Knowledge Management

Nourishing & Enhancing your communication and intelligence.

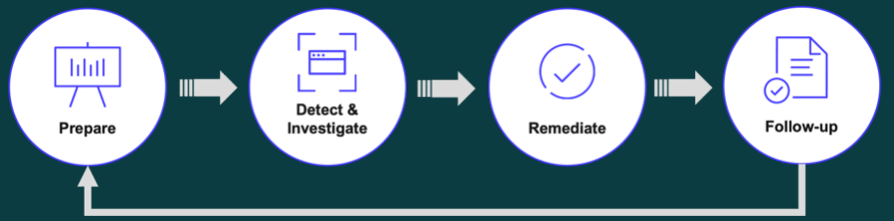
Rebecca Lois Taylor (Secureworks®, United Kingdom)

Rebecca Taylor | LinkedIn

8

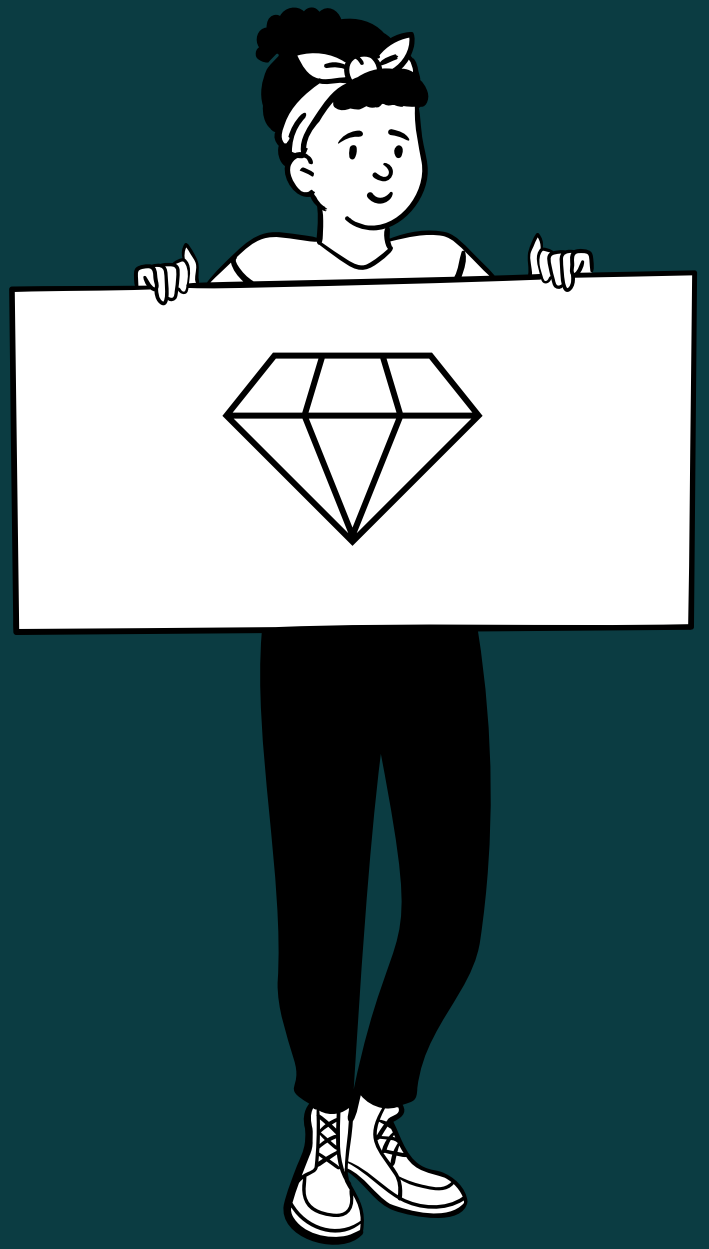
Secureworks®

WOMEN IN TECH EXCELLENCE AWARDS 2022 Nominee



Todays Topics

- Key Constructs
- Reactive incidents – Workstreams and Data Management
- Safe communications
- Toolkits, procedures and spin ups
- Embrace your new ‘intelligence’
- Q&A



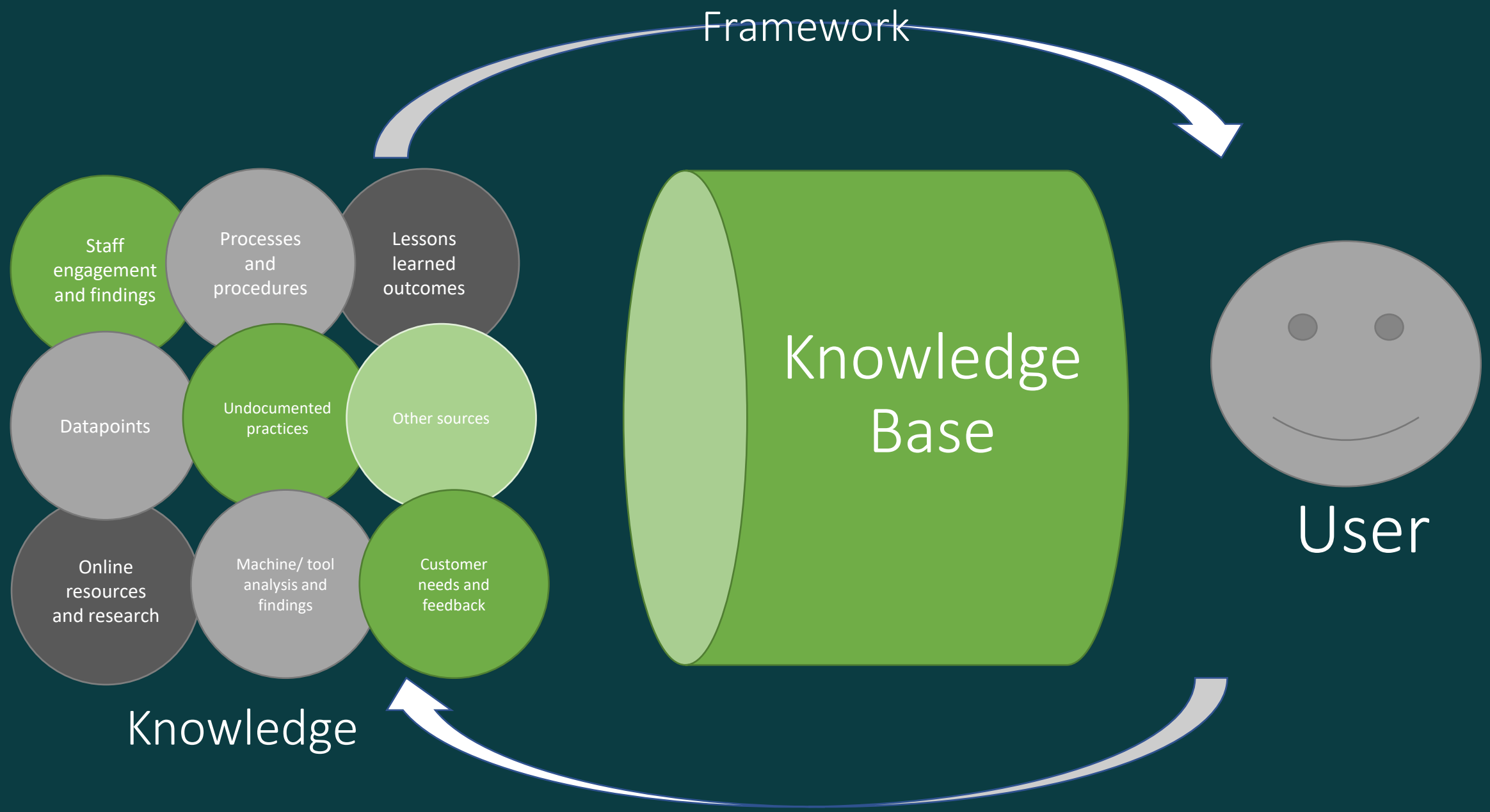
"An investment in knowledge, pays the best interest"

Benjamin Franklin

What is Knowledge Management?

