



DUBLIN

IRELAND 2022

34th ANNUAL FIRST CONFERENCE
JUNE 26 - JULY 1

#FIRSTCON22

Knowledge Management

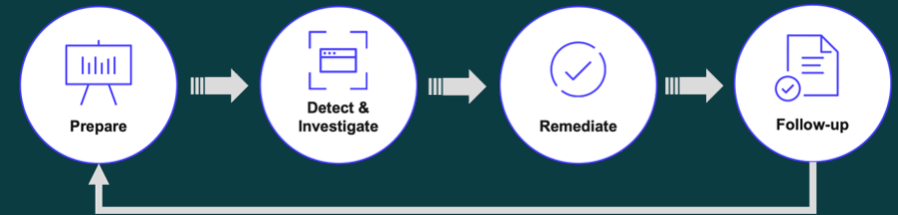
Nourishing & Enhancing your communication and intelligence.

Rebecca Lois Taylor (Secureworks®, United Kingdom)

[Rebecca Taylor | LinkedIn](#)



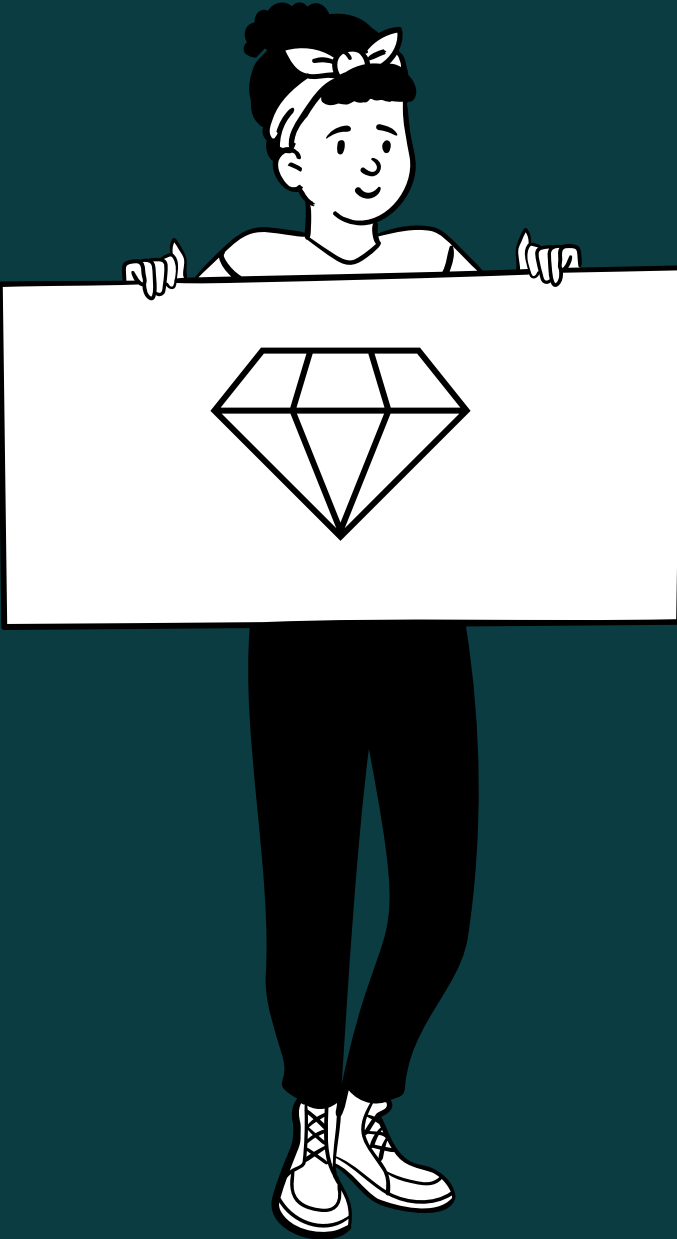
Nominee



GSEC
Prince2
ITIL V4
GISF

Today's Topics

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



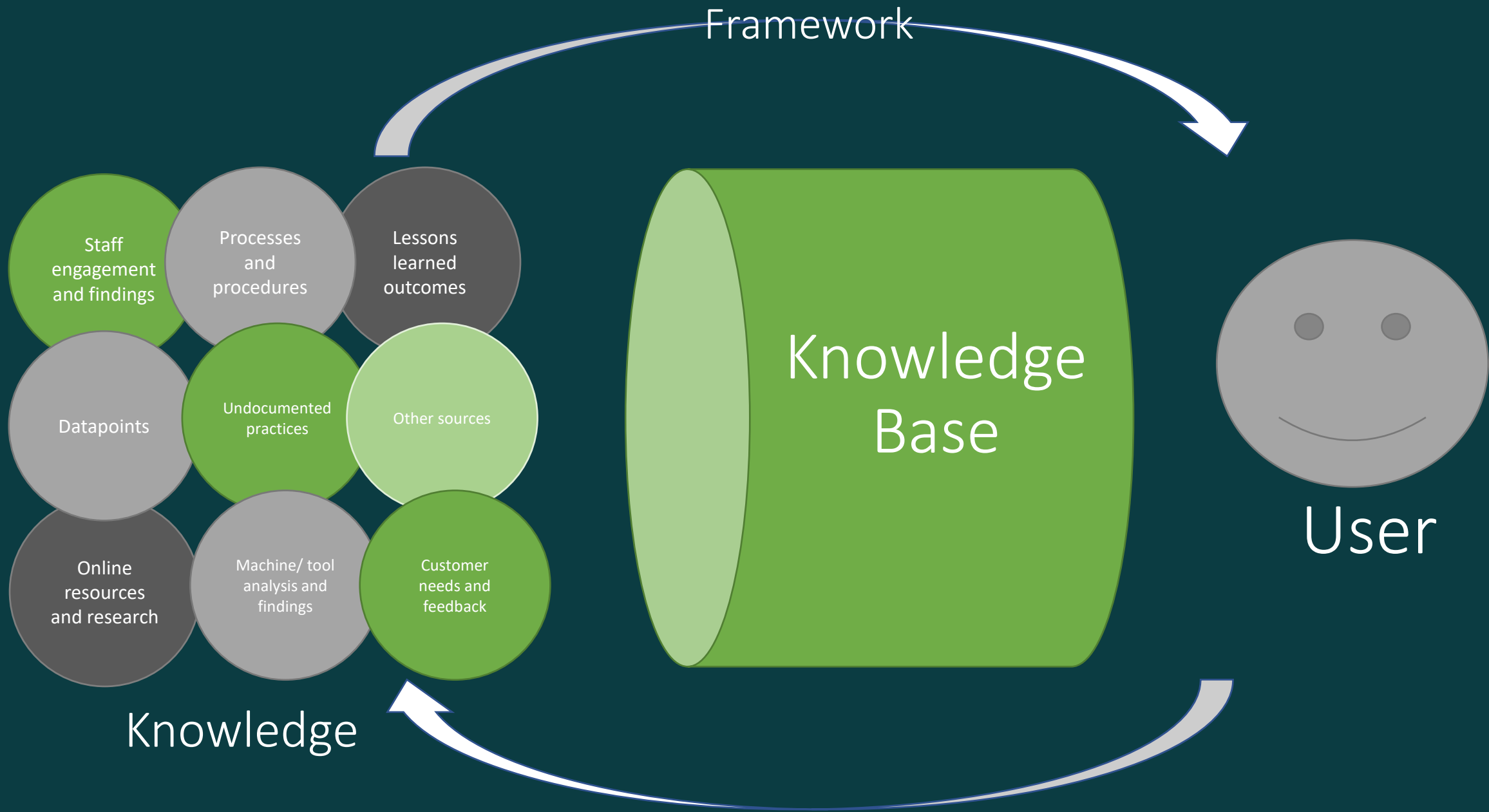
“An investment in knowledge,
pays the best interest”

Benjamin Franklin

What is Knowledge Management?

