CERT-EU

EU-LISA INDUSTRY
ROUNDTABLE 1&2 JUNE 2023

TLP:GREEN

DETECTION IN THE CLOUD

JAMES BARR, ENG

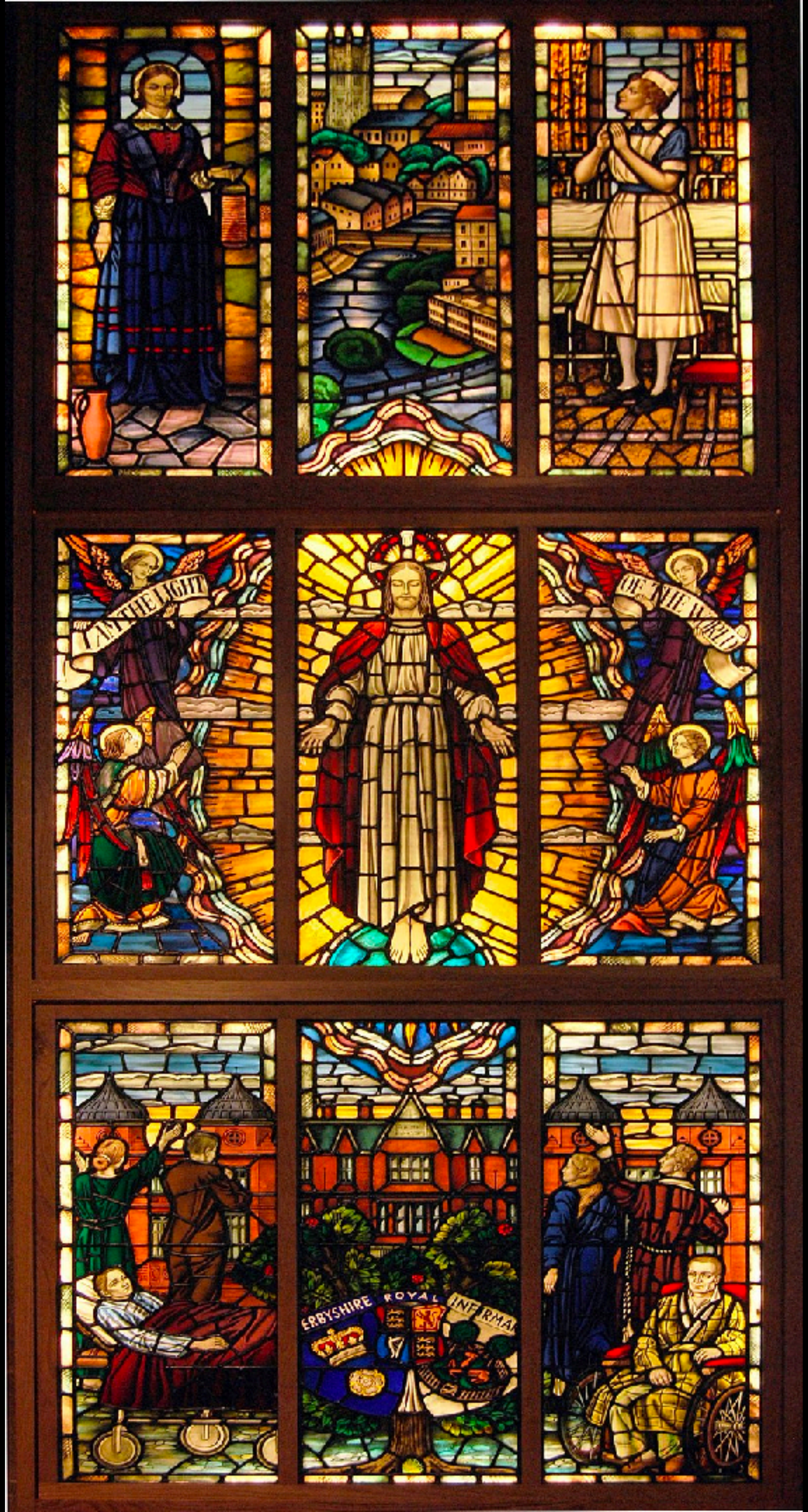
2-Jun-2023 /
Version 2.0.2

IMPORTANT NOTICE

THIS PRESENTATION IS **TLP:GREEN**

YOU MAY SHARE **TLP:GREEN** INFORMATION WITH PEERS AND PARTNER ORGANISATIONS WITHIN YOUR COMMUNITY, BUT NOT VIA PUBLICLY ACCESSIBLE CHANNELS

