Detica

BAE SYSTEMS

Advanced Persistent Threats - They are Everywhere!

Doug Stuart, Technical Director

CSM-ACE Conference: November 2012

Detica

BAE SYSTEMS

Some of our TDL4 analysis

The dropper is packed with an interesting packer that **disguises the protected executable** underneath as a normal code 'normal' code produced by the protector is **designed to fool AV engines.**

Finally, the dropper **extracts a malicious Master Boot Record and Volume Boot Record**, and installs them along other components in the system

Apart from several malicious components, the dropper contains some legitimate resources as well (the PROXY32 and PROXY64 ones). **These 'proxy' resources are likely dropped and run in order to trick behavioural analysis systems** into believing that the sample in question does not only look nice statically (as explained above), but the files that it drops dynamically are also legitimate, some with the valid digital signatures.

This stealthiness makes the extremely vicious TDL4 also very crafty as it manages to bypass many AV solutions on the spot.

TDL4 has a component called CMD32/CMD64 that **fetches JPEG images from the blogs** specified in its configuration file.

Steganography algorithm is used to conceal the text within the images, it is impossible to recover the text.

Applying this function over all JPEG images from the 2 previously mentioned blogs, allows assembling the C&C domain list. **Once the new C&C servers go live, TDL4 will visit them and request updated configuration from them.**

This vicious cycle may potentially go on indefinitely. Until there is at least one live domain or one live blog, the masterminds behind the botnet have a chance to inject a new portion of the domains and blogs into this deadly whirlpool, preserving full control over the victims.

As a result, when the user clicks a link returned by Google Search, the "url=" parameter will be replaced with a different web page, leading to skewed analytics, fraudulent monetization via AdSense, clickjacking, Search Engine Optimisation (SEO) poisoning, and other **click fraud that constitutes the "cash cow" business for the TDL/TDSS group.**

http://stratsec.blogspot.com.au/

Detica

BAE SYSTEMS

Is it a new world order?

- 10 years ago:
  - We built our company on the mantra that “security is just another business function”
  - We aimed to remove the “scaremongering” and legitimise our industry
  - We had a fortress mentality……

- Today’s threats need a new approach:
  - We now live in an ever increasing hyper-connected world
  - A wide-range of threat actors with a wide-range of motivations
  - Attacks are highly sophisticated and built to avoid detection
  - Attacks are now ***very targeted*** and are ***relentless***
  - Existing controls are proving to provide limited protection

Detica

BAE SYSTEMS

Today's topics

- Understanding targeted attacks
- Detecting targeted attacks – the challenge!
- Taking an analytical approach
- Implementing the analytical process
- The role of the analyst and engineer

Detica

BAE SYSTEMS

What do we mean by “targeted attacks”?

NOT Accidental data loss

NOT Actions by malicious insiders

NOT Denial of service attacks

NOT Viruses, worms, botnets or other indiscriminate malware

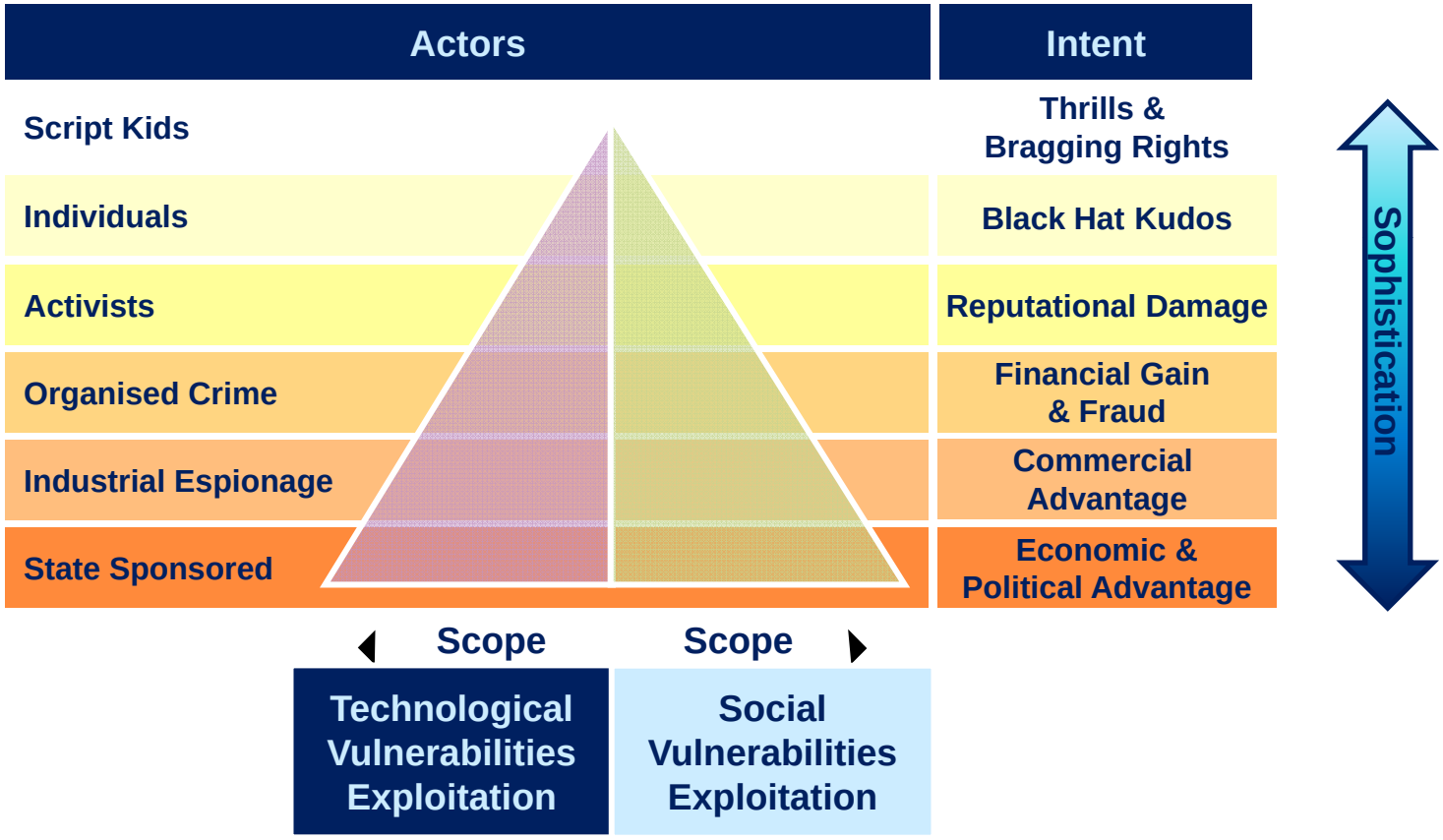
→ Determined efforts to break in to a specific network to steal data or access sensitive systems

