

Initial Access with Gophish



Matt Glass

CISSP, CEH

[linkedin.com/in/matthewglass2/](https://www.linkedin.com/in/matthewglass2/)







Creator: Jordan Wright



Gophish is an open-source phishing toolkit that can be used by businesses and penetration testers to quickly setup and execute phishing campaigns.





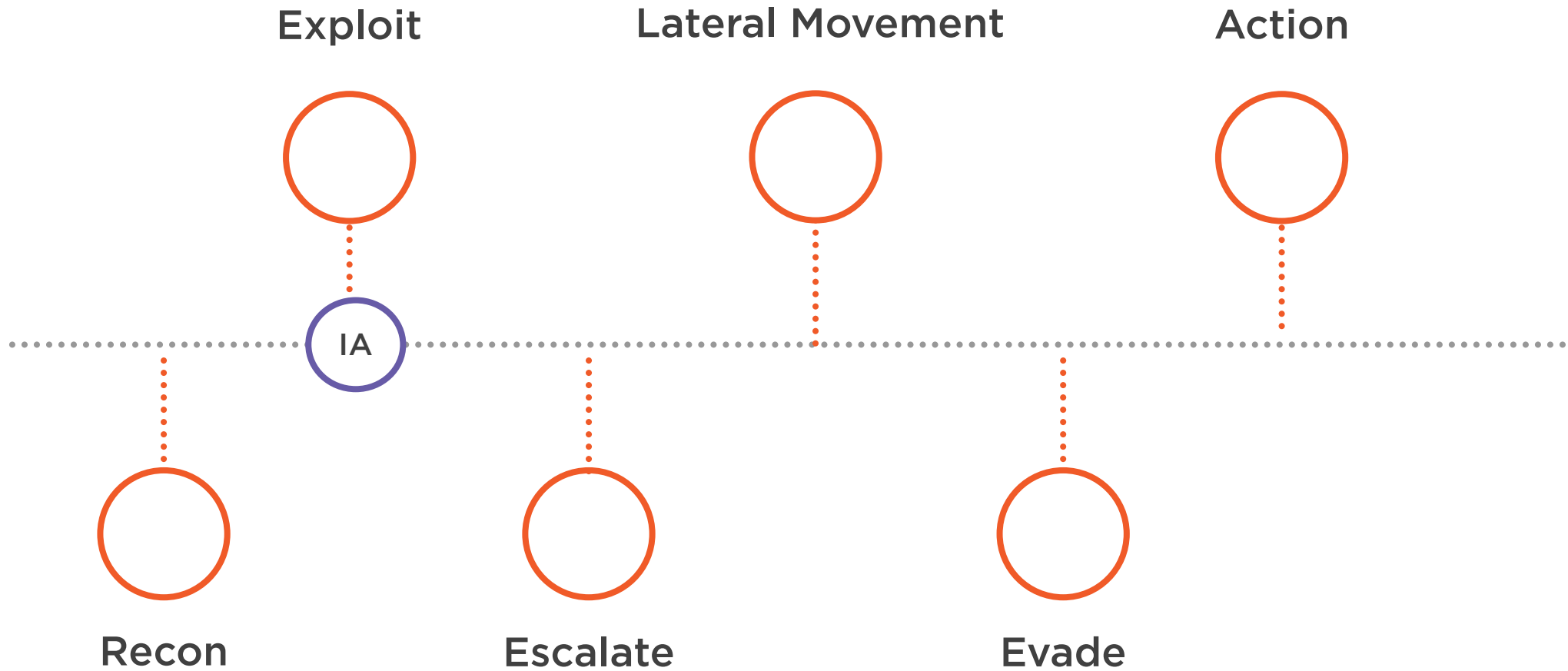
Gophish is a phishing toolkit to test an organization's security awareness.

It can be downloaded from www.getgophish.com or on GitHub.

Gophish is useful due to its simplicity to install and operate.



