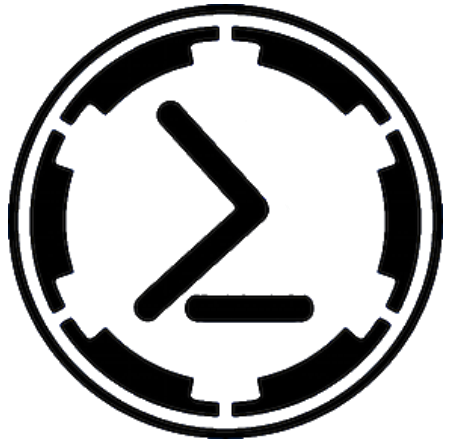
Persistence with Empire

Rishalin Pillay

OFFENSIVE CYBER SECURITY AUTHOR & SPECIALIST

@r1shal1n



PowerShell Empire (PSEmpire) Creator: @harmjoy, @sixdub, @enigma0x3, rvrsh3ll, @killswitch_gui & @xorrior.
https://github.com/EmpireProject/Empire/

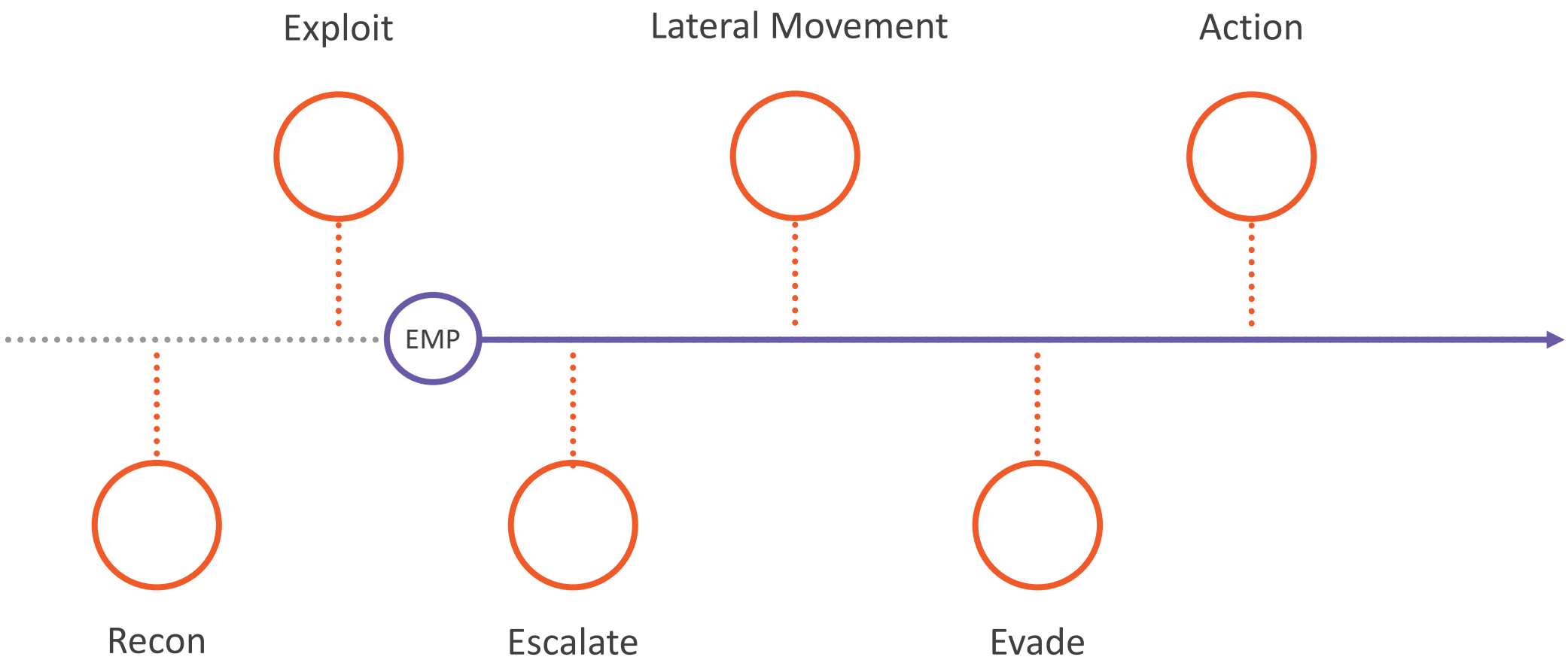
Empire : Maintained by BC-Security
https://github.com/BC-SECURITY/Empire/

Empire 3 is a pure PowerShell post exploitation framework. It merged the previous PowerShell Empire and Python EmPyre projects.

