

Red Team Tools to Emulate Adversary Techniques with MITRE ATT&CK

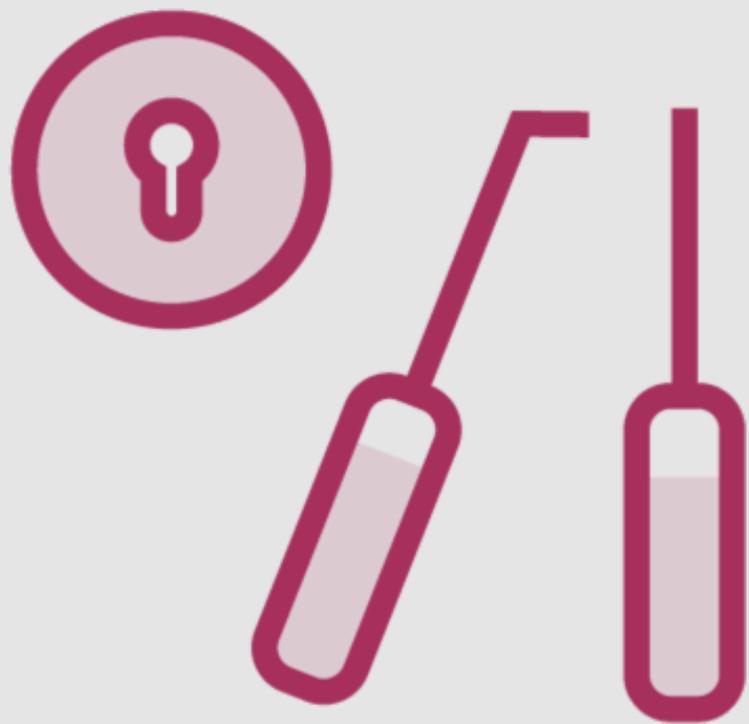


Aaron Rosenmund

AUTHOR EVANGELIST - INCIDENT RESPONSE

@arosenmund www.aaronrosenmund.com



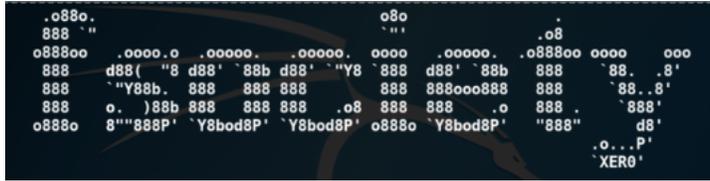


What are red team tools?

Who uses red team tools?

Who are you calling red team?





Creators of the Open Source & Free
Cyber Security Tools

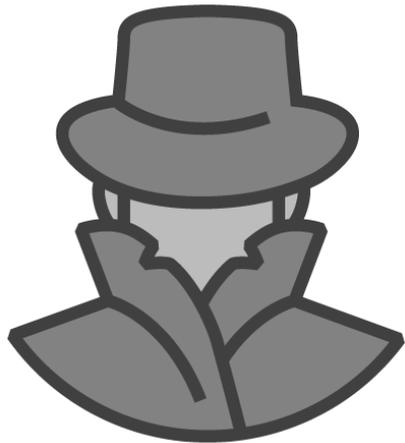
Thank You

You are leading the way in innovation fueled by
passion and everyone is benefiting.





Fremdlastung



Pen-testing vs Red Teaming

What is the difference?

