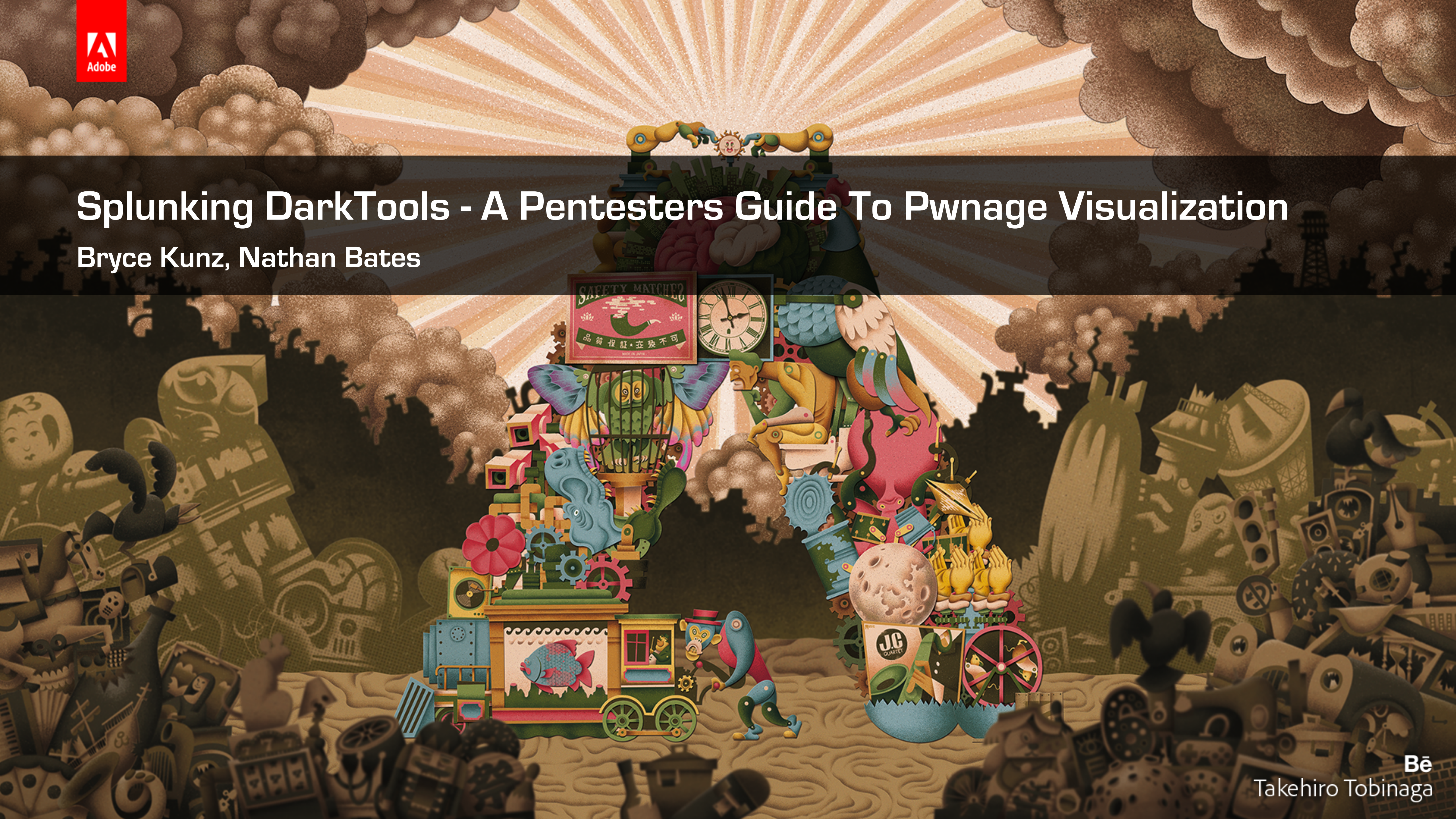
Splunking DarkTools - A Pentesters Guide To Pwnage Visualization

Bryce Kunz, Nathan Bates



Takehiro Tobinaga

Who are we?

- Bryce
- Nathan

Buy now!

- **Acquired!**

Hole in One!

- Execs Happy!

Attack Surface

- VS. the little guy!

Stubborn

- As a Mule!

Swoop In

- To Save The Day!