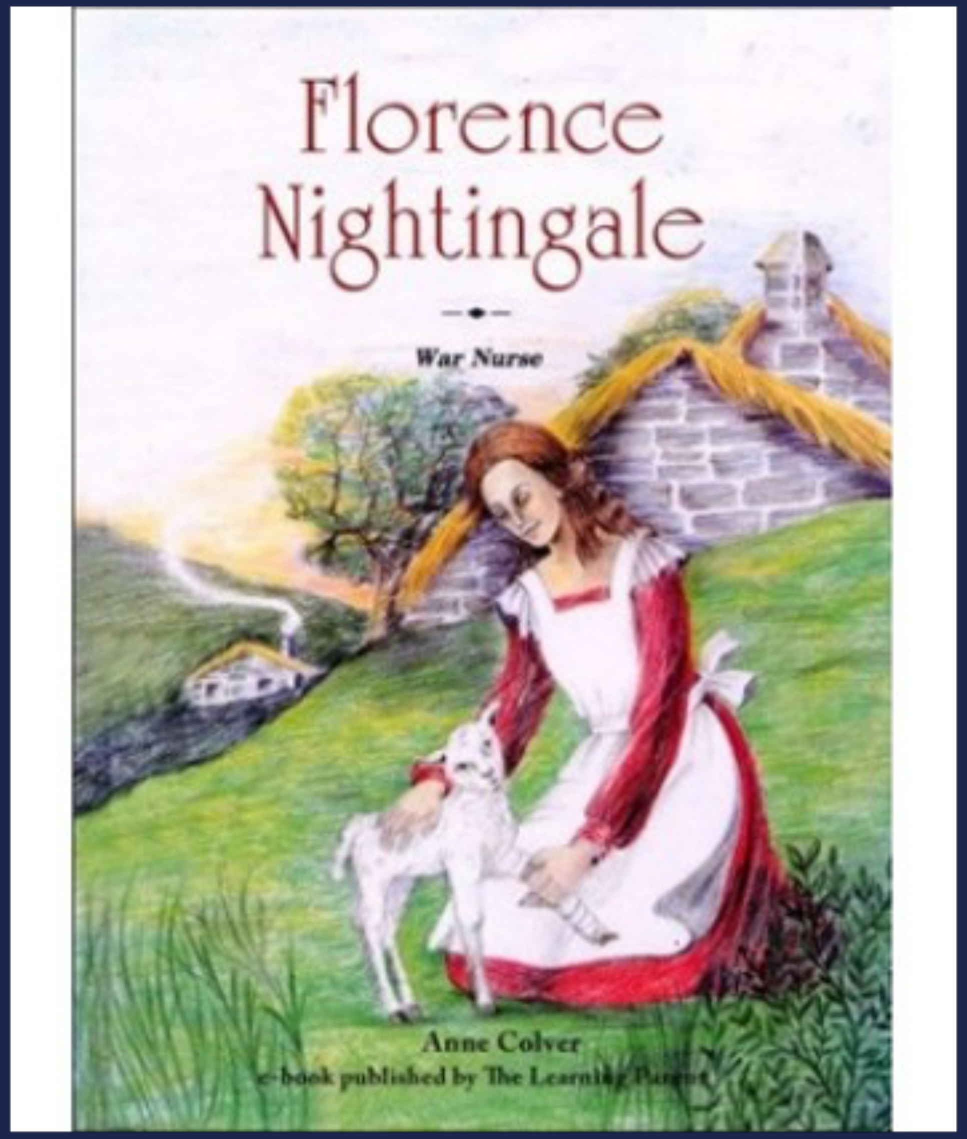
CERT-EU

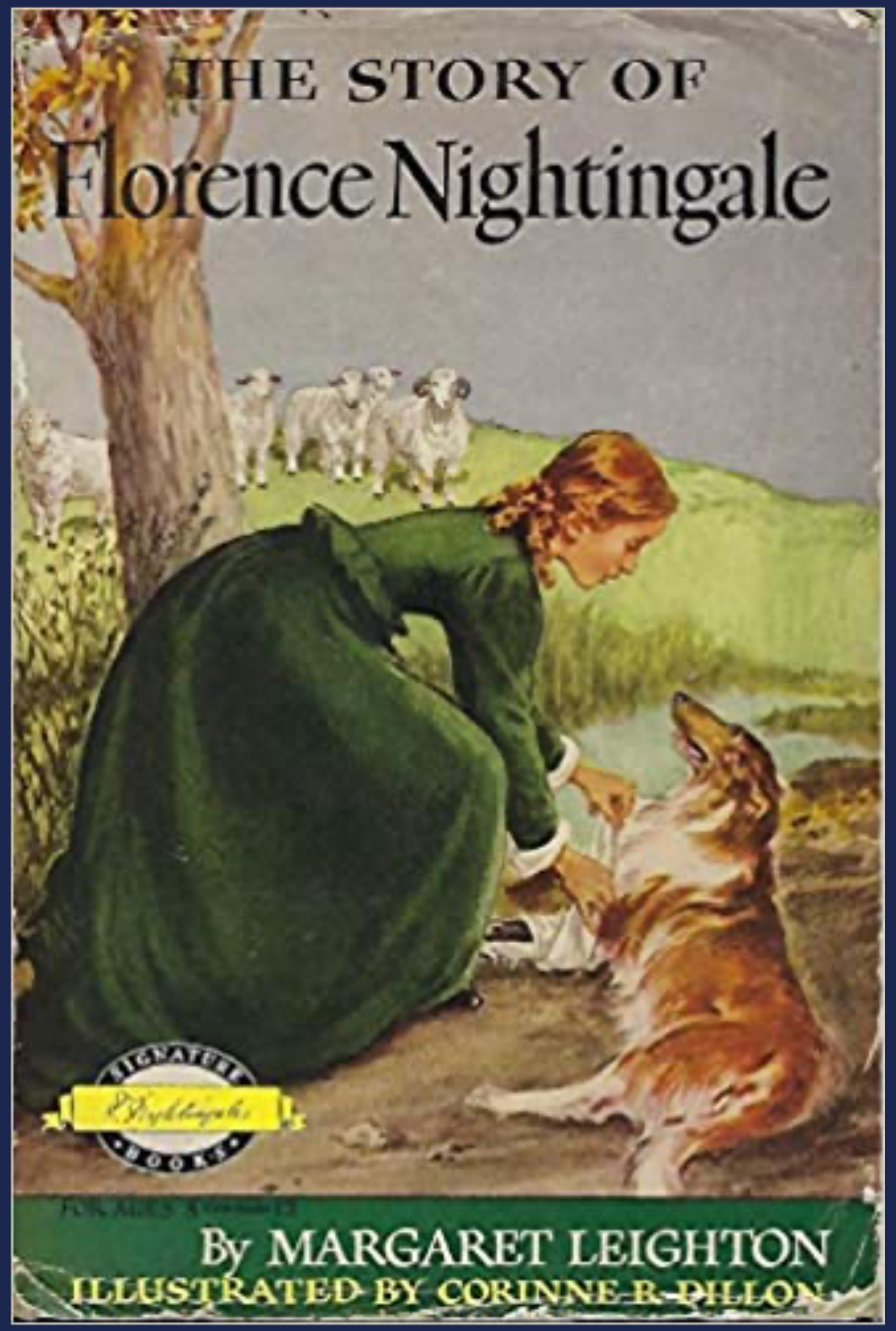


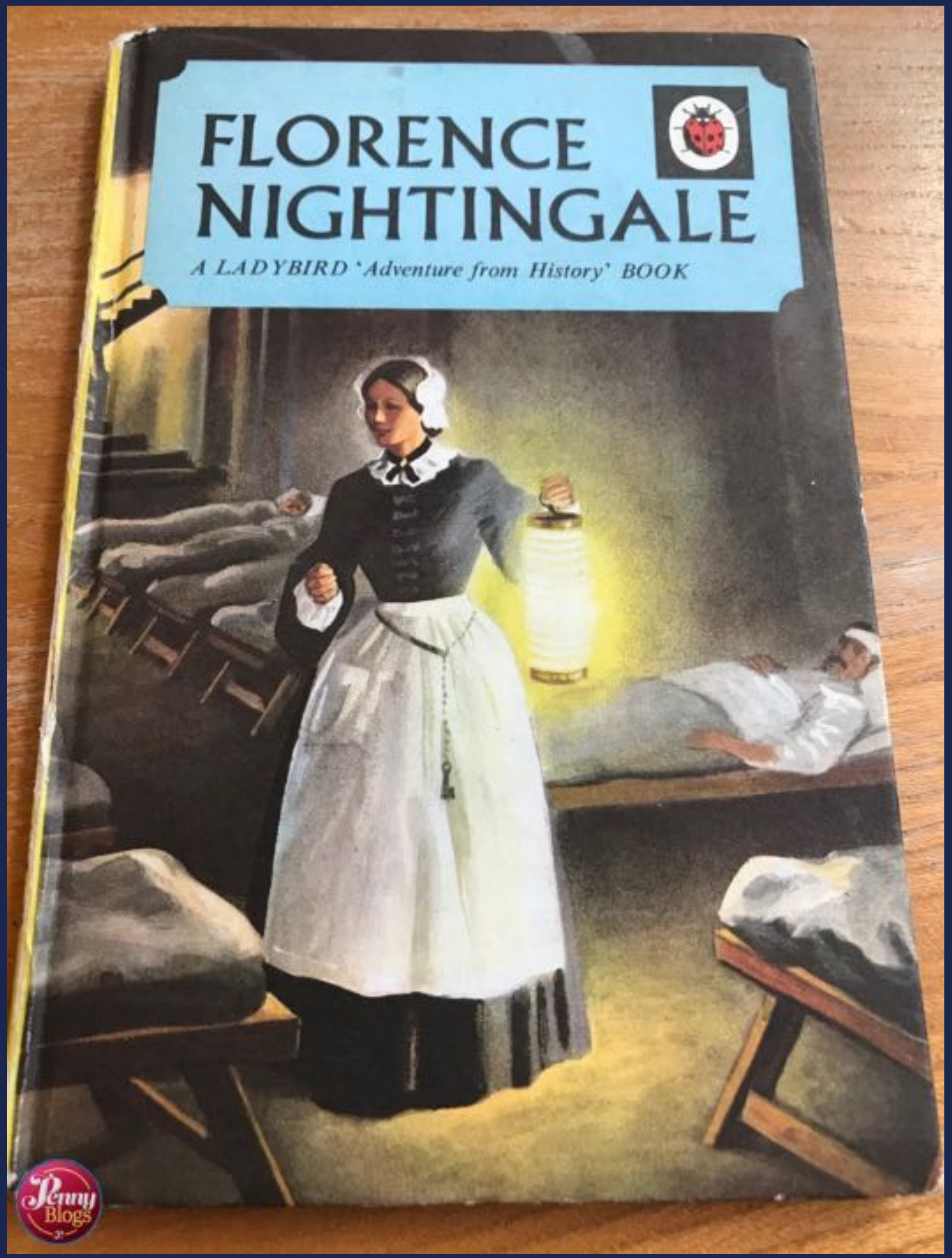
LONG LONG AGO, FAR FAR AWAY

Before the Cloud

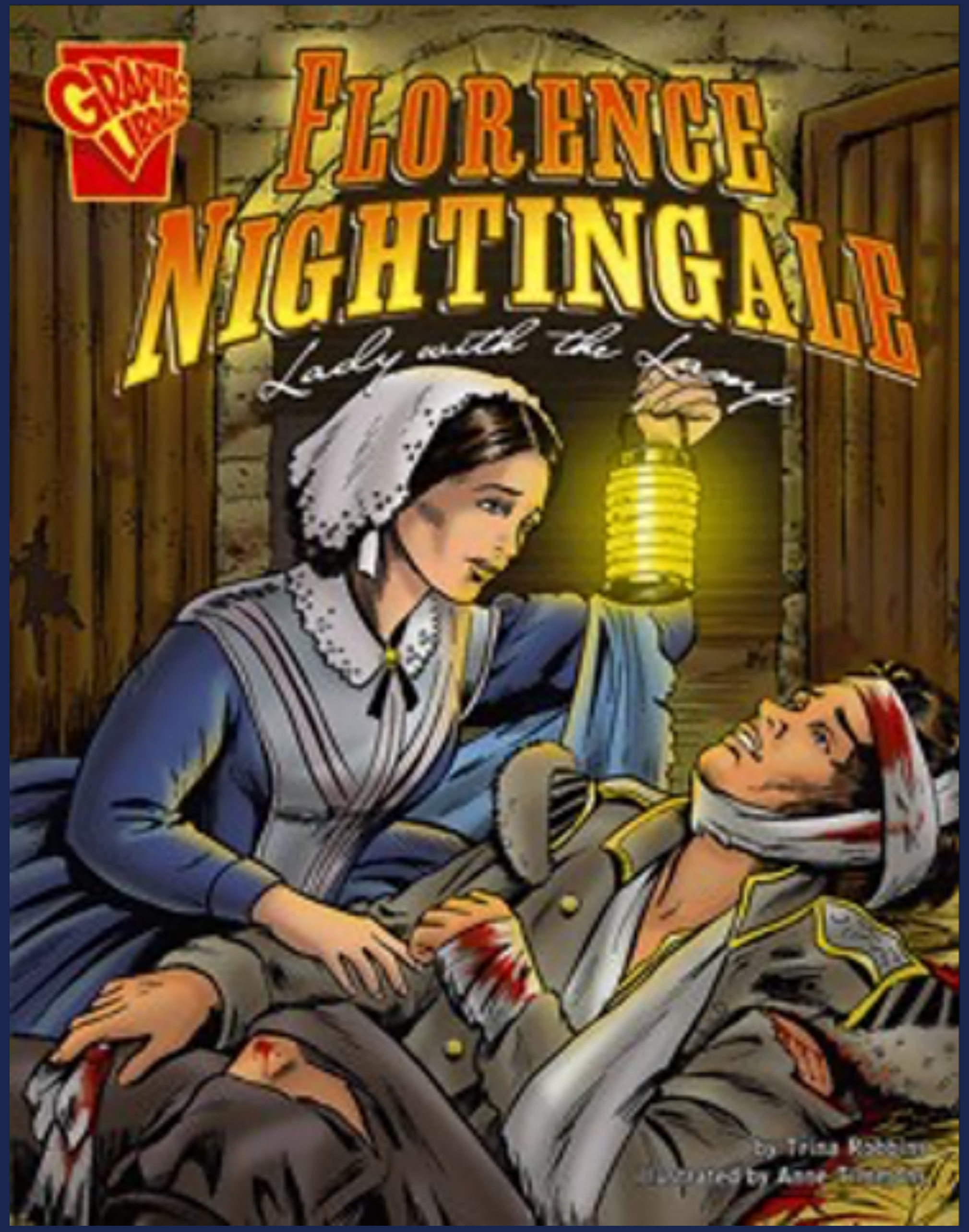
FLORENCE NIGHTINGALE "LADY WITH THE LAMP" - ICONIC VICTORIAN NURSE







ONE OF FIRST BOOKS I EVER READ



SOMEWHAT MISLEADING VISUALISATIONS

Actually a pioneer in **statistics** and **data visualisation**

TLP:GREEN

FOUNDER OF MODERN NURSING, SIGNIFICANTLY REDUCED DEATH RATES BY IMPROVING HYGIENE AND LIVING STANDARDS.

