splunk> .conf2017

Splunking DarkTools: A Pentesters Guide To Pwnage Visualization

Bryce Kunz I Nathan Bales

September 2017 I Washington DC

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> .conf2017

Who Are We?

- Bryce
- Nathan

Buy Now!

- Acquired!

Hole in One!

- Execs Happy!

Attack Surface

- VS. the little guy!

Stubborn

- As a Mule!

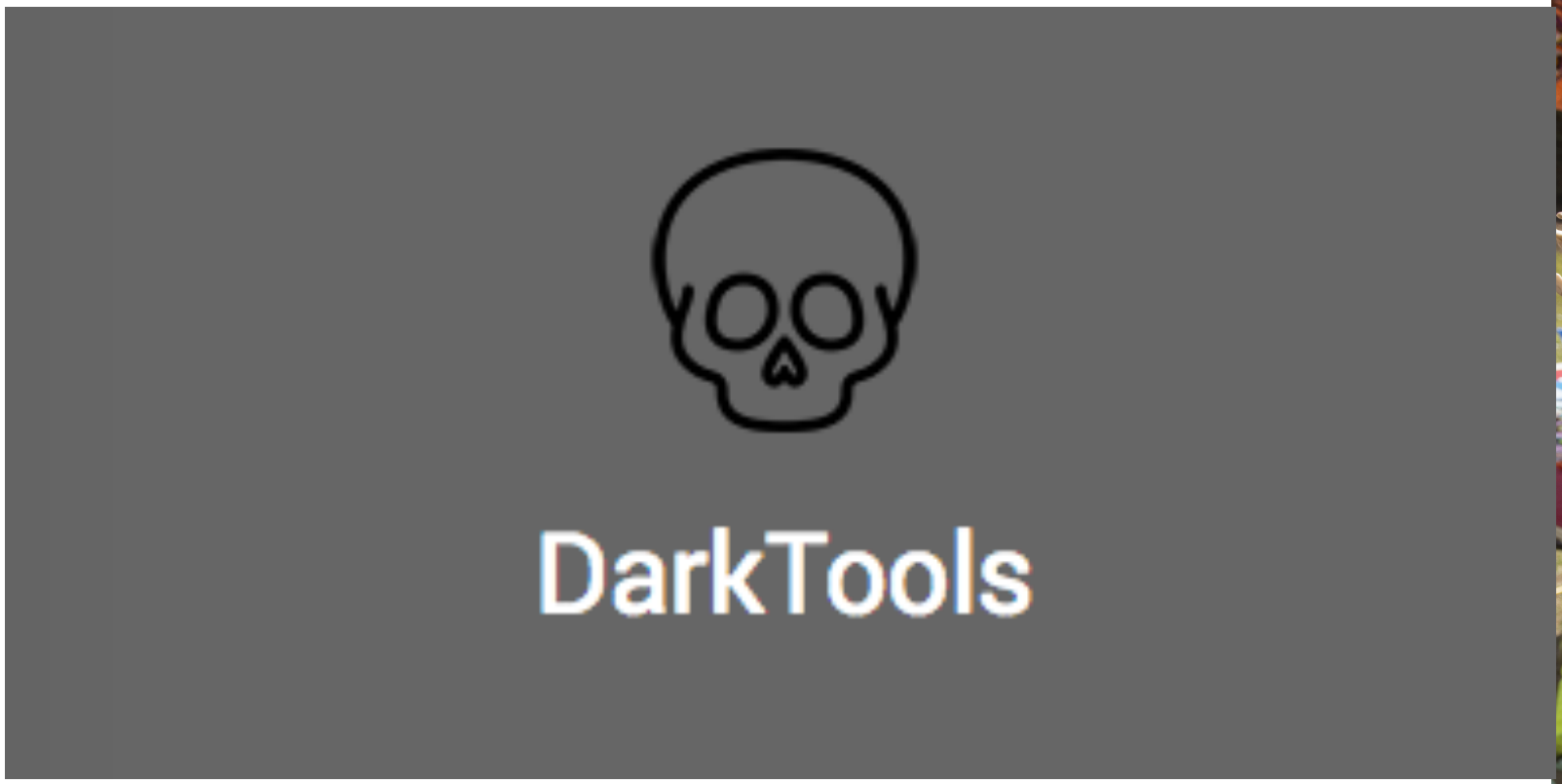
Swoop In

- To Save The Day!

