# SANS578

# Aa

# Bb

**Bias** *[b1/p32]*

**Bias Example** *[b1/p33]*

**Bias Field of View** *[b1/p40]* Each person and org has a limited field of view into threats. This is determined by the operation environent and intelgence reqs tthth

**Bias: Anchoring/Focusing Bias** *[b4/p28]* Anchoring refers to beginning with an assumption or assessment and then adjusting one's assessment as new information becomes available, rather than taking the information as a whole fir an assessment.

**Bias: Cognitive Biases** *[b4/p26]* Constrains on how we think that influence incorrect decisions and assessments. Create your own version of reality where inaccurate judgments and illogical interpretations occur.

**Bias: Confirmation Bias** *[b4/p29]* Include or Reject evidence based on its alignment to a preferred hypothesis. Also includes the tendency to ascribe more or less significance to evidence based on its support of a preferred hypothesis or outcome.

**Bias: Congruence Bias** *[b4/p30]* related to Confirmation Bias but in a more abstract way. It is the failure to adequately present and test alternative competing hypotheses and instead find different ways to present data that tests an existing hypothesis.

**Bias: Experience** *[b4/p36]*

**Bias: Hindsight Bias** *[b4/p31]* Tendency to see an unpredictable event as an obvious result of a set of conditions or parameters.

**Bias: Identify and Defeating** *[b4/p22]* All analysts have Bias.

**Bias: Illusory Correlation** *[b4/p32]* Tendency to observe a correlation between two observations when no such correlation exists, particularly when those observations are each relatively unusual.

**Bias: Mirror Image** *[b4/p27]* type of cognitive bias. Mirror images are when we fool ourselves into believing that the entity/person/etc would behave in any way similar to what we would.

# Cc

# Dd



# Ee



# Ff



# Gg



# Hh

# Ii

**Indicator** *[b1/p66]* Data + Context = Indicator. Indicator must INDICATE something.

**Indicator Fatigue** *[b1/p73]*

**Indicator Life Cycle** *[b1/p67]*

**Indicator Life Cycle** *[b2/p77]*

**Indicator Life Span** *[b1/p72]*

**Indicator Types** *[b3/p34]*

**Indicator: Behavioural Analytics** *[b1/p89]*

**Information to Change (Leaked)** *[b5/p115]*

**Intelligence** *[b1/p18]*

**Intelligence Consumption: Active Defence** *[b1/p85]*

**Intelligence Consumption: Active Defence** *[b1/p85]*

**Intelligence Consumption: Architecture** *[b1/p87]*

**Intelligence Consumption: Architecture** *[b1/p87]*

**Intelligence Consumption: Intelligence** *[b1/p84]*

**Intelligence Consumption: Intelligence** *[b1/p84]*

**Intelligence Consumption: Offense** *[b1/p83]*

**Intelligence Consumption: Passive Defence** *[b1/p86]*

**Intelligence Consumption: Passive Defense** *[b1/p86]*

**Intelligence Consumption: To Generation** *[b1/p98]*

**Intelligence Driven Hypothesis** *[b4/p64]*

**Intelligence Generation Versus Consumption** *[b1/p80]*

**Intelligence Lifecycle** *[b1/p38]*

**Intelligence Requirement (Planning Collection)** *[b1/p115]*

**Intelligence Requirements** *[b1/p56]*

**Intelligence Requirements Examples** *[b1/p97]*

**Intelligence Sources** *[b1/p20]*

**Intelligence: Gain/Loss** *[b2/p49]*

**Intended Audience** *[b1/p96]* The intended audience and their goals determine the type of threat intelligence generated and how it is to be used.

**Intro to Diamond Model** *[b2/p28]*

**Intrusion Overlaps** *[b4/p102]*

**Intrusions** *[b1/p57]* Core of all CTI is Intrusion Analysis. Intrustions are any attempt, successful or failed that the adversary makes to compromise or attack systems.

**IOC - Active Defence** *[b1/p85]*

**IOC - Passive Defence** *[b1/p86]*

**IOC Vertices** *[b2/p28]*

**Iran CIB Pros and Cons** *[b5/p82]*

# Jj

**Judgment** *[b1/p27]* The role of an analyst is not simply to collect information about a particular incident or entity and present it as a list of facts. It is to assess what that information signifies and how it impacts.

# Kk



# Ll



# Mm

# Nn



# Oo



# Pp



# Rr

# Ss

# Tt



# Uu



# Vv