Execution: Unicorn

Matt Glass

CISSP, CEH

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

```
                                                ,/
                                               //
                                             ,//
                                 ___   /|   |//
                             `__/\_ --(/|___/-/
                          \|\_-\___ __-_`- /-/ \.
                         |\_-___,-\_____--/_)' ) \
                          \ -_ /     __ \( `( __`\|
                          `\__|      |\)\ ) /(/|
   ,._____.,           ',--//-|      \  |  '   /
  /     __. \,         / /,---|       \       /
 / /    _. \  \       `/`_/ _,'        |     |
|  | ( (  \   |     ,/\'__/'/          |     |
|  \  \`--, `_/_------______/          \(   )/
| | \  \_. \,                           \___/\
| |  \_   \  \                                \
\ \    \_ \   \   /                            \
 \ \  \._  \__ \_|      |                       \
  \ \___  \      \      |                        \
   \__ \__ \  \_ |      \                         |
   |  \_____ \  ____     |                        |
   | \  \__ ---' .__\    |        |               |
   \  \__ ---   /   )    |        \              /
    \   \____/ / ()(     \          `---_       /|
     \__________/(,--__   \_________.    |    ./ |
       |     \ \ `---_\--,           \   \_,./   |
       |      \  \_ ` \   /`---_______-\   \\    /
        \     \.___,`|   /              \   \\   \
         \    |  \_ \|   \              (   |:    |
          \   \      \    |             /  / |    ;
           \   \      \    \          ( `_'   \  |
            \.  \      \.   \          `__/   |  |
             \   \       \.  \                |  |
              \   \        \  \               (  )
               \   |        \  |              |  |
                |  \         \ \              I `
                ( __;        ( _;            ('-_';
                |___\        \___:            \___:
```

Creator: Dave Kennedy

Unicorn is a simple tool for using the PowerShell downgrade attack. The open-source tool available on GitHub.

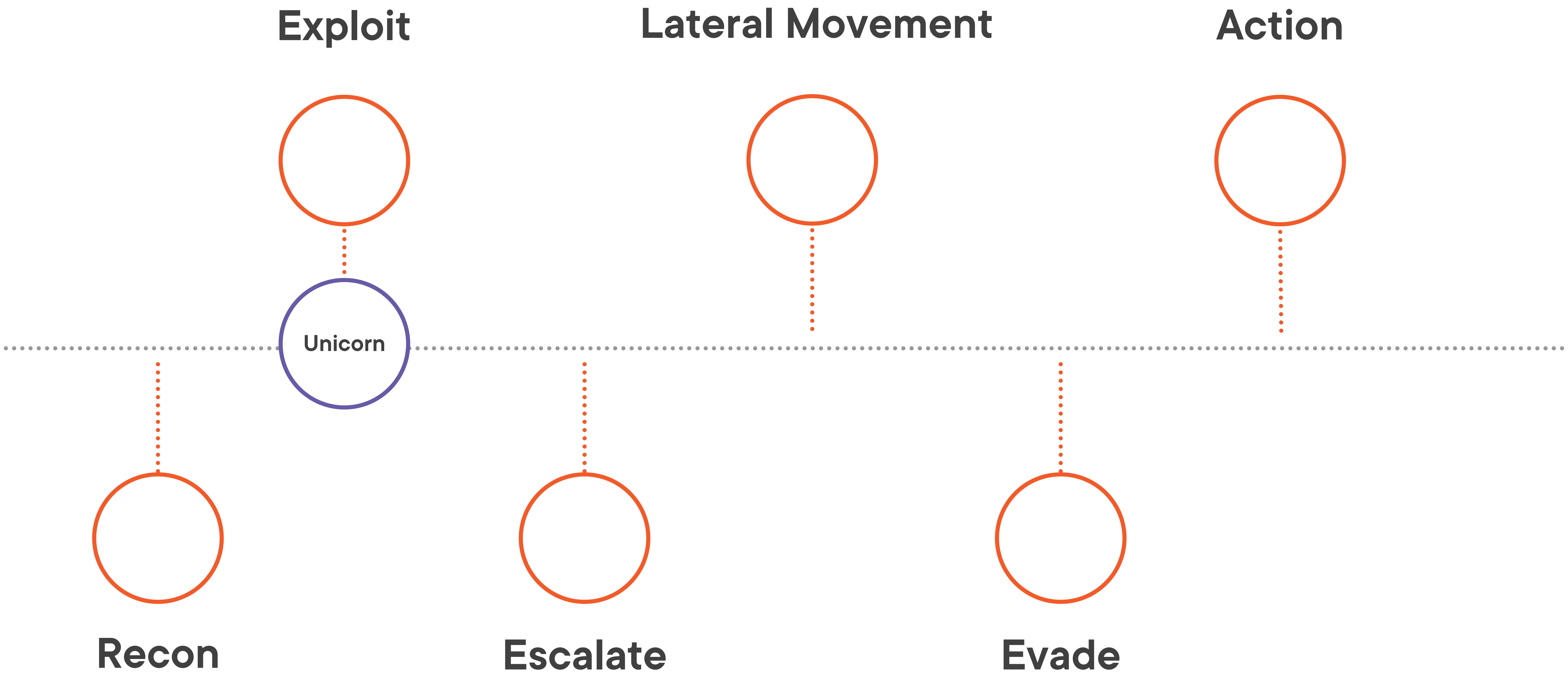
Unicorn generates PowerShell commands with payloads.

