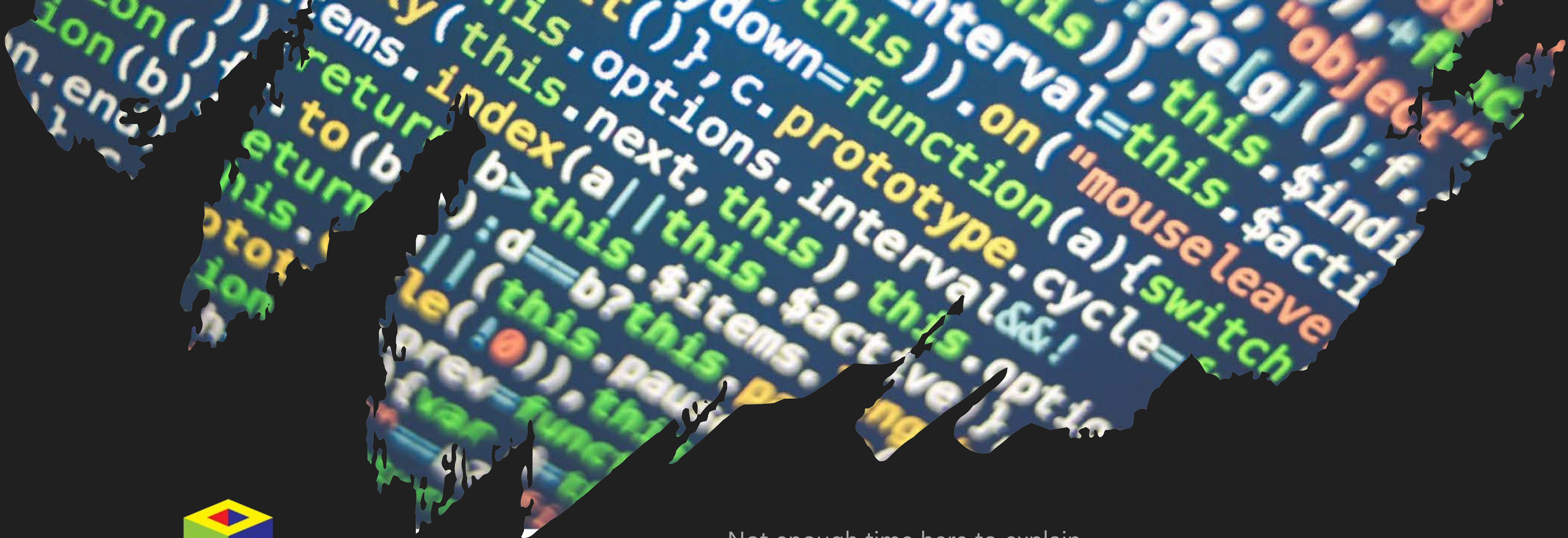
Social Engineering Forensics

Aaron Crawford
Insider Security Agency



Aaron Crawford

whoami

Not enough time here to explain.
Find me after this talk.

