

Execution: Donut



Matt Glass

CISSP, CEH

<https://www.linkedin.com/in/matthewglass2/>







Creator: TheWover



**Donut is an open-source shellcode generation tool.
The open-source tool available on GitHub and enables
in-memory execution of VBScript, JScript, EXE, DLL
files and dotNET assemblies**





Donut is a shellcode generator.

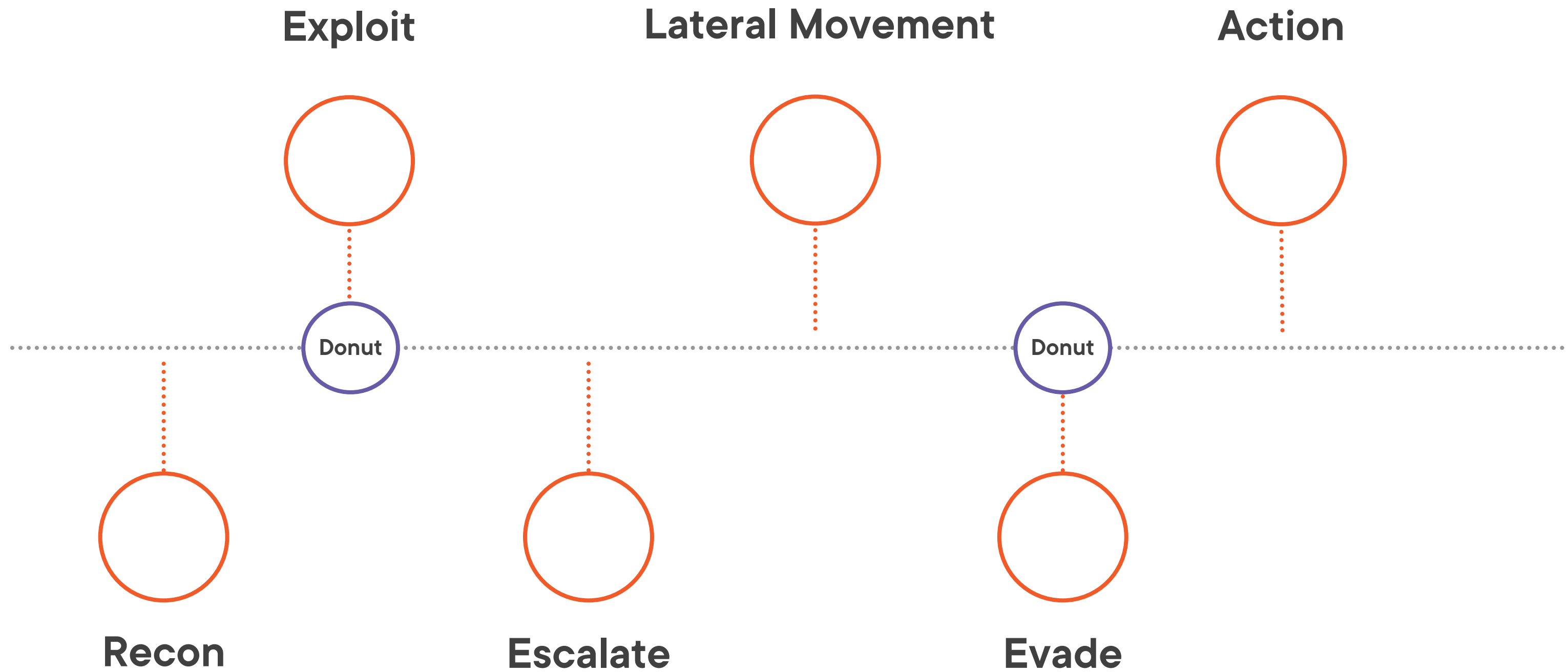
Donut is available on GitHub.

Donut enables in-memory execution of a variety of file types.

Donut exploits the way Windows machines handle dotNET execution to evade defenses.