ONE OF FIRST INFOGRAPHICS

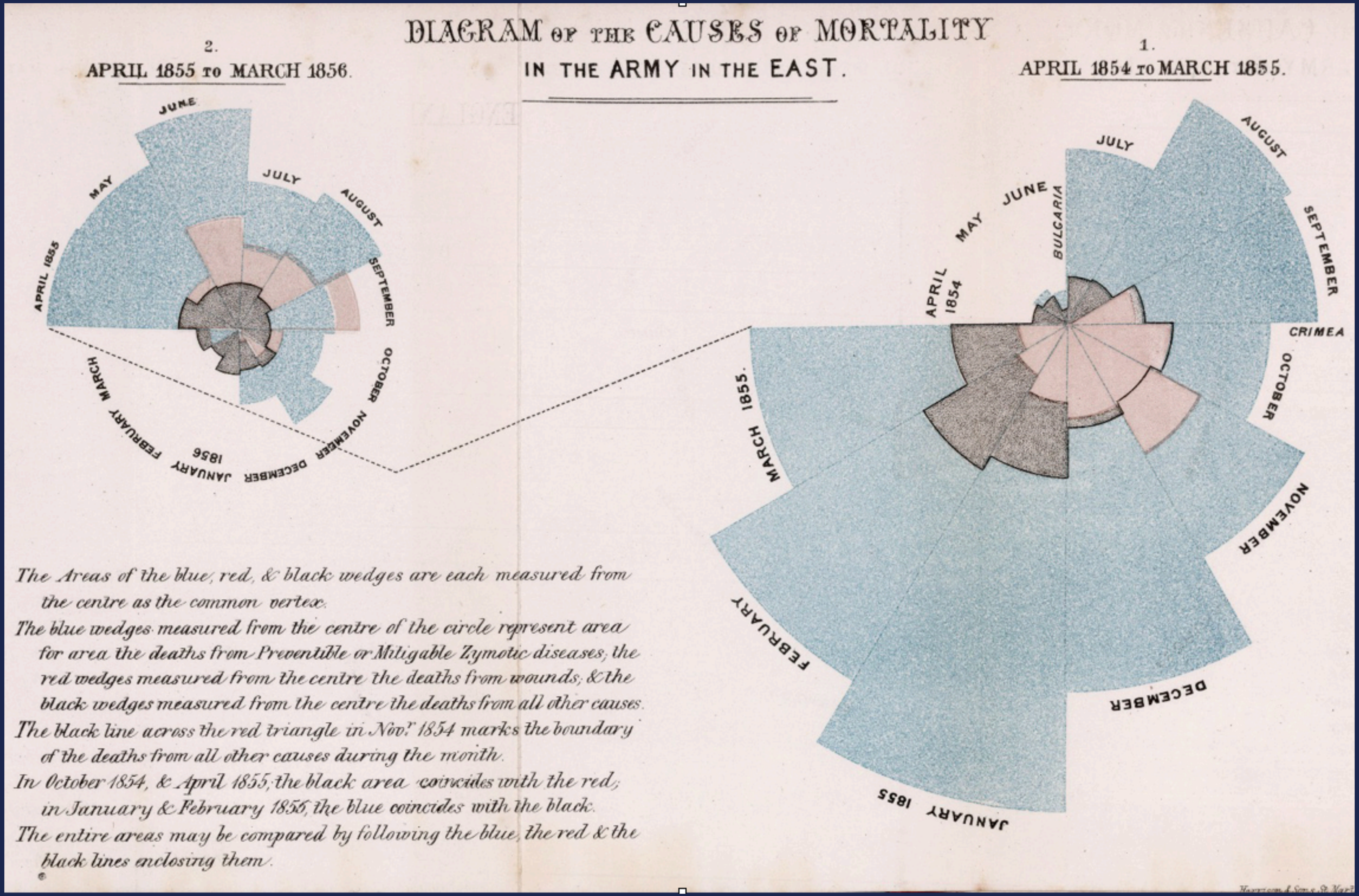


DIAGRAM of the CAUSES of MORTALITY

IN THE ARMY IN THE EAST.

The Areas of the blue, red, & black wedges are each measured from the centre as the common vertex.

The blue wedges measured from the centre of the circle represent area for area the deaths from Preventible or Mitigable Zymotic diseases; the red wedges measured from the centre the deaths from wounds; & the black wedges measured from the centre the deaths from all other causes.

The black line across the red triangle in Nov.^{r} 1854 marks the boundary of the deaths from all other causes during the month.

In October 1854, & April 1855, the black area coincides with the red; in January & February 1856, the blue coincides with the black.

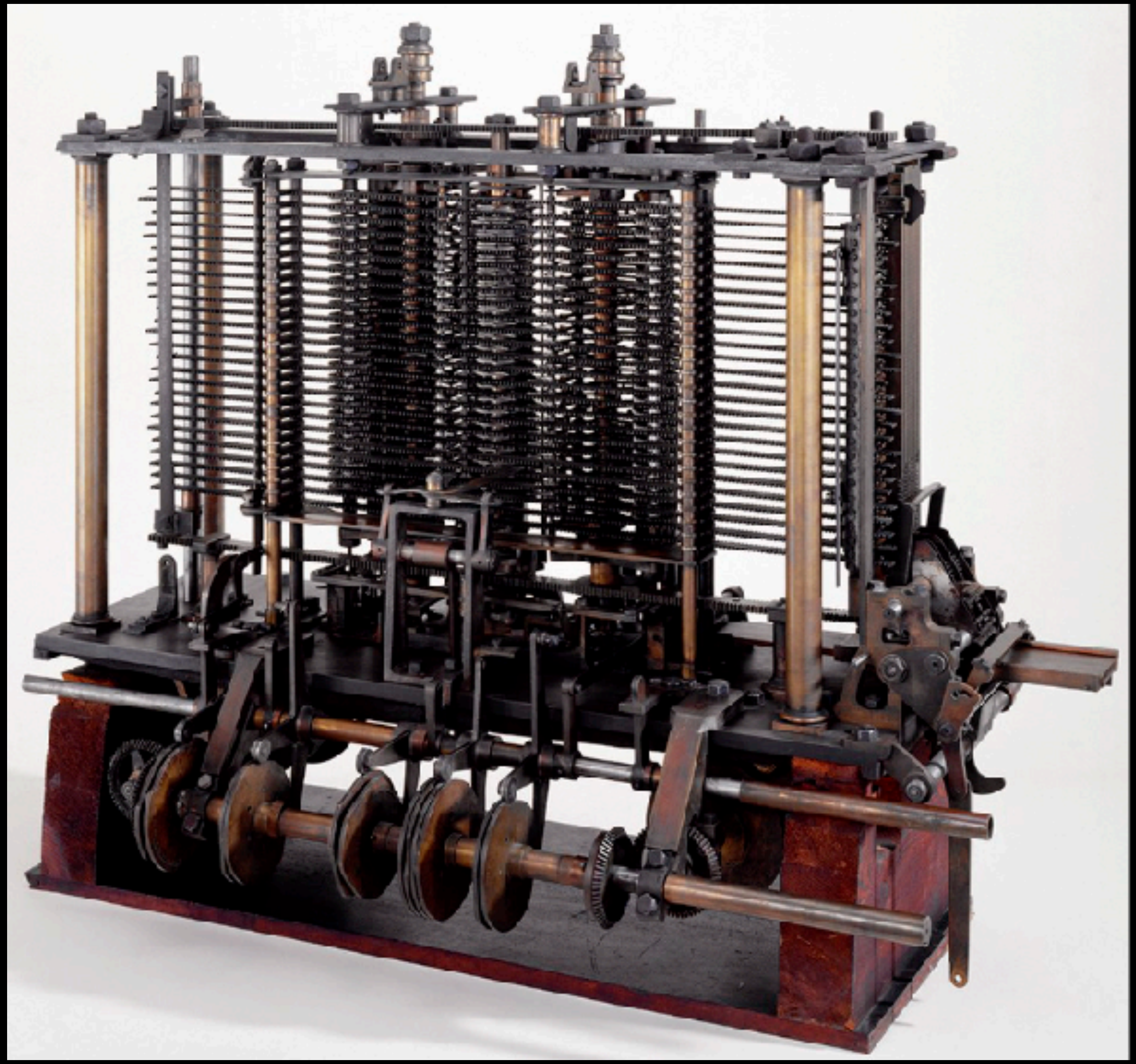
The entire areas may be compared by following the blue, the red & the black lines enclosing them.

LOG, COUNT, PRESENT, ACT

NIGHTINGALE'S ROSE DIAGRAM (CIRCULAR HISTOGRAM)

PROFOUND IMPACT - HIERARCHY NOTICED

TLP:GREEN



NOT SO LONG AGO OR FAR AWAY

Before the Cloud

A CLIENT/SERVER SYSTEM I WORKED ON BEFORE CLOUD (15-20 YEARS AGO)

LOGS MB AND NOT PRESENTABLE

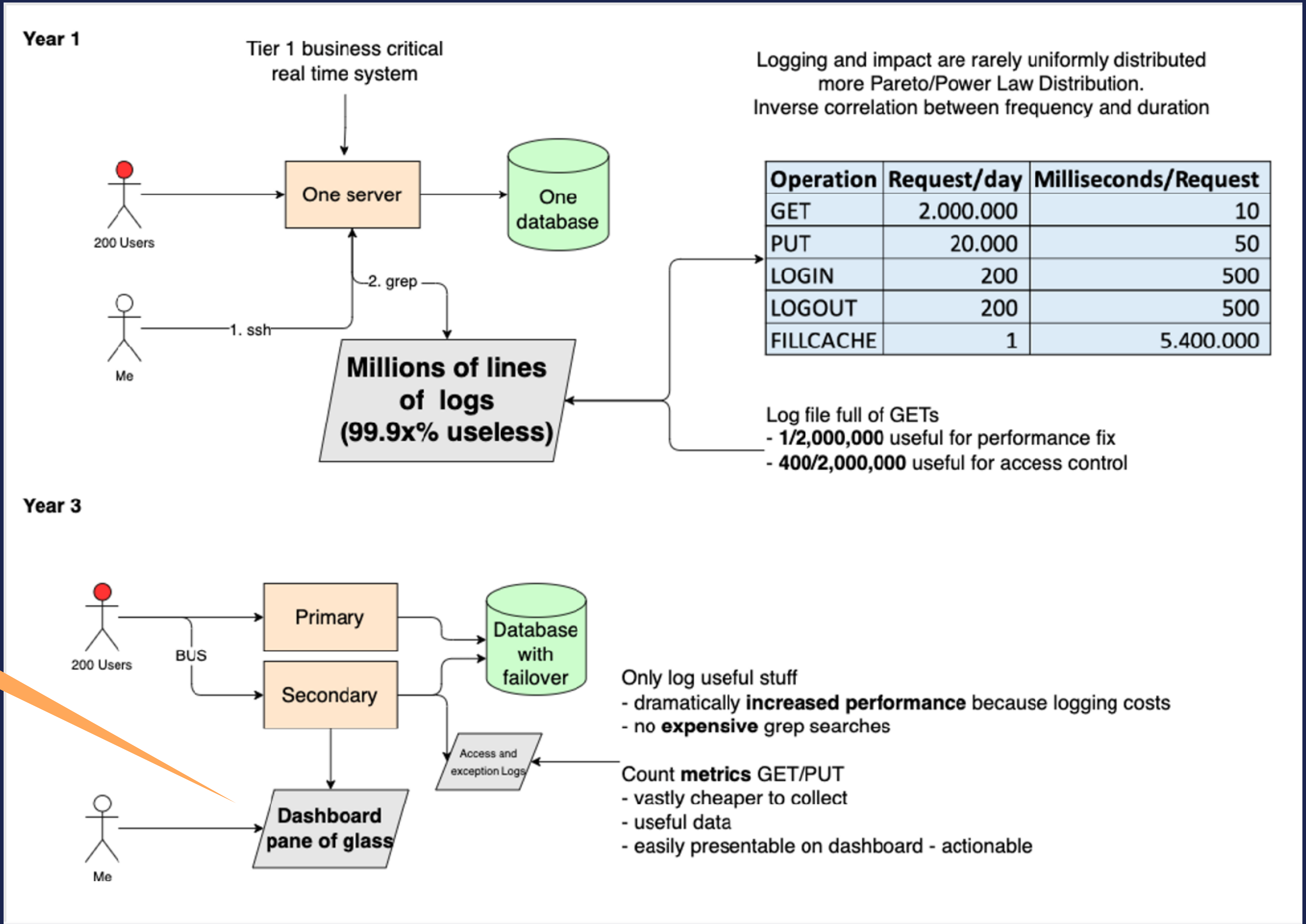
SYBASE SQL (ORACLE AND USB, AND SOME EXOTIC KDB)

