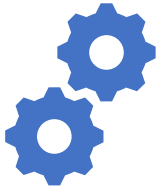
Intelligence Theory in the SOC

The ideas behind operational workflows

Background

Cyber Security is a relatively “new” field

Academic, Industry studies tend to focus on the technical

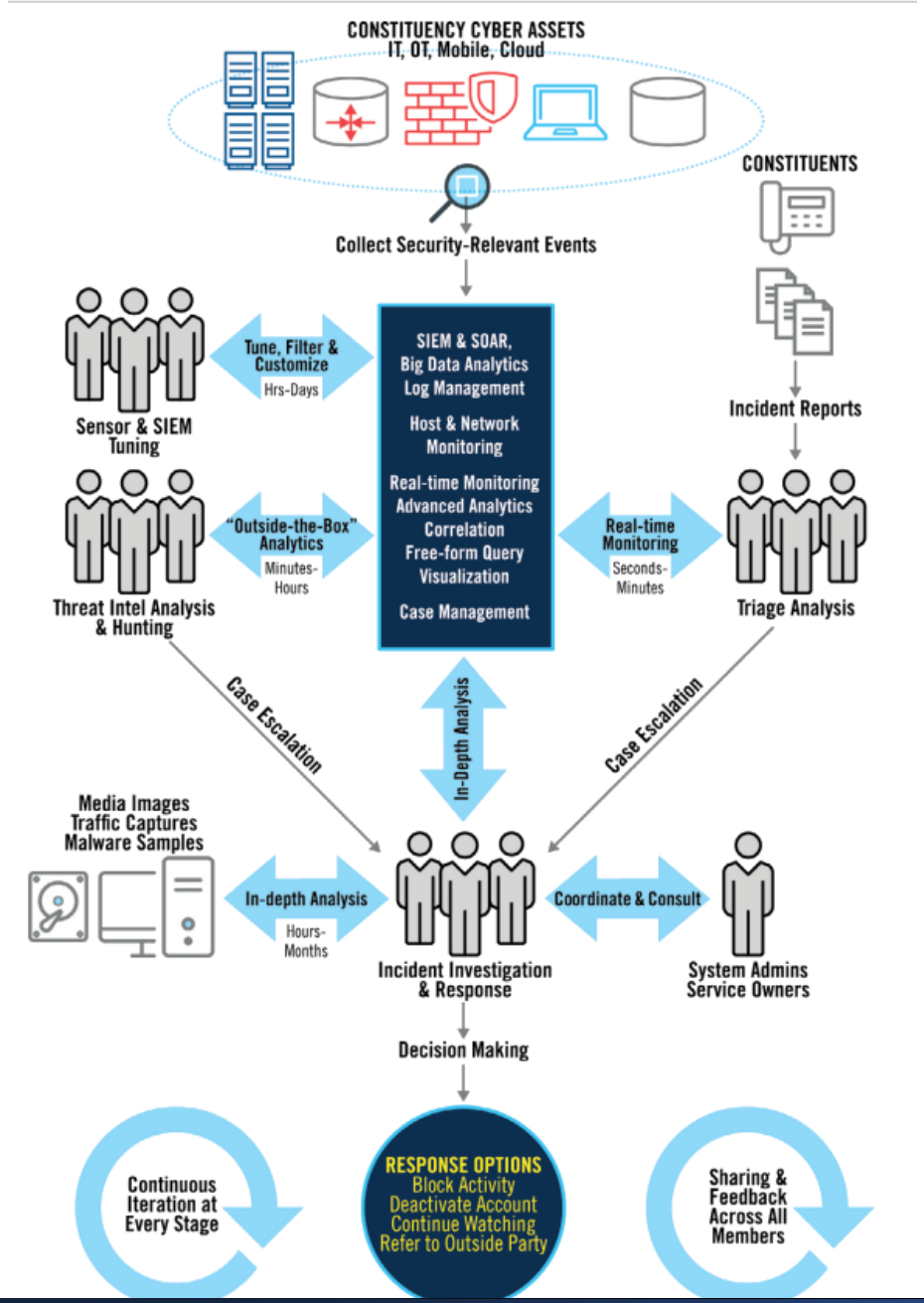


University focuses on technical capabilities, and technical theory

Very little organisational research into Security Operations

What is a SOC?

- A SOC is a team, primarily composed of cybersecurity specialists, organized to prevent, detect, analyze, respond to, and report on cybersecurity incidents.
- Provide a means for constituents to report suspected cybersecurity incidents.
- Provide incident handling assistance to constituents.
- Disseminate incident-related information to constituents and external parties.



