Command and Control with Covenant

Aaron Rosenmund

AUTHOR EVANGELIST – INCIDENT RESPONSE

@arosenmund   www.aaronrosenmund.com

#
COVENANT

COVENANT

Creator: Ryan Cobb

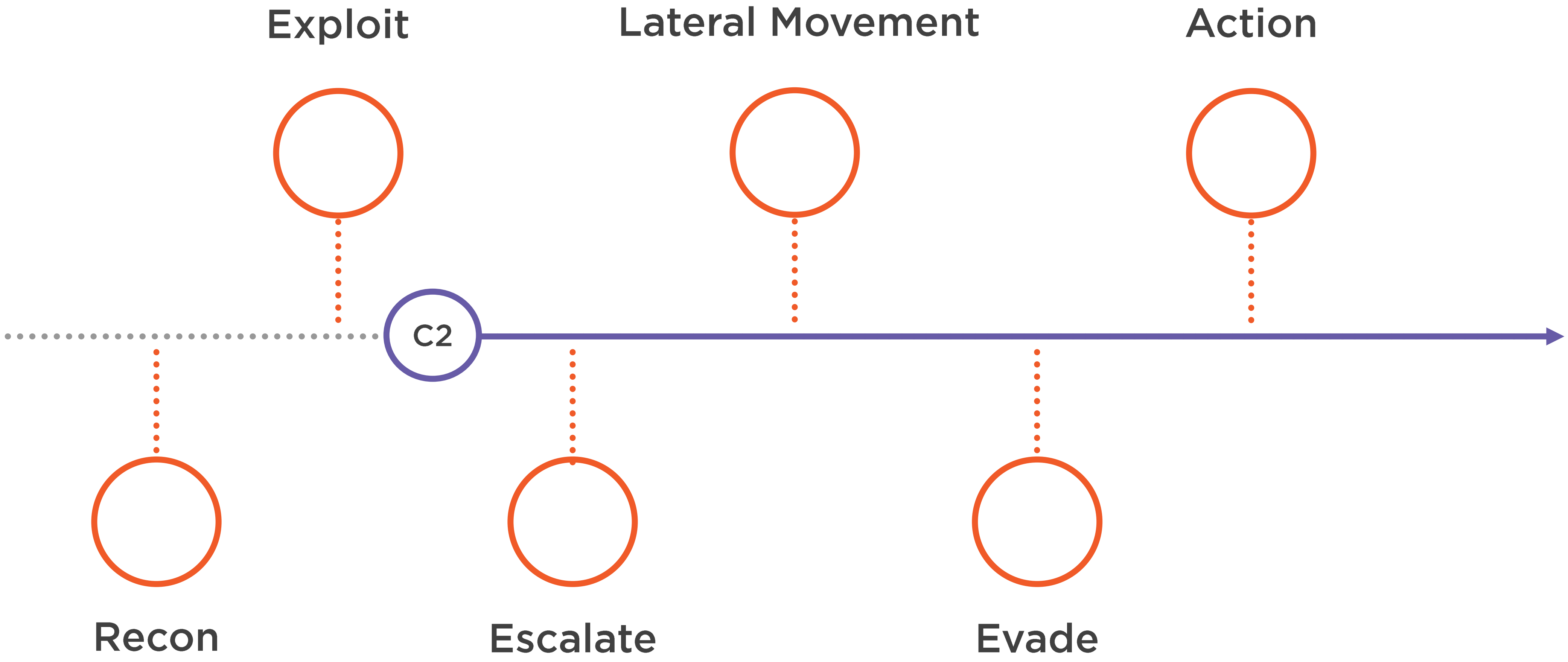
For use in adversary emulation of collaborative command and control. An evolution away from burned PowerShell based capabilities that highlights the attack surface of .NET

Open source red team operations C2 framework written in C#

Available at github.com/cobbr/Covenant for download and compilation with dotnet core across platforms

Cross platform compatible and uses Roslyn API for dynamic compilating of implants

