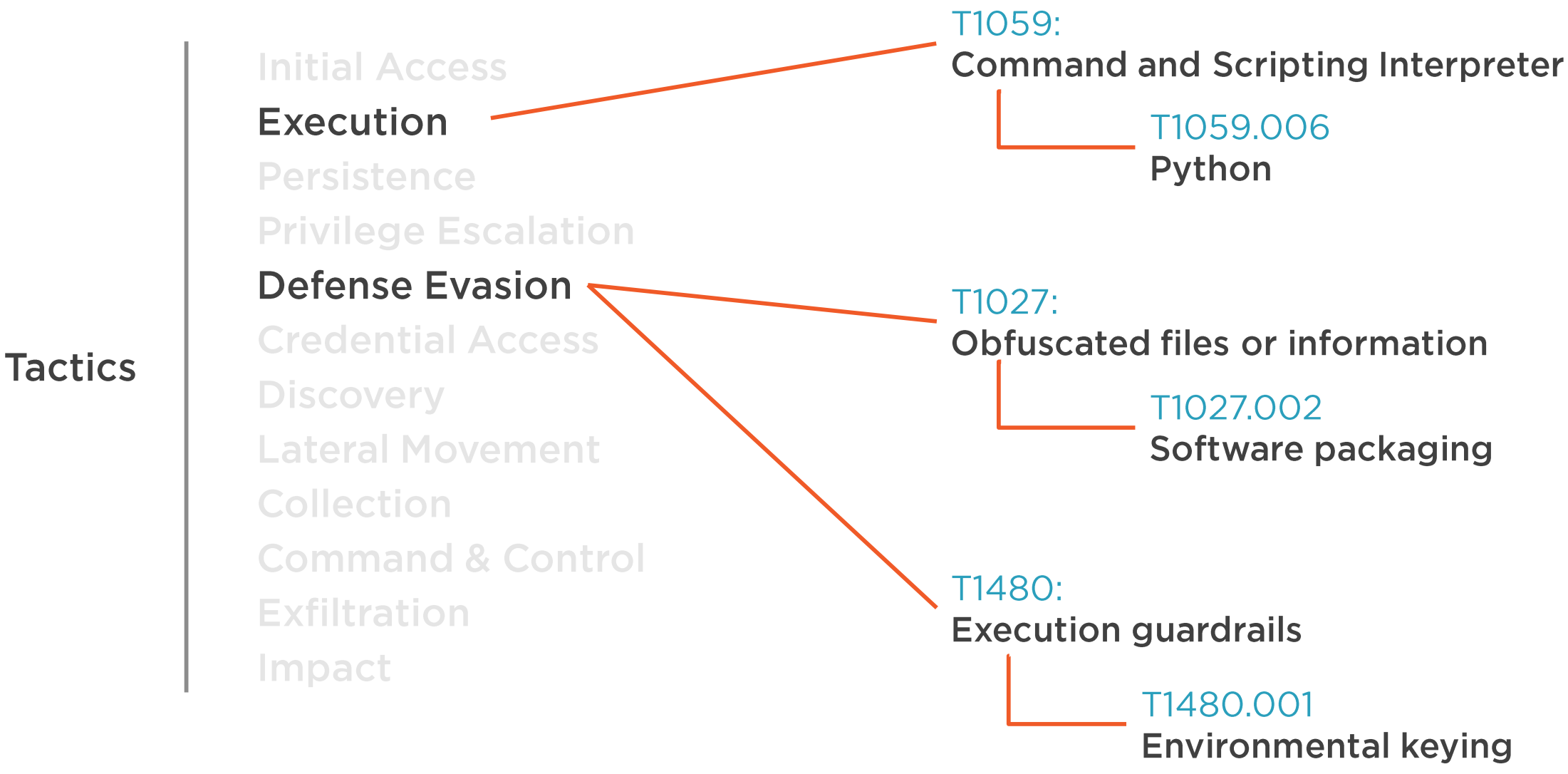
Kill Chain


Exploit
Lateral Movement
Action
Veil
Recon
Escalate
Evade

MITRE ATT&CK

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

MITRE ATT&CK


Tactics
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command & Control
Exfiltration
Impact
T1059:
Command and Scripting Interpreter
T1059.006
Python
T1027:
Obfuscated files or information
T1027.002
Software packaging
T1480:
Execution guardrails
T1480.001
Environmental keying