11 Strategies of a World Class Cyber Security Operations Centre

PROVIDES A TOP DOWN VIEW ON STRUCTURING A SOC

FOCUSES ON *STRATEGY*

FEW TOOLS, RESOURCES THAT LOW-MID LEVEL PERSONNEL CAN IMPLEMENT

Threat Intelligence

To evolve from a reactive organisation a SOC will need to produce, consume, fuse CTI.

***Ten Strategies* identified:**

Impacts and Benefits

Key Artefacts

Integration Techniques

Core Requirements

Great tools for managers, not so useful for engineers.

Threat Intelligence

CTI EXAMPLES	NOT CTI
Finished Unstructured Threat Reporting	IP Addresses
Structured Threat Reporting	Domain Names
Curated Subscriber Reports and Feedback	Email Addresses
	Malware samples
	Virus Signatures
	PCAP Captures
	DNS Logs
	Intrusion Detection Alerts
	System Logs
	Social Media

Journey

Intelligence Academia

Considers itself a “new” field

- Began in the ‘40s
- Most works were stifled by the Cold War

Unsure if it is even a “profession”

- What defines being a “professional”?

Unsure on the definition of “intelligence”

- When you’re discussing “intelligence” what are you referring to?

Still surrounded by a world of secrecy

- Knowledge is Power

What are we covering?

What are we covering?

Defining and Contextualising Intelligence

How can a SOC be viewed in the eyes of Intelligence

Analytical Processes

Further Resources

Defining and Contextualising Intelligence

Defining and Contextualising Intelligence

Intelligence deals with all the things which should be known in advance of initiating a course of action. (Hoover Commission, 1955)

The product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries or areas. (JP 1-02)

Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding (JP 1-02)

Reduced to its simplest terms, intelligence is knowledge and foreknowledge of the world around us—the prelude to decision and action by US policymakers (CIA)

“Intelligence = Information”?

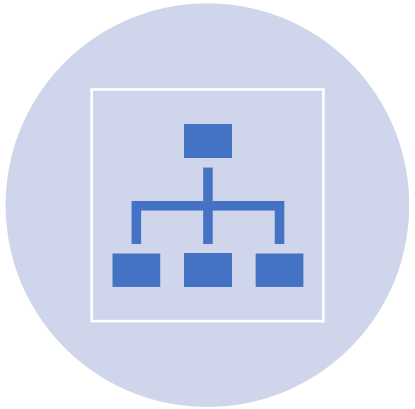
Defining and Contextualising Intelligence

On one hand, [intelligence] refers to an organization collecting information and on the other to the information that has been gathered. (Walter Lacquer, 1985)

Intelligence is the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers; the products of that process; the safeguarding of these processes and this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities. (Mark Lowenthal, 2002)

Defining and Contextualising Intelligence

“INTELLIGENCE IS KNOWLEDGE”