Kill Chain

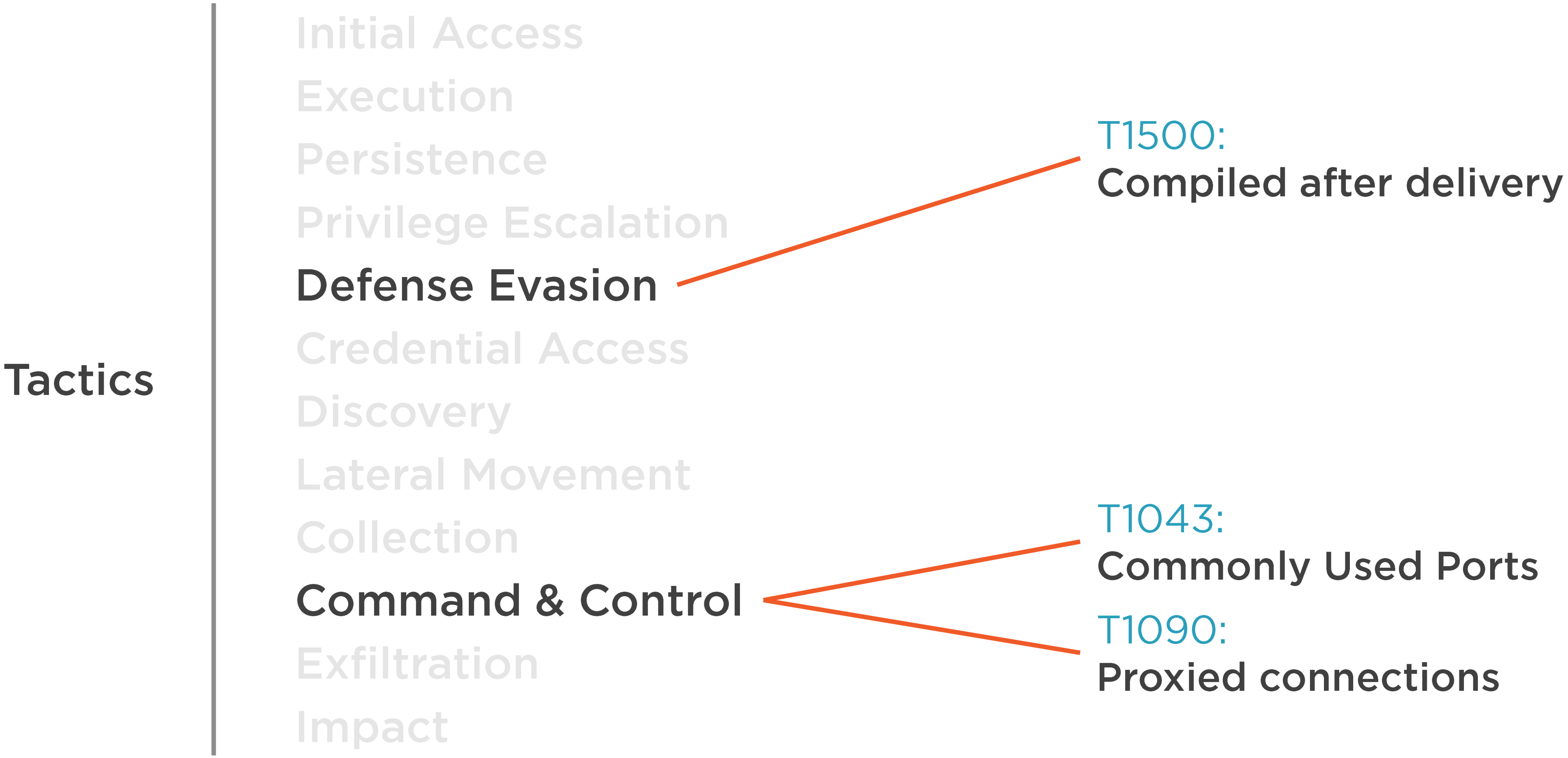


MITRE ATT&CK

Tactics

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

MITRE ATT&CK