Pentest

Tests all applications and services

Test against all things looking for any exploit

Provide a report but don't generally interact

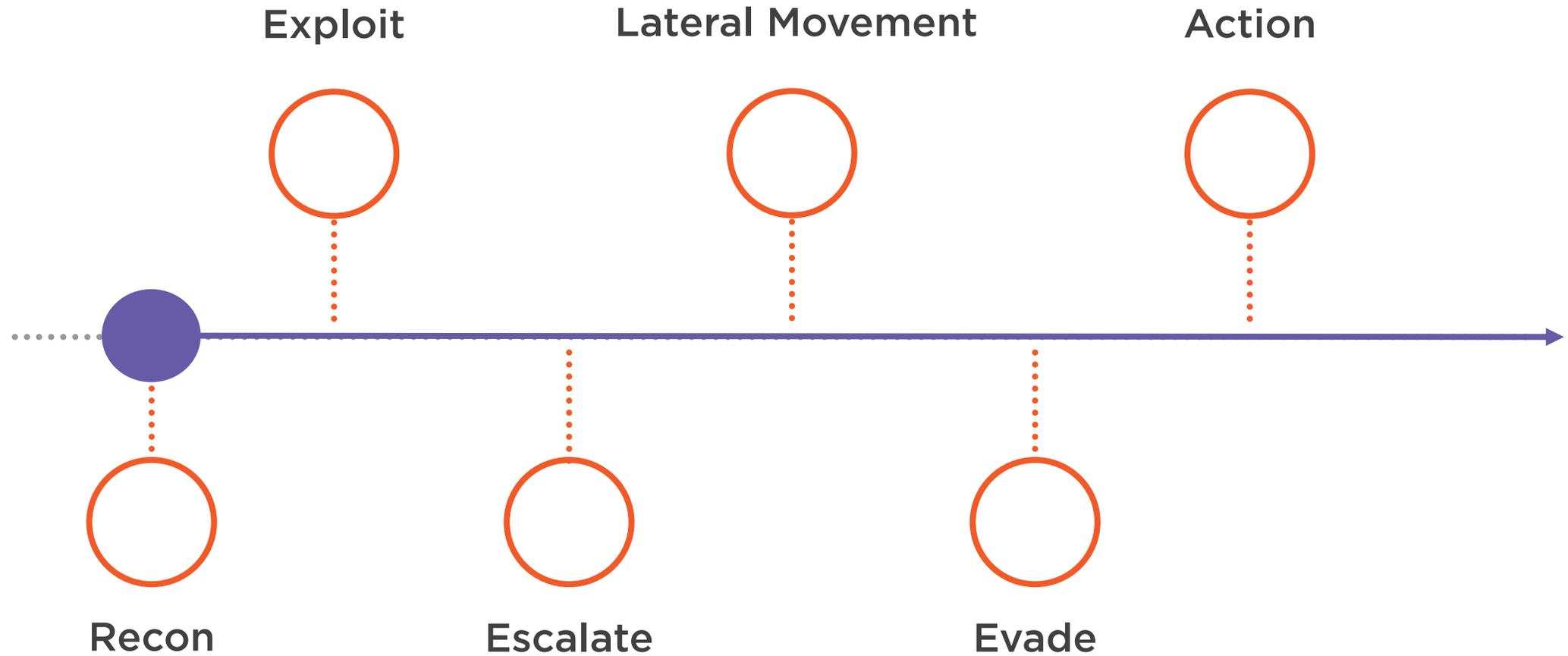
Red Team Operation

Emulates known adversary group behavior

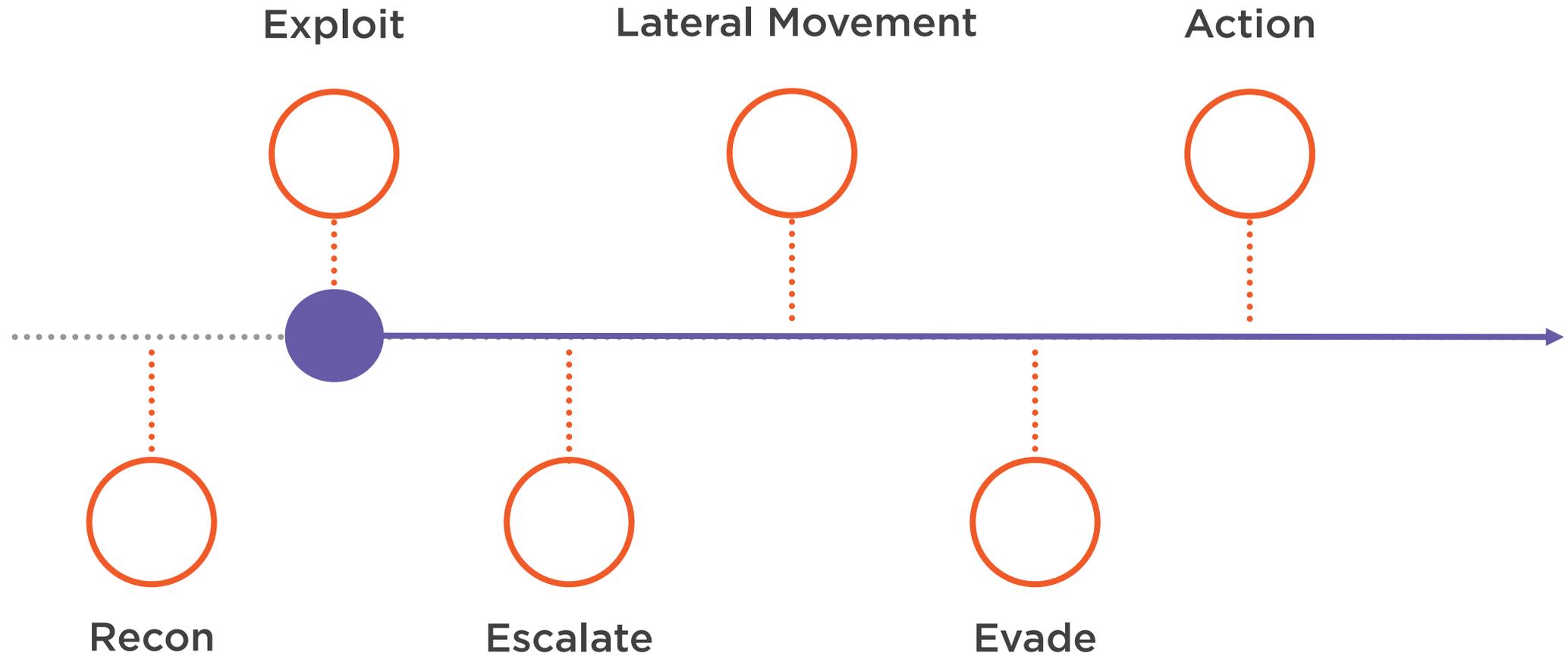
Replicate techniques over full attack lifecycle