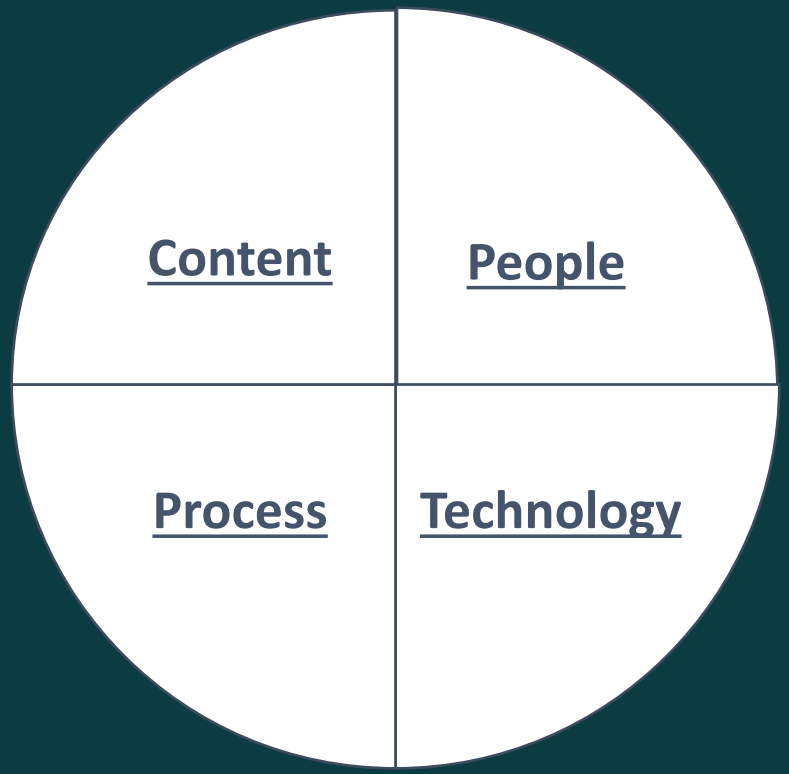
‘Knowledge management is the **process of more effectively collecting, sharing, maintaining or managing, and deploying organizational knowledge**. As a discipline, knowledge management recognizes three basic forms of knowledge: explicit knowledge, tacit, and implicit knowledge’

Source: Heavy AI



Facilitate **knowledge creation** and **sharing** via a rich user experience that motivate employees to **contribute through reward and recognition** initiatives, aligned to objectives.

Create a **measurable** increase in productivity and performance effectiveness by **connecting people** to people and associated knowledge.



Create an environment that supports the identification of opportunities or problems to **trigger knowledge processes** that enable organizational learning

Leverage knowledge technologies which provide **rich user experiences** and **simplify access** to people, information and knowledge relevant to the business need, to drive long term value and incentivize.

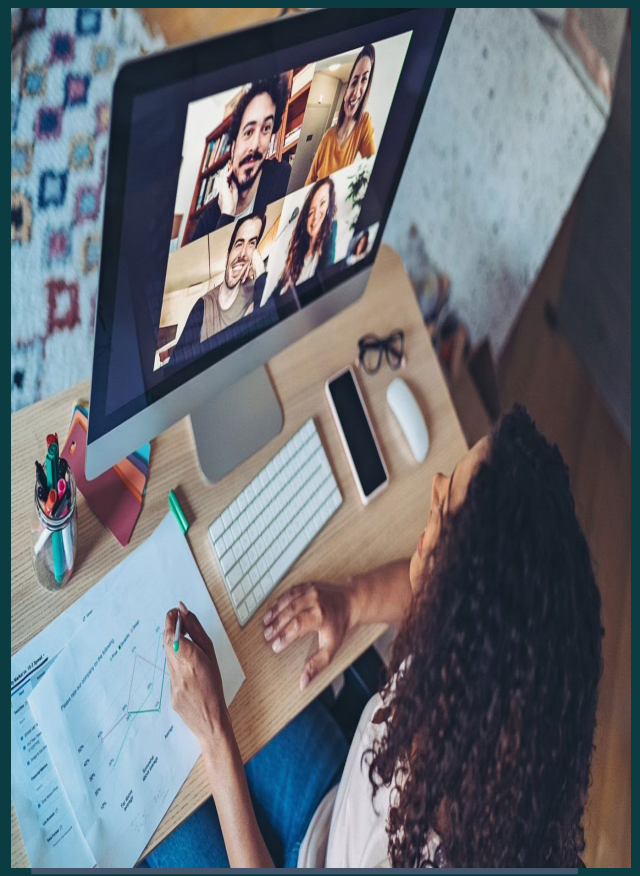
Framework

Important to note…

- MANY frameworks and tools available which include content management.
  - Master Data Management
- Ultimately every business transaction requires reliable information.
- Small changes can make an immediate difference.
- Often, we already have tools and methods in house we can utilize for better knowledge management.

Barriers

Privacy



Control

Purpose

Motivation

Change

“Knowledge is of no value
unless you put it into practice”

Anton Chekhov

Priorities

Communication

Tempo/SLAs

Communication Plans

Critical Findings

Boundaries

Governance

- Notification or disclosure requirements
- Supporting documents and specific investigations

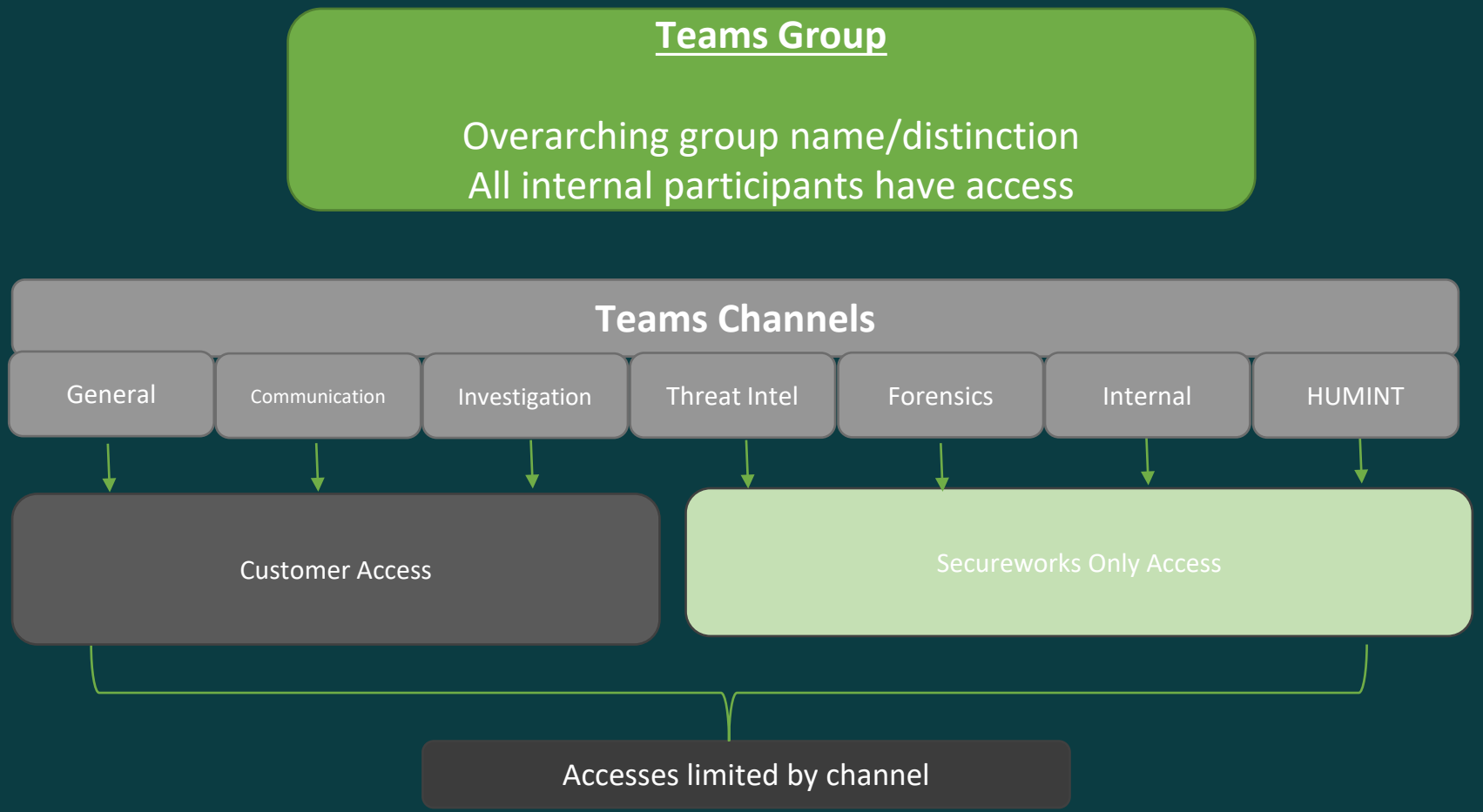
Insurance

- Caveats
- Notification responsibilities
- Reporting
- Approved IR provider

Legal

- Frameworks and notifications
- Privilege
- Litigation preparation
- Law Enforcement

