

Command and Control with PoshC2



Jeff Stein

CISSP, GCED, CEH, CHFI, SECURITY+

www.securityinobscurity.com







Creator: Nettitude

PoshC2 is a proxy aware Command and Control framework used to assist with red teaming, post-exploitation and lateral movement.





Open source Command and Control framework

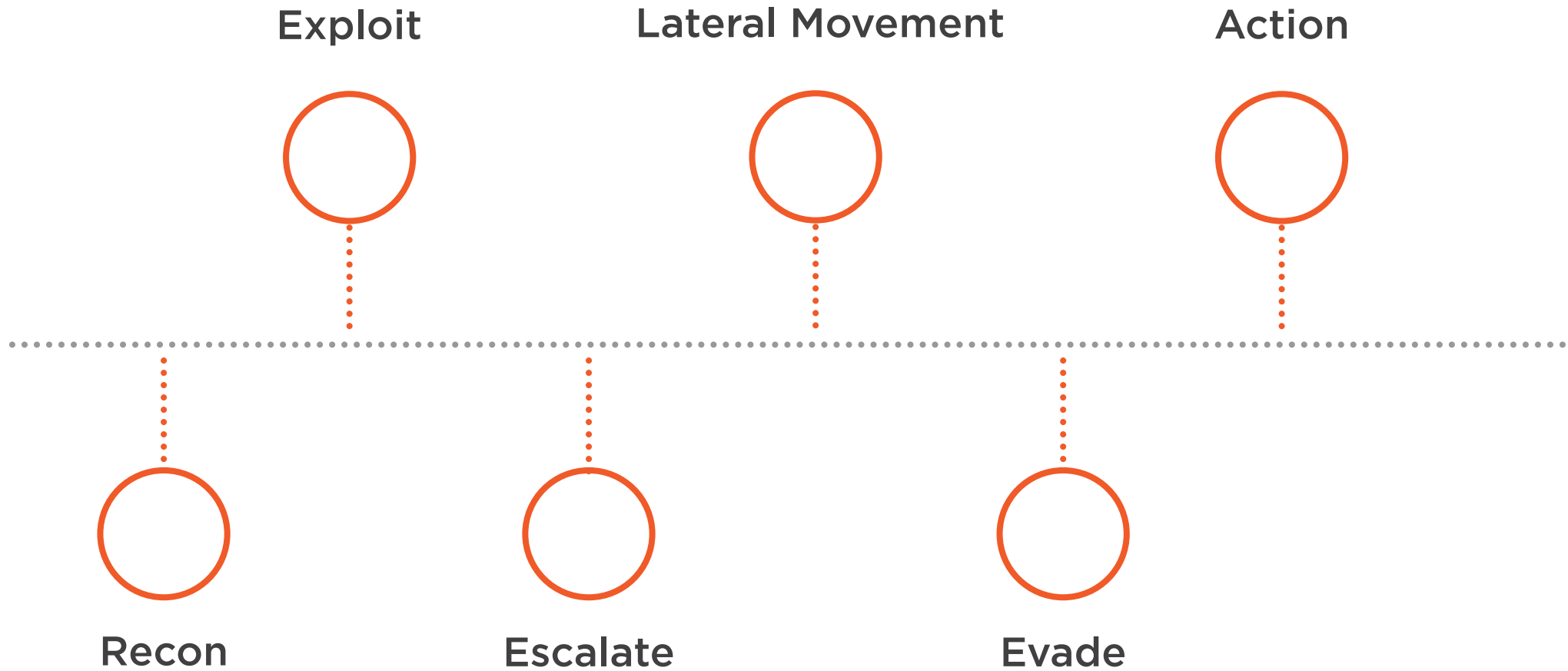
Available from the PoshC2 github repository: <https://github.com/nettitude/PoshC2>

Module approach extends the PoshC2's command and control capabilities.