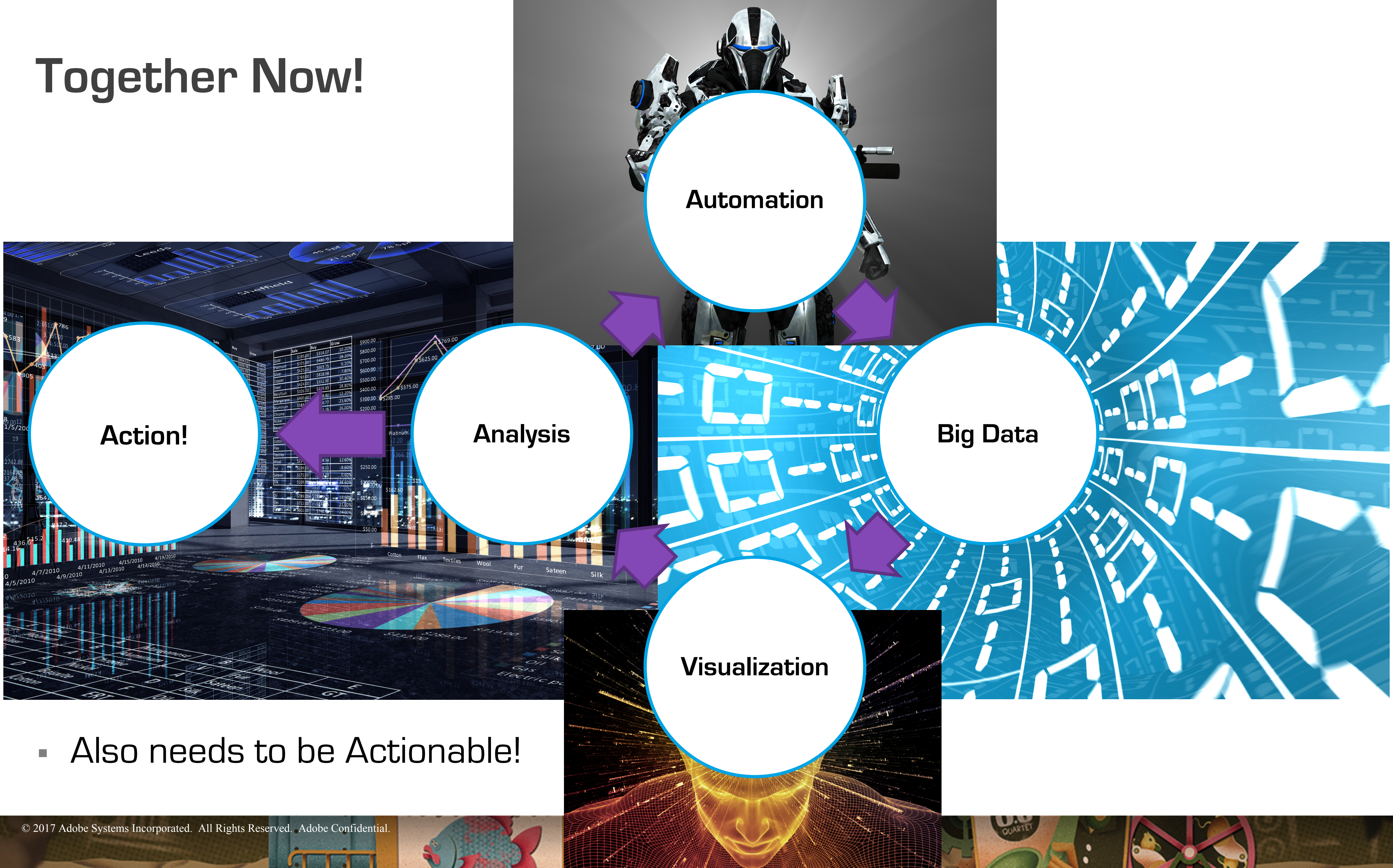
Chaotic

- Lacks Integration
- Unnecessarily Hard
- Weak Scaling

DarkTools Demo

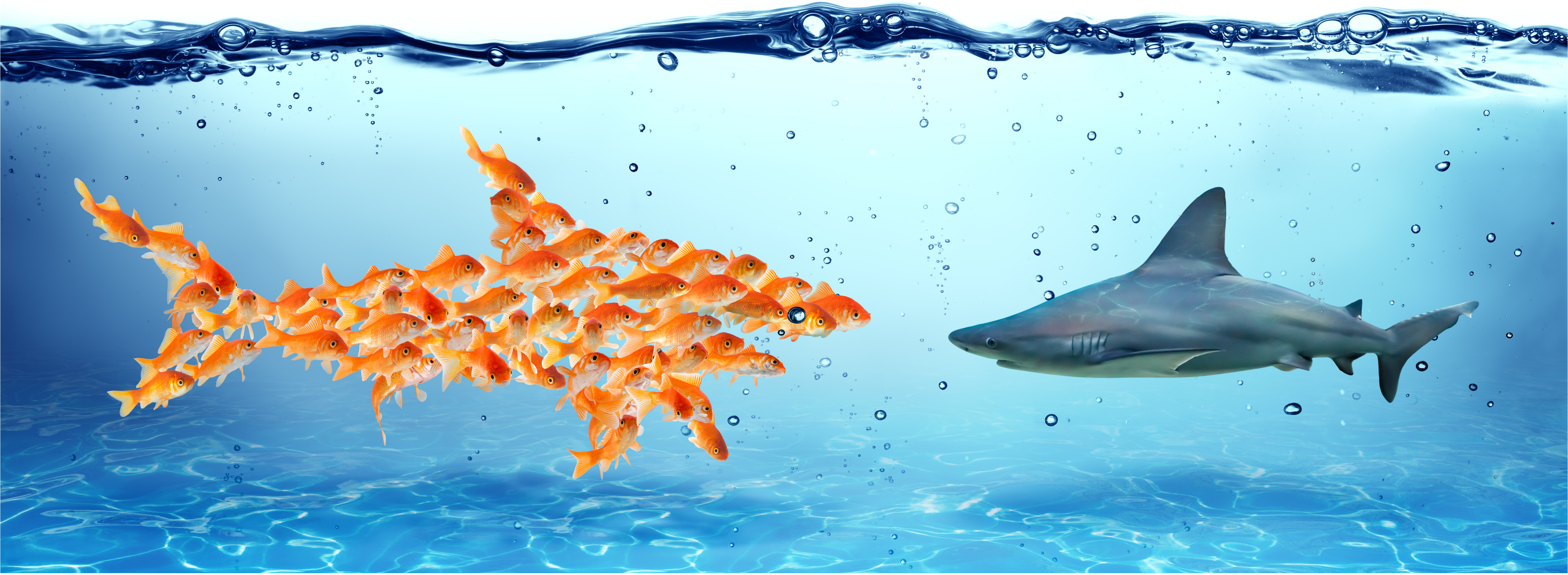
- Pirate Skelton's agree, it’s **easy** & **scalable**!

Together Now!



- Also needs to be Actionable!