Workstreams



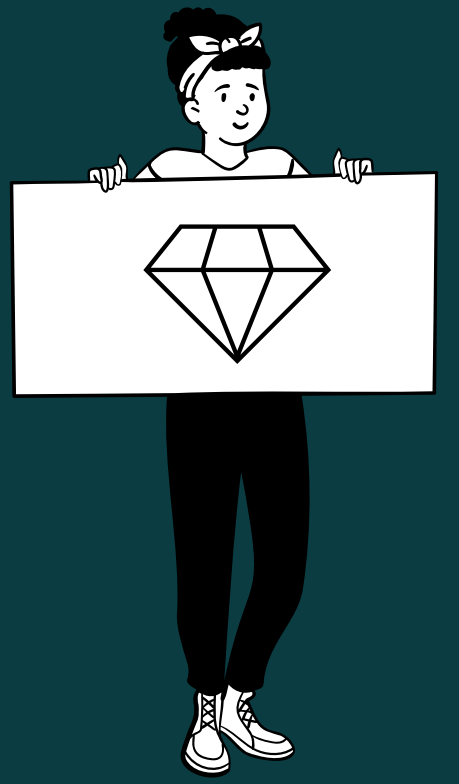
Templates

- Templates for collaboration instances and customer facing materials.
  - **Get them pre-approved!**

- Templates for data collection and information sharing-
  - Time Trackers and Employee Details.
  - Contacts and Reasonable Adjustments.
  - Indicator of compromise trackers/ Tasks Trackers.
  - Threat actor traits and timelines.
  - Intelligence Intake Forms.

Knowledge and Intelligence

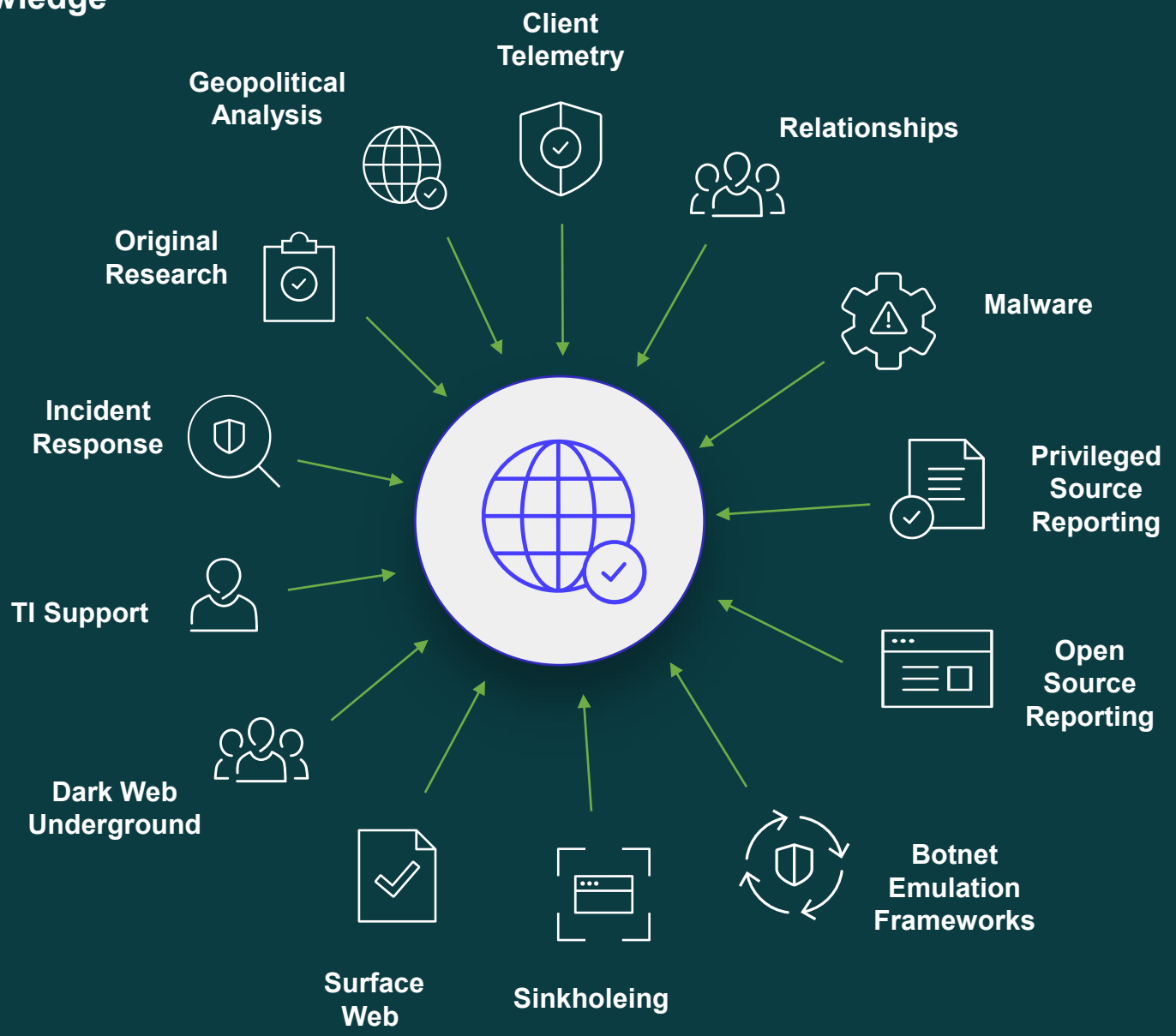
- What information do we need to be capturing and where?
- How can this benefit both/other organisations?
- What are the workstreams and my expectations of them?
- How do we collaborate?
- How do I connect the dots?



