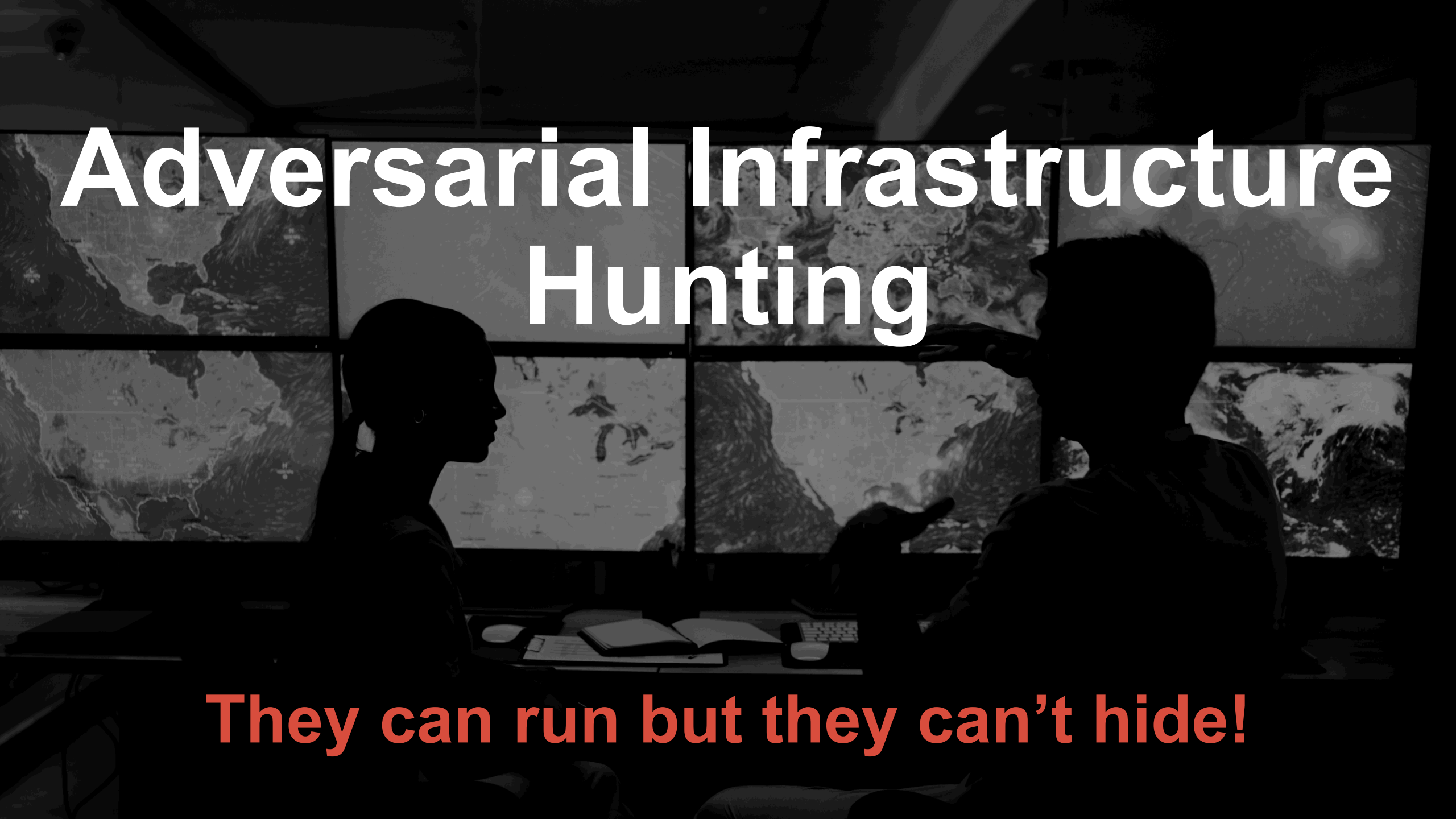

DEATH CON



Adversarial Infrastructure Hunting

They can run but they can’t hide!

whoami

Name: Gavin Knapp

Location: Wales

Background: Rugby, Cyber Security Consulting, Security Operations, Threat Intelligence

