

Command and Control with Pupy



Matt Glass

CISSP, CEH

[linkedin.com/in/matthewglass2/](https://www.linkedin.com/in/matthewglass2/)



Pupy

Creator: Nicolas Verdier
(@n1nj4sec)

Pupy is an open source remote administration and post exploitation tool written in python. Pupy executes in memory, allowing it to leave a low footprint. Pupy also offers multiple communications channel options to mask traffic.



Pupy

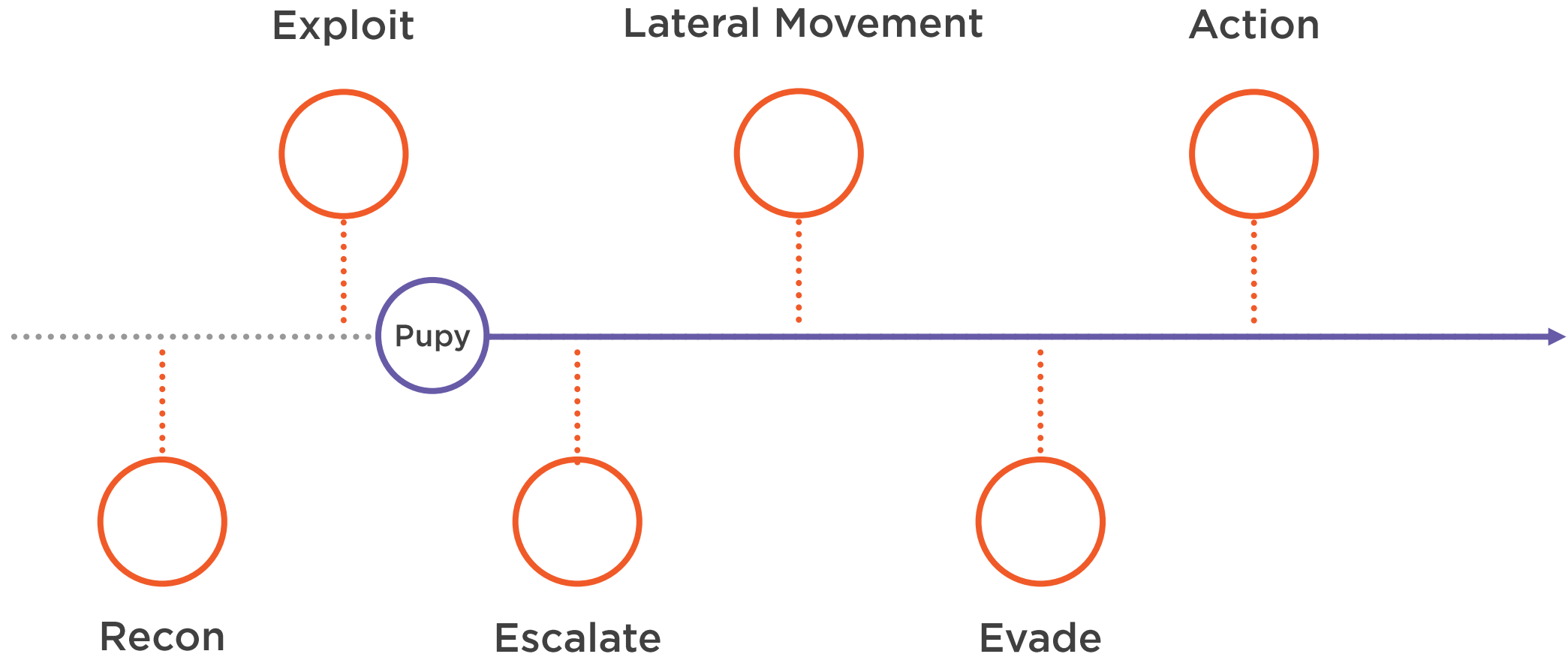
Post exploitation tool to manage exploited clients from a central server

Open source project, can be downloaded from their GitHub page

Pupy has multiple advantages, including a low footprint, multiple channel encryption options, and built-in privilege escalation options



