

# Command and Control with Merlin

---



**Zach Roof**

LEAD SECURITY ENGINEER

@zachroofsec [www.zachroofsec.com](http://www.zachroofsec.com)





**MERLIN**





Creator: Russel Van Tuyl



“Evade network detection during a penetration test/red team exercise by using a protocol that existing tools aren’t equipped to understand or inspect”





Open source C2 framework written in Golang

Agents: Mac, Linux, Windows, Javascript

Notes: [github.com/zachroofsec/command-and-control-with-merlin](https://github.com/zachroofsec/command-and-control-with-merlin)

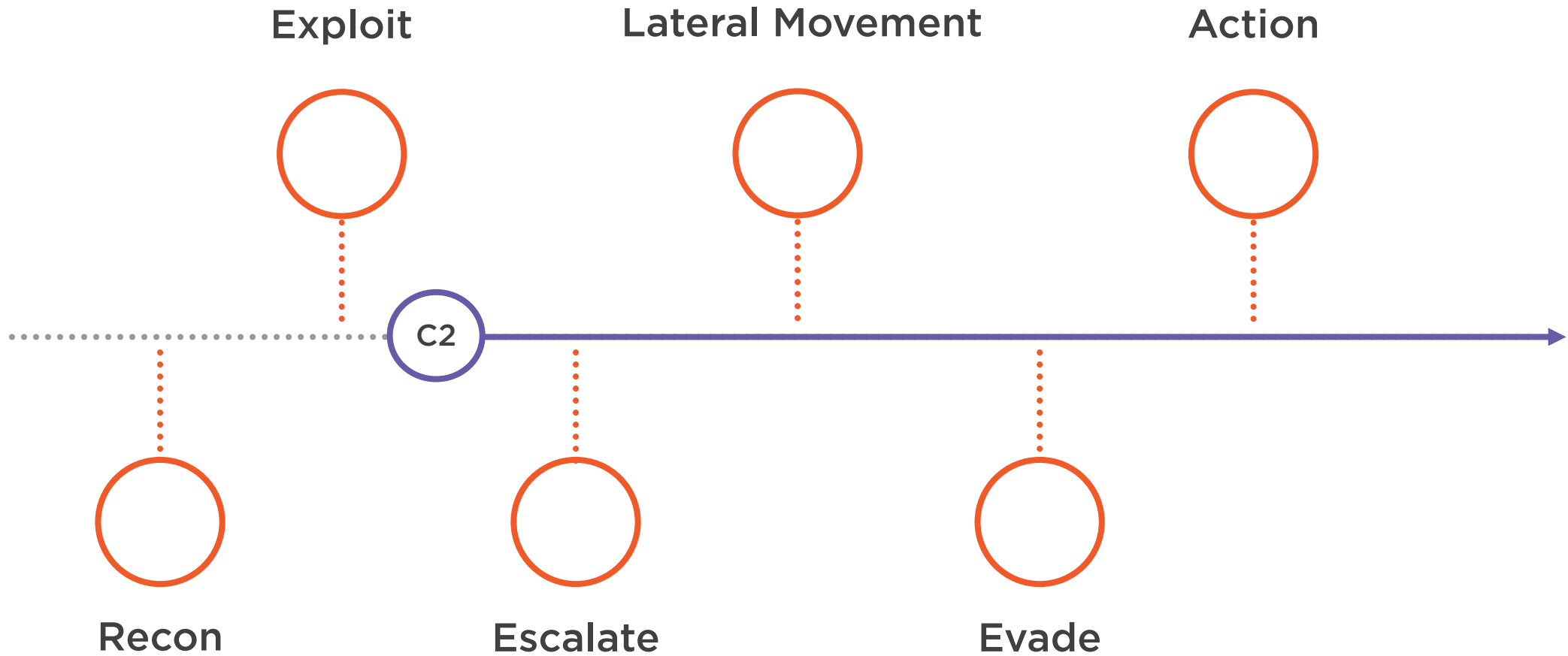
Docs: [merlin-c2.readthedocs.io/](https://merlin-c2.readthedocs.io/)

Available at [github.com/Ne0nd0g/merlin](https://github.com/Ne0nd0g/merlin)