Twitter: @squirrelsnabrrl
@Insider_Agency

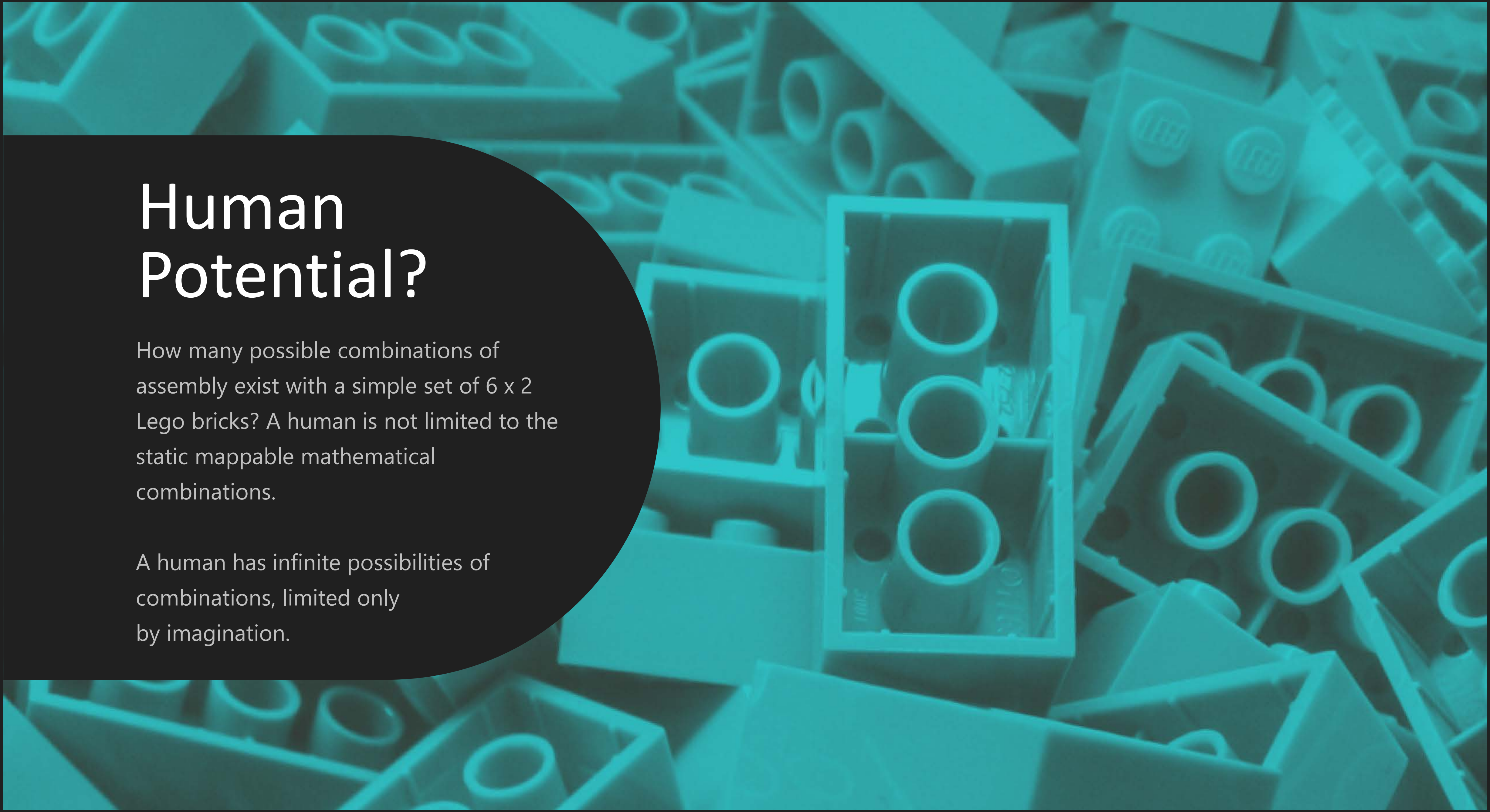
web: www.theinsideragency.com

Hashtags: #SocialEngineeringTips #SocialOperator #LearnSocialEngineering #HackerHired

Human Potential?

How many possible combinations of assembly exist with a simple set of 6 x 2 Lego bricks? A human is not limited to the static mappable mathematical combinations.

A human has infinite possibilities of combinations, limited only by imagination.



What is…

Social Engineering?