Kill Chain



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

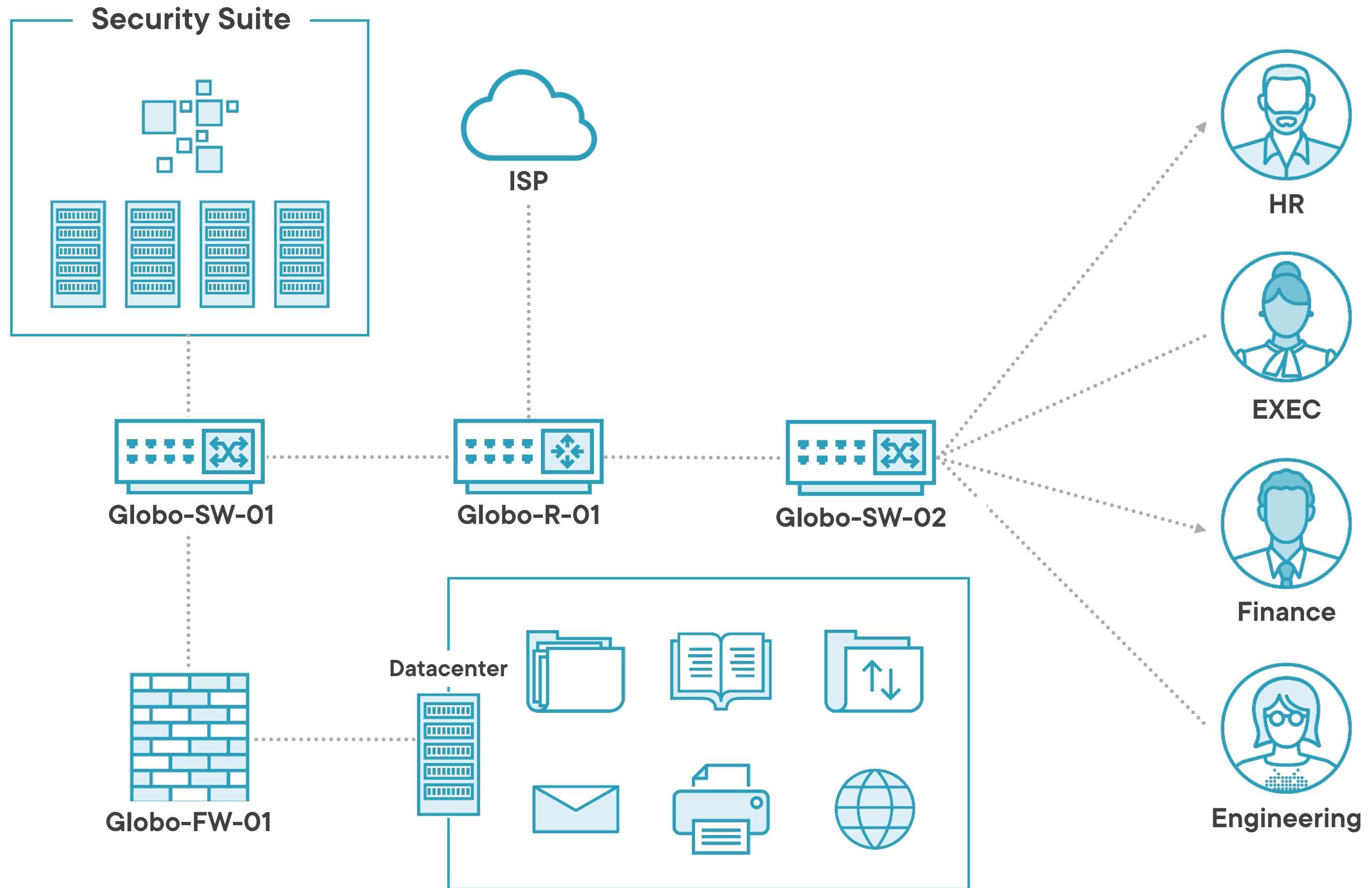
Impact

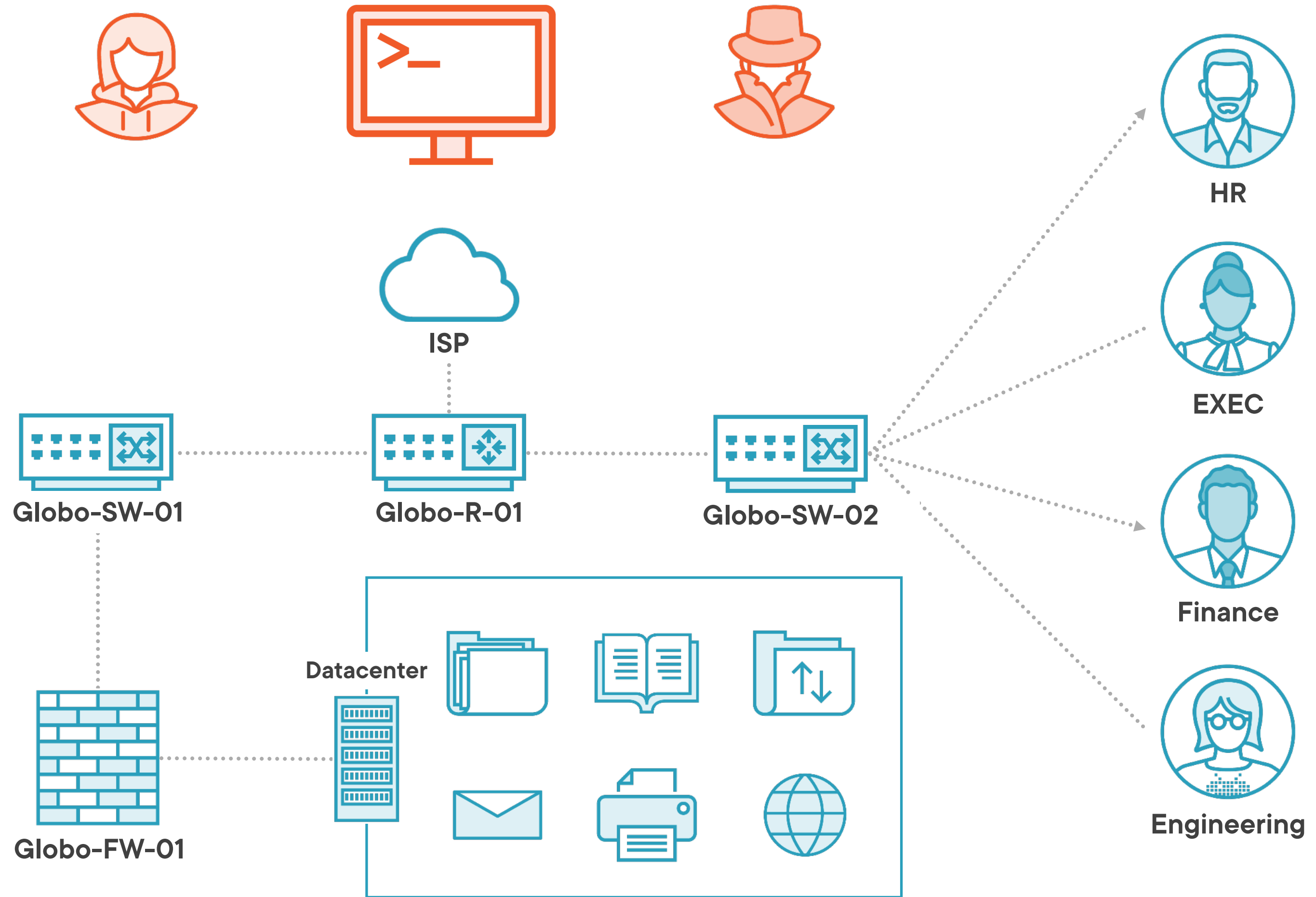
T1106:
Native API

