

An abstract graphic featuring a complex network of interconnected nodes and lines, resembling a molecular structure or a data network, set against a dark background with bokeh light effects.

HOW TO CREATE A GOOD INTELLIGENCE PRODUCT

(We're not talking about *just* Cyber
Threat Intelligence)

An abstract graphic featuring a dark background with a complex network of white dots and lines, resembling a molecular structure or a data network. The dots are of varying sizes and are connected by thin, light gray lines, creating a sense of depth and connectivity.

HOW CAN I APPLY INTELLIGENCE TO MY SECURITY OPERATIONS?

While creating this talk I found it to represent more about *how can I as an Cybersecurity Professional apply intelligence.*



BACKGROUND

ANALYTIC PRODUCT?

- Overreliance on Third Party Intelligence
- Lack of contextual understanding for the intelligence that we did have
- We're producing a lot of intelligence
- We don't know it
- You probably are too

3

In trying to develop my last companies SOC we wanted to create our own intelligence. Most organisations with an intelligence function have it spun up by ex-defence, ex-spy type individual
Surely I can find some learning online?

Academia for cybersecurity mainly points at the next and best AI ML Threat Fabric Security ETL Mindshare possibility. Not much academic development has been done in the space of processes, teams, and people.

However intelligence academia is big and bold, and a lot to learn from. When I shifted my education focus from *cyber* to *intelligence* I came to realise that:
We have a lot of intelligence, we don't know it, and most cyber professionals probably do to.

WE'RE USED TO SEEING THESE...

Table of Contents

About This Report

Executive Summary

2020 CYBER THREAT INTELLIGENCE REPORT
By Authentic8

Cybersecurity INSIDERS
November Threat Report 2021 – June

| 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. |

4

ACSC, Crowdstrike threat reeports.
CVEs and new vulnerabilities.

WE NEVER CONSIDERED THIS

| Acme Corporate Office Threat Exploitability Matrix | | Asset | | | | | | | | | | | | | | |
|-------------------------------------------------------|---------------------|--------|------------------|-------------|---------------|----------|-------------|--------------|-----------------|------------------|----------------|-----------------------|-----------------|--------|----------------|--------|
| Threat Source | | User | Office Equipment | Client Data | Internal Data | Software | Database(s) | Connectivity | Host machine(s) | Mobile Equipment | File Server(s) | Authentication Server | Security Server | Switch | Gateway device | WAP |
| Natural | Storm | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low |
| | Natural Disaster | Medium | Medium | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low |
| Environmental | Power outage | Low | Medium | Low | Low | Low | Medium | Medium | Medium | Low | Medium | Medium | Medium | Medium | Medium | High |
| | Water damage | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low |
| | Fire | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low |
| | Radio Interference | Low | Low | Low | Low | Low | Low | Low | High | Low | Low | Low | Low | Low | Low | Low |
| | Resource Misuse | Low | Low | Low | Low | Medium | Low | Medium | High | Low | Low | Low | Low | Low | Low | Low |
| | Unauthorized access | Low | Medium | Medium | Low | Medium | Medium | Low | Low | Medium | Medium | Medium | Medium | Medium | Medium | Medium |
| | Terrorism | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low | Low |
| | Sabotage | Low | Medium | Medium | Medium | Low | Medium | Low | Low | Low | Low | Low | Low | Low | Low | Low |

Project context for Next Generation Firewall im

The following project is for the Next Generation Firewall implementation proposal. It includes the requirements of the client company architecture, high performance features, etc.