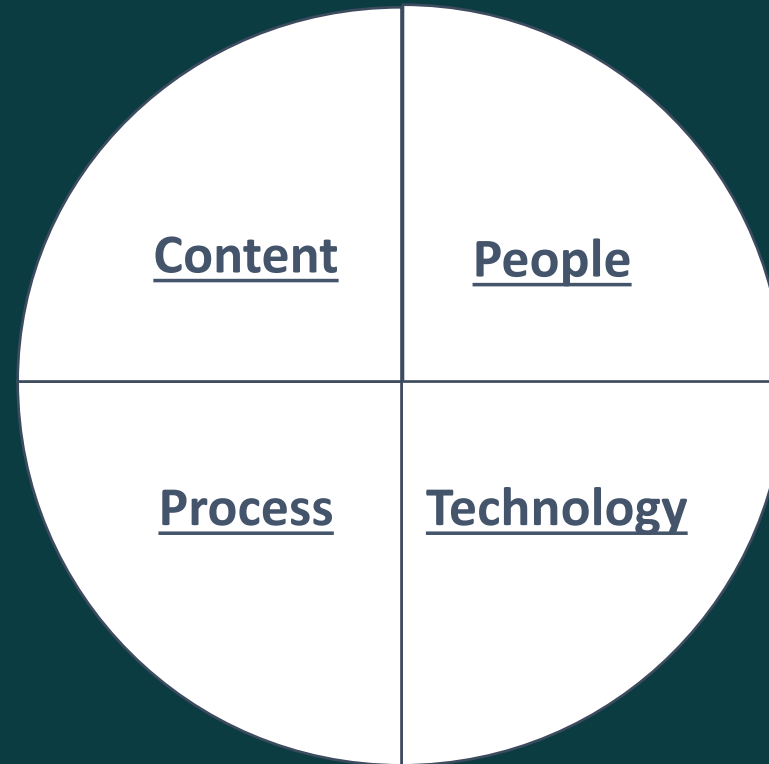
‘Knowledge management is the **process of more effectively collecting, sharing, maintaining or managing, and deploying organizational knowledge**. As a discipline, knowledge management recognizes three basic forms of knowledge: explicit knowledge, tacit, and implicit knowledge’

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



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

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



Governance

- Notification or disclosure requirements
- Supporting documents and specific investigations