Always assess if there are any gaps, new desires or changes – Review your templates and the answers to these at least quarterly

Data → Investigations → Knowledge

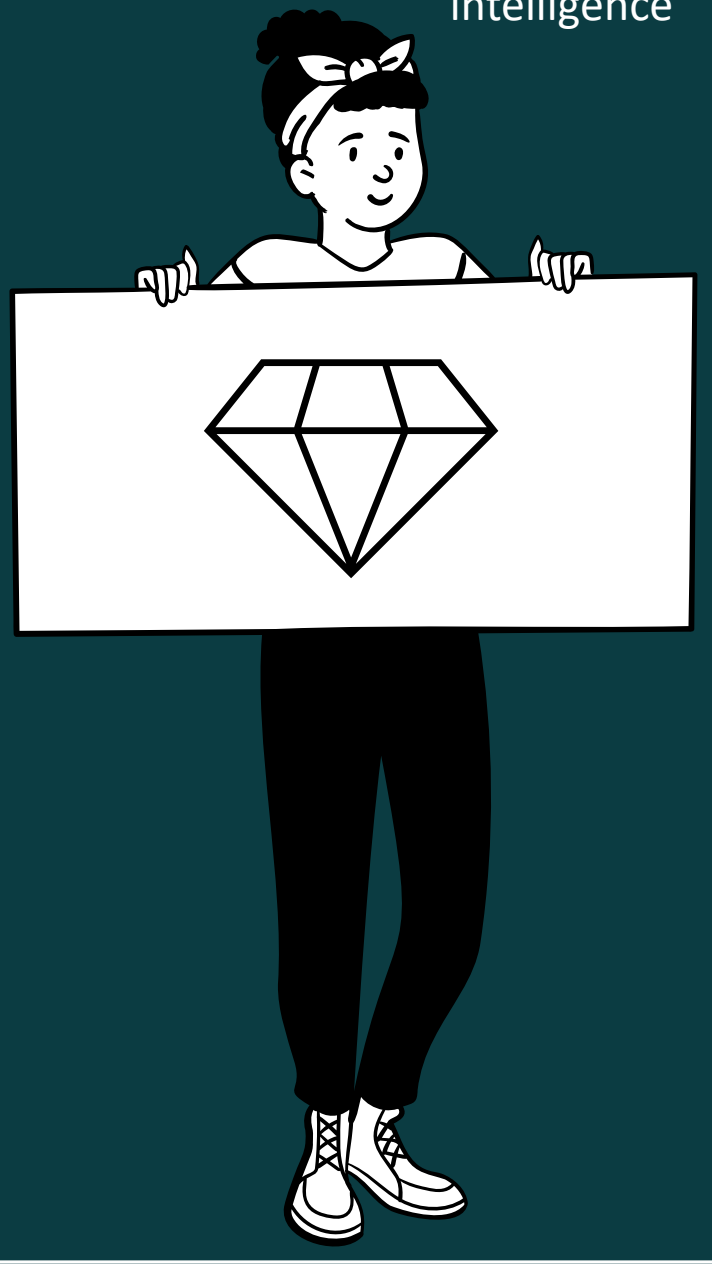
Embracing your intelligence



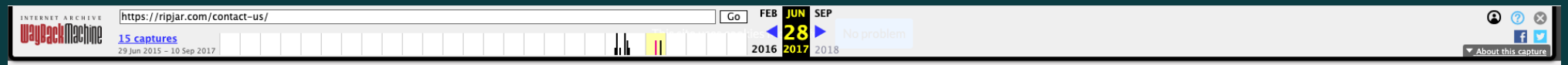
Ok…

So I collect these raw datapoints you have called out…

What could it become?
What could I gain?
Where could these gems go?



Embracing your intelligence



ripjar

HOME PLATFORM SOLUTIONS CAREERS ABOUT LOG IN

Ripjar was founded by a team of talented engineers from the UK Government who have been successfully discovering actionable insights in complex data for many years