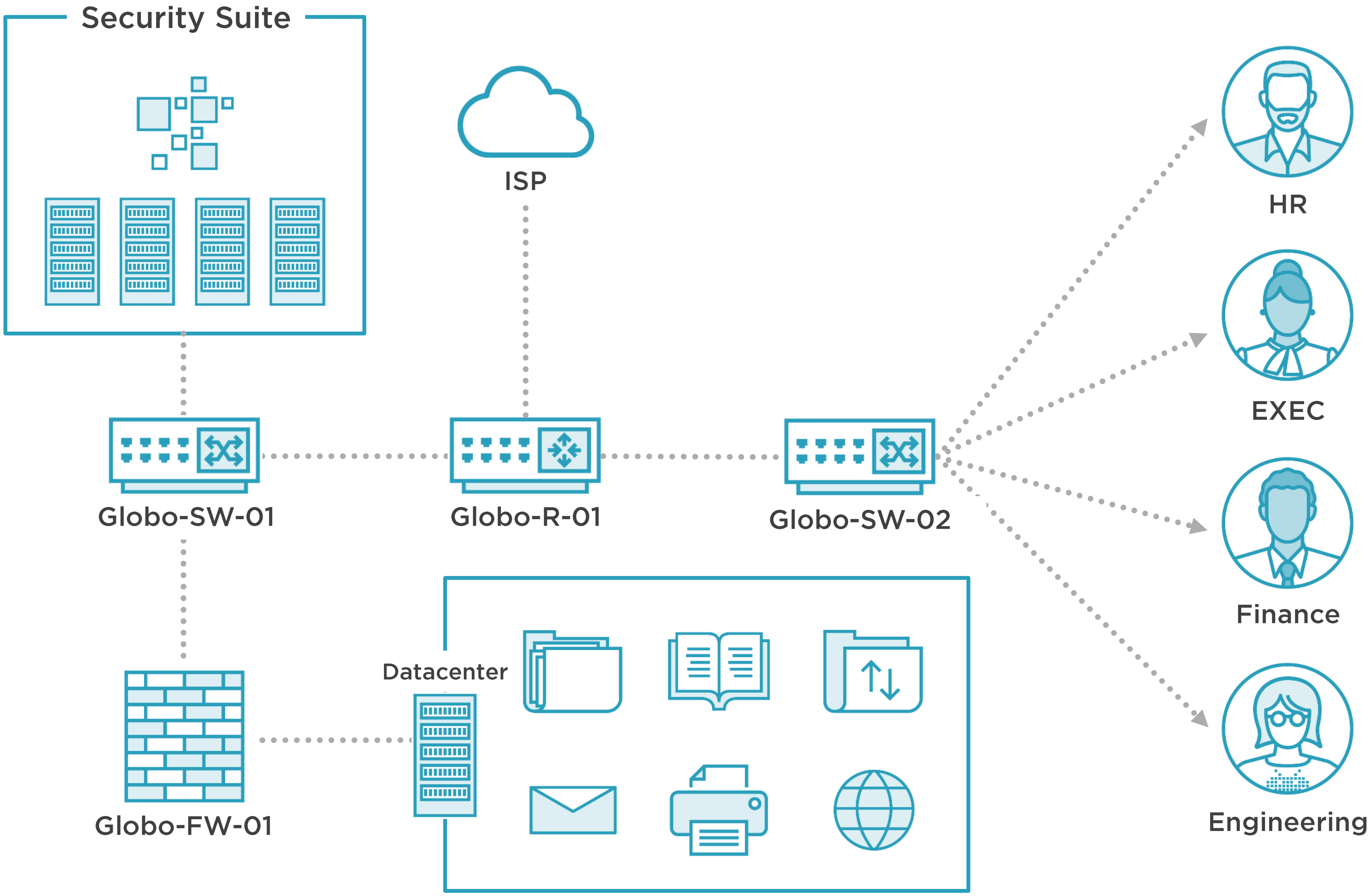
Tactics

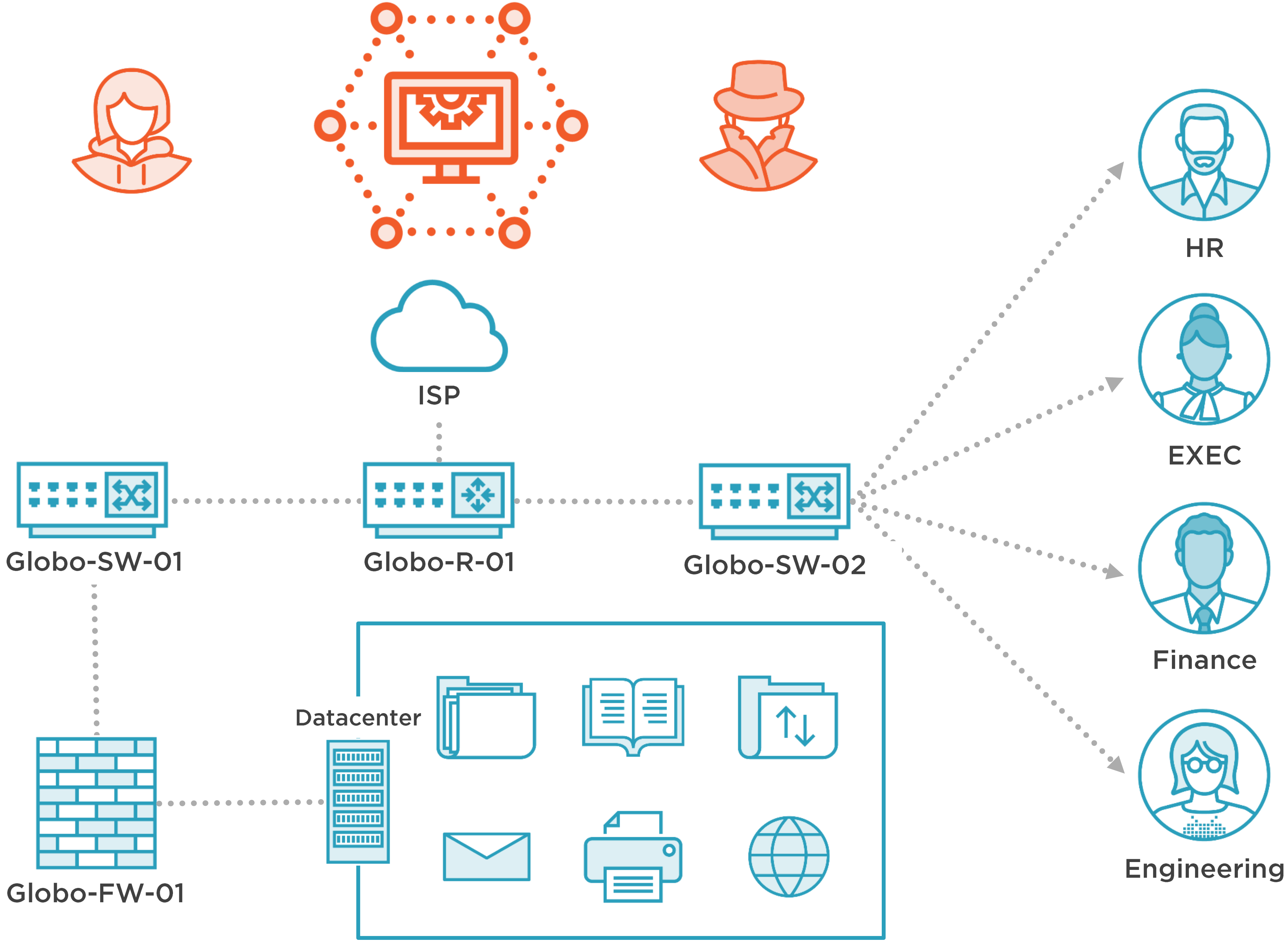
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- **Defense Evasion**
- Credential Access
- Discovery
- Lateral Movement
- Collection
- **Command & Control**
- Exfiltration
- Impact