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

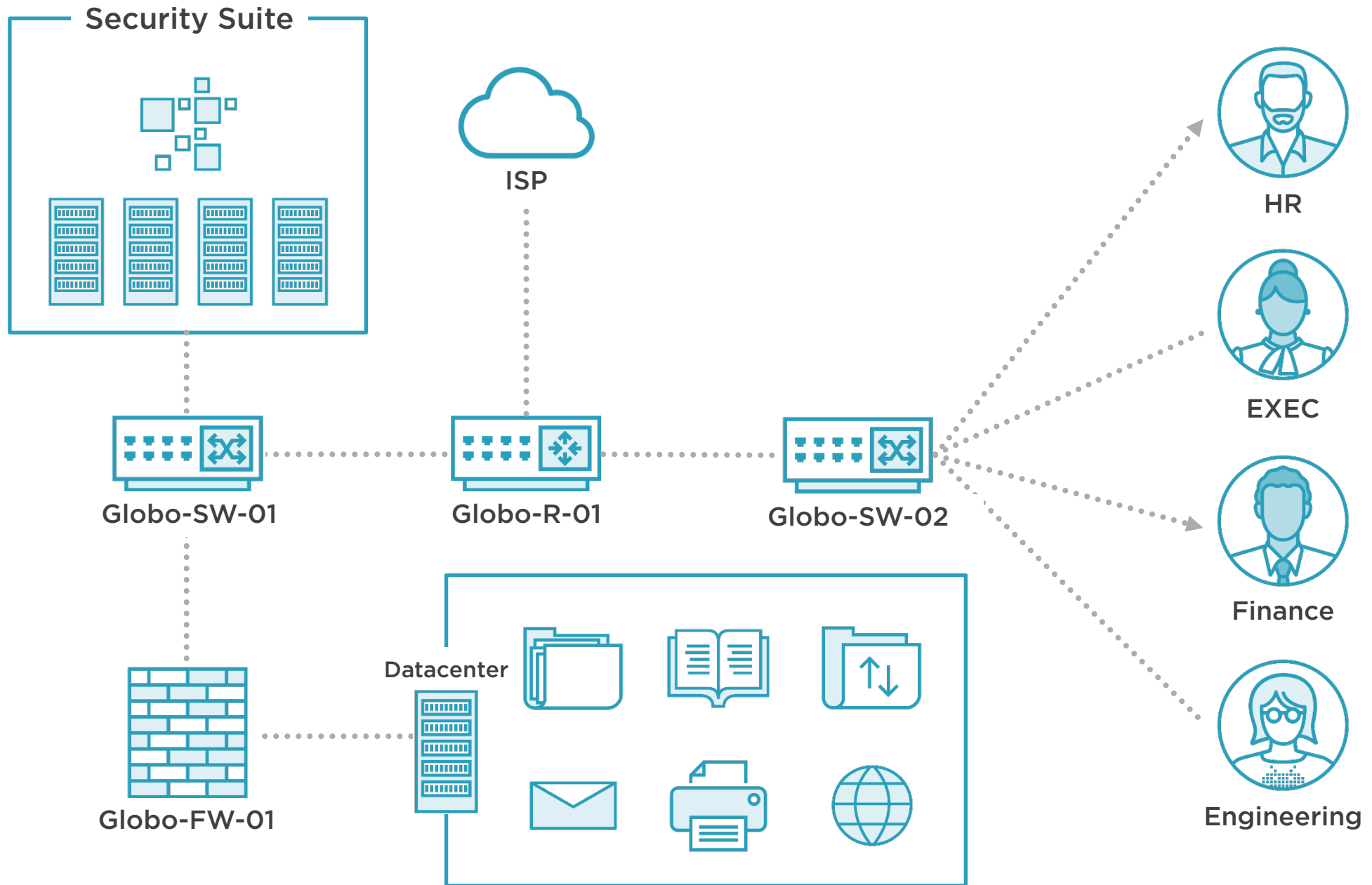
Impact

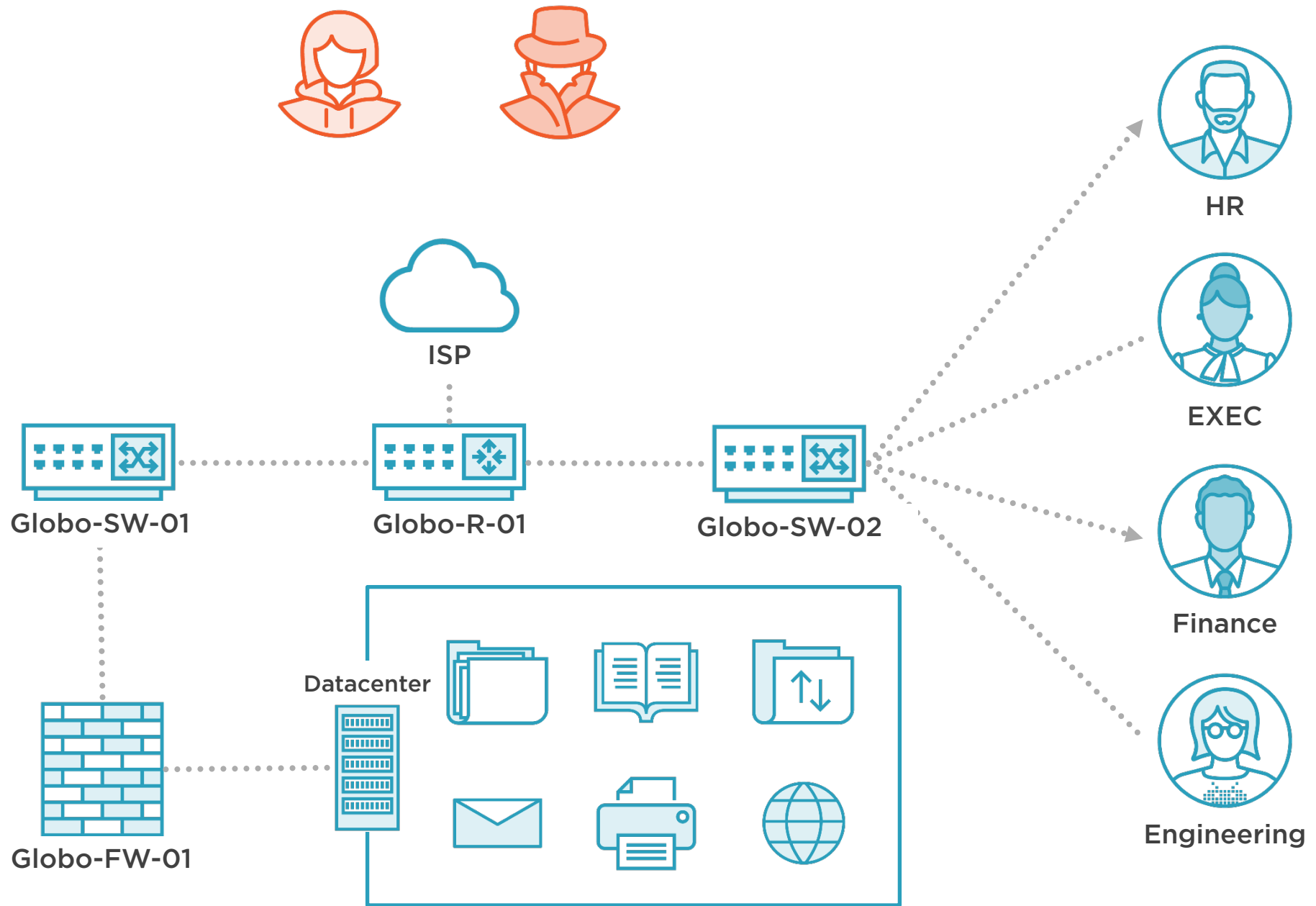
T1566:
Phishing