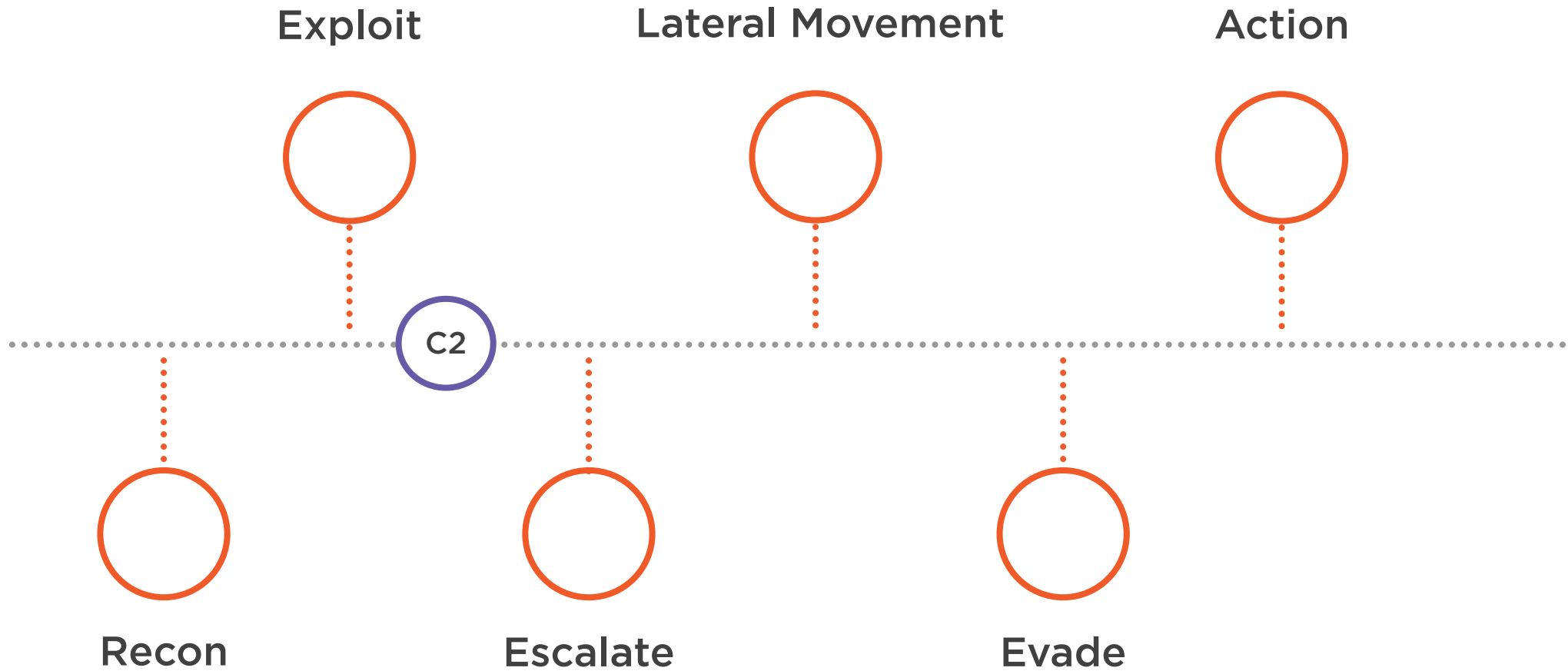
Configurable implant beacon feature allows you to effectively evade defensive measures



