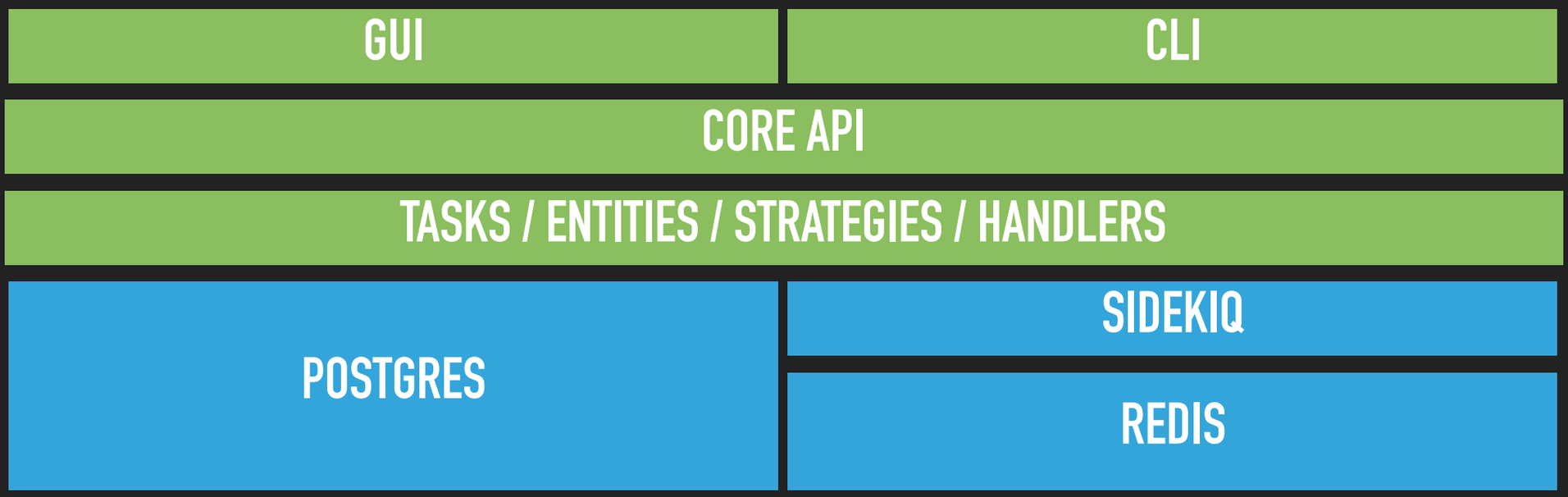
ATTACK SURFACE DISCOVERY WITH…

INTRIGUE

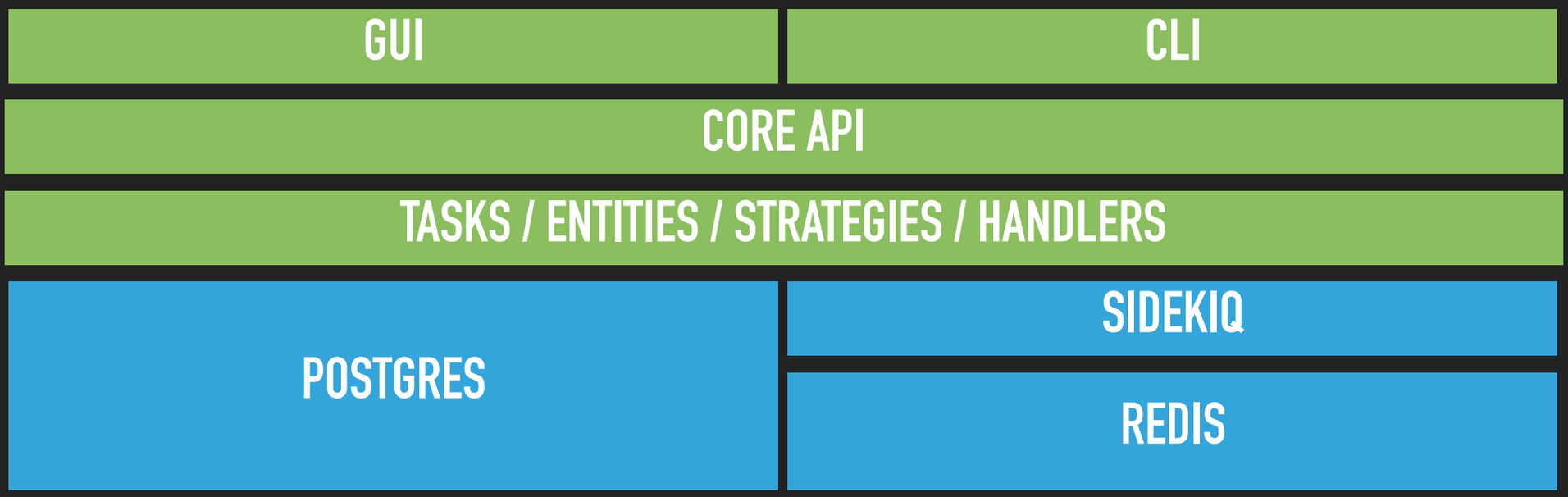
INTRIGUE IS....