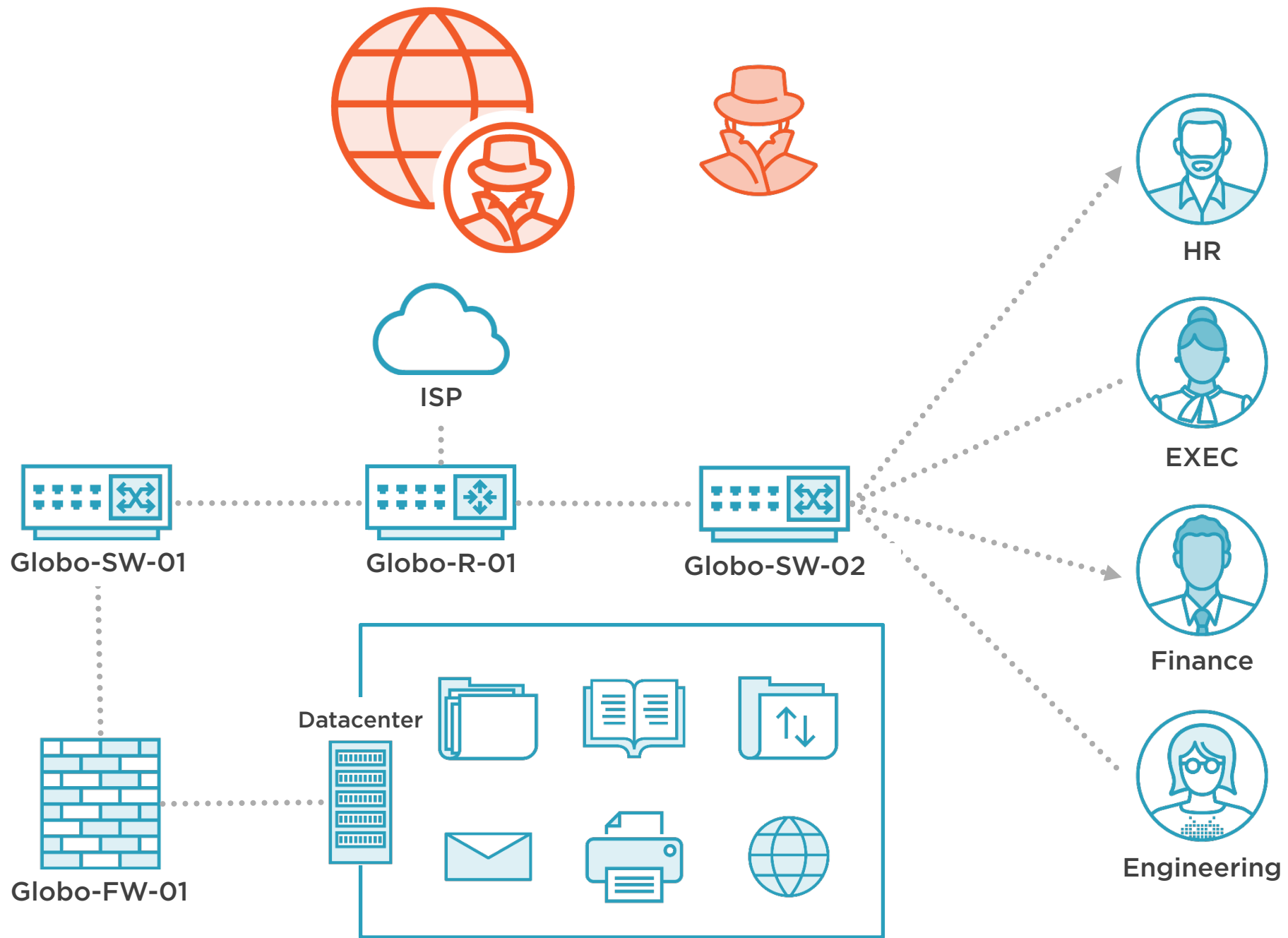
T1566.001:
Spearphishing Attachment

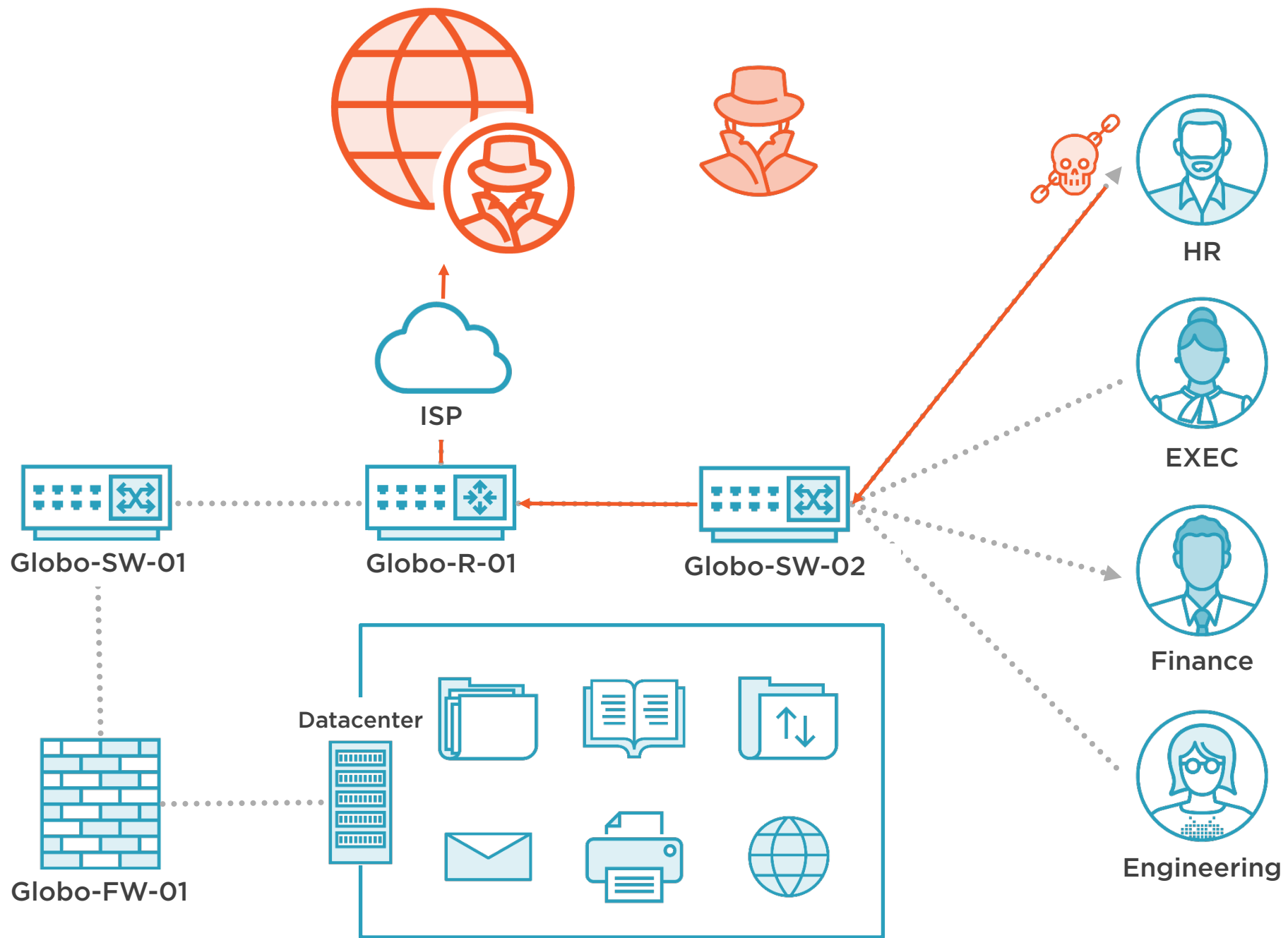
T1566.002:
Spearphishing Link

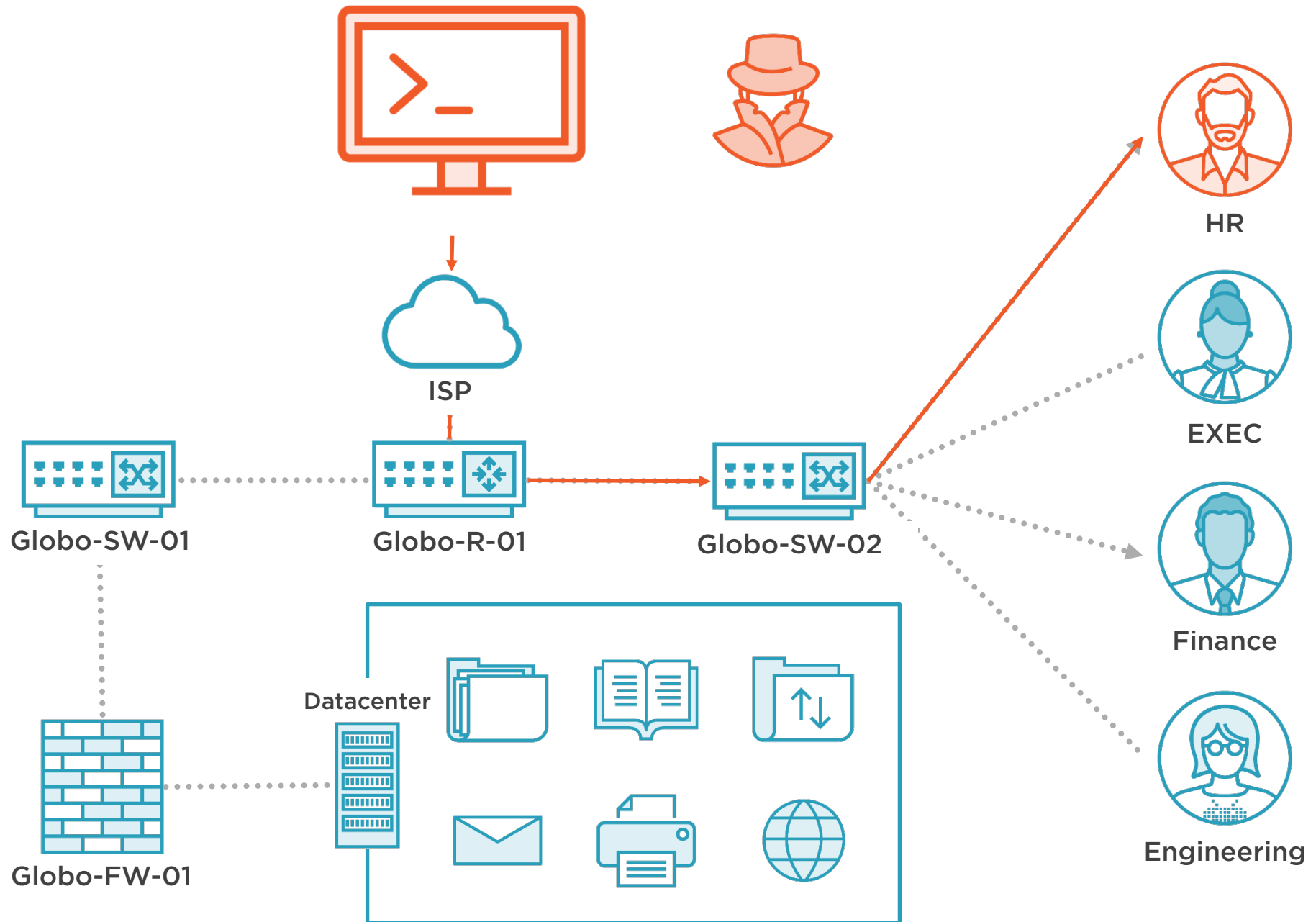