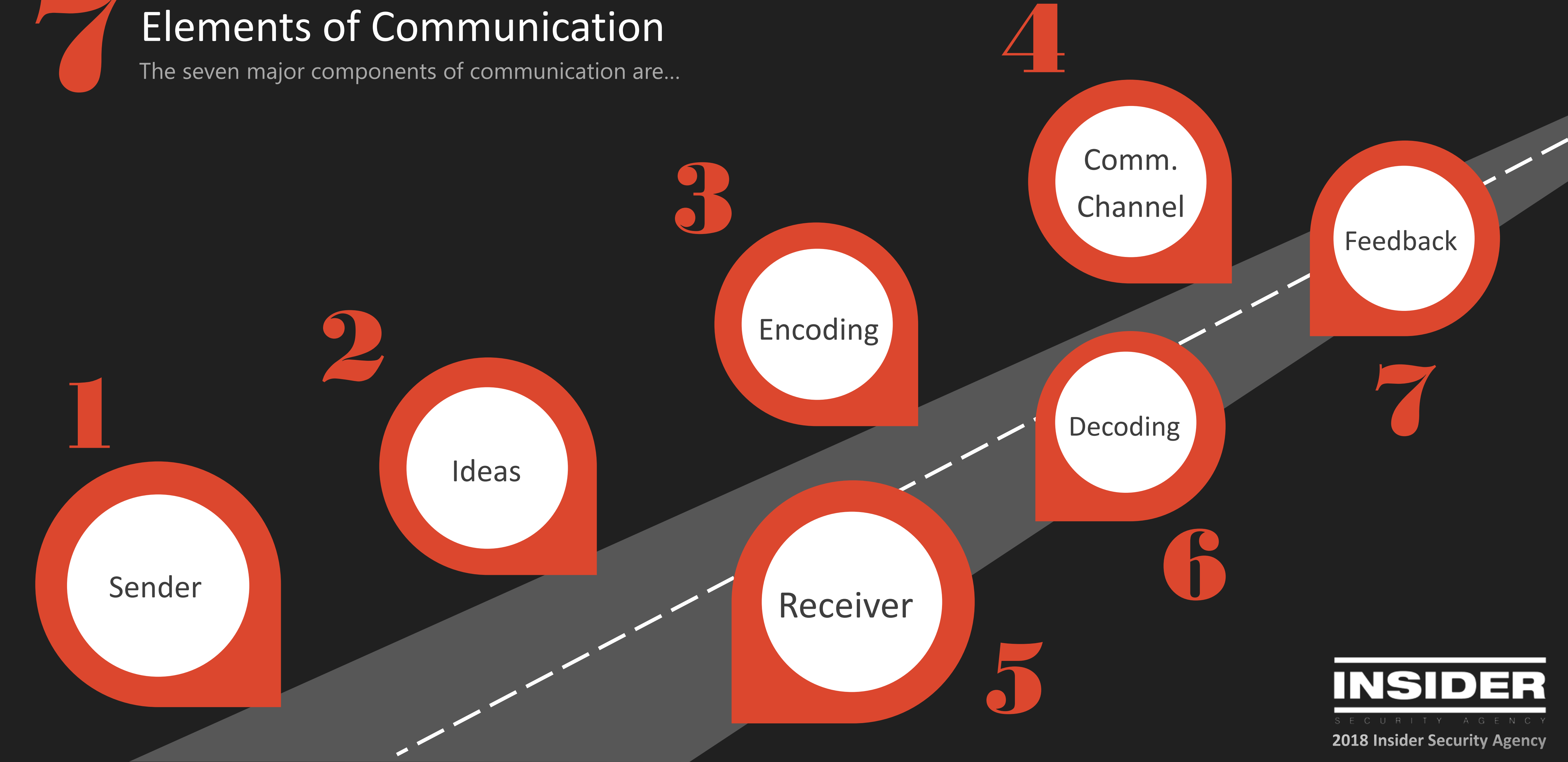
Social Engineering for the sake of this talk is the process of obtaining information, services or goods by the manipulation of another human or group's reality through verbal and or non-verbal communications.

While hacking relates to the manipulation of technology, social engineering, relates to the hacking or manipulation of the human or non-technical elements.

7 The Seven Major

Elements of Communication

The seven major components of communication are…



INSIDER SECURITY AGENCY

2018 Insider Security Agency

What is…

Forensics?

Forensics is the science driven process of collecting information for the use in legal matters such as court evidence.

What is…

Forensic Questioning?

Forensics questioning is the process in which evidence is collected through a thoroughly vetted and guided framework of questions, that help to gather information while maintaining the integrity of the evidence and avoids altering the subject's perception, recollection and the ability to communicate.