Starkiller Creator: BC-Security
https://github.com/BC-SECURITY/Starkiller/

Multi-user GUI for interfacing with the Empire server.

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

Persistence

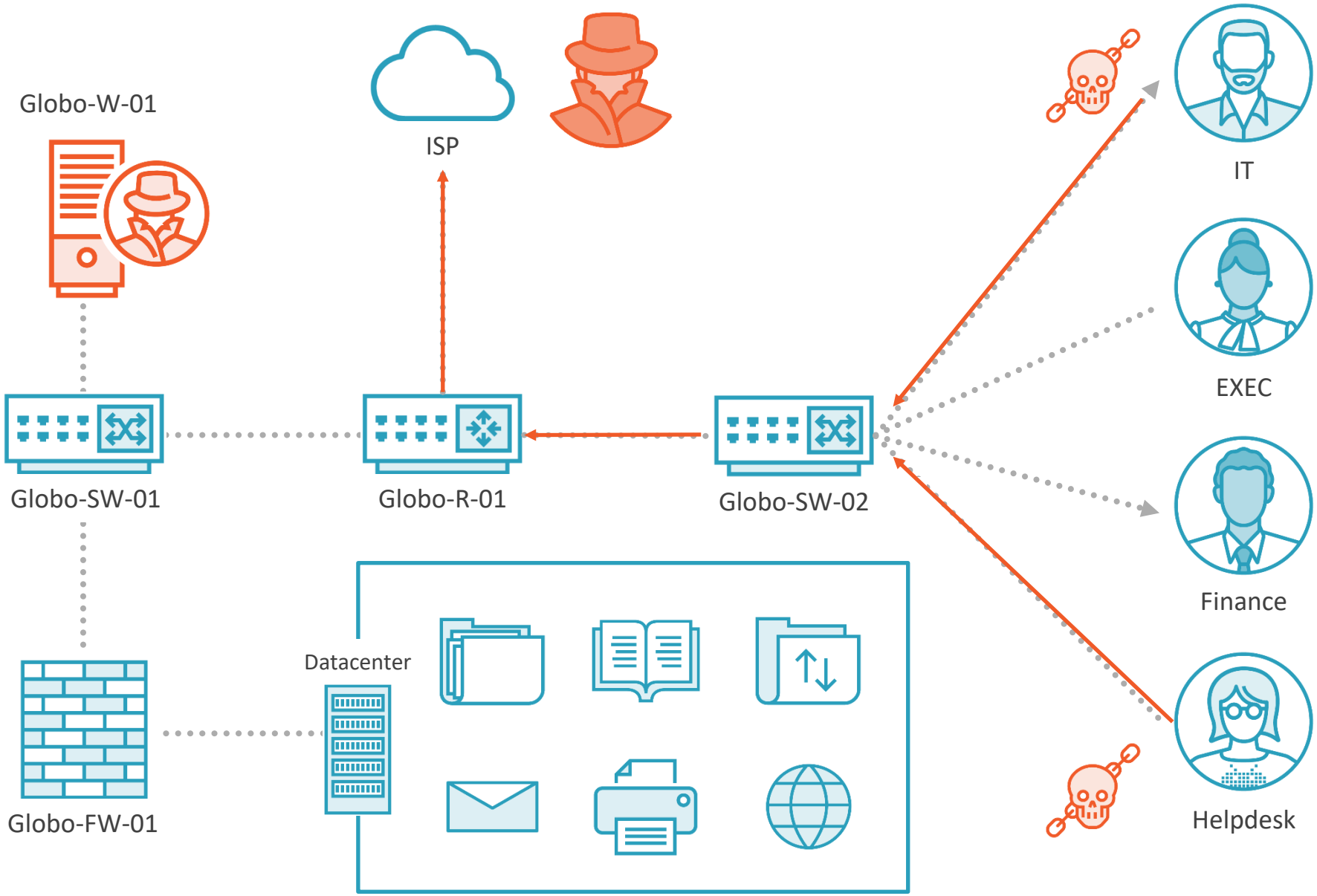
- T1547.001 Boot or Logon Autostart Execution
- T1136.001 Create Account: Local Account
- T1053.002 Scheduled Task/Job
- T1546.003 Event Triggered Execution