NB in some contexts described as Advanced Persistent Threat or APT

Detica

BAE SYSTEMS

Targeted attacks – actors and intent

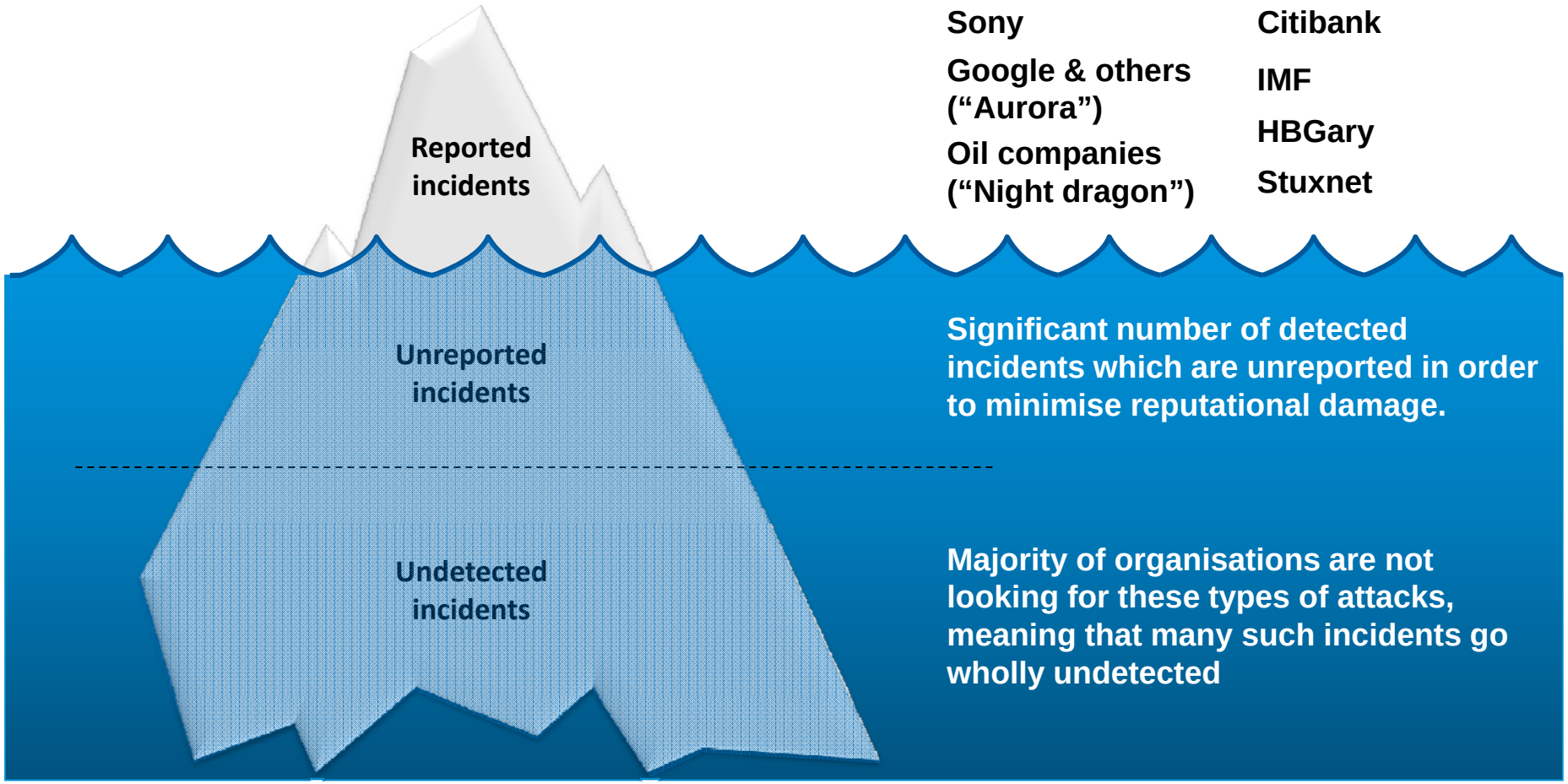


Detica

BAE SYSTEMS

The targeted attack iceberg

Successful targeted attacks



Sony

Google & others ("Aurora")

Oil companies ("Night dragon")

Citibank

IMF

HBGary

Stuxnet

Significant number of detected incidents which are unreported in order to minimise reputational damage.

Majority of organisations are not looking for these types of attacks, meaning that many such incidents go wholly undetected

Detica

BAE SYSTEMS

Targeted attack techniques

- Spearphishing
- Drive-by-downloads
- Trojans
- Backdoors
- Fake software
- Supply chain compromise
- Man-in-the-middle
- Rootkits
- Botnets
- Zero-day exploits
- SQL injection
- Cross Site Scripting
- Password stealing
- Pharming
- Domain obfuscation
- Evil maid attacks
- USB sticks
- Keyloggers

…and whatever else provides a good cost-benefit trade-off given the attacker's expected gain

For a well resourced, sophisticated and determined attack against a high profile target, the attacker will adapt their techniques to avoid standard controls and detection techniques to achieve their aims