Provide actionable results for detection

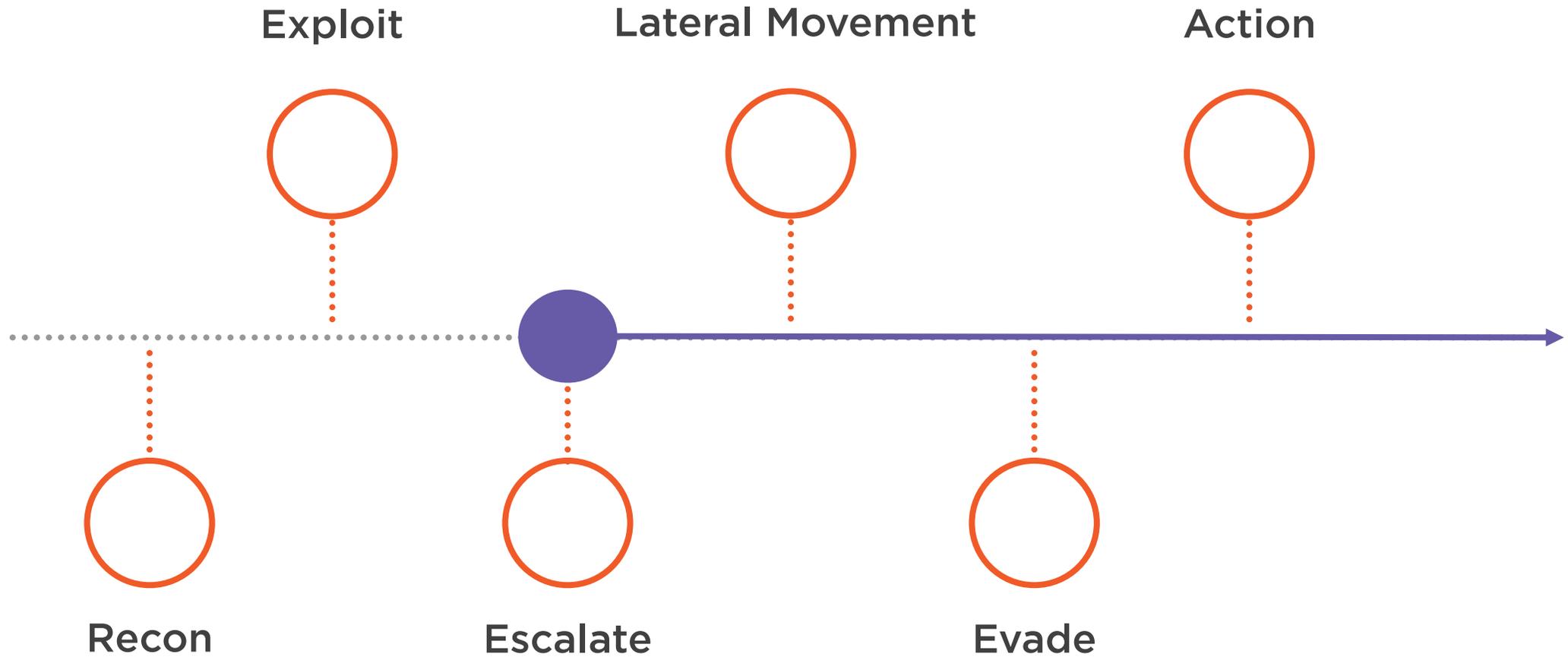
Kill Chain



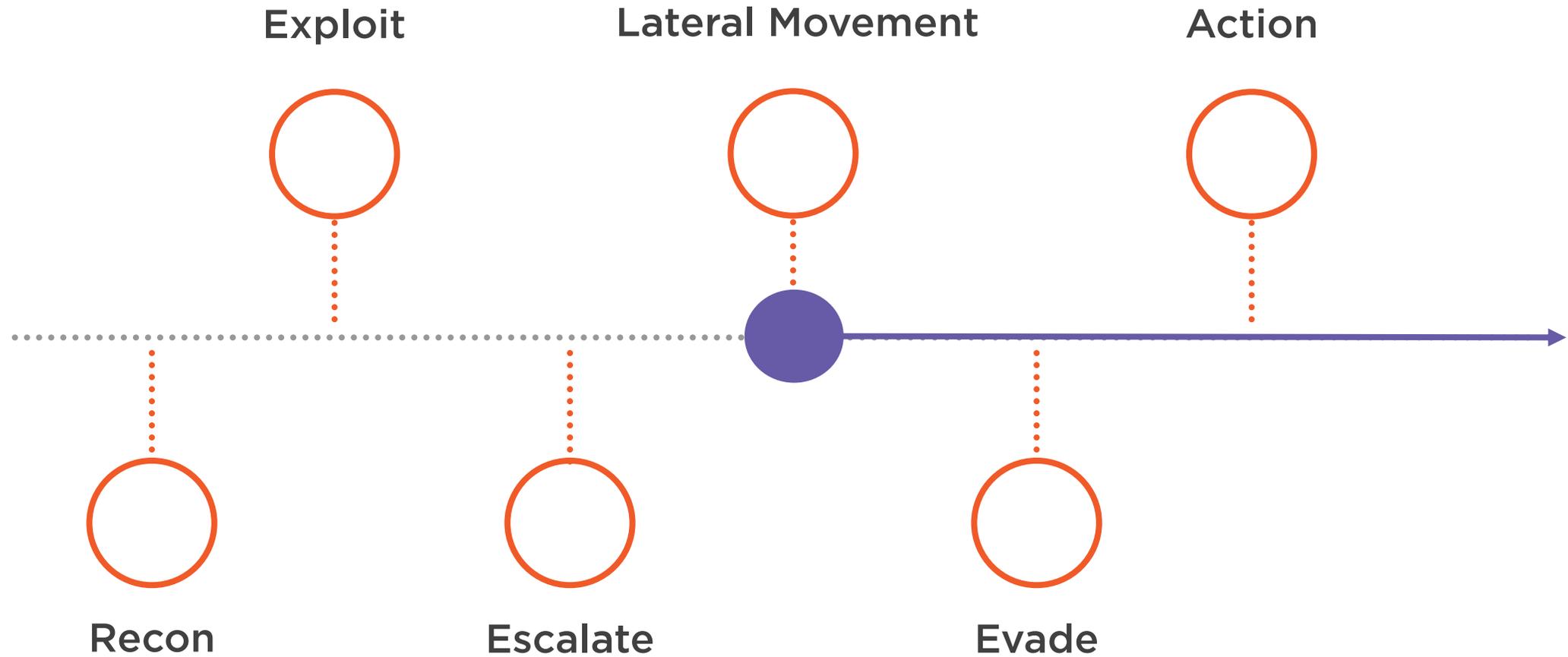
Kill Chain



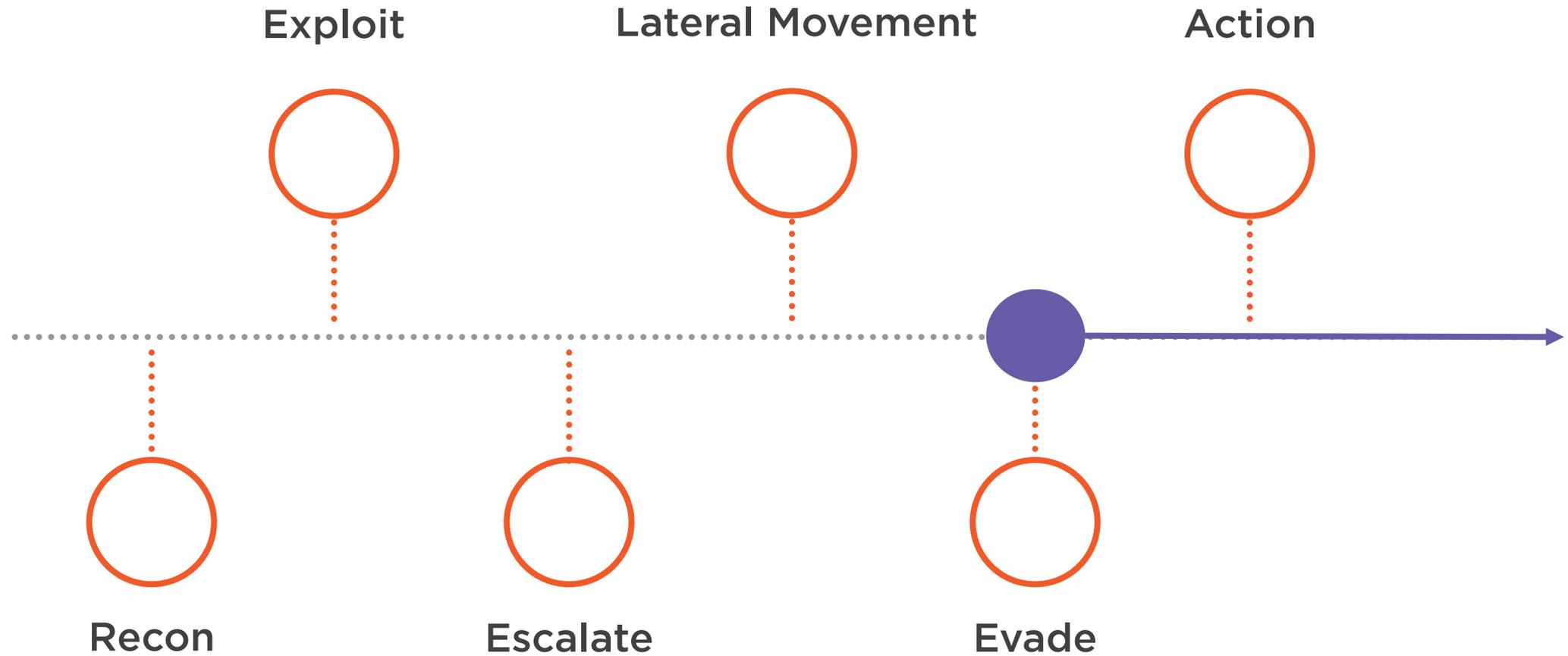
Kill Chain



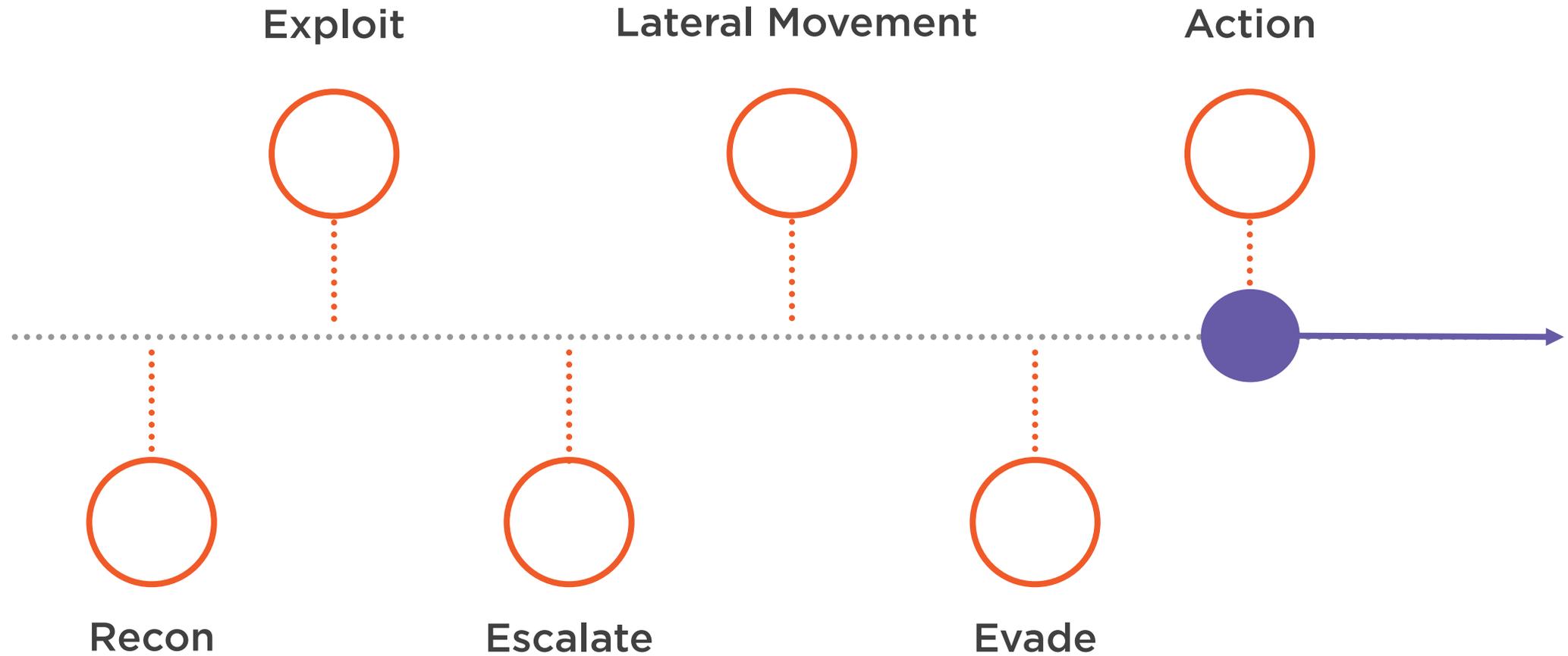
Kill Chain



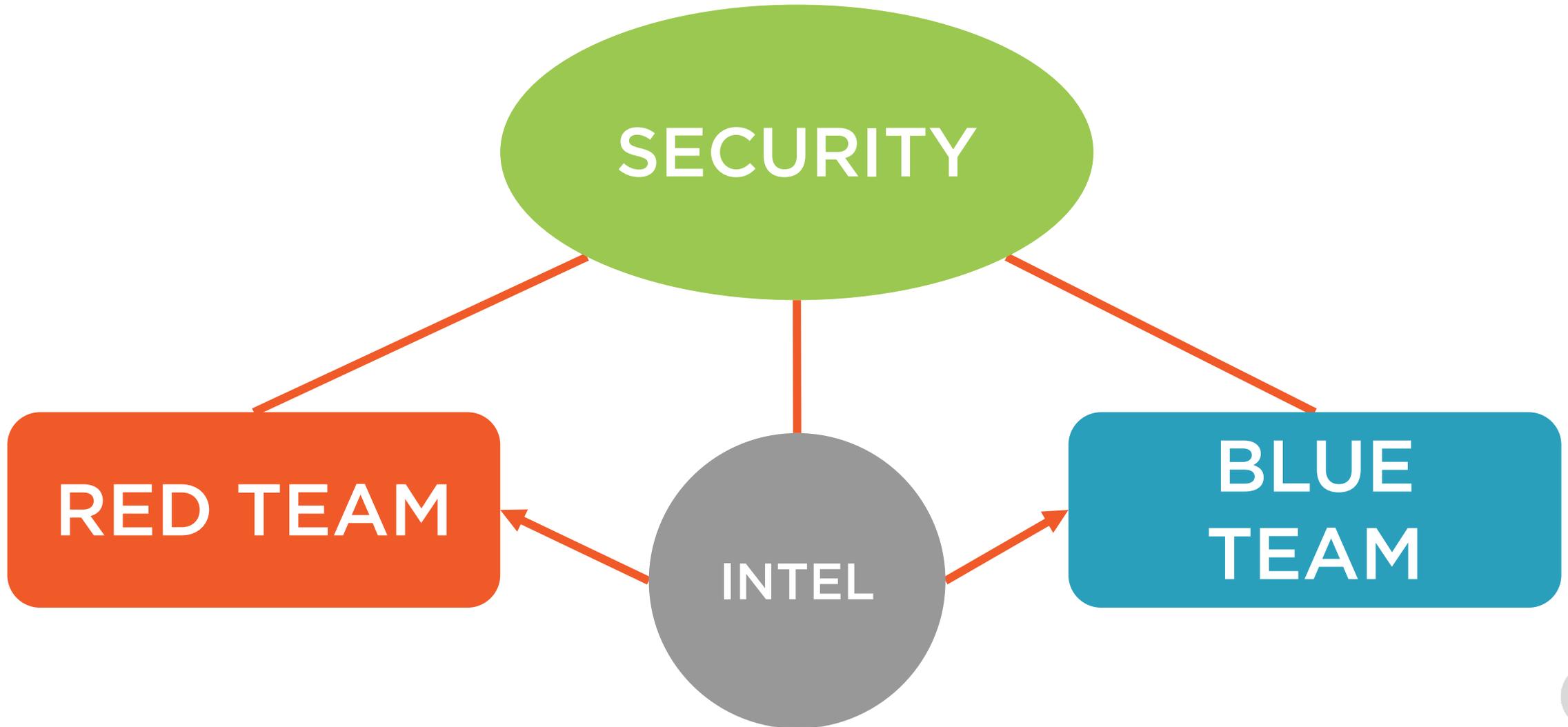
Kill Chain



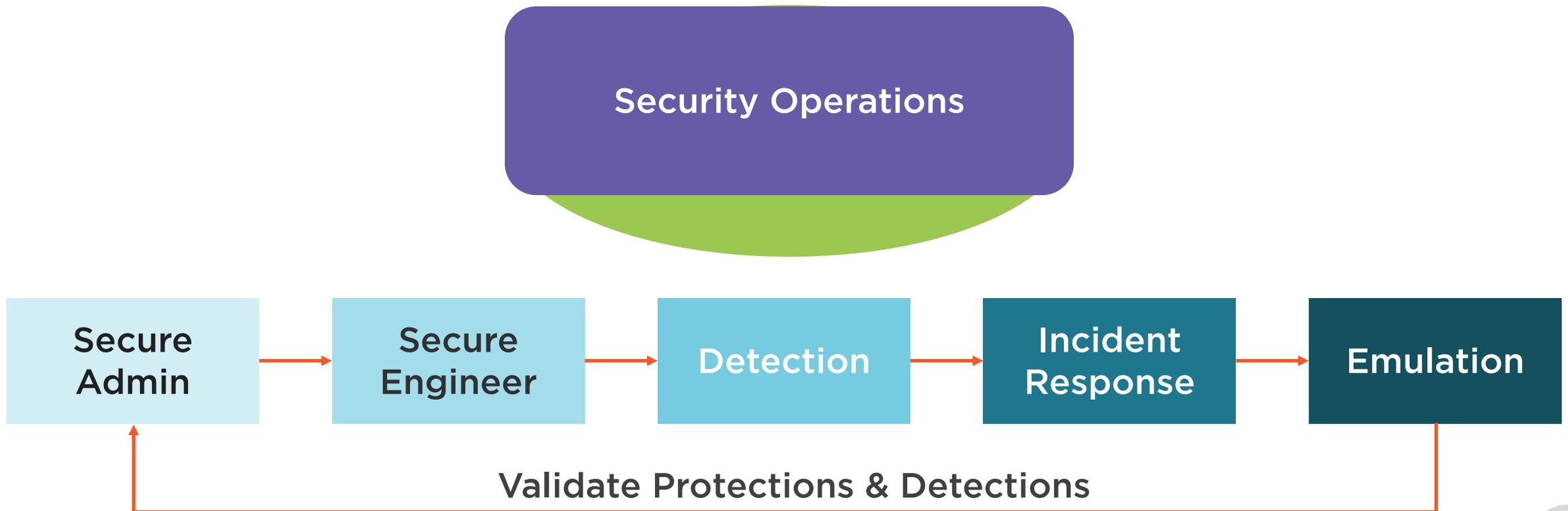
Kill Chain



Internal Red Team



Purple Team Concept



MITRE PRE-ATT&CK

Tactics

Technical Information Gathering
People Information Gathering
Organizational Information Gathering
Technical Weakness Identification
People Weakness Identification
Organization Weakness Identification
Adversary Opsec
Establish and Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities



MITRE ATT&CK

Pre-Tactics

Technical Information Gathering
People Information Gathering
Organizational Information Gathering
Technical Weakness Identification
People Weakness Identification
Organization Weakness Identification
Adversary Opsec
Establish and Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

