

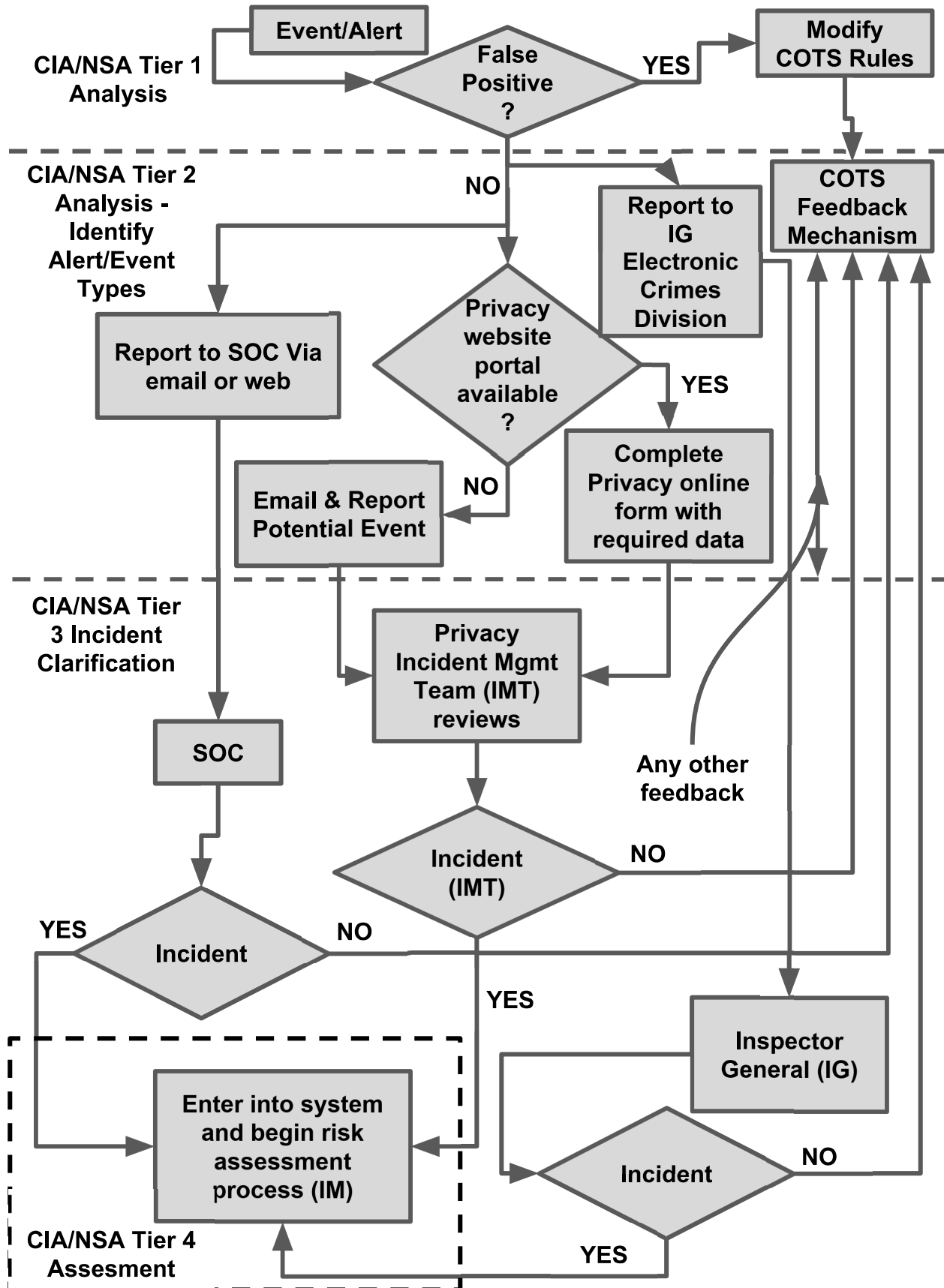


FIG. 1

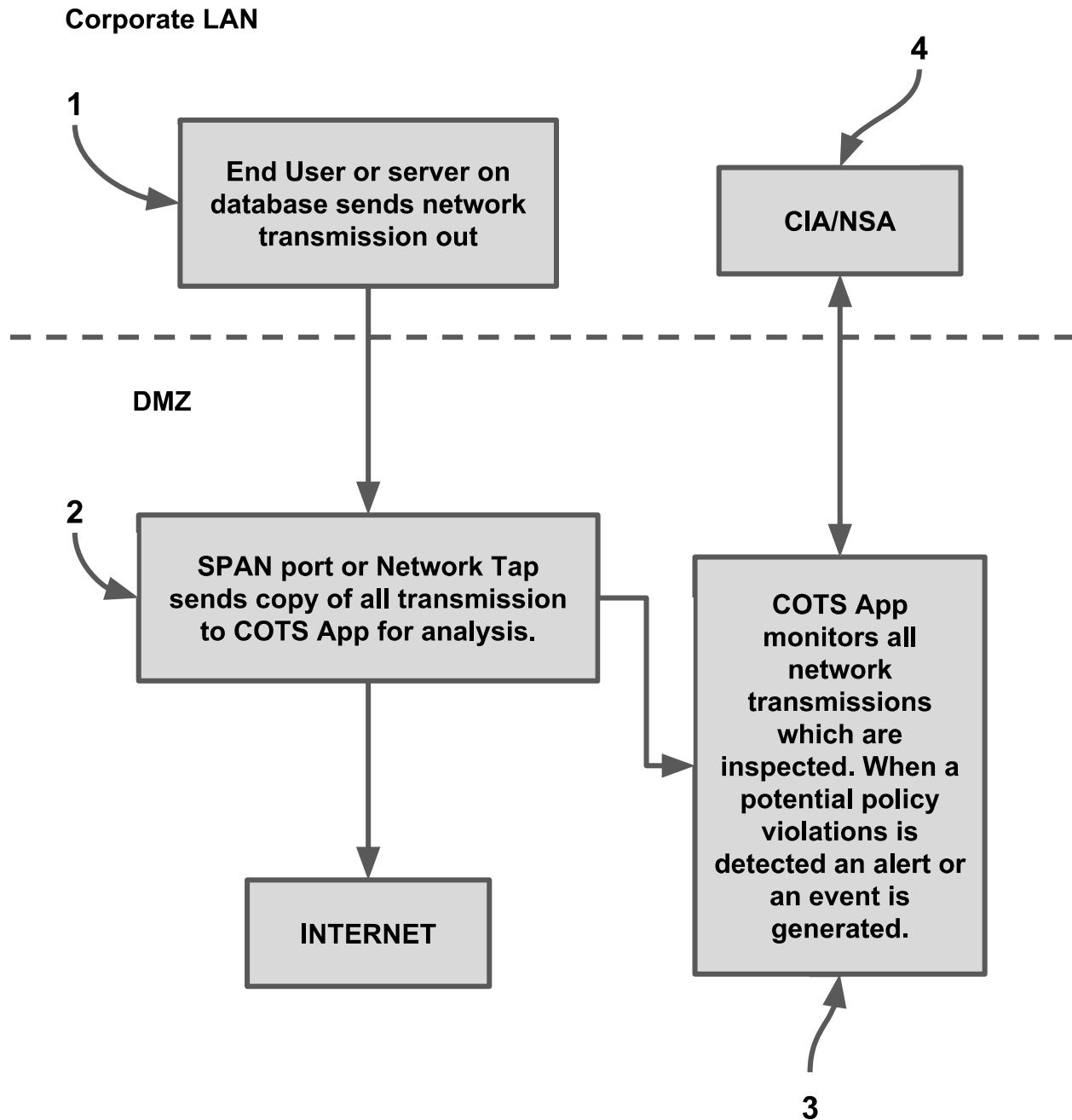