DASHBOARD SAVED THE DAY

NOT ALL LOGS CREATED EQUAL (FAR FROM UNIFORM)

DETECTION RULES ARE BASED ON ON LOGS AND METRICS

METRICS KB AND EASY TO PRESENT



Logging and impact are rarely uniformly distributed more Pareto/Power Law Distribution. Inverse correlation between frequency and duration

Operation	Request/day	Milliseconds/Request
GET	2.000.000	10
PUT	20.000	50
LOGIN	200	500
LOGOUT	200	500
FILLCACHE	1	5.400.000

Log file full of GETs
- **1/2,000,000** useful for performance fix
- **400/2,000,000** useful for access control

Only log useful stuff
- dramatically **increased performance** because logging costs
- no **expensive** grep searches

Count **metrics** GET/PUT
- vastly cheaper to collect
- useful data
- easily presentable on dashboard - actionable

CERT-EU

BRIEFLY: NEAR REAL TIME DASHBOARD MESSAGES/SECOND PER 15 MINUTES

LOG, COUNT, PRESENT, ACT

MORNING START

ACTION: LAZY LOADING

MONDAY 10:45 MARKET ACTION

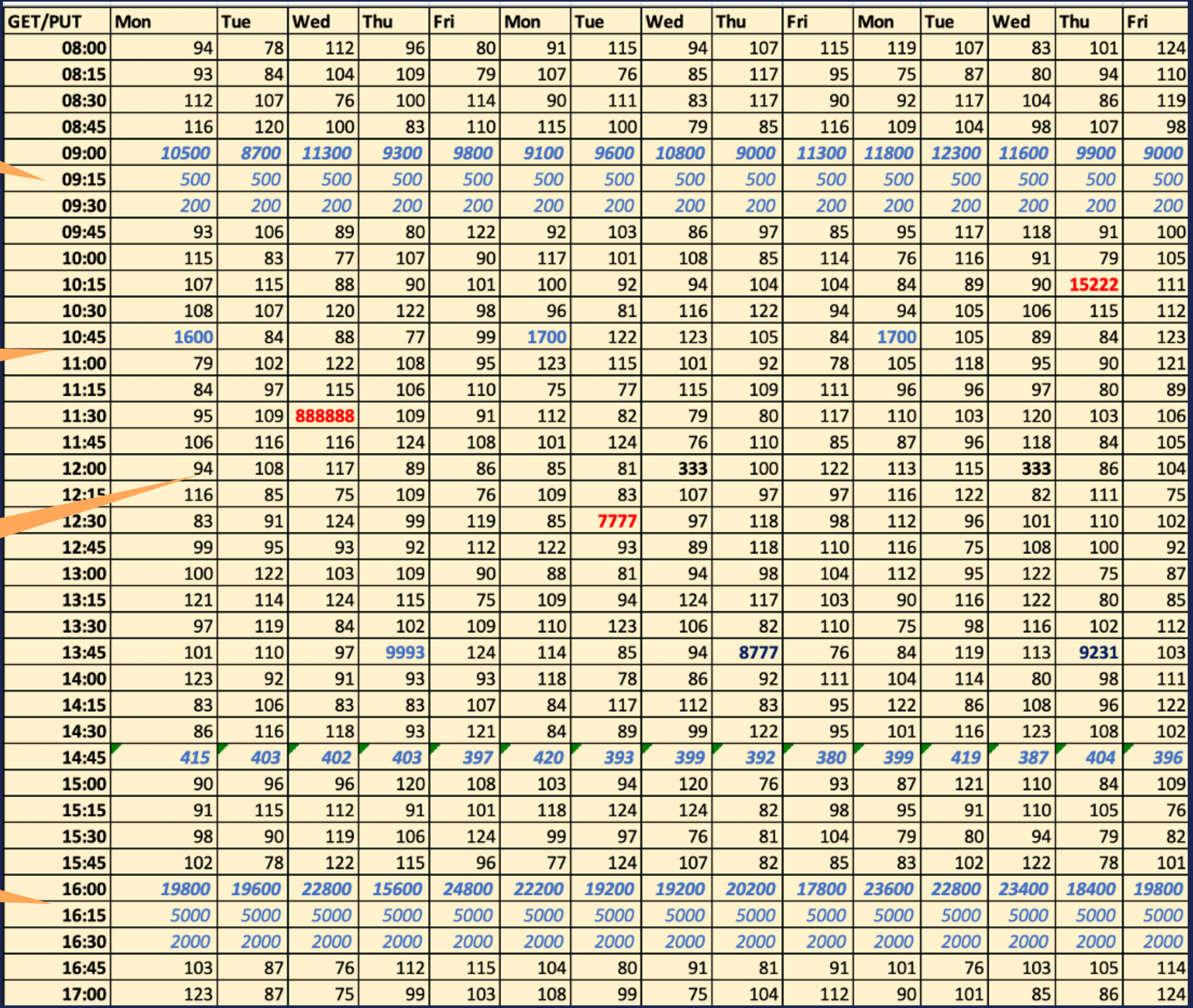
ACTION: REDUCE LOAD

OUTLIER

ACTION: ONE ROGUE IN SWITZERLAND

US MARKET OPENS

ACTION: REDUCE AND STAGGER LOAD



GET/PUT	Mon	Tue	Wed	Thu	Fri	Mon	Tue	Wed	Thu	Fri	Mon	Tue	Wed	Thu	Fri
08:00	94	78	112	96	80	91	115	94	107	115	119	107	83	101	124
08:15	93	84	104	109	79	107	76	85	117	95	75	87	80	94	110
08:30	112	107	76	100	114	90	111	83	117	90	92	117	104	86	119
08:45	116	120	100	83	110	115	100	79	85	116	109	104	98	107	98
09:00	*10500*	*8700*	*11300*	*9300*	*9800*	*9100*	*9600*	*10800*	*9000*	*11300*	*11800*	*12300*	*11600*	*9900*	*9000*
09:15	*500*	*500*	*500*	*500*	*500*	*500*	*500*	*500*	*500*	*500*	*500*	*500*	*500*	*500*	*500*
09:30	*200*	*200*	*200*	*200*	*200*	*200*	*200*	*200*	*200*	*200*	*200*	*200*	*200*	*200*	*200*
09:45	93	106	89	80	122	92	103	86	97	85	95	117	118	91	100
10:00	115	83	77	107	90	117	101	108	85	114	76	116	91	79	105
10:15	107	115	88	90	101	100	92	94	104	104	84	89	90	**15222**	111
10:30	108	107	120	122	98	96	81	116	122	94	94	105	106	115	112
10:45	1600	84	88	77	99	1700	122	123	105	84	1700	105	89	84	123
11:00	79	102	122	108	95	123	115	101	92	78	105	118	95	90	121
11:15	84	97	115	106	110	75	77	115	109	111	96	96	97	80	89
11:30	95	109	**888888**	109	91	112	82	79	80	117	110	103	120	103	106
11:45	106	116	116	124	108	101	124	76	110	85	87	96	118	84	105
12:00	94	108	117	89	86	85	81	**333**	100	122	113	115	**333**	86	104
12:15	116	85	75	109	76	109	83	107	97	97	116	122	82	111	75
12:30	83	91	124	99	119	85	**7777**	97	118	98	112	96	101	110	102
12:45	99	95	93	92	112	122	93	89	118	110	116	75	108	100	92
13:00	100	122	103	109	90	88	81	94	98	104	112	95	122	75	87
13:15	121	114	124	115	75	109	94	124	117	103	90	116	122	80	85
13:30	97	119	84	102	109	110	123	106	82	110	75	98	116	102	112
13:45	101	110	97	9993	124	114	85	94	**8777**	76	84	119	113	**9231**	103
14:00	123	92	91	93	93	118	78	86	92	111	104	114	80	98	111
14:15	83	106	83	83	107	84	117	112	83	95	122	86	108	96	122
14:30	86	116	118	93	121	84	89	99	122	95	101	116	123	108	102
14:45	*415*	*403*	*402*	*403*	*397*	*420*	*393*	*399*	*392*	*380*	*399*	*419*	*387*	*404*	*396*
15:00	90	96	96	120	108	103	94	120	76	93	87	121	110	84	109
15:15	91	115	112	91	101	118	124	124	82	98	95	91	110	105	76
15:30	98	90	119	106	124	99	97	76	81	104	79	80	94	79	82
15:45	102	78	122	115	96	77	124	107	82	85	83	102	122	78	101
16:00	*19800*	*19600*	*22800*	*15600*	*24800*	*22200*	*19200*	*19200*	*20200*	*17800*	*23600*	*22800*	*23400*	*18400*	*19800*
16:15	*5000*	*5000*	*5000*	*5000*	*5000*	*5000*	*5000*	*5000*	*5000*	*5000*	*5000*	*5000*	*5000*	*5000*	*5000*
16:30	*2000*	*2000*	*2000*	*2000*	*2000*	*2000*	*2000*	*2000*	*2000*	*2000*	*2000*	*2000*	*2000*	*2000*	*2000*
16:45	103	87	76	112	115	104	80	91	81	91	101	76	103	105	114
17:00	123	87	75	99	103	108	99	75	104	112	90	101	85	86	124