We have used these skills to create an unrivalled visualisin

Contact Addresses

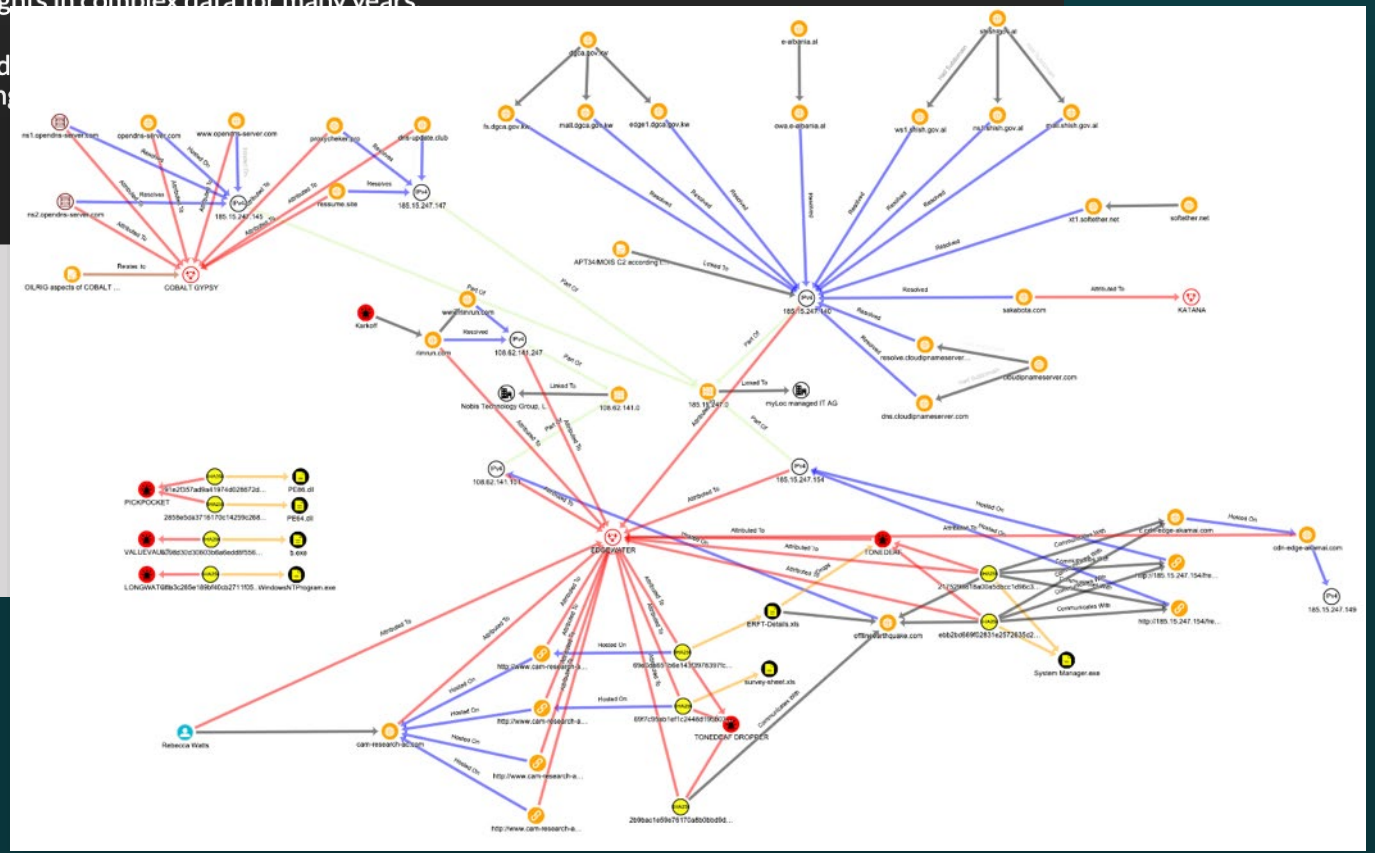
Sales: sales@ripjar.com

Sales: +44 203 198 2250

Cheltenham Office: +44 1242 312052

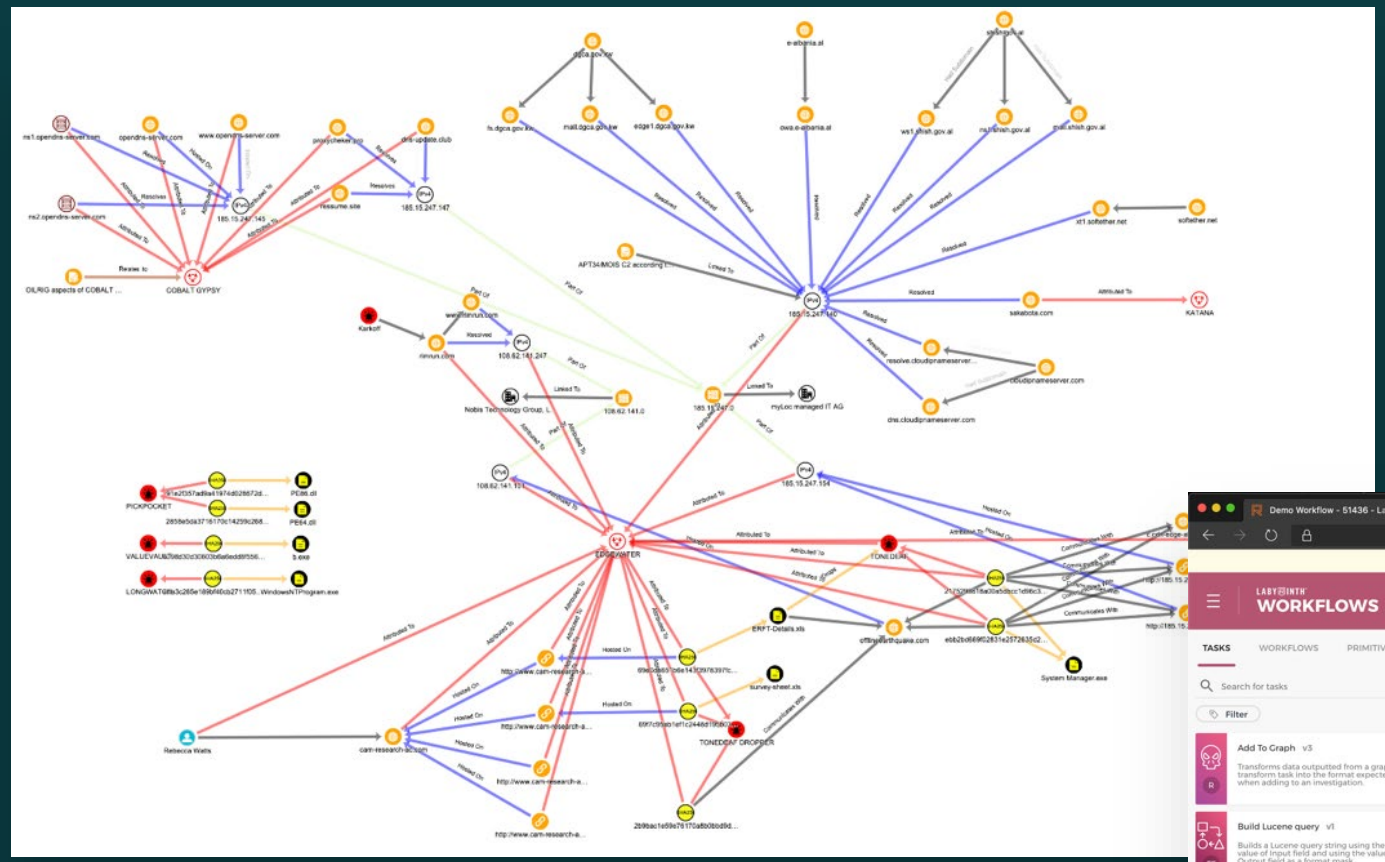
Support: +44 333 300 1295

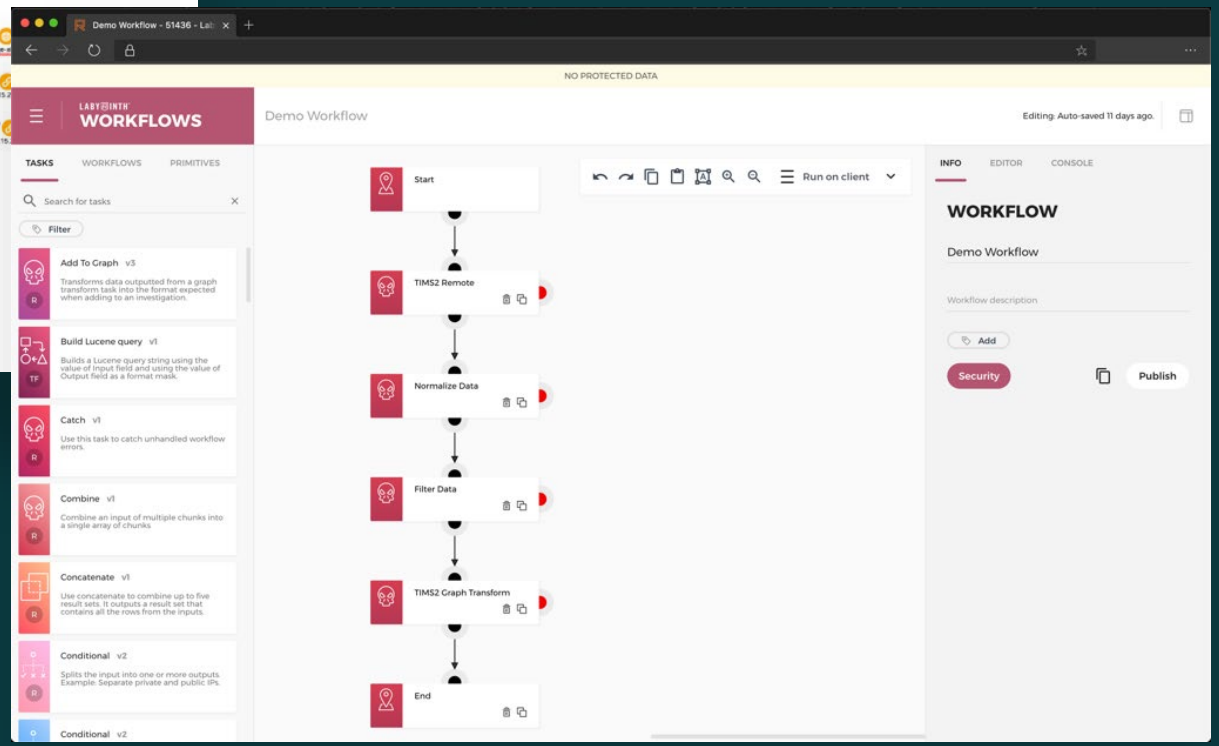
Jobs: jobs@ripjar.com