Payload

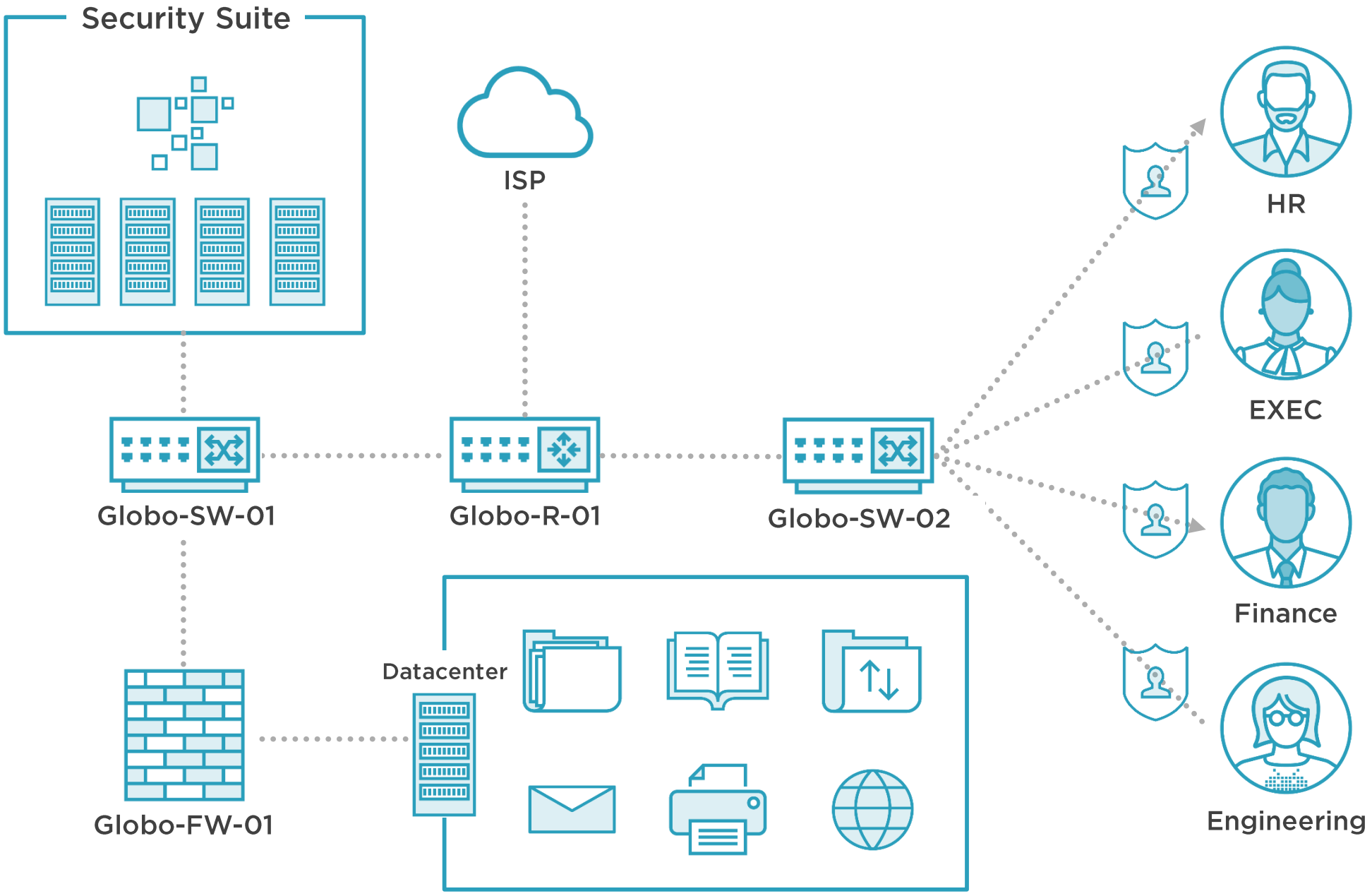
- Meterpreter
- Shellcode Inject
- Custom payload

