

SANS578

Aa

ACH for Intrusion-Cluster Correlation [b4/p76]

Actions on Objectives - Network Pivoting
[b2/p85]

Active Defence Intelligence Consumption
[b1/p85]

Activity Group [b1/p58]

Additional OSINT [b3/p74]

AlienVault OTX [b3/p75]

Analysis [b1/p26] examination of the elements or structure of something. Breaking something down into constituent parts to understand its operation. Think about how we arrive at conclusions instead of accepting what we see.

Analysis In Action [b1/p30]

Analysis of Competing Hypotheses [b4/p39-48]

Analysis of Competing Hypotheses [b4/p39]

Analysis of Competing Hypotheses: Determine Evidentiary Dependence [b4/p46]

Analysis of Competing Hypotheses: Diagnostics
[b4/p43]

Analysis of Competing Hypotheses: Hypotheses
[b4/p41]

Analysis of Competing Hypotheses: Prioritize the Hypotheses [b4/p45]

Analysis of Competing Hypotheses: Refine the Matrix [b4/p44]

Analysis of Competing Hypotheses: Report Conclusions [b4/p47]

Analysis of Competing Hypotheses: Support the Hypotheses [b4/p42]

Analysis: Link Analysis Tools [b4/p53]

Analysis: Types of Analysis [b4/p51]

Analyst [b1/p7] Fully analyze successful and unsuccessful intrusions by threat actors. Construct descriptions of campaigns, actors and organizations. Seek out, collect and properly exploit intelligence from others. Generate intelligence from their own data sources and share it accordingly. Manage intelligence to further the objectives of the org

Analytic Doctrine [b1/p24]

Approaches to Attribution [b5/p100] TRUE
ATTRIBUTION

Assets Exposed to the Internet [b3/p76]

Attribution [b5/p99]

Attribution as an Intelligence Requirement
[b5/p98]

Attribution: Example Use Case [b5/p103]

Attribution: Never Straightforward [b5/p104]

Attribution: Without Attribution [b5/p102]

Autonomous System Numbers (ASN) Lookup
[b3/p45-46]

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 environment and intelligence 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

C2 Decoding [b2/p93]

C2 Domain Registration [b3/p38]

Campaign [b1/p60] Campaigns are identified as the mission focus of the adversary across multiple intrusions.

Case Study: APT10 & APT31 [b4/p93-96]

Case Study: APT10 and Cloud Hopper [b5/p87-92]

Case Study: Axiom [b5/p5-10]

Case Study: Carbanak [b1/p106-112]

Case Study: CVE-2012-1761 [b3/p100]

Case Study: Epic Turla Out of This World C2 [b3/p51]

Case Study: GlassRAT [b3/p61-64]

Case Study: Hacking Team [b5/p29-33]

Case Study: HEXANE [b3/p4-9]

Case Study: Human Operated Ransomware [b4/p4-11]

Case Study: Lazarus Group [b5/p121-127]

Case Study: MoonLight Maze [b1/p10-16]

Case Study: New York Stock Exchange (NYSE) Computer Glitch [b4/p33]

Case Study: Operation Aurora [b1/p45-50]

Case Study: Operation Bodyguard [b1/p22]

Case Study: Panama Papers [b4/p59-66]

Case Study: Poison Hurricane [b3/p44]

Case Study: Promethium and Neodymium [b1/p74-79]

Case Study: Soviet Disinformation Operations [b5/p116]

Case Study: The First Ever Electric Grid Focused Malware [b1/p100 - 101]

Case Study: Turkey Pipeline Explosion [b4/p35]

Categorize Evidence using Threat Definition [b5/p112]

Cluster 1-2-1 Mapping [b4/p73]

Cluster 1-2-1 Mapping: Issues [b4/p74]

Collective Intelligence Framework [b3/p72]

Command and Control [b2/p22]

Commands: awk [b2/p107]

Commands: date [b2/p71, 76, 91]

Commands: grep [b2/p71, 76, 91, 96, 107]

Commands: openssl [b2/p24, 107]

Commands: perl [b2/p107]

Commands: ra [b2/p68]

Commands: sed [b2/p107]

Commands: UnRAR [b2/p109]

Common Informal Fallacies [b4/p21]

Counter Intelligence [b1/p21] Identification, assessment, and neutralization of adversary intelligence activities