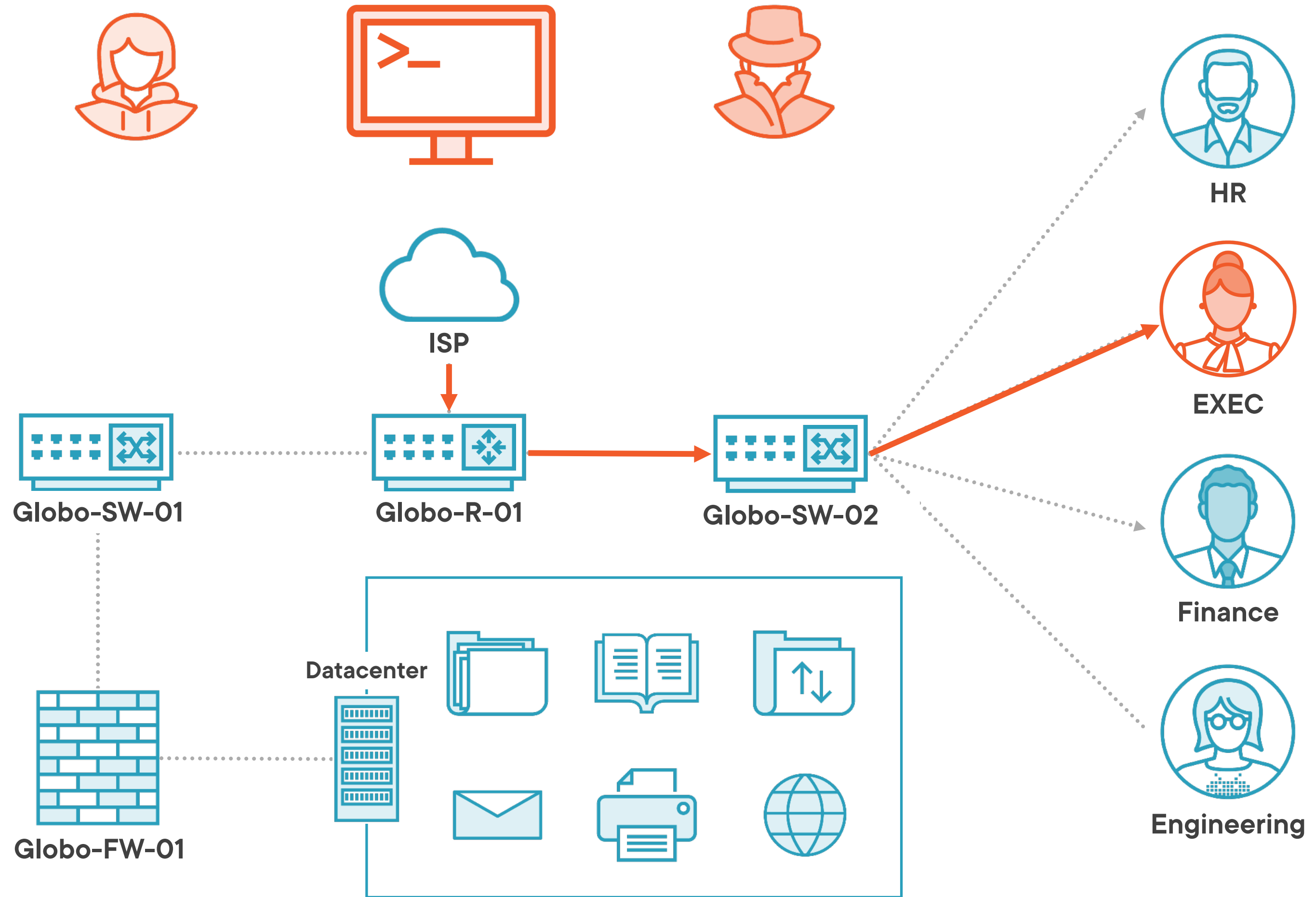
T1055.001:
**Dynamic-link Library
Injection**