FIG. 2

Data/Alerts/Events From Various Devices

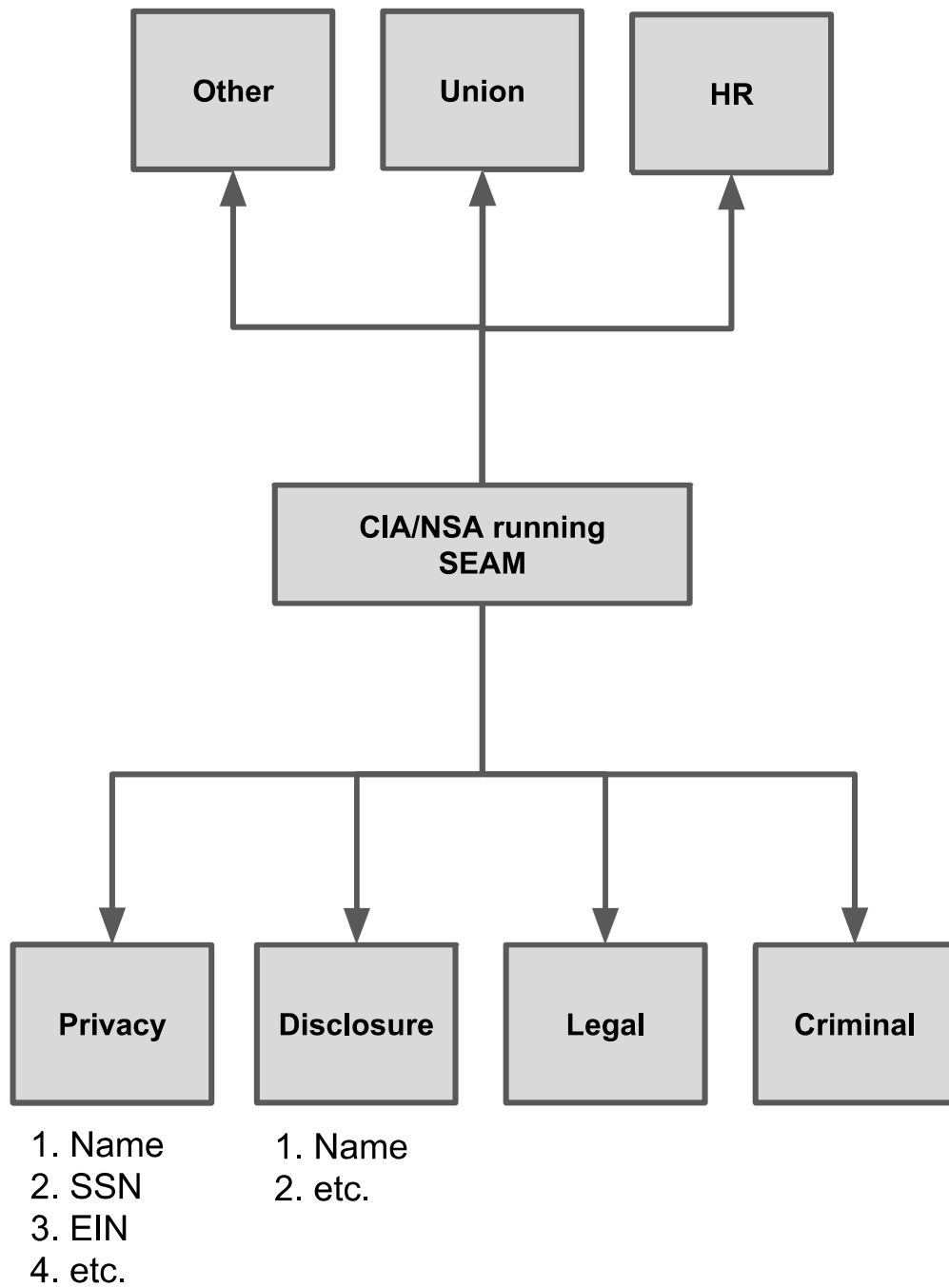