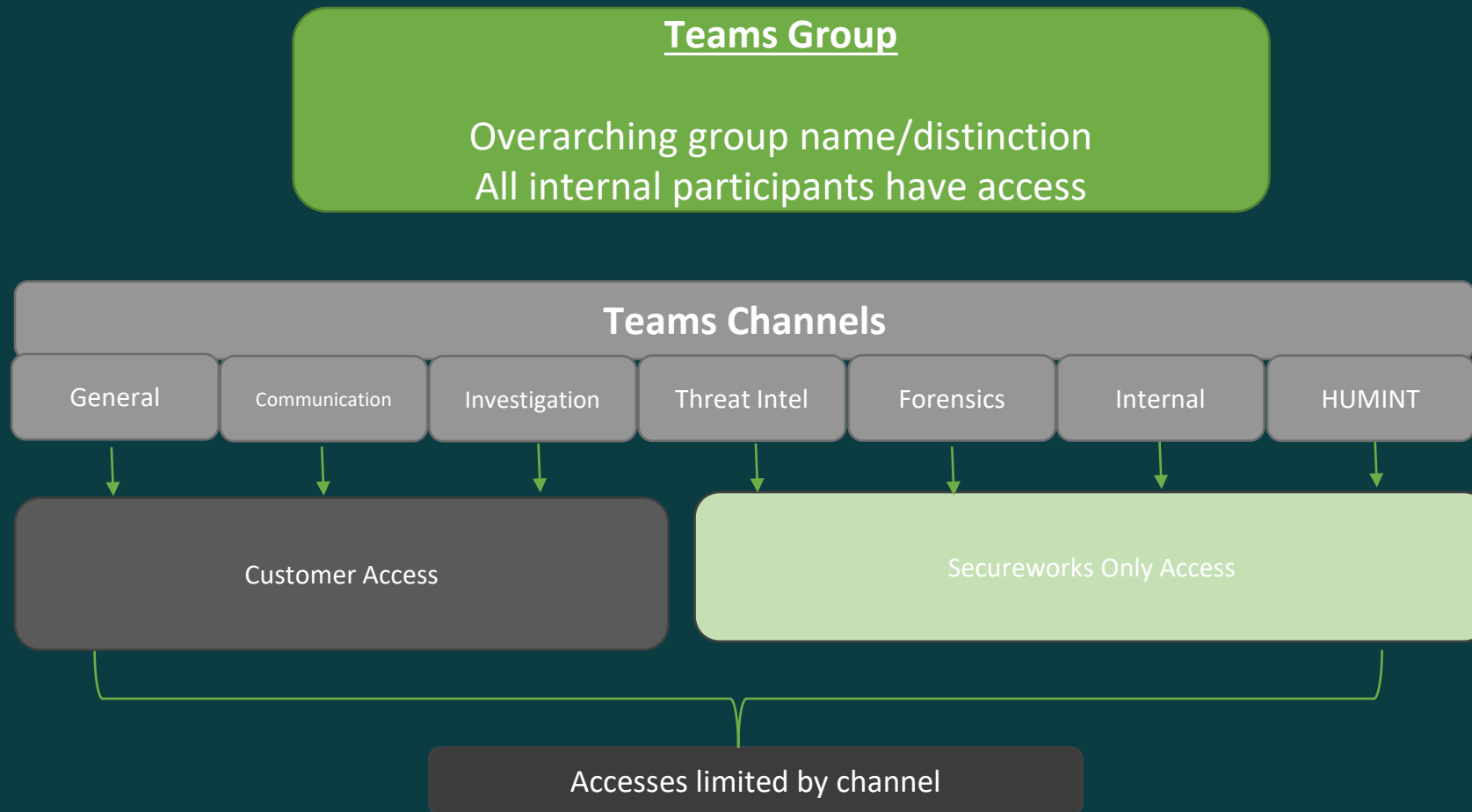
Insurance

- Caveats
- Notification responsibilities
- Reporting
- Approved IR provider

Legal

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

Workstreams



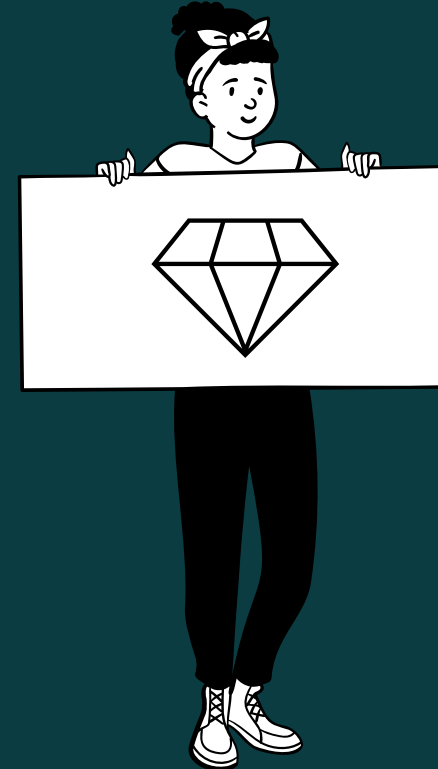
Templates