Course of Action [b2/p28]

Course of Action Matrix [b2/p39]

Course of Action: Deceive [b2/p45]

Course of Action: Degrade [b2/p44]

Course of Action: Deny [b2/p42]

Course of Action: Destroy [b2/p46]

Course of Action: Detect [b2/p41]

Course of Action: Discover [b2/p40]

Course of Action: Disrupt [b2/p43]

Course of Action: Selection and Exclusivity [b2/p47] All Passive CoA should be followed and ONE active/Mitigation CoA should be selected

CTI Terminology [b1/p53]

Cum hoc ergo propter hoc [b4/p34] Confusion of correlation and causation.

CVE-2014-0160 [b2/p17]

CVE-2014-6271 [b2/p17]

CVE-2014-7169 [b2/p17]

CVE-2016-4117 [b1/p76]

Cyber Kill Chain - Delivery [b2/p14]

CyberChef [b3/p78]

Dd

Data Analysis [b4/p55]
Data Pivoting [b3/p32-33]
Data Pivoting: Example [b3/p35-37]
Data vs Intelligence [b1/p41]
Data-Driven Versus Conceptually-Driven Analysis [b1/p28]
DataSploit [b3/p74]
DC3 Malware Tool [b3/p23]
DDNS Dynamic DNS Domains [b3/p40]
DDNS: For Adversaries [b3/p42]
DDNS: Legitimate but Compromised [b3/p43]
DDNS: Manager [b3/p41]
Defining Cyber Threat Intelligence [b1/p52]
 Analyzed Information about the hostile intent, opportunity and capability of an adversary that satisfies a requirement.
Deriving Intent [b5/p109]
Details, Roles and Requirements [b2/p55-56]
Diamond Model [b2/p33-36]
Diamond Model Activity Group [b4/p82]
Diamond Model Axioms [b2/p29]
Diamond Model Information [b2/p137]
Diamond Model Shortcut (Rule of 2) [b4/p89]
Diamond Model: Analytic Findings [b5/p74]
Diamond Model: Meta Features [b4/p81]
Diamond: Adversary [b2/p31]
Diamond: Capability/TTP [b2/p33]
Diamond: Infrastructure [b2/p34]
Diamond: Victim [b2/p35]
Disk Forensics [b2/p112]
Disk Forensics [b2/p97]
DNS Cache-Poison [b2/p45]
DomainTools [b3/p54-57]

Ee

Effective Report Writing [b5/p77]
Equation Group Pros and Cons [b5/p85]
Exfiltration [b2/p109]
External Intrusion Report [b4/p80]

Ff

Fallacies: Informal [b4/p21] Appeal to the Stone, Argument from Silence, Argument from Repetition
Fallacies: Logical [b4/p23] Anecdotal Fallacy + Appeal to Probability
Fallacies: Other Common Fallacies [b4/p25] Burden of Proof, Middle Ground
False Flags [b5/p117]
Full Packet Capture [b2/p88]

Gg

Generate Hypotheses [b1/p29]
Generating Intelligence Requirements [b1/p114]
 When generating intelligence requirements, it would be great if consumers could articulate exactly what they need and expect from the CTI function.
Geographical Information [b3/p77]
Geographical Information and Maps [b3/p77]
Geopolitical Conflict [b5/p106]
Geopolitical Conflict Intersects Cyber [b5/p106]

Hh

Hindrances to Good Analysis [b1/p32]
HTTP Traffic Analysis [b2/p70]

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. Intrusions 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

Key Indicator Examples [b1/p70-71]

Kill Chain: Actions on Objectives [b2/p25]

Kill Chain: Actions on Objectives Example [b2/p27]

Kill Chain: Command and Control [b2/p22]
Controller – Adversary System

Kill Chain: Command and Control Example [b2/p24]

Kill Chain: Completion [b2/p80]

Kill Chain: Delivery [b2/p14]

Kill Chain: Delivery Example [b2/p15]

Kill Chain: Exploitation [b2/p17]

Kill Chain: Exploitation Example [b2/p18]

Kill Chain: Installation [b2/p19]

Kill Chain: Installation Example [b2/p20]

Kill Chain: Overview [b2/p6]

Kill Chain: Overview [b2/p6]

Kill Chain: Recon [b2/p8]

Kill Chain: Recon Example [b2/p10]

Kill Chain: Weaponization [b2/p12]

Kill Chain: Weaponization Example [b2/p13]

Ll

Leveraging OSINT [b3/p67]

Limit Bias [b1/p32]

Link Analysis [b4/p52]

Logrotate [b2/p61]

Mm

Maltego [b3/p107-112]

Maltego (Link/Entities) [b3/p108] Entity has an icon in the headers.