Top-Level Controls Maturity

| Category | Control | Priority Rank | No. Of Impacts | Maturity Gap to Plan | Priority |
|---------------|----------------------------------------------------------------|---------------|----------------|----------------------|----------|
| Identify (ID) | Asset Management (ID.AM) | 1 | 1 | -0.8 | Low |
| | Business Environment (ID.BE) | 16 | 1 | -0.8 | Low |
| | Governance (ID.GV) | 18 | 1 | -0.8 | Low |
| | Risk Assessment (ID.RA) | 14 | 1 | -0.8 | Low |
| | Risk Management Strategy (ID.RM) | 16 | 1 | -0.8 | Low |
| Protect (PR) | Supply Chain Risk Management (ID.RC) | 17 | 2 | -0.5 | Low |
| | Identity Management, Authentication and Access Control (PR.AC) | 10 | 2 | -0.8 | Low |
| | Awareness and Training (PR.AT) | 20 | 2 | -0.8 | Low |
| | Data Security (PR.DS) | 4 | 2 | -0.2 | Low |
| | Information Protection Processes and Procedures (PR.IP) | 12 | 1 | -0.5 | Low |
| Detect (DE) | Maintenance (PR.MA) | 1 | 4 | -0.7 | Low |
| | Protective Technology (PR.PT) | 13 | 3 | -0.8 | Low |
| | Assets and Events (DE.AE) | 15 | 1 | -0.8 | Low |
| | Security Continuous Monitoring (DE.CM) | 5 | 3 | -0.8 | Low |
| | Detection Processes (DE.DP) | 10 | 3 | -0.8 | Low |
| Respond (RS) | Response Planning (RS.RP) | 2 | 1 | -1.0 | Low |
| | Communication (RS.CO) | 9 | 2 | -0.7 | Low |
| | Analysis (RS.AN) | 16 | 2 | -0.5 | Low |
| | Mitigation (RS.MI) | 7 | 1 | -0.8 | Low |
| | Improvements (RS.IM) | 11 | 2 | -0.5 | Low |
| Recover (RC) | Recovery Planning (RC.RP) | 26 | 2 | -0.2 | Low |
| | Improvements (RC.IM) | 10 | 3 | -0.8 | Low |
| | Communications (RC.CO) | 8 | 1 | -0.7 | Low |

Project context for Next Generation Firewall implementation proposal

This slide highlights the project context for the Next Generation Firewall implementation proposal. It includes the requirements of the client company and the key deliverables to the service provider organization, such as scalable architecture, high performance features, etc.

Your Requirements

- NGFW solution that can be scaled to accommodate the growing network infrastructure and business requirements
- High-performance capabilities without compromising network speed and throughput
- Granular control over network applications to ensure regulatory compliance, optimize bandwidth utilization, and prevent unauthorized use
- Centralized management console or platform that provides a unified view of the network security and allows efficient policy management, monitoring, and reporting
- Add requirements here

Key Deliverables

- Our NGFW solution offers scalable architecture that can accommodate increased network traffic, additional users, and future expansion plans
- Solution is designed to deliver high-performance capabilities without compromising network speed and throughput
- Provides comprehensive application visibility and control features
- Add deliverable here

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Risk assessments, proposals you're preparing for management, the maturity assessment you need to do for your insurance renewal.



CONTEXTUALISING
INTELLIGENCE

HOW TO DEVELOP A
GOOD ANALYTICAL
PRODUCT

6



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

Joint Publication 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

Central Intelligence Agency


7

Thinking about intelligence, it's difficult to define because ultimately what we are talking about is a social science based on human nature.

Hoover Commission (Centralisation of US Agencies, elimination of waste, fraud, inefficiency)