Chaotic

- Lacks Integration
- Unnecessarily Hard
- Weak Scaling

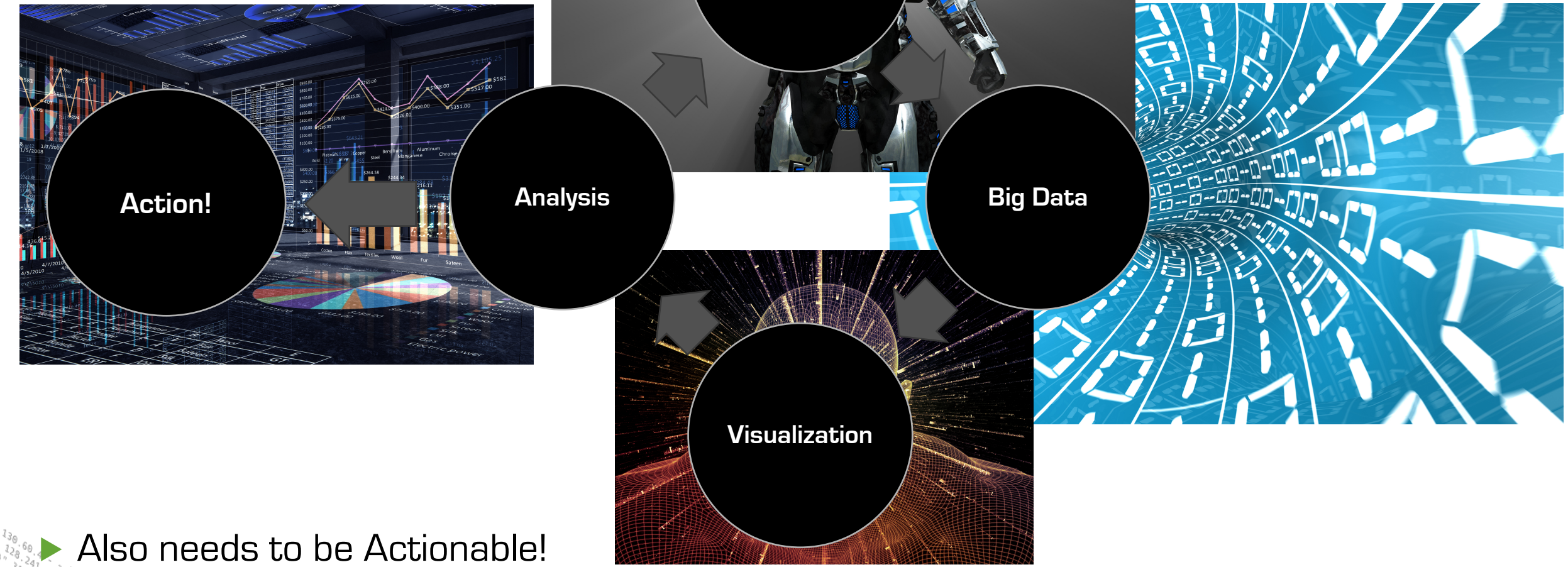
DarkTools Demo



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

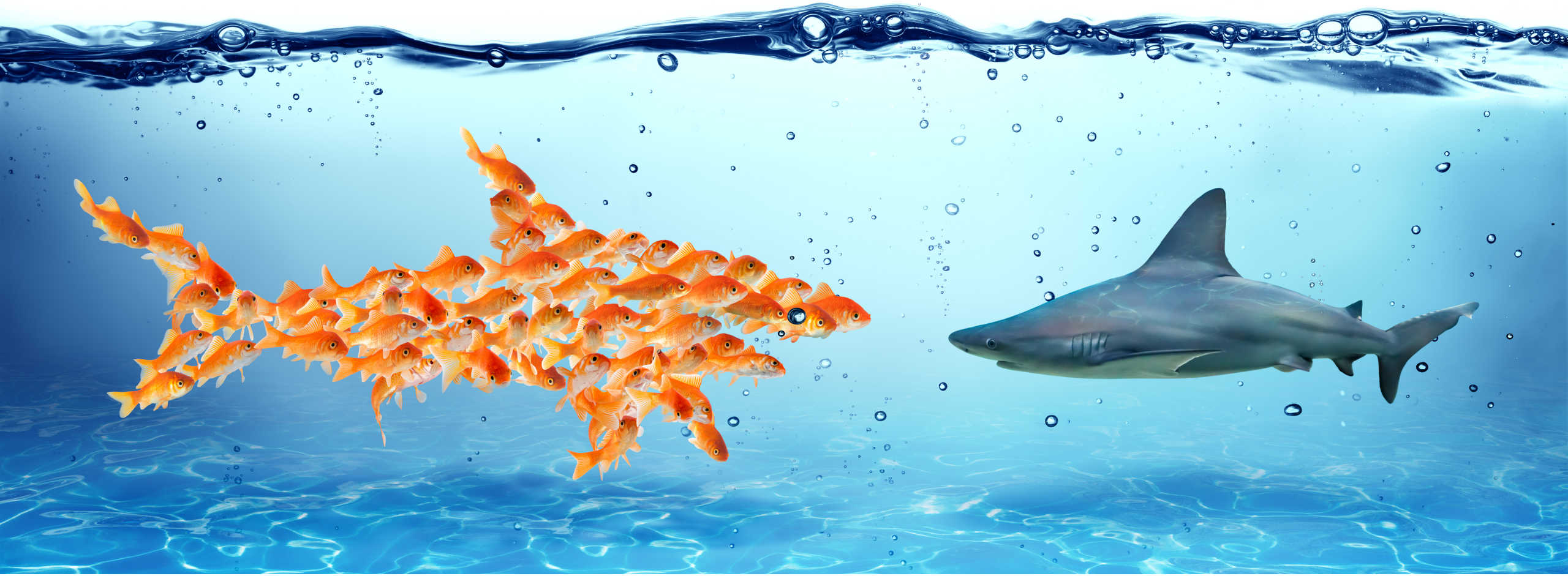
Demo 1

Together Now!



- Also needs to be Actionable!