- An extensible framework for automated OSINT and reconnaissance - many similar concepts to metasploit + maltego
- Oriented toward discovering organizational attack surface
- Written in (mostly) ruby, available as a Docker or AMI
- Designed for technical users
- Useful to think of -core like an engine

ARCHITECTURE



ARCHITECTURE



CORE CONCEPTS

- Entities
- Enrichment
- Tasks
- Aliasing
- Strategies

ENTITIES

- Entities are defined “things”
- Tasks can be run on an entity
- Only real requirement is that they have a **single name**
  - However, validation can include more than just the name
- Automated “enrichment” process allows us to know more about entities

```
as_number
aws_credential
aws_s3_bucket
credential
dns_record
dns_server
email_address
file
finger_server
ftp_server
github_repository
github_user
http_header
info
ip_address
mongo_service
net_block
network_service
organization
person
phone_number
physical_location
screenshot
software_package
ssh_server
ssl_certificate
string
uri
web_account
```

DEMO: CREATING & ENRICHING AN ENTITY

TASKS

- Tasks operate on allowed entities
- Either enrich existing, or create new entities
- Same concept as transforms, modules, etc in other frameworks
- May pull in data from other API (Censys, Shodan etc)
- Key method… run()

```
aws_ec2_gather_instances
aws_gather_ranges
aws_s3_brute
aws_s3_loot
convert_entity
create_entity
dns_brute_srv
dns_brute_sub
dns_brute_tld
dns_lookup_mx
dns_lookup_txt
dns_recurse_spf
dns_snoop_cache
dns_transfer_zone
email_harvest
email_validate
example
finger_extraction
ftp_banner_grab
host_geolocate
masscan_scan
net_block_expand
network_service_fuzz
nmap_scan
phone_number_lookup
search_bing
search_censys
search_edgar
search_github
search_github_code
search_opencorporates
search_phishtank
search_project_honeypot
search_shodan
search_towerdata
search_whoisology
uri_brute
uri_check_security_headers
uri_extract_metadata
uri_gather_and_analyze_lin
ks
uri_gather_robots
uri_gather_sitemap
uri_gather_ssl_certificate
uri_gather_technology
uri_http_auth_brute
uri_http_screenshot
uri_spider
uri_youtube_metadata
web_account_check
whois
whois_org_search

enrich/enrich_dns_record
enrich/enrich_ip_address
enrich/enrich_uri
enrich/
web_stack_fingerprint
```

DEMO DNS SUBDOMAIN BRUTEFORCE (TASK)

ALIASING AND META-ENTITIES

- All entities have one name in Intrigue domain model
- But what about DNS? (Or VHosts)?
- Enter... Aliasing

Page: 1 Results: 0 .. 99 previous next

name	aliases
[x] DnsRecord: mastercard.com	[IpAddress: 216.119.209.64]
[x] IpAddress: 216.119.209.64	[DnsRecord: mastercard.com]

Vs

Page: 1 Results: 0 .. 99 previous next

name
[IpAddress: 216.119.209.64] [DnsRecord: mastercard.com]

DEMO: DATA EXPLORATION

STRATEGIES

- Allow us to recursively iterate to a selected depth
- Essentially… when an entity is created, run these tasks…
- Key method: self.recurse()

```
def self.recurse(entity, task_result)
  if entity.type_string == "DnsRecord"
    unless entity.created_by?("whois")
      start_recursive_task(task_result,"whois",entity, [
          {"name" => "create_contacts", "value" => false }])
    end
  else
    task_result.log "No actions for entity: #{entity.type}##{entity.name}"
    return
  end
end
```

DEMO:

EXPLORING AN ORGANIZATION'S FOOTPRINT