Lateral Movement: WMIOps

Matt Glass
CISSP, CEH

linkedin.com/in/matthewglass2/

WMIOps

WMIOps

Creator: Chris Truncer

WMIOps is a PowerShell script that leverages the capabilities of WMI to perform actions on Windows hosts, either local or remote.

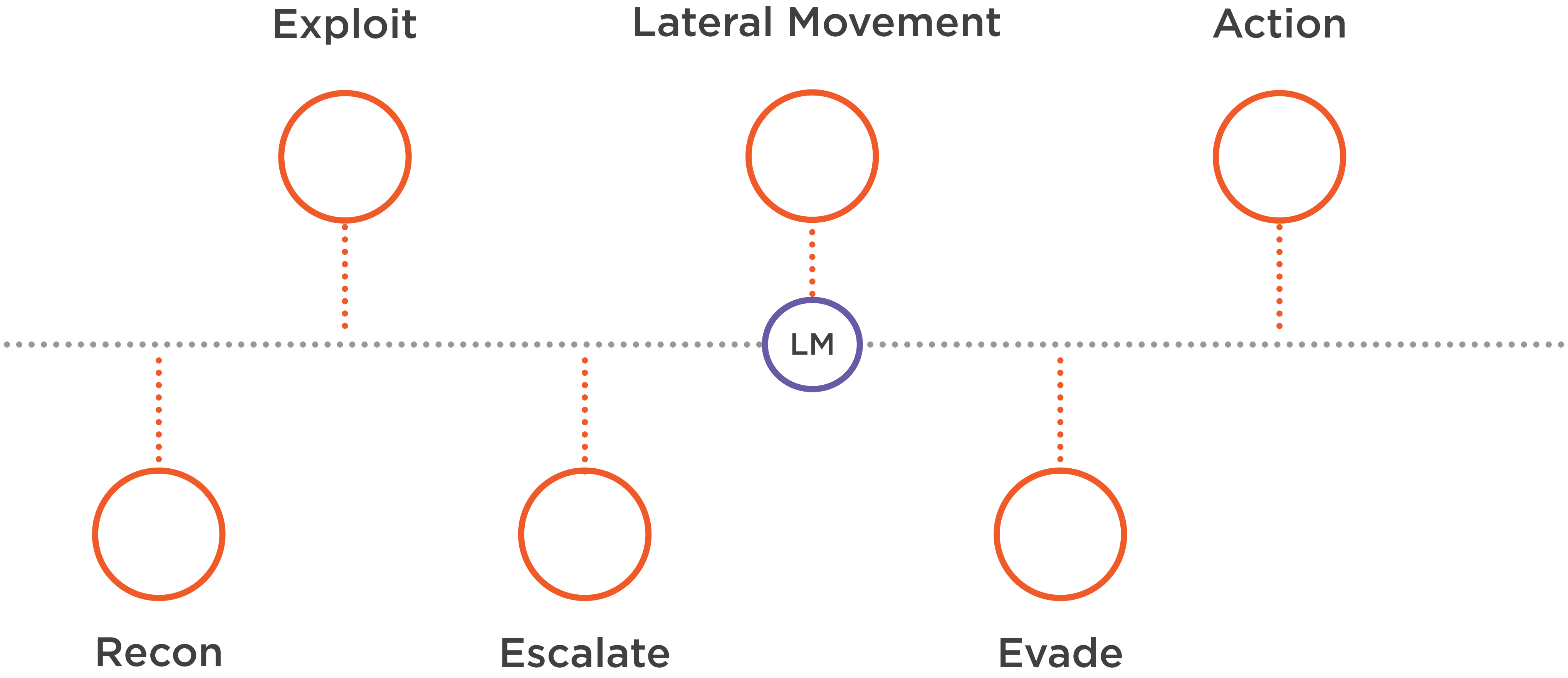
WMIOps

WMIOps is a PowerShell script that performs actions on Windows hosts

You can download it from GitHub

WMIOps allows you to execute PowerShell commands on other Windows hosts from an exploited machine.