Enterprise 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

Techniques

T1020 Automated exfiltration
T1002 Data compressed
T1022 Data encrypted
T1030 Data transfer size limits
T1048 Exfil over alternative protocol
T1041 Exfil over C2
T1011 Exfil over alt network medium
T1052 Exfil over physical medium
T1029 Scheduled transfer
T1537 Transfer data to cloud account



MITRE ATT&CK

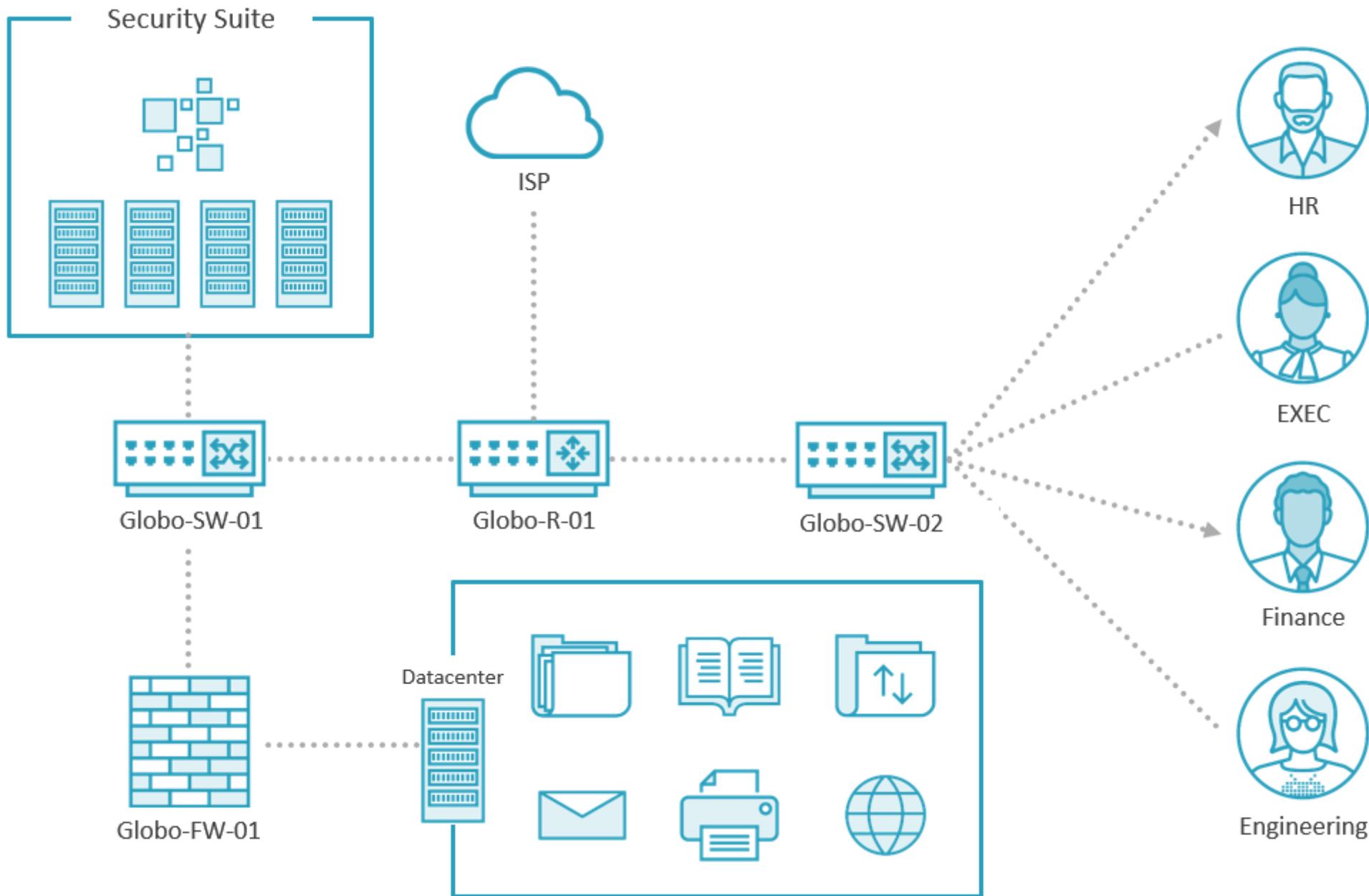
Techniques

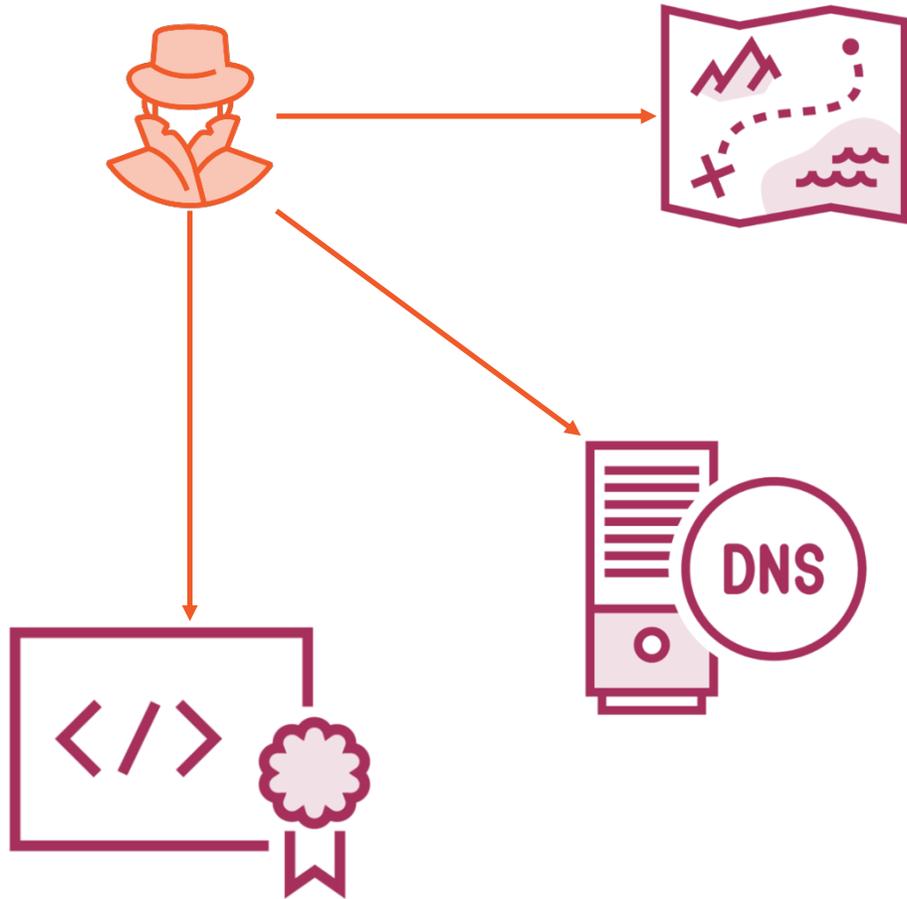
- T1020 Automated exfiltration
- T1002 Data compressed
- T1022 Data encrypted
- T1030 Data transfer size limits
- T1048 Exfil over alternative protocol
- T1041 Exfil over C2
- T1011 Exfil over alt network medium
- T1052 Exfil over physical medium
- T1029 Scheduled transfer
- T1537 Transfer data to cloud account