FIG. 3

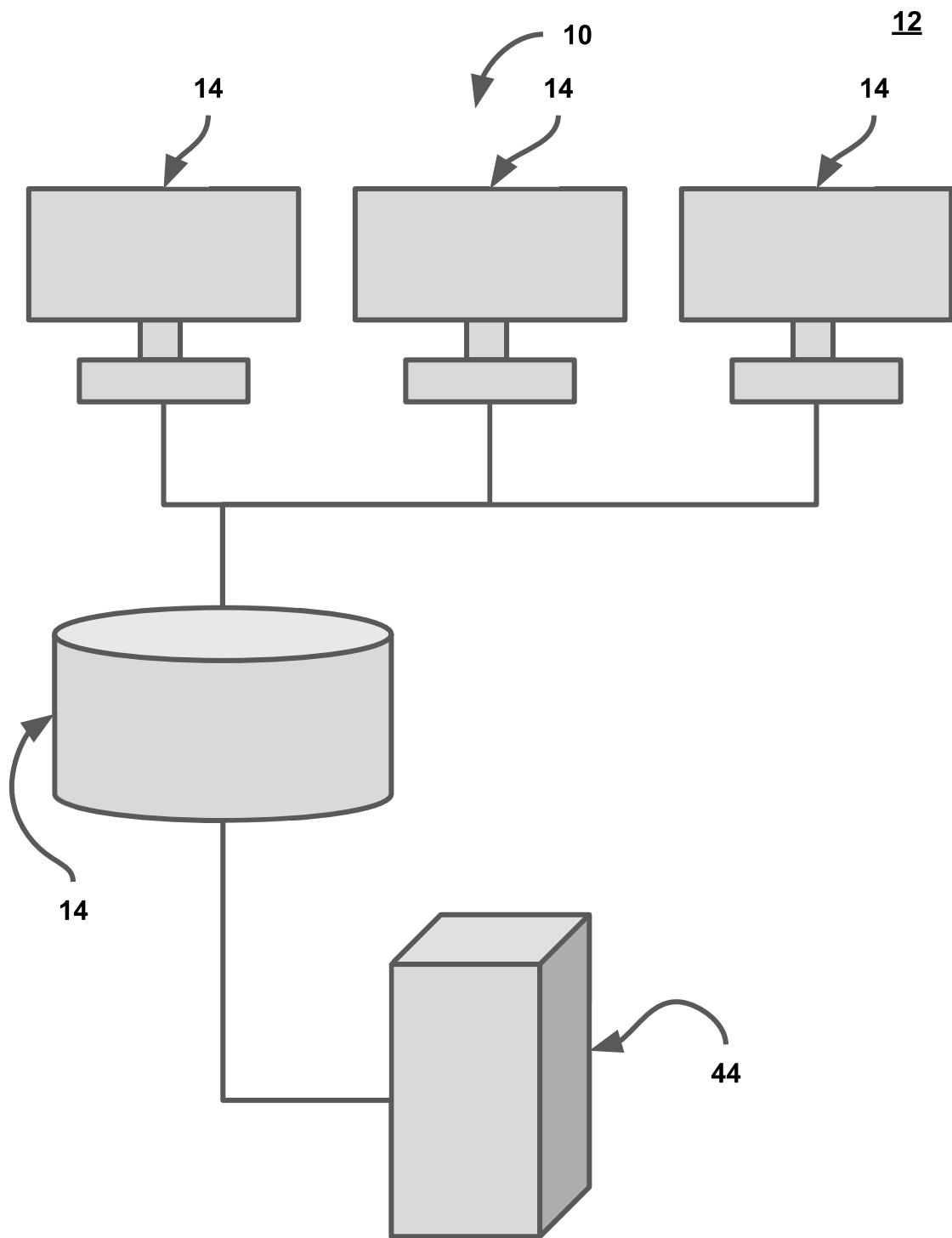


FIG. 4

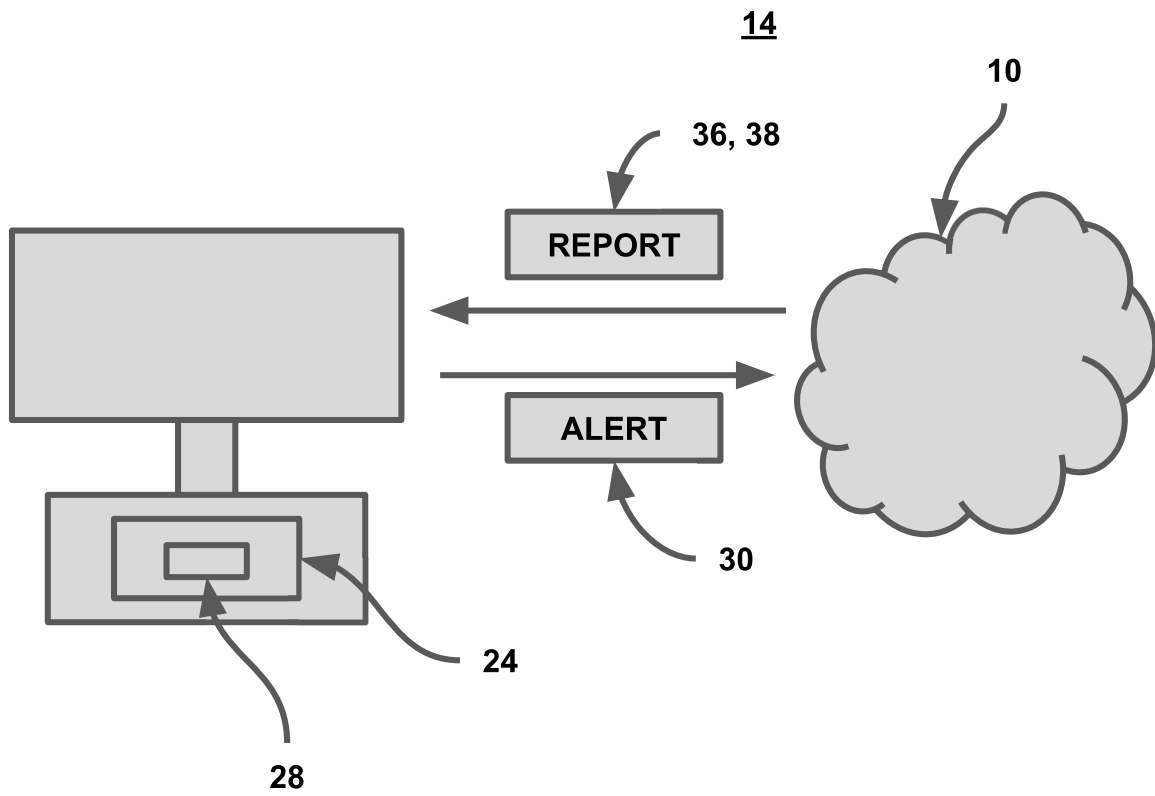