Kill Chain



MITRE ATT&CK and Pupy



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

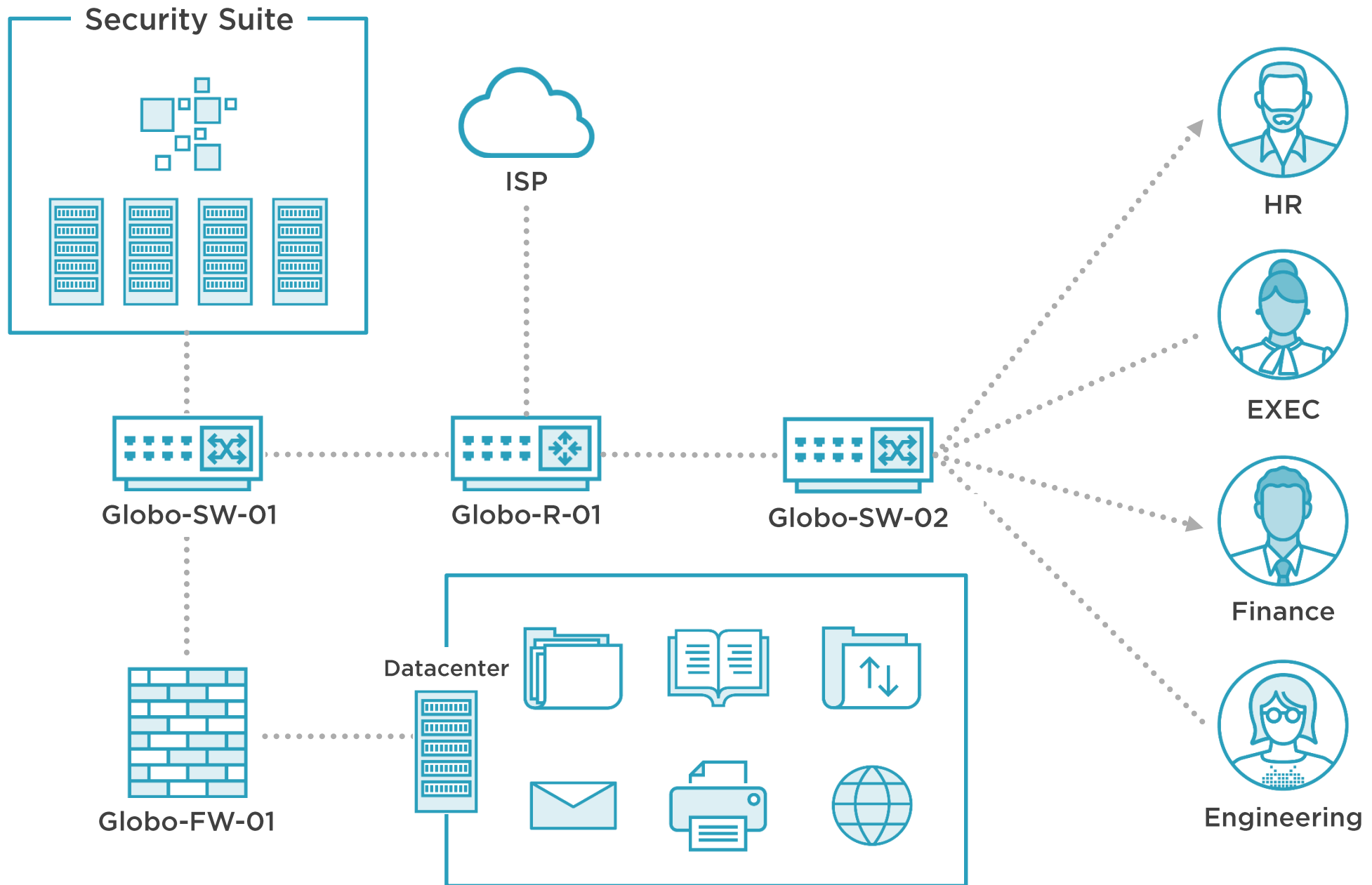
Impact

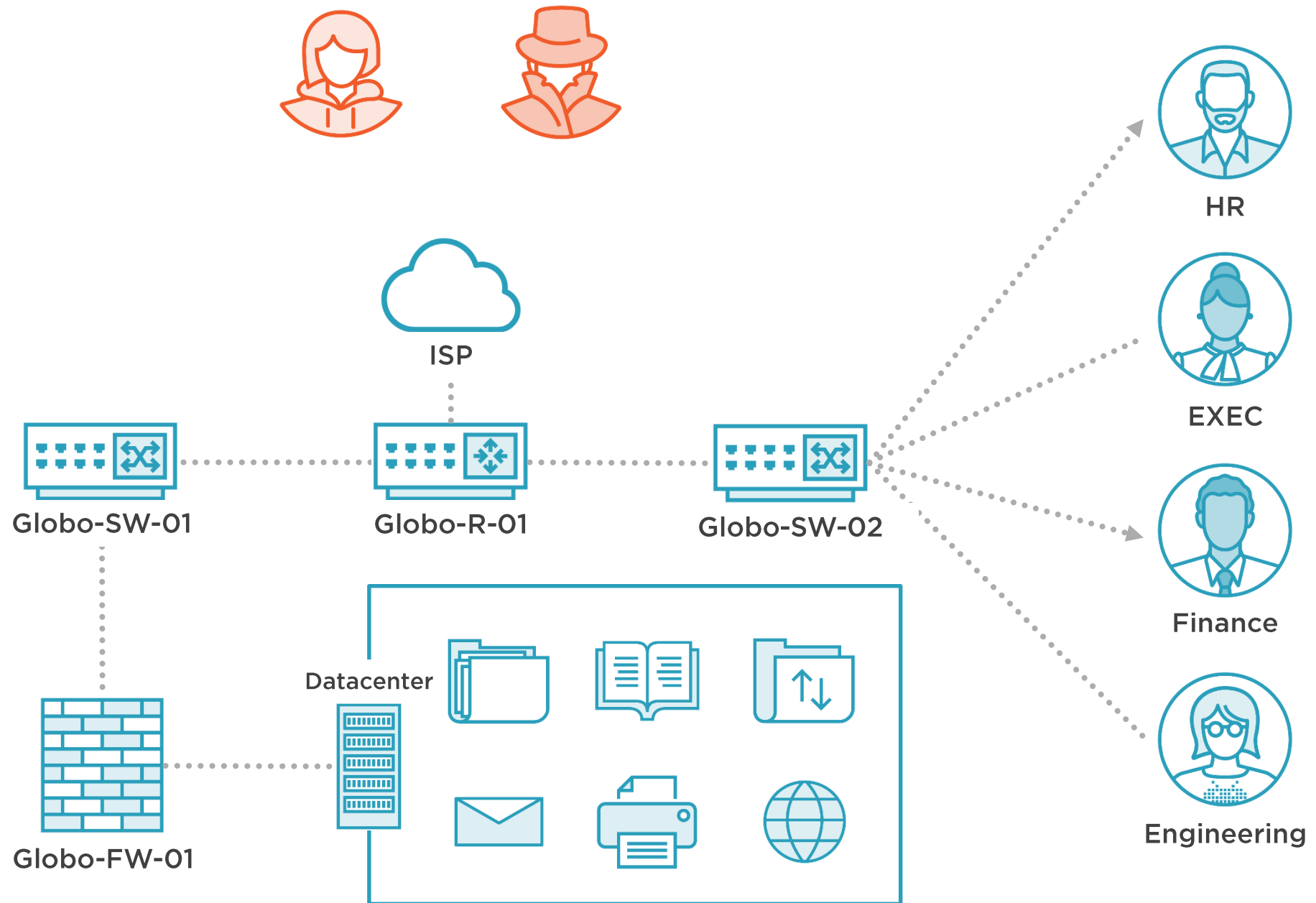
T1003:
Credential Dumping

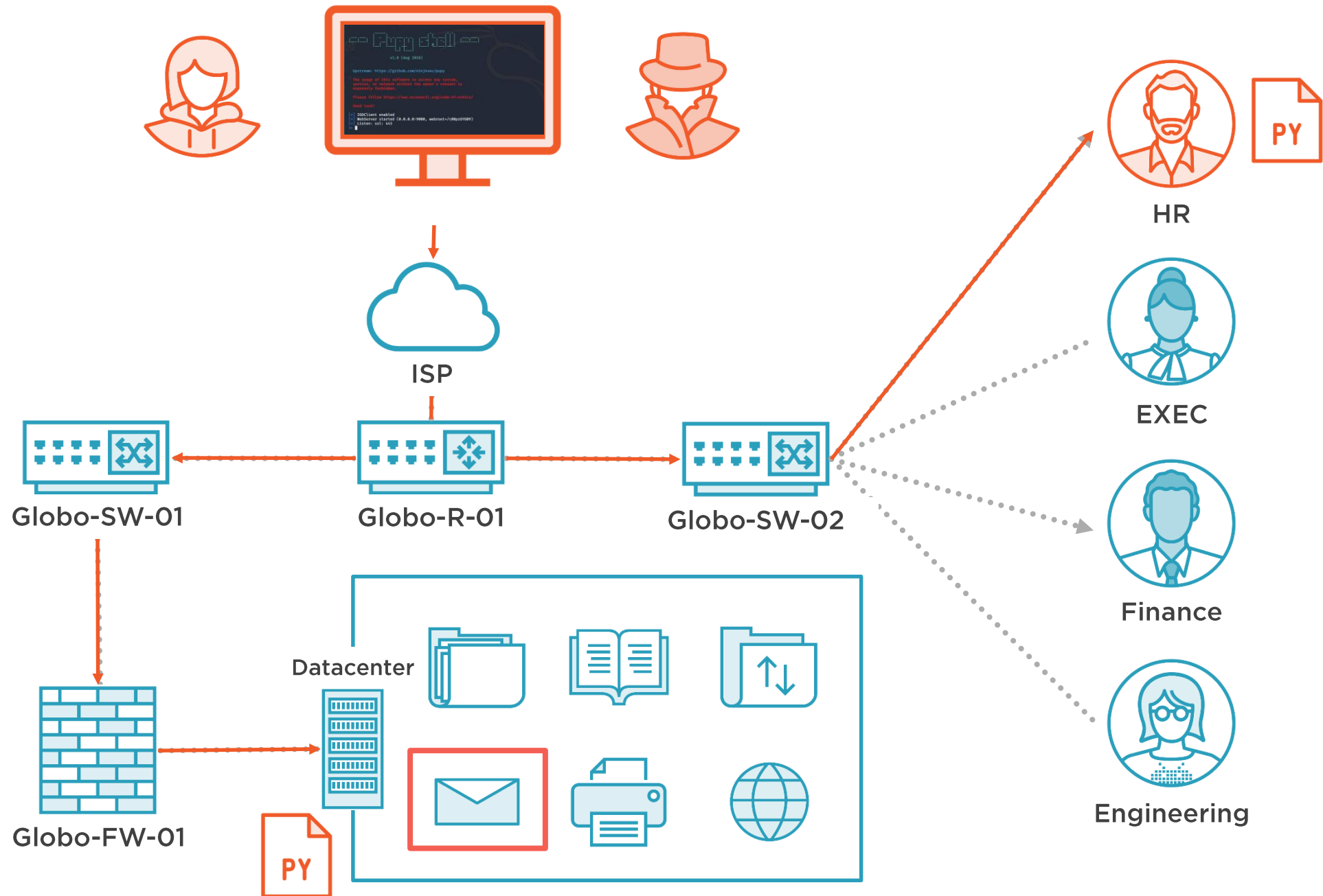
T1056:
Input Capture

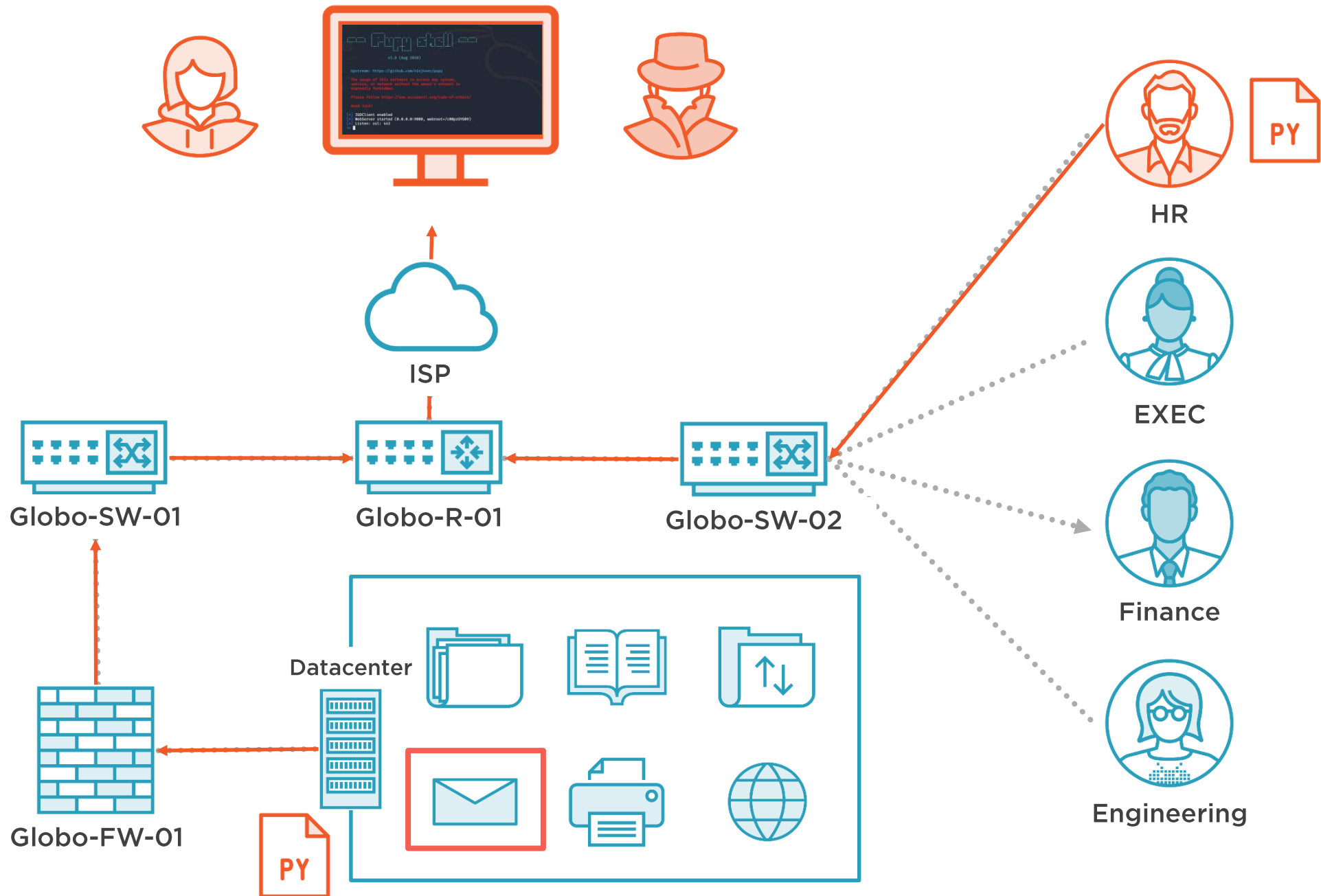
