Privilege Escalation with UACMe

Malek Mohammad
Information Security Consultant

www.linkedin.com/in/malekmohammad

UACMe

UACMe

Creator: hFireF0x

Privilege escalation tool to defeat Microsoft Windows User Account Control. It has over 60 exploits that can be used to bypass Windows UAC consent box. This is a small command line tool that performs the task consistently

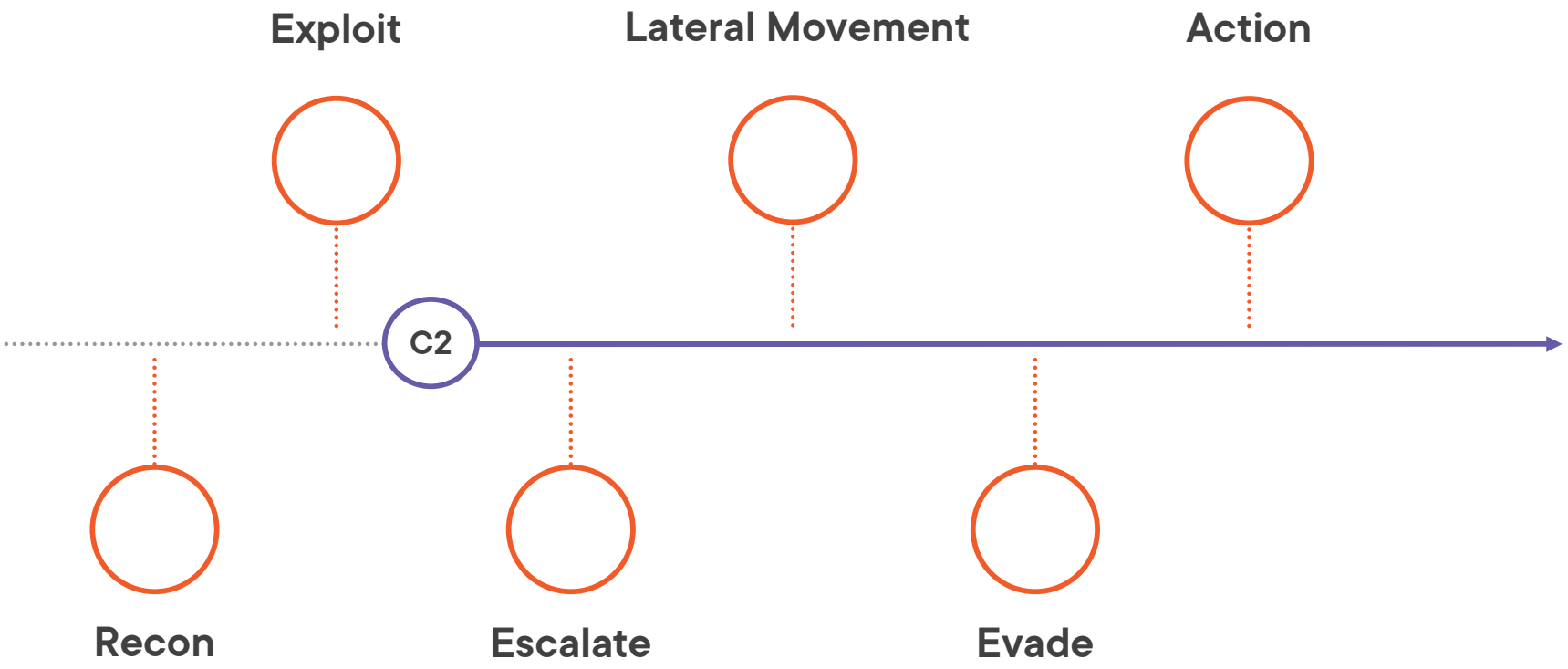
UACMe

Privilege Escalation tool that can be used by Red, Blue teamers and APT groups