Kali Linux 2020.3

Up to date:

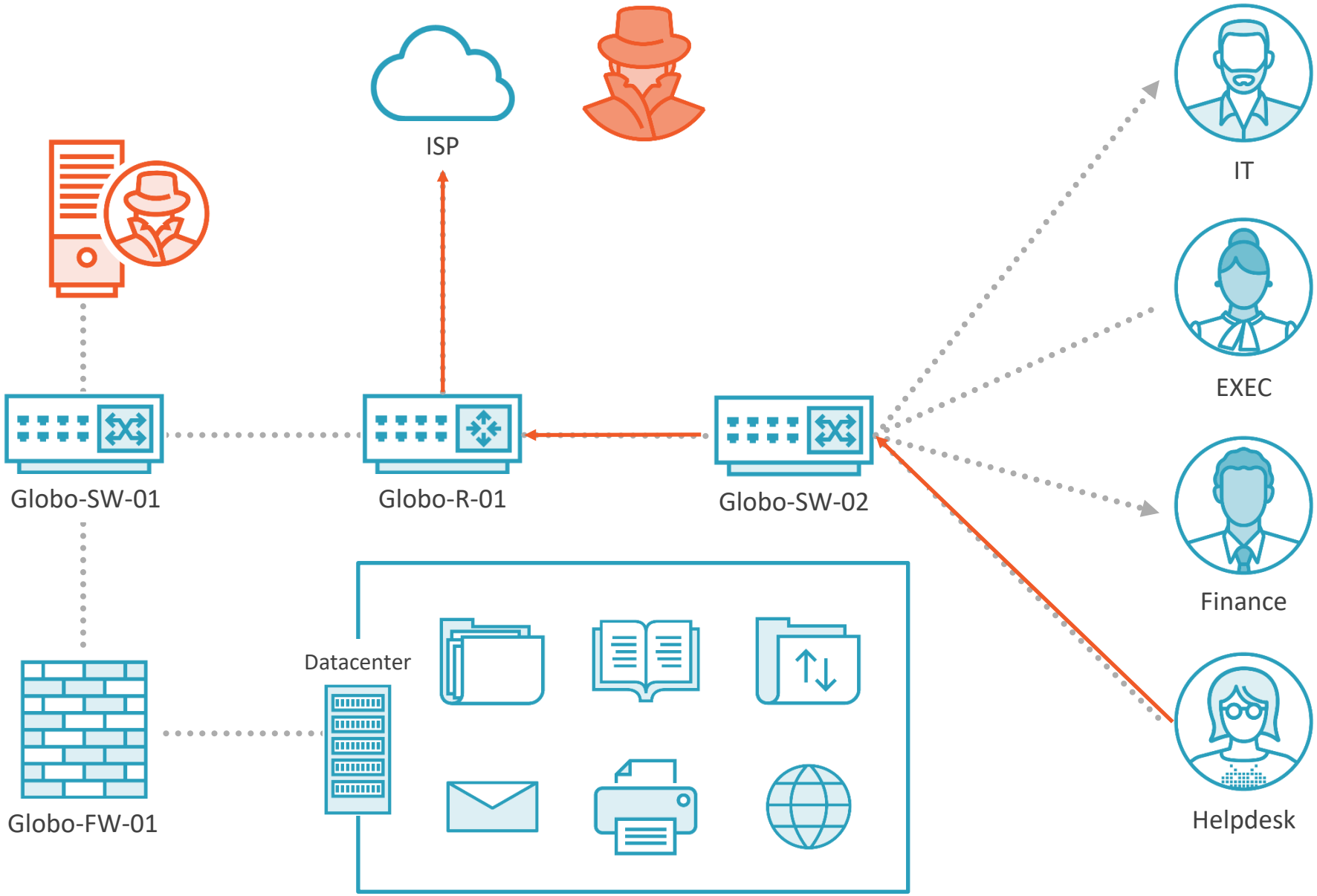
apt-get update

apt-get upgrade


Globo-W-01
ISP
IT
EXEC
Finance
Helpdesk
Globo-SW-01
Globo-R-01
Globo-SW-02
Datacenter
Globo-FW-01