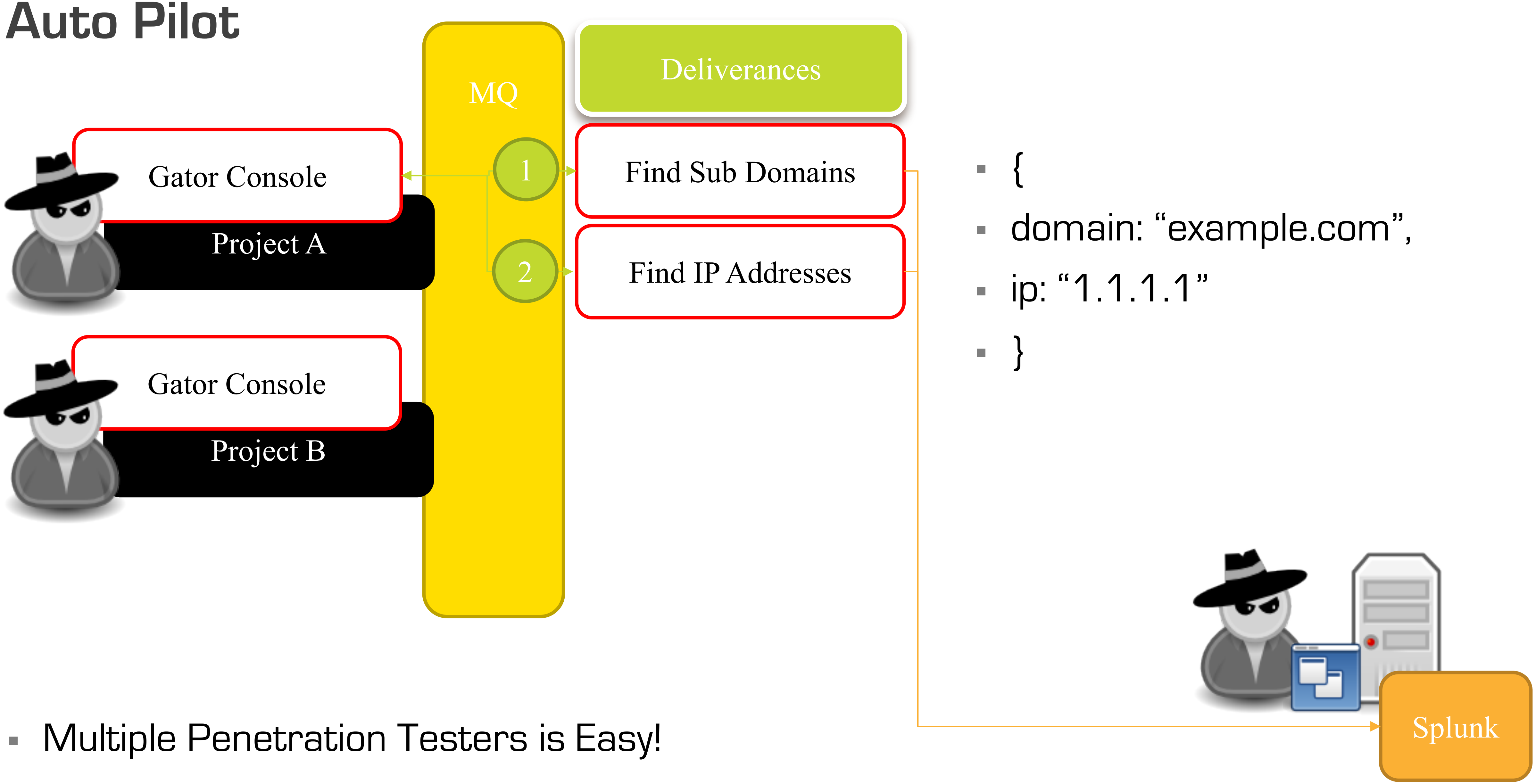
Collaboration



Visualization!

- Of Big Data!