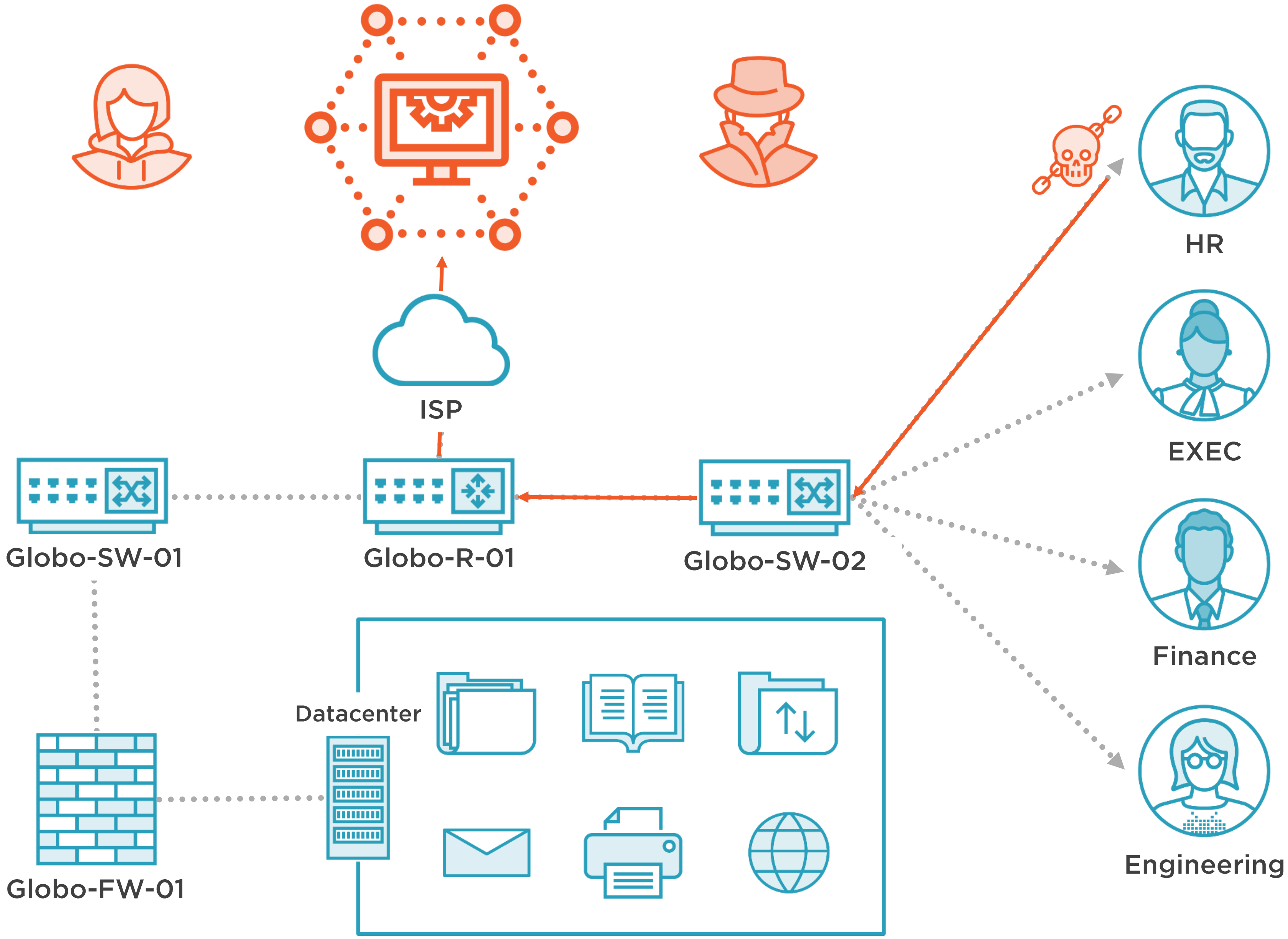
T1500:
Compiled after delivery

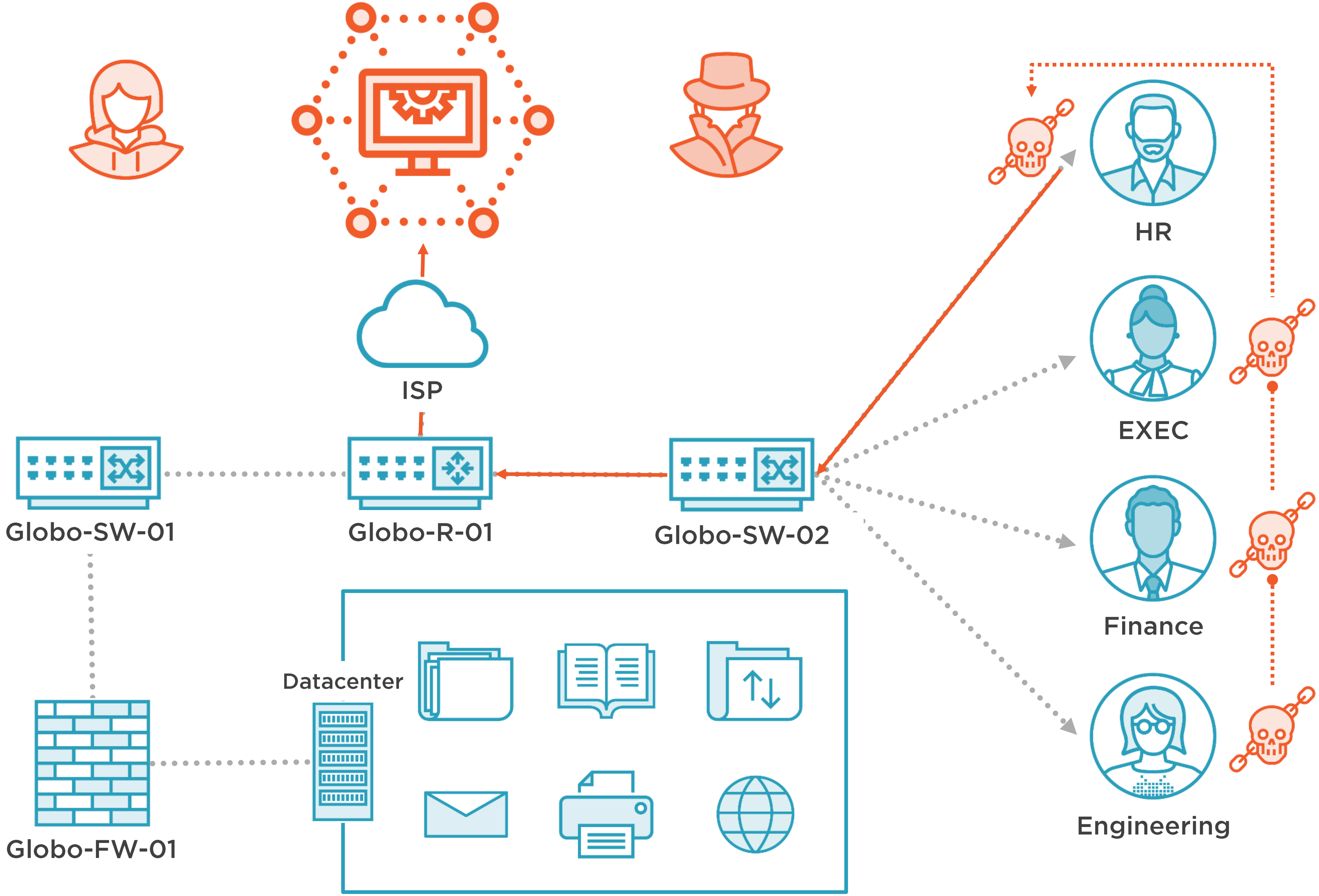
T1043:
Commonly Used Ports

T1090:
Proxied connections


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


HR
ISP
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
HR
EXEC
Finance
Engineering
Datacenter
Globo-FW-01


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

Demo Place Holder

Demo:

Installing & Logging In - 3 min

- DOTNET Core - MacOSx, Linux, Windows
- We are using docker that is how it is intended
- Login create a user name

More Information

Know thy self, know thy enemy. ~ Sun Tzu

Covenant Capabilities

Listener Profiles

https://github.com/cobbr/Covenant/wiki/Listener-Profiles

API Usage

https://github.com/cobbr/Covenant/wiki/Using-The-API

Command and Control

C2-Next Generation

https://blog.stealthbits.com/next-gen-open-source-c2-frameworks/

Types of C2 Channels

- DNS
- HTTPS
- Custom