Unicorn is available on GitHub.

Unicorn enables in-memory execution of shellcode.

Unicorn uses a PowerShell downgrade attack to execute your own shellcode, cobalt strike, or Metasploit payloads.

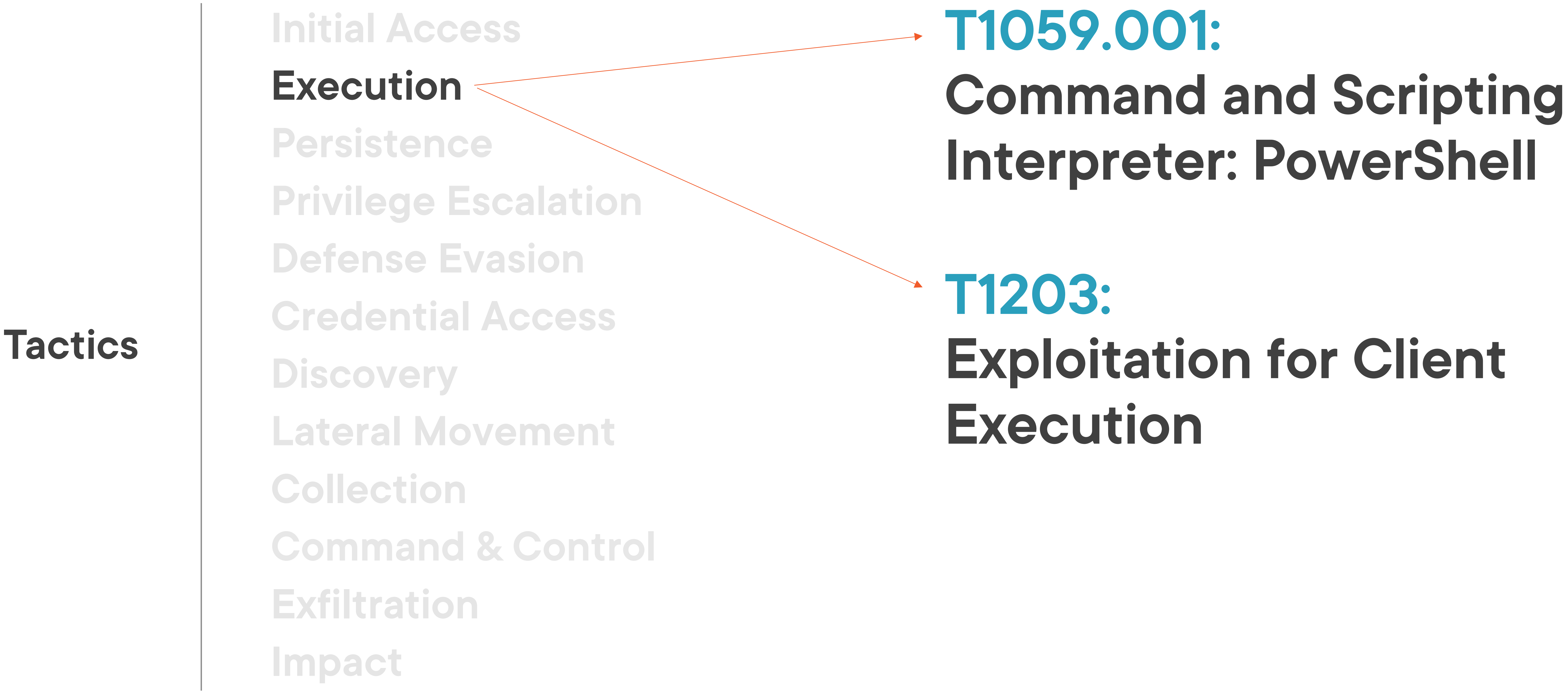
Kill Chain


Exploit
Lateral Movement
Action
Unicorn
Recon