FIG. 5

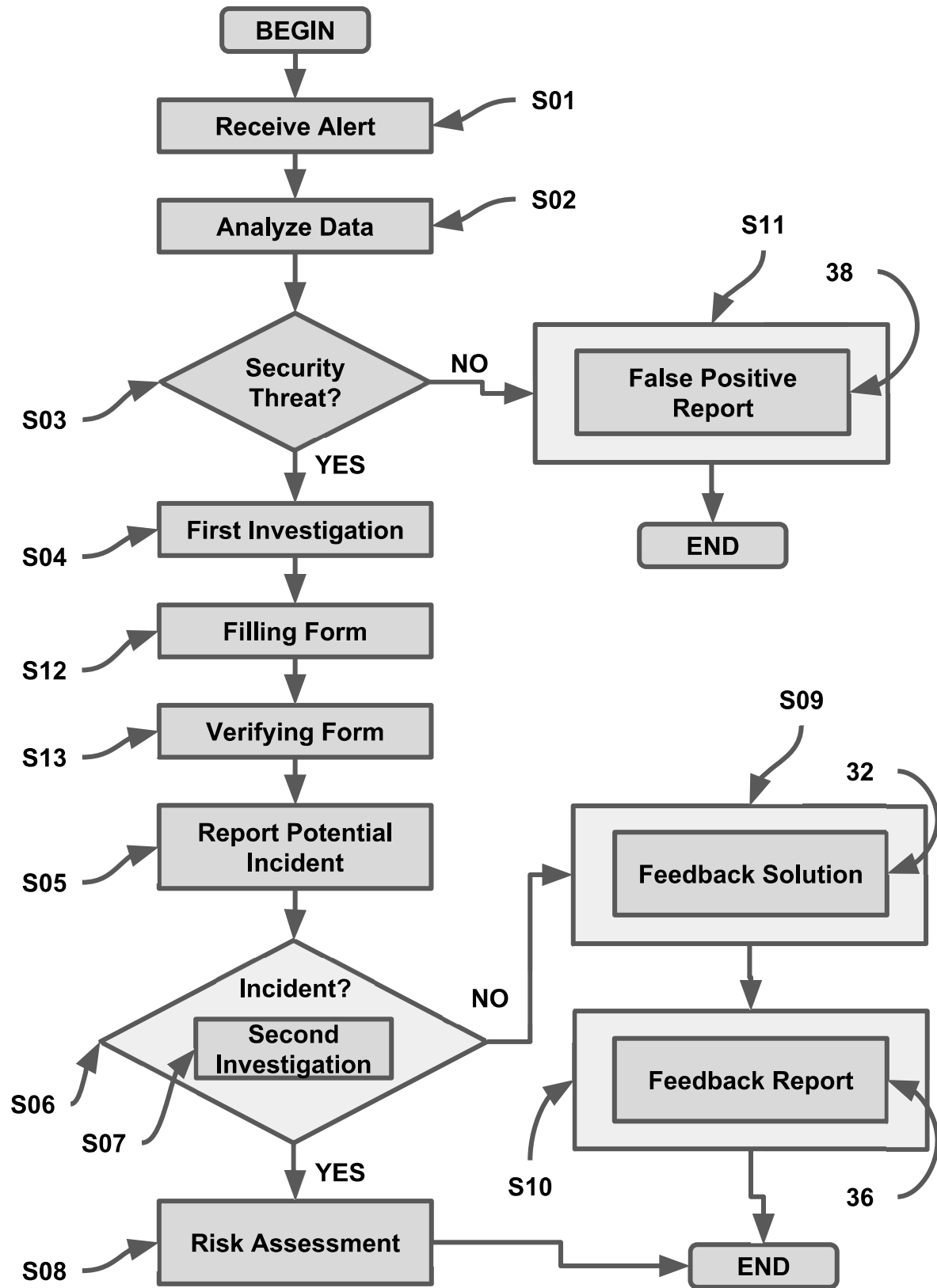


FIG. 6

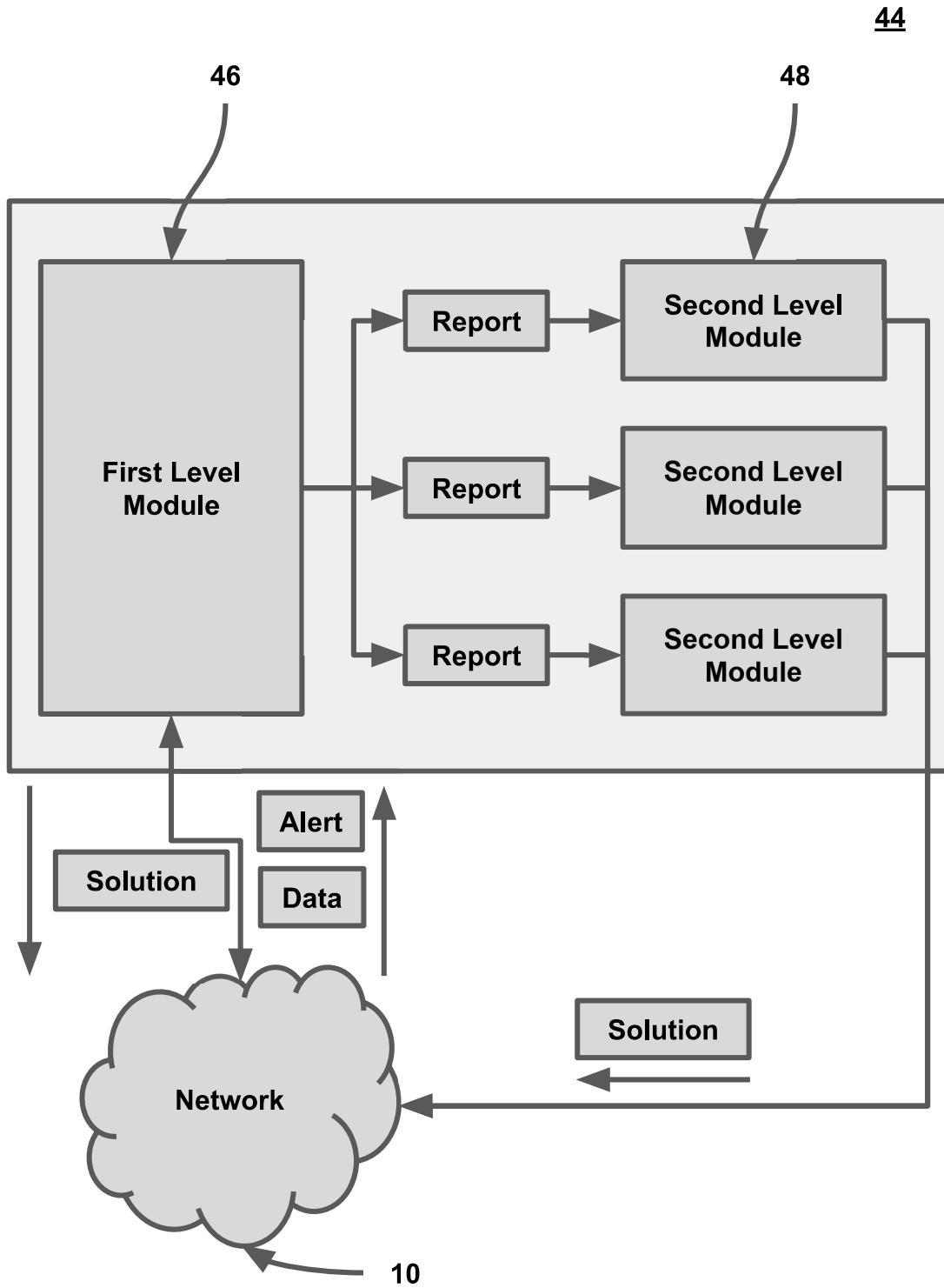