Collaboration

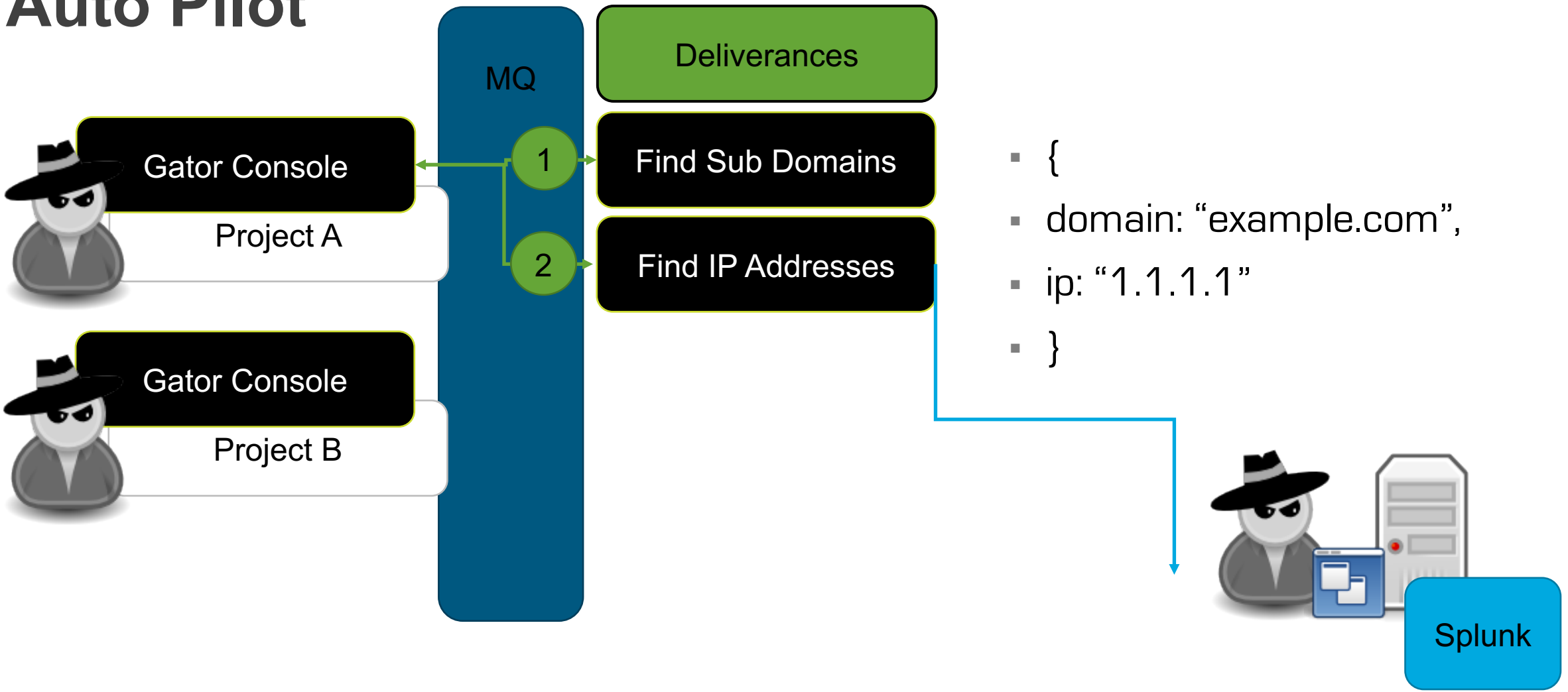


splunk> .conf2017

Visualization!

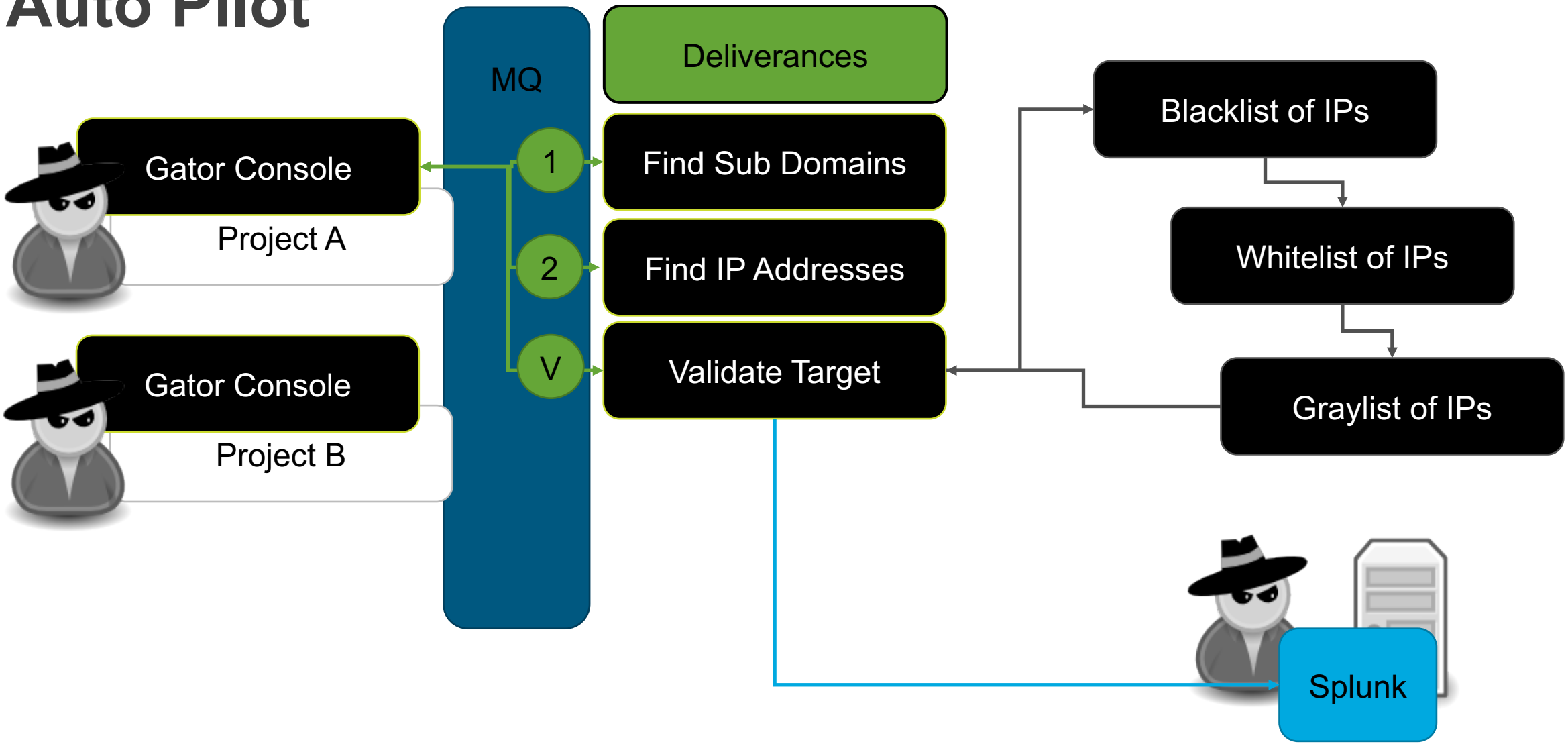
- Of Big Data!