- 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



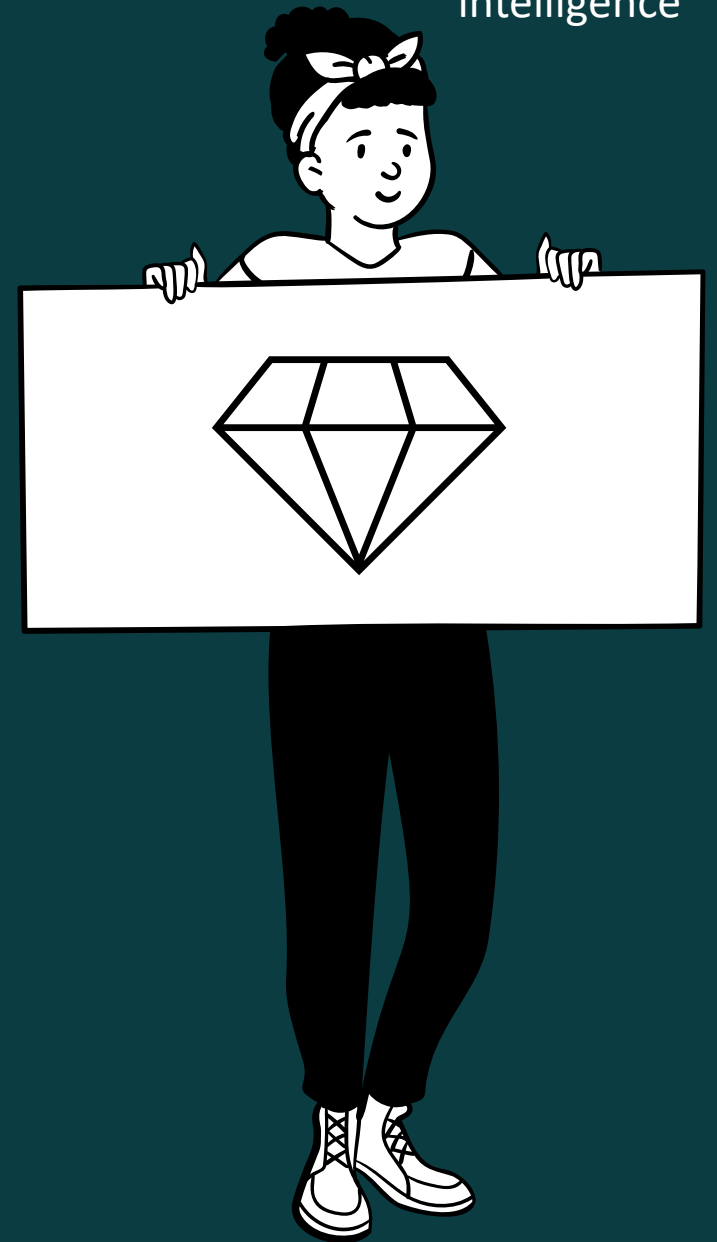
Data → Investigations → Knowledge



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 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 visualising