Detica

BAE SYSTEMS

Detecting targeted attacks – the challenge

Known rules and signatures

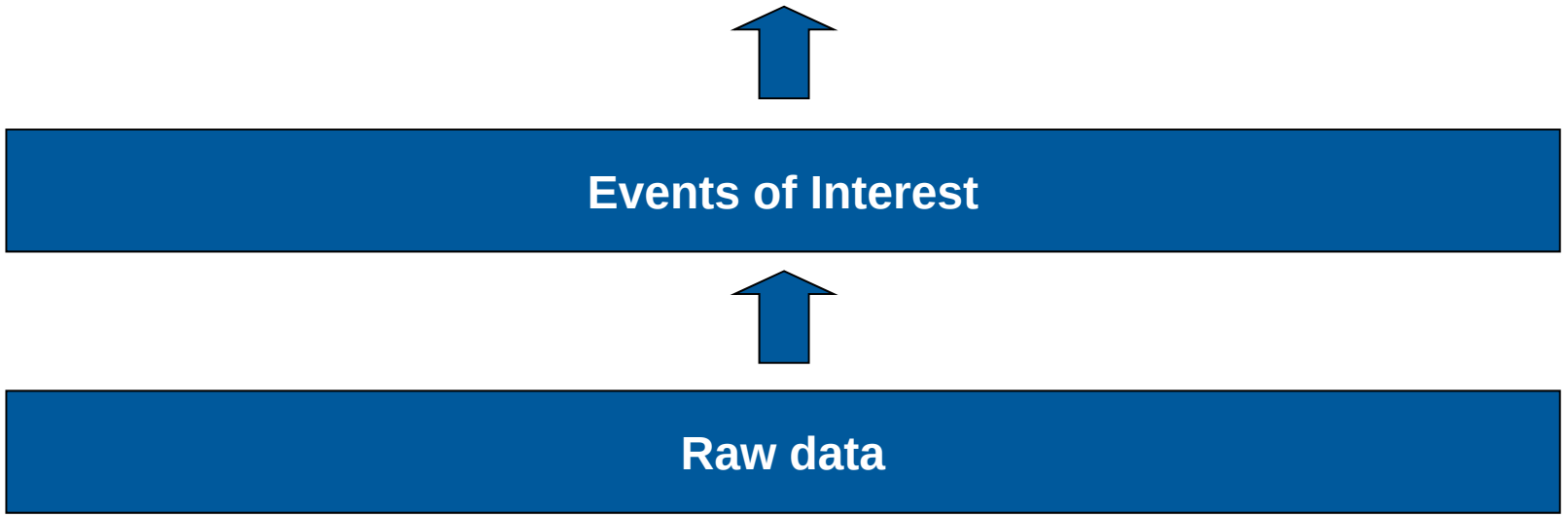
Too easy for well resourced and determined adversaries to evade

Detica

BAE SYSTEMS

Detecting targeted attacks – the challenge

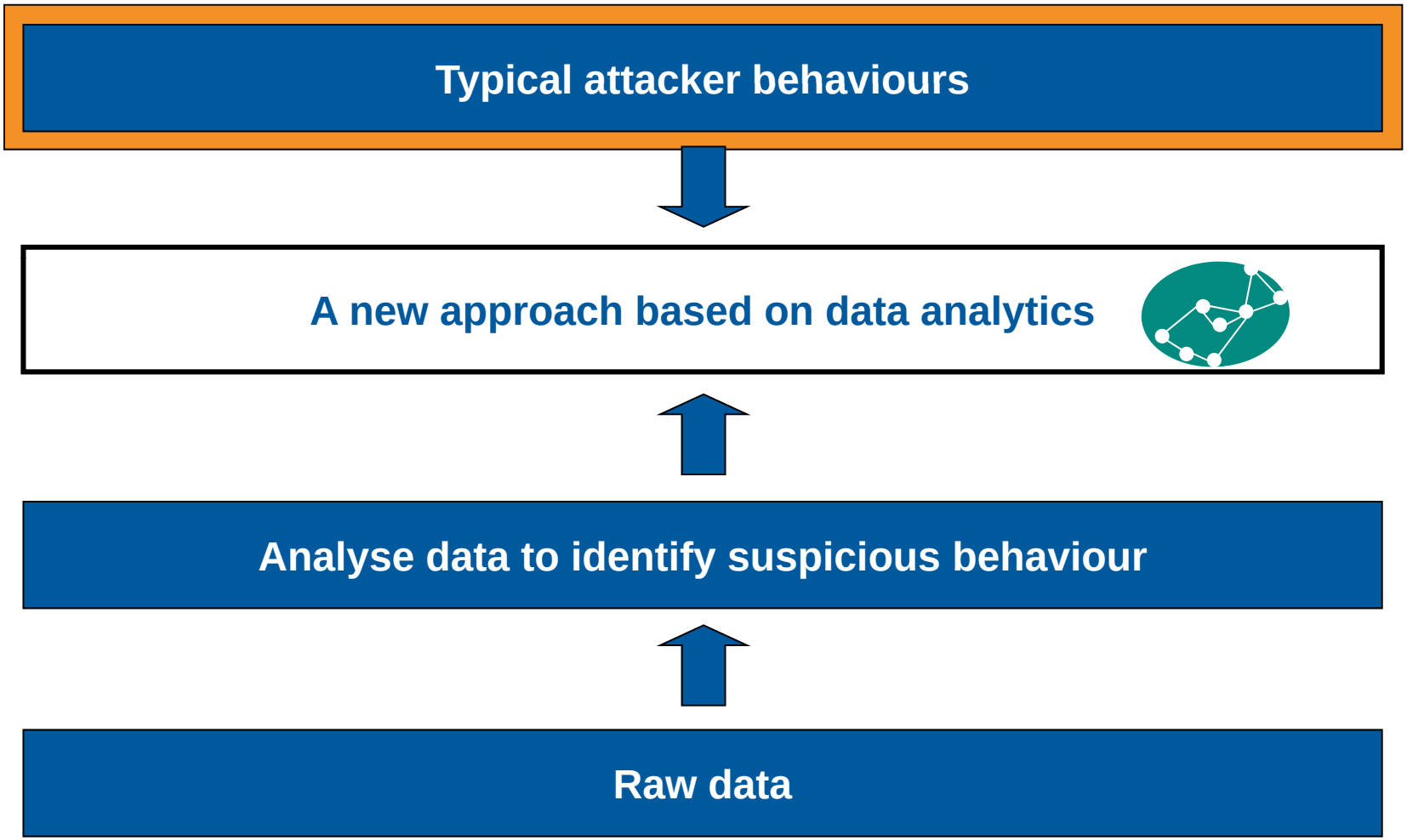
Too many false positives to derive actionable intelligence