Auto Pilot



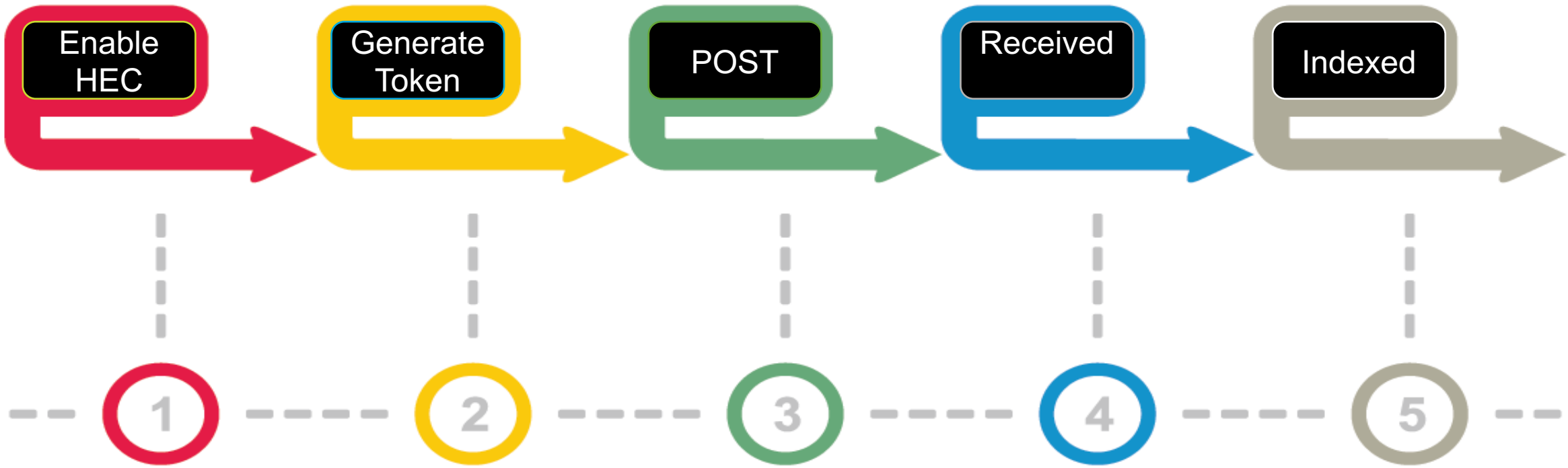
- Multiple Penetration Testers is Easy!

Auto Pilot



- Ensure targets are within scope!

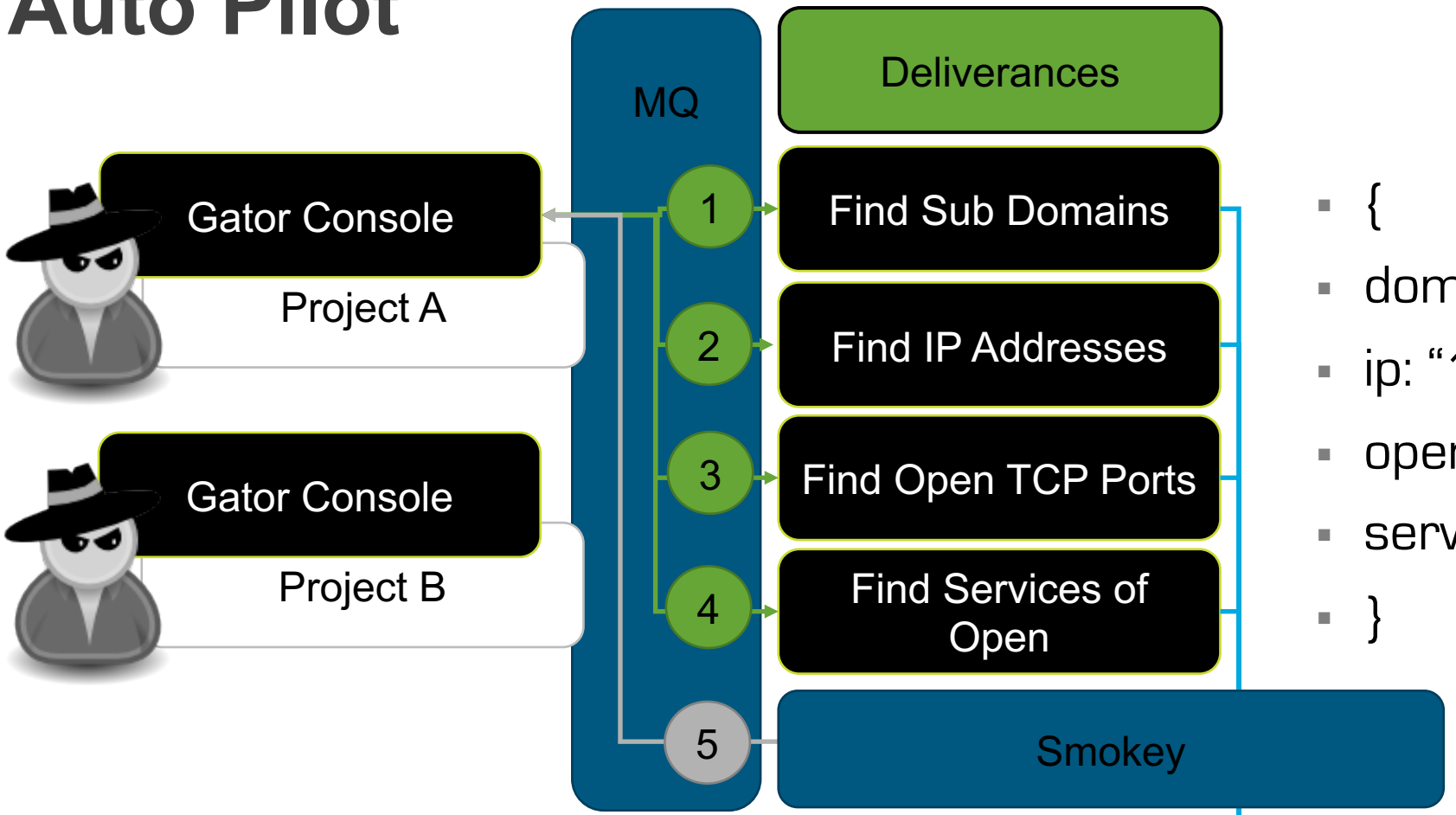
HTTP Event Collector (HEC)



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":"14999417261621nhsgtgmhkoolfhjffaguyiiflclfbuhqj"
}’