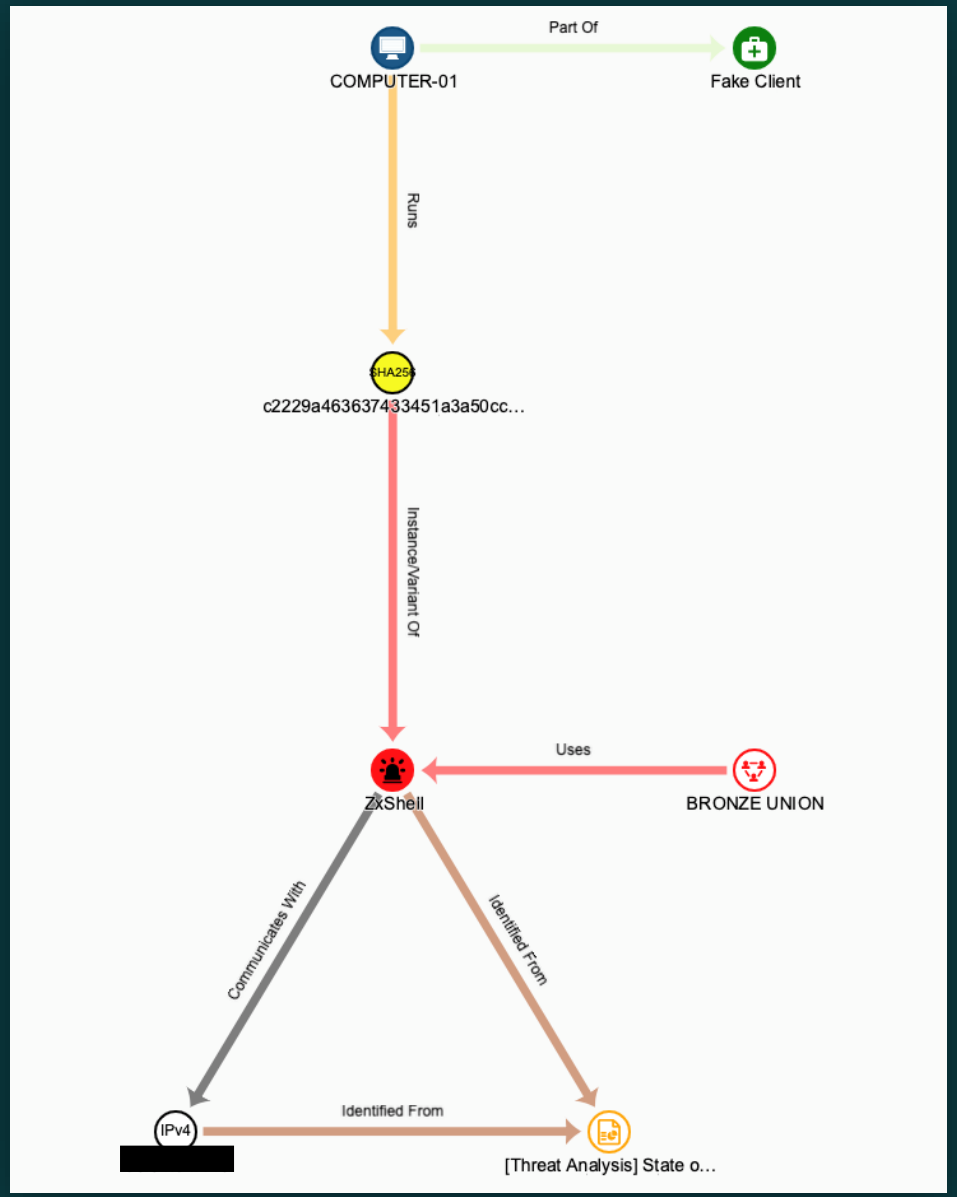
TIMS

Mapping of telemetry and datapoints



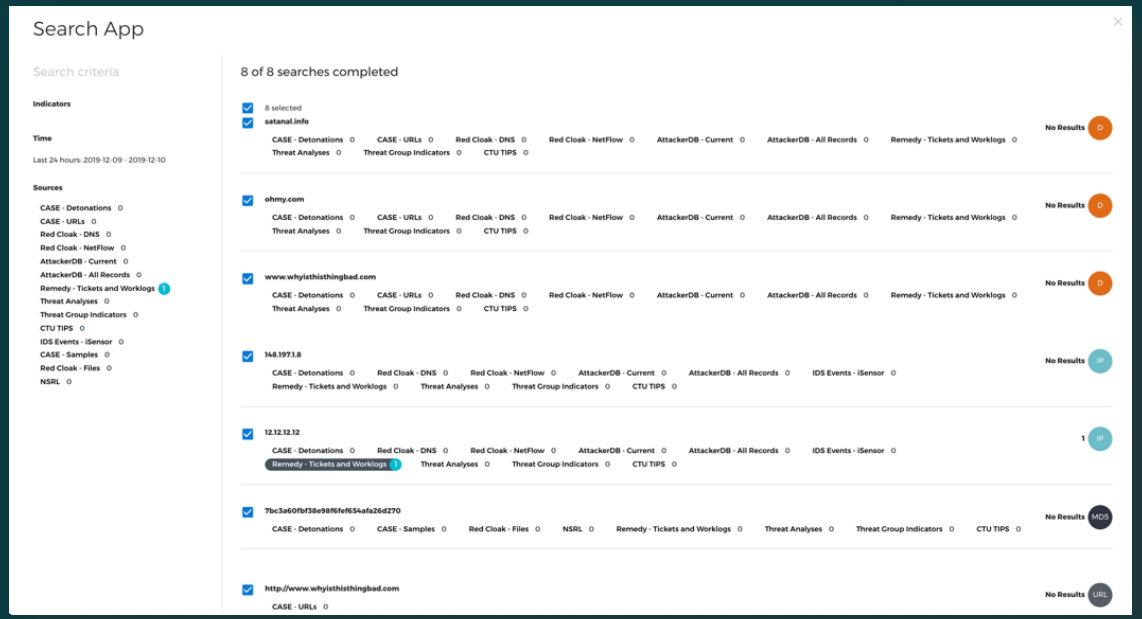


Workflows to aid data access, normalization and customisations

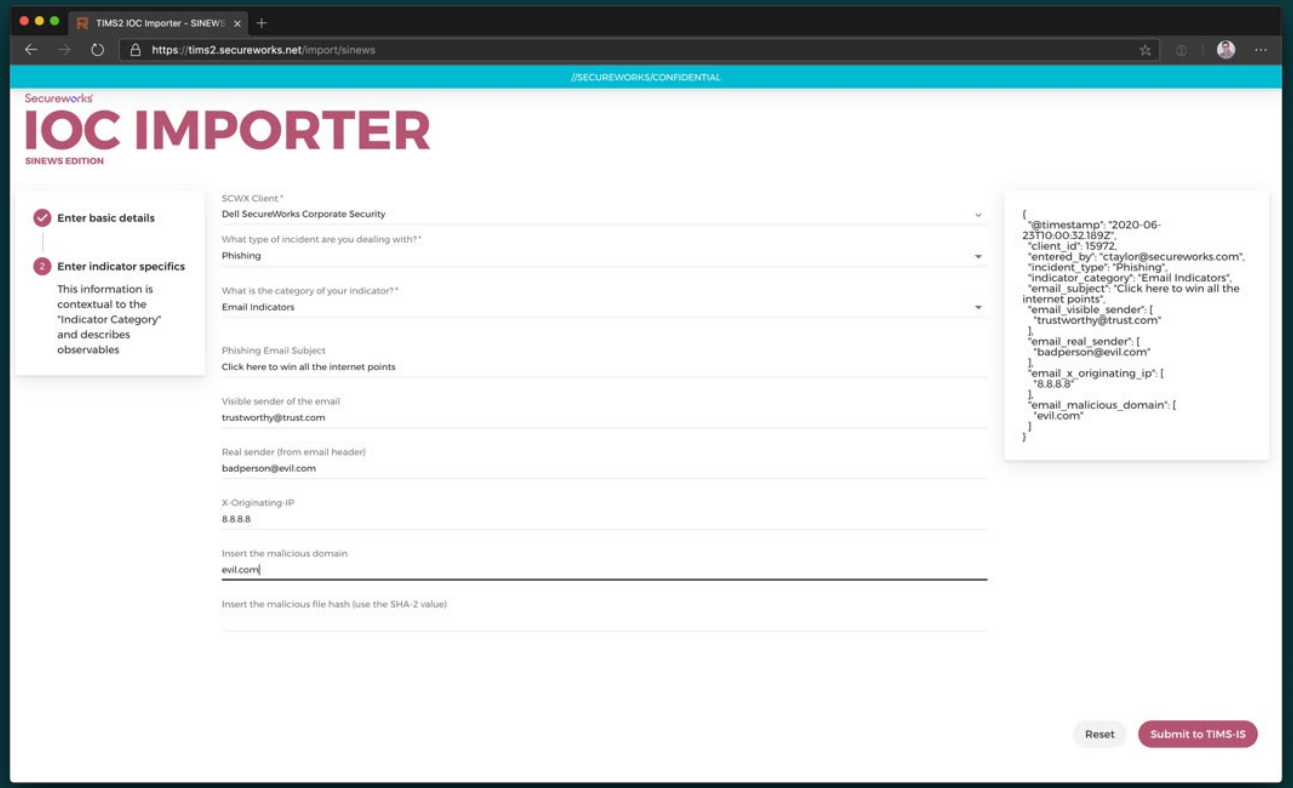


Bringing together data from multiple sources from intelligence, telemetry and enrichments…