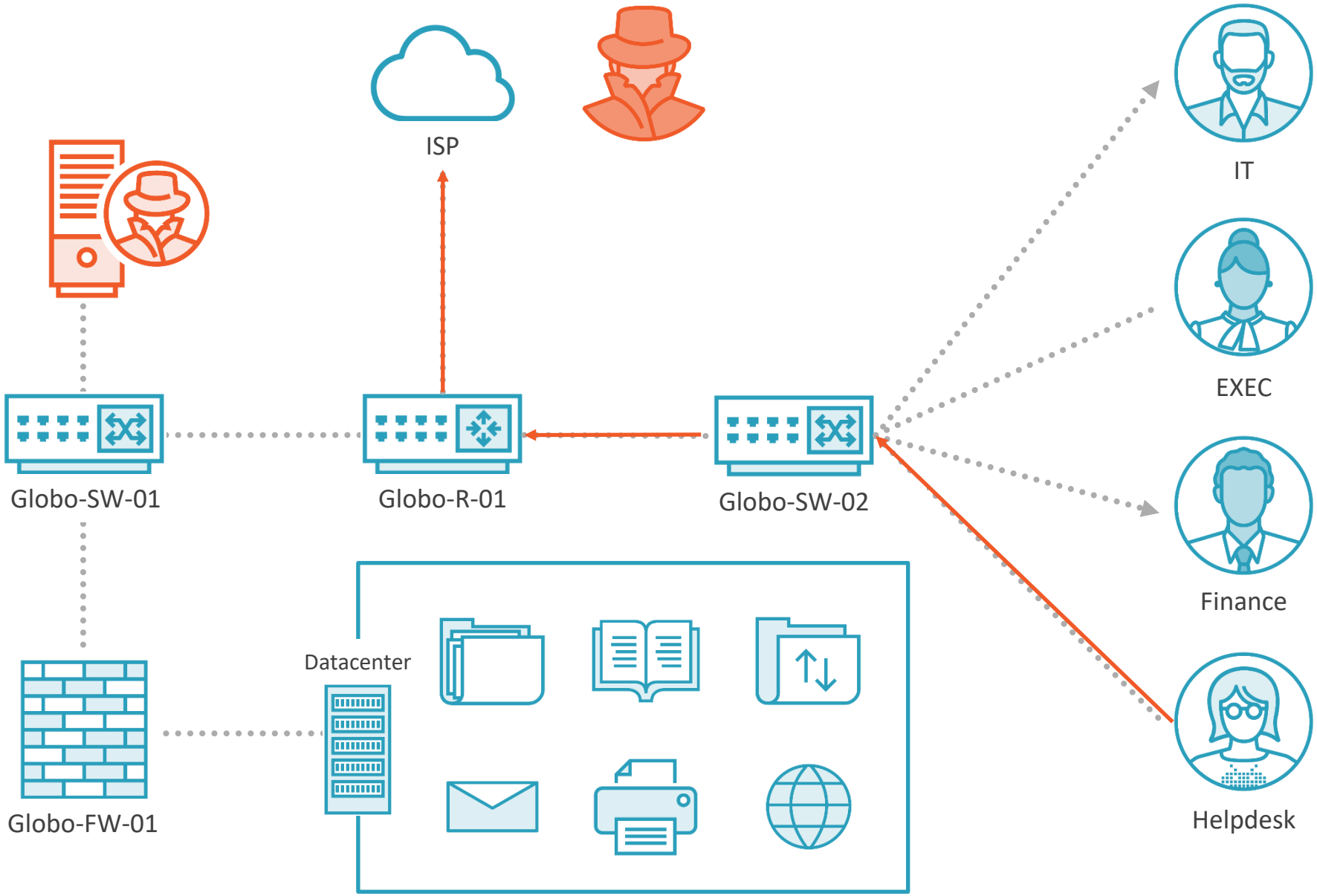
Demo

Obtaining a high integrity agent


ISP
IT
EXEC
Finance
Helpdesk
Globo-SW-01
Globo-R-01
Globo-SW-02
Globo-FW-01
Datacenter