Contact Addresses

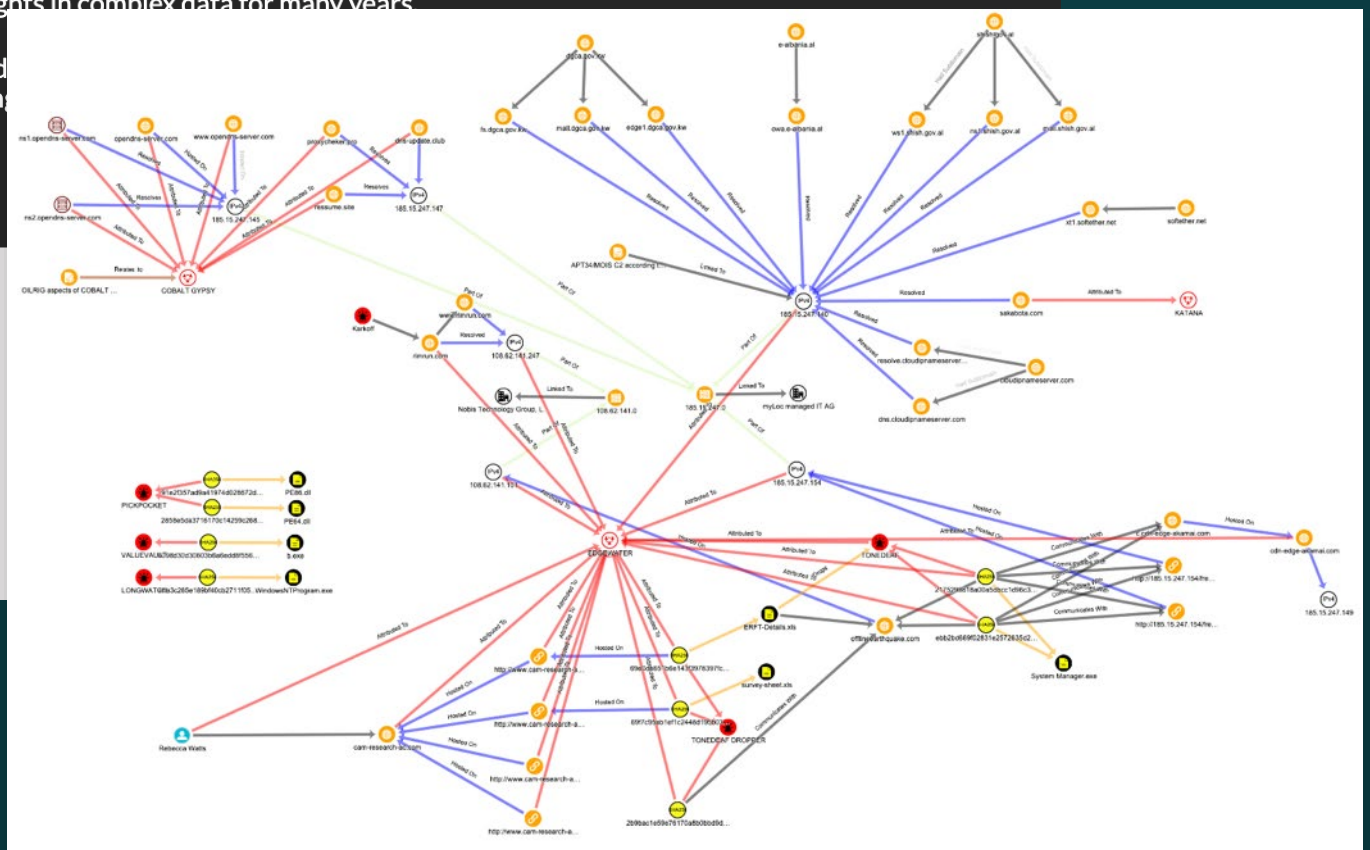
Sales: sales@ripjar.com

Sales: +44 203 198 2250

Cheltenham Office: +44 1242 312052

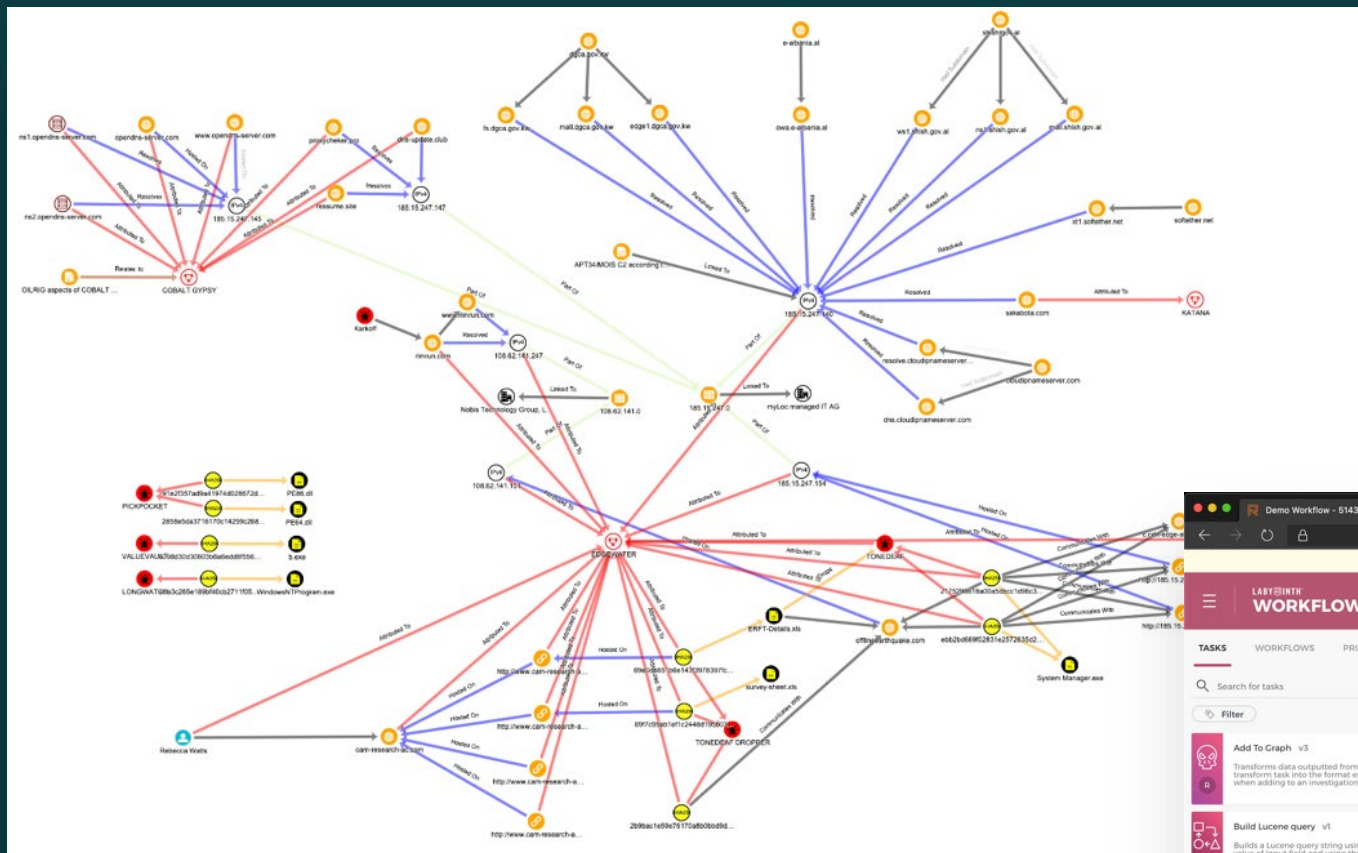
Support: +44 333 300 1295