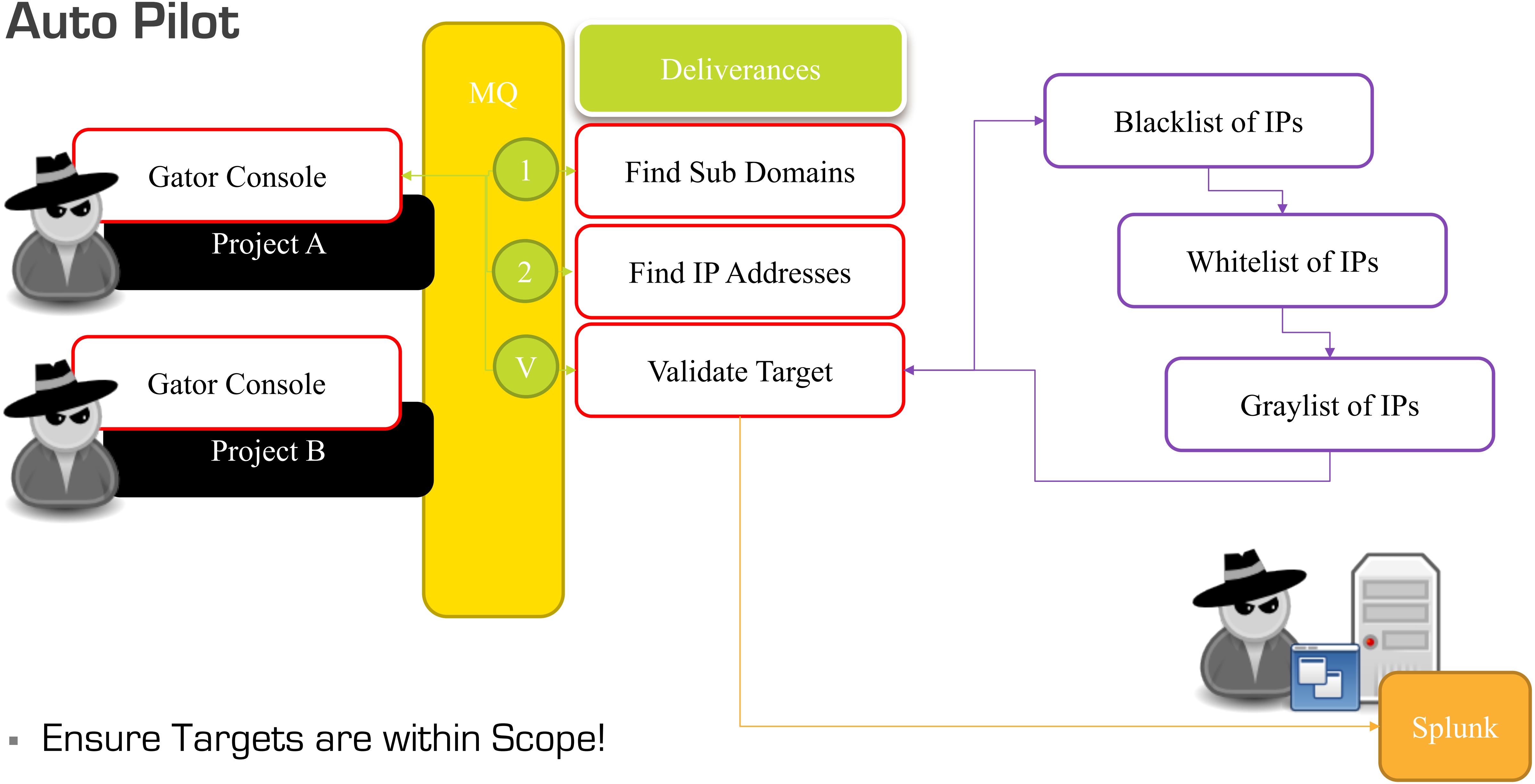
Auto Pilot



- {
- domain: “example.com”,
- ip: “1.1.1.1”
- }

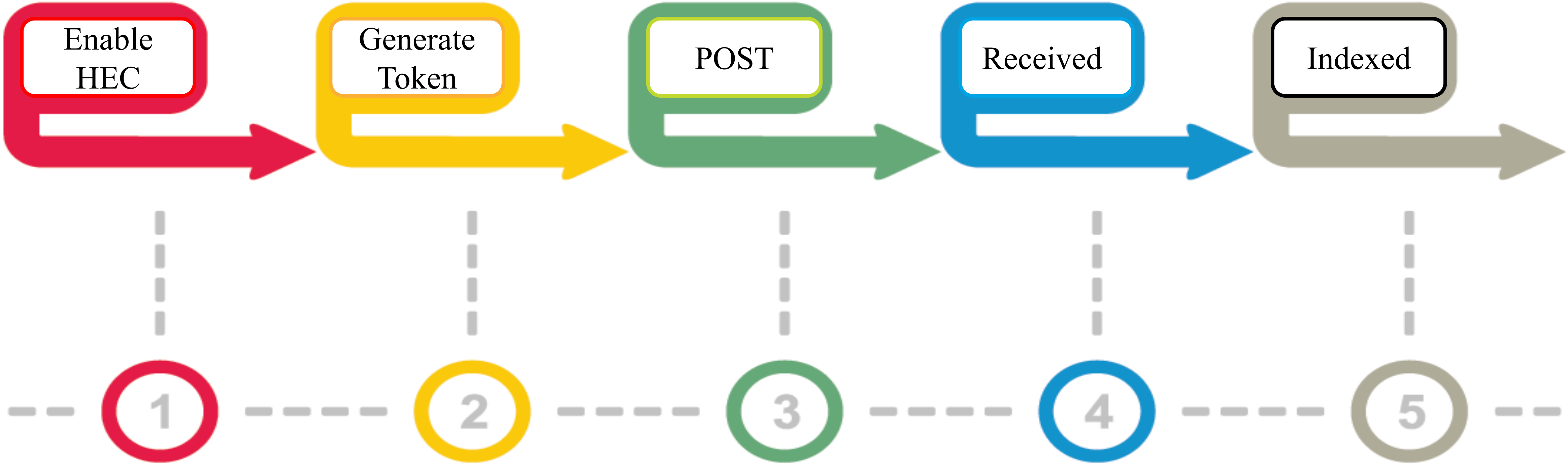
- Multiple Penetration Testers is Easy!

Auto Pilot



- Ensure Targets are within Scope!

HTTP Event Collector (HEC)



Enable HEC

Generate Token

POST

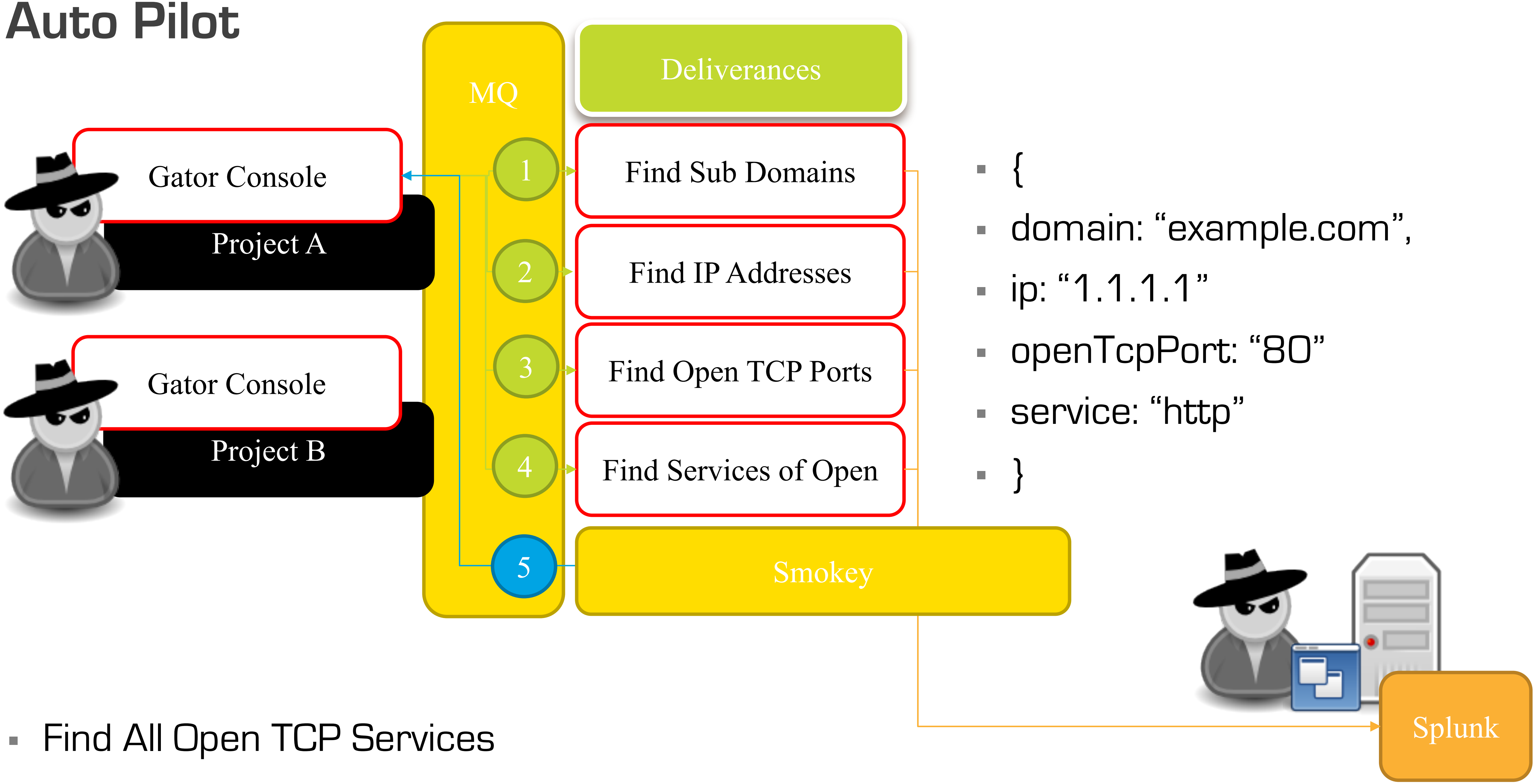
Received

Indexed

HEC POST

```
curl -k -H "Authorization: Splunk 12345678-1234-1234-1234-1234567890AB"
https://localhost:8088/services/collector/event -d
‘{
  "project":"DARKGRIFTER",
  "domain":"confluence.darkgrifter.com",
  "ip":"34.251.221.65",
  "protocol":"tcp",
  "port":"22”,
  "service":"ssh",
  "selectortype":"target",
  "severity":"INFO",
  "uniq_selector_id":"1499928119449hcobwltkfnnqtnjgwgtbconodklovmqru",
  "uniq_target_id":"1499941726162nhsgtgmhkoolfhjffaguyiiflclfbuhqj"
}’
```