GitHub: https://github.com/m4nbat/

X: @knappresearchlb

Tool Accounts

Shodan: https://account.shodan.io/login

Virustotal: https://www.virustotal.com
- No accounts needed

Abuse.ch Hunting: https://hunting.abuse.ch
- No accounts needed

URLScan: https://urlscan.io/
No accounts needed

Infrastructure Hunting Challenge

Infrastructure-hunting.co.uk

Registration Code: 6660666

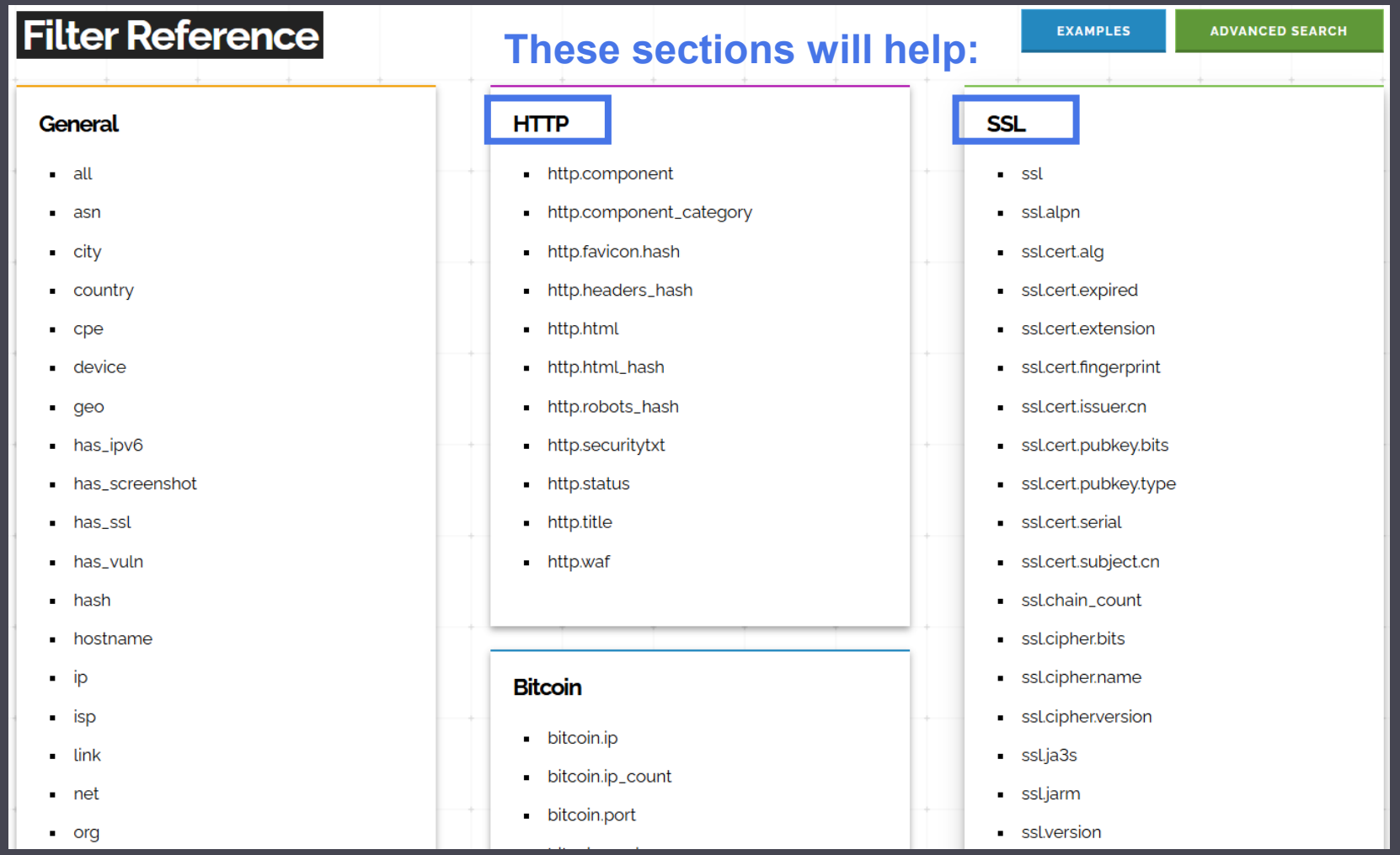
Tool Cheat Sheets and Guides

Shodan:

Search:
https://www.shodan.io/

Search Filters:
https://www.shodan.io/search/filters

Advanced Filter Search:
https://www.shodan.io/search/advanced



Filter Reference

These sections will help:

EXAMPLES | ADVANCED SEARCH

General

- all
- asn
- city
- country
- cpe
- device
- geo
- has_ipv6
- has_screenshot
- has_ssl
- has_vuln
- hash
- hostname
- ip
- isp
- link
- net
- org

HTTP

- http.component
- http.component_category
- http.favicon.hash
- http.headers_hash
- http.html
- http.html_hash
- http.robots_hash
- http.securitytxt
- http.status
- http.title
- http.waf

Bitcoin

- bitcoin.ip
- bitcoin.ip_count
- bitcoin.port

SSL

- ssl
- ssl.alpn
- ssl.cert.alg
- ssl.cert.expired
- ssl.cert.extension
- ssl.cert.fingerprint
- ssl.cert.issuer.cn
- ssl.cert.pubkey.bits
- ssl.cert.pubkey.type
- ssl.cert.serial
- ssl.cert.subject.cn
- ssl.chain_count
- ssl.cipher.bits
- ssl.cipher.name
- ssl.cipher.version
- ssl.ja3s
- ssl.jarm
- ssl.version

Tool Cheat Sheets and Guides

URLScan:

Help with searches: navigate to https://urlscan.io/search/#* and click the “Help” button as illustrated below:

Search for domains, IPs, ASN, and Hashes etc.

Help & Examples

Attention: Consult the Search API Reference for searchable fields and additional tips.

- Search requests (through the UI or API) are subject to your individual Search API Quotas. Make sure to use your API key.
- The query field uses the ElasticSearch Query String to search for results.
- All queries are run in filter mode, sorted by date with the more recent scans first. There is no scoring of search results.
- You can group and concatenate search-terms with brackets `( )`, `AND`, `OR`, and `NOT`. The default operator is `AND`.
- You can concatenate terms within a group, e.g. `page.domain:(foo.com OR bar.com)`.
- **Always** use the field names of the fields you want to search. Wildcards for the field-name are **not** supported! Field names are **case sensitive**!
- **Always** escape reserved characters with backslash: `+ - = && || > < ! ( ) { } [ ] ^ " ~ * ? : \ /`
- **Limit** the time-range if possible using `date`, e.g. `date:>now-7d` or `date:>now-1y`.
- The `date` allows relative queries like `date:>now-7d` or range-queries like `date:[2020-01-01 TO 2020-02-01]` or both combined.
- You can only use leading wildcard searches and regular expression searches on supported fields, and only as a signed-in user.
- Everything is indexed as **lowercase**, even if the Search API returns values in a case-preserving manner.
- Regular expressions are always anchored to beginning/end of the tokens (implicit ^ and $). Make sure to prefix/suffix with `.*` to match infix strings.
- Domain fields contain the whole domain and each smaller domain component, i.e. `domain` can be searched by *google.com* which will find hits for *www.goo*

Examples - Common searches and multiple query terms combined

- page.ip:* AND date:>now-7d Non-empty scans in the past seven days
- page.url.keyword:https\:\/\/www.paypal.com\/* Page URL Prefix search
- domain:paypal.com AND NOT page.domain:paypal.com Domain was contacted but isn't the page/primary domain
- page.domain:(paypal.com~ AND NOT paypal.com) Fuzzy Search for domain name (excluding the legitimate domain)
- page.domain:(/payp.*/ AND NOT paypal.com) Regex Search for domain name (excluding the legitimate domain)
- page.ip:(148.251.0.0\/16 AND NOT 148.251.45.170) AND date:[2018 TO 2019] IP from subnet excluding one particular IP, seen in 2018
- page.asn:AS24940 OR page.asnname:hetzner Page hosted on this AS, search by ASN or AS Name (**Note**: Search with 'AS' prefix!)
- page.url:"wp-content/uploads/" OR filename:"wp-content/uploads/" AND date:>now-1M Path `wp-content/uploads` either in page.url or by subrequest
- hash:d699f303... A resource with this SHA256 was downloaded

Tool Cheat Sheets and Guides

Virustotal: https://www.virustotal.com