



## USE CASES

Identifying search terms and mapping to alerts

# IDENTIFYING SEARCH TERMS AND MAPPING TO ALERTS

- › The purpose of this module is to elaborate on use cases already raised in the sales modules and link them up to Skurio core packages and alert templates.
- › Some guidance is provided on gather search terms, including an exercise encouraging you to complete some open source research to identify search terms related to your company.

# PROTECT YOUR DATA, WHEREVER IT LIVES.

## Four categories of data

Staff

- Corporate networks
- Cloud Apps
- Shadow IT

Infrastructure

- Servers
- Sites & Apps
- Domains & IP addresses







Customers

- Personal Information
- Login Details
- Transactions

Business

- Source Code
- Intellectual Property
- Trade Secrets

# SEARCH TERM CATEGORIES

 <h3>Email Addresses</h3> <p>Use the email address template to monitor for potentially compromised email addresses belonging to your organisation.</p> <p>Let's go</p>	 <h3>IP Addresses</h3> <p>Use the IP address template to monitor for single IPs or IP ranges belonging to you that appear on any of our sources.</p> <p>Let's go</p>	 <h3>Keywords</h3> <p>Use the keyword template to search for your company and product names, or other text strings which identify your data.</p> <p>Let's go</p>
 <h3>Domains</h3> <p>Use the domains template to monitor for mentions of domain names that appear on any of our monitored channels.</p> <p>Let's go</p>	 <h3>Financial Information</h3> <p>Use the financial template to identify any credit or debit cards that may belong to you using our pattern matching interface.</p> <p>Let's go</p>	 <h3>Typosquatting</h3> <p>Monitor for newly registered domains similar to your own, which could be used for phishing, fraud or to impersonate your brands.</p> <p>Let's go</p>

**NEW!**

# USE CASE MAPPING TO ALERTS

Skurio Alerts	Login Credentials	Assets & Infrastructure	Employee Data	Customer Data
Email Addresses	Corporate email domain	User principal names (UPN) Specific email addresses used to authenticate to systems	VIP personal email addresses*	
IP Addresses		IPv4 addresses		
Domains	Web domains of services holding credentials	Corporate email domain Web domains Sub domains Fully qualified server names (FQDN)	Web domains of services holding employee data	
Keywords	Names of third-party services holding credentials	Your company names(s) Database column/field information IPv6 addresses Unique keywords or phrases describing business critical systems Known unpatched vulnerabilities (CVEs)	Your company name(s) Database column/field information	Your company names(s) Database column/field information
Financial Information			VIP credit card IIN/BIN with supporting identifying keywords	Loyalty card IIN/BIN
Typosquatting		Web domains Product/service names		
BreachMarker			Synthetic identities**	Synthetic identities**

\* With permission from VIP

\*\* Create synthetic identities as BreachMarkers in Skurio platform then insert into database

# GATHERING SEARCH TERMS

- › IT department:
  - › IT asset lists
  - › Database structures
- › Customer web sites
  - › 'About us' page – board/executive, physical addresses
  - › Corporate affairs to explore wider company structure
- › Risk & compliance personnel
  - › Information asset registry
- › Open-source research (OSINT)
  - › e.g., DNSDumpster for sub-domains, IP addresses

# GATHERING SEARCH TERMS

## Exercise

- › Use your company as an example:
  - › What are the names of products and services that are potentially vulnerable?
  - › Who are the VIPs?
  - › What physical addresses are associated to the company?
- › Navigate to DNS Dumpster <https://dnsdumpster.com/> (or similar)
  - › Use your web domain to identify company infrastructure
  - › Export results and use the output to try and work out what IP addresses are associated to shared/public resources (such as Microsoft/Outlook) and what are directly related to your organisation (such as [www.skurio.com](http://www.skurio.com))



THANK YOU

COMMERCIAL IN CONFIDENCE