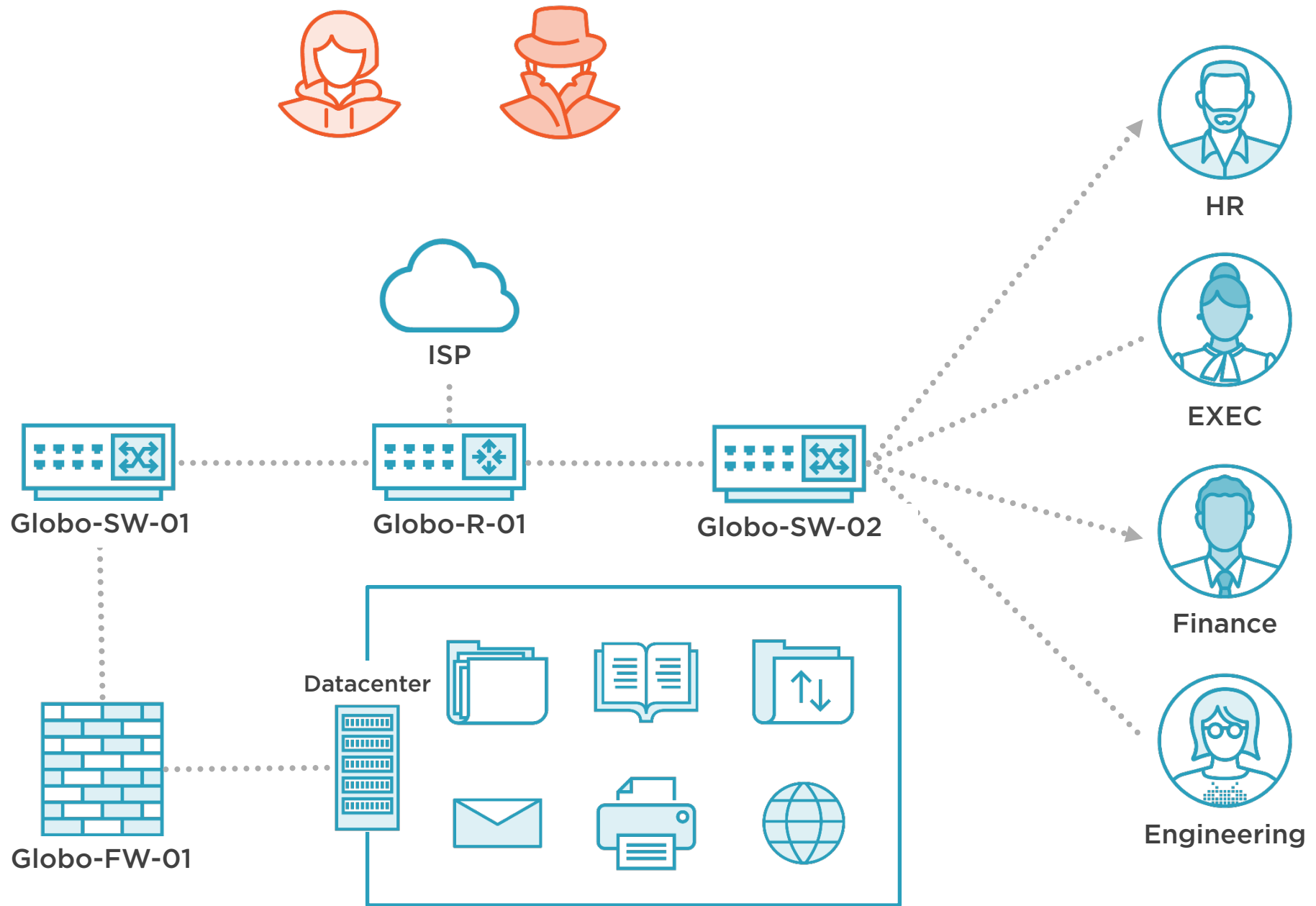


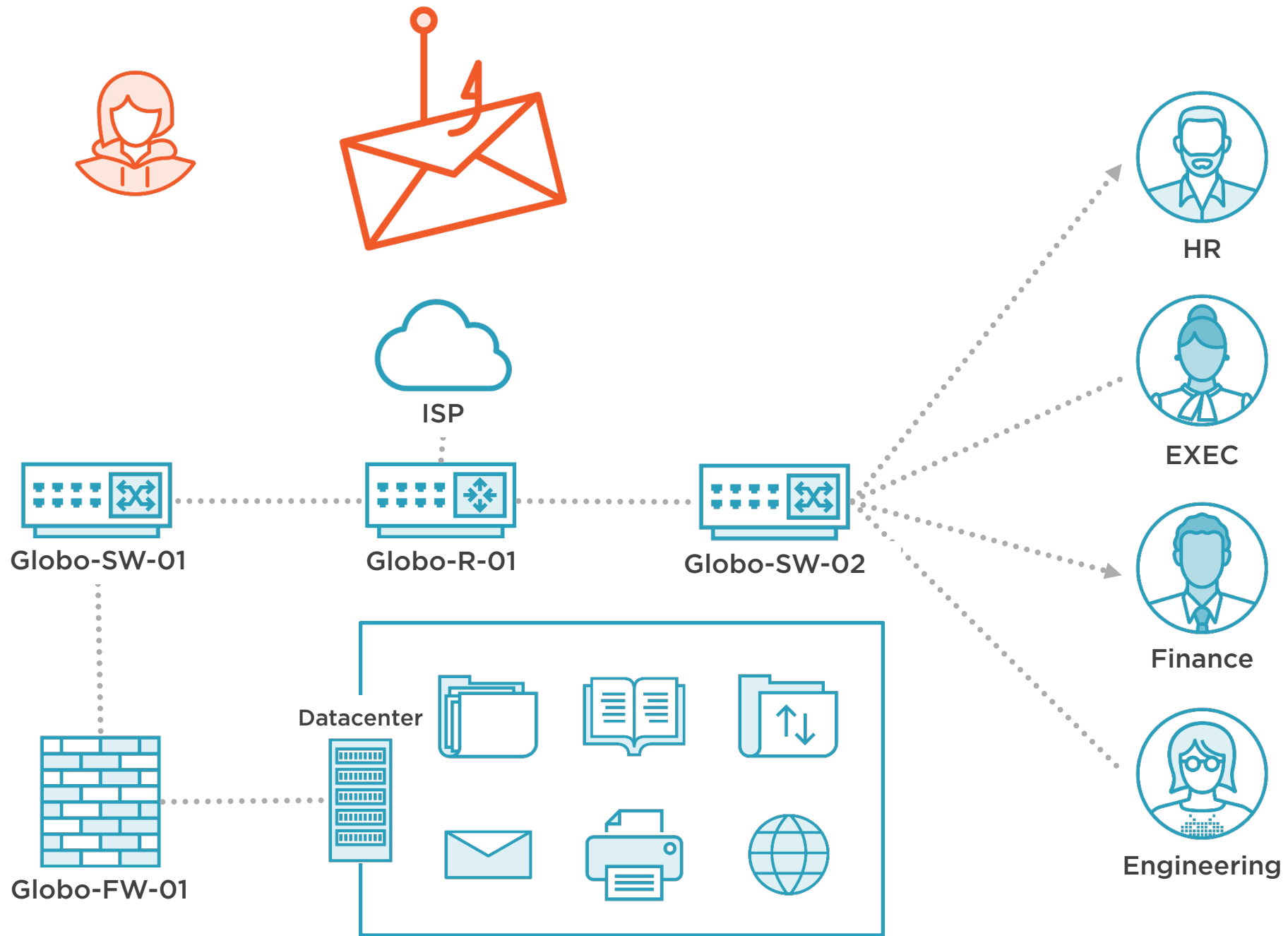


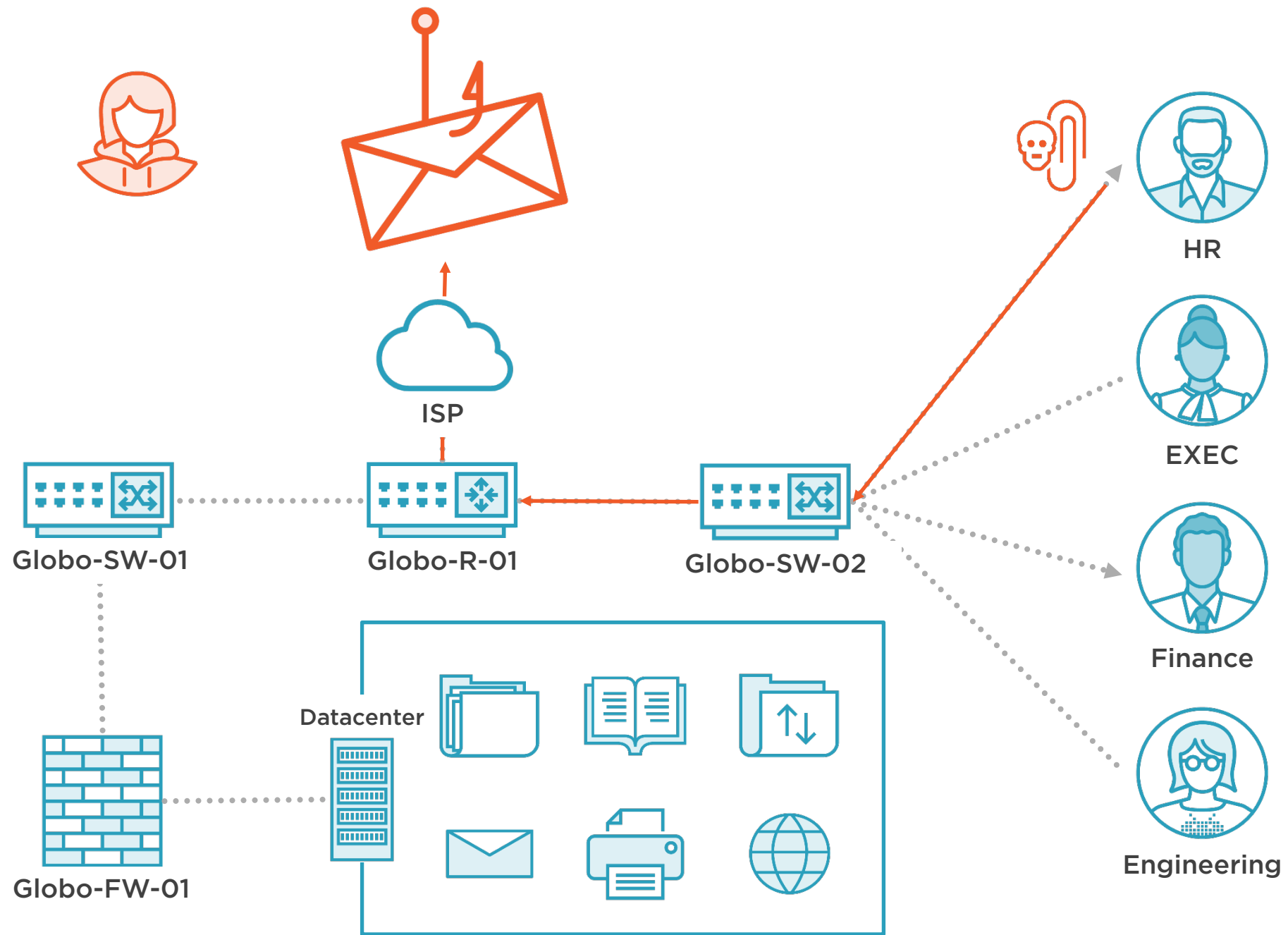


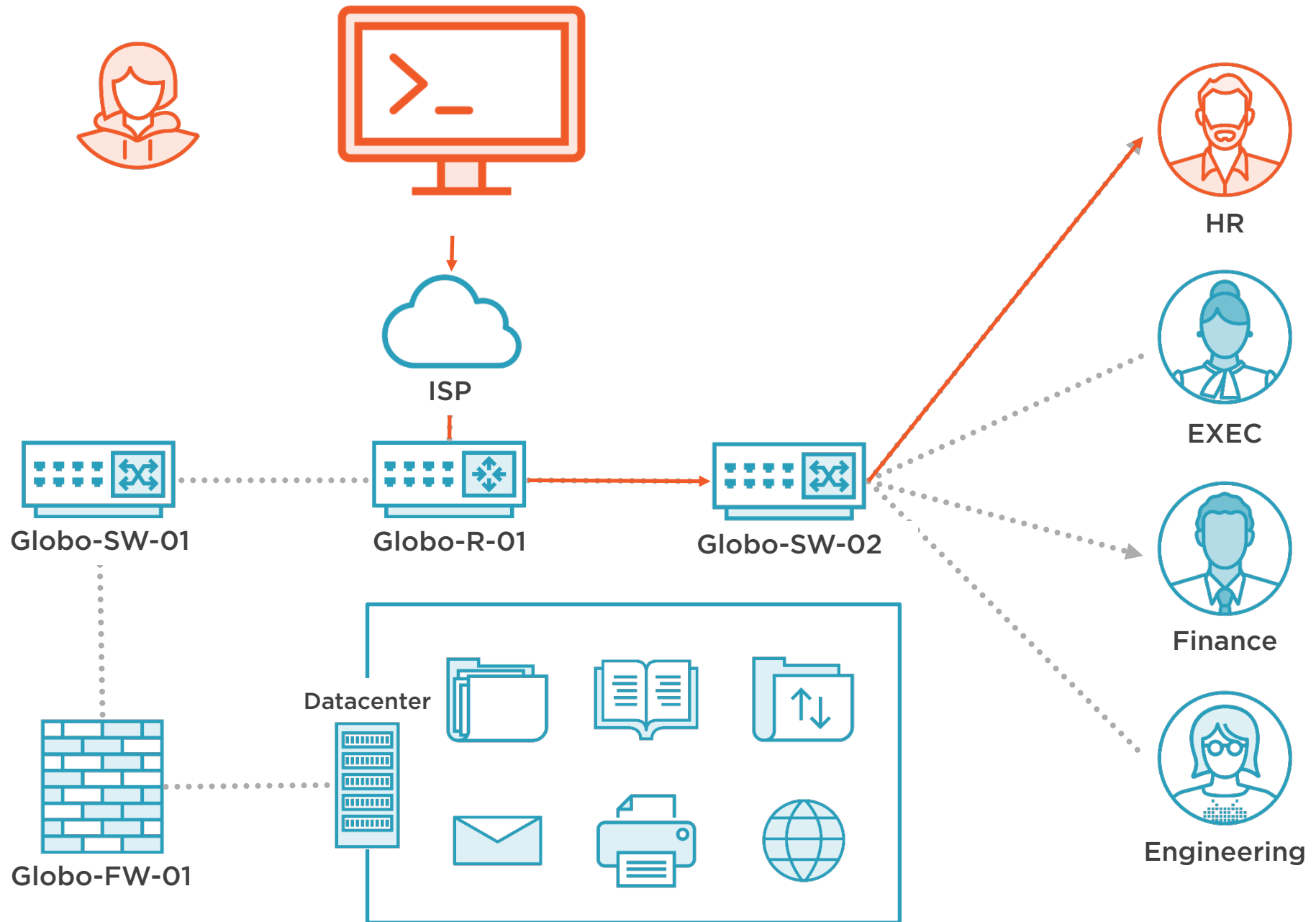












Demo



Getting started with Gophish

- Obtain Gophish and start it on your hacking workstation
- Explore the menus and options we will use for a phishing campaign



Demo



Use Gophish to prepare for a phishing campaign by malicious link

- Use Gophish to create the phishing email
- Use Gophish to configure a landing page for the malicious link

Creating the email and landing page are needed for a malicious link campaign



Demo



Use Gophish to configure emails with malicious attachments

- Use Gophish to create an email directing the target to an attachment
- Upload a malicious attachment to Gophish

Gophish enables you to use multiple phishing techniques and campaigns