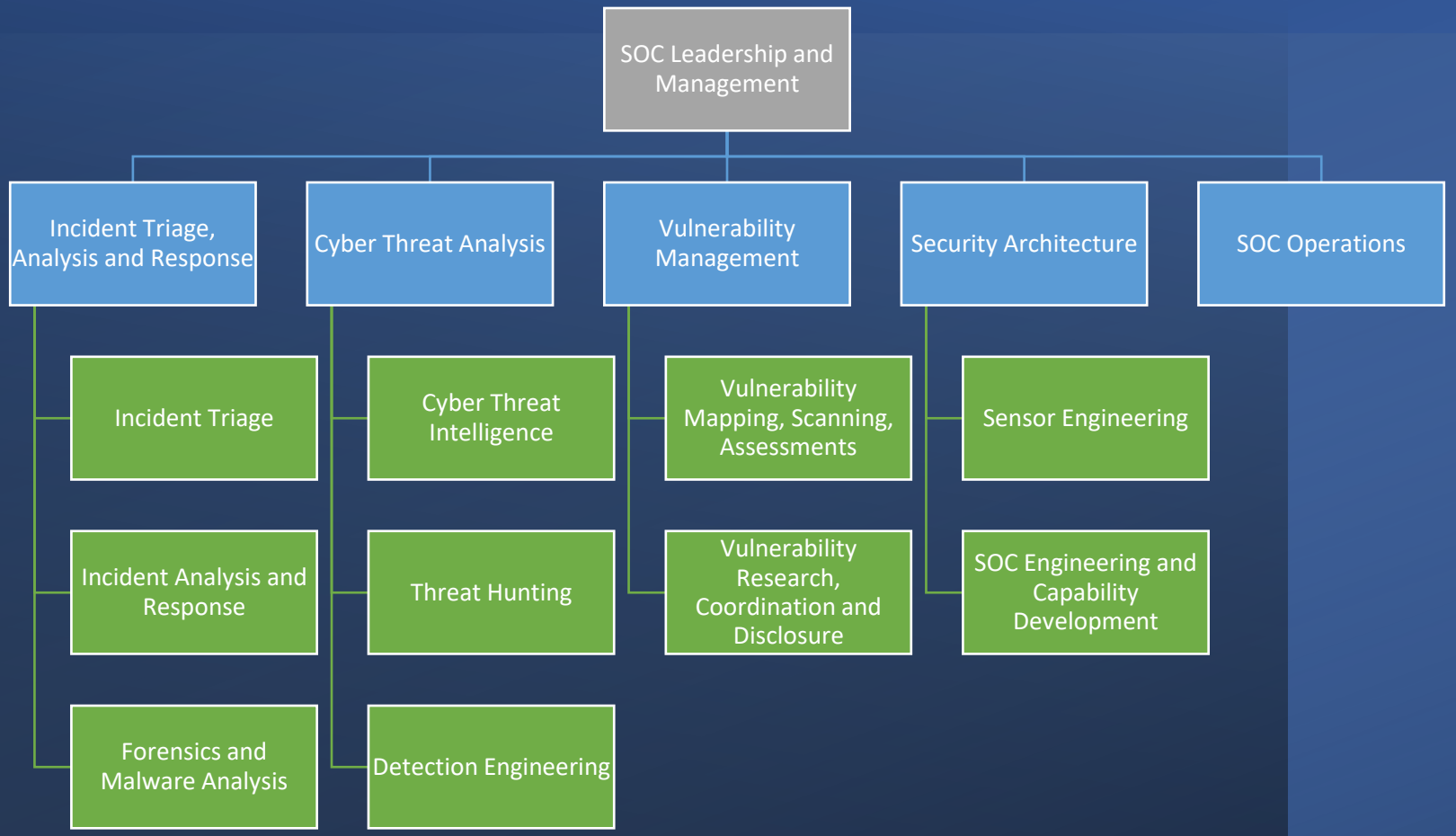
“INTELLIGENCE IS ORGANISATION”

“INTELLIGENCE IS ACTIVITY”