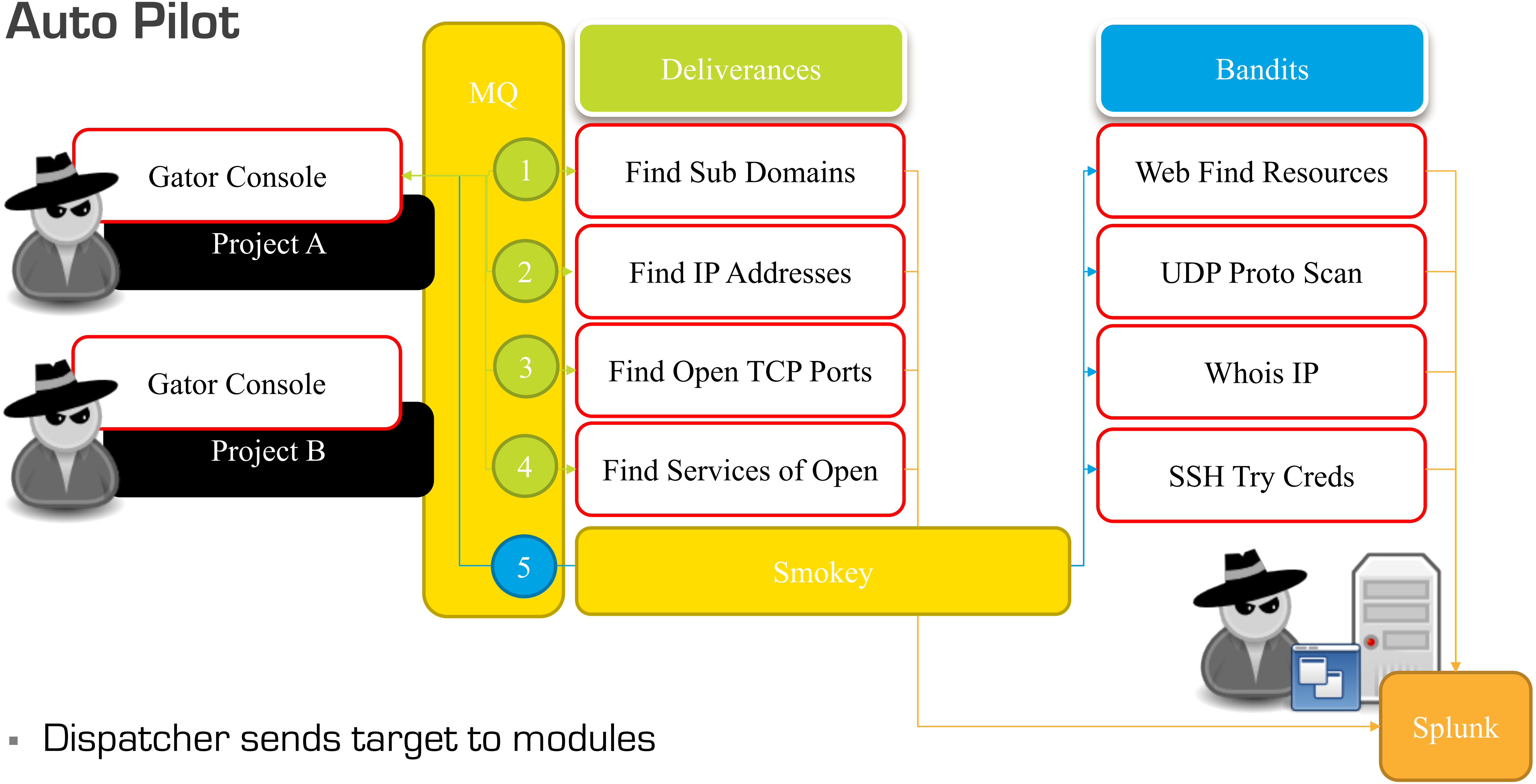
Auto Pilot



- {
- domain: “example.com”,
- ip: “1.1.1.1”
- openTcpPort: “80”
- service: “http”
- }

- Find All Open TCP Services

Auto Pilot



- Dispatcher sends target to modules

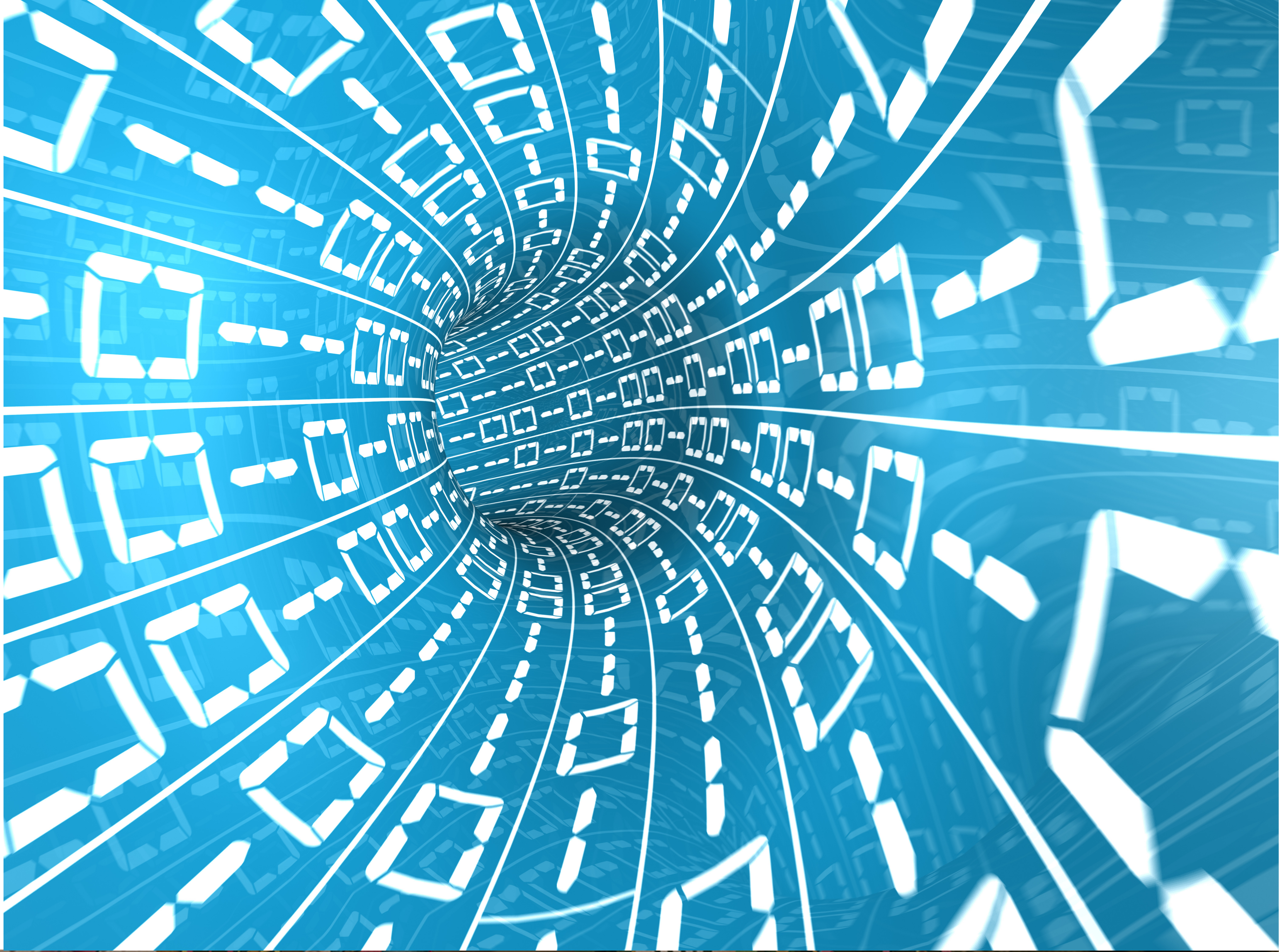
Why Splunk?