JP 1-02 US Joint Chiefs Dictionary

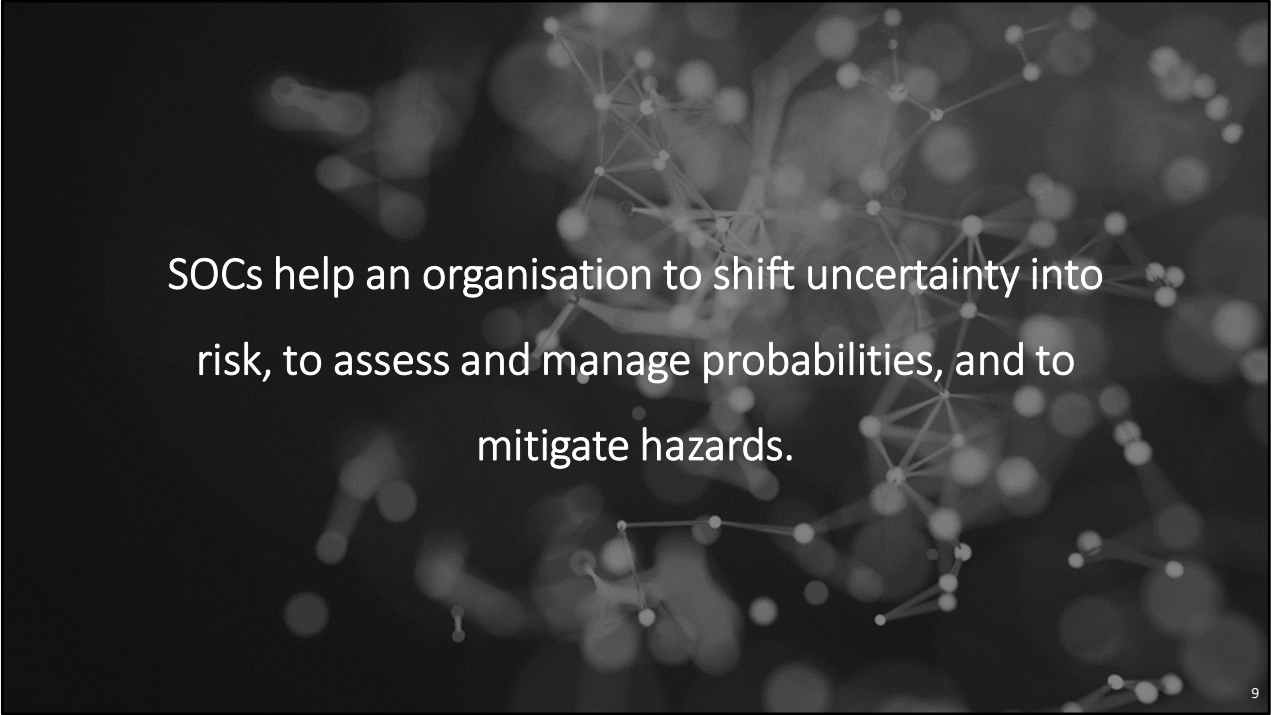
These quotes are referring to policy making, but it's pretty simple to shift context.



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

8

‘Intelligence as risk shifting.’ Michael Warner 2009

An abstract graphic featuring a dark background with a complex network of white dots and lines, resembling a molecular structure or a data network. The dots are of varying sizes and are connected by thin, light gray lines, creating a sense of interconnectedness and complexity.

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

Our role in cybersecurity operations fits nicely within the bounds that intelligence professionals typically operate in.



INTELLIGENCE AND CYBERSECURITY

- Intelligence is more than just Cyber Threat Intelligence
- While we all *consume* intelligence, we also need to shift our mindset and become *producers*.
- As cybersecurity professionals we're expected to develop and deliver advice on problems (issues, threats, risk) to clients (managers, decision-makers, customers).
- We should provide insight to these problems in the form of *understanding, context, and warning*.

10

Intelligence is a core concept for us working as Cybersecurity Professionals, but most of us don't realise it. We spend so much time thinking about how we can be cool hackers, what the next novel TTP is, etc, that we don't think about our core role of supporting the business.

In our role supporting the business, we need to shift our thinking from being intelligence *consumers* to intelligence *producers*. Producing intelligence for our clients (managers, decision-makers, paying customers, etc).

We probably already spend a lot of time creating intelligence without knowing it...