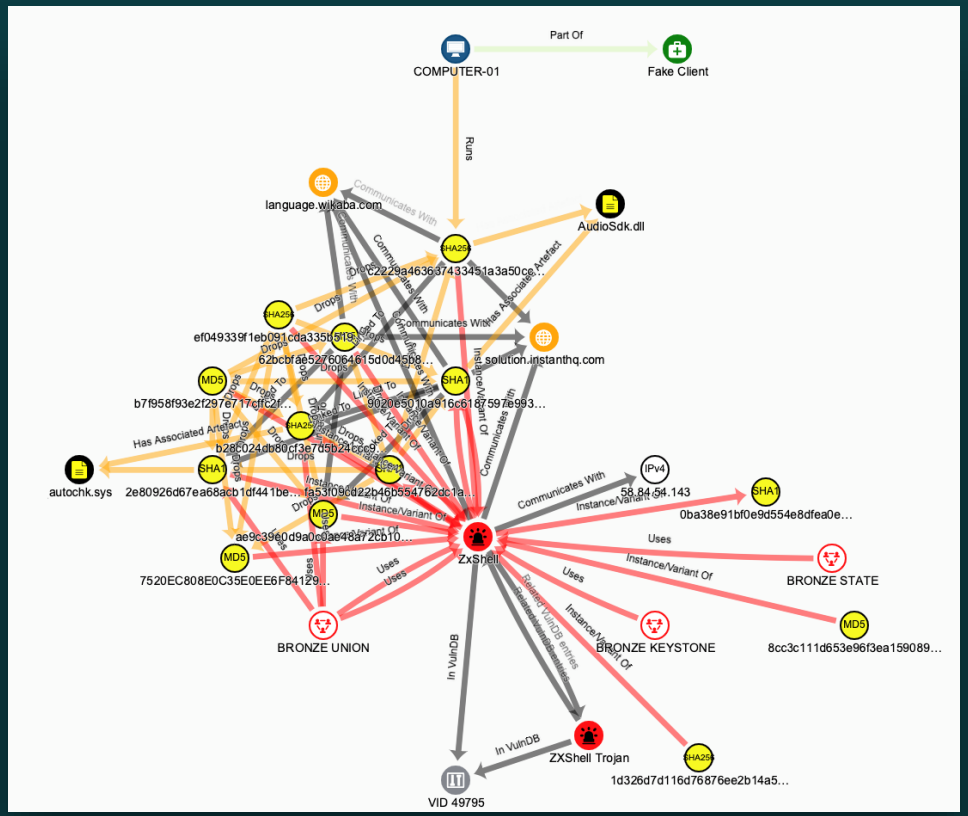
Making it searchable and accessible…



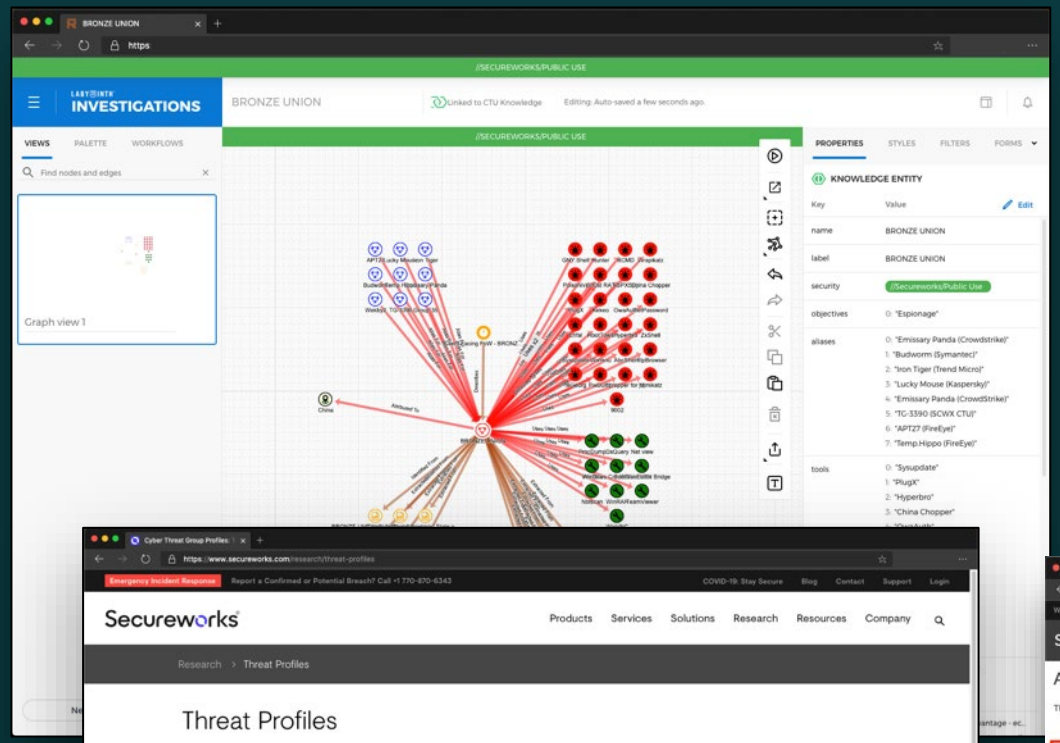
Quick ingestion of data….

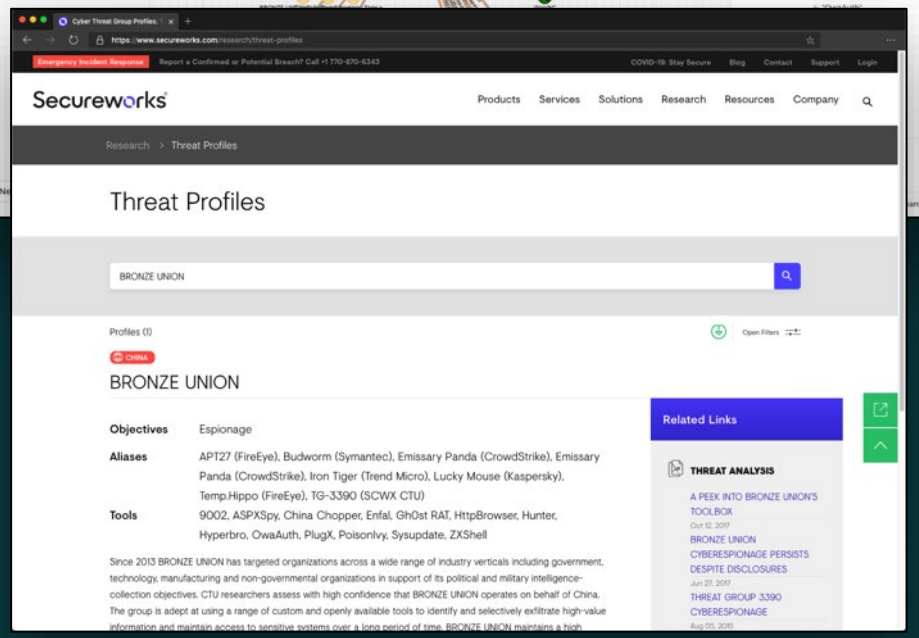


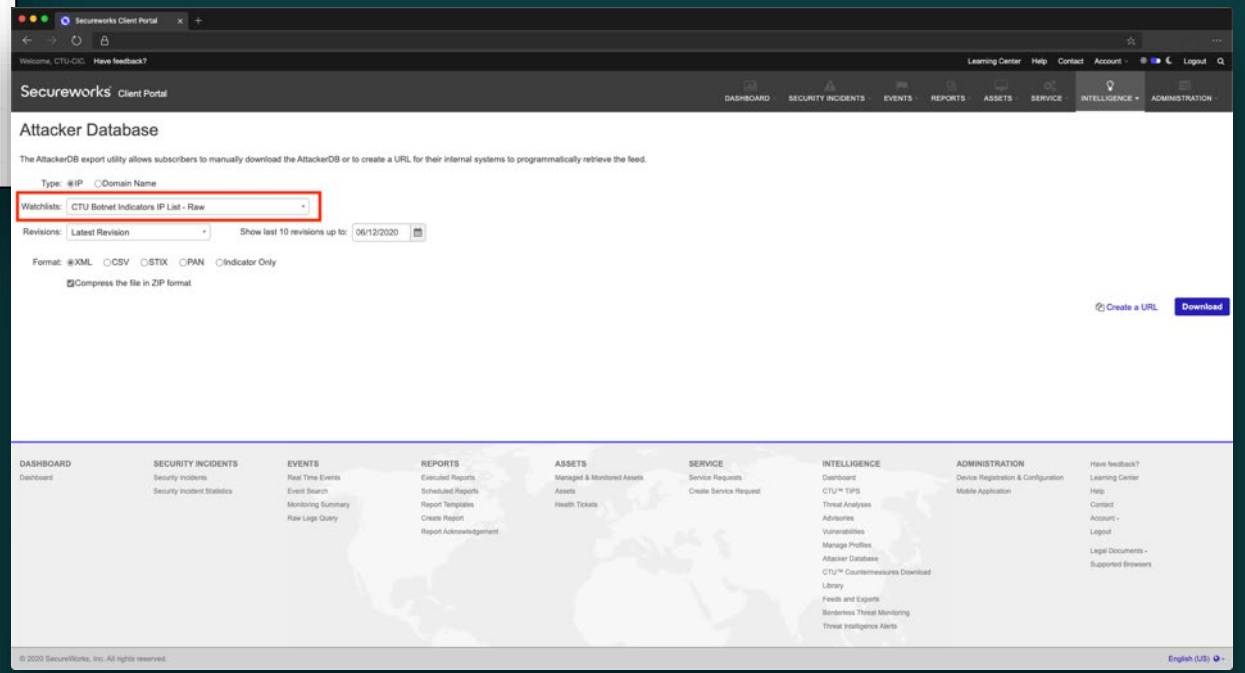
To connect the dots between datapoints and engagements….