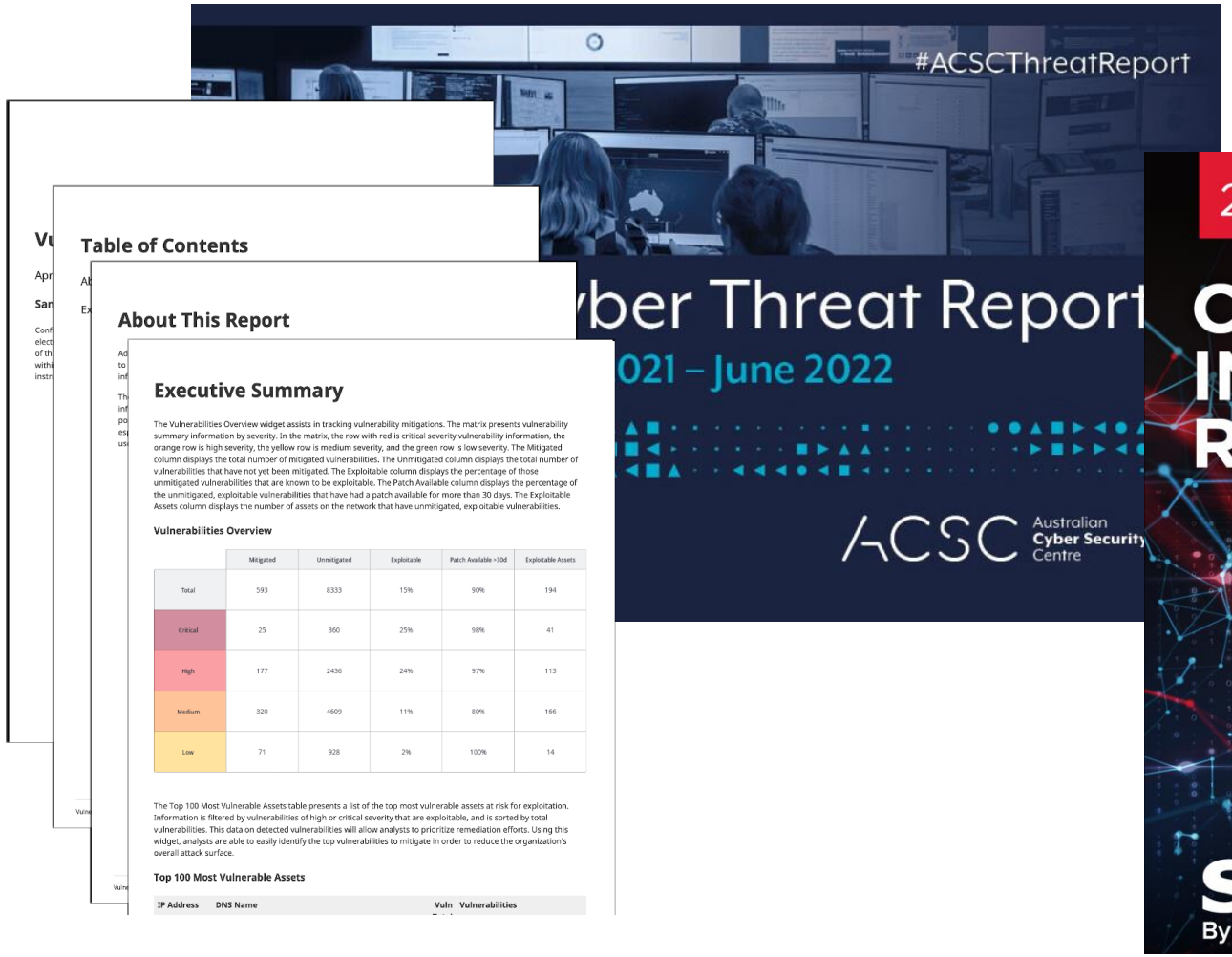
Understanding intelligence context is the biggest trap in pandoras box. If you want to take lessons learned from the Intelligence Community, you will always be fighting against this.