Detica

BAE SYSTEMS

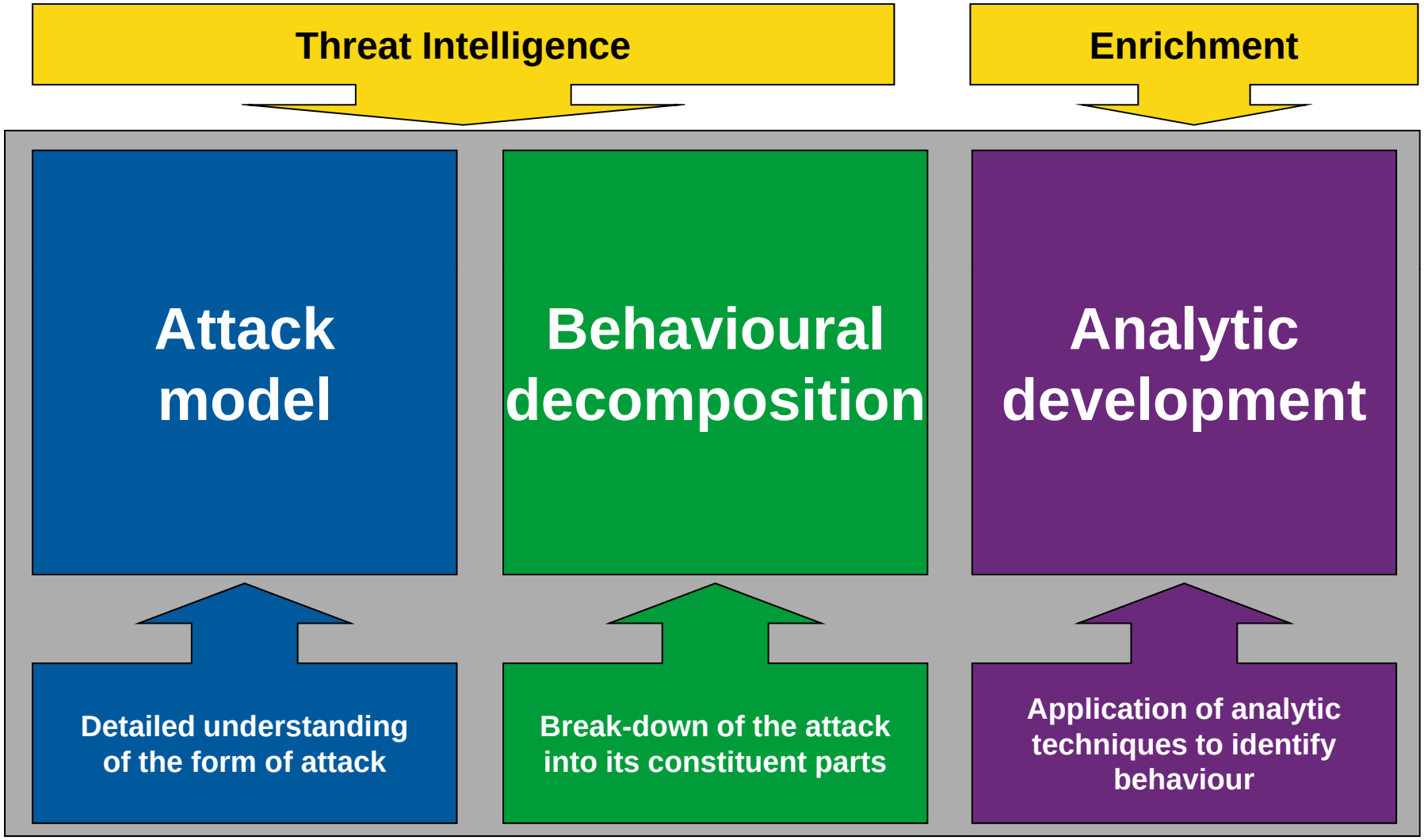
A new approach – data analytics!