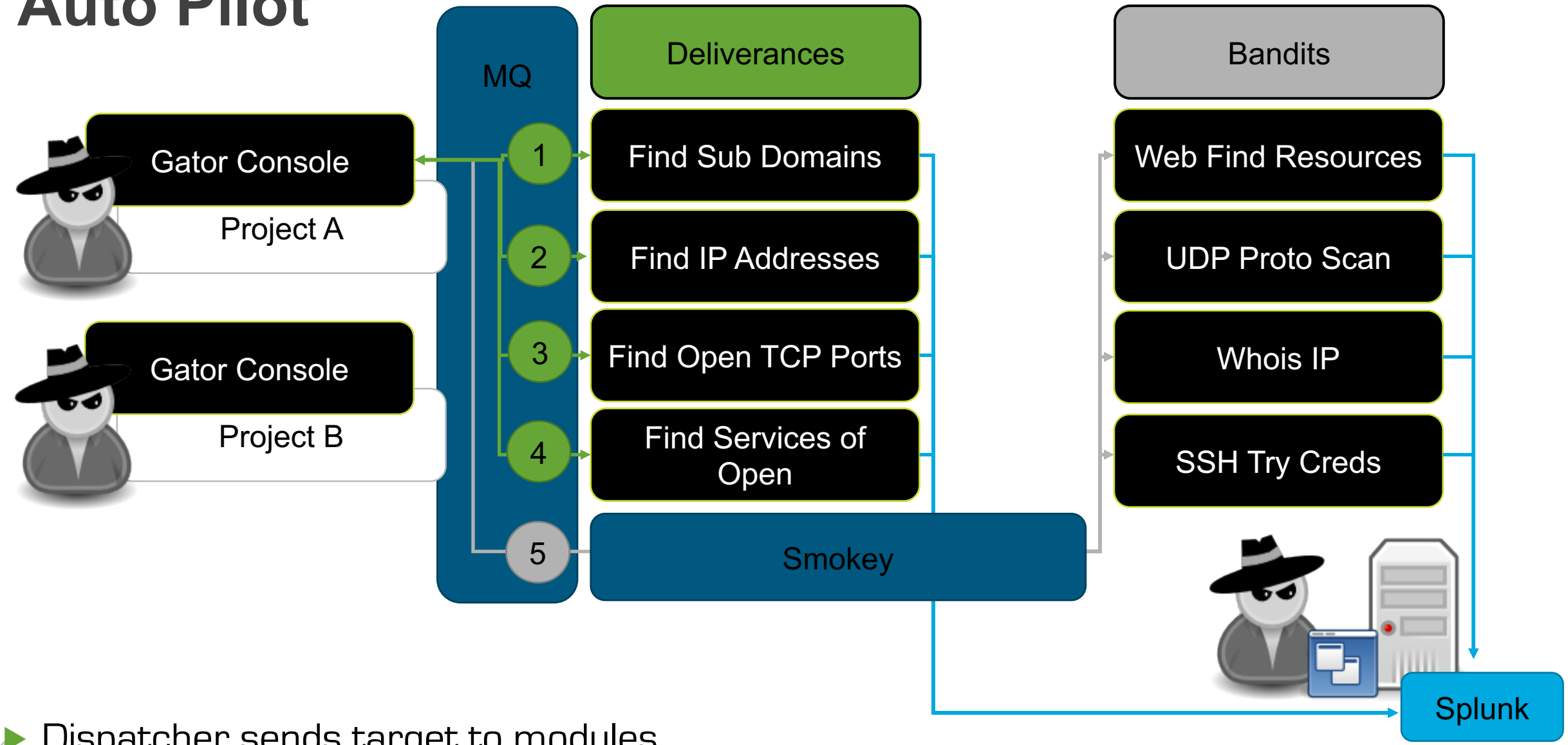
Auto Pilot



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

- Find All Open TCP Services

Auto Pilot

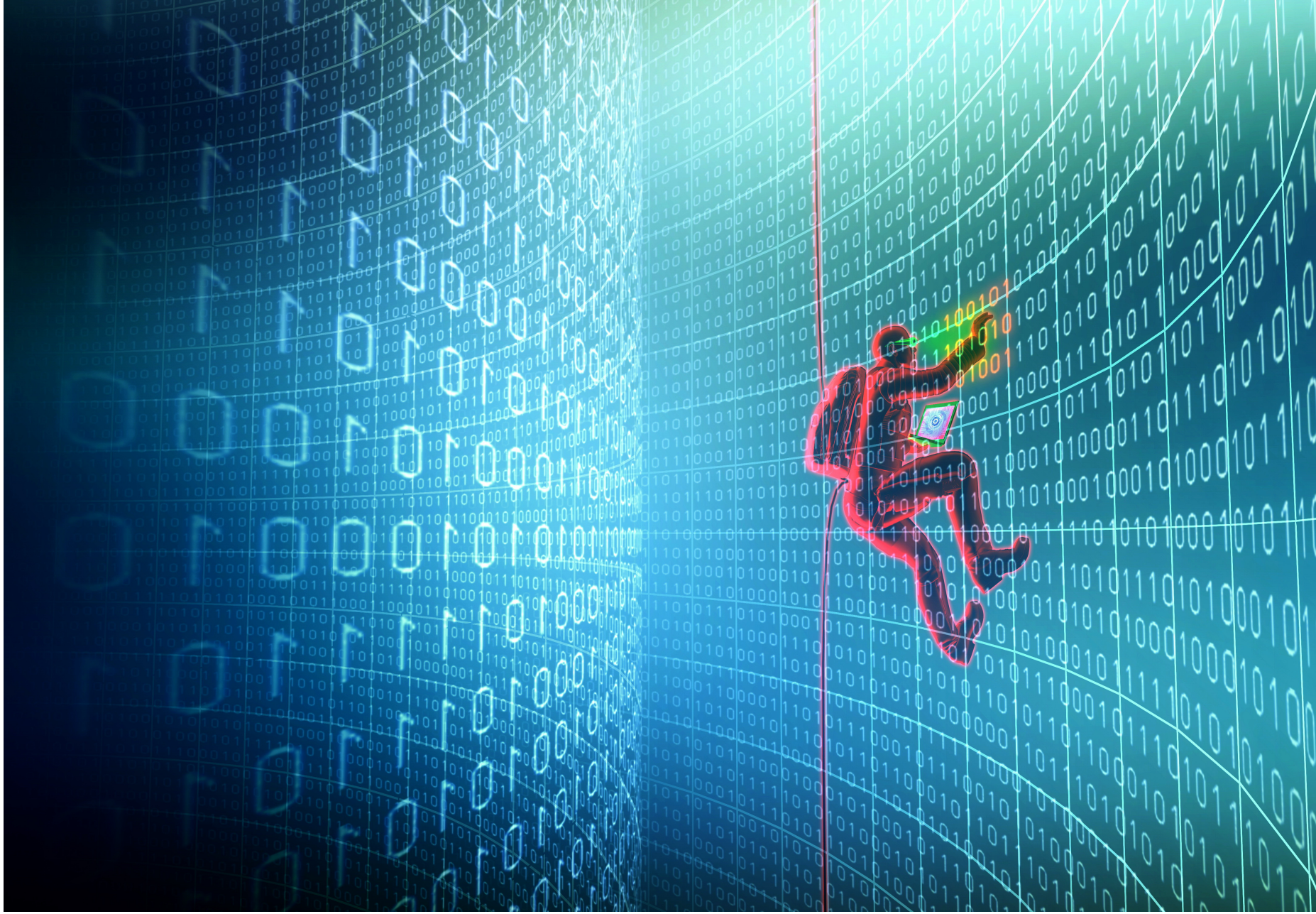


- Dispatcher sends target to modules

Why Splunk?