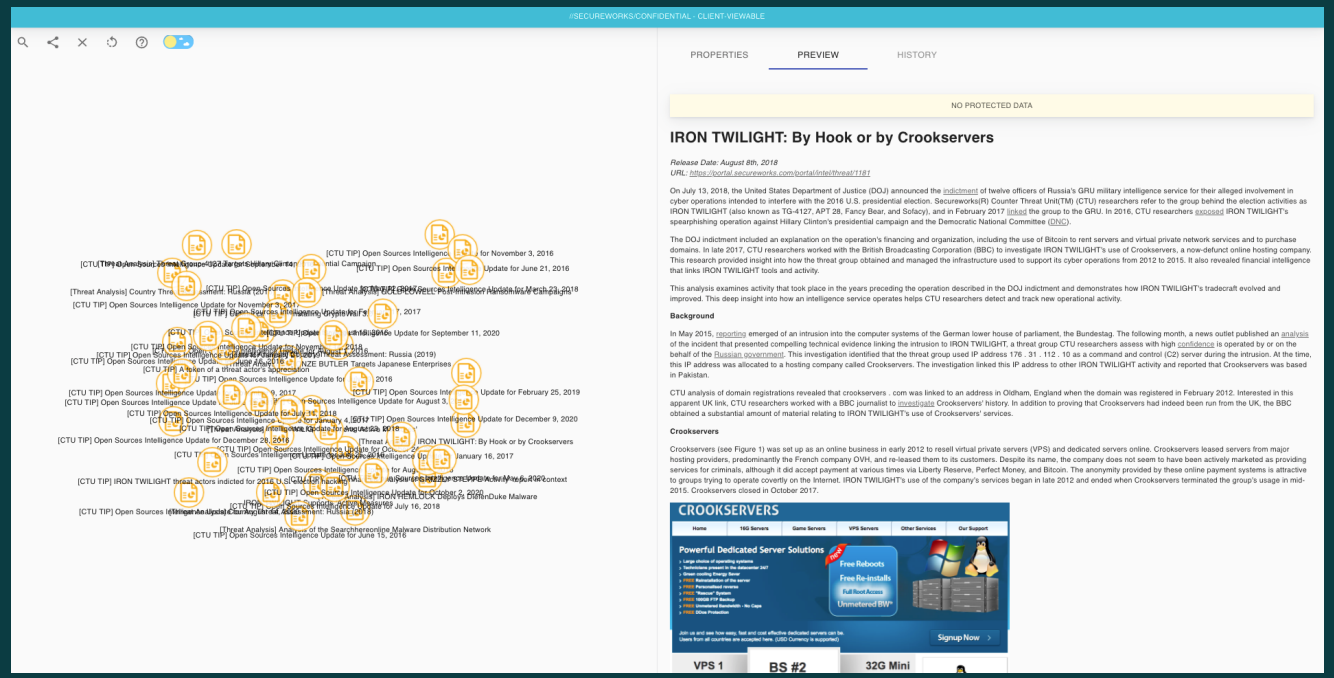
This all together feeds into our automation processes, particularly customer facing threat profiles, briefings, botnet emulations and data collection techniques …

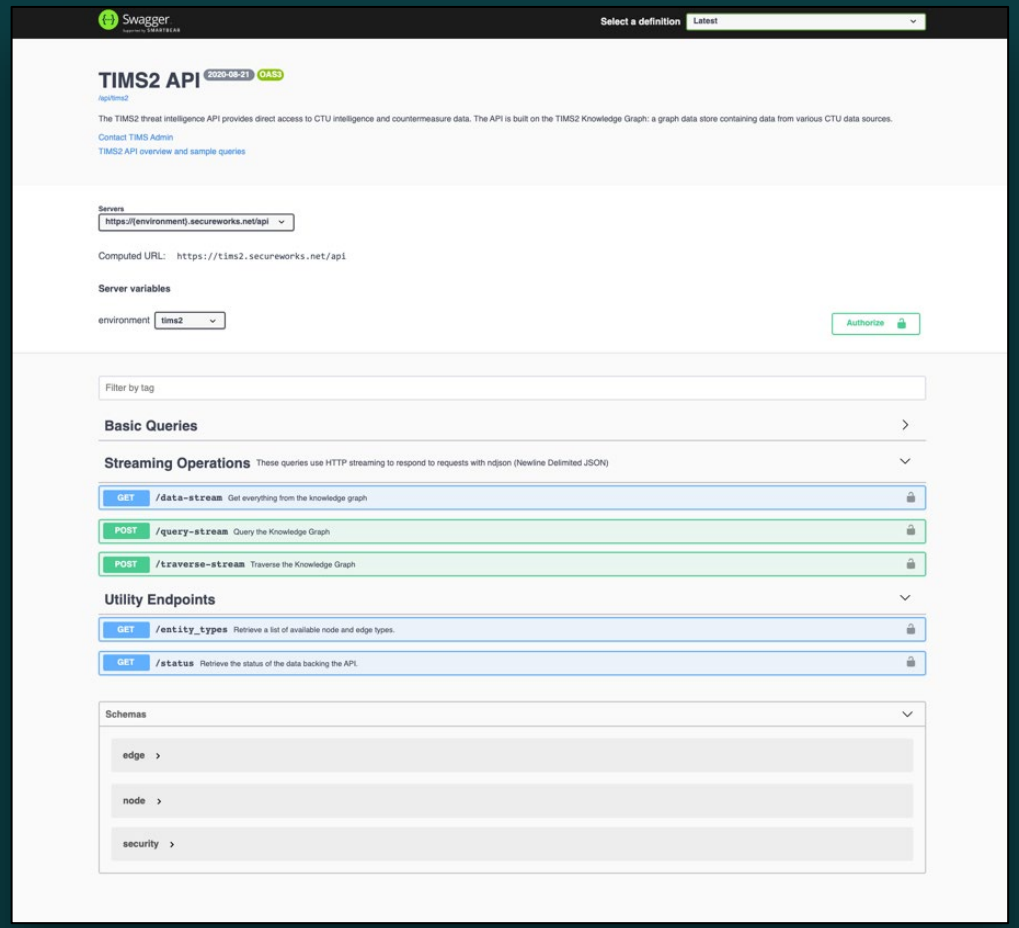






As well as API streams and accessible knowledge browsers…





"An investment in knowledge, pays the best interest"

Benjamin Franklin

You need to -

- Understand what you collect now and what you do with it.
- Understand what you want to collect and why you don't already.
- What's the plan? What framework and mechanism?

- **Templatise** the basics to allow for consistency.
- Prioritize strong **communication**, **workstreams and data capture.**
- Take **small steps** – It isn't about expensive solutions, it's about what works for the organisation, and what is relevant to you.

"Knowledge is power. Knowledge shared is power multiplied"

Robert Boyce