Kill Chain

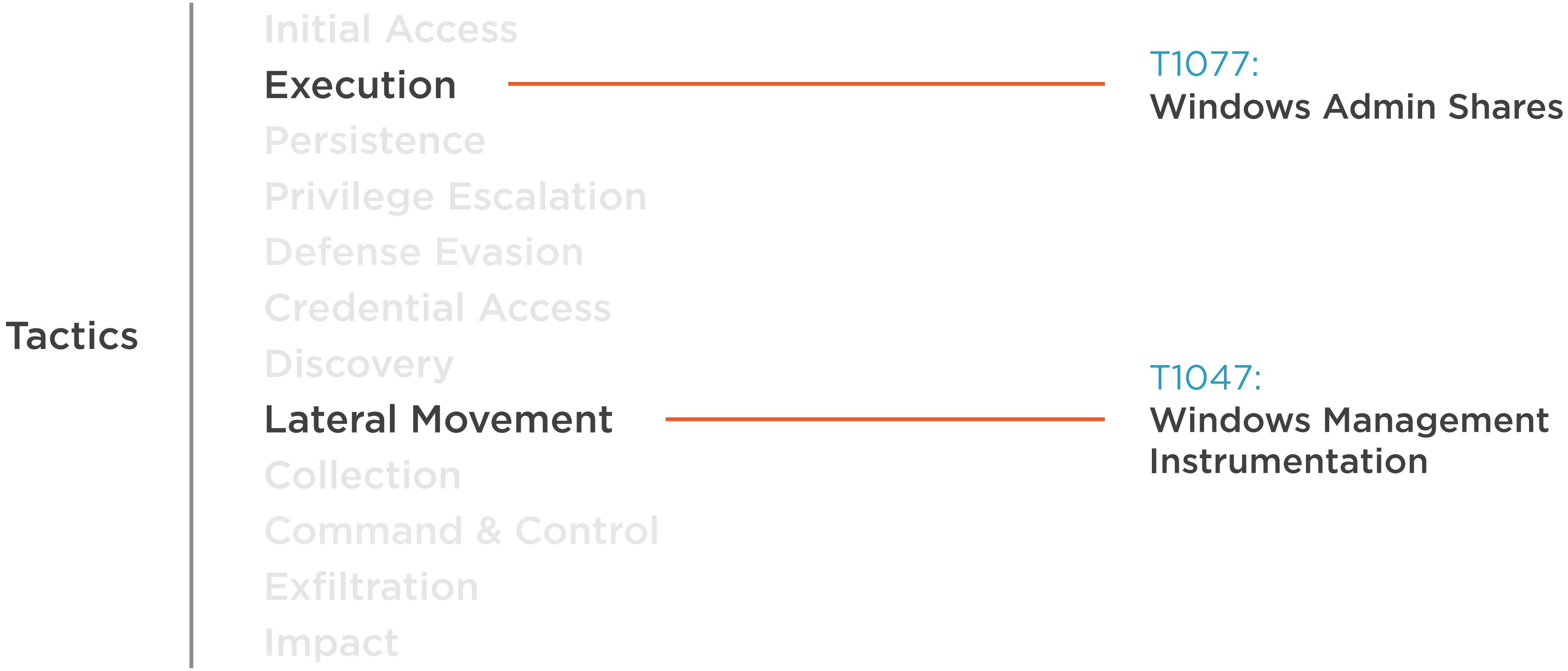


MITRE ATT&CK

Tactics

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