Looking at a SOC through an Intelligence Lens

Contextualising a SOC



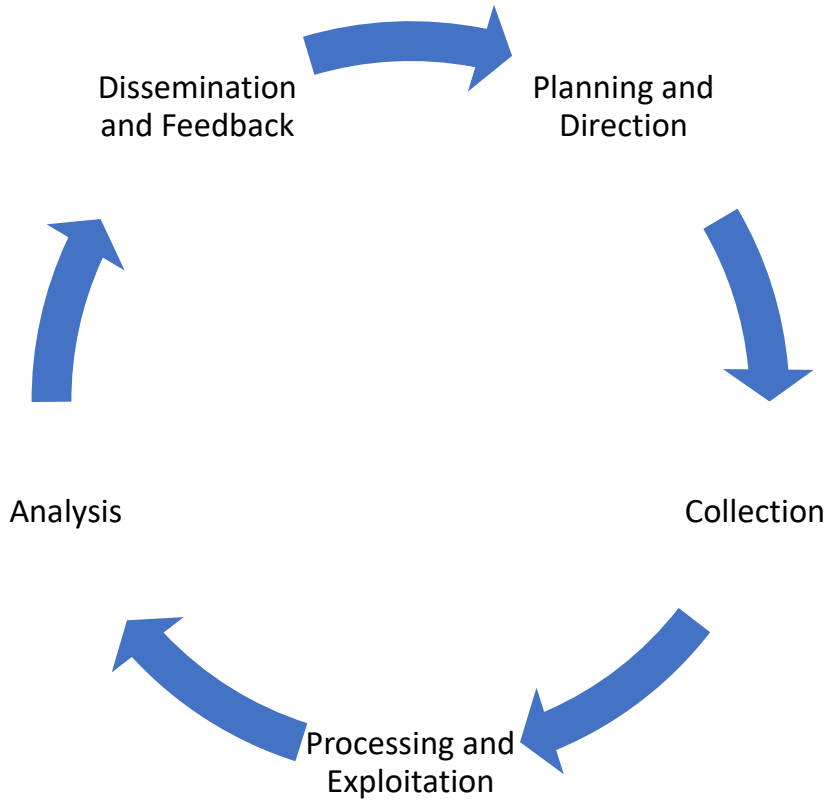
SOC: Intelligence as a Product



Risk Rating	Overall Risk	CVSS 2 Score	Description
CRITICAL	20 - 25	9.0 – 10	Vulnerability was discovered that has been rated as critical and requires resolution as quickly as possible.
HIGH	12 - 16	7.0 – 8.9	Vulnerability was discovered that has been rated as important and requires resolution in the short term.
MEDIUM	6 - 9	4.0 – 6.9	Vulnerability was discovered that has been rated as medium criticality and should be resolved as part of the ongoing security maintenance of the system.
LOW	3 - 5	2.0 – 3.9	Vulnerability was discovered that has been rated as low criticality and should be addressed as part of routine maintenance tasks.
VERY LOW	1 - 2	1.0 – 1.9	Vulnerability was discovered that has been rated as very low criticality and should be addressed to meet with industry standard benchmarks.
INFO	0	0 – 0.9	A finding was discovered that has been rated as informational and normally does not present a risk, but is included for information only.

SOC: Intelligence as an Agency

SOC: Intelligence as a Process



Contextualising a SOC

‘Spies help a sovereign to shift uncertainty into risk, to assess and manage probabilities, and to mitigate hazards.’ (Warner, 2009)

Contextualising a SOC

‘Spies help a sovereign to shift uncertainty into risk, to assess and manage probabilities, and to mitigate hazards.’ (Warner, 2009)

SOCs help an organisation to shift uncertainty into risk, to assess and manage probabilities, and to mitigate hazards.

Analytical Techniques

The Scope of Intelligence Product

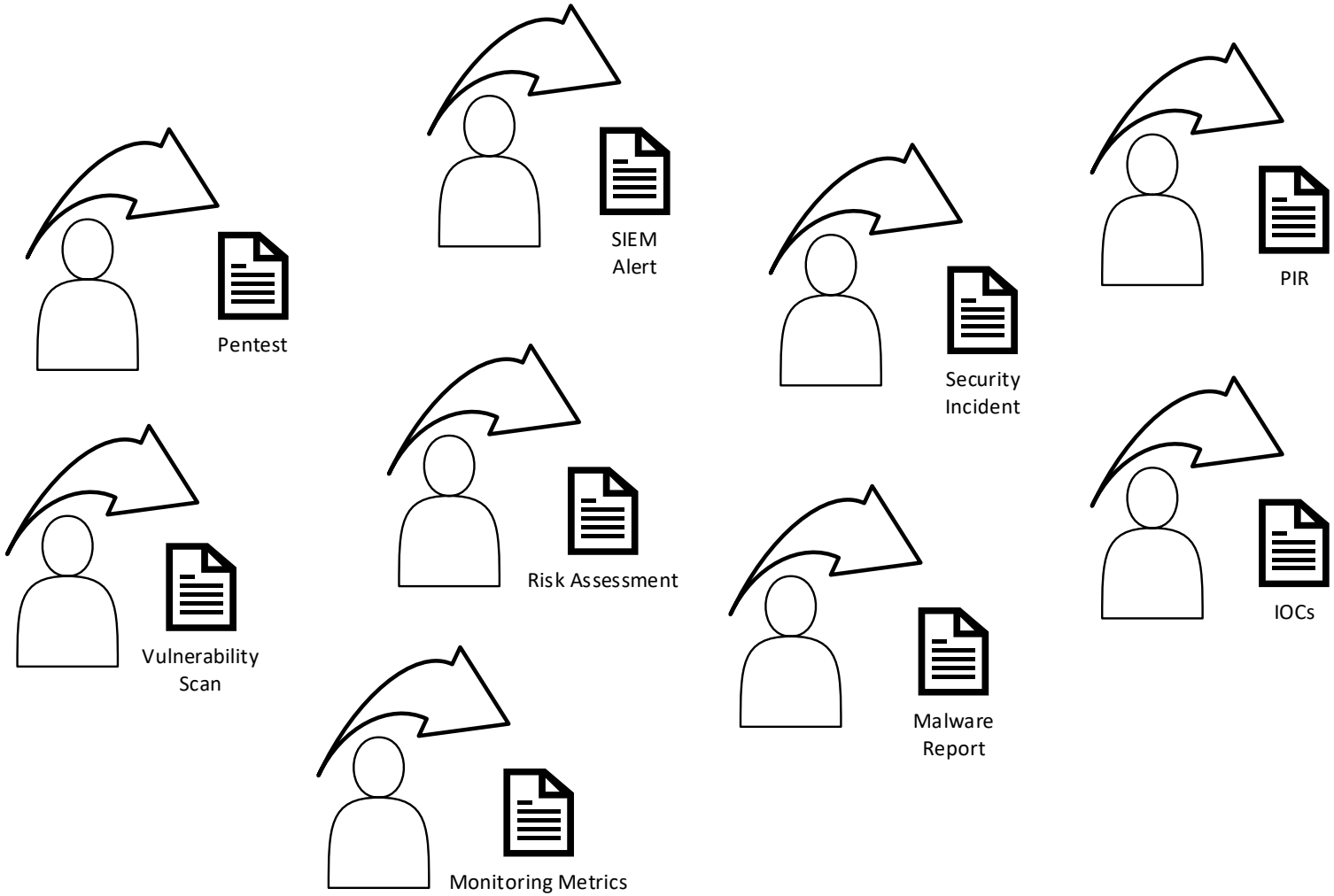
All elements of the SOC *can* create Intelligence Product