Jobs: jobs@ripjar.com



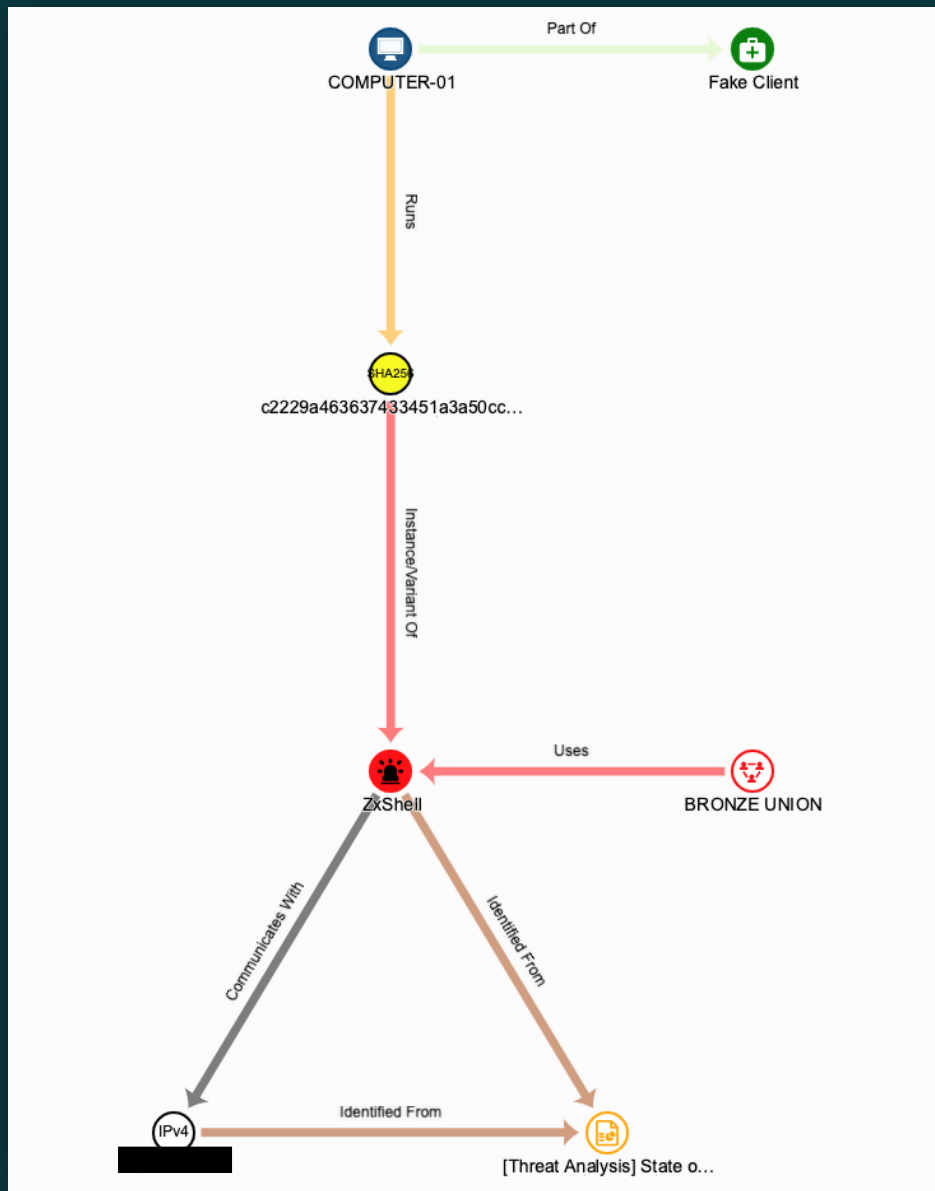
TIMS

Mapping of telemetry and datapoints

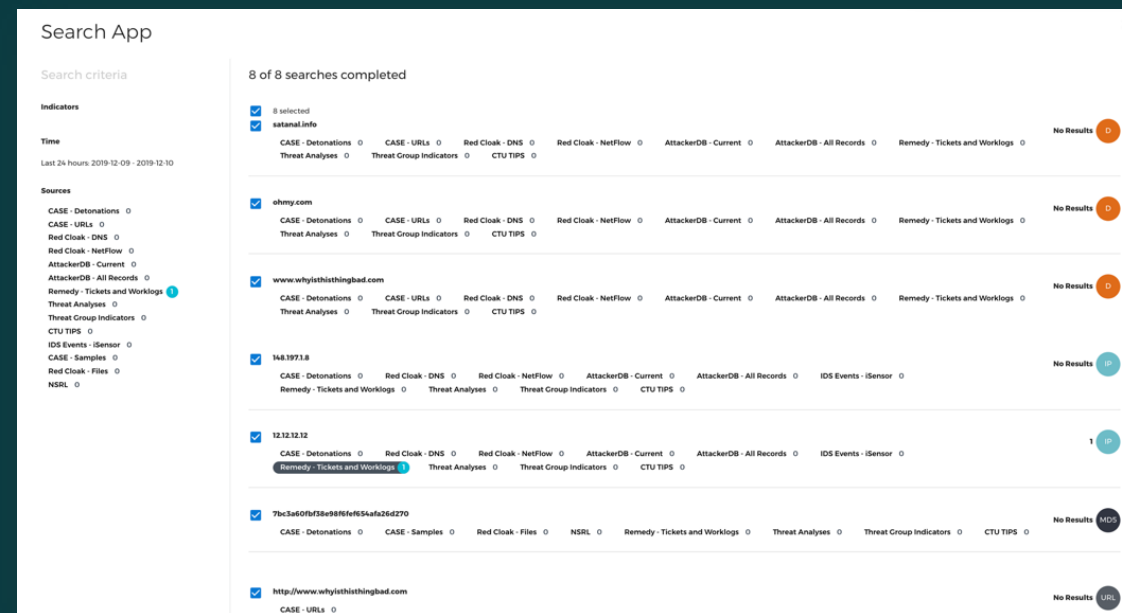


Workflows to aid data access, normalization and customisations