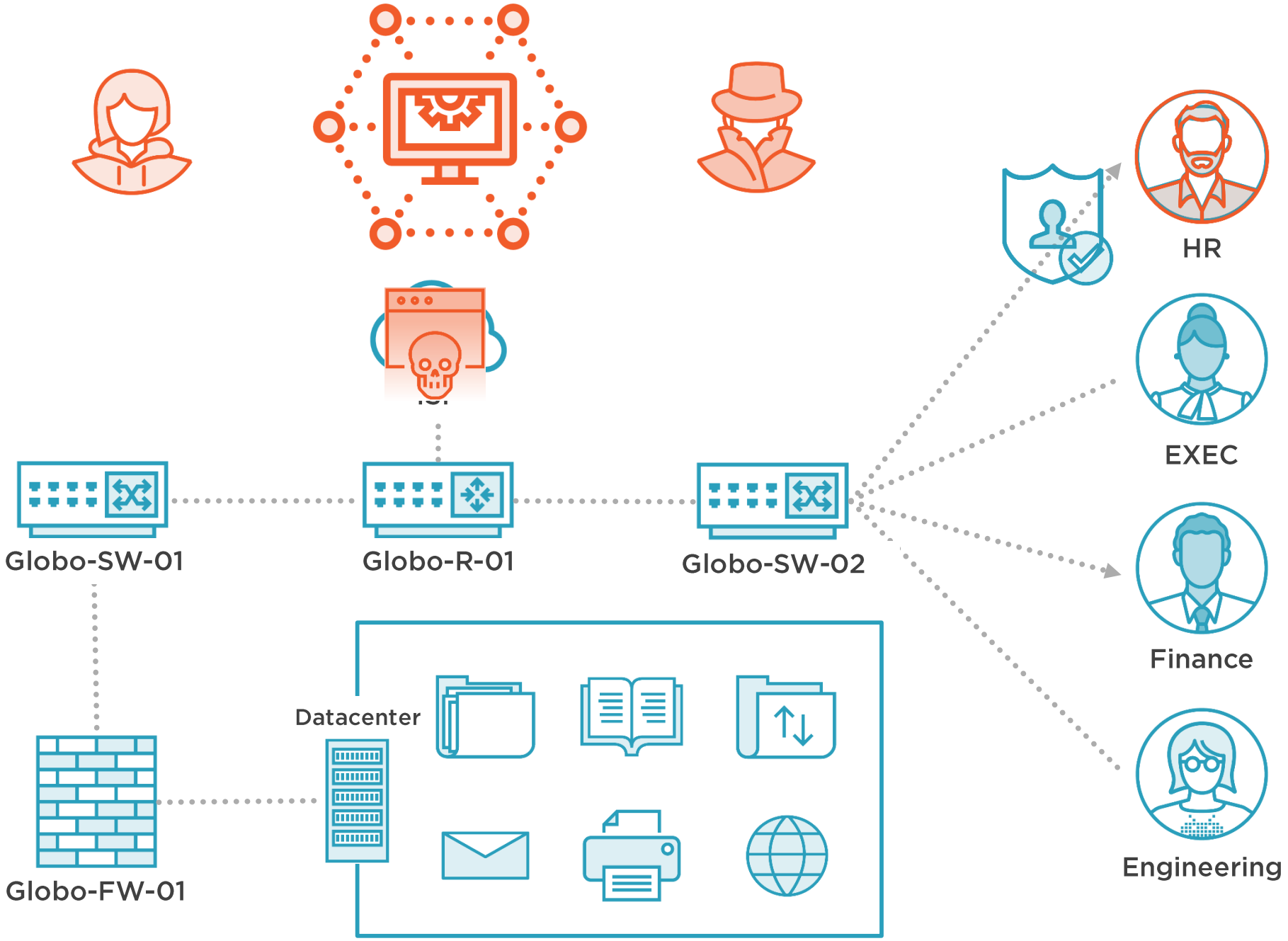
Encryption/ Obfuscation

- Pyherion
- PEScarmbler
- Backdoor Factory
- Etc.

Native compilation

- Python
- C#
- C


Security Suite
ISP
HR
EXEC
Finance
Engineering
Globo-SW-01
Globo-R-01
Globo-SW-02
Globo-FW-01
Datacenter


HR
EXEC
Finance
Engineering
Globo-SW-01
Globo-R-01
Globo-SW-02
Datacenter
Globo-FW-01

Demo

Installation tips and tricks

First use instructions and common usage syntax

Use of main features on live targets or in live environment

More Information

Veil Capabilities

Shellcode generation with Ordnance

https://github.com/Veil-Framework/Veil/wiki#ordnance

PyHerion obfuscation

https://www.veil-framework.com/pyherion/

Veil CLI commands

Defense Evasion

Recompiling PyInstaller to disable DEP

https://www.veil-framework.com/dep-pyinstaller

Create your own payload

https://www.veil-framework.com/tutorial-veil-payload-development/