But do they?

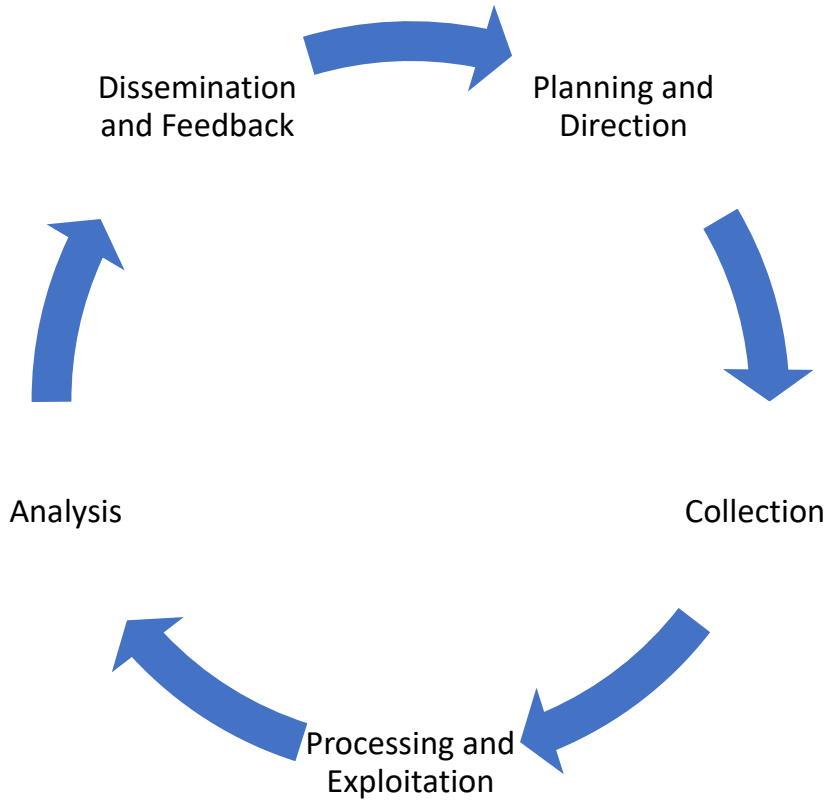
Threat Intelligence

CTI EXAMPLES	NOT CTI
Finished Unstructured Threat Reporting	IP Addresses
Structured Threat Reporting	Domain Names
Curated Subscriber Reports and Feedback	Email Addresses
	Malware samples
	Virus Signatures
	PCAP Captures
	DNS Logs
	Intrusion Detection Alerts
	System Logs
	Social Media

The Scope of Intelligence Product



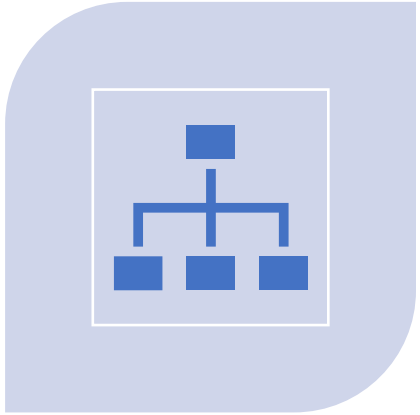
SOC: Intelligence as a Process



Intelligence Cycle for a Data Driven World

Understanding your Audience

STRATEGIC INTELLIGENCE: INFLUENCES HIGH-LEVEL POLICY DECISION MAKING.