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



Making it searchable and accessible...

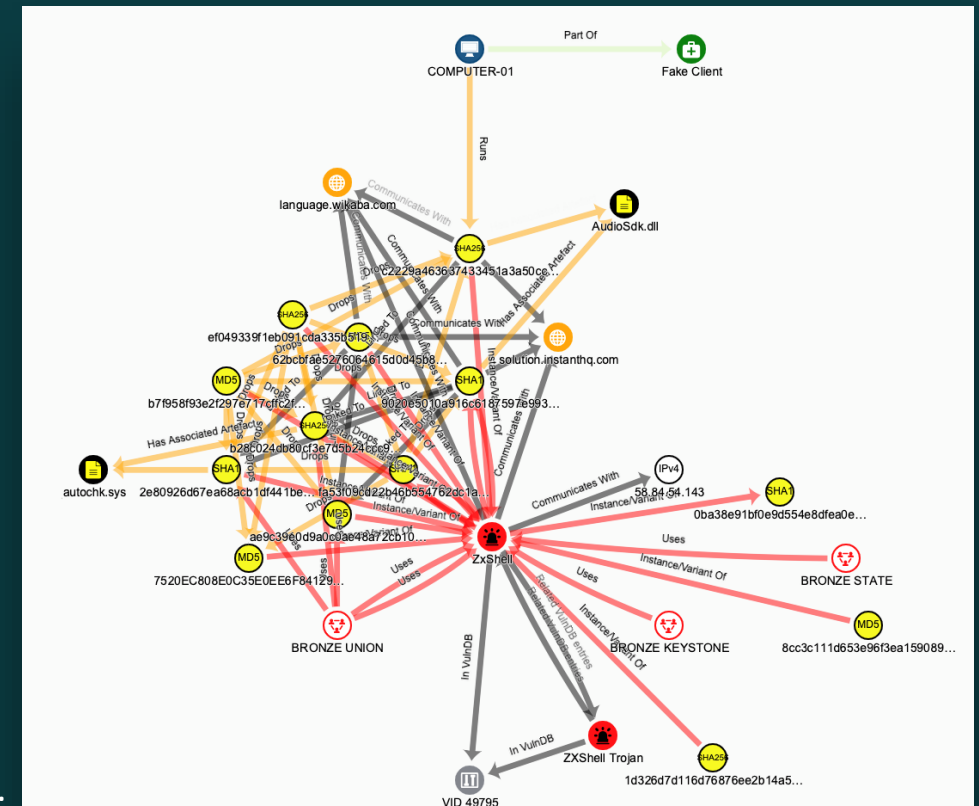


Embracing your intelligence

Quick ingestion of data....