MITRE ATT&CK

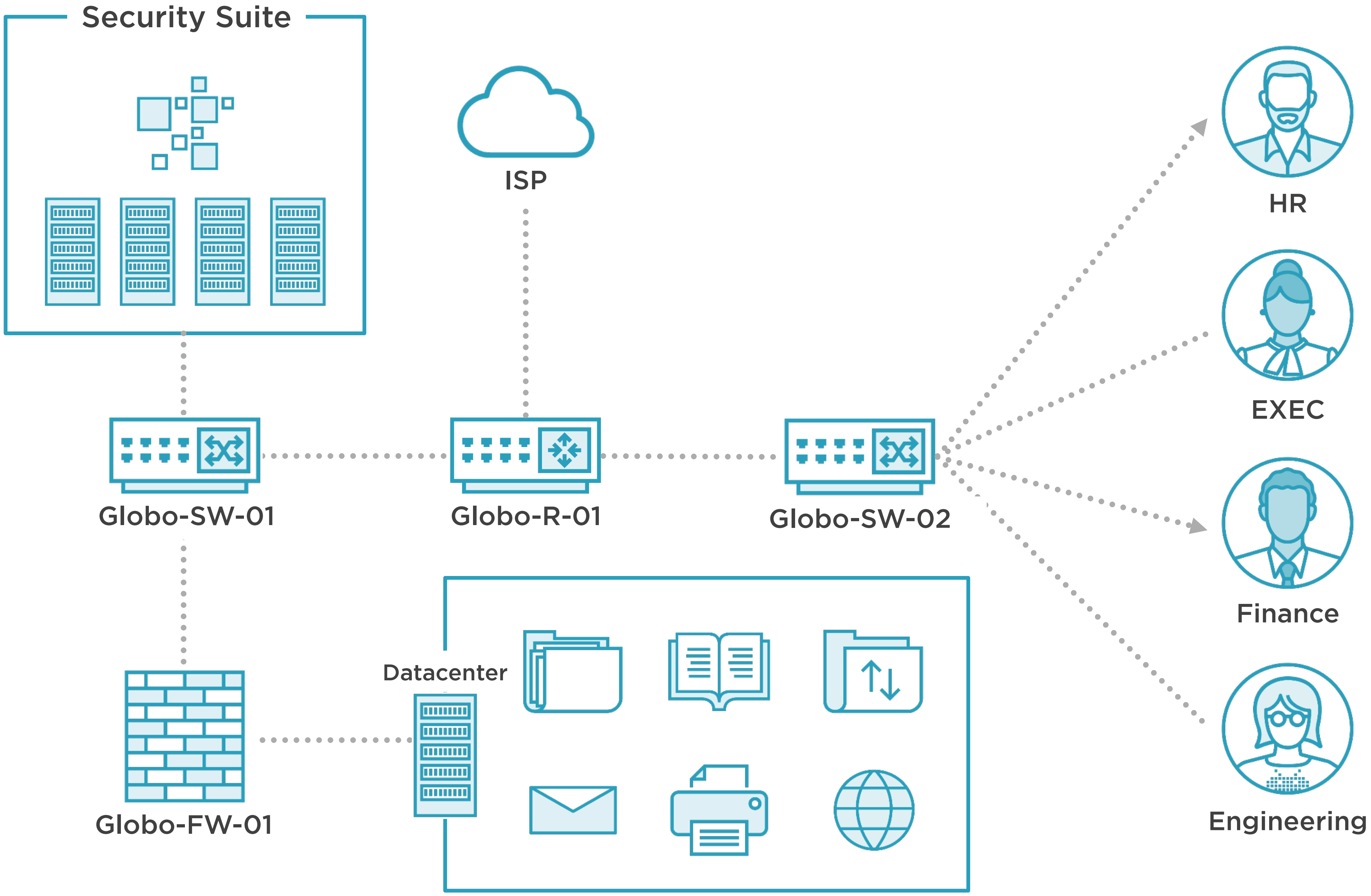


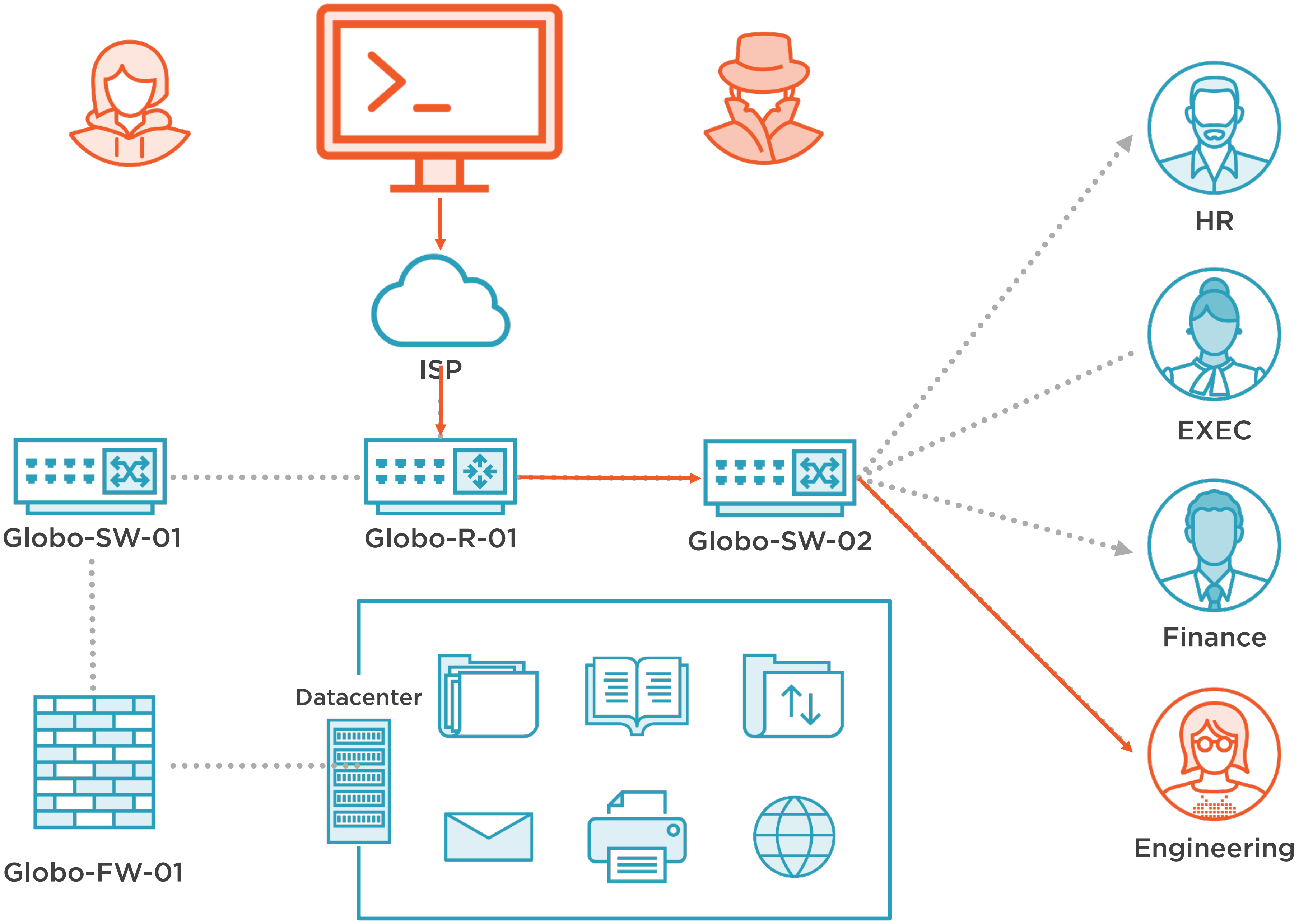