STRATEGIC INTELLIGENCE



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

OPERATIONAL INTELLIGENCE



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

TACTICAL INTELLIGENCE



Support BAU business functionality

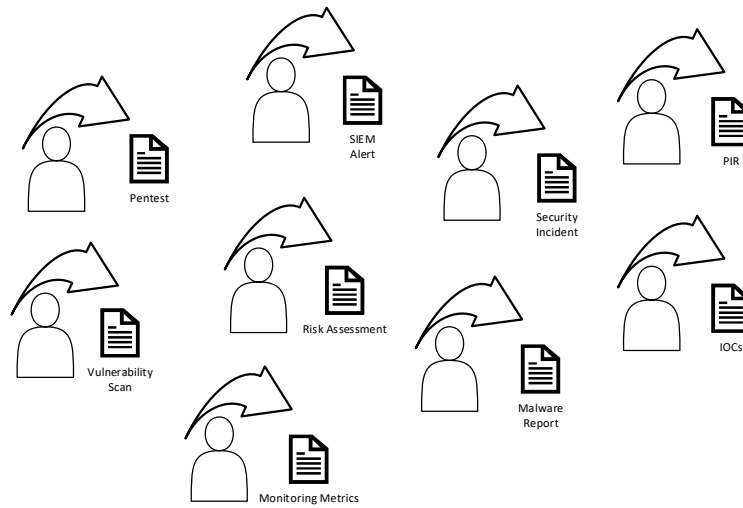


Provide decision makers with
intelligence on imminent or recent
threats or vulnerabilities

13

The typical stuff that we are probably most used to.

THE SCOPE OF INTELLIGENCE PRODUCT

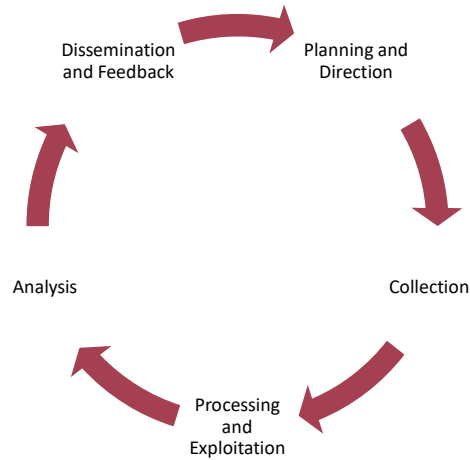




DEVELOPING AN INTELLIGENCE PRACTICE

15

INTELLIGENCE CYCLE



16

Common problems with the intelligence cycle.

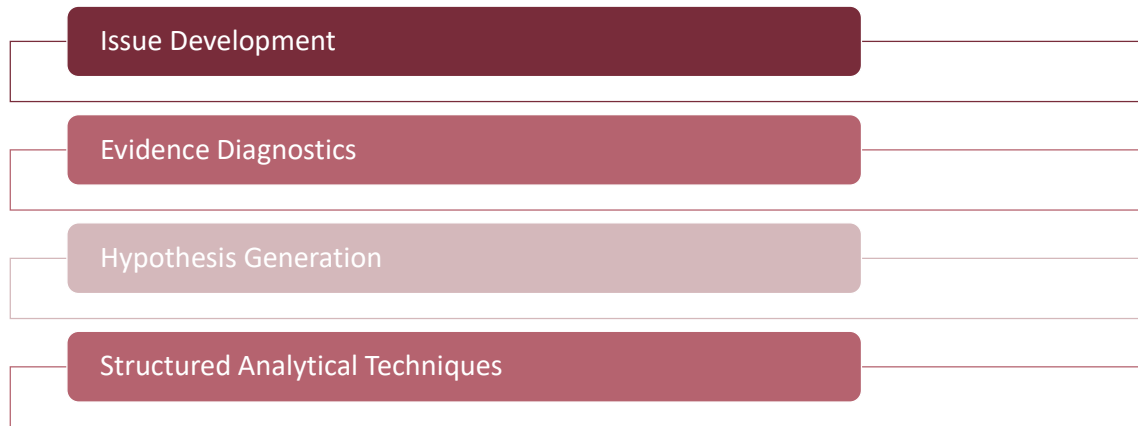
Arthur Hulnick "What's wrong with the intelligence cycle" recommended reading Mark Phythian "Understanding the Intelligence Cycle"

A reused concept and something people should be familiar with unconsciously.