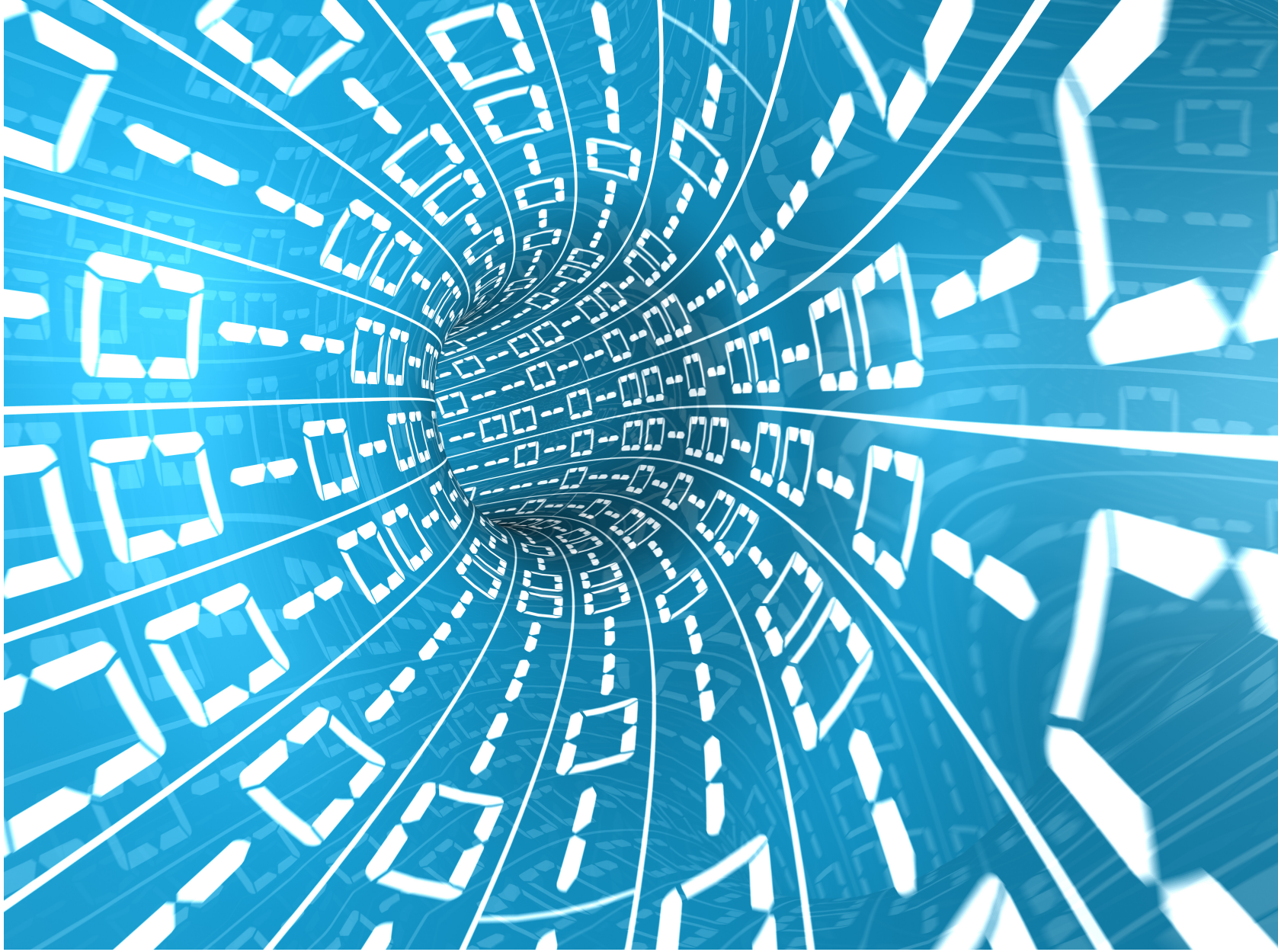
- Simple & Scalable
- Enterprise Security

- Already in use!