FIG. 7

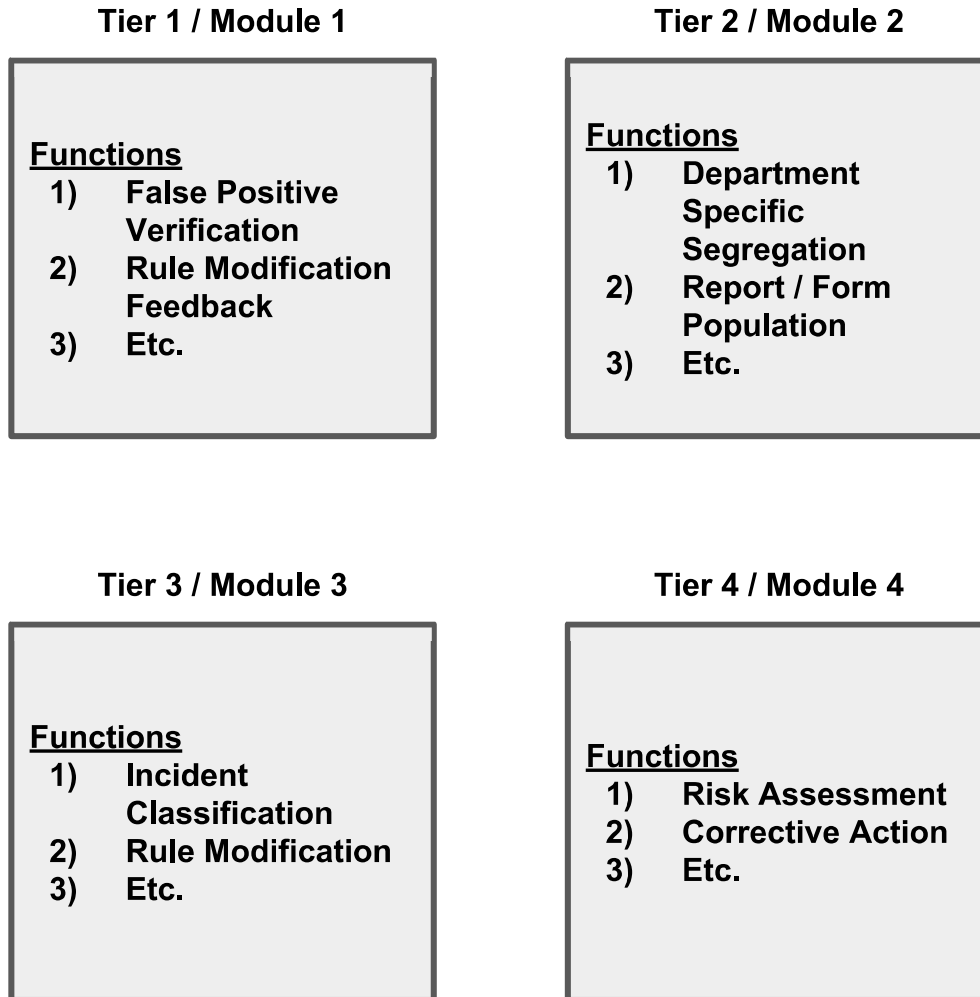


FIG. 8

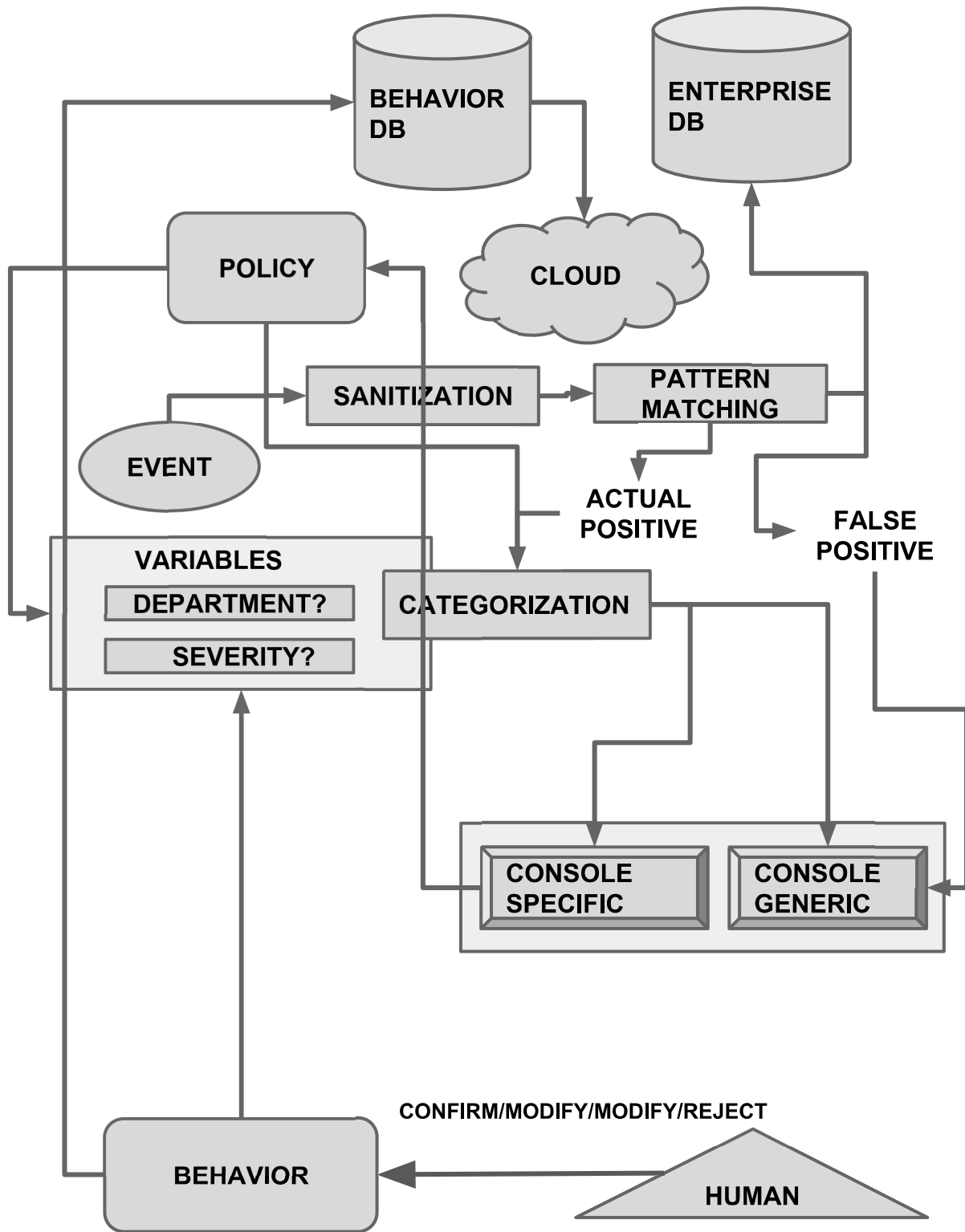