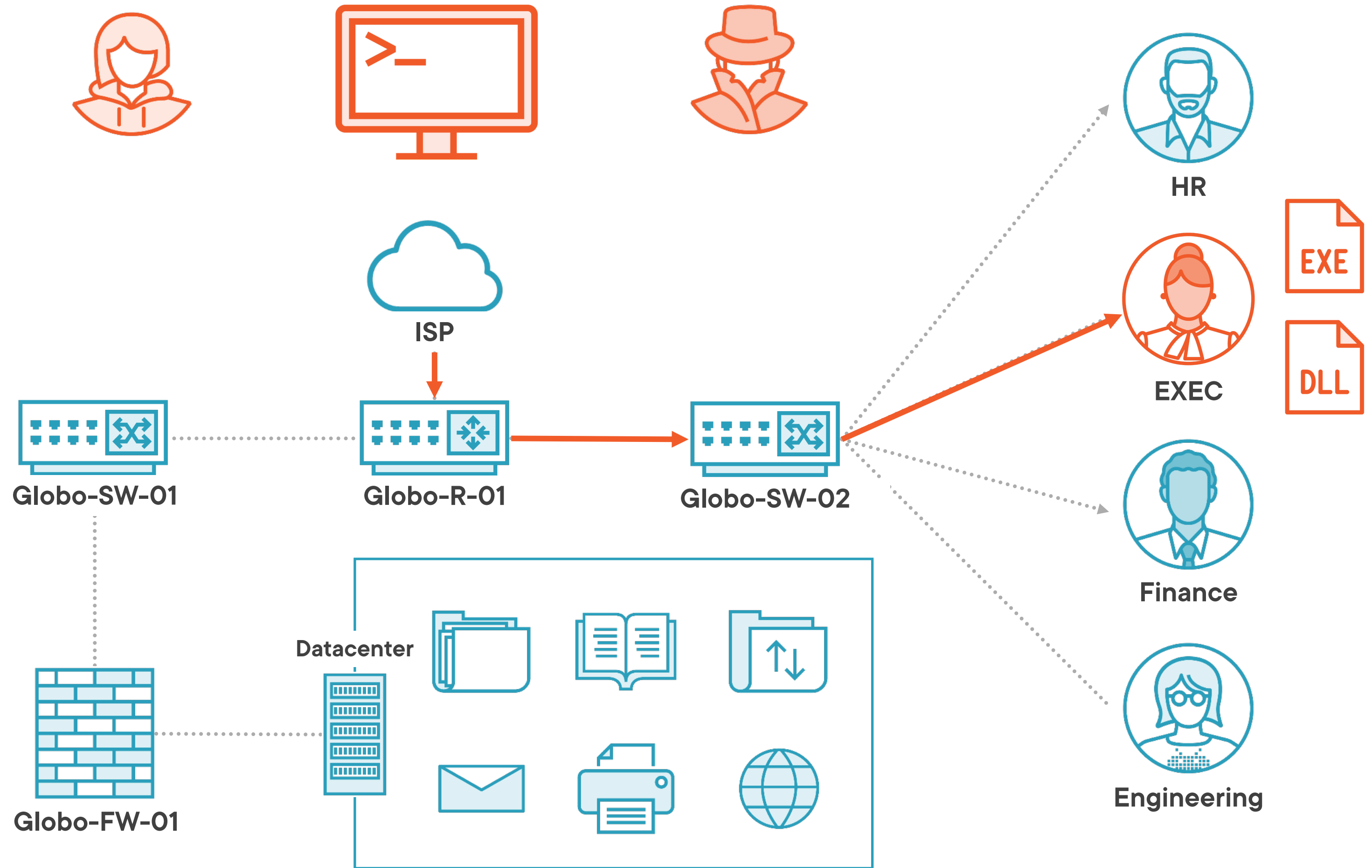
T1055.002:
**Portable Executable
Injection**