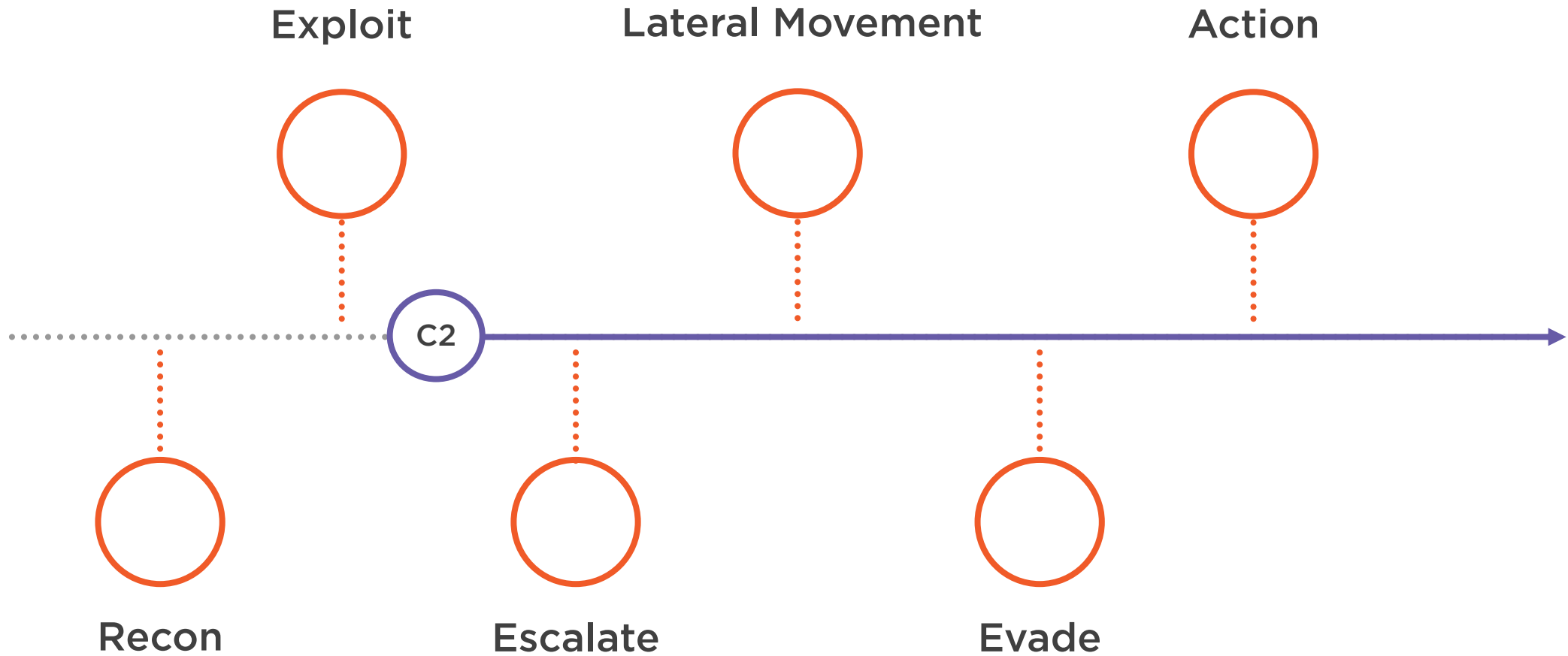
Kill Chain



Kill Chain



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



MITRE ATT&CK

Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

T1087:

Account Discovery



MITRE ATT&CK

Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

T1087:
Account Discovery

T1087.001
Local Account



MITRE ATT&CK

Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

T1087:
Account Discovery

T1087.001
Local Account

T1071:
Application Layer Protocol



MITRE ATT&CK

Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

T1087:
Account Discovery

T1087.001
Local Account

T1071:
Application Layer Protocol

T1071.001
Web Protocols



MITRE ATT&CK

Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

T1087:
Account Discovery

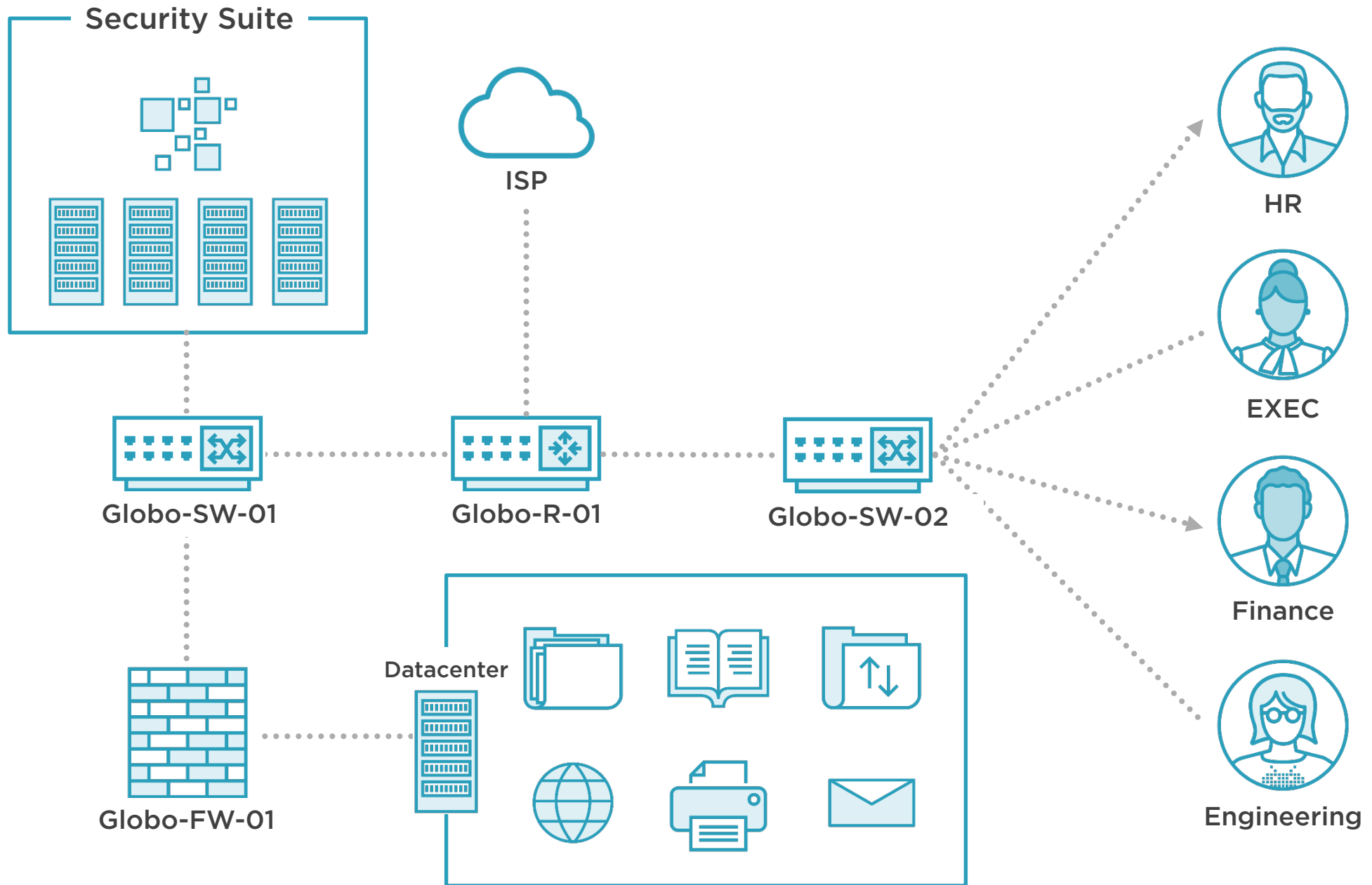