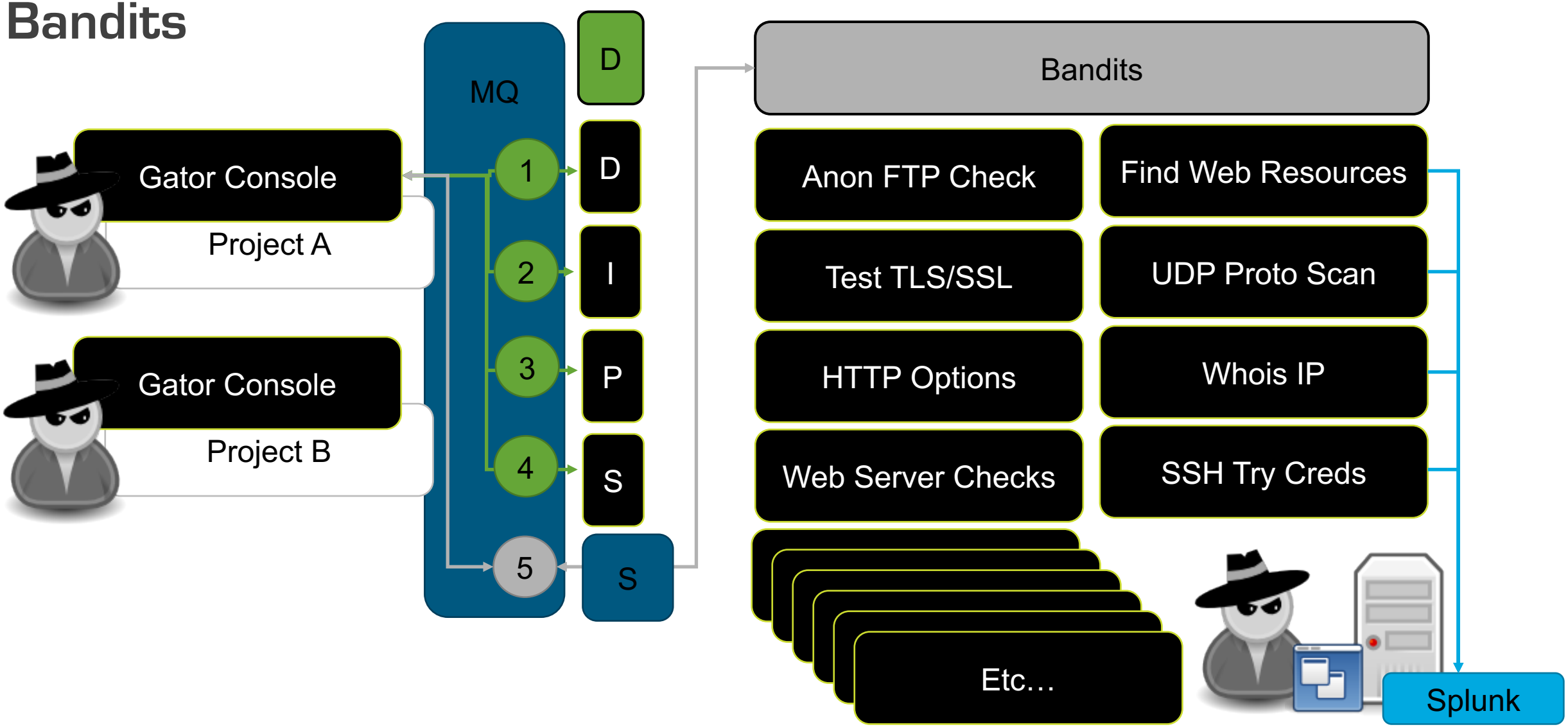


Splunk Setup

- 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:
```

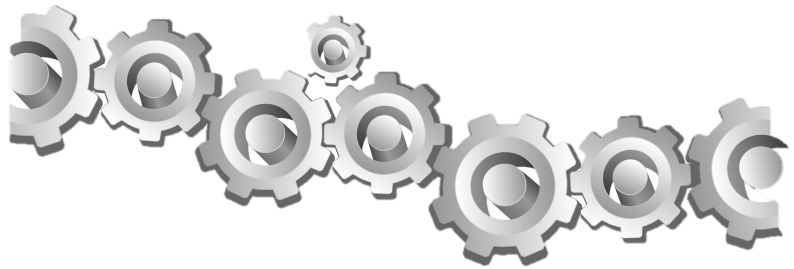
- splunkEvent() – Sends a JSON object to Splunk