J. Victor Haberman *Medical Record* 1920: "first it notices things and events; then it registers or remembers how present impressions associate with those that the mind already recalls; then it analyzes and comprehends similarities and differences; and finally it combines the resulting knowledge elements to complete a train of thought or to span gaps in available evidence"

FM 30-5 1940 and then *Intelligence is for Commanders* 1948

ANALYTIC METHODOLOGIES



17

Properly Identifying the issue or problem

Ensuring evidence is systematically reviewed

Creatively determining reasonable options or alternatives

Systematically reviewing hypotheses or options to gain insight for better understanding and presentation

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?

18

Questions of preference are broadly irrelevant. Questions of Fact only have one correct answer.

Questions of Judgement are where the quality of the answer can vary wildly and issue development, proper identification of the issue is important

The first step of the intelligence cycle was Planning and Direction.

Where is the WMD in Iraq? How do we protect critical functions from DoS?

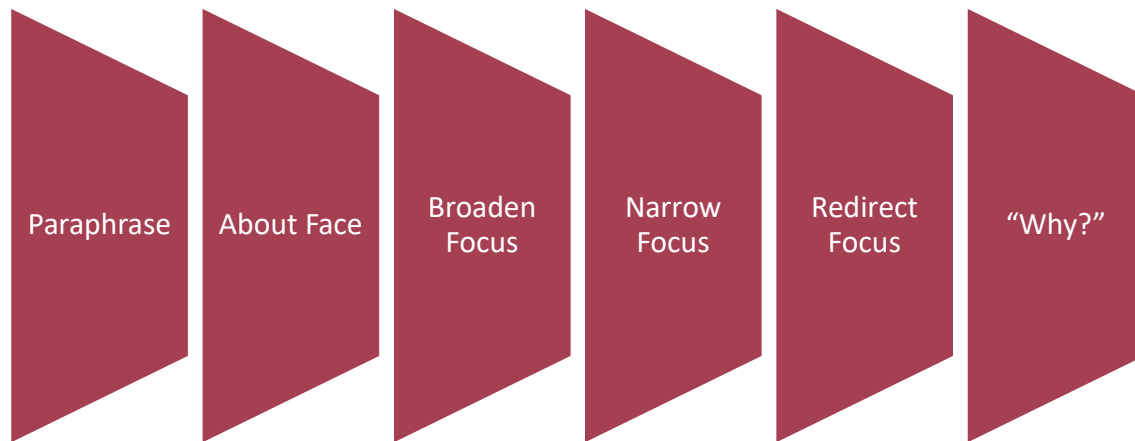
When China launches rockets into Taiwan, will the Taiwanese government collapse? When the MRI network is attacked, will we detect it?

What's the status of the Indian air defence system? How many APTs are attacking us?

Who is voting for Queen Elizabeth in the election?

“Issue Development” can be seen as a lengthy process for anyone not used to systematically breaking down a problem.

ISSUE DEVELOPMENT



19

Redefine the issue in several different ways without losing the original meaning. Review results to see if they provide a better foundation upon which to conduct research and assessment

Turn the issue on its head. Is the issue actually the one asked, or the opposite?

Instead of focusing on only one piece of the puzzle, step back and look at several pieces together. What is the issue before you connected to?

Can the issue be broken down further. Take the question and ask about the components that make up the problem.

What outside forces impinge on this issue?

Keep asking "why" until you believe the real problem emerges.

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

20

Are there multiple points of view in this report?
Who wrote the report, what organisation do they belong to?
Does the source have specific motivation or background bias?

In 2015 a report was published by Norse talking about a campaign of attacks done by Iran. After reviewing the raw data it was identified that they were classing a “scan” against a port typically used by ICS equipment as an attack. The report turned out to be sponsored by a political think tank.

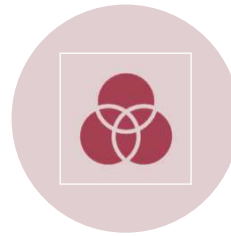
What collection platform was used, what gaps exist in coverage?
Are there any known anomalies or artifacts associated with collection?
Is the signal new, or known?