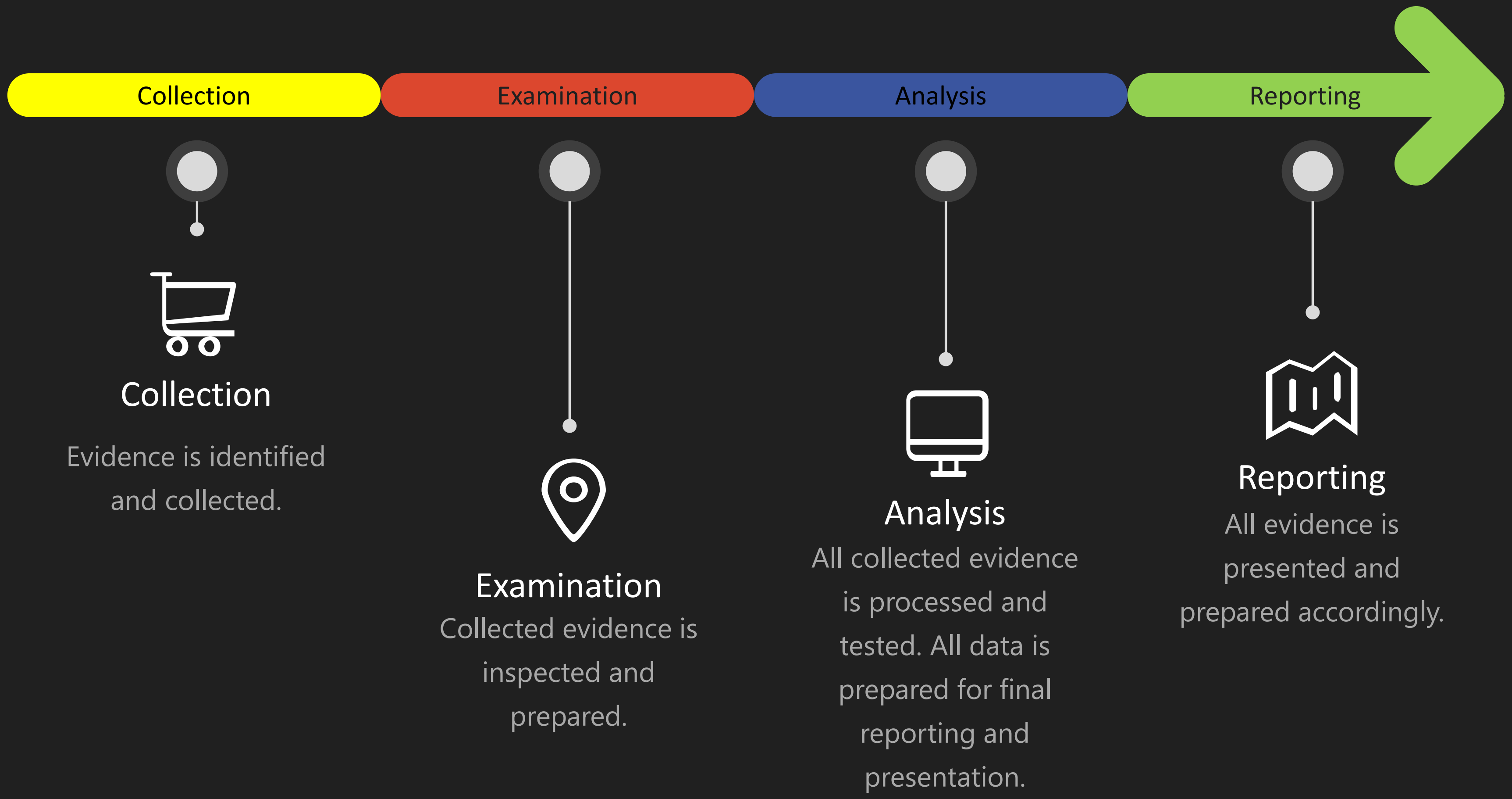
INSIDER
SECURITY AGENCY

What is…

Chain of Custody?

The maintained chronological documentation of an incident's evidence that records the sequence of control, transfer, analysis and disposition of all collected evidence whether physical or electronic.

Basic Forensic Process



Collection — Examination — Analysis — Reporting

Collection

Evidence is identified and collected.

Examination

Collected evidence is inspected and prepared.