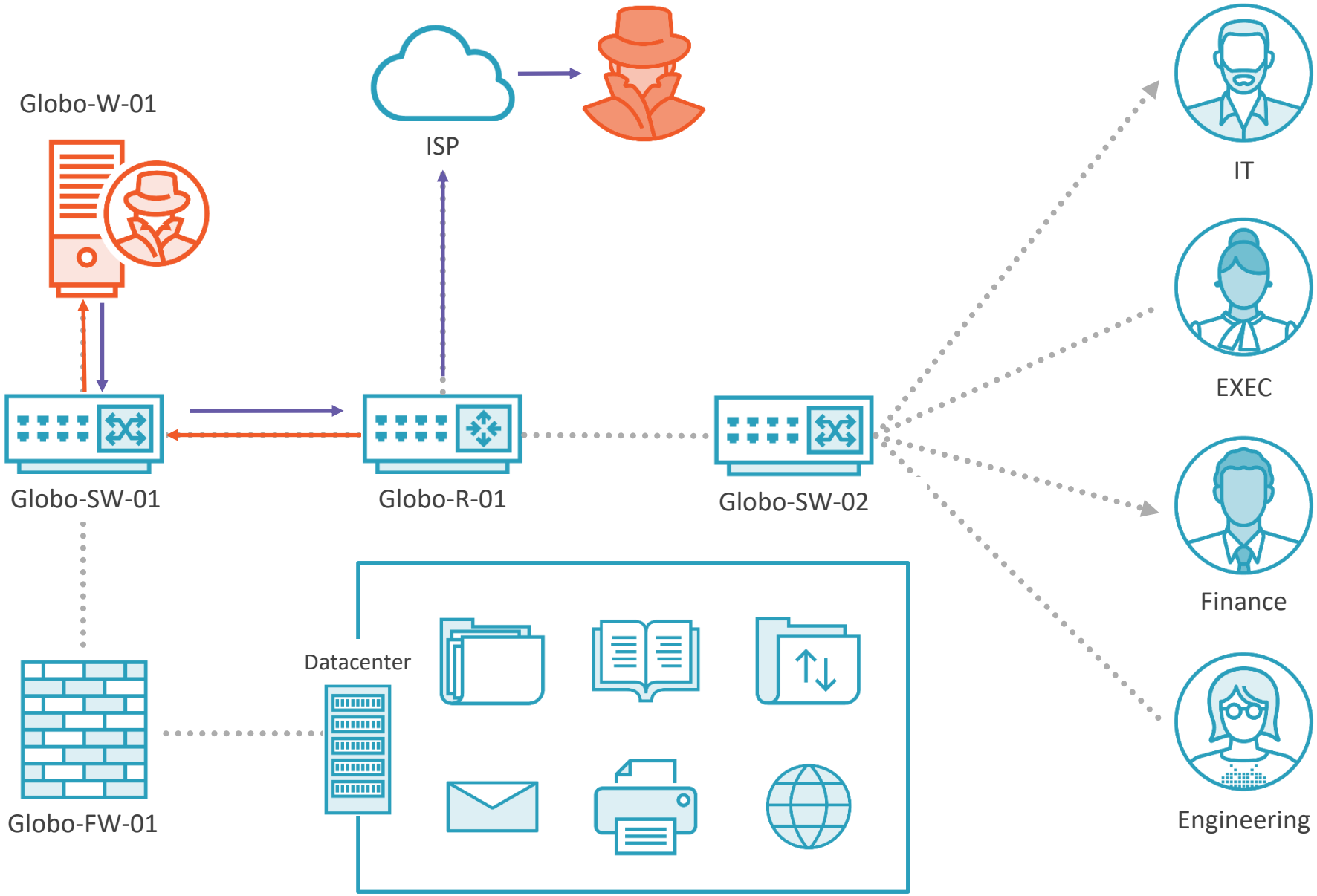
Demo

Obtaining persistence with a WMI attack


ISP
IT
EXEC
Finance
Helpdesk
Globo-SW-01
Globo-R-01
Globo-SW-02
Globo-FW-01
Datacenter