EASY TO SEE PATTERNS AND PRESENT TO STAKEHOLDERS

TLP:GREEN

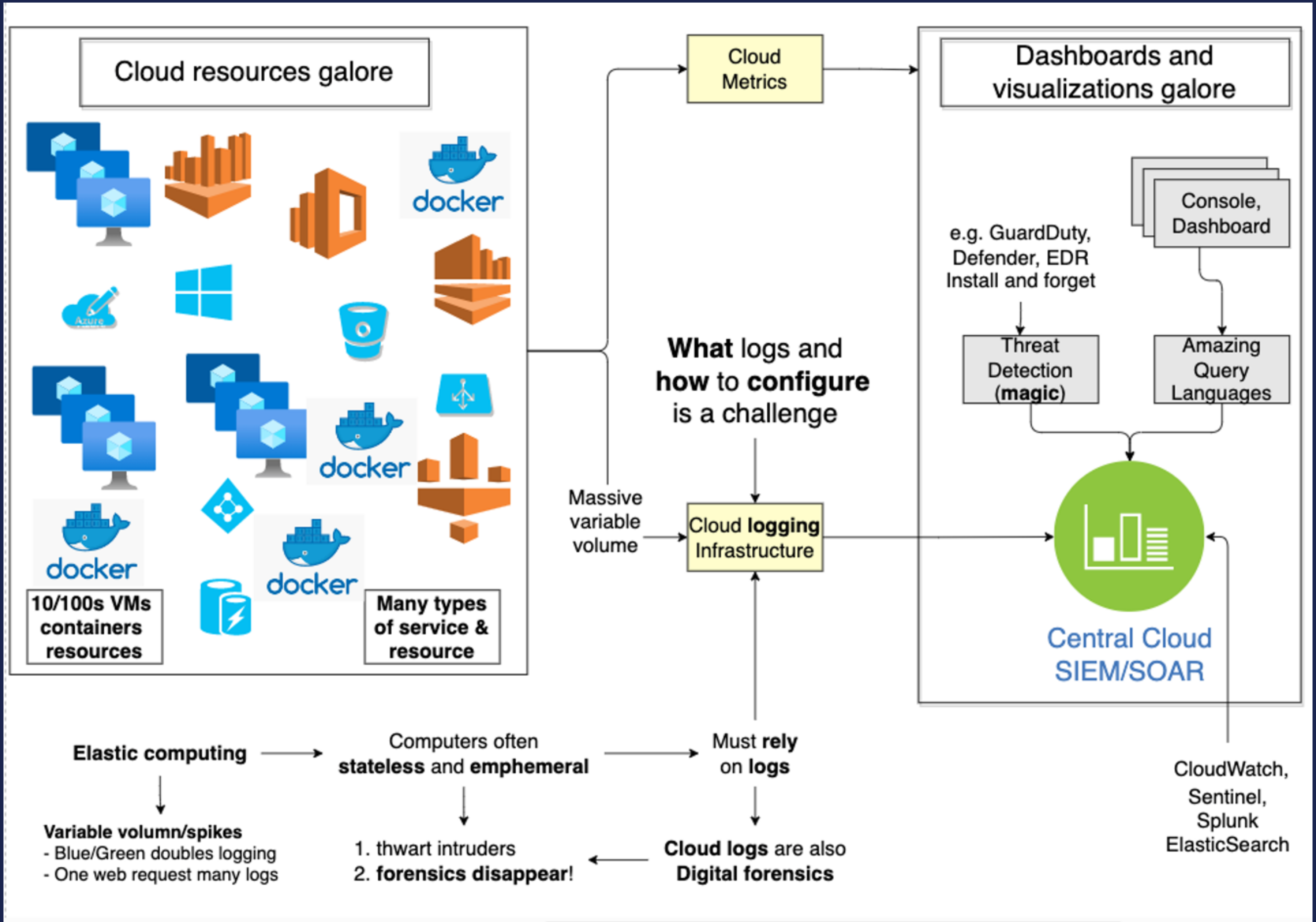
ANY SUFFICIENTLY ADVANCED TECHNOLOGY IS INDISTINGUISHABLE FROM MAGIC – ARTHUR C. CLARKE

The Cloud ERA

THE MODERN CLOUD ENVIRONMENT

MASSIVE DATA, COMPUTE AND RICH TOOLS

WHAT ARE THE GAPS IN DETECTION?



Cloud resources galore
docker
10/100s VMs containers resources
Many types of service & resource
Cloud Metrics
Dashboards and visualizations galore
e.g. GuardDuty, Defender, EDR Install and forget
Console, Dashboard
Threat Detection (magic)
Amazing Query Languages
What logs and how to configure is a challenge
Massive variable volume
Cloud logging Infrastructure
Central Cloud SIEM/SOAR
CloudWatch, Sentinel, Splunk ElasticSearch
Elastic computing
Computers often stateless and emphemeral
Must rely on logs
Variable volumn/spikes
- Blue/Green doubles logging
- One web request many logs
1. thwart intruders
2. forensics disappear!
Cloud logs are also Digital forensics

LOG, COUNT, PRESENT, ACT

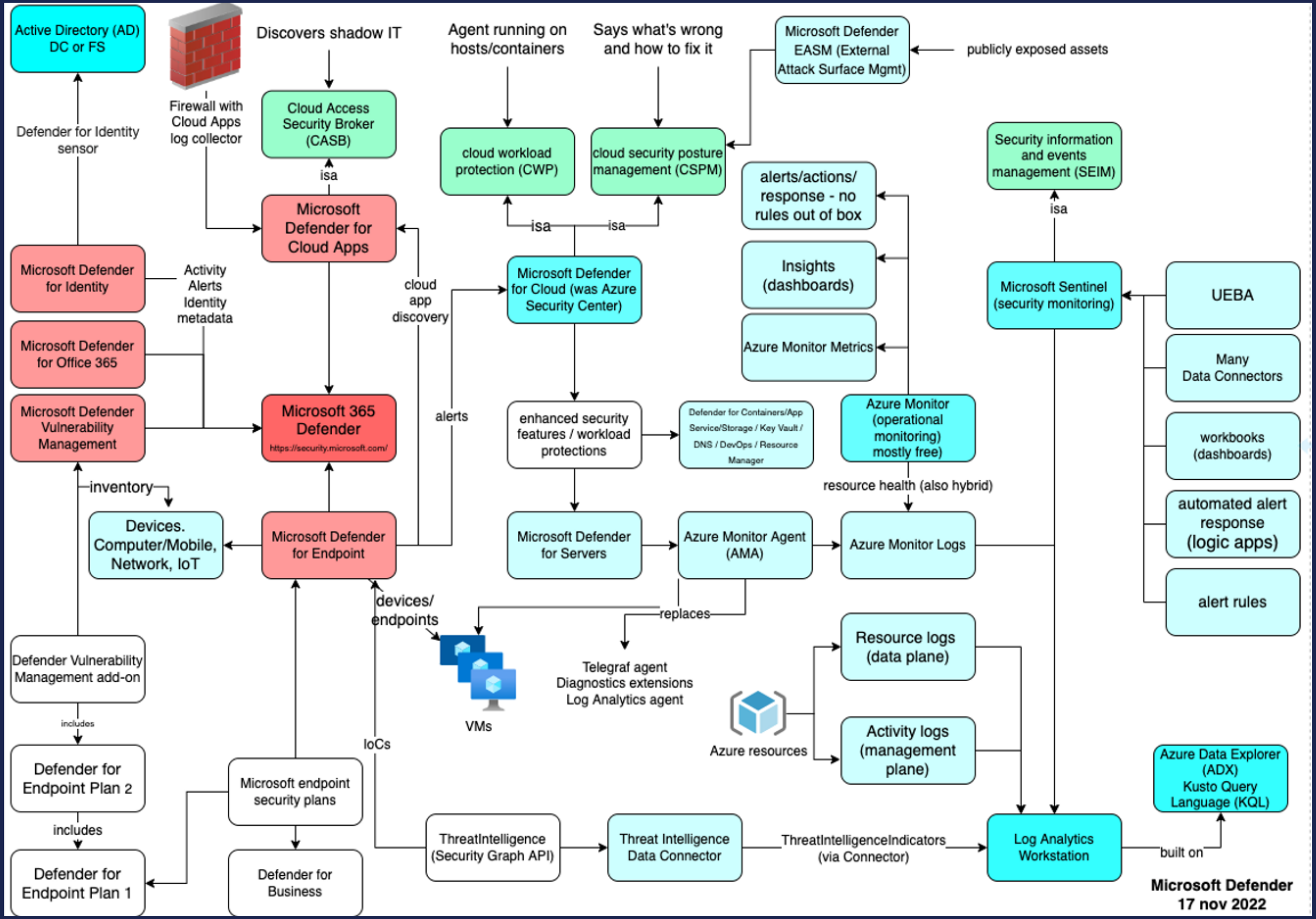
LOTS OF MAGIC AND LOTS OF DETAIL

DETECTION RULES OF QUERY LANGUAGES

SO MANY POSSIBLE ACTIONS NEEDS AUTOMATION

TLP:GREEN

VERY BRIEFLY SCRATCHING THE SURFACE OF MICROSOFT DEFENDER …



Active Directory (AD) DC or FS

Defender for Identity sensor

Firewall with Cloud Apps log collector

Discovers shadow IT

Cloud Access Security Broker (CASB)

isa

Microsoft Defender for Cloud Apps

Agent running on hosts/containers

Says what's wrong and how to fix it

Microsoft Defender EASM (External Attack Surface Mgmt)

publicly exposed assets

cloud workload protection (CWP)

cloud security posture management (CSPM)

isa

isa

alerts/actions/ response - no rules out of box

Insights (dashboards)

Azure Monitor Metrics

Security information and events management (SEIM)

isa

Microsoft Sentinel (security monitoring)

UEBA

Many Data Connectors

workbooks (dashboards)

automated alert response (logic apps)

alert rules

Microsoft Defender for Identity

Activity Alerts Identity metadata

Microsoft Defender for Office 365

Microsoft Defender Vulnerability Management

cloud app discovery

Microsoft Defender for Cloud (was Azure Security Center)

Microsoft 365 Defender https://security.microsoft.com/

alerts

enhanced security features / workload protections

Defender for Containers/App Service/Storage / Key Vault / DNS / DevOps / Resource Manager

Azure Monitor (operational monitoring) mostly free)

resource health (also hybrid)

inventory

Devices. Computer/Mobile, Network, IoT

Microsoft Defender for Endpoint

Microsoft Defender for Servers

Azure Monitor Agent (AMA)

Azure Monitor Logs

devices/ endpoints

replaces

VMs

Telegraf agent Diagnostics extensions Log Analytics agent

Azure resources

Resource logs (data plane)

Activity logs (management plane)

Defender Vulnerability Management add-on

includes

Defender for Endpoint Plan 2

includes

Defender for Endpoint Plan 1

Microsoft endpoint security plans

Defender for Business

IoCs

ThreatIntelligence (Security Graph API)

Threat Intelligence Data Connector

ThreatIntelligenceIndicators (via Connector)

Log Analytics Workstation

built on

Azure Data Explorer (ADX) Kusto Query Language (KQL)