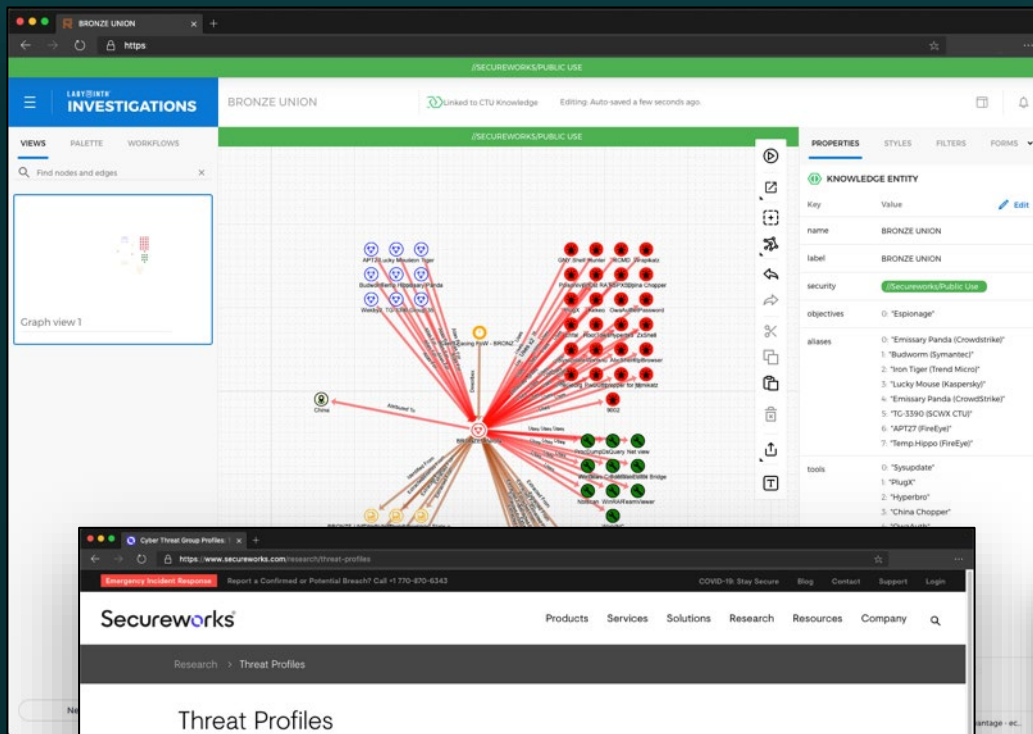
```
{
  "@timestamp": "2020-06-23T10:00:32.189Z",
  "client_ip": "15972",
  "entered_by": "ctaylor@secureworks.com",
  "incident_type": "Phishing",
  "indicator_category": "Email Indicators",
  "email_subject": "Click here to win all the internet points",
  "email_visible_sender": [
    "trustworthy@trust.com"
  ],
  "email_real_sender": [
    "badperson@evil.com"
  ],
  "email_x_originating_ip": [
    "8.8.8.8"
  ],
  "email_malicious_domain": [
    "evil.com"
  ]
}
```

To connect the dots between datapoints and engagements....



Embracing your intelligence

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



Objectives Espionage

Aliases APT27 (FireEye), Budworm (Symantec), Emissary Panda (CrowdStrike), Emissary Panda (CrowdStrike), Iron Tiger (Trend Micro), Lucky Mouse (Kaspersky), Temp.Hippo (FireEye), TG-3390 (SCWX CTU)

Tools 9002, ASPXSpy, China Chopper, Enfal, Gh0st RAT, HttpBrowser, Hunter, Hyperbro, OwaAuth, PlugX, PoisonIvy, Sysupdate, ZXShell

Related Links

- A PEEK INTO BRONZE UNIONS TOOLBOX Oct 18, 2019
- BRONZE UNION CYBERESPIONAGE PERSISTS DESPITE DISCLOSURES Jun 27, 2017
- THREAT GROUP 3390 CYBERESPIONAGE Aug 05, 2016

Attacker Database

The AttackerDB export utility allows subscribers to manually download the AttackerDB or to create a URL for their internal systems to programmatically retrieve the feed.

Type: IP Domain Name

Watchlists: **CTU Botnet Indicators IP List - Raw**

Revisions: Latest Revision Show last 10 revisions up to: 06/12/2020

Format: XML CSV STIX PAN Indicator Only

Compress the file in ZIP format

Create a URL Download

As well as API streams and accessible knowledge browsers...

The screenshot shows a web browser window with a URL bar containing "#SECUREWORKS-CONFIDENTIAL - CLIENT-VIEWABLE". The page is divided into two main sections. On the left, there is a vertical list of intelligence updates, each accompanied by a circular icon with a letter 'C' and a date. On the right, a detailed article titled "IRON TWILIGHT: By Hook or by Crookservers" is displayed. The article includes a release date of August 8th, 2018, and a URL. The text discusses the United States Department of Justice's announcement regarding Russian GRU military intelligence service involvement in the 2016 U.S. presidential election. It mentions the use of Bitcoin for financing and the role of Crookservers, a virtual private network (VPN) provider, in hosting the infrastructure. The article also includes a background section detailing the discovery of the Crookservers domain and its connection to the Iron Twilight operation.

The screenshot shows the Swagger API documentation page for the TIMS2 API. The page is titled "TIMS2 API" and includes a "Select a definition" dropdown menu set to "Latest". Below the title, there is a description of the API: "The TIMS2 threat intelligence API provides direct access to CTU intelligence and countermeasure data. The API is built on the TIMS2 Knowledge Graph: a graph data store containing data from various CTU data sources." There are links for "Contact TMS Admin" and "TIMS2 API overview and sample queries". A "Servers" section shows a dropdown menu with the URL "https://environment.secureworks.net/api". Below this, the "Computed URL" is "https://tims2.secureworks.net/api". A "Server variables" section shows a dropdown menu for "environment" set to "tims2" and an "Authorize" button. The page also features sections for "Basic Queries", "Streaming Operations", "Utility Endpoints", and "Schemas".

“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