Detica

BAE SYSTEMS

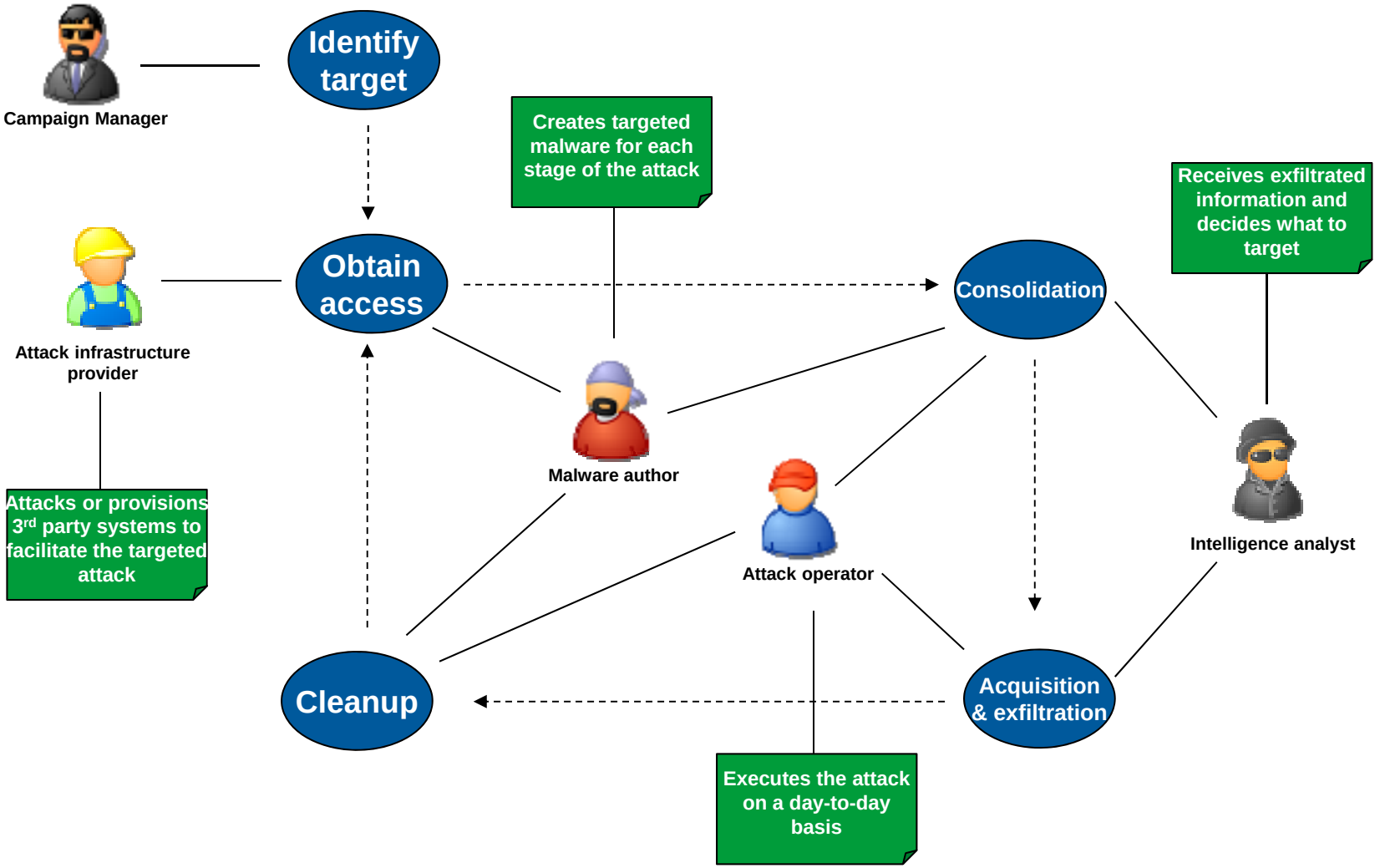
Taking an analytical approach to the problem



Detica

BAE SYSTEMS

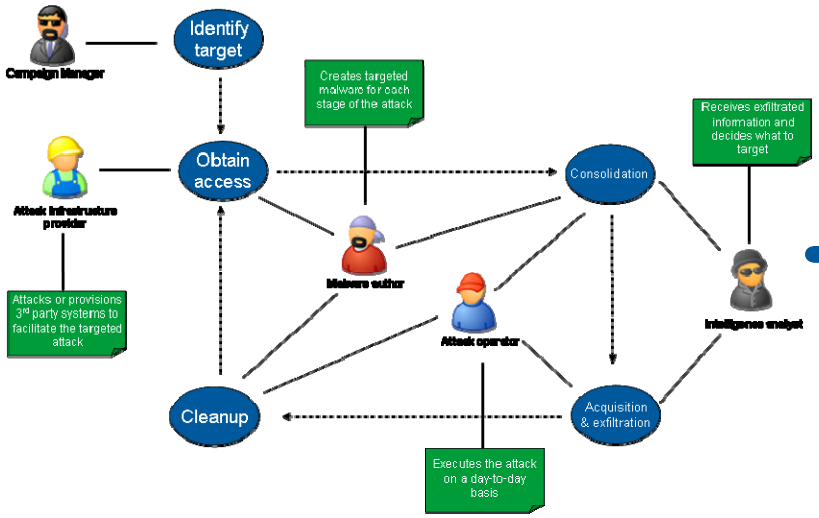
Attack model



Detica

BAE SYSTEMS

Behavioural decomposition



- Reconnaissance
- Infiltration
- Beaconing
- Persistence
- Command & control
- Staging
- Exfiltration
- Clean up

Detica

BAE SYSTEMS

Analytic development example

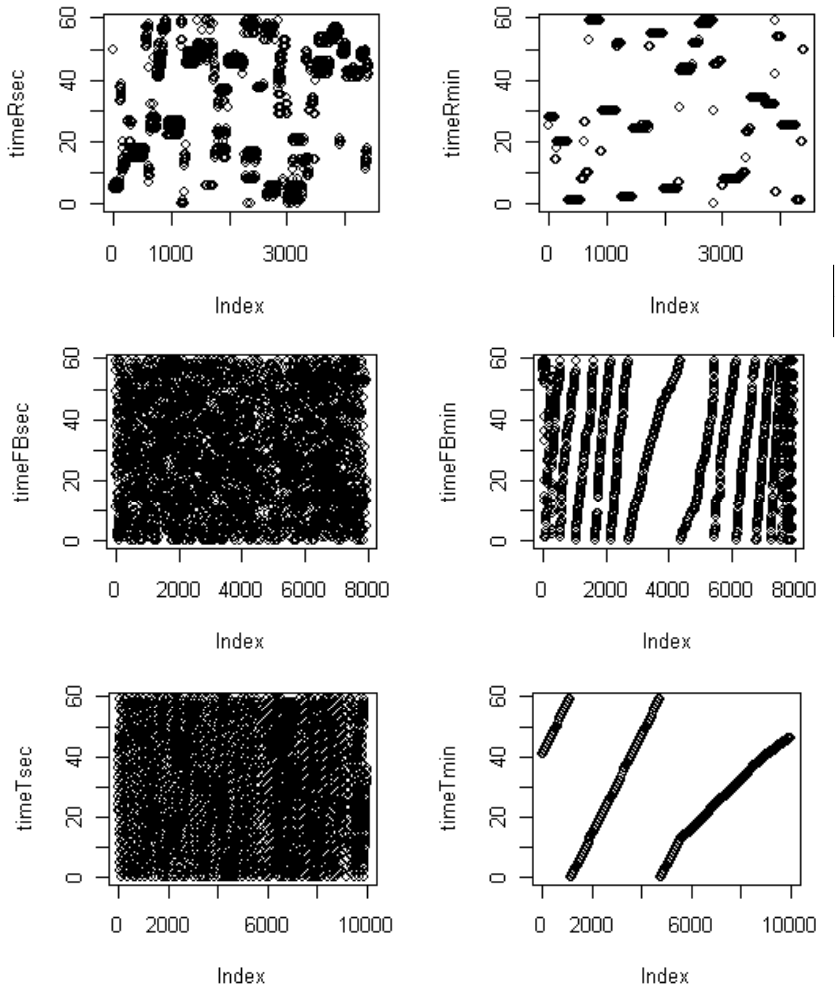
Periodic transfer of data to establish a command and control channel