Tactics

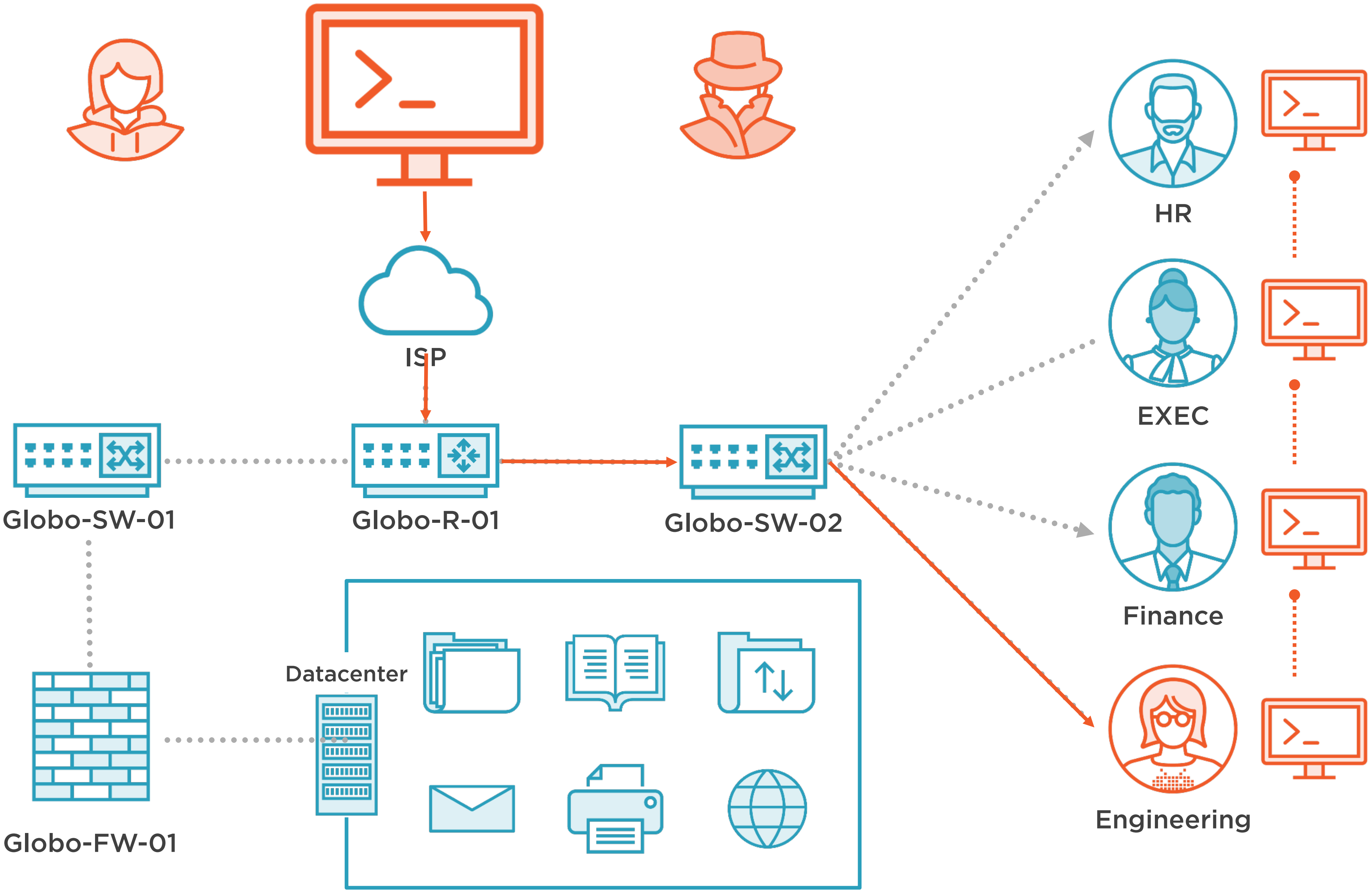
- Initial Access
- **Execution**
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- **Lateral Movement**
- Collection
- Command & Control
- Exfiltration
- Impact