T1087.001
Local Account

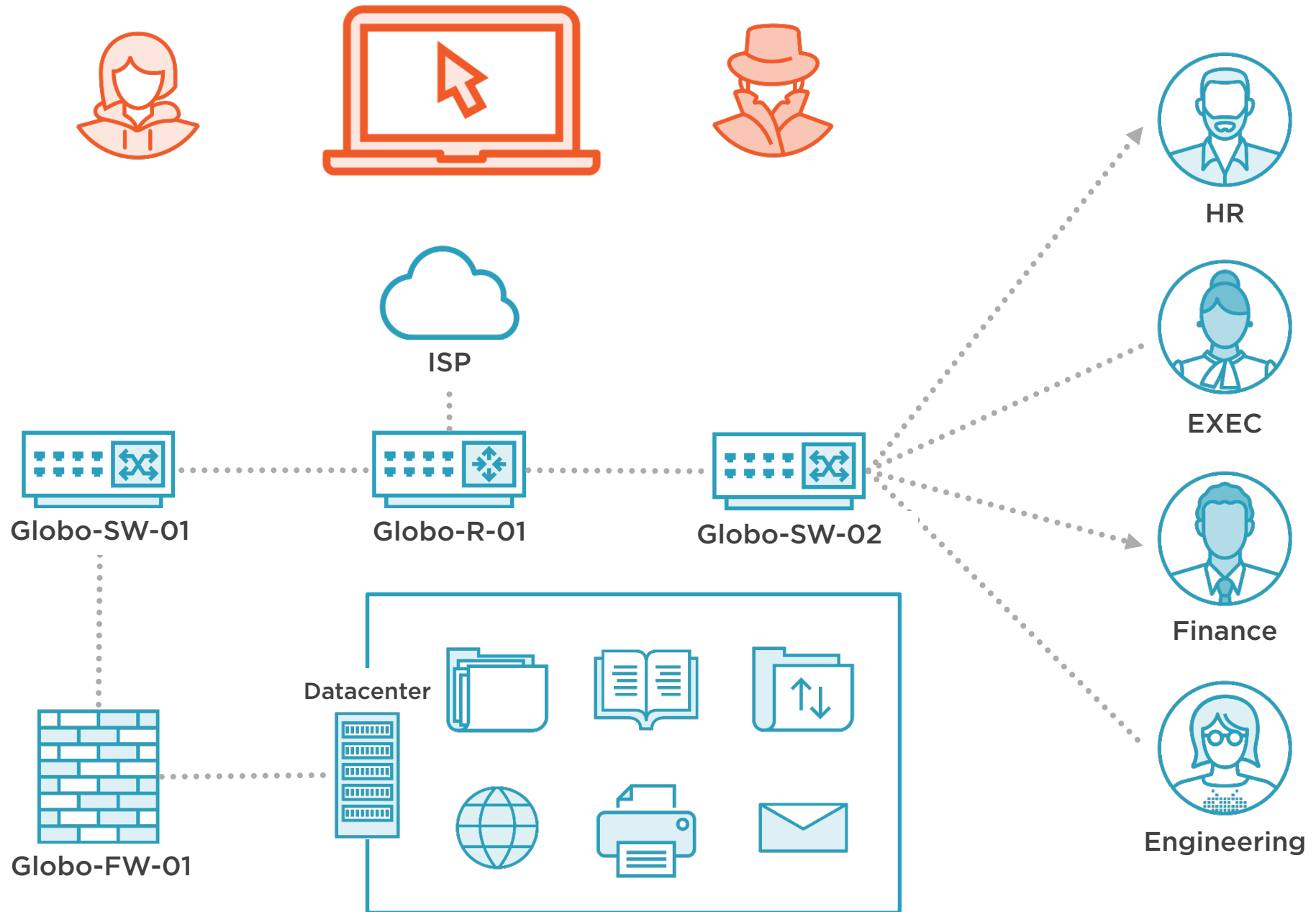
T1071:
Application Layer Protocol

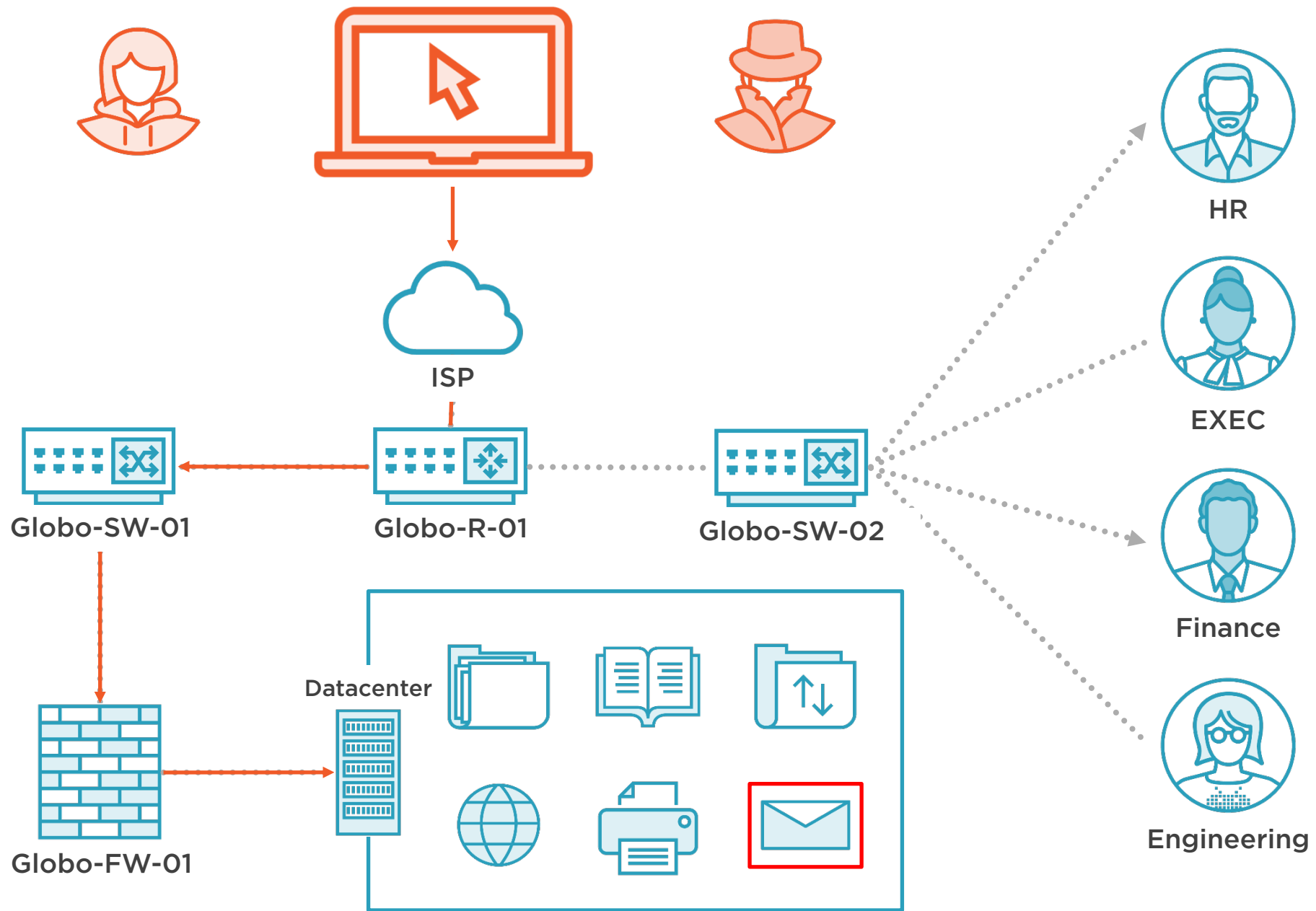
T1071.001
Web Protocols

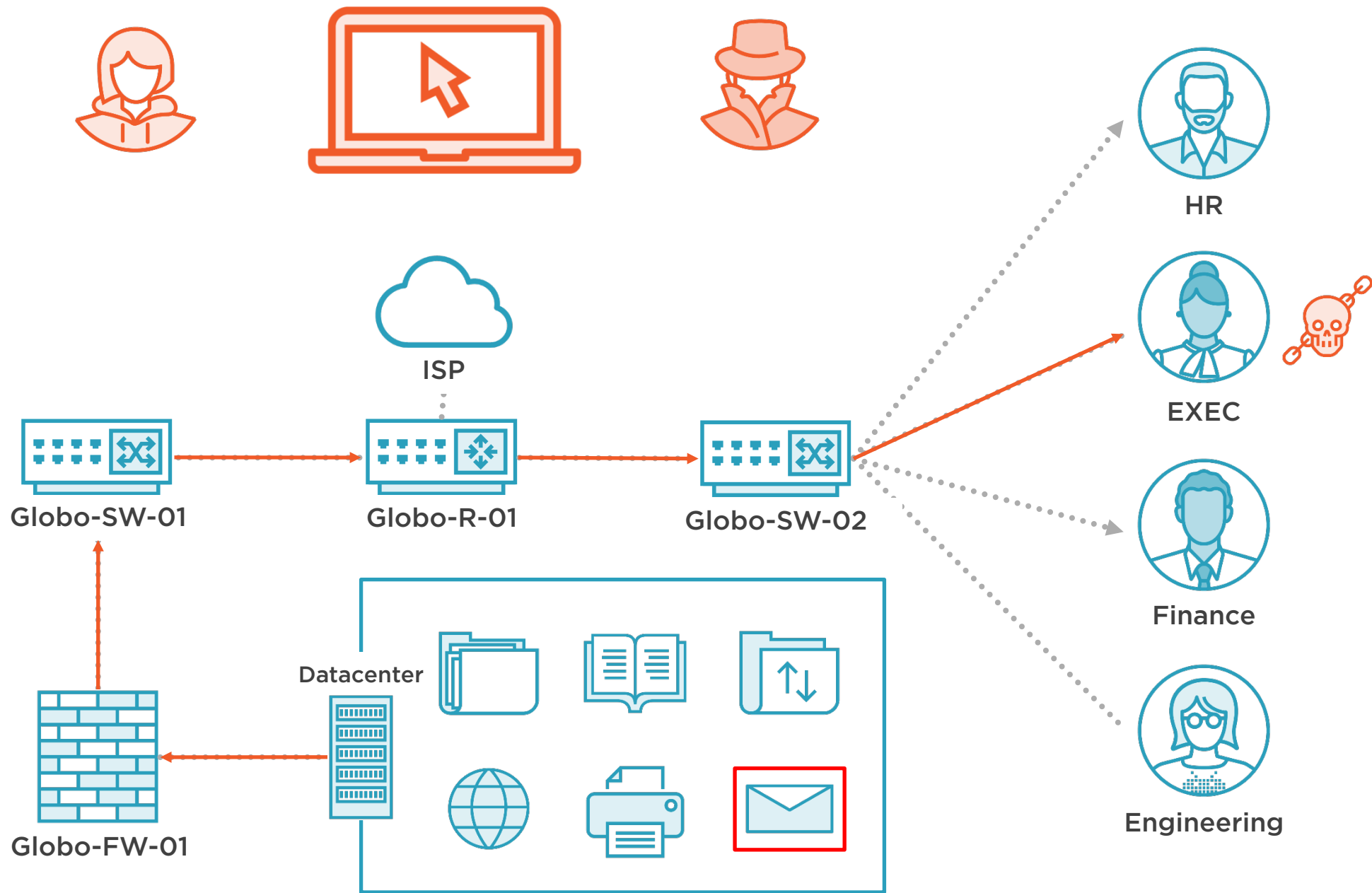
T1219:
Remote Access Software

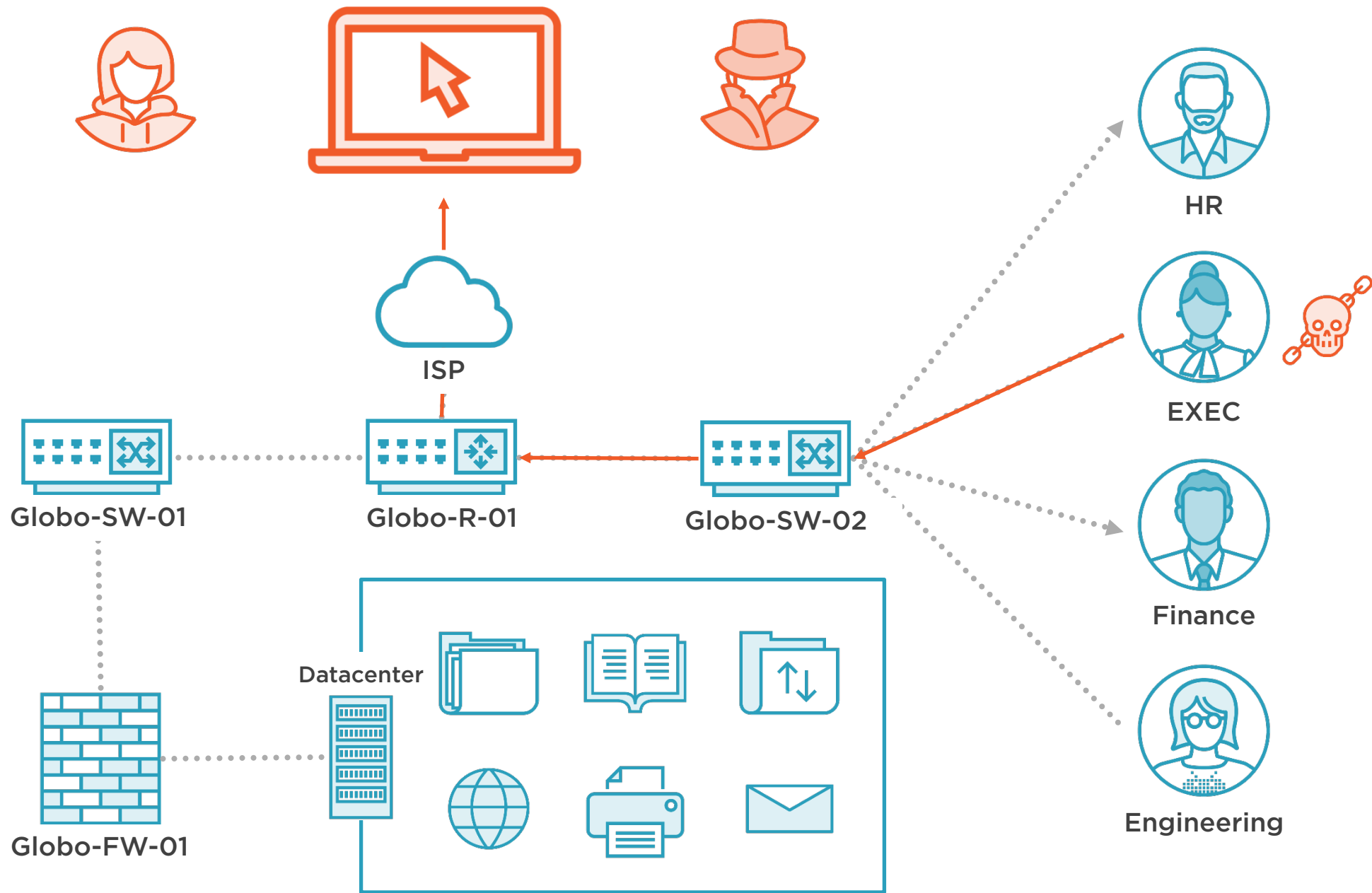


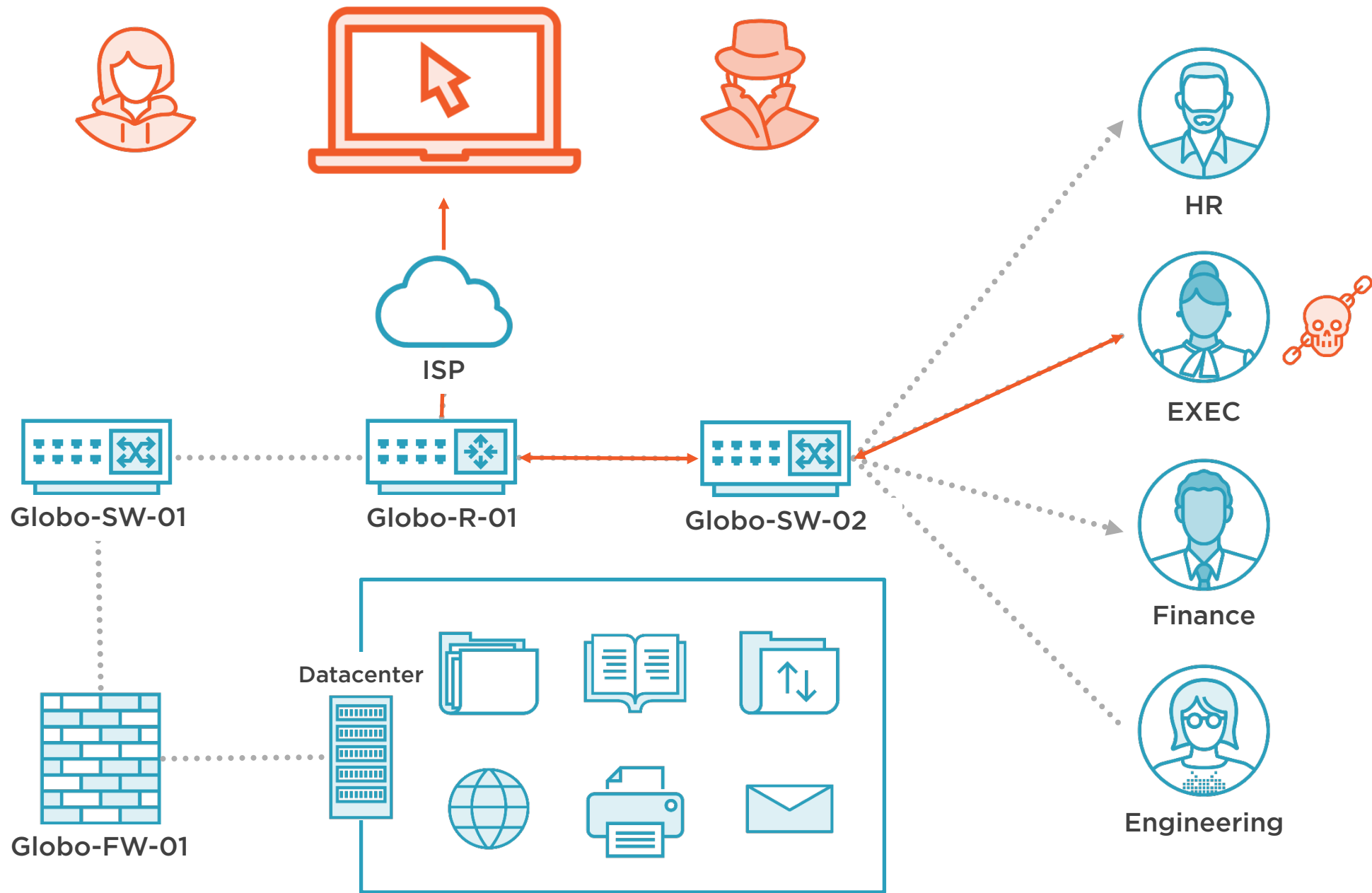