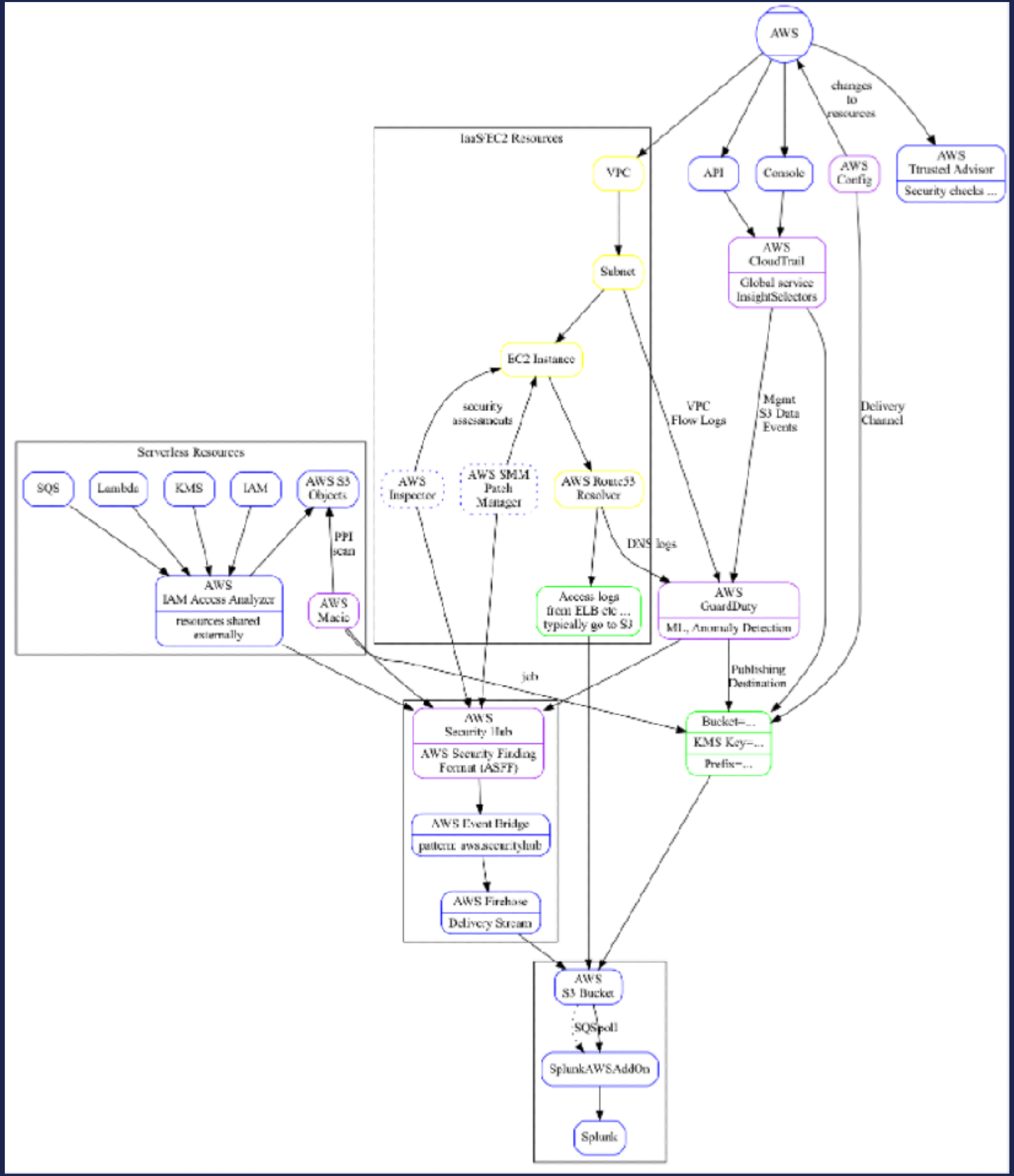
Microsoft Defender 17 nov 2022

CAN BE VERY COMPLEX

IN PRACTICE DEFENDER DOES A LOT OF MAGIC

TLP:GREEN

VERY BRIEFLY SCRATCHING THE SURFACE OF AWS SECURITY SERVICES ...



CAN BE VERY COMPLEX

IN PRACTICE GUARDDUTY (ETC) DOES A LOT OF MAGIC

I WILL LEAVE COMPARING AWS AND AZURE TO OTHERS

TLP:GREEN

DETECTION RULES ARE BASED ON LOGS AND METRICS

LOG, COUNT, PRESENT, ACT

- There are lots and lots of detection rules
  - Cloud detection rules (and remediation) clearly documented:
    - aws-managed-rule-groups-threat-signature.html
    - guardduty_finding-types-active.html
    - defender-for-cloud/alerts-reference
- Threat Intelligence upload & custom rules also well documented.

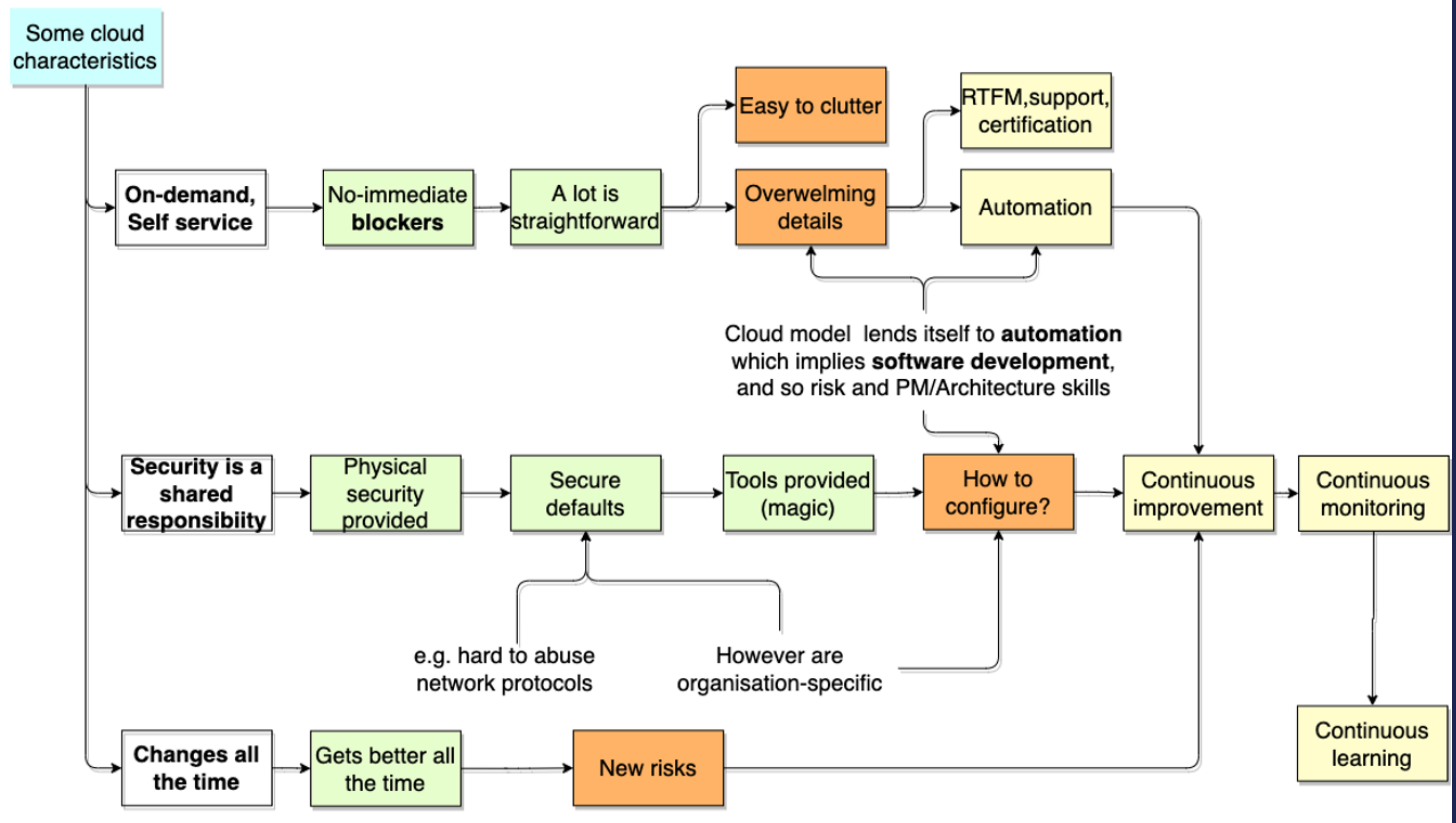
WHY SO MANUAL?