T1032:
Standard Cryptographic
Protocol

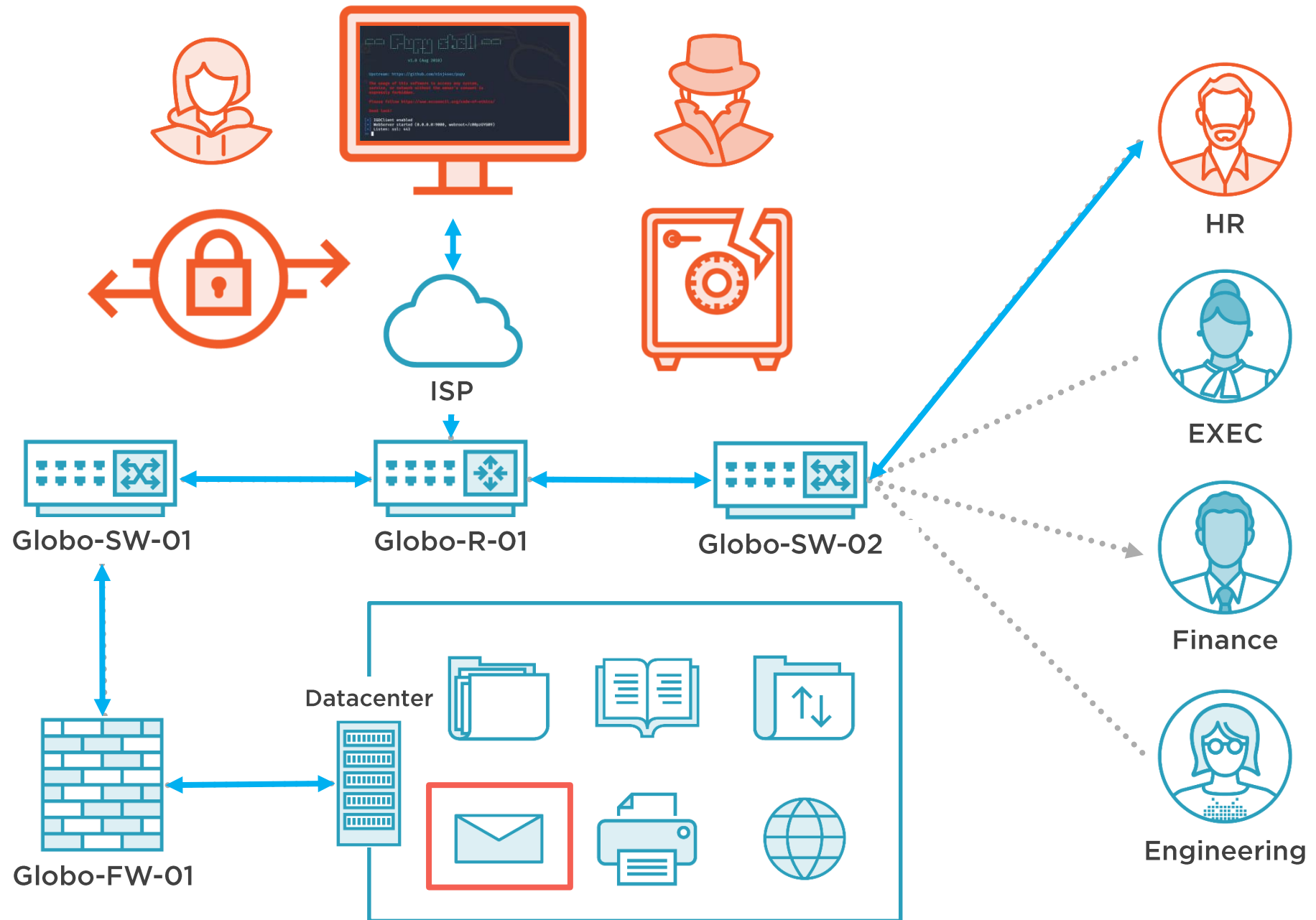












Demo



Starting the Pupy server and navigating through options

- Start Pupy on the “hacking” workstation
- Explore options in Pupy and navigate its interface



Demo



Configuring transport options and establishing multiple client sessions

- Configure transport encryption options in Pupy to mask traffic
- Start clients on multiple target machines to establish sessions with the Pupy server

Using these features will allow you to establish sessions with clients

The transport options allow you to mask traffic and make it appear legitimate



Demo



Discovering credentials and escalating privileges with Pupy

- Utilize tools within Pupy to discover credentials on target machines
- Utilize tools within Pupy to escalate privileges to administrator or SYSTEM permissions on targets

Using these tools will allow you to spoof credentials or act as an administrator



Demo



Capturing user input

- Utilize tools within Pupy to capture input from a user operating the target machine
- Transfer the captured input to the Pupy server

Using these tools enables a hacker to capture screenshots, keystrokes, mouse clicks, audio, and even video