- Simple & Scalable
- Enterprise Security

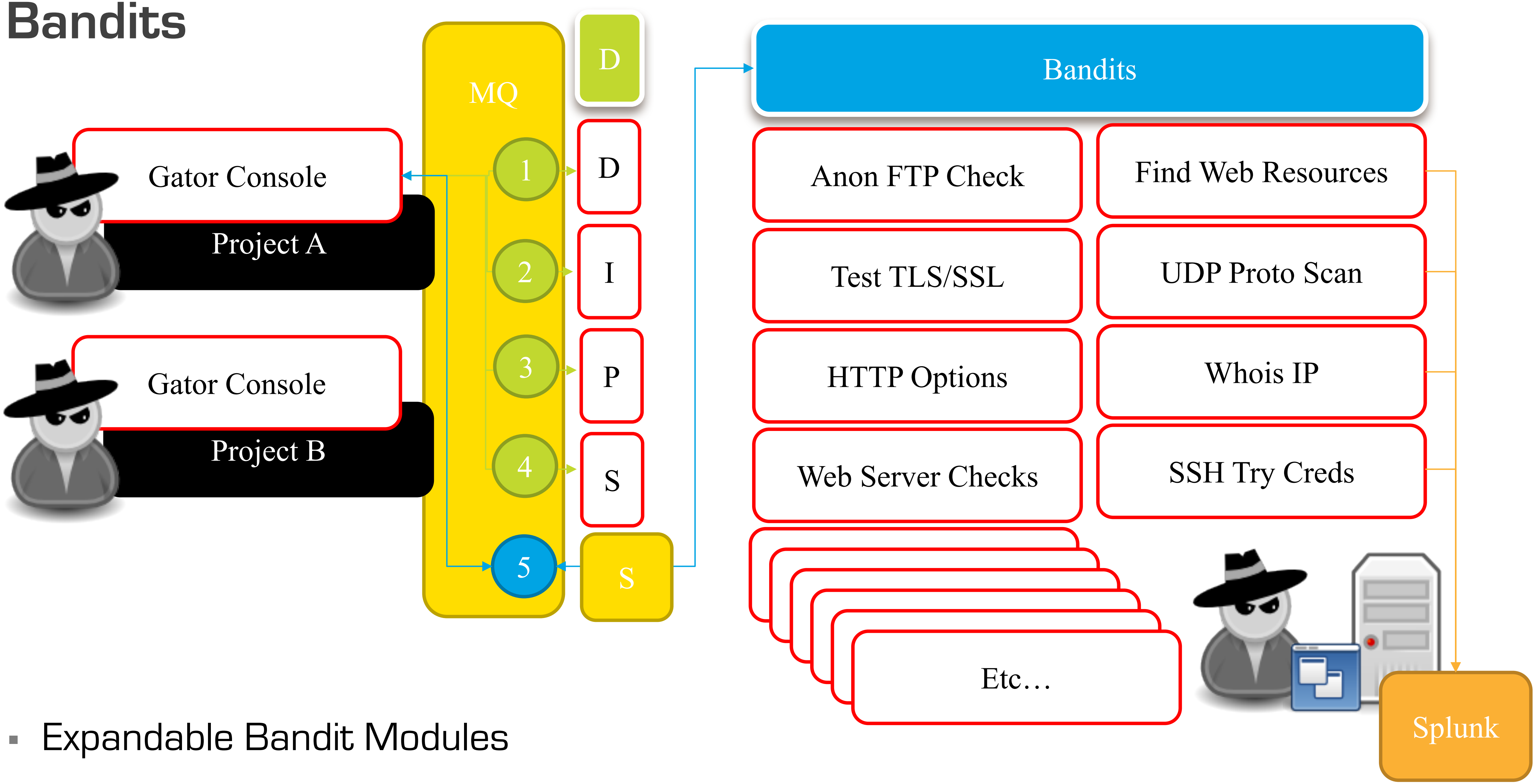
- Already in use!

Splunk Setup

- Splunk Install
- Create Index
- HEC
- Install Apps



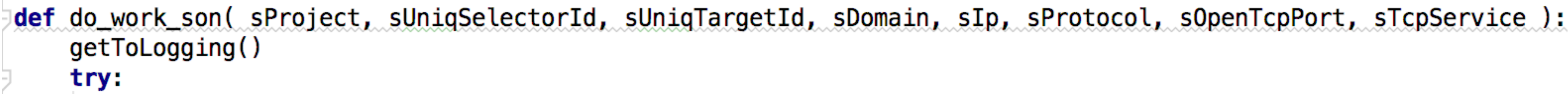
Bandits



- Expandable Bandit Modules

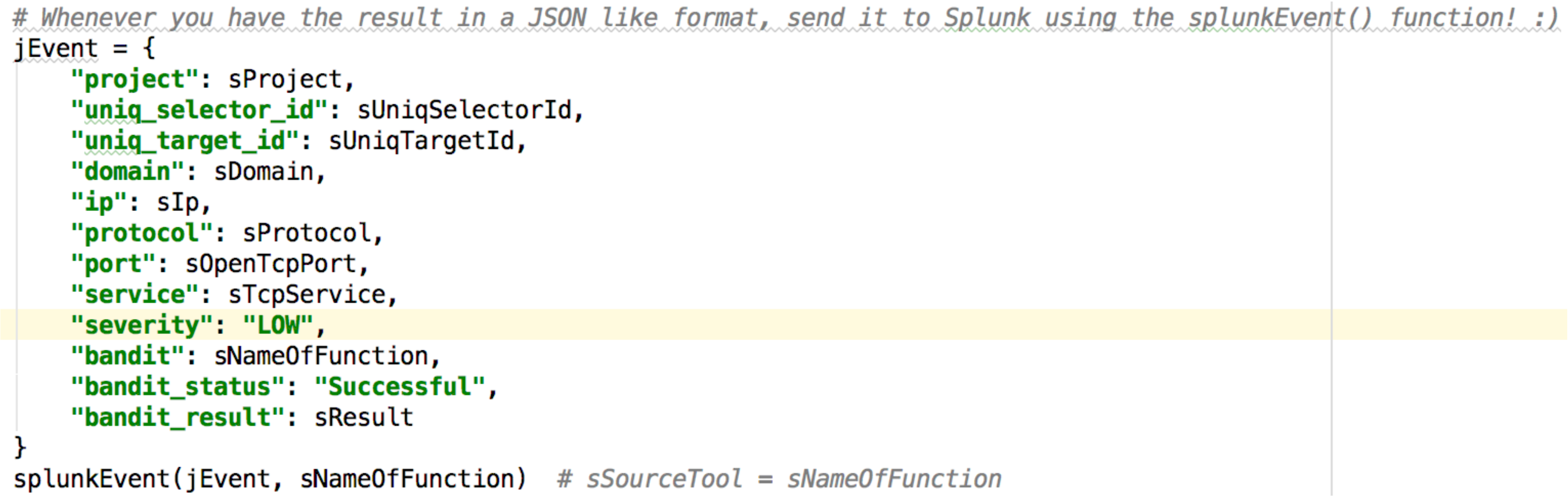
Template Bandit

- do_work_son() – Place logic within the try



```
def do_work_son( sProject, sUniqSelectorId, sUniqTargetId, sDomain, sIp, sProtocol, sOpenTcpPort, sTcpService ):
    getToLogging()
    try:
```