FIG. 9

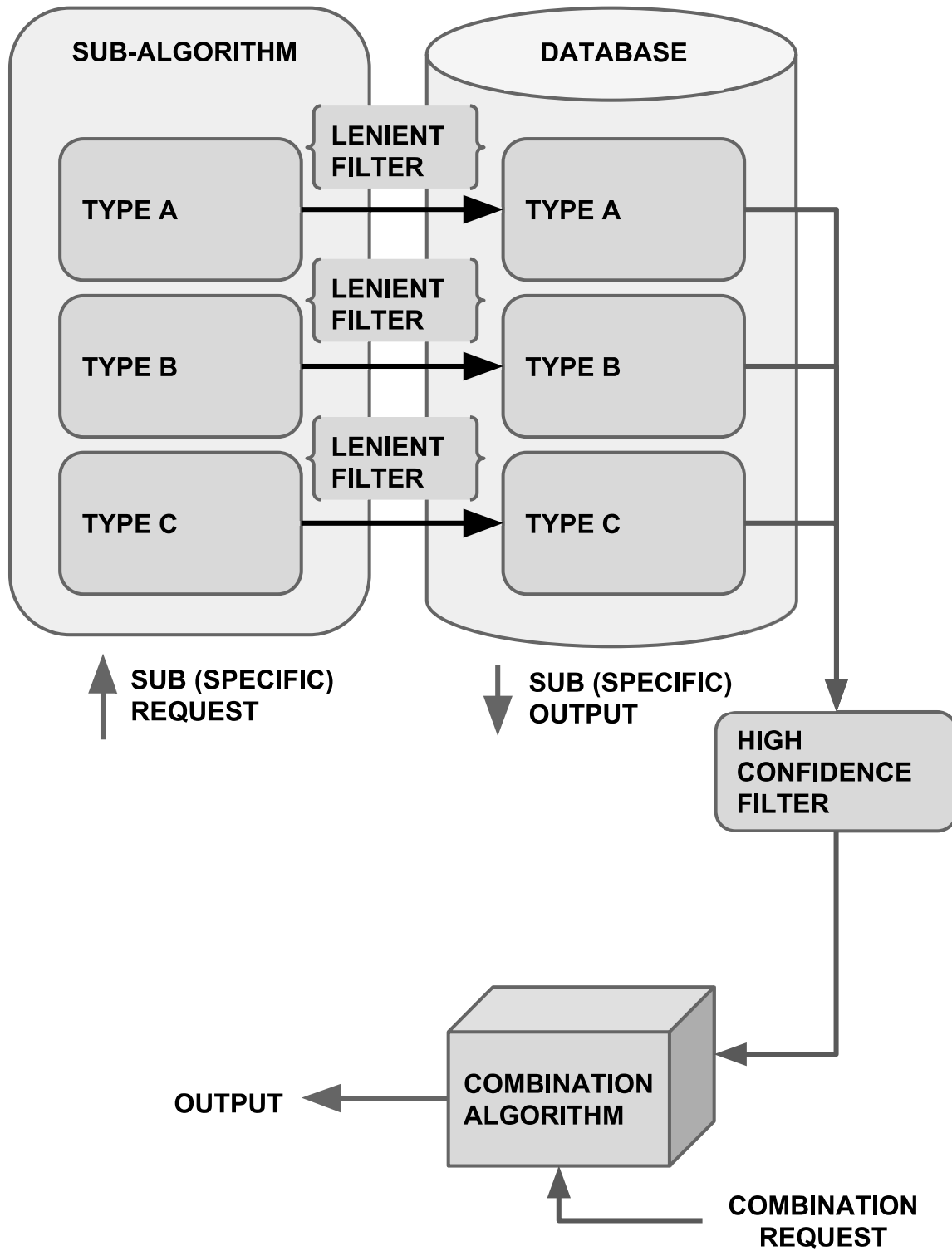


FIG. 10