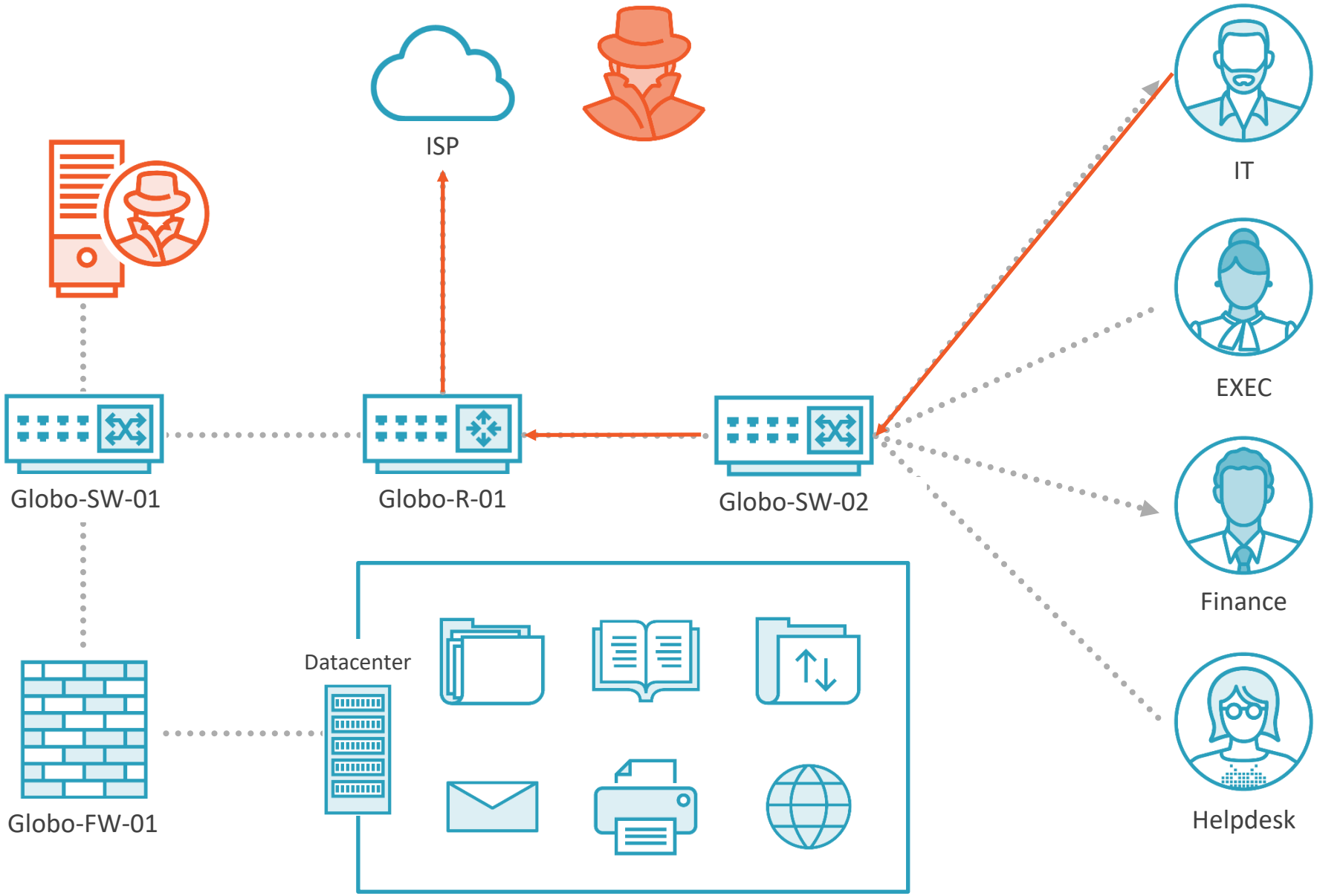
Demo

Obtaining persistence a registry implant


Globo-W-01
ISP
IT
EXEC
Globo-SW-01
Globo-R-01
Globo-SW-02
Finance
Datacenter
Engineering
Globo-FW-01