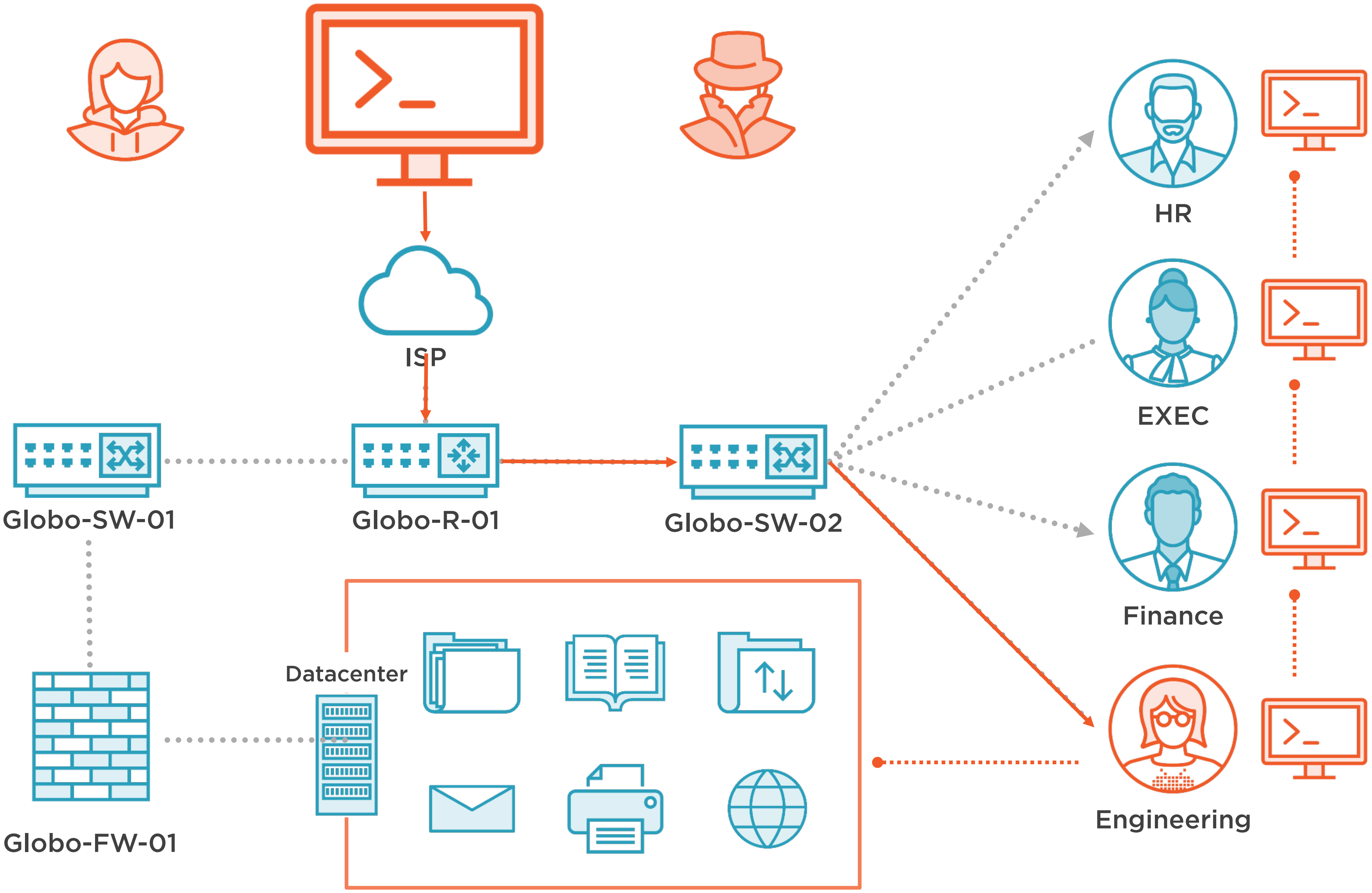
T1077:
Windows Admin Shares

T1047:
Windows Management Instrumentation


Security Suite
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
HR
EXEC
Finance
Engineering
Datacenter
Globo-FW-01


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


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

Demo

Getting started with WMIOps

- Obtain the WMIOps scripts and place them on an exploited machine
- Explore the available options

Demo

Use WMIOps to execute PowerShell commands on other Windows machines

- Use WMIOps commands to execute PowerShell commands
- Use WMIOps to manipulate services and scheduled jobs remotely

Using these features will allow you to run commands on remote workstations

Demo

Use WMIOps to gather information from remote Windows hosts

- Use WMIOps commands to gather system information
- Use WMIOps to create a share and move files between systems

WMIOps enables you to gather system information and move files between machines

Demo

Use WMIOps to run PowerShell scripts and manipulate services to laterally move through a network

- Use WMIOps to run PowerShell scripts remotely and access additional systems
- Use WMIOps PowerShell commands to enable remote PowerShell access

Using these techniques allows you to move laterally though a network

More Information

Know thy self, know thy enemy. ~ Sun Tzu

WMIOps uses and history

WMIOps usage

https://github.com/FortyNorthSecurity/WMIOps

WMIOps release blog post

https://www.christophertruncer.com/introducing-wmi-ops/

Lateral movement

MITRE ATT&CK lateral movement

https://attack.mitre.org/tactics/TA0008/

Other Windows tools for lateral movement

- Remote Desktop
- PsExec
- WinRM