Sub-Techniques

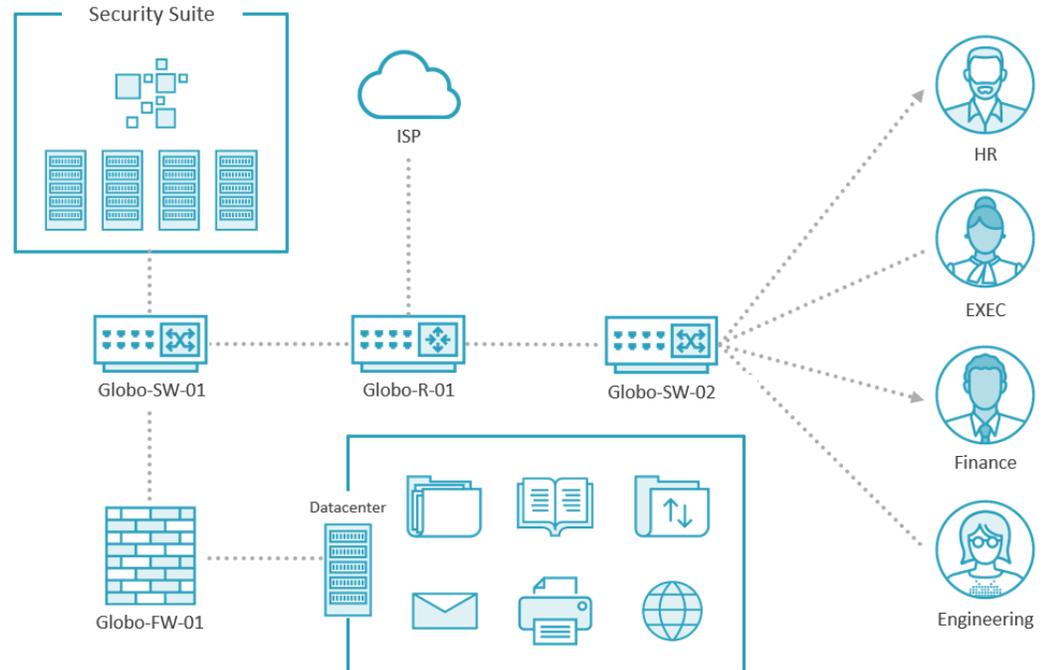
- Exfil over symmetric encrypted non-C2 protocol
- Exfiltration over asymmetric encrypted non-c2 protocol
- Exfiltration over unencrypted/obfuscated non-c2 channel