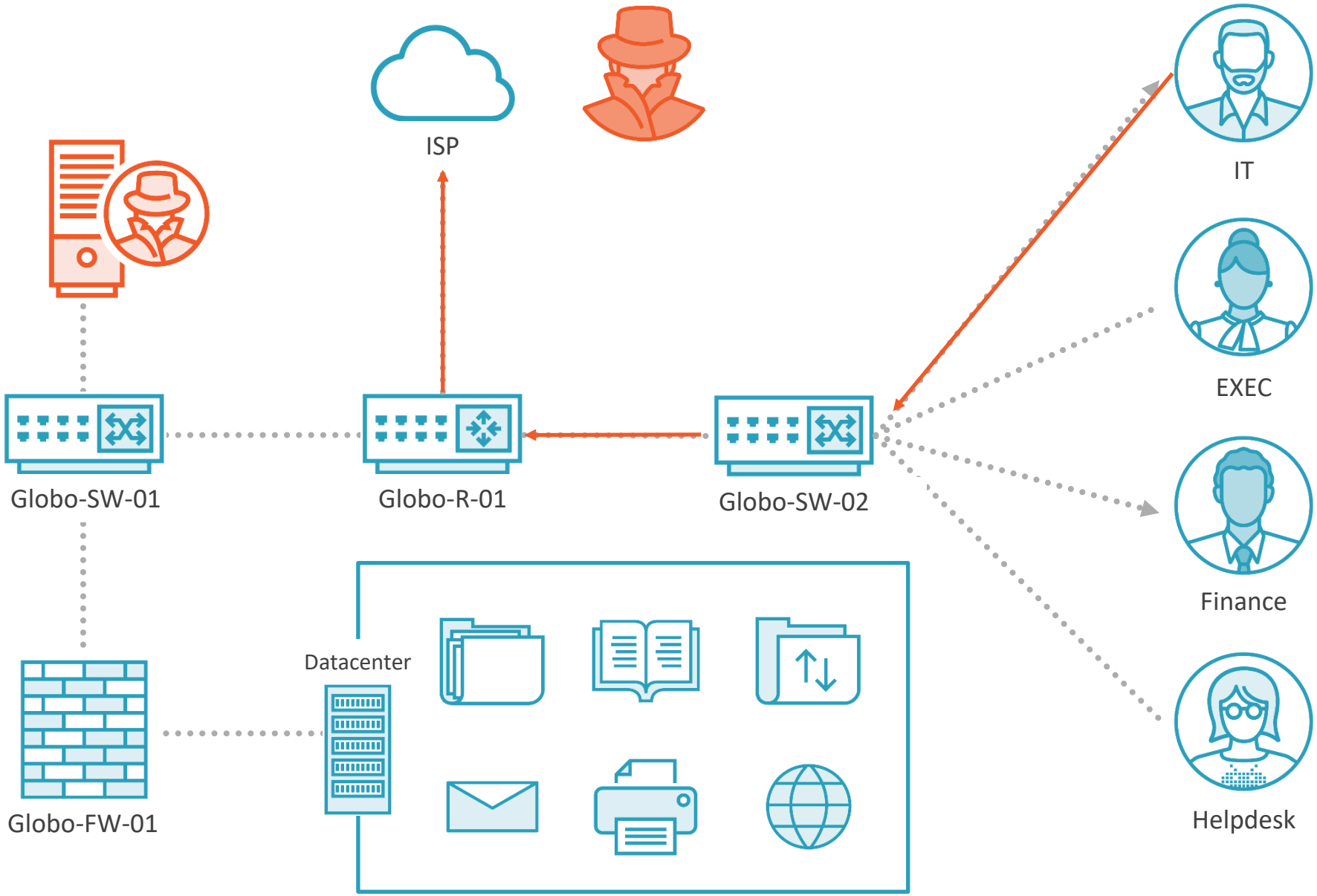
Demo

Obtaining persistence with a scheduled task


ISP
IT
EXEC
Finance
Helpdesk
Globo-SW-01
Globo-R-01
Globo-SW-02
Globo-FW-01
Datacenter

Demo

Obtaining persistence using PowerBreach


ISP
IT
EXEC
Finance
Helpdesk
Globo-SW-01
Globo-R-01
Globo-SW-02
Globo-FW-01
Datacenter

More Information

Documentation

Empire Documentation

https://www.powershellempire.com/

Related Information

Command and Control with Empire– Pluralsight

MITRE ATT&CK Software Page

- https://attack.mitre.org/software/S0363/

Thank you!

Rishalin Pillay
Cybersecurity Author &
Specialist