OPERATIONAL INTELLIGENCE: SUPPORTS OPERATIONAL LEADERS IN MAKING DECISIONS ON RESOURCE ALLOCATION AND THE TRIAGING OF OPERATIONAL PRIORITIES.

TACTICAL INTELLIGENCE: FOCUSES ON THE SPECIFIC ATTRIBUTES OF TARGET ENTITIES AND IDENTIFIES NEW OPPORTUNITIES.

Targeting Intelligence: Strategic

ASSIST IN DEVELOPING CORPORATE STRATEGY AND POLICY

MONITOR THE INTERNATIONAL OR GLOBAL SITUATION

ASSIST IN DETERMINING PROCUREMENT STRATEGIES

SUPPORT THE DESIGN AND CREATION OF LONG-TERM BUSINESS PLANS

Targeting Intelligence: Operational

FOCUS ON CAPABILITIES AND INTENTIONS OF ADVERSARIES

IDENTIFY ADVERSARY CENTERS OF GRAVITY AND CRITICAL VULNERABILITIES

MONITOR CHANGES WITHIN THE INDUSTRY

ANALYZE THE OPERATIONAL ENVIRONMENT

SUPPORT OPERATIONAL PROJECTS AND INITIATIVES

Targeting Intelligence: Tactical

SUPPORT BAU BUSINESS FUNCTIONALITY

PROVIDE DECISION MAKERS WITH INTELLIGENCE ON IMMINENT OR RECENT THREATS OR VULNERABILITIES

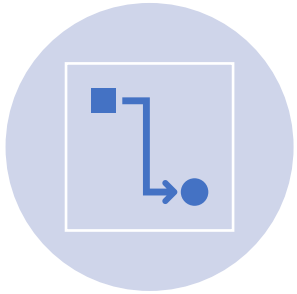
Intelligence Analysis

INFORMATION **PLUS** ANALYSIS EQUALS INTELLIGENCE

INTELLIGENCE SHOULD BE **PROCESSED**

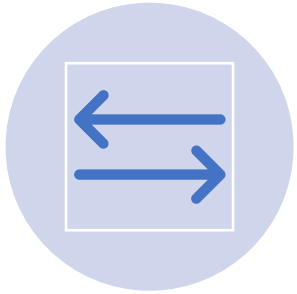
REPEATING RAW INFORMATION DOES NOT REPRESENT INTELLIGENCE

Intelligence Analysis

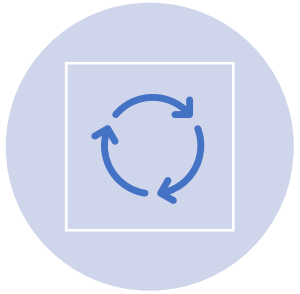


For credibility there must be some understanding for how a conclusion was reached

Intelligence does not have to be certain



Changing an assessment based on new information is fundamentally important



While an intelligence analysis may be “finished”, do not consider that the end.

Intelligence Analysis

SAY WHAT YOU KNOW
(FACTS)

SAY WHAT YOU DON’T KNOW
(INFORMATION GAPS)

SAY WHAT YOU THINK
(ANALYSIS)

Intelligence Analysis

- Why
- Why not
- How
- What if
- How does X compare to Y?
- What is the evidence for X?

Analytic Methodologies

- Issue Development
- Evidence Diagnostics
- Hypothesis Generation
- Structured Analytical Techniques

