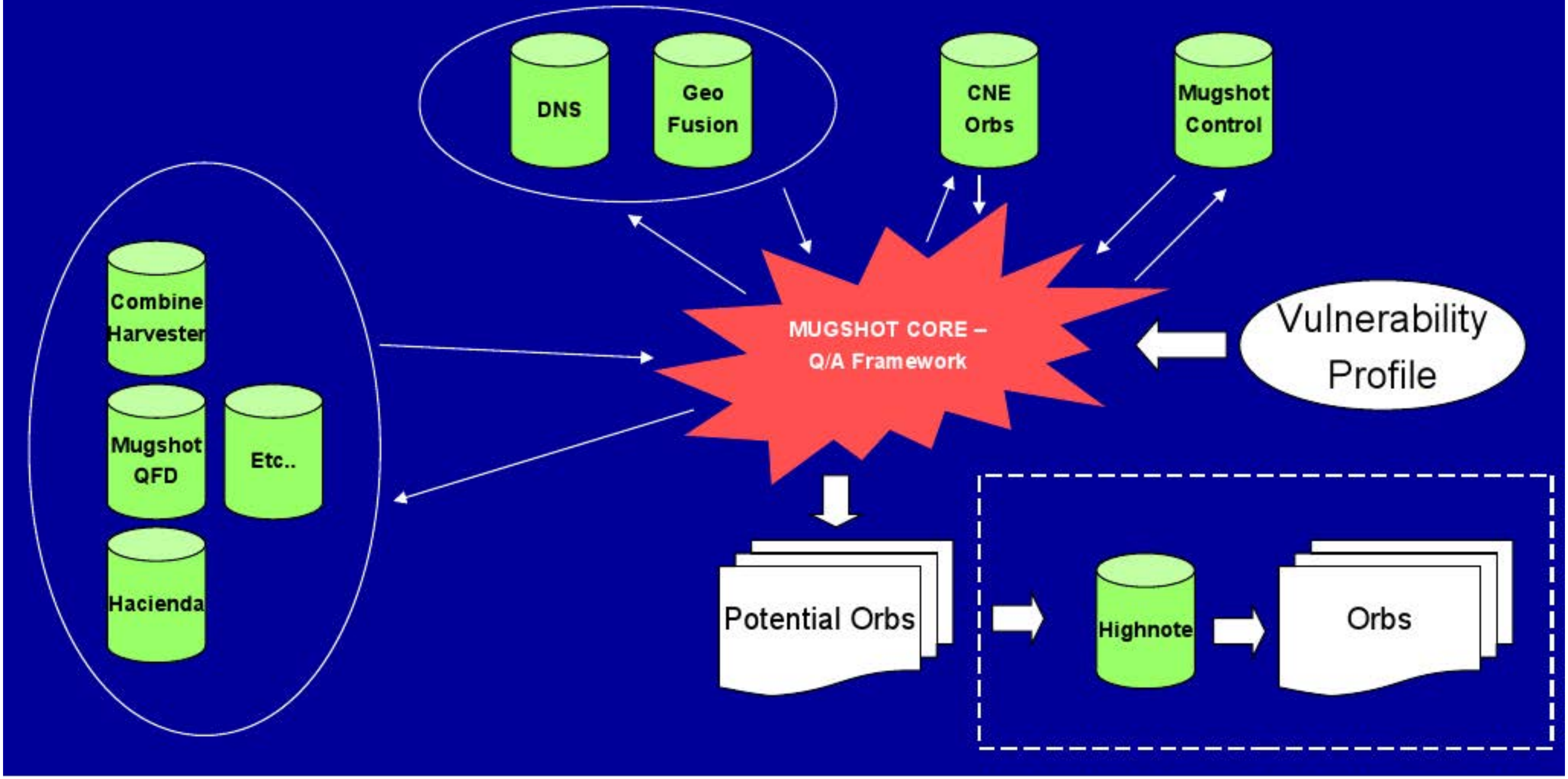
Use Case 1: Finding Orbs



DNS

Geo Fusion

CNE Orbs

Mugshot Control

Combine Harvester

Mugshot QFD

Etc..