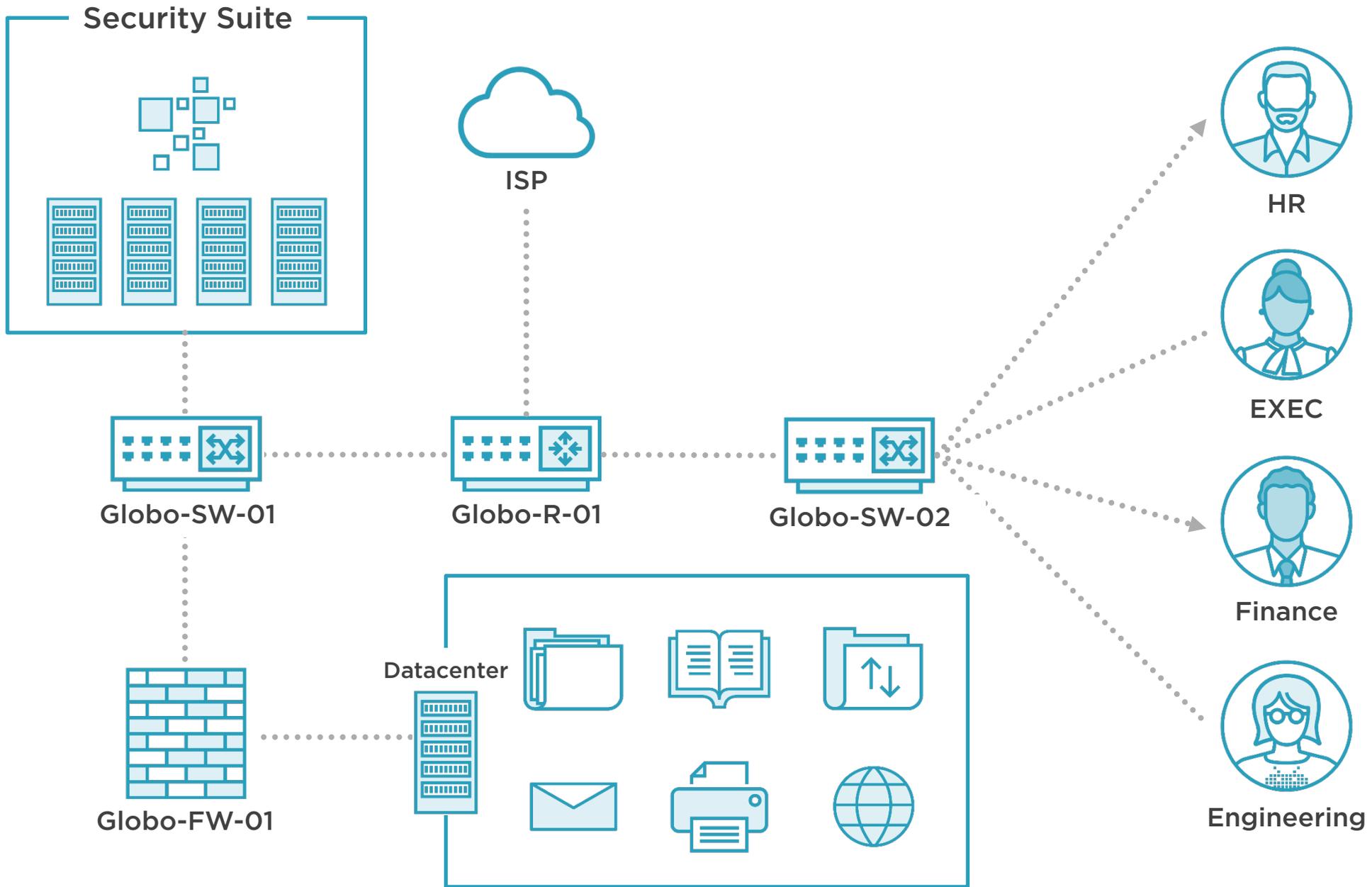


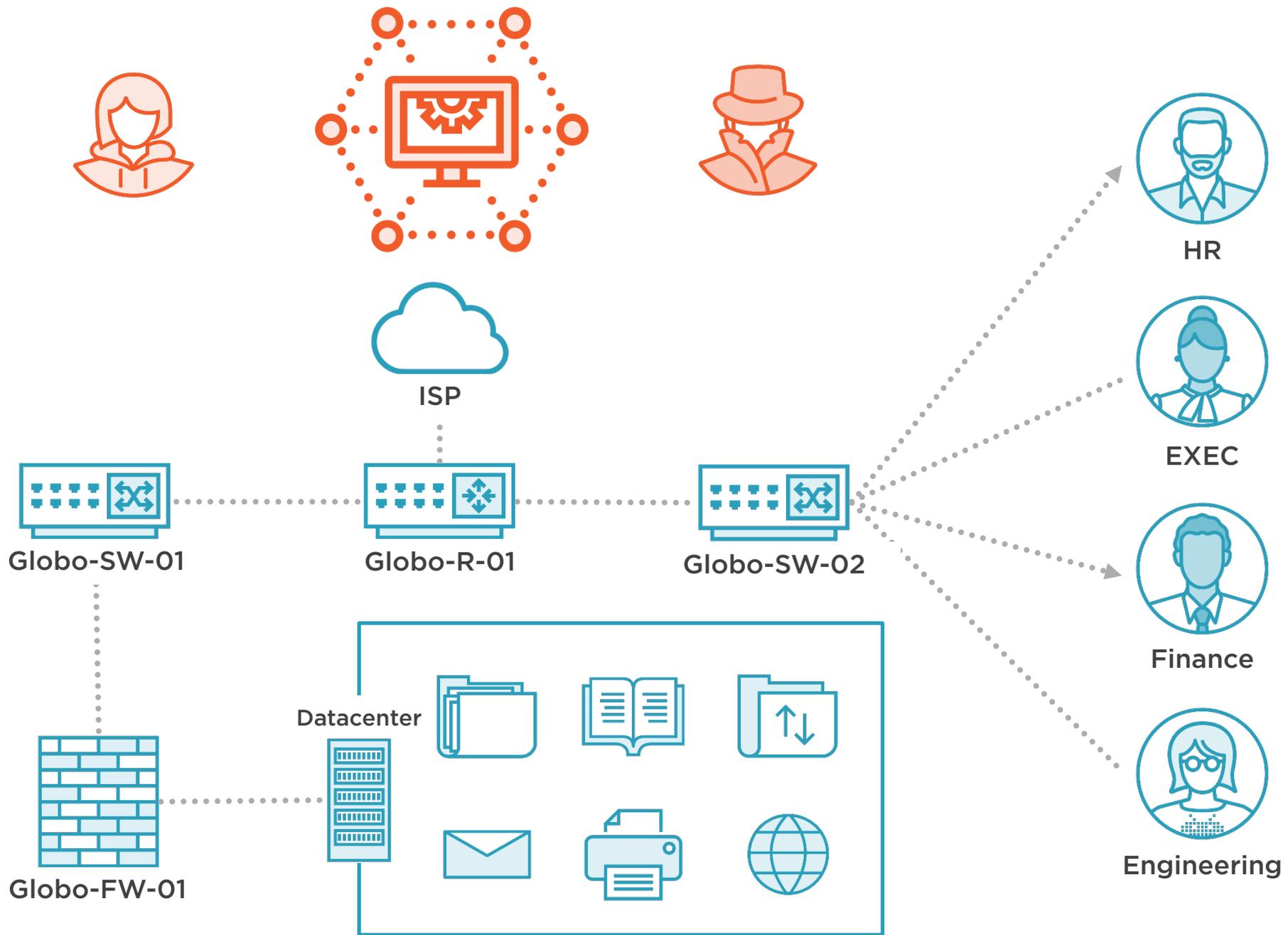


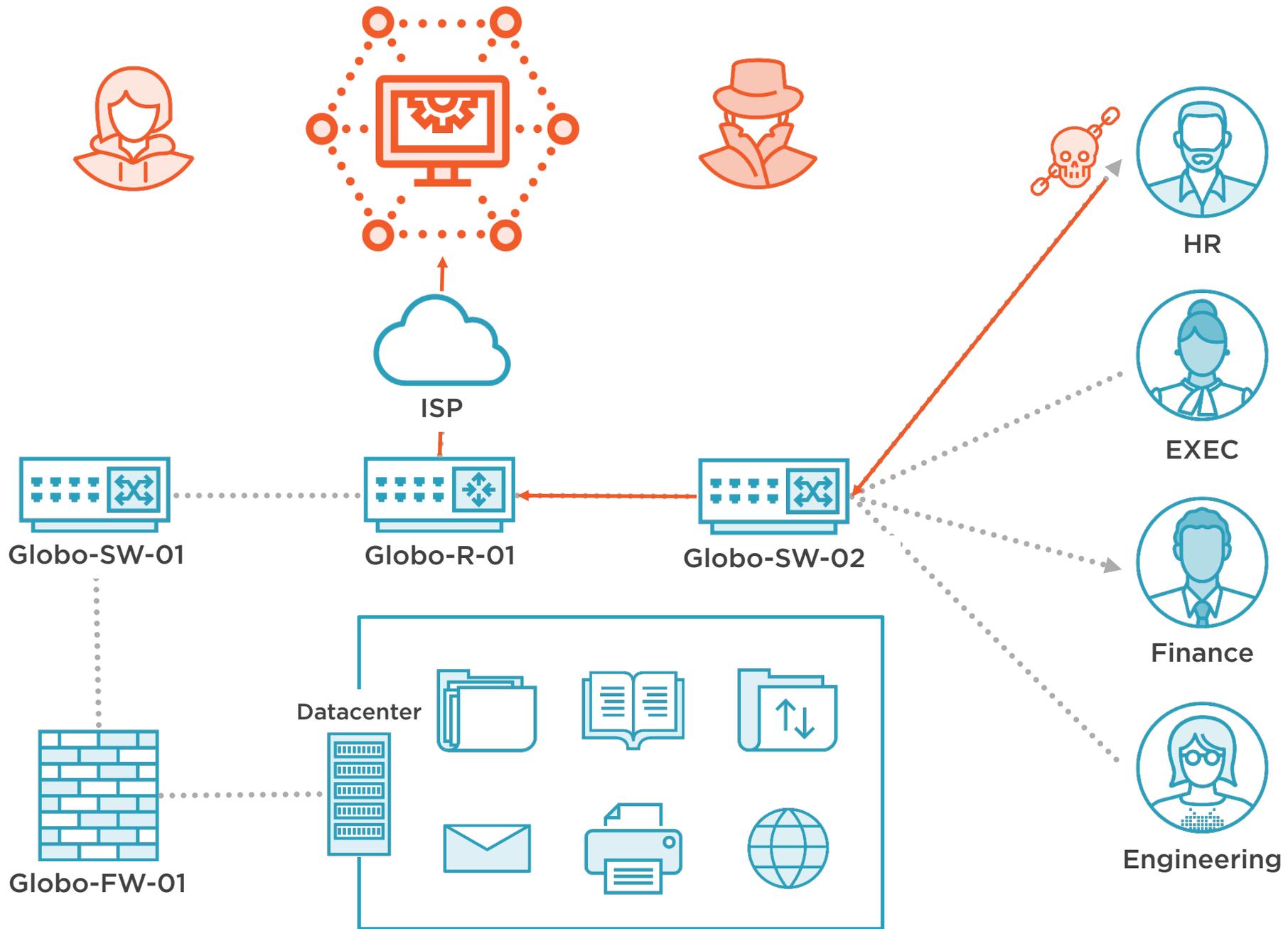


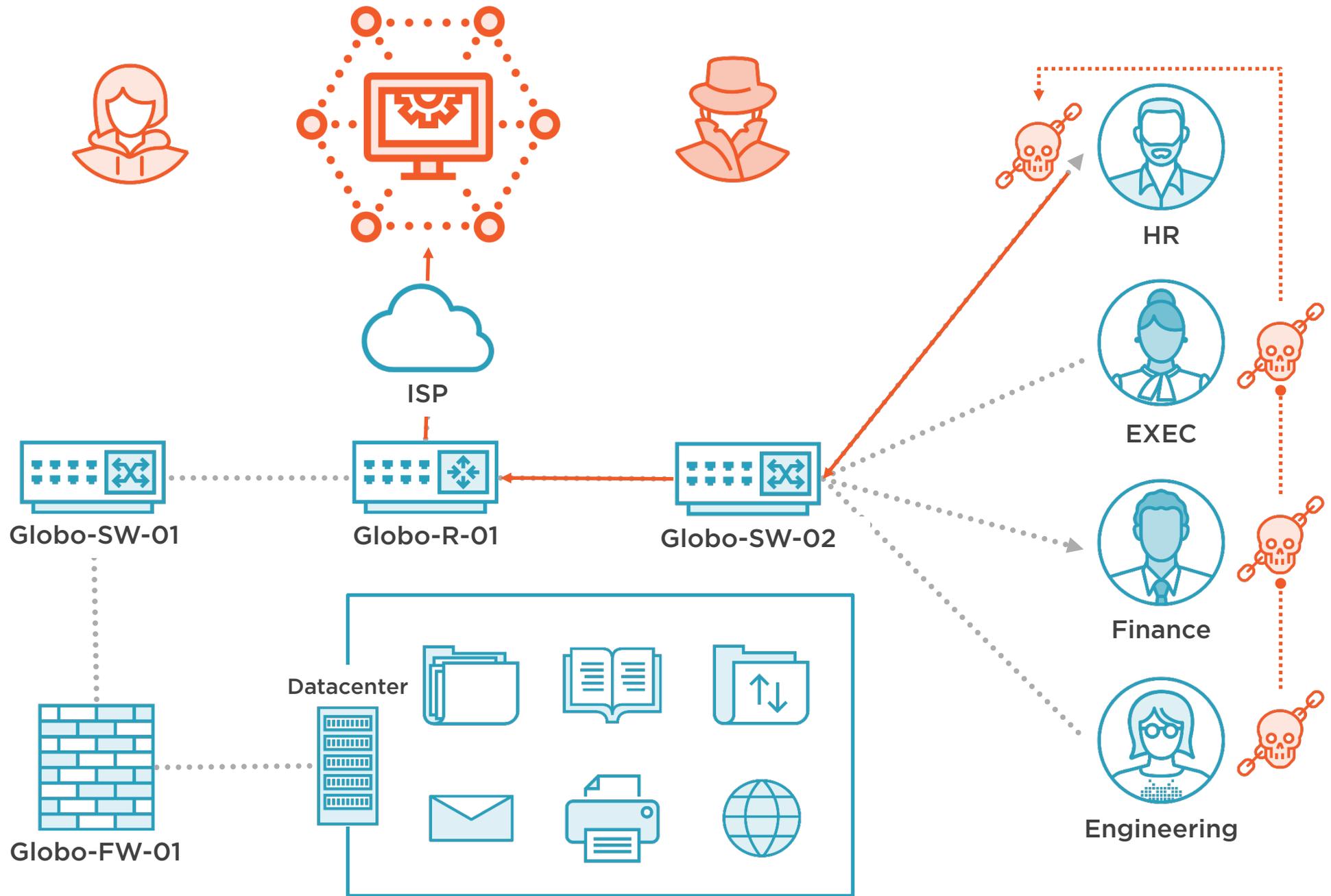
This is passive!



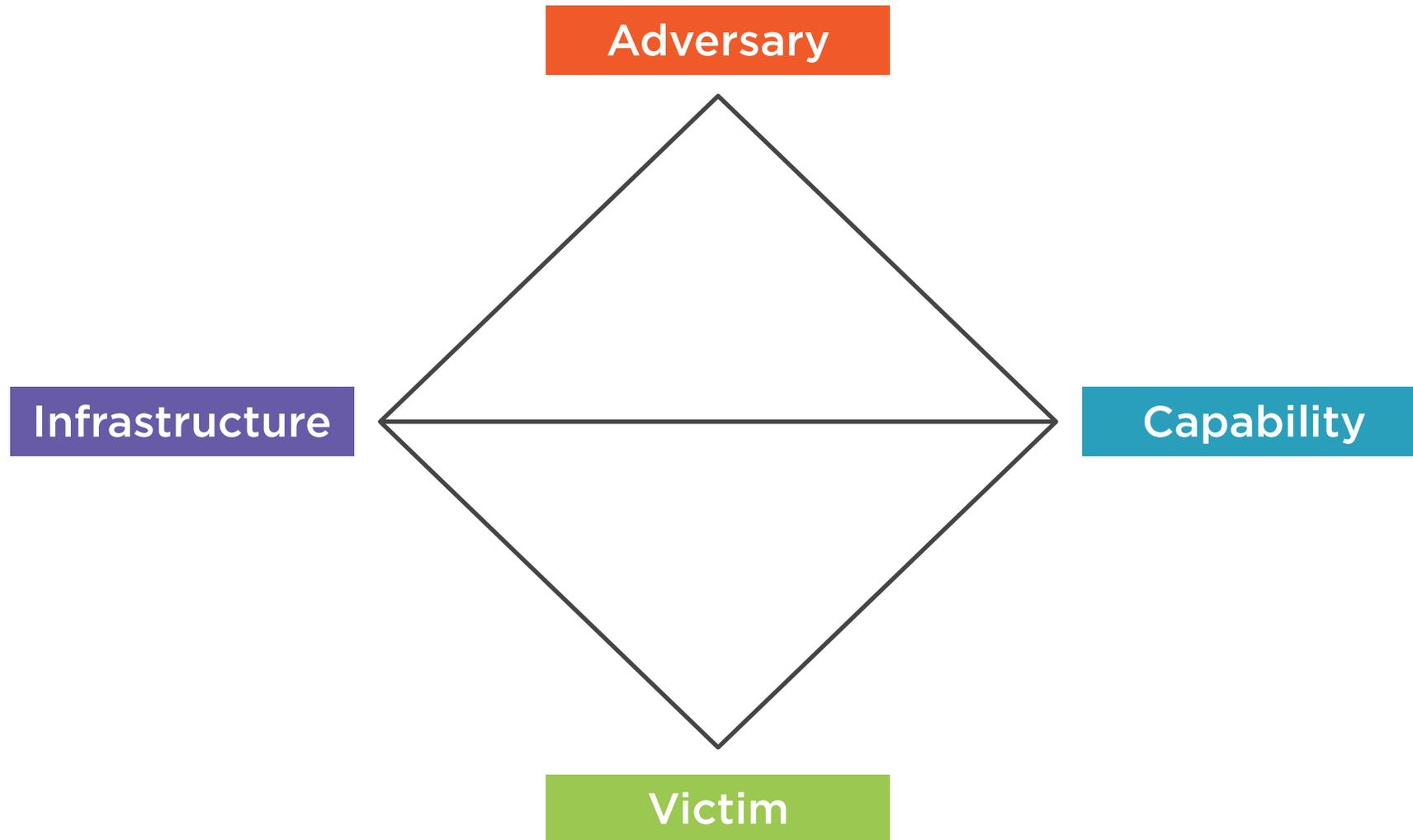








Diamond Model for Intrusion Analysis



Bottom Line

Who are the **Adversaries**

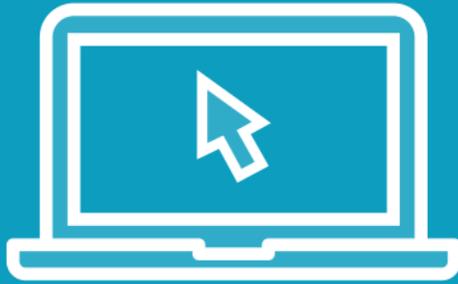
That have the money and people for the **Infrastructure**

And the technical **Capability**

Combined with intent to compromise your **Industry**



Demo



MITRE ATT&CK Navigator

- Most likely/dangerous
- <https://mitre-attack.github.io/attack-navigator/enterprise/>



More Information

APT Information

Know Your APTs

<https://www.fireeye.com/current-threats/apt-groups.html>

ATT&CK Navigator

<https://mitre-attack.github.io/attack-navigator/enterprise/>

Fight Like the Adversary

<https://app.pluralsight.com/paths/skill/red-team-tools>

Threat Intelligence Information

Integrating Red Team Operations

<https://app.pluralsight.com/library/courses/pentesting-red-blue-purple-teams-exec-briefing/table-of-contents>

Focused Threat Intelligence

- <https://www.nationalisacs.org/member-isacs>
- <https://www.virustotal.com/graph/>
- <https://www.infragard.org/>