Differentiate anomalous behaviour from legitimate activity

Legitimate browsing

Facebook

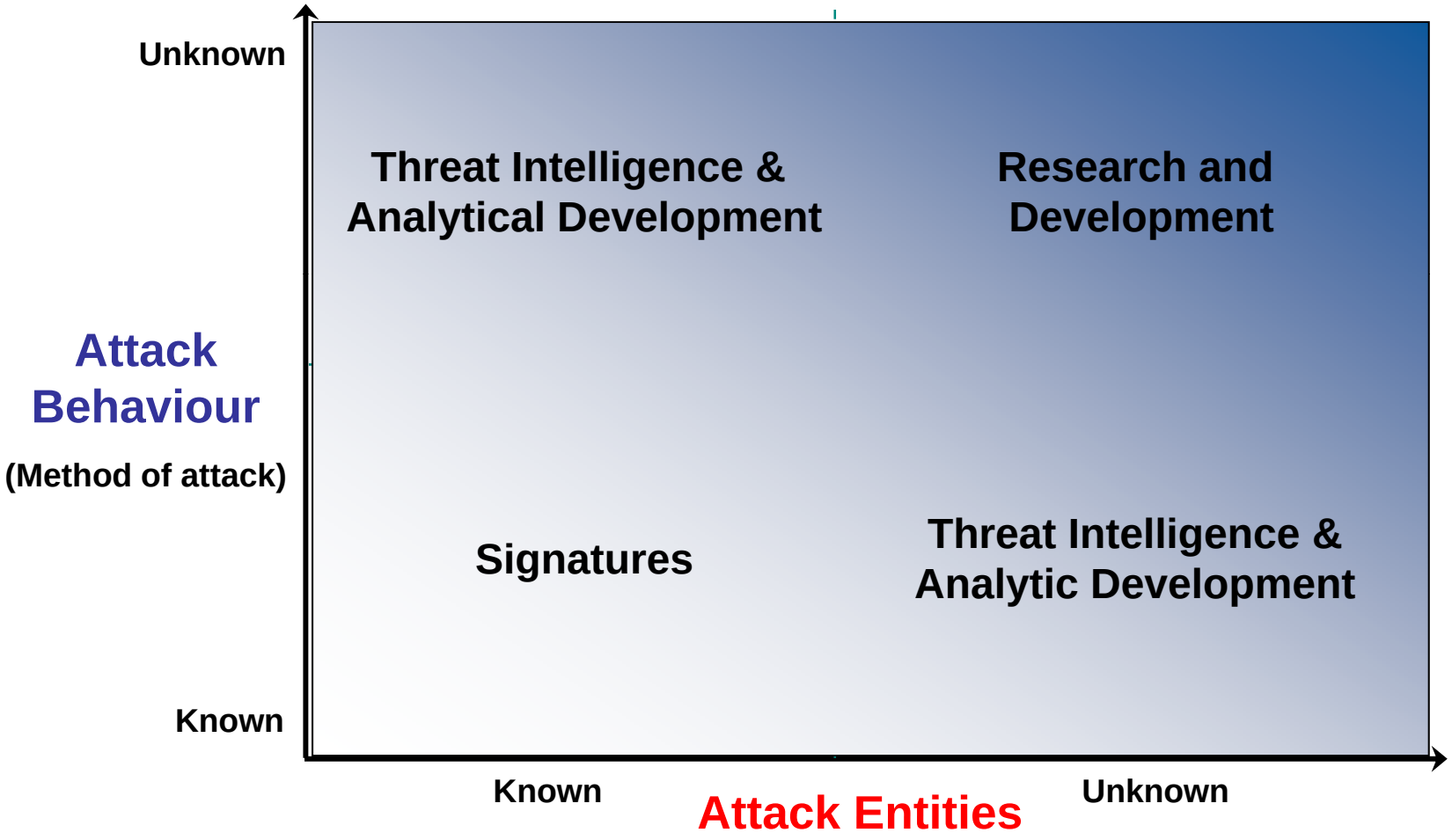
Attack



Detica

BAE SYSTEMS

Approach and methodology – holistic



Detica

BAE SYSTEMS

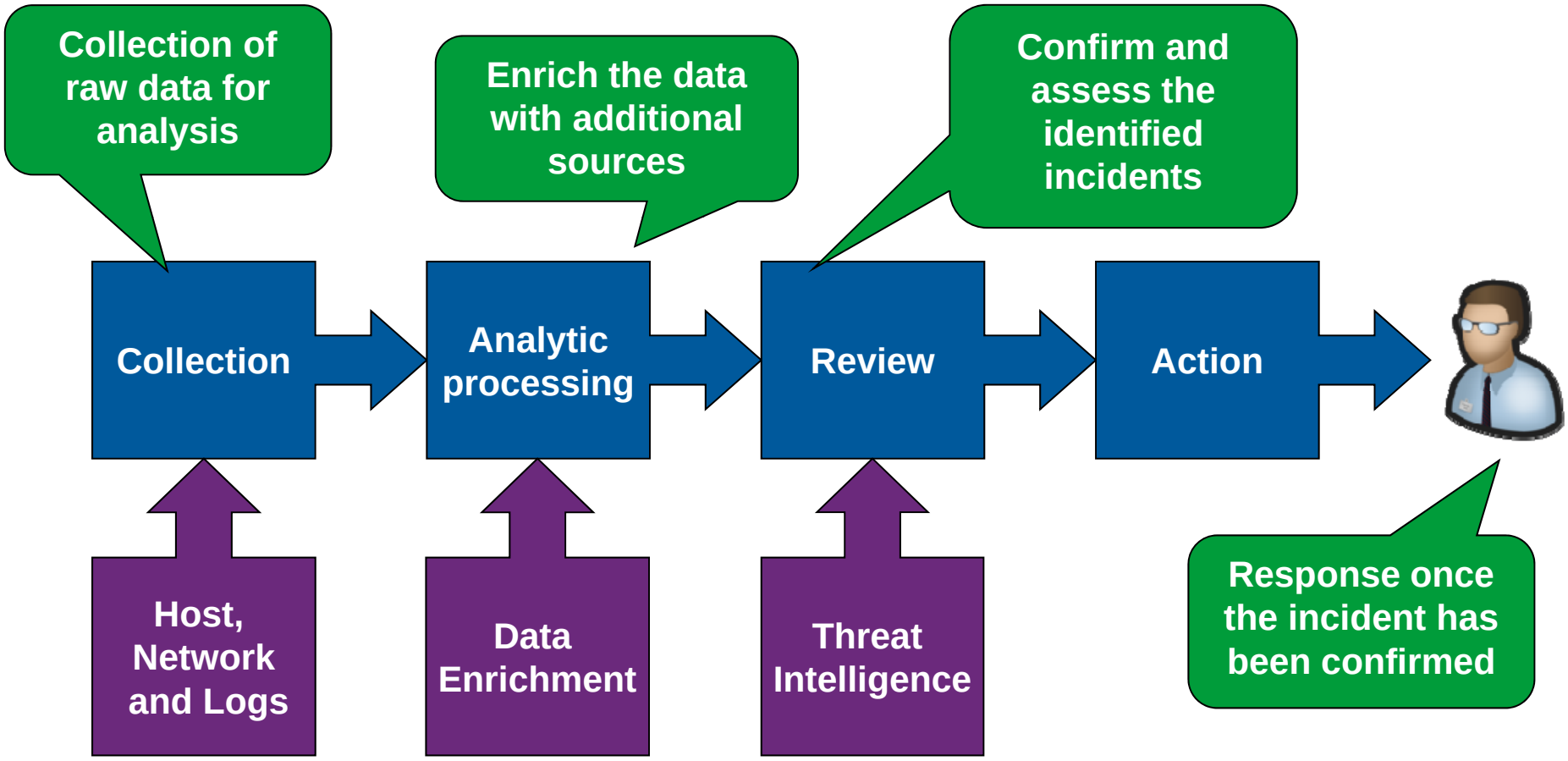
The data analytics process

- **Data collection** from a range of sources:
  - Data from passive network probes about every network transaction
  - Data from host agents about every process, file changes, etc
  - Log files from a wide range of platforms and application
- **Analytical processing** of collected data:
  - Determines high risk anomalous behaviours
  - Enrich the data set with additional data feeds
  - Generate suspicious activity indicators
- **Review** of processed data:
  - Analysts review and visualise
  - Confirm the detection of serious incidents
- **Action** on determined incidents:
  - Responders deal with identified and qualified incidents