You can get it from this repo
www.github.com/hfiref0x/UACME

This is nearly the perfect tool to use against misconfigured servers

Kill Chain



MITRE ATT&CK

Tactics

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact

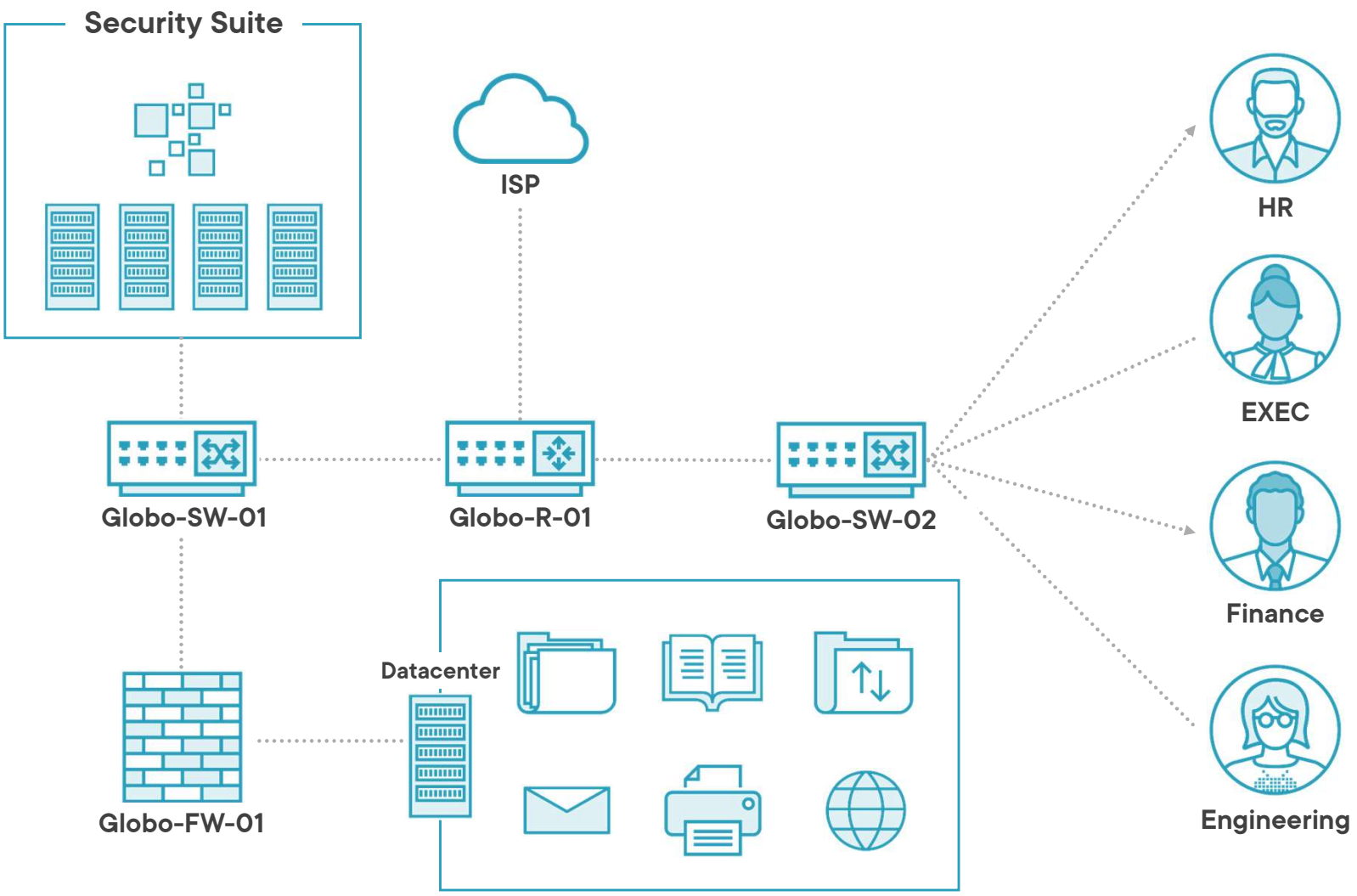
MITRE ATT&CK

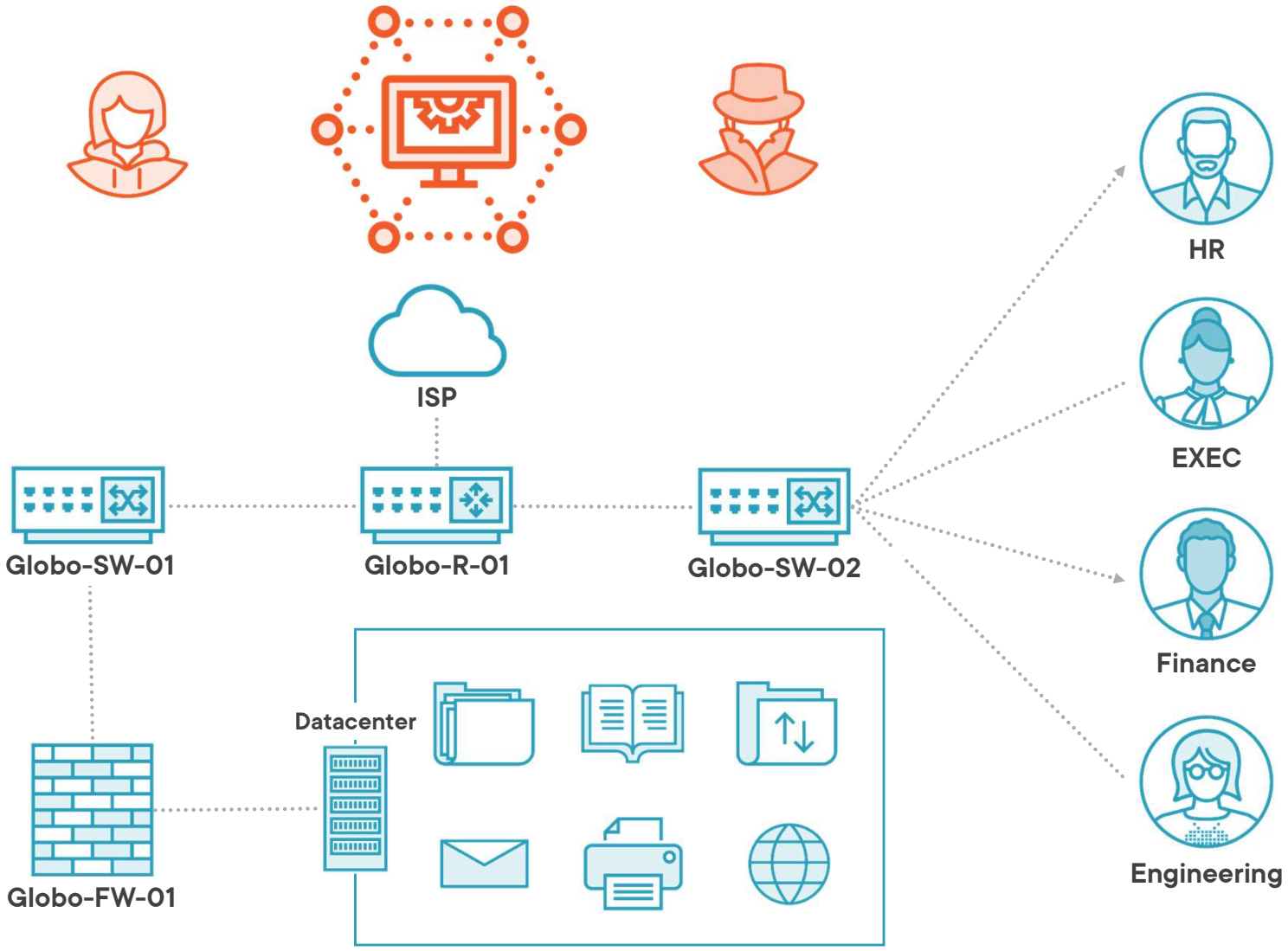
Tactics

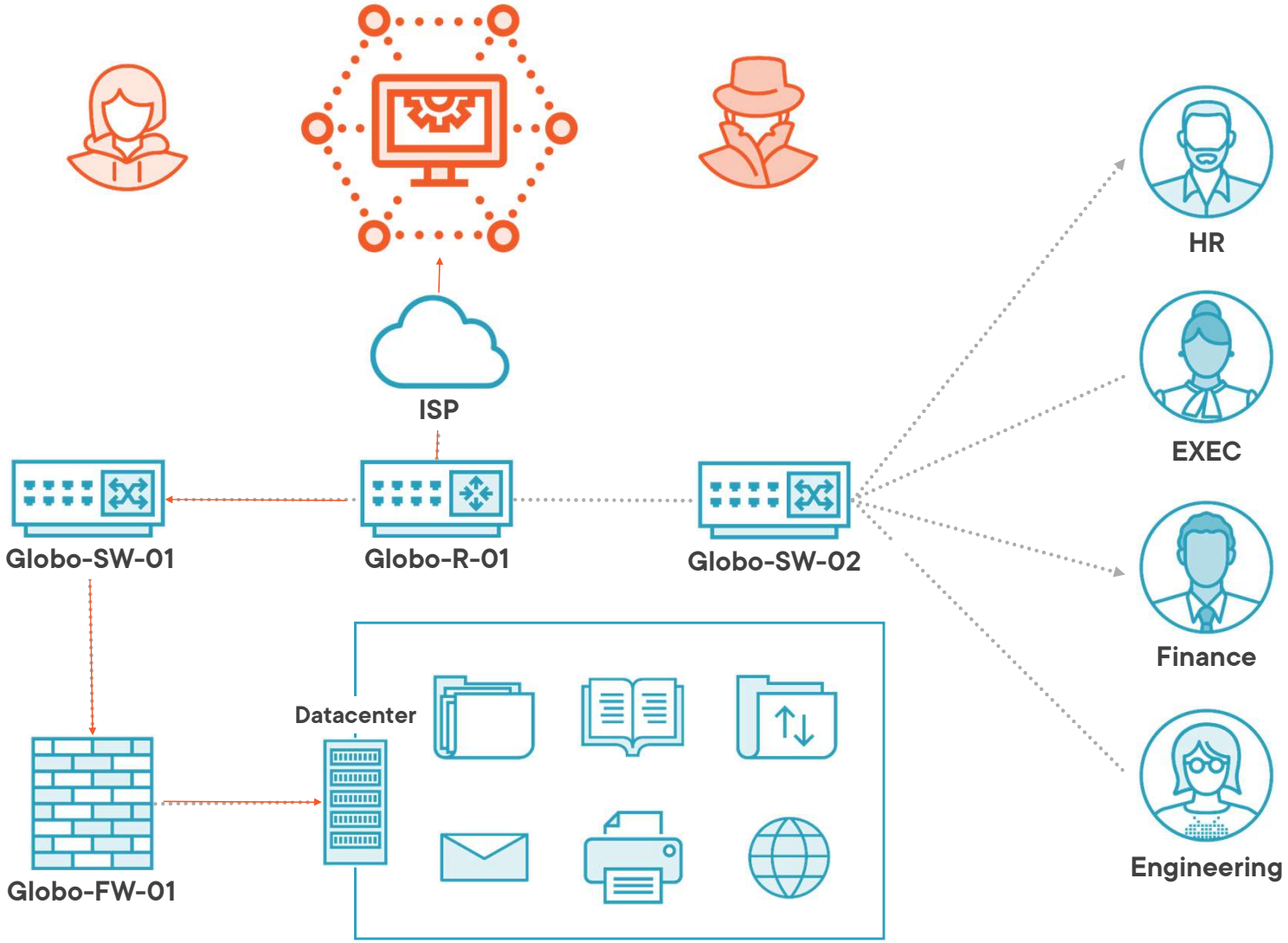
- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact

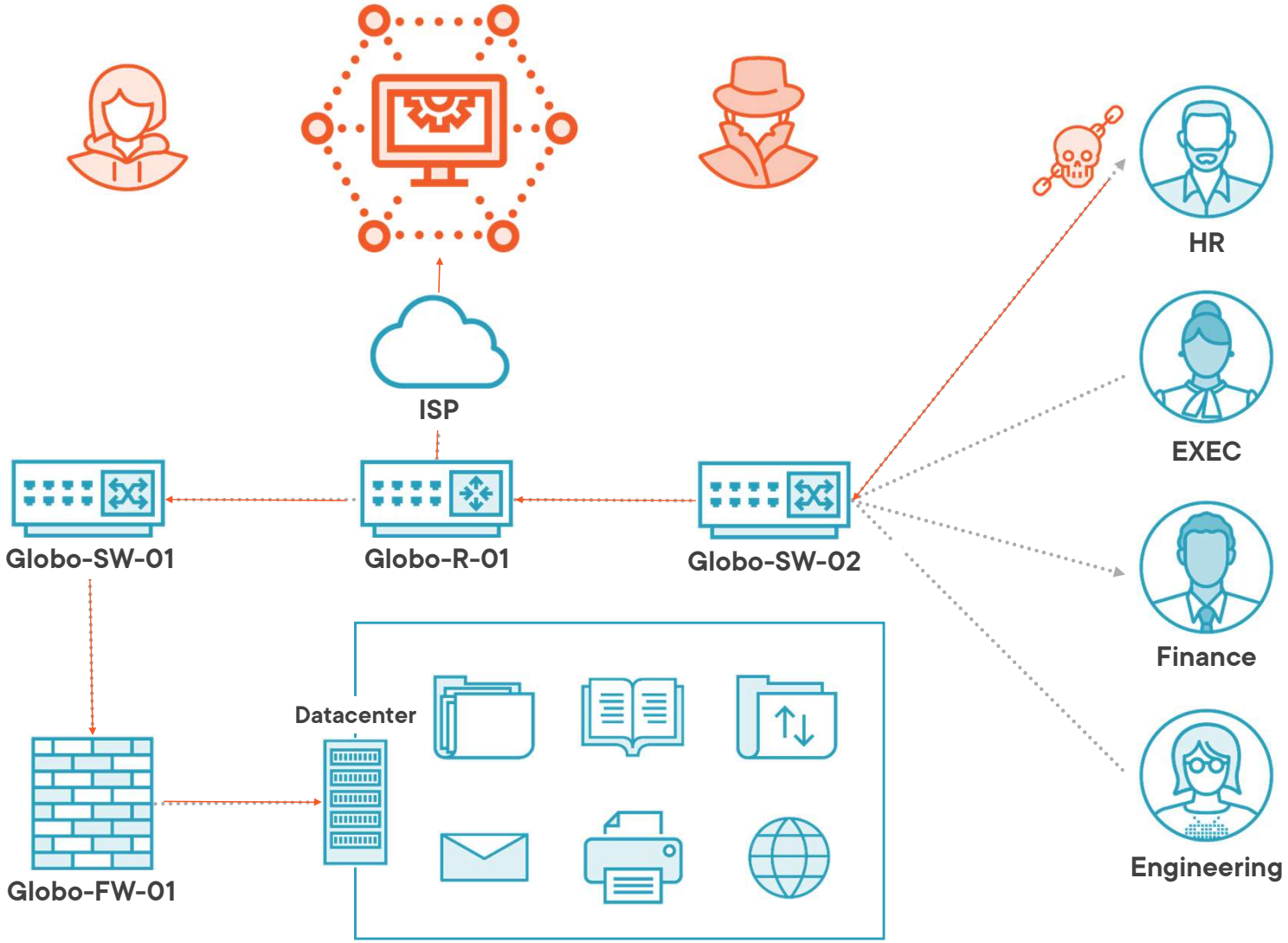
T1548:
Abuse Elevation Control Mechanism