Hacienda

MUGSHOT CORE – Q/A Framework

Vulnerability Profile

Potential Orbs

Highnote

Orbs

[redacted]

Benefits

- Automated Vulnerability Assessment
  - Using Vulnerability Profiles for Remote and Content Delivery vectors
- Automated Target Development and Monitoring
  - Identify and characterise target machines
- Profiles machines, including:
  - Browser, OS, PSP, Patch History
  - Activity
  - Download
- Automated Target Technology Tracking (Stats & Trends)
  - Browsers, OS, PSP etc
- ORB Identification
  - Initial ten fold increase in Orb Identification rate over manual process

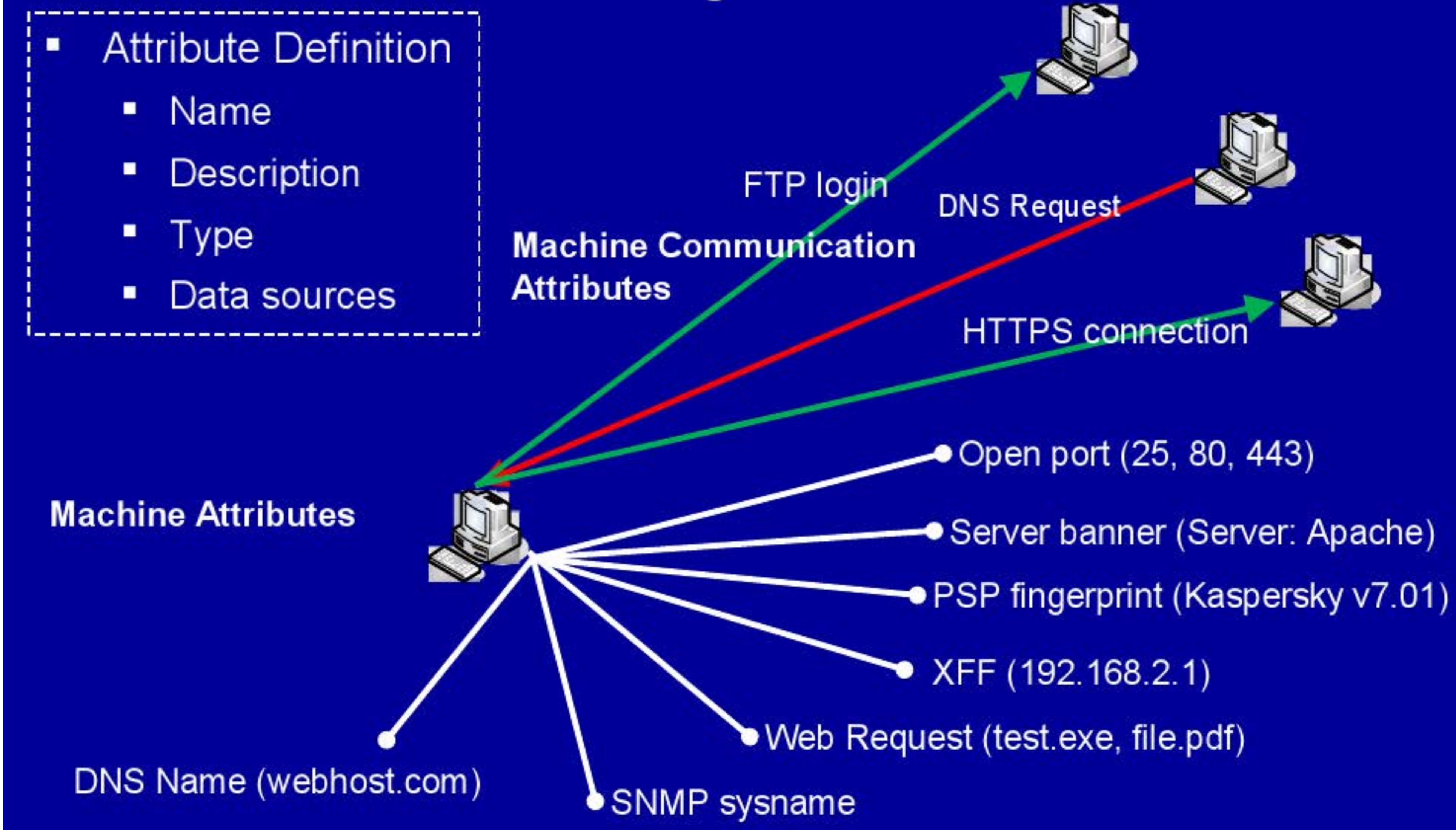
GCHQ

[redacted]

UK TOP SECRET STRAP 1

Defining Attributes

- Attribute Definition
  - Name
  - Description
  - Type
  - Data sources



GCHQ

[redacted]

MUGSHOT GOALS

- Automated Target Characterisation and Monitoring
  - Automatically understand everything **important** about **CNE target networks** from passive and active sources.
- Automated Un-Targeted Characterisation
  - Automatically understand everything **important** about **all machines** on the Internet from passive and active sources.

[redacted]