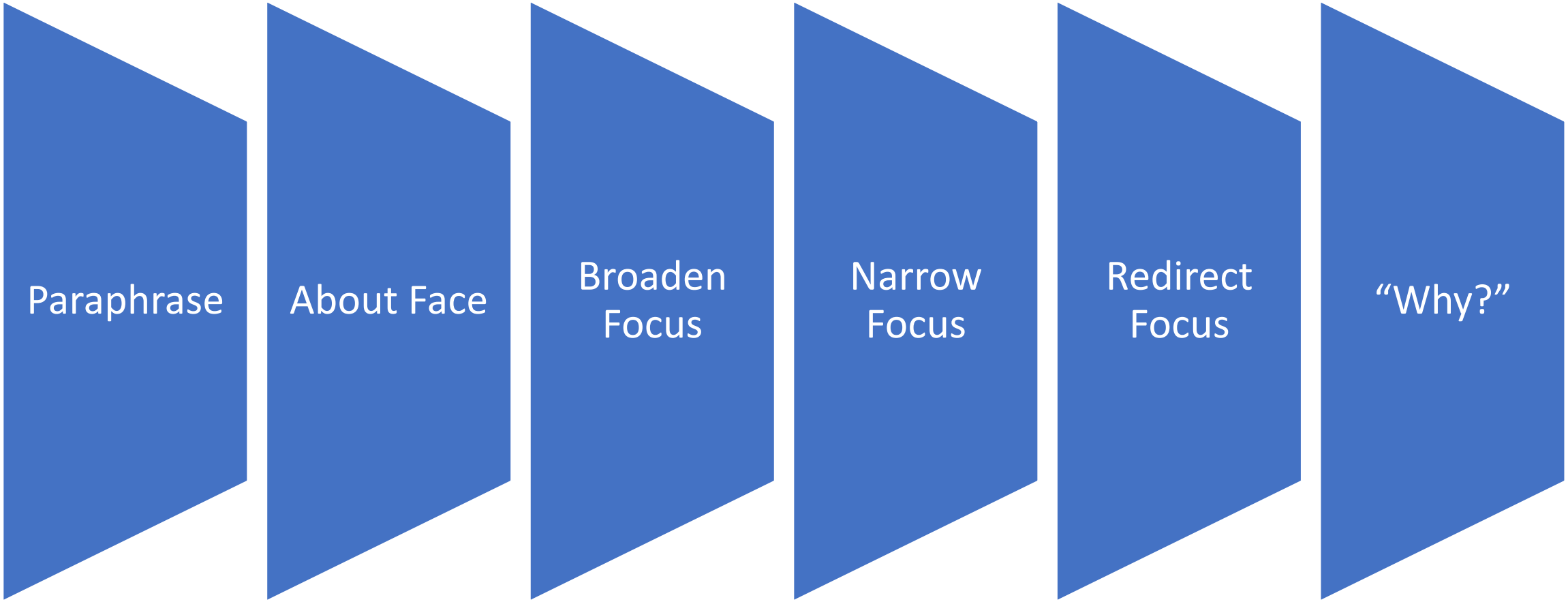
Issue Development

Answering Questions of Judgement

Proper identification can save a lot of time

- Solution Driven?
- Assumption Driven?
- Too broad or ambiguous?
- Too narrow or misdirected?

Issue Development



Evidence Diagnostics

It is important to step back and consider the quality of your information

Reliability, Viability

Low reliability or quality does not immediately disqualify the information.

Where analysts work in the same area for long periods of time, incremental changes may be missed

Hypotheses Generation

PRELIMINARY EXPLANATIONS OR POSSIBLE OUTCOMES THAT ARE MEANT TO BE TESTED.

MULTIPLE WORKING HYPOTHESES ARE HIGHLY RECOMMENDED.

Hypotheses Creation – Divergent/Convergent

- ORGANISE THE GROUP
- FOCUS ON A SPECIFIC TOPIC OR QUESTION
- HAVE EVERYONE WRITE DOWN ONE IDEA BEFORE DISCUSSION STARTS
- GENERATE AS MANY IDEAS AS POSSIBLE, DISMISS NOTHING
- TAKE A BREAK
- GROUP IDEAS BY THEME
- REVIEW AND CONSIDER

Structured Analytic Techniques

BREAKING DOWN INFORMATION INTO SUBSETS UNTIL THE HYPOTHESES IS FOUND TO BE EITHER SENSIBLE OR UNTRUE.

HELP ANALYSTS MAKE SENSE OF COMPLEX PROBLEMS

LET ANALYSTS COMPARE AND WEIGH INFORMATION AGAINST EACH OTHER

ENSURE ANALYSTS FOCUS ON THE ISSUE UNDER STUDY

FORCE ANALYSTS TO CONSIDER ONE ELEMENT AT A TIME

AID ANALYSTS IN OVERCOMING THEIR MINDSETS AND BIASES

Further Resources

Reading List

- Sherman Kent – Strategic Intelligence for American World Policy (1951)
- Peter Gill & Mark Phythian - Developing Intelligence Theory (2018)
- Mark Phythian – Understanding the Intelligence Cycle (2013)
- Mandeep Dhami - Critical Review of Analytic Techniques (2016)
- Mark Harrison - Tradecraft to standards: Moving Criminal Intelligence Practice to a Profession through the Development of a Criminal Intelligence Training and Development Continuum (2020)
- Rob Johnson – Analytic Culture in the US Intelligence Community (2005)
- John Gentry – Professionalisation of Intelligence Analysis: A Skeptical Perspective (2016)

Thank you