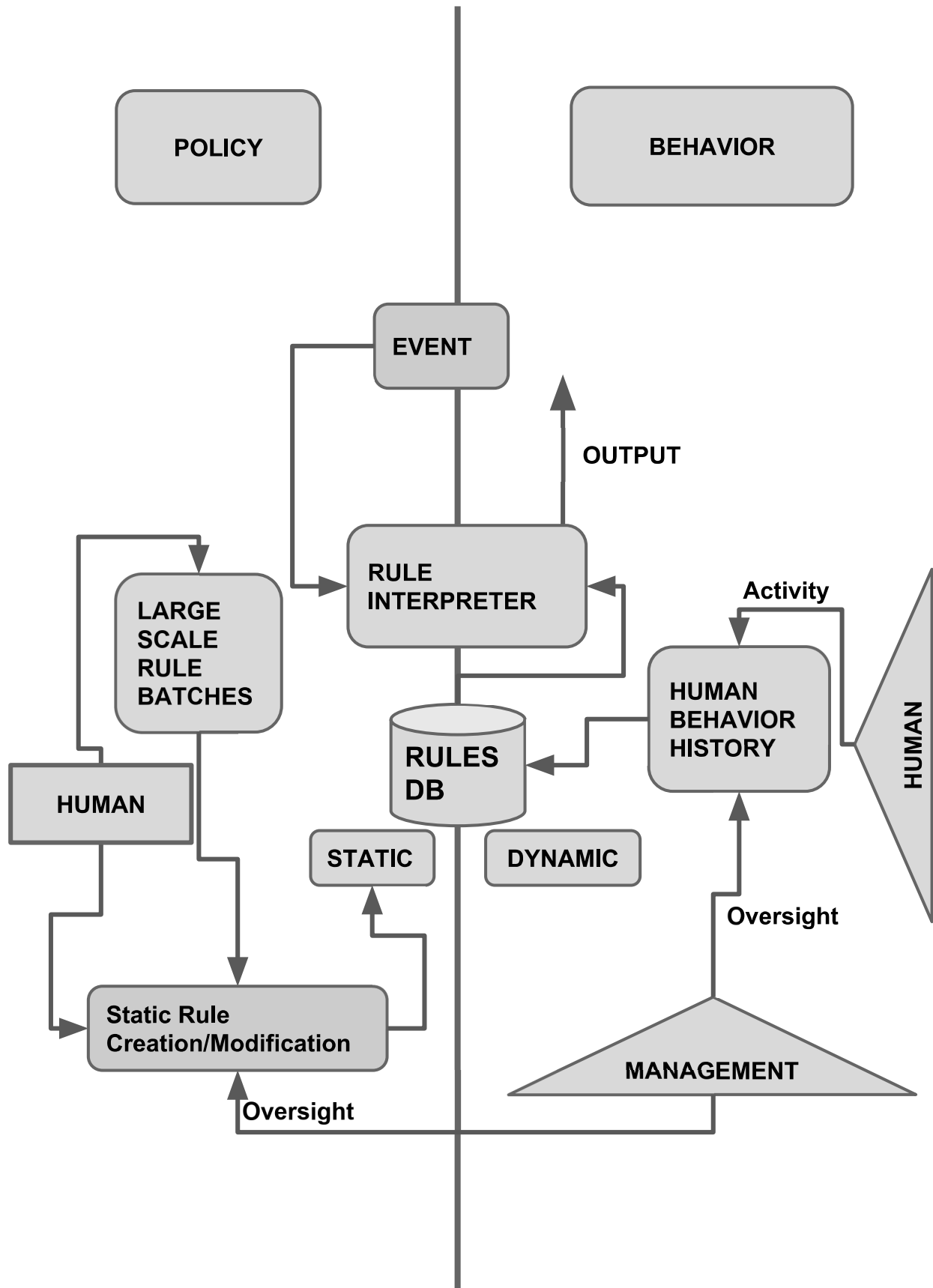


FIG. 11

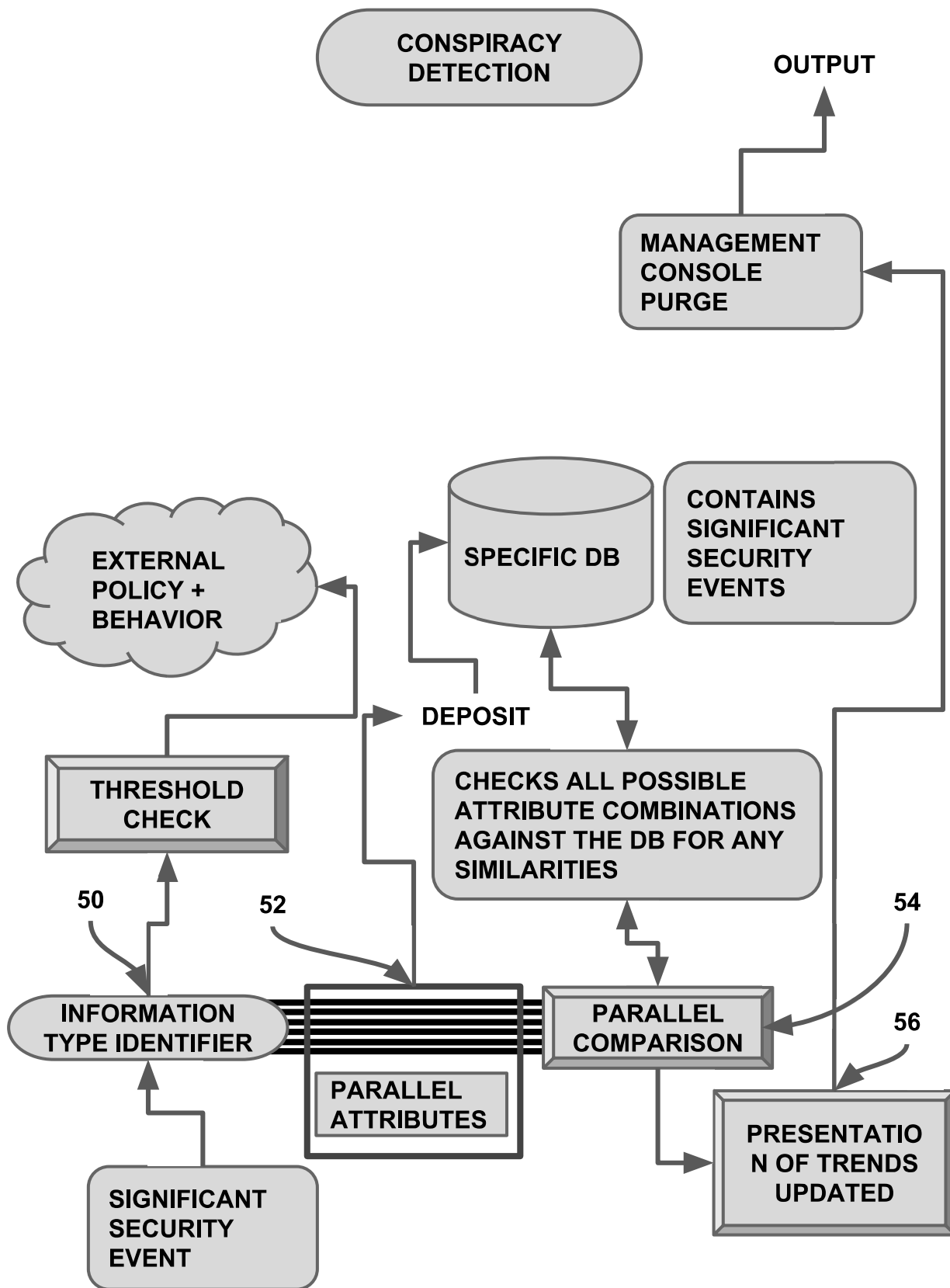


FIG. 12