Does this relate to the main problem?
Does this make sense with what we know/ think?
Is this consistent with previous information? If not, what caused the change?

HYPOTHESES GENERATION



Preliminary explanations or possible outcomes that are meant to be tested.



Multiple working hypotheses are highly recommended.

21

The moment one has offered an original explanation for a phenomenon which seems satisfactory, that moment affection for their intellectual child springs into existence, and as the explanation grows into a definite theory their parental affections cluster about this offspring and it grows more and more dear to them. There springs up also unwittingly a pressing of the theory to make it fit the facts and a pressing of the facts to make them fit the theory.

TC Chamberlin 1897

Divergent/Convergent thinking

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 | |

22

Create a diverse group of SMEs

Focus the groups brain power on a specific issue. Not so broad that no solution is possible, not so narrow that creativity wont help

Write down notes, come to the meeting with an idea

Suspend judgement, do not eliminate ideas. Put all ideas on post-it notes

Take a break as activity dies down. Maybe repeat a few times.

Group ideas by theme, set aside anything that do not easily fit with any group. Select the themes or outliers that deserve further attention

Which of the alternatives are reasonable and would meet the goals of the decision maker?

What are the alternatives shortcomings?

What are the alternatives benefits?

Attempt to mitigate each shortcoming with actions the decision maker could take.

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

23

Mandeep Dhmi Critical Review of Analytic Techniques

Sorting
Chronologies
Timelines
Adversary Intentions Matrix
Link Charts (Node Charts)
Event Trees
Event Mapping
Subjective Probability
Weighted Ranking

CORE RULES



ANSWER THE “SO WHAT”



ADDRESSES THE
QUESTION



PROVIDES CONTEXT AND
UNDERSTANDING

24

Why does this matter? Why should your boss care? Answer this question up front - Key Judgements, Executive Summary.

There's usually a question or problem that's defined. Remember, we as professionals are delivering advice on those problems (threats, risk, etc). Sometimes this question will be given to you (we're looking at a new firewall product, what's the risk associated with deploying FortiGates) or it might be more generic (we want to know about cyber crime trends facing our customers).

Provides context to the problem and insight and understanding to the person reading it. It's not just a repetition of facts. Repeating raw information does not represent intelligence

CORE RULES



TELL A STORY



CONCISE BUT
DESCRIPTIVE



THINK ABOUT THE
AUDIENCE

25

Humans are receptive to stories. We understand concepts in terms of stories. It doesn't matter what the issue is, you will find that your audience will engage better with your product. Think about storytelling in terms of explaining a situation.

Short and easy to read. Only include what's important, and what readers need to know. Who, What, How, Why, Where, When.

Written with the audience in mind. Executives (Strategy), Managers (Operational), Technical Specialists in the Networking team (Tactical). Consider an appendix for details you don't need.

CORE RULES



CONSISTENT & LOGICAL



STANDS ALONE

26

Use of terminology, presentation, words that are used. Does it go from A>B>C.

It should be able to be read on it's own, by itself, and self-contained. It can reference to other areas, but people should be able to read this document by itself and understand the issue it's dealing with. Even if it was written for your boss, they might pass it on to another team or taken to the executives.

FINALLY



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

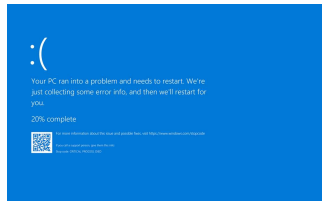


While an intelligence analysis may be “finished”, do not consider that the end.

IF NOTHING ELSE...



**SAY WHAT YOU
KNOW**
(State the facts)



**SAY WHAT YOU
DON'T KNOW**
(Acknowledge information gaps)



**SAY WHAT YOU
THINK**
(Conduct your Analysis)

THANK YOU



Conor Aitken



[Oscar-Geare/presentations-
and-papers \(github.com\)](#)