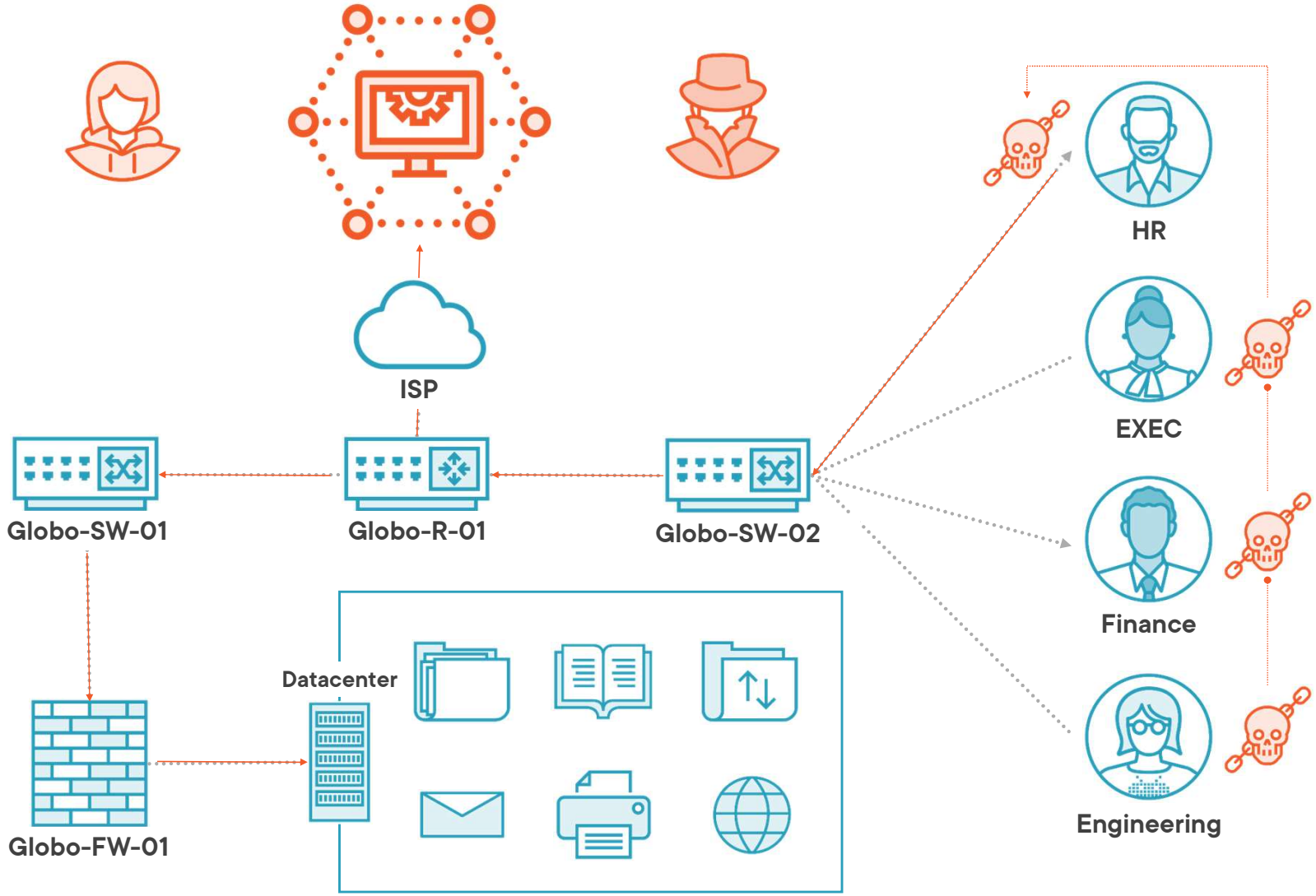
T1548.002:
Bypass User Account Control


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


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


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


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


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