- splunkEvent() – Sends a JSON object to Splunk



```
# Whenever you have the result in a JSON like format, send it to Splunk using the splunkEvent() function! :)
jEvent = {
    "project": sProject,
    "uniq_selector_id": sUniqSelectorId,
    "uniq_target_id": sUniqTargetId,
    "domain": sDomain,
    "ip": sIp,
    "protocol": sProtocol,
    "port": sOpenTcpPort,
    "service": sTcpService,
    "severity": "LOW",
    "bandit": sNameOfFunction,
    "bandit_status": "Successful",
    "bandit_result": sResult
}
splunkEvent(jEvent, sNameOfFunction)  # sSourceTool = sNameOfFunction
```

Making the Data more Usable

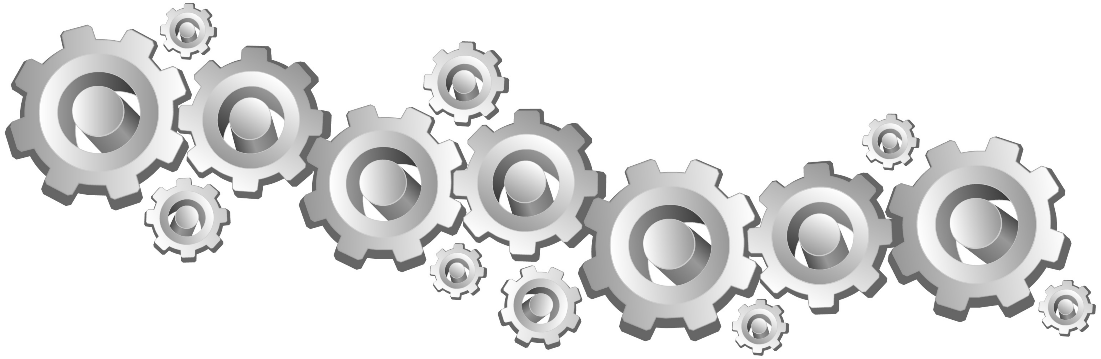
<u>Field Extraction</u>

- Before Splunk
  - JSON, AutoKV, etc
  - Done in python

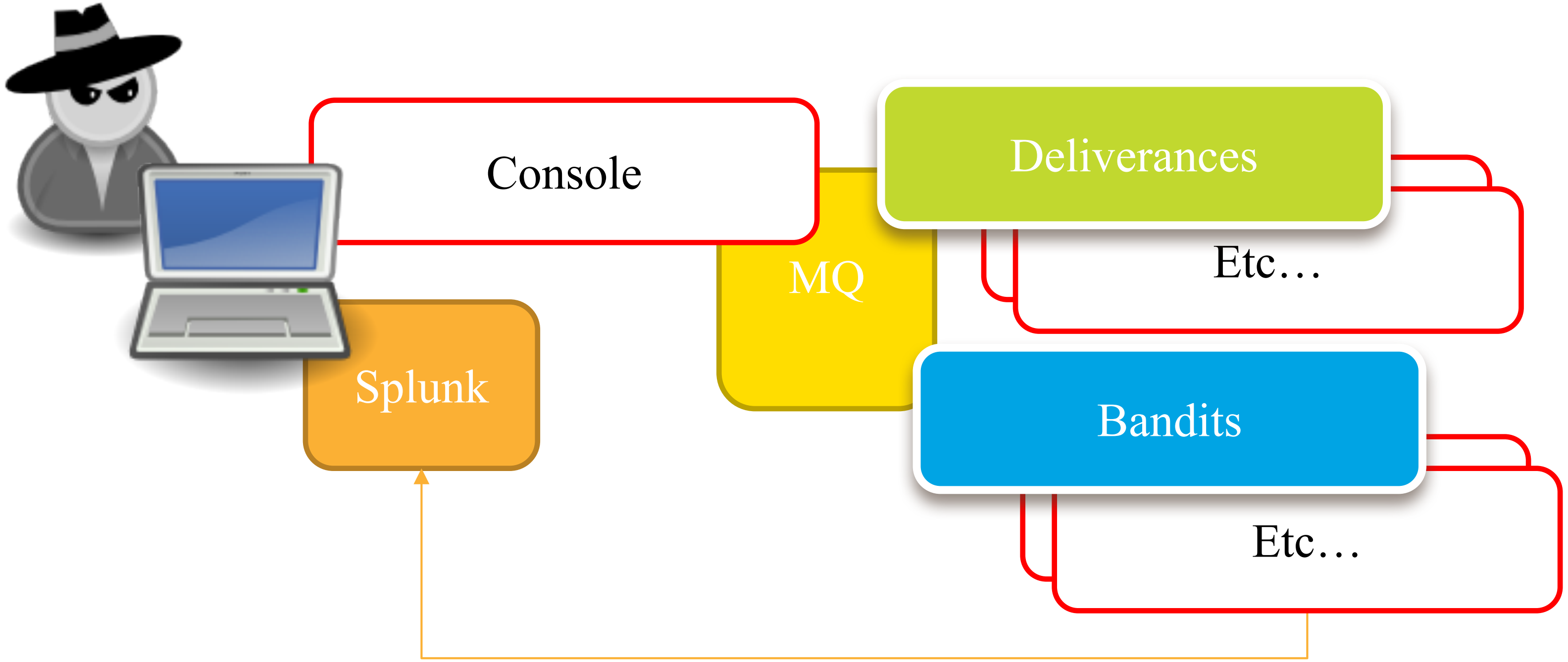
- In Splunk
  - Per sourcetype
  - Regex, field extraction, etc
  - Pros.conf,