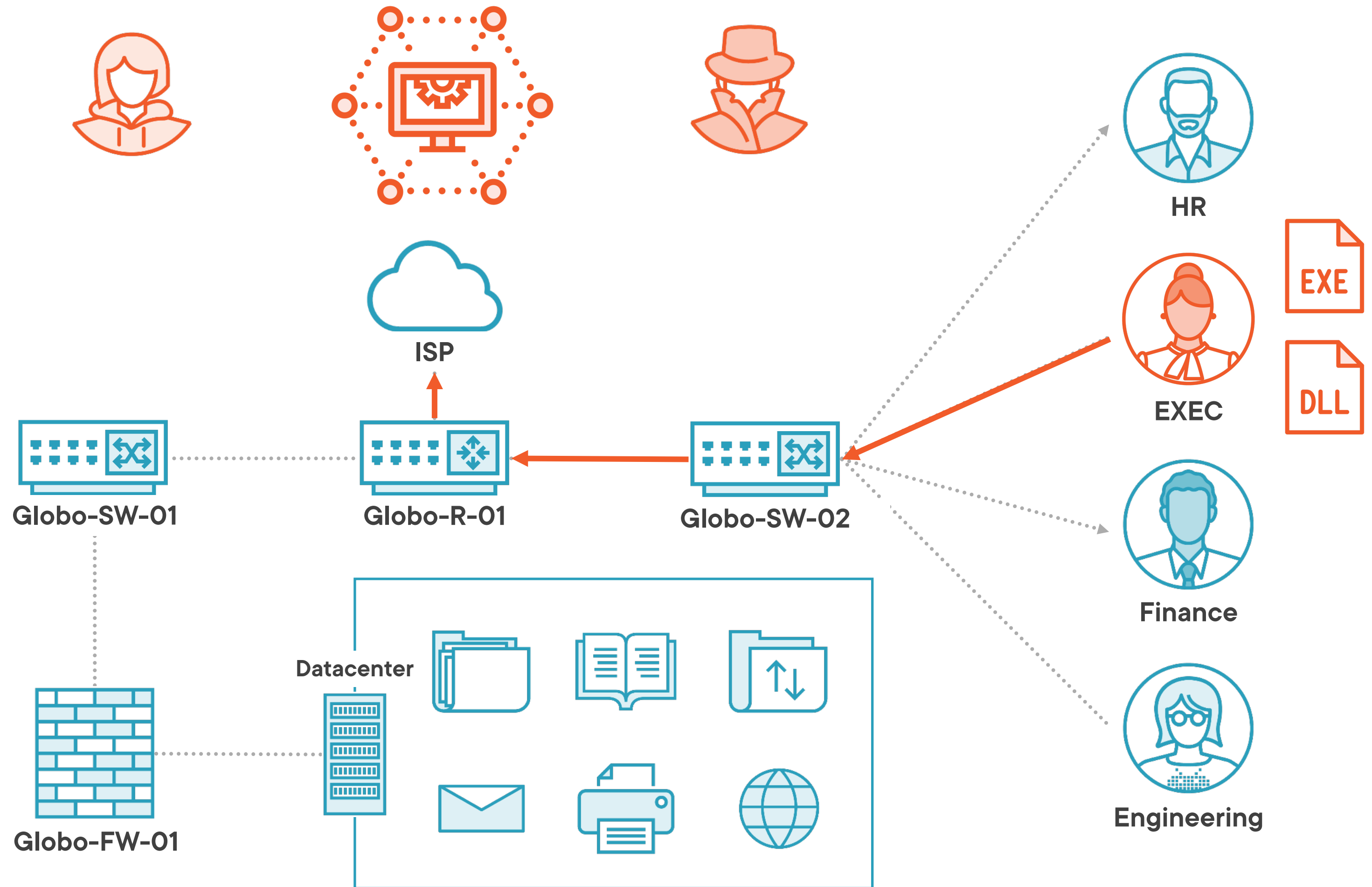












Demo

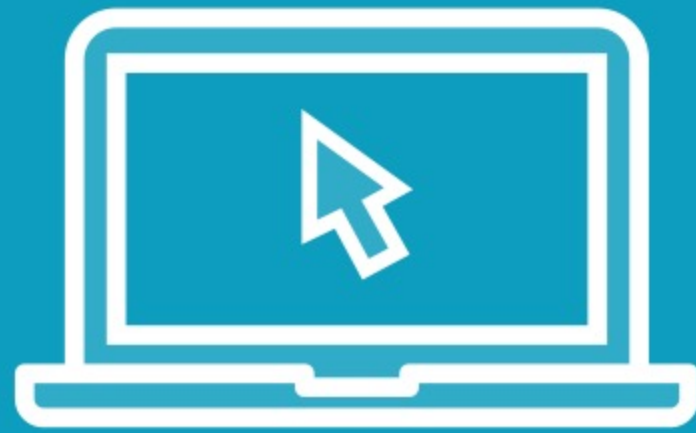


Shellcode Generation with Donut

- Lab environment
- Exploring Donut's options
- Explore additional built-in tools



Demo



Use Donut to inject malicious code into a running process

- **Generate necessary shellcode**
- **Inject malicious code into a process**

Using these features allows you to execute malicious code in memory by exploiting vulnerabilities in the native API and evade defense mechanisms.



Demo



Generate Shellcode from a DLL for process injection

- Generate shellcode for injection
- Inject the malicious code into a running process

Using these features allows you to execute malicious code in memory by exploiting vulnerabilities in the native API and evade defense mechanisms.