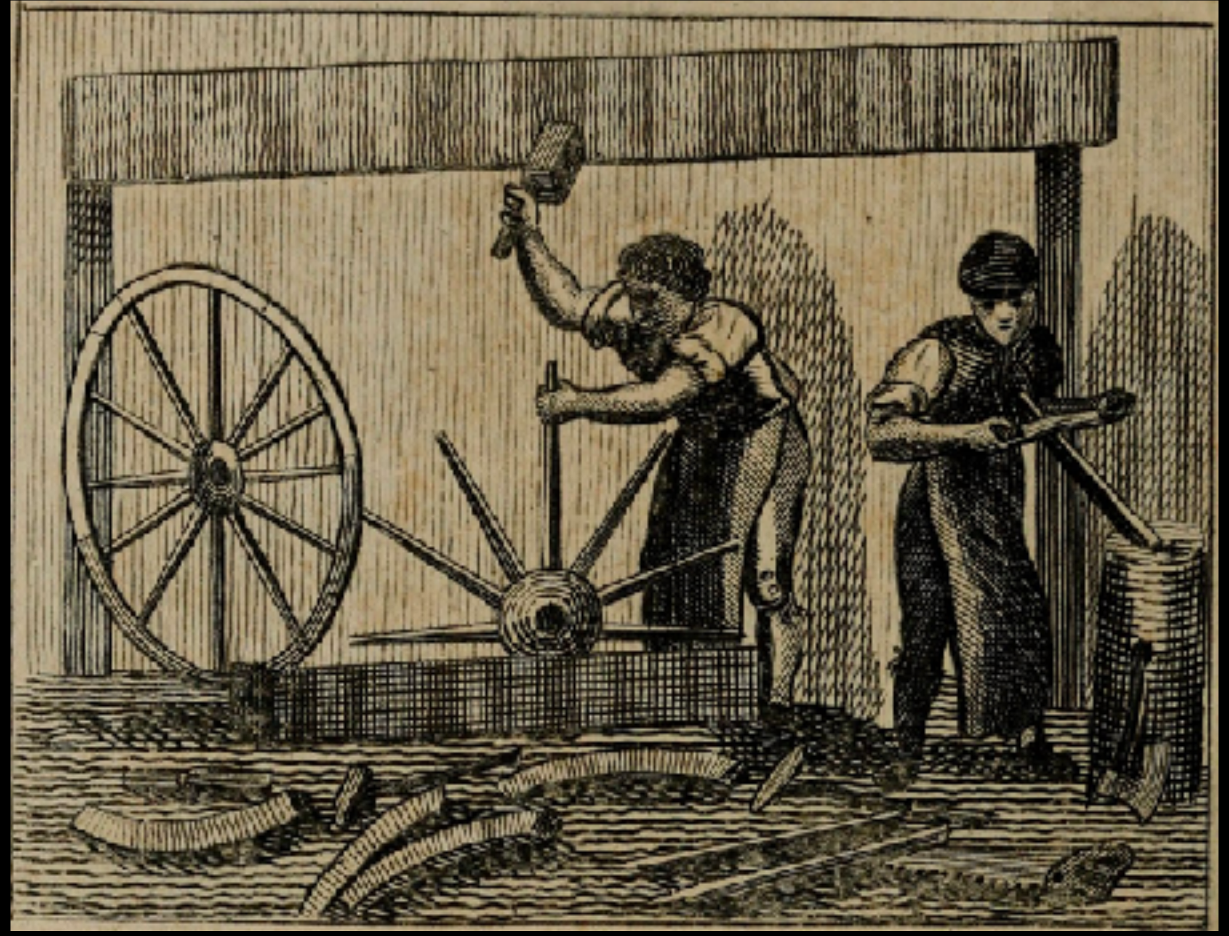
ALSO WITH M365 ASSESSMENTS

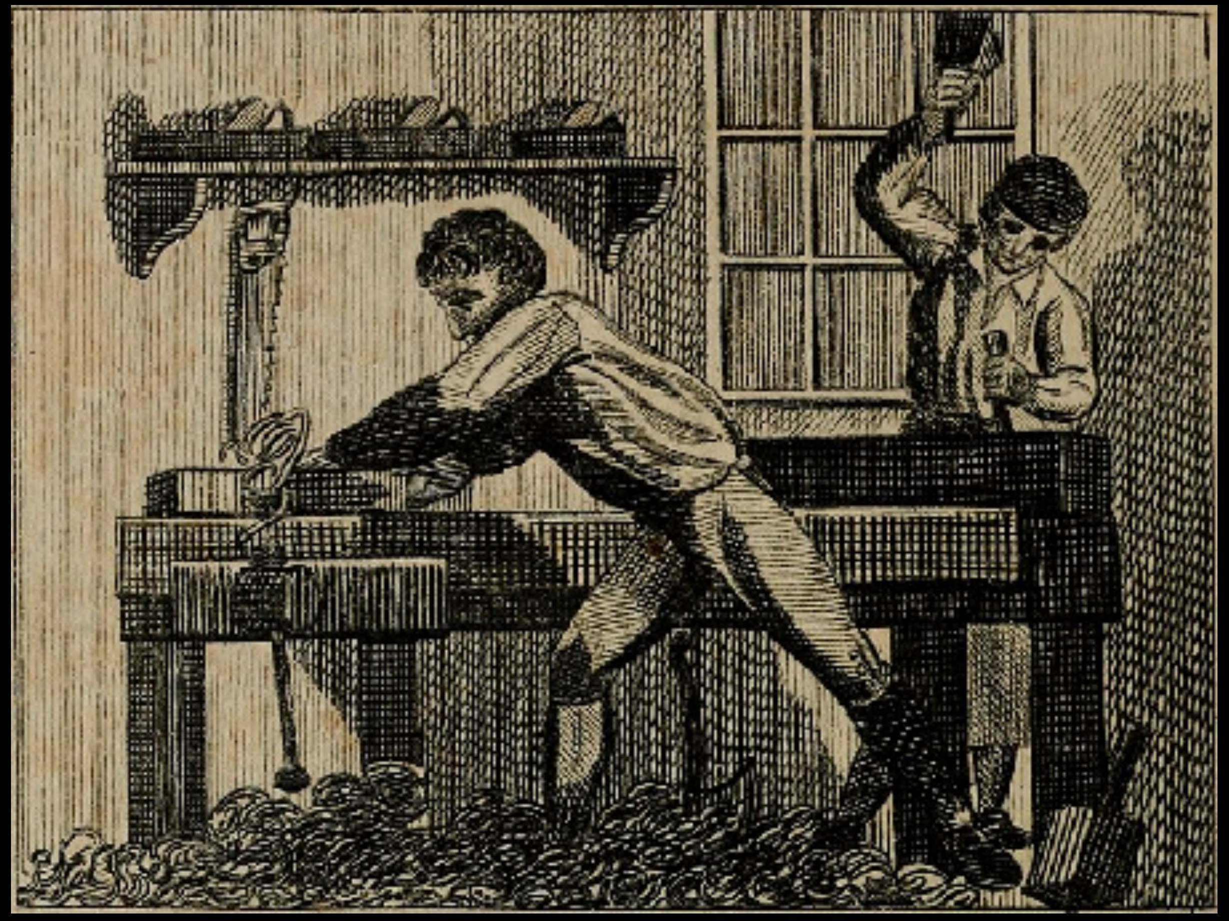
WHAT ARE THE GAPS?

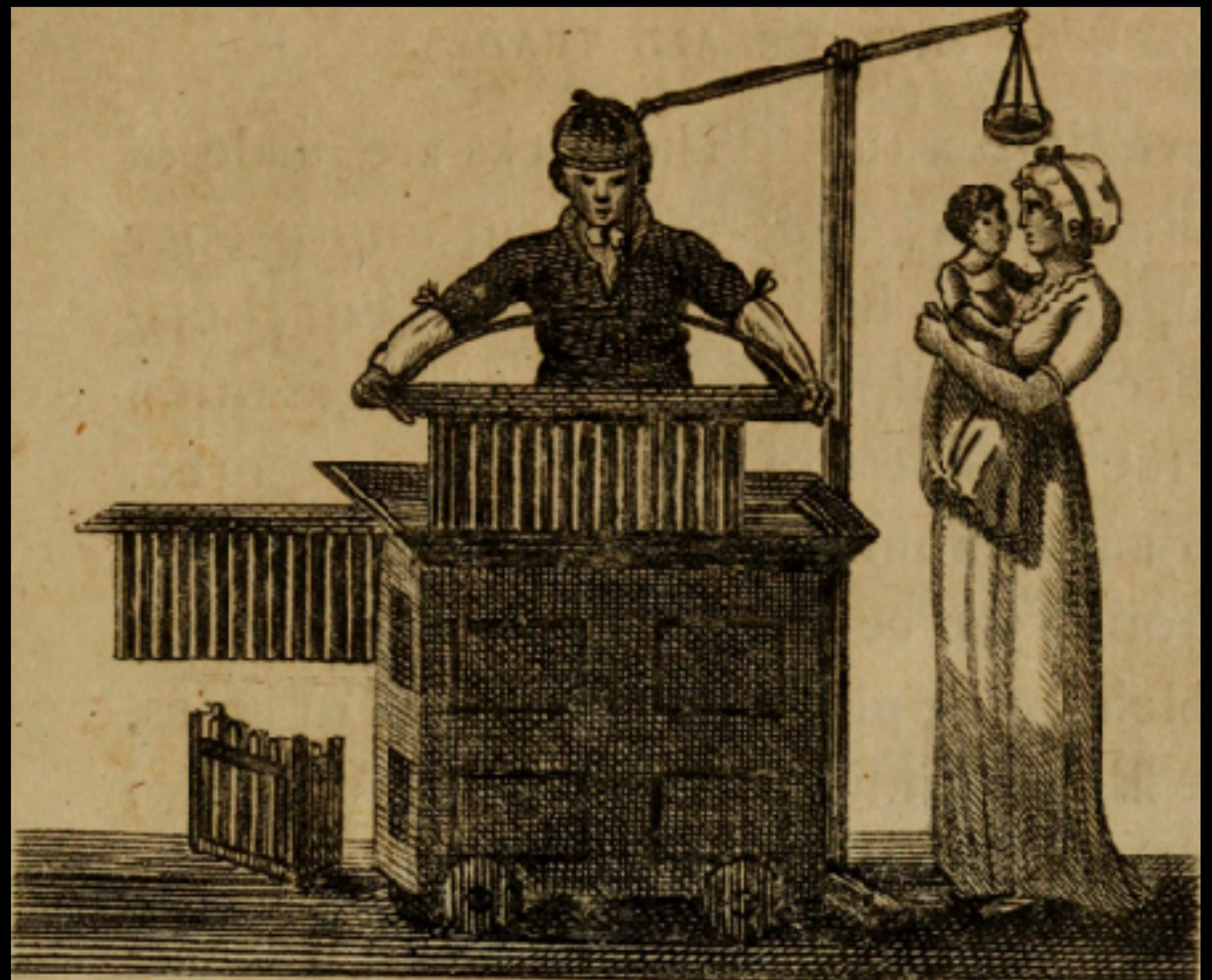
WHAT COULD BE MAGICALLY PREVENTED OR REMEDIATED?

CLOUD BRINGS CONSISTENCY, OVERWELMING RICHNESS, NEEDS AUTOMATION


Some cloud characteristics
On-demand, Self service
No-immediate blockers
A lot is straightforward
Easy to clutter
Overwelming details
RTFM,support, certification
Automation
Cloud model lends itself to automation which implies software development, and so risk and PM/Architecture skills
Security is a shared responsibiity
Physical security provided
Secure defaults
Tools provided (magic)
How to configure?
Continuous improvement
Continuous monitoring
e.g. hard to abuse network protocols
However are organisation-specific
Changes all the time
Gets better all the time
New risks
Continuous learning