Maltego: Casefile Bubble ChartView [b4/p54]

Malware Configuration Data [b3/p16]

Configuration data can be another extremely important dataset when evaluating Malware. Not only does some Config data give insights to the dev team such as a mutex. But some can also be set by the operators of the malware and speak more to specific clusters.

Malware Header Metadata [b3/p13]

Malware Information Sharing Platform [b4/p15]

Malware: Code Reuse [b3/p14] Code Reuse is a very effective tool to link malware samples together and potentially intrusions. Very rarely do adversaries create entirely unique code for their operations. Can help reveal links in the Adversary feature of the Diamond Model.

Malware: Collection [b3/p11] Malware is an adversary tool to operate in the environment and achieve their objectives. Not all adversaries need malware (they are use LOLBAS) but it is commonly leveraged.

Malware: Human Fingerprints [b3/p12] We can extract something from the malware which may indicate something about the human behind the capability instead of just components of the capability.

Measuring Threat Feeds [b3/p70]

Memory Analysis Volatility [b2/p63]

Memory Forensics [b2/p95]

Mental Model [b1/p35]

Mental Models [b1/p35] Mental Models are experience-based assumptions and expectations of the way the world operates.

Merge Diamond Model and Kill Chain [b2/p36]

Milestones [b4/p48] Analytical conclusions should always be regarded as tentative. As evidence may change in time.

MindMup [b1/p43]

MISP [b4/p15-17]

MITRE ATT&CK [b2/p50]

MITRE ATT&CK: Groups [b4/p71]

MITRE ATT&CK: TTP [b2/p51]

Nn

Names/Identifiers [b4/p69]

Naming Conventions [b4/p70]

Netflow [b2/p67-68]

Oo

Observations for CTI Analysts: Closing Thoughts [b5/p96]

Observations for CTI Analysts: Communicating Broadly [b5/p93]

Observations for CTI Analysts: Human Fingerprints [b5/p94]

Observations for CTI Analysts: Timelines [b5/p95]

Offense [b1/p83]

Open-Source Intelligence [b3/p66] Open-Source Intelligence Collection (from libraries, public records, or the internet)

Operational: Additional Resources [b5/p40]

Operational: Adversary Operations [b5/p36]

Operational: Campaign Heatmap [b5/p51]

Operational: Completeness [b5/p57]

Operational: Email Delivery Success [b5/p56]

Operational: Embrace Metrics [b5/p50]

Operational: Incident One-Slider [b5/p53]

Operational: ISAC and ISAO [b5/p39]

Operational: Methods of Sharing Best Practice [b5/p46]

Operational: Mitigation Scorecard [b5/p55]

Operational: National-Level Government Information [b5/p38]

Operational: Organizational Heatmaps [b5/p52]

Operational: Partners and Collaboration [b5/p37]

Operational: STIX 2.* [b5/p45]

Operational: STIX 2.1 Objects [b5/p44]

Operational: STIX/TAXII [b5/p41]

Operational: TAXII Implementations [b5/p43]

Operational: Threat Intelligence [b5/p35]

Operational: Woe the Lowly Metric [b5/p49]

Pp

Passive DNS Vantage [b3/p47]

Passive DNS: Free/Paid [b3/p49]

Passive DNS: Mnemonic [b3/p50]

Passive DNS: Providers [b3/p48]

Persona [b2/p108]

Pivot: C2 [b2/p87]

Pivot: Host [b2/p86]

Pivot: Network [b2/p85]

Priority Intelligence Requirement (PIR) [b1/p95]

Proofpoints North Korea Report Pro and Cons [b5/p80]

Proxy Logs [b2/p70]

Purposes of CTI Teams [b1/p99] CTI Teams can support various roles within an organizations, from the SOC to VM to the CISO and the board of directors. The role will depend on the needs of that organization.