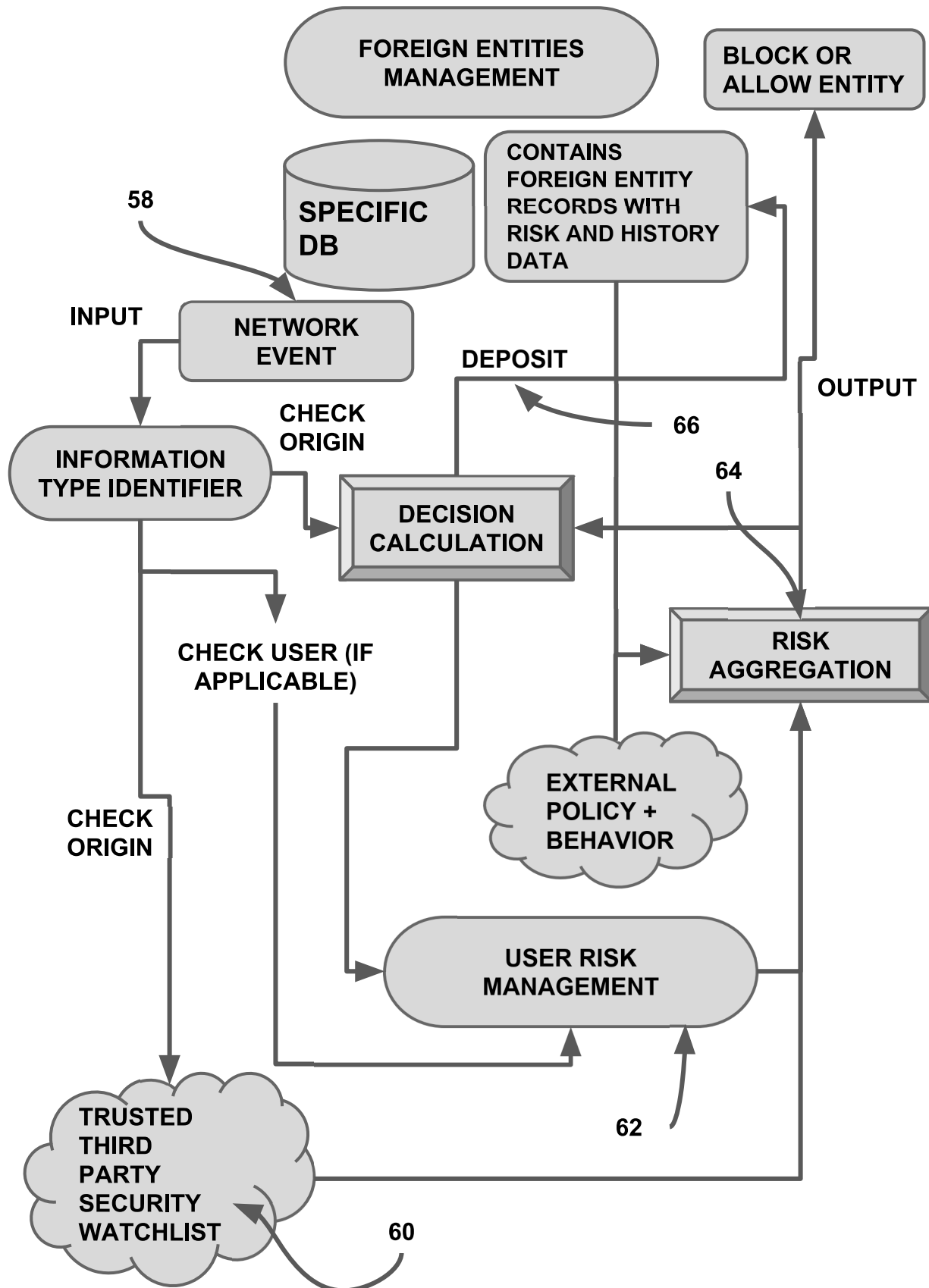


FIG. 13

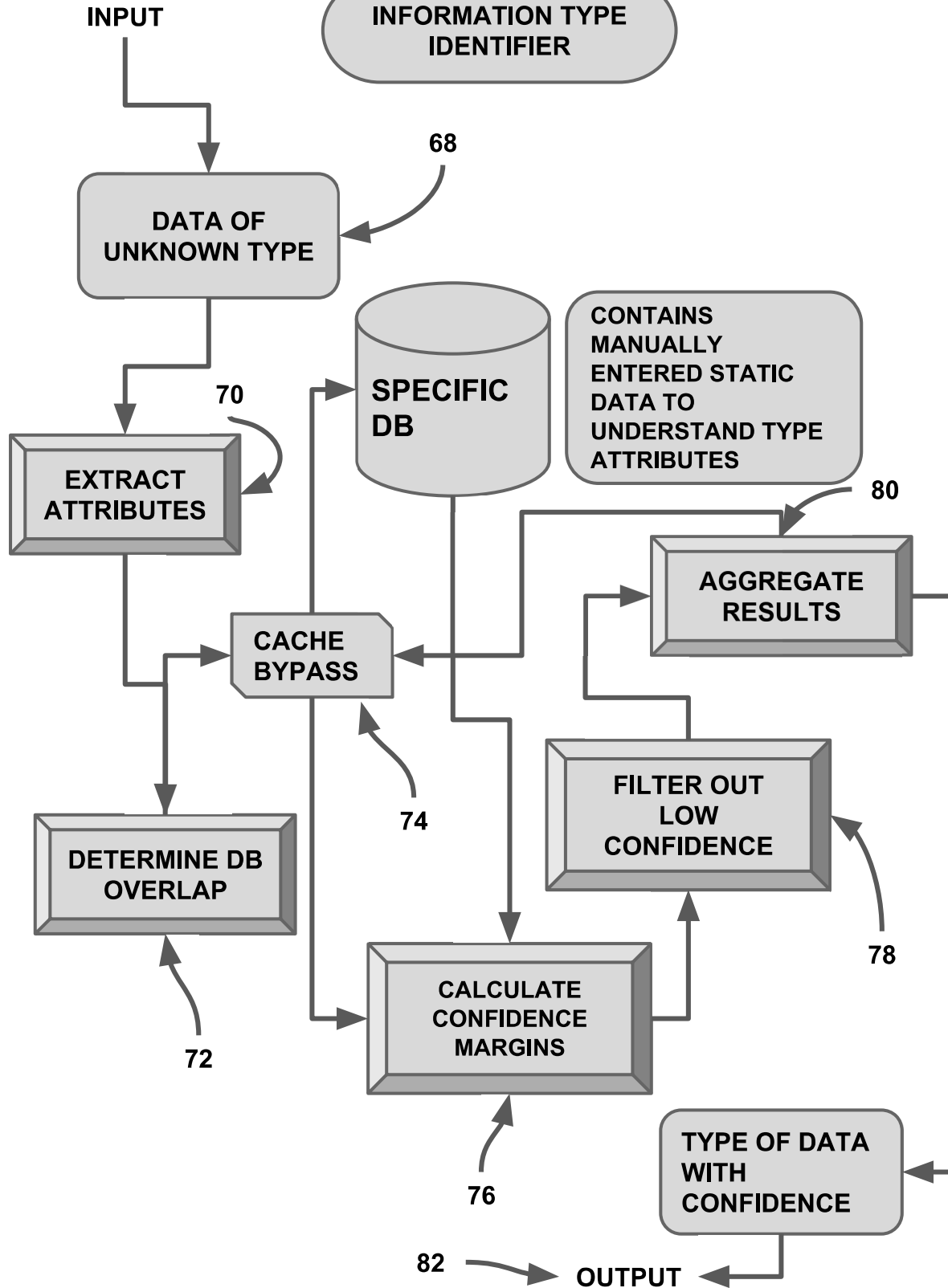


FIG. 15