Escalate
Evade

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

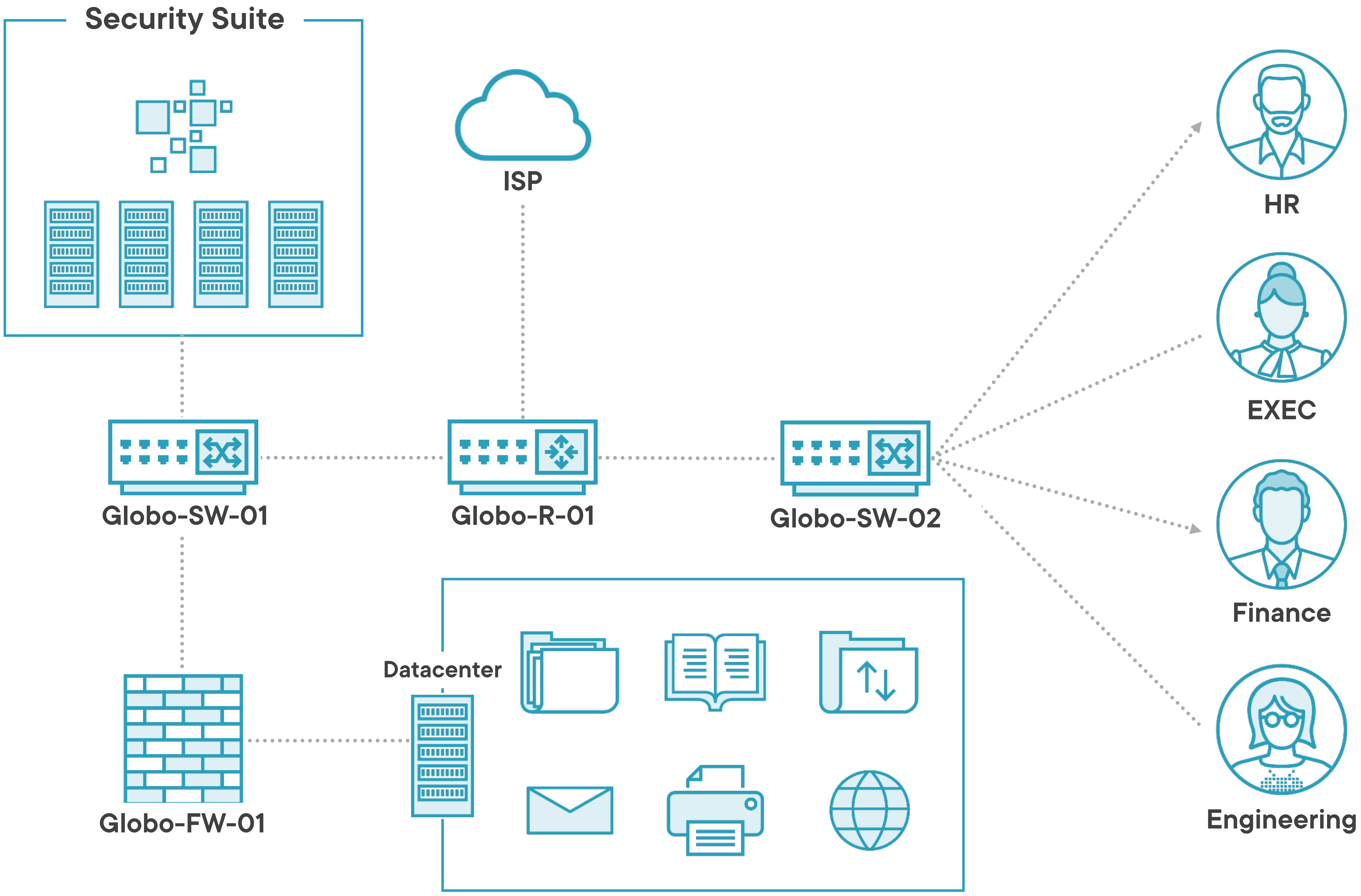


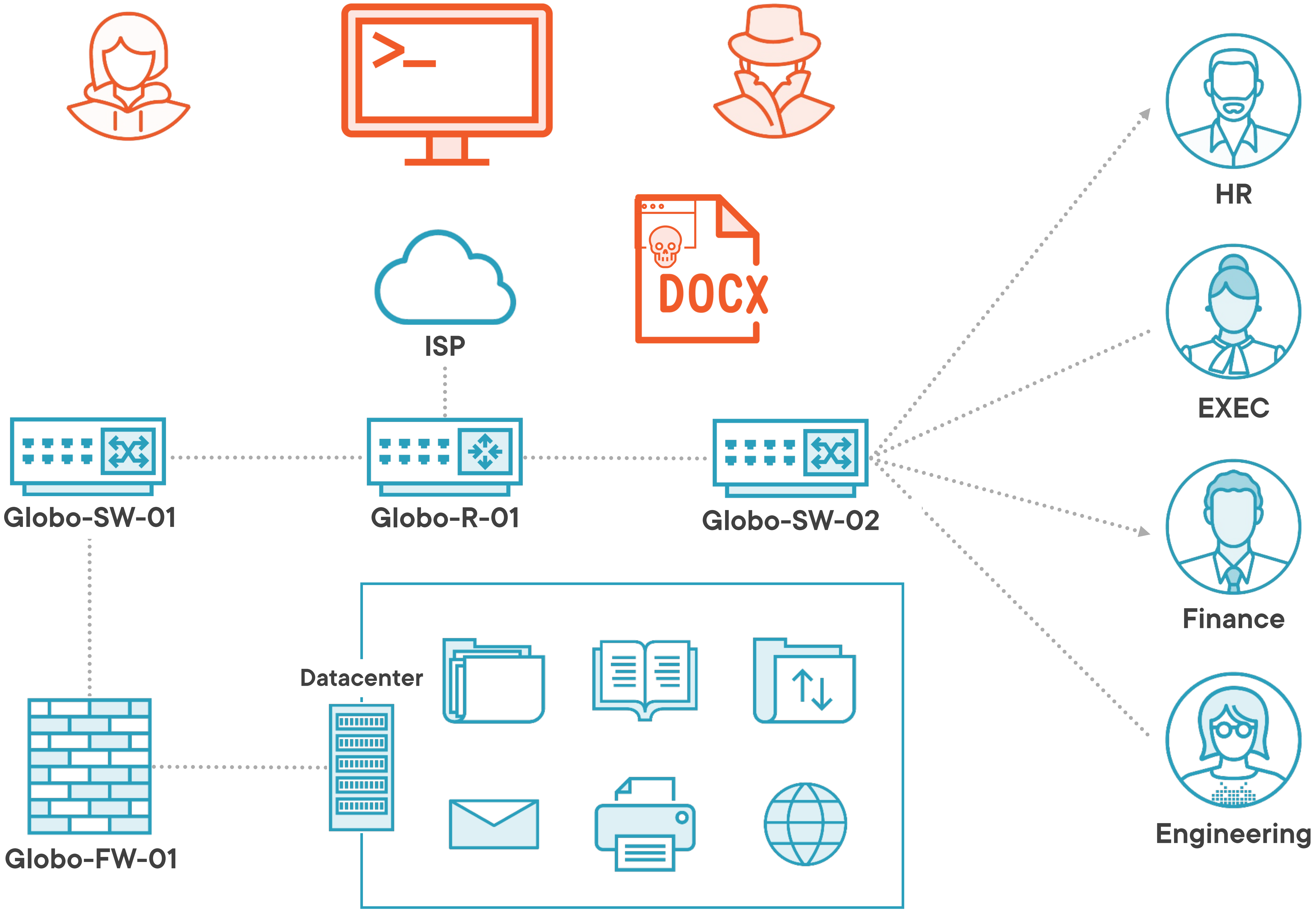