- Lookups
  - Scheduled Searches to combine sourcytpes that ouput as lookups

- GeoIP
  - Adding location data to visualize locations

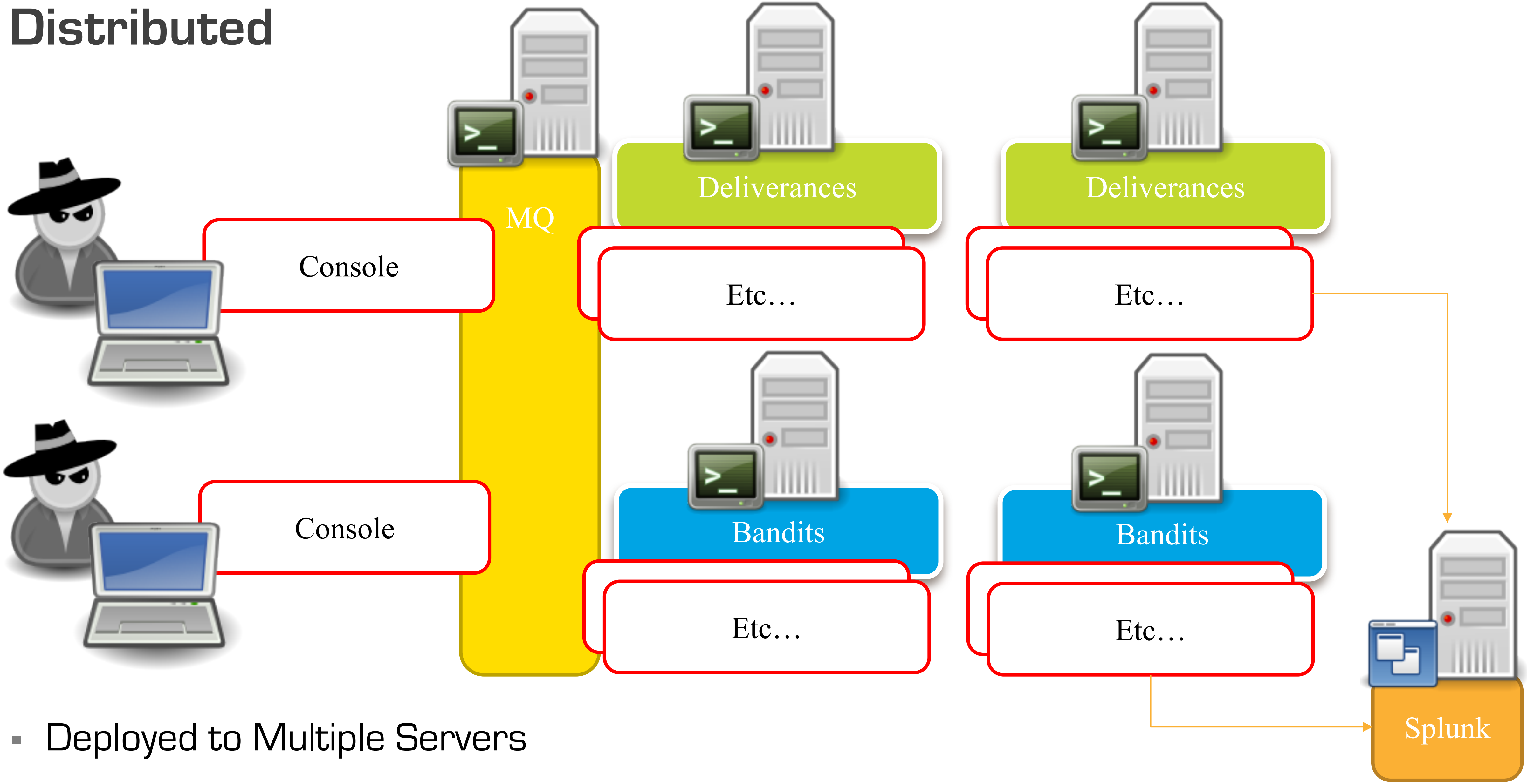


Standalone



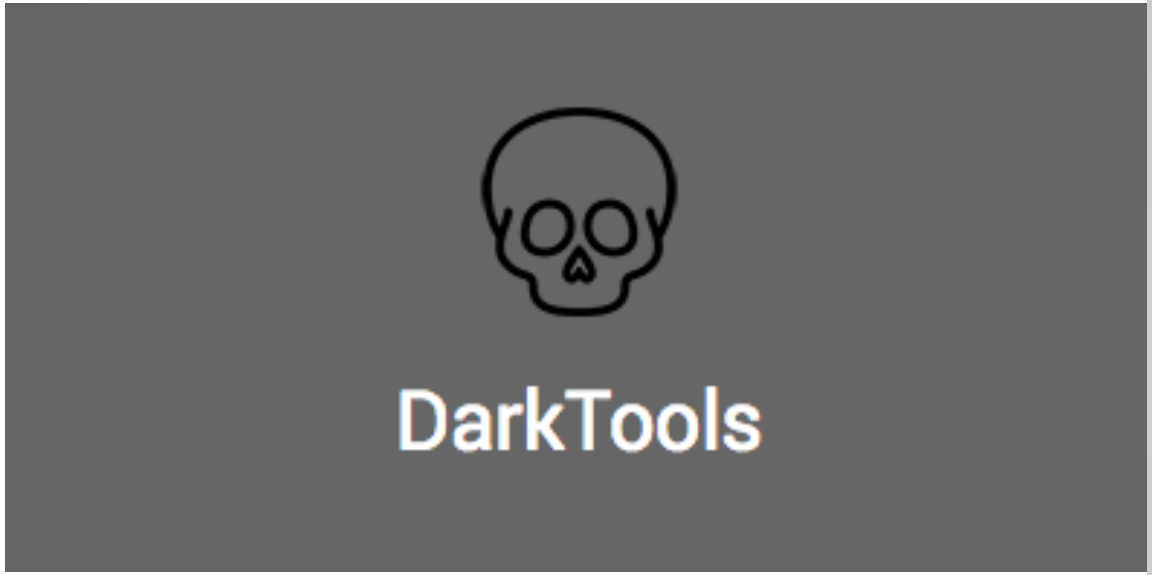
- All In One

Distributed



- Deployed to Multiple Servers

DarkTools Demo



Hipster Skelton's agree,

- it’s **easy** & **scalable**!

Future Versions

- More Modules w/ Checks
- Data Model for Splunk
- Correlation within Splunk
- Trending within Splunk
- Machine Learning ToolKit (MLTK)
- API for More Integrations
- Etc…

Questions?

@TweekFawkes

@brutes_

Requirements:

- Splunk 6.2+ – https://www.splunk.com/en_us/download/splunk-enterprise.html
- DarkTools App – https://github.com/brutes1/darktools_bh
- Sankey Diagram App – https://splunkbase.splunk.com/app/3112/
- TA-geoip – https://github.com/georgestarcher/TA-geoip

Adobe

MAKE IT AN EXPERIENCE