Detica

BAE SYSTEMS

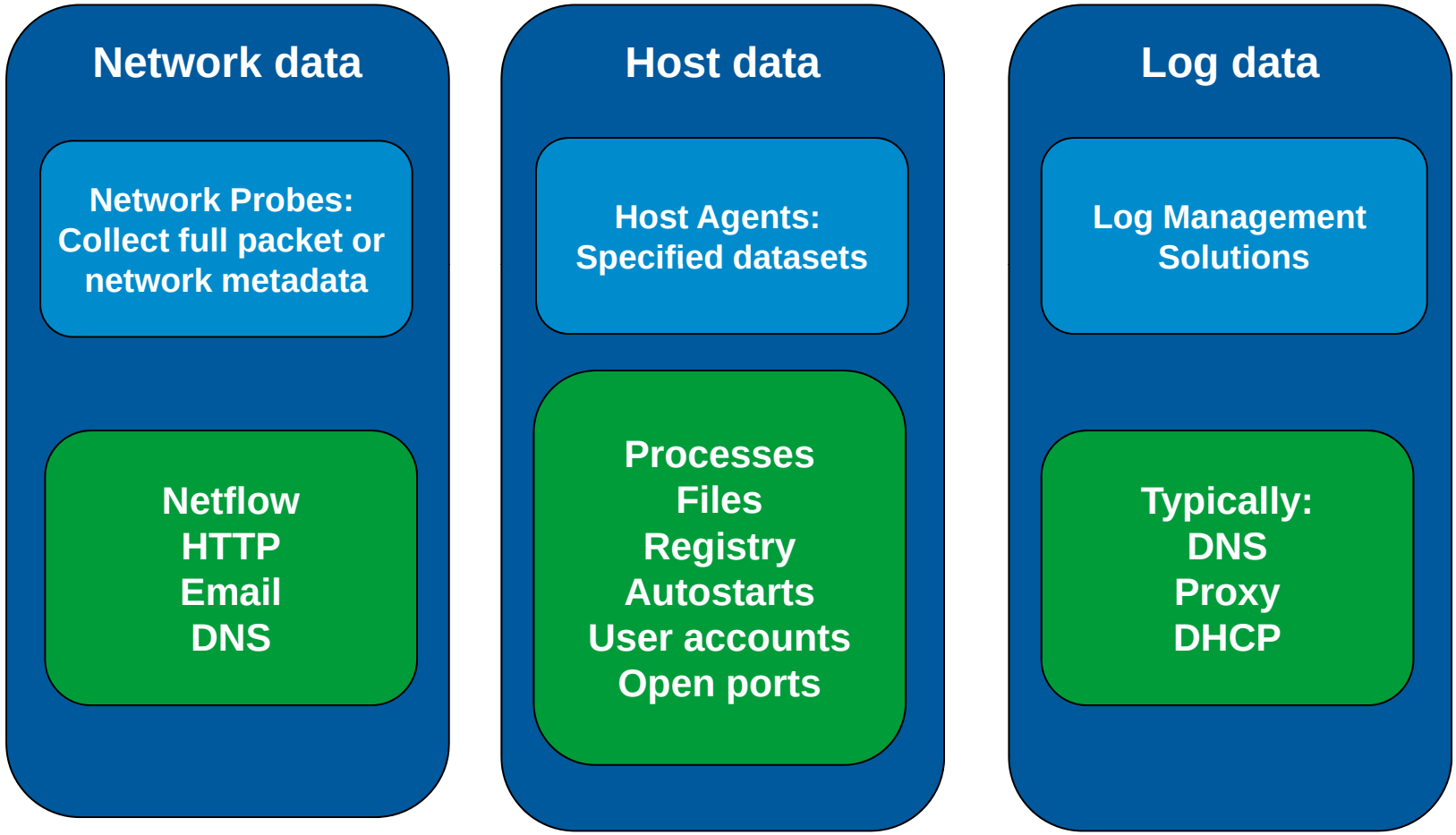
The analytics process



Detica

BAE SYSTEMS

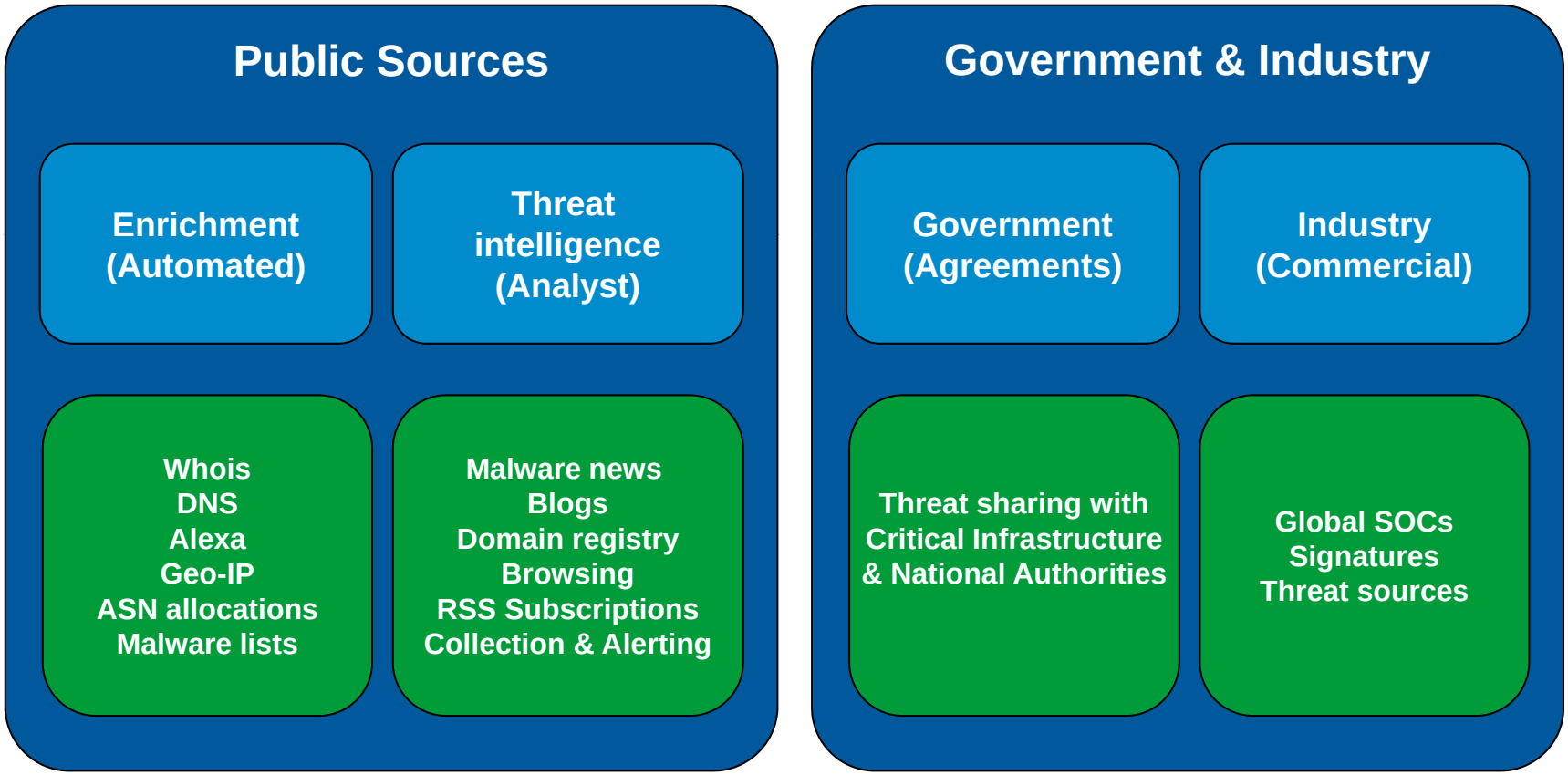
Data collection – event data



Detica

BAE SYSTEMS

Other inputs to the analytics process



Detica

BAE SYSTEMS

Importance of the analyst and engineer

- A data analytics approach aims to:
  - Reduce false positives and the network noise
  - Allow our smartest and high-demand analysts and engineers to concentrate on the things that matter
  - Ultimately, identify as quickly as possible, targeted and persistent attacks that might otherwise go undetected
- The human becomes even more important:
  - Threat intelligence
  - Analytical development
  - Research and development
  - Incident response

It still takes a human to catch a human

Detica

BAE SYSTEMS

Better detection – key requirements

1. **Detect and investigate** suspicious activity rather than relying on detection of “known bad” malware or network traffic
2. Detect suspicious behaviour based on a combination of **statistical analysis** and deep understanding about **attacker tradecraft**
3. Gather data about **all network activity** in order to mine it for evidence of suspicious behaviour
4. **Fuse data from multiple sources** in the network in order to detect suspicious behavioural patterns that span multiple systems
5. Be ready to gather and process **many Terabytes of data** in order to achieve this
6. Requires ready access to **skilled analysts** and high quality **threat intelligence**