Tactics

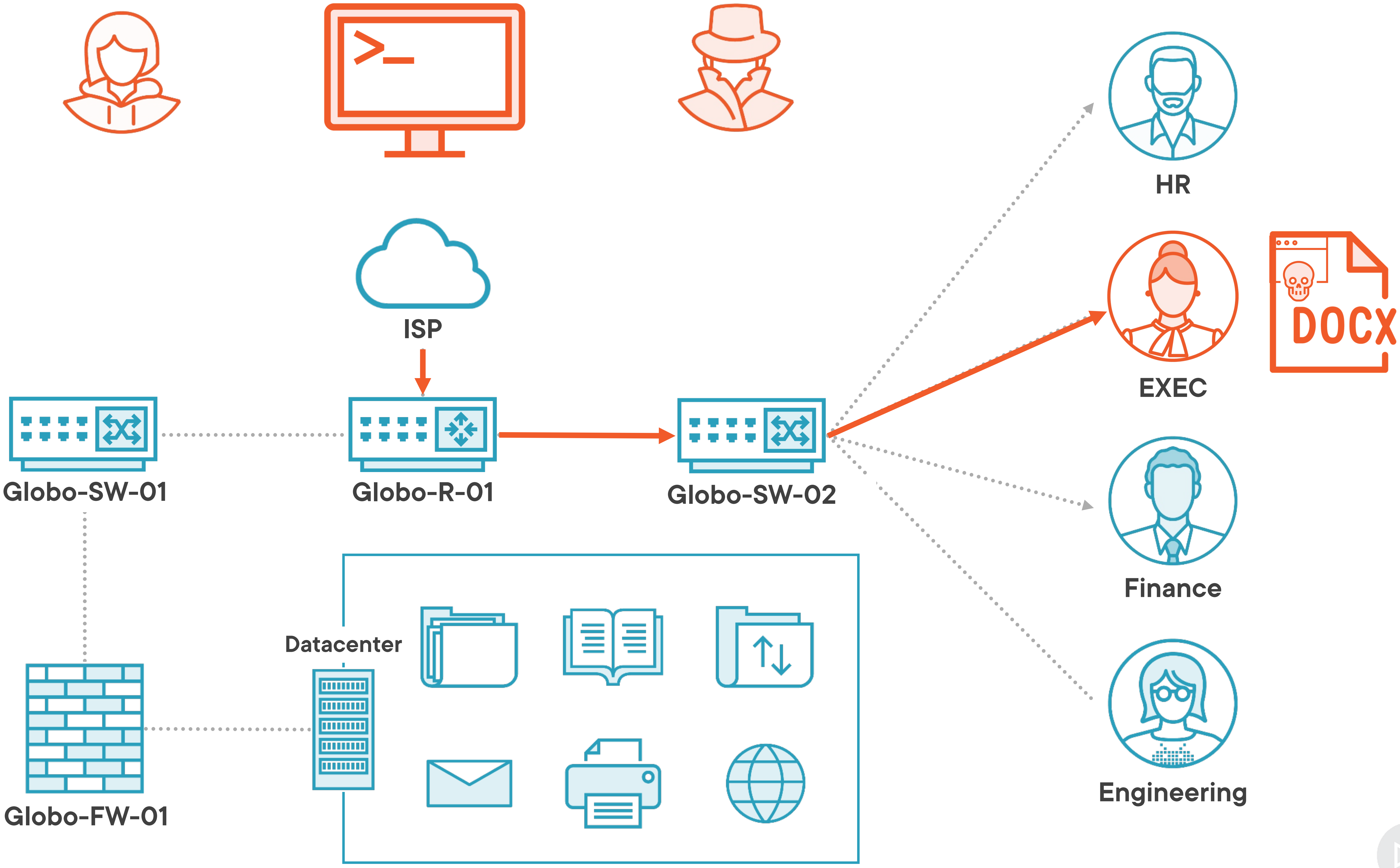
- Initial Access
- **Execution**
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact

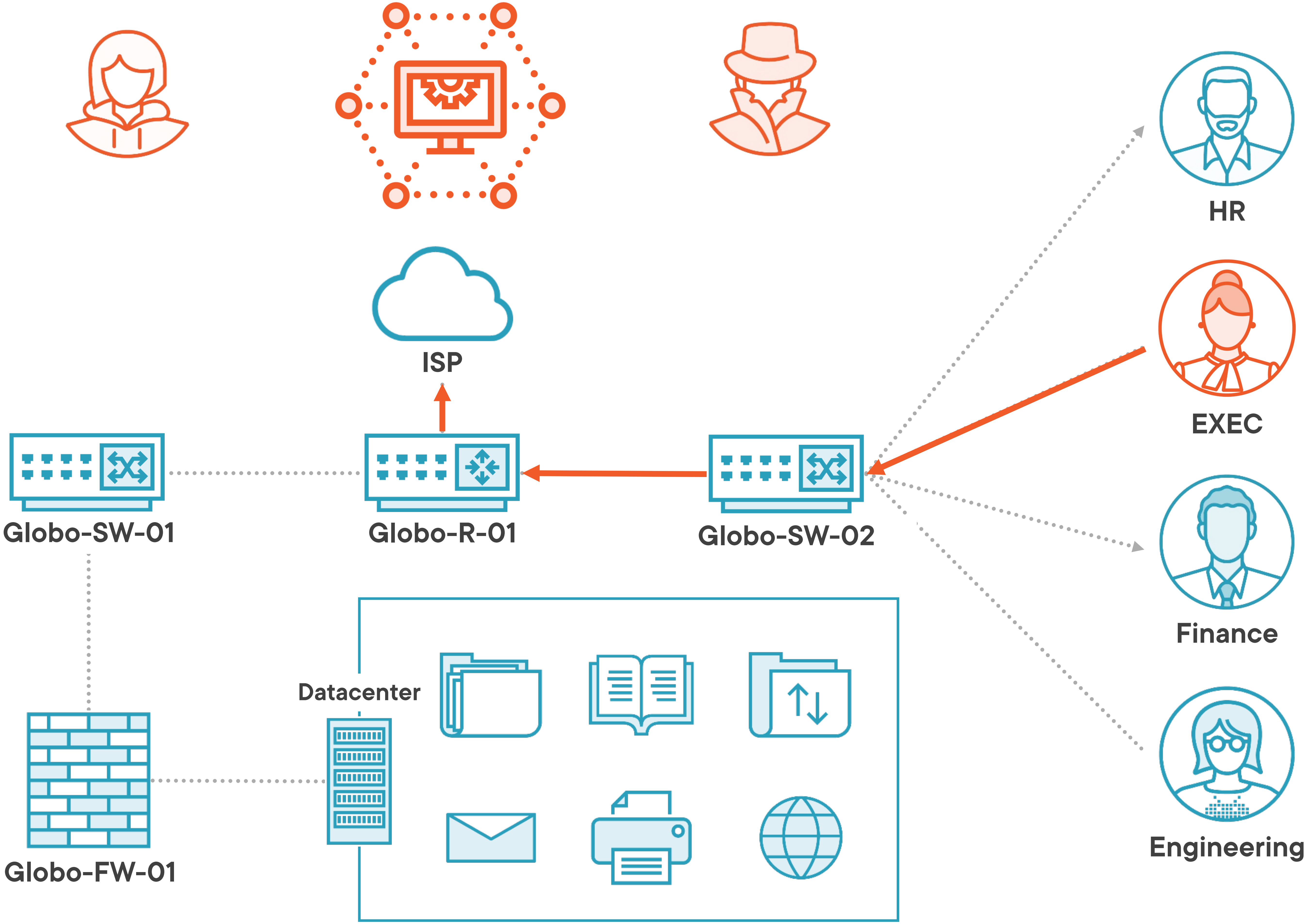
T1059.001:
Command and Scripting Interpreter: PowerShell

T1203:
Exploitation for Client Execution


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


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


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


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

Demo

PowerShell Attacks with Unicorn

- Lab environment
- Exploring Unicorn’s options
- Explore additional built-in tools

Demo

Creating payloads for client execution

- Generate PowerShell command
- Create multiple payloads using Unicorn

Using these features allows you to easily create multiple attacks for execution.

Demo

Execute payloads on a remote host

- Execute the attacks we generated in the previous demo
- Observe the results in our lab

Executing the payloads allows us to test our Unicorn commands on a target.

Demo

Creating payloads with custom shellcode

- Generate shellcode outside of Unicorn
- Reformat for use with Unicorn
- Generate a payload with shellcode
- Test the attack on a remote host

Using these features allows you to incorporate your own Shellcode into these attacks with Unicorn.