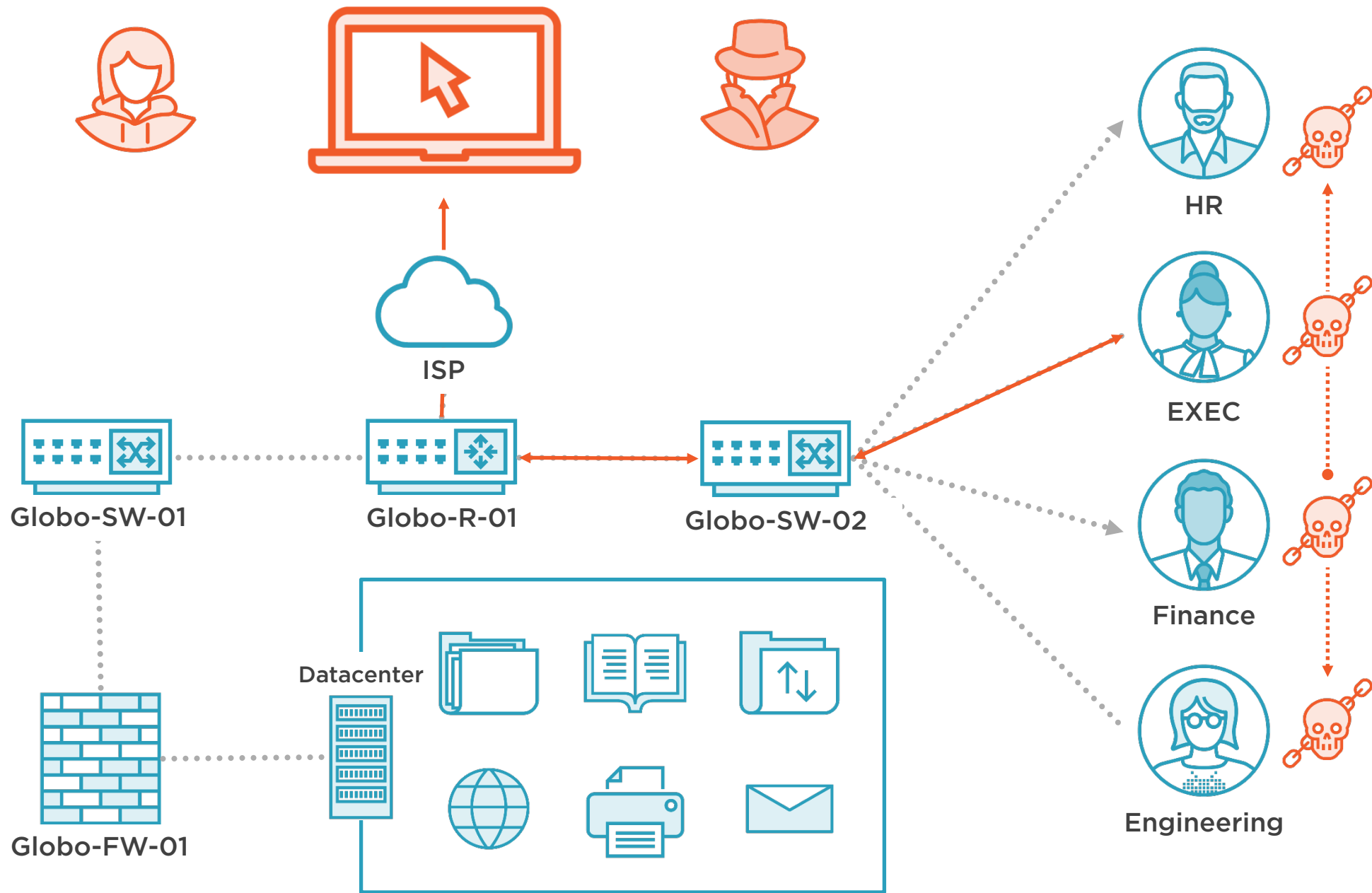












Demo



Review our PoshC2 server configuration

Enumerate our target company

- Identify potential targets

Gain initial access to deploy our implant to a victim system



Demo



Plan our post exploitation activities by enumerating our victim system

- Identify system vulnerabilities
- Search for accounts with privilege access

Exfiltrate data from identified network share locations



Demo



Harvest admin credentials to escalate our privileges

Enumerate the victim network to identify additional systems to exploit

Move laterally across the network