Pyramid of Pain [b1/p90]

Rr

RecordedFuture [b3/p86-89]

Reported Intrusion [b2/p66]

Reproduce AOA [b2/p88]

Responder Action [b2/p64]

Retire Clusters [b4/p91]

Reverse Engineering [b2/p99]

Rosetta Stone [b4/p72]

Rule of 2 (COA) [b2/p47]

Ss

Security from Outside Perimeter [b3/p96]

Sherman Kent [b1/p23]

Shodan [b3/p76]

Sliding Scale of Cyber Security [b1/p81]

State Attribution [b5/p110]

State Attribution: ACH Matrix Example
[b5/p114]

Storing Collected Intelligence [b4/p13] It is important to store collected information and intelligence in your environment. Storing it in a usable and quickly accessible format allowed it to be made available to those who need it.

Storing Collected Intelligence: Best Practices
[b4/p18]

Storing/Sharing Platforms [b4/p14]

Strategic: Assessments [b5/p73] ASSESSMENTS ARE NOT FACTS

Strategic: Confidence Assessments [b5/p75]

Strategic: Constructing Assessments [b5/p76]

Strategic: Diamond Model and Analytic Findings [b5/p74]

Strategic: Estimative Language [b5/p70]

Strategic: Estimative Scales [b5/p72]

Strategic: Making the Business Case for Security [b5/p64]

Strategic: Observation Versus Interpretation
[b5/p68]

Strategic: Outcome Indictments [b5/p63]

Strategic: Report Expectations [b5/p65]

Strategic: Reports/Narrative-Form Intelligence
[b5/p67]

Strategic: Threat Intelligence [b5/p62]

Structured Analytic Techniques [b1/p37]

Structured Analytic Techniques assist analysts in deriving better analysis (both consistency and approach) while reducing the impact of Bias. SAT's will not reduce fallacies, which are flaws in the application of logic.

Structured Analytic Techniques: Example Tools
[b1/p42] Brainstorming Tools & Sorting Tools.

Synthesis [b1/p26]

System Analysis [b1/p118]

Tt

Tactical: Audience [b5/p12]

Tactical: Complex YARA [b5/p17]

Tactical: Validating Signatures and IOCs
[b5/p27]

Tactical: YARA [b5/p13]

Tactical: YARA Hex Special Values [b5/p16]
Hex contains question marks for wildcards.

Tactical: YARA Key Points [b5/p15]

Tactical: YARA Rule Conditions [b5/p21]
Shows example conditions

Tactics, Techniques and Procedures (TTP)
[b1/p63]

Target-Centric Intelligence Analysis (Non-Linear) [b1/p121]

Temporal Data Analysis [b4/p56]

Thinking About Thinking and Perception
[b1/p29] Deriving a conclusion should be much like a forensic process: defensible, repeatable and understandable. Perception should be an active process instead of a passive one.

Threat [b1/p55] Intent + Opportunity + Capability.
Organizations must know what their threats are to accurately collect and use threat intelligence.

Threat Actor [b1/p59]

Threat Behavioural Analytics [b1/p89]

Threat Data Feeds [b3/p68]

Threat Detection [b1/p88]

Threat Intelligence Quotient (TIQ) Test
[b3/p69]

Threat Modelling [b1/p119]

Threat Modelling: Example [b1/p123-125]

Threat Modelling: Granular [b1/p126]

TimeCard URL [b2/p132]

TLS Cert [b3/p93] Subject contains the domain

TLS Cert: Datastore [b3/p94]

TLS Cert: Scan Providers [b3/p96]

TLS Searching Tips [b3/p97]

Tools and Tradecraft [b1/p48]

Trade Craft [b1/p64]

Trade Craft [b1/p54]

Traffic Light Protocol [b1/p61]

Trend Analysis [b4/p58] Kill Chain or Diamond Model completion yields intelligence. Intelligence over time reveal patterns between intrusions.

True Attribution [b5/p100]

Uu

Understanding Opportunity [b5/p113]

URL Structure [b2/p74]

Vv

VERIS [b1/p127] The Vocabulary for Event Recording and Incident Sharing is a framework that provides a common language for describing security incidents in a structured and repeatable manner

VERIS: Fundamentals [b1/p128]

VirusTotal [b3/p19]

VirusTotal: Details [b3/p21]

VirusTotal: Enterprise [b3/p22]

VirusTotal: Results [b3/p20]