```
# 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
```

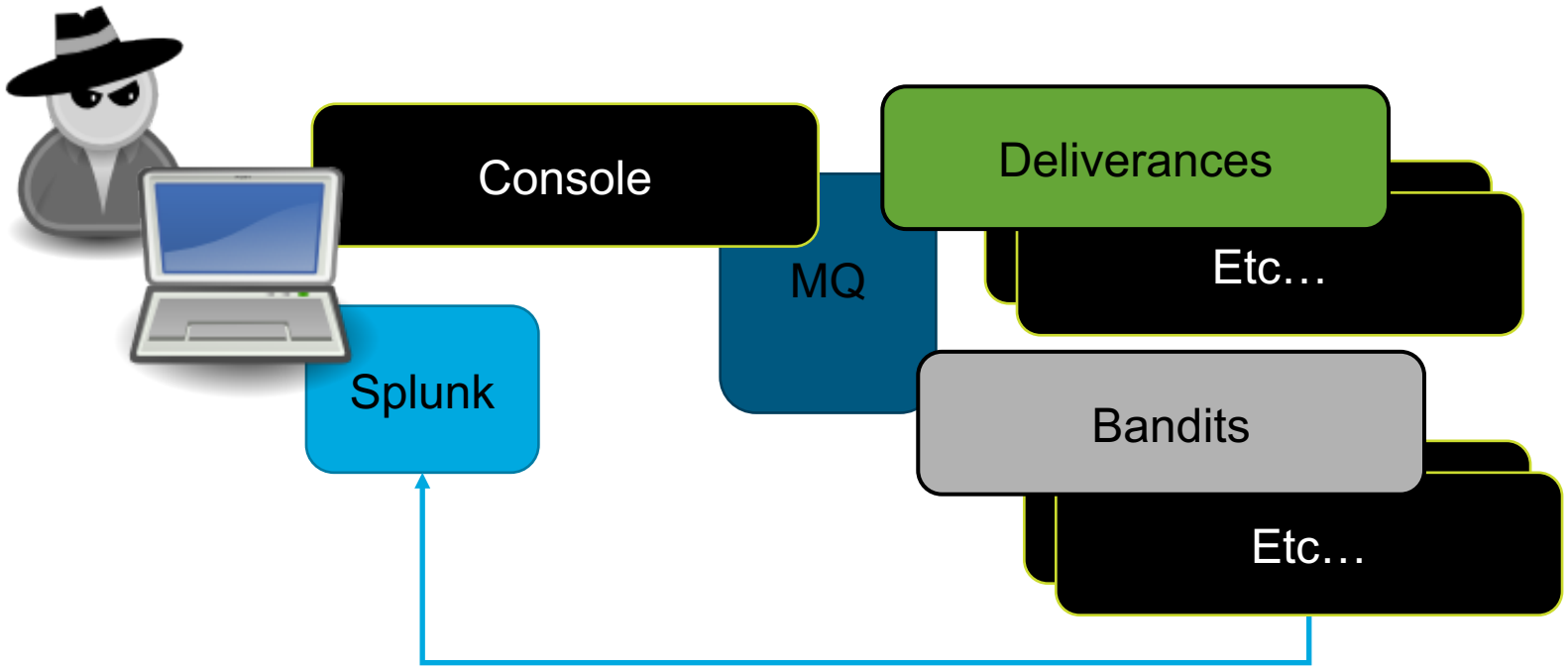
Making the Data More Usable

Field Extraction

- 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

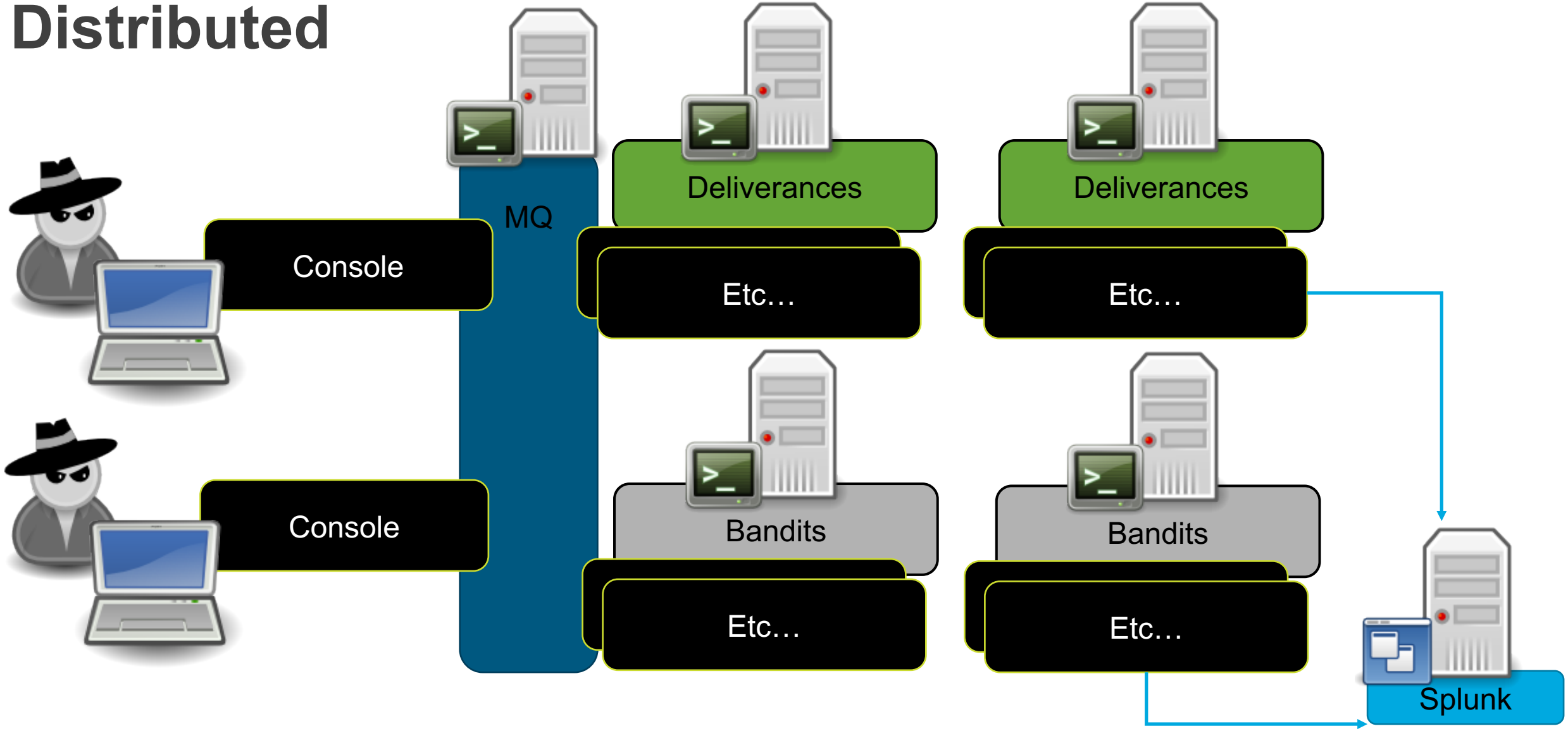


Standalone



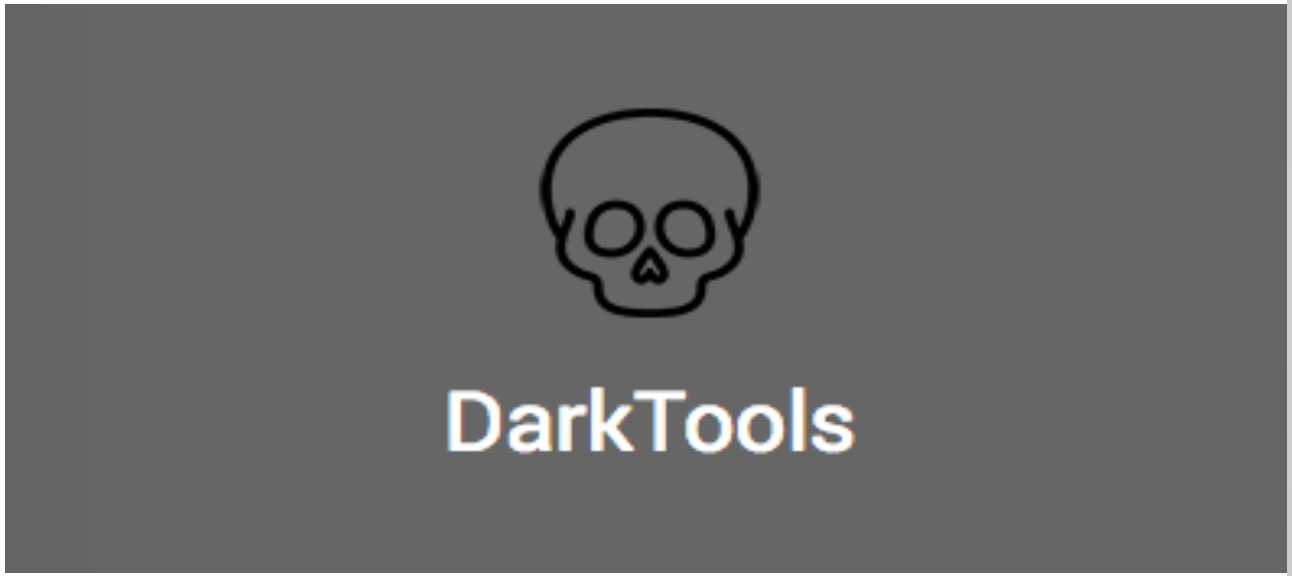
- All In One

Distributed



- Deployed to Multiple Servers

DarkTools Demo



Hipster Skelton's agree,

- It’s easy & scalable!

Demo 2

splunk> .conf2017

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

MAKE IT AN EXPERIENCE

Thank You

Don't forget to rate this session in the .conf2017 mobile app