Protocols: HTTP/1.1, HTTP/2, HTTP/3



# 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

T1105:

Ingress Tool Transfer

T1071:

Application Layer Protocol

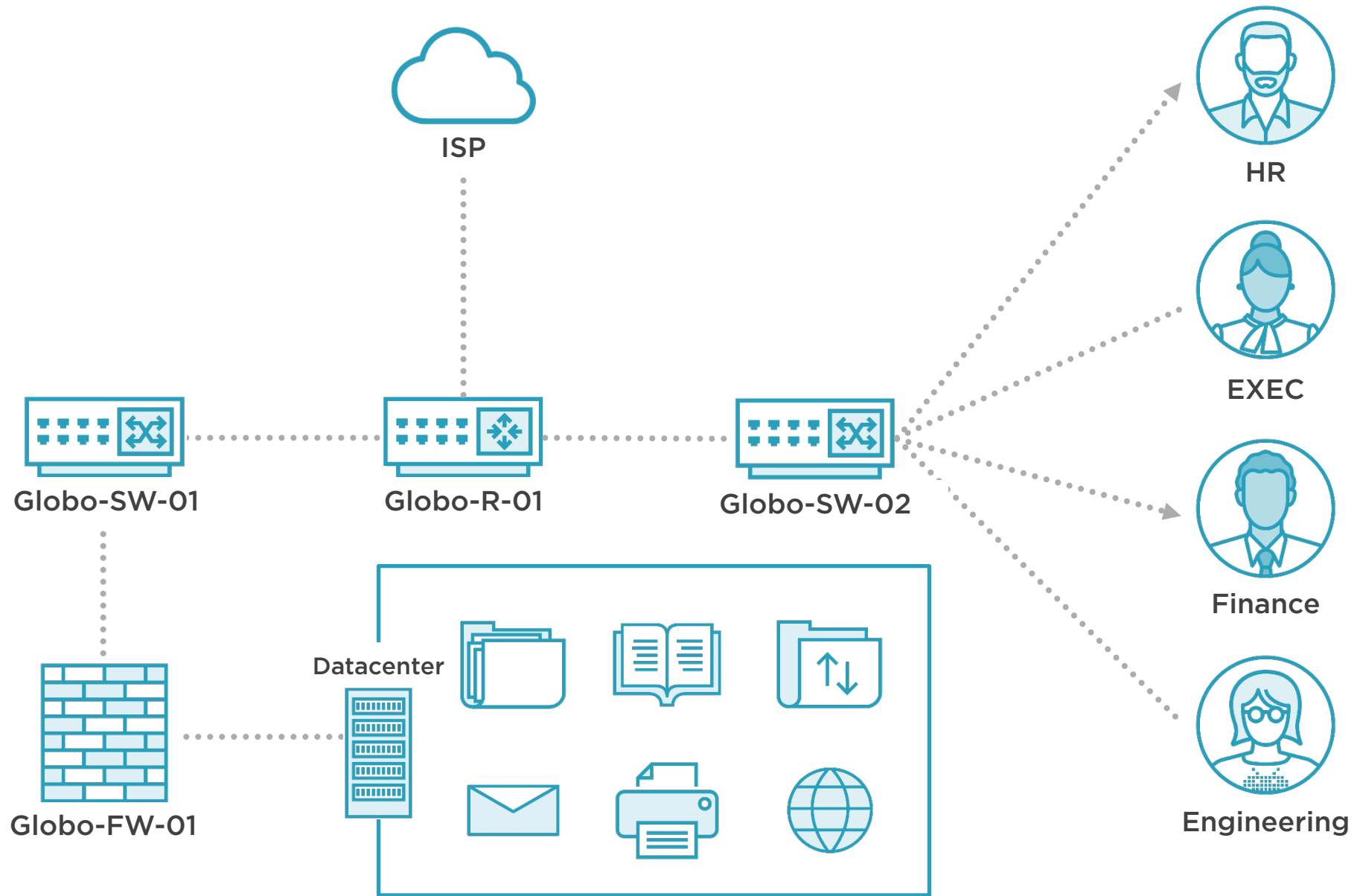
T1041:

Exfiltration Over C2 Channel

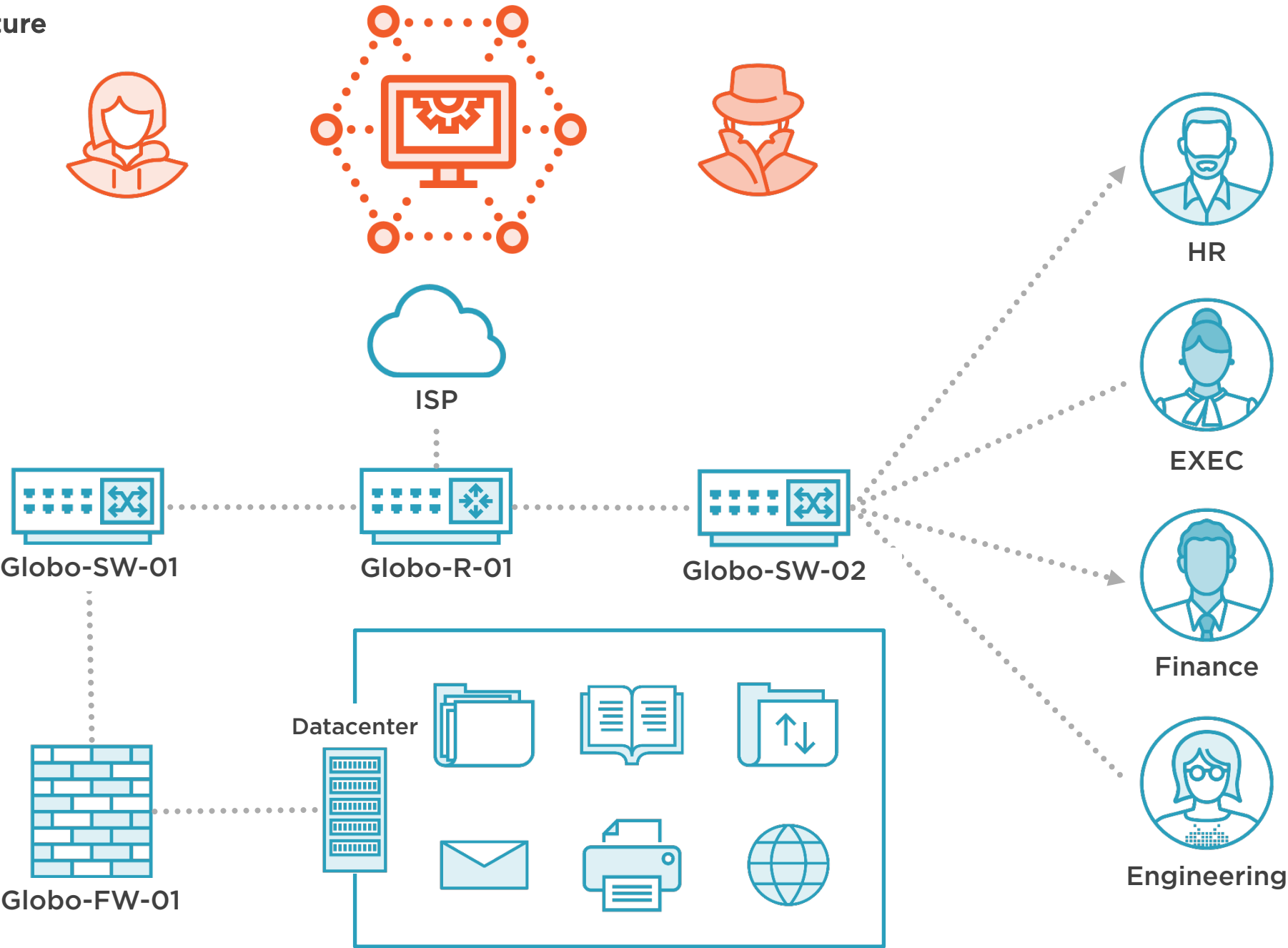
T1071.001:

Web Protocols

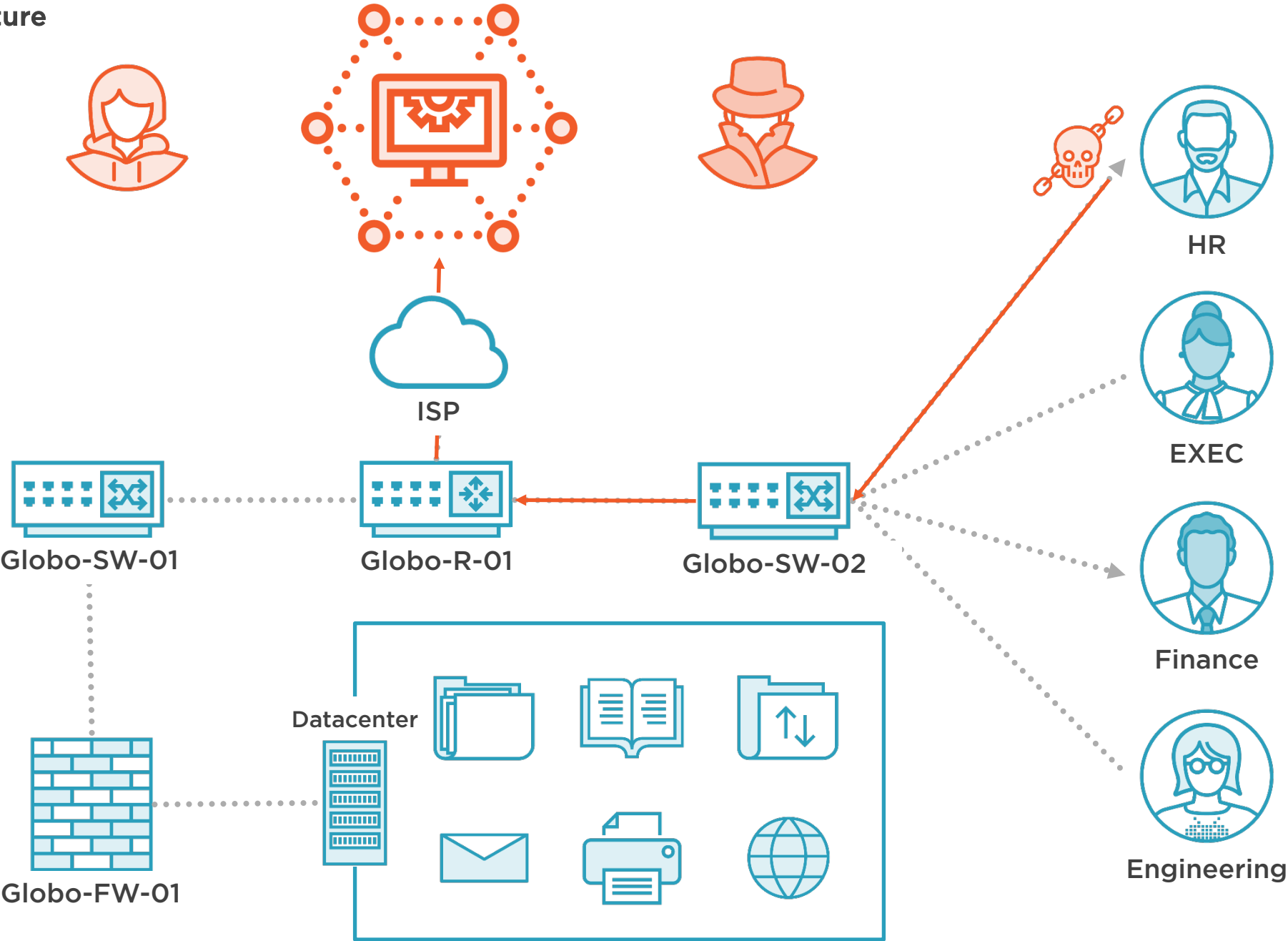




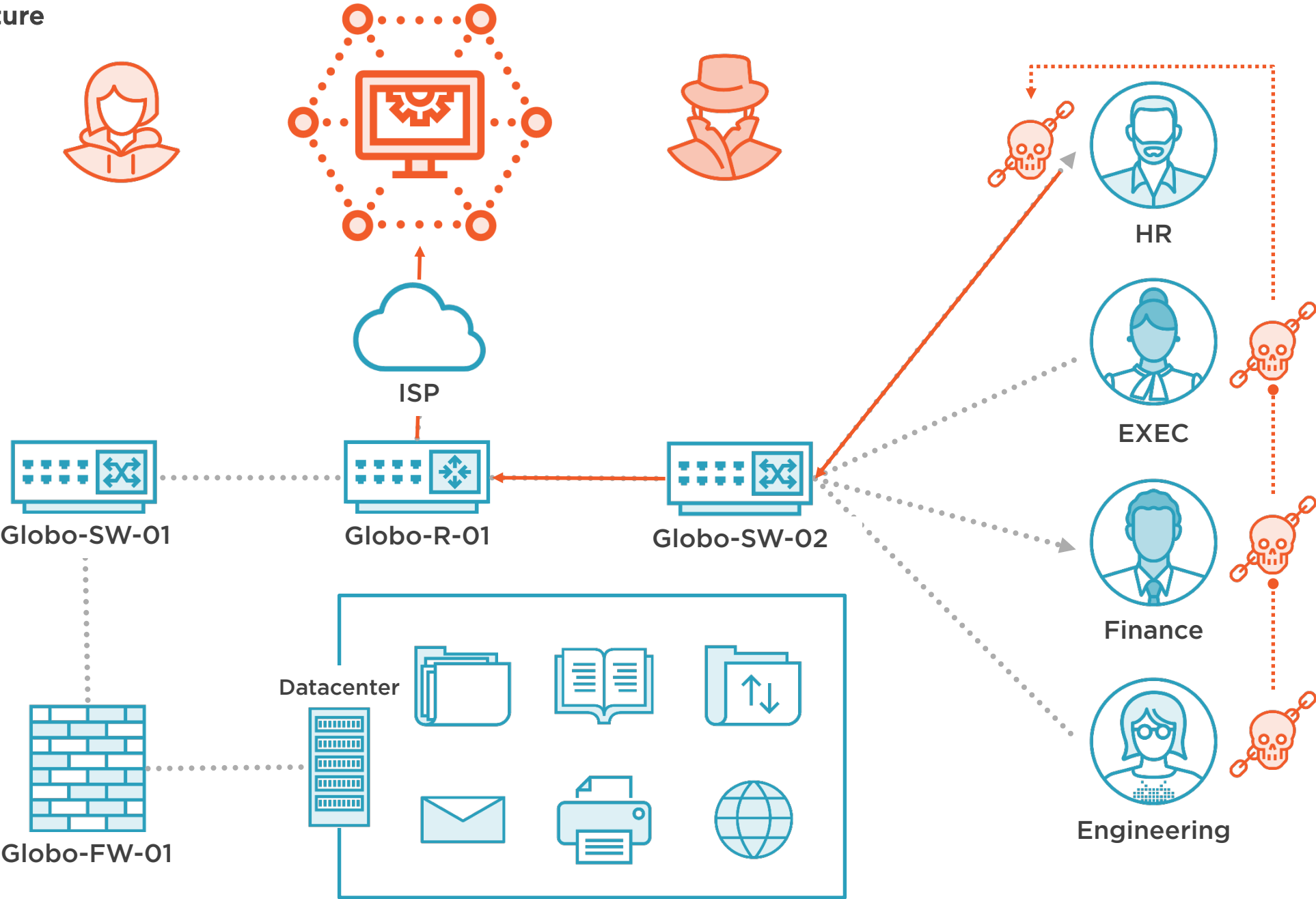
Red Team Infrastructure



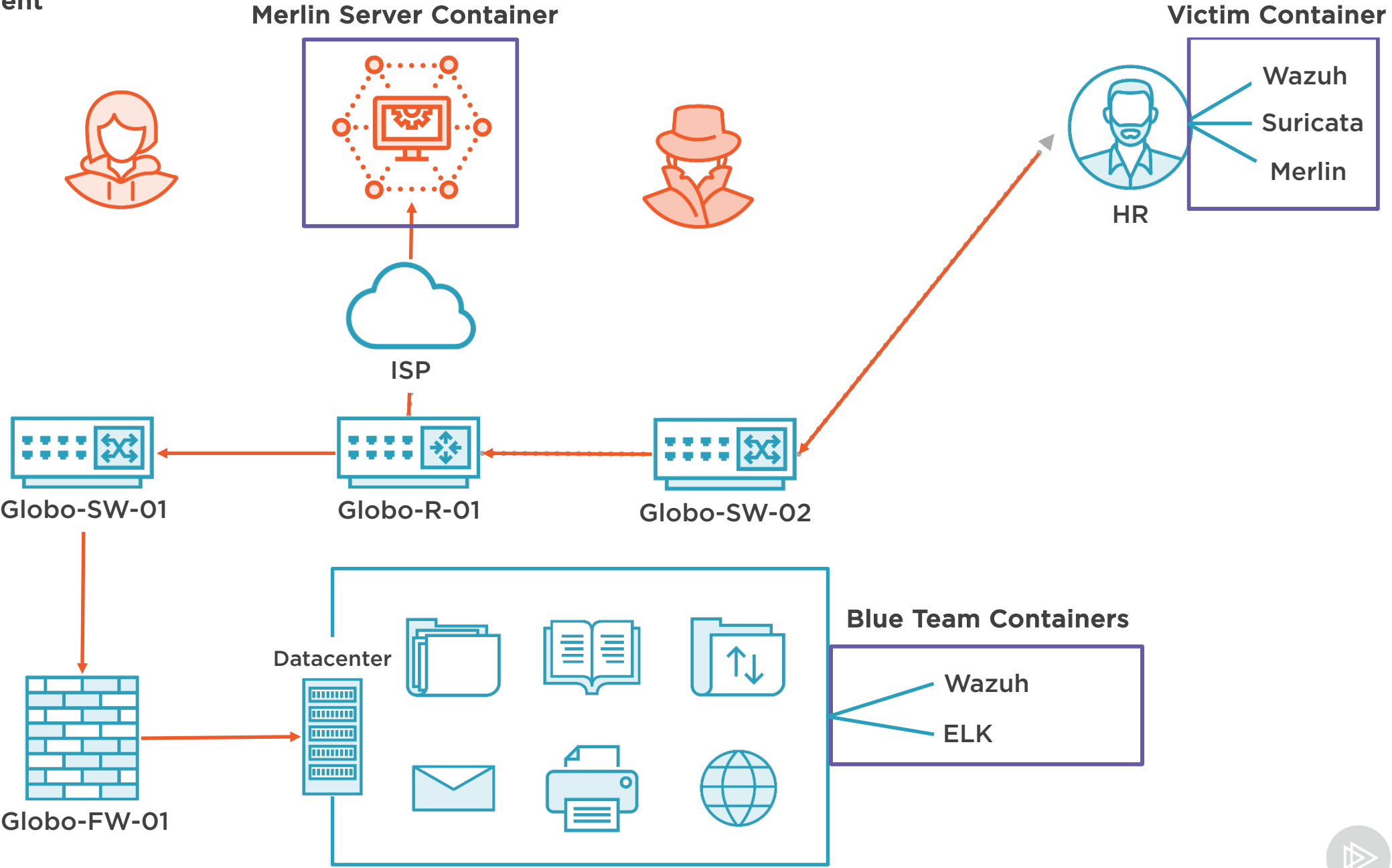
Red Team Infrastructure



Red Team Infrastructure



Simulation Environment



# Additional Resources

## Capabilities

<https://www.sans.org/reading-room/whitepapers/protocols/paper/36877>

<https://medium.com/@Ne0nd0g/merlin-adds-module-support-f121175412e>

<https://medium.com/@Ne0nd0g/merlin-adds-dll-agent-powershell-invoke-merlin-script-6127b3d7cbcd>

<https://merlin-c2.readthedocs.io/en/v0.9.0-beta/misc/blogs.html>

## Related Information

### Web Protocols

<https://attack.mitre.org/techniques/T1071/001/>

### Supporting Technology

- HTTP/2
- <https://developers.google.com/web/fundamentals/performance/http2>
- HTTP/3
- <https://quicwg.org/base-drafts/draft-ietf-quic-http.html>



# Command and Control with Merlin

---



**Zach Roof**

LEAD SECURITY ENGINEER

@zachroofsec [www.zachroofsec.com](http://www.zachroofsec.com)