JACK OF ALL TRADES AND MASTER OF NONE – CAN’T SEE WOOD FROM THE TREES

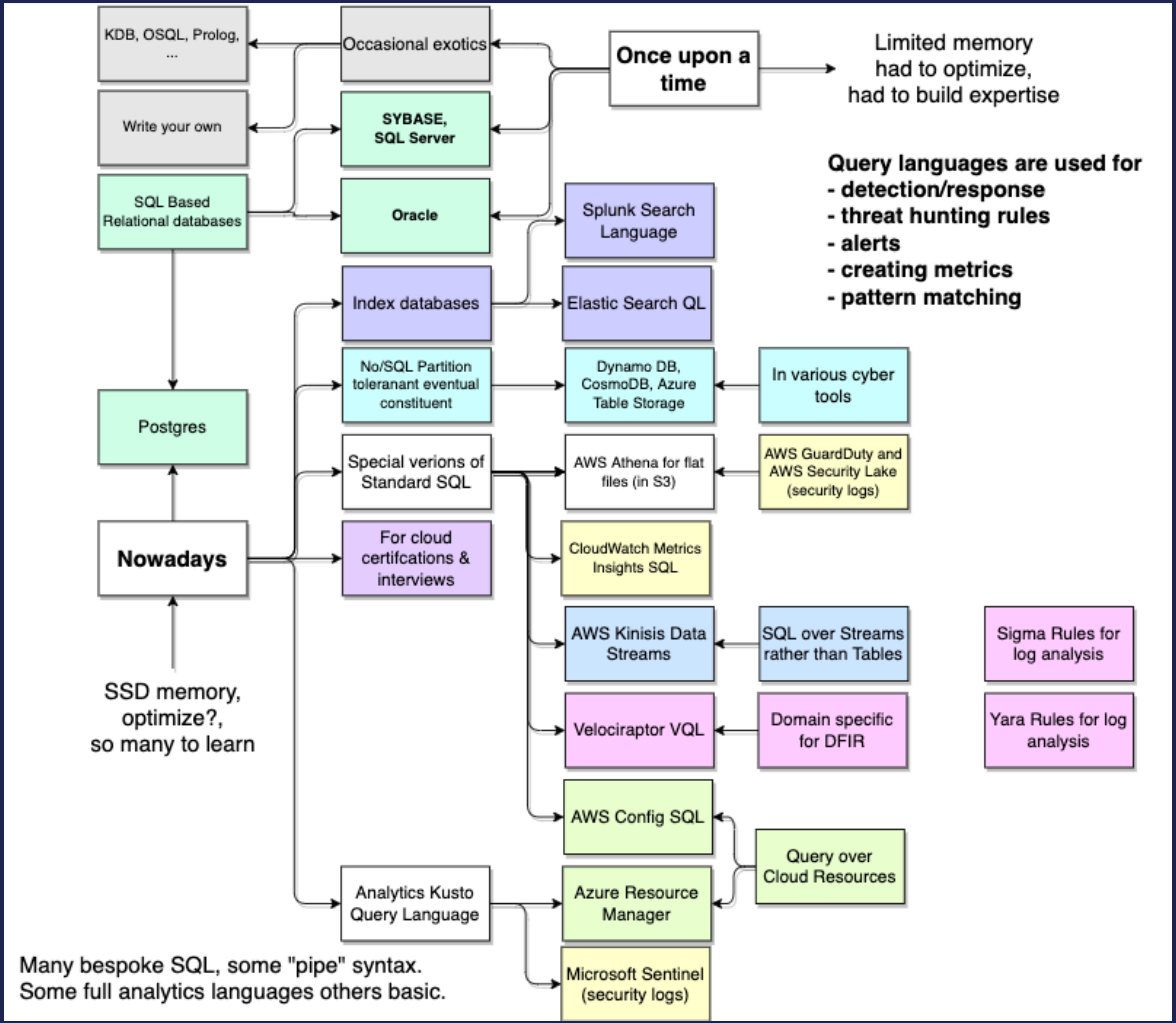
Anecdotes

ALL THE ADVANCED QUERY LANGUAGES TO LEARN AND MASTER(?)

15 YEARS AGO HAD TO KNOW SYBASE OR ORACLE SQL

NOWADAYS DOES ANYONE EXPECT TO KNOW ANYTHING SPECIFIC :-)

HAVING SAID THAT FOR AZURE KUSTO VERY GOOD



Once upon a time

Limited memory
had to optimize,
had to build expertise

Occasional exotics

KDB, OSQL, Prolog, ...

Write your own

SYBASE, SQL Server

Oracle

SQL Based Relational databases

Postgres

Nowadays

SSD memory,
optimize?,
so many to learn

Index databases

Splunk Search Language

Elastic Search QL

No/SQL Partition toleranant eventual constituent

Dynamo DB, CosmoDB, Azure Table Storage

In various cyber tools

Special verions of Standard SQL

AWS Athena for flat files (in S3)

AWS GuardDuty and AWS Security Lake (security logs)

For cloud certifcations & interviews

CloudWatch Metrics Insights SQL

AWS Kinisis Data Streams

SQL over Streams rather than Tables

Velociraptor VQL

Domain specific for DFIR

Sigma Rules for log analysis

Yara Rules for log analysis

AWS Config SQL

Query over Cloud Resources

Analytics Kusto Query Language

Azure Resource Manager

Microsoft Sentinel (security logs)

Query languages are used for
- detection/response
- threat hunting rules
- alerts
- creating metrics
- pattern matching

Many bespoke SQL, some "pipe" syntax.
Some full analytics languages others basic.

LOG, COUNT, PRESENT, ACT

ARGUABLY BASIC TECH FOR DETECTION

VERY FLEXIBLE - EXPENSIVE FOR BIG DATASETS -OPTIMIZE AVOID LOGS

TLP:GREEN

A FIRST EXPERIENCE OF DETECT AND RESPOND AND DEVSECOPS

DETECT

RESPOND

PROTECT

- **Shocked** to see our **development** environment on my phone!
  - A) **SysOps** had always set up a firewall
  - B) I could **fix** it in **minutes** myself without any **drama -** no escalations, incidents, email judo, finger pointing or firings
- I could take responsibility for **security** from early in development rather than an afterthought.
  - I could happily do **Dev**, **Sec** and **Ops** hence **DevSecOps**.

MY BANKING BACKGROUND

IN DEV - PROTECT, DETECT, RESPOND JUST PART OF LIFECYCLE

AI MAGIC

HUMAN/AI ERROR

- **ChatGPT** created a script to create a VM without a unique admin password.
- Defender automatically **detected** a **brute force** attack.
  - **Automatic response** would **isolate** machine- keep forensics.
  - **Guardrails** could prevent this going forward.

DETECT

RESPOND

PROTECT

BLAMELESS REVIEW VS BLAME CULTURE

CAUGHT BUT WHY EVEN POSSIBLE? WHY SO MANUAL. IS IT REALLY MATURE?

TLP:GREEN

CLUTTER AND CLOUD RESOURCES

“Discard everything that does not spark joy?” – Marie Kondo’s Art of Tidying

WE END UP MONITORING CLUTTER

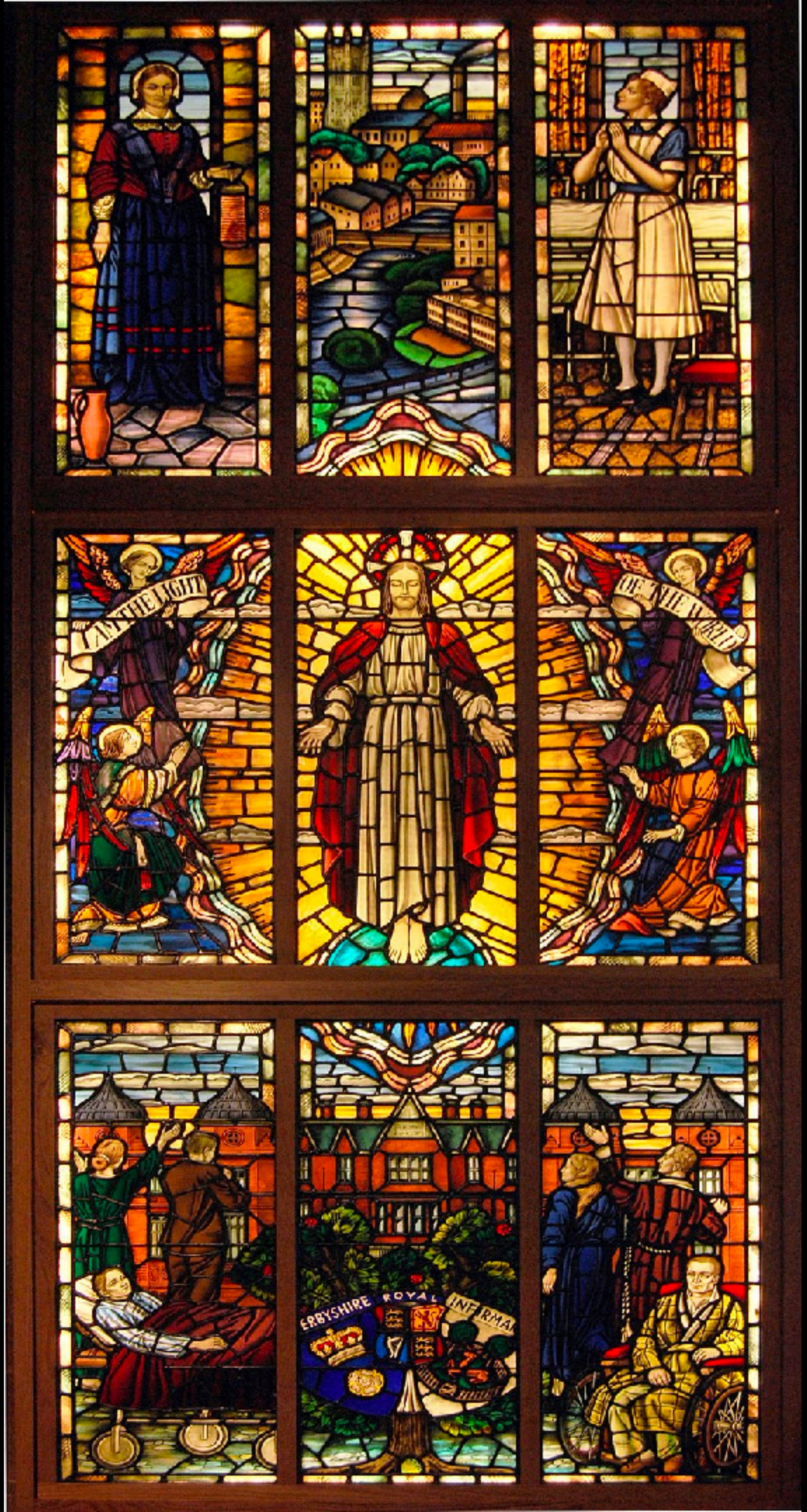
- Software & resources **hang around, cost &** add to **attack surface**
  - POCs, tests, unused features, functionality migrated …
  - How to make sense of **> 100 default workspace** and other **legacy** cloud resources?

SOMEONE HAS TO PAY THE TECHNICAL DEBT

EASY TO DETECT

- **Easy to query** Cloud Resources, **get rid of any we don’t need,** can mostly re-create on-demand - **Infrastructure as Code (IaC)**.
  - Virtual machines need **patched**, **upgraded**, **backed up**, **monitored** – **Managed Cloud services** - App Services, Batch, …

BE RUTHLESS



CONCLUSION

SOME NEEDS A LOT OF CARE AND CONFIGURATION AND SOME IS MAGIC

LOG, COUNT, PRESENT, ACT

- I am sure many people in the hospital were probably very aware of the issue and the solution. Florence Nightingale's magic was to find a way to **package** and **present** to get **action**.
- I am sure many people are very aware of what and how to **detect** and **automatically** respond. I feel much work needs to done to **package** it all up **seamlessly** and **efficiently.**

10 years CERT-EU

THINK CONSTITUENT
CREATE VALUE

https://cert.europa.eu
secretariat@cert.europa.eu
@CERTEU