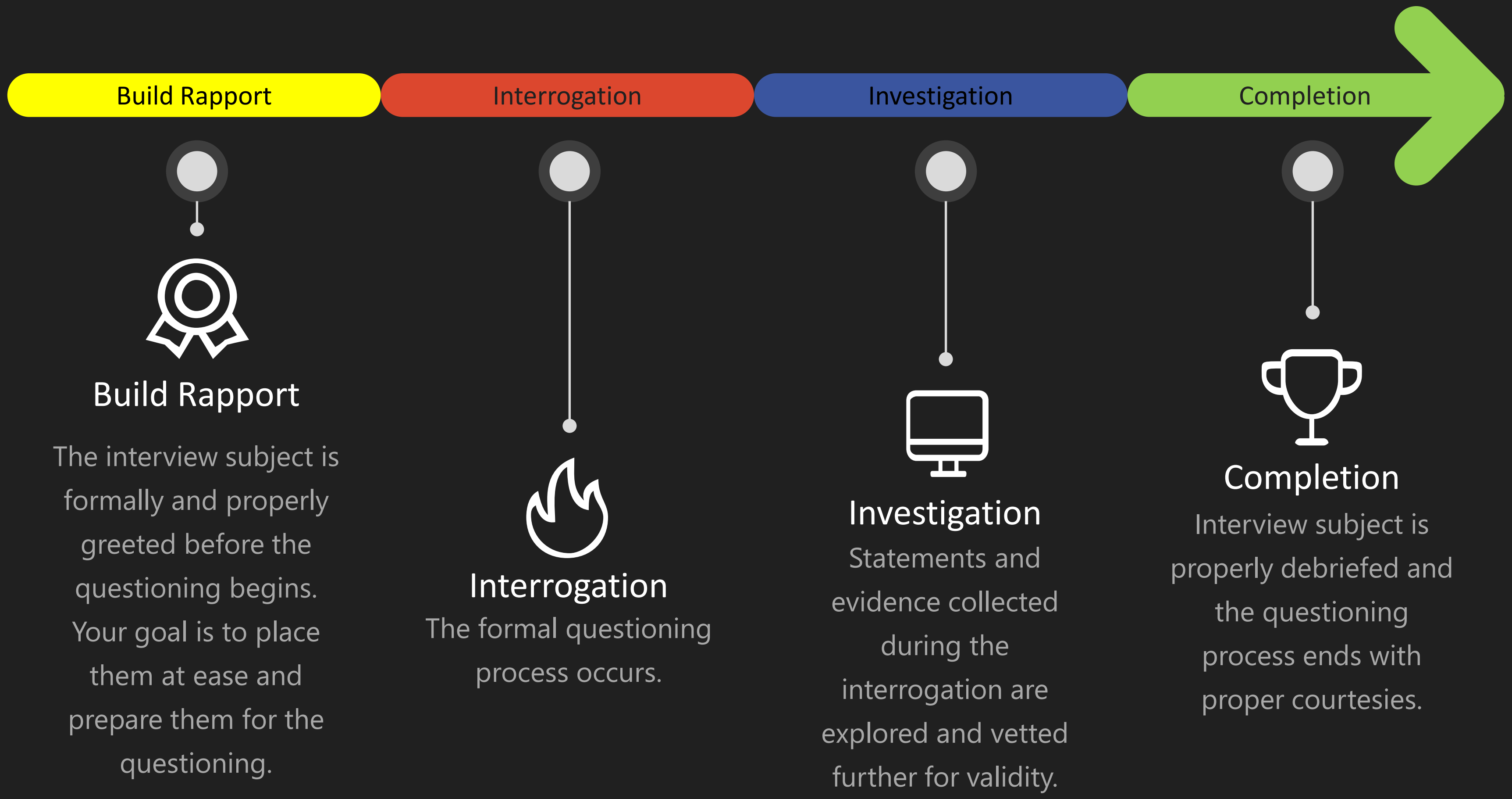
Analysis

All collected evidence is processed and tested. All data is prepared for final reporting and presentation.

Reporting

All evidence is presented and prepared accordingly.

Basic Forensic Questioning Process



Build Rapport

Interrogation

Investigation

Completion

Build Rapport

The interview subject is formally and properly greeted before the questioning begins. Your goal is to place them at ease and prepare them for the questioning.

Interrogation

The formal questioning process occurs.

Investigation

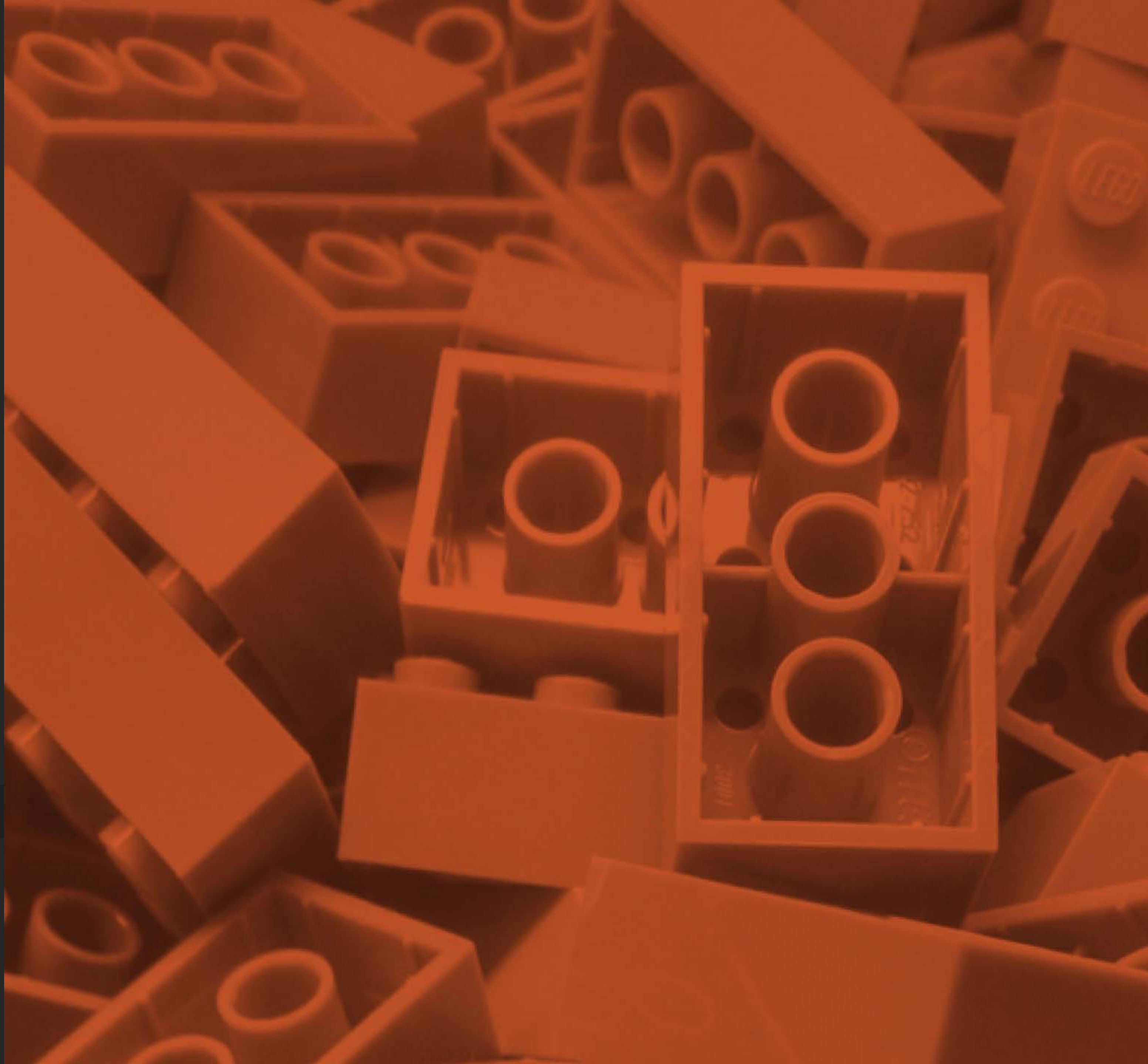
Statements and evidence collected during the interrogation are explored and vetted further for validity.

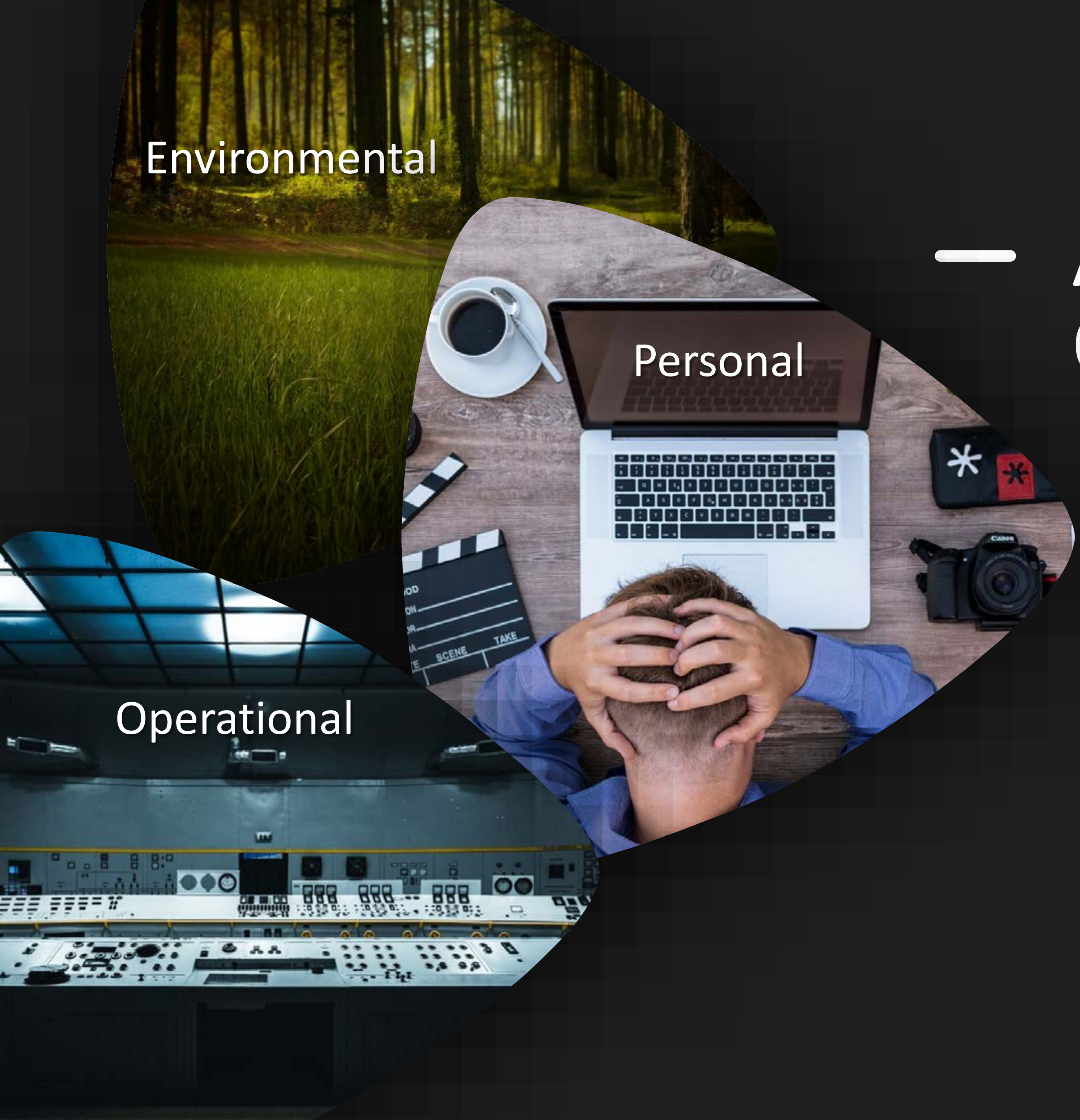
Completion

Interview subject is properly debriefed and the questioning process ends with proper courtesies.

Always seek legal guidance before proceeding in any investigation to ensure that all recording and documentation methods are legal and acceptable!

Always ask a lawyer!





Areas of Questioning

1 **Environmental**
Relates to the impact of workplace conditions on productivity and morale

2 **Personal**
Relates to the human element and the personal space only occupied within the company

3 **Operational**
Relates to the policies and procedures and how they impact both the individual and the enterprise

INSIDER
SECURITY AGENCY

Can you describe how it feels when you arrive to work, when you return from lunch and when you leave for the day? "

Environmental Example

“

Can you walk us through your daily routine when you arrive on site for the work day? “

Personal Example

“

Can you describe to us step-by-step your process to report any security incidents to the proper company channels? “

Operational Example

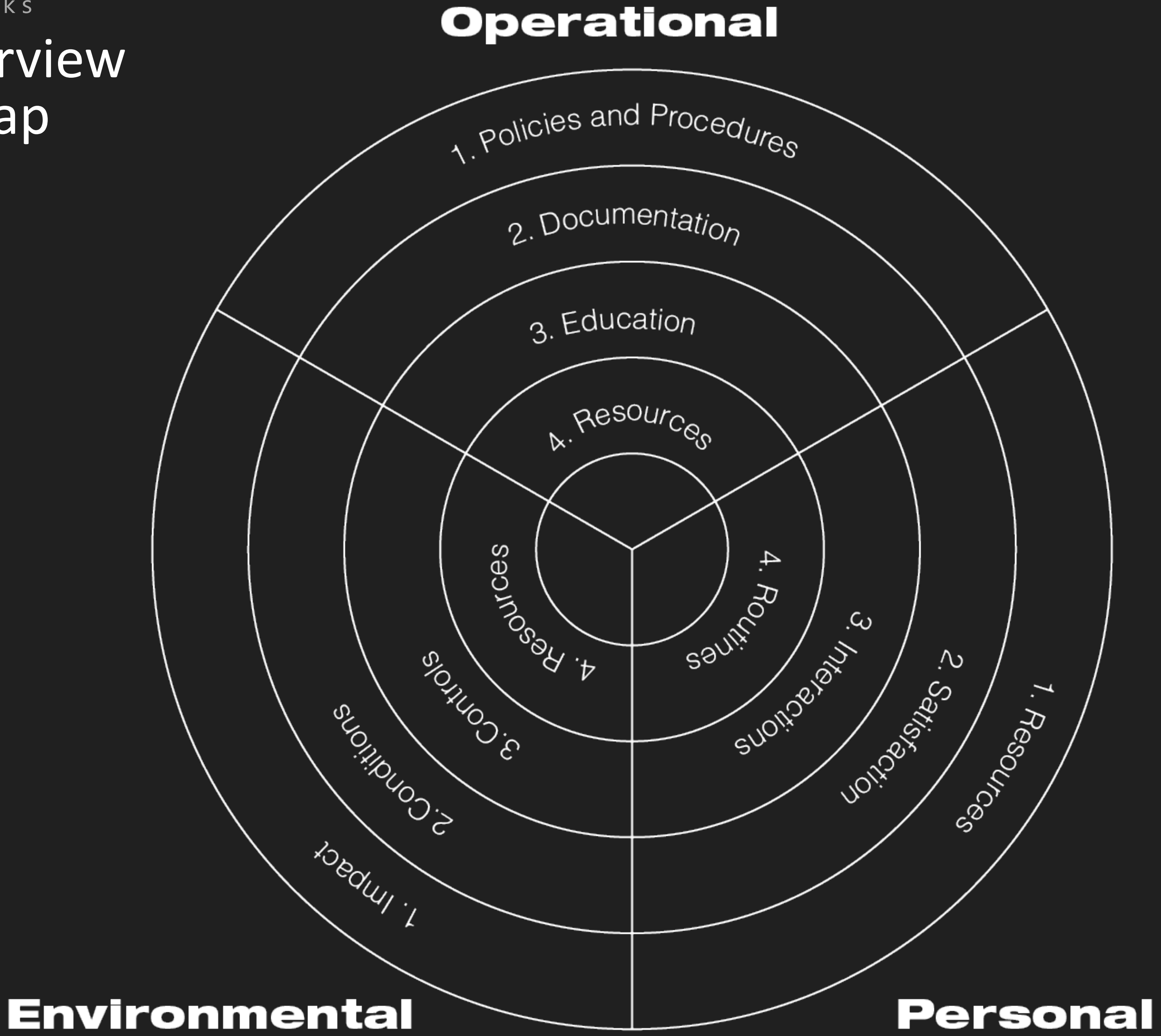
DON'T FORGET...

Always keep your line of questioning anchored within the guidelines and requirements of the investigation. You are a supporting resource and role.

Keep Questions Simple

Question Banks

Forensic Interview Region Map



Operational

1. Policies and Procedures
2. Documentation
3. Education
4. Resources

Environmental

1. Impact
2.Conditions
3.Controls
4. Resources

Personal

1. Resources
2. Satisfaction
3. Interactions
4. Routines

HOW TO QUANTIFY?

How to show ROI/Impact from collected evidence.

— Let the evidence craft the narrative…

- **Keep questions relevant to the current environment and enterprise**
- **Keep questions direct but not personal to the impacted party's life outside of work**
- **Look for the link to processes and education**
- **Identify the habits**

Where to go from here?

This talk has simply been the introduction to the concepts and ideas behind forensics for social engineering. For additional resources and questions please feel free to contact:

Web: www.theinsideragency.com
LinkedIn: Insider Security Agency
Twitter: @squirrelsnabrrl
@Insider_Agency
YouTube: Squirrels In A Barrel
Hashtags: #SocialEngineeringTips #SocialOperator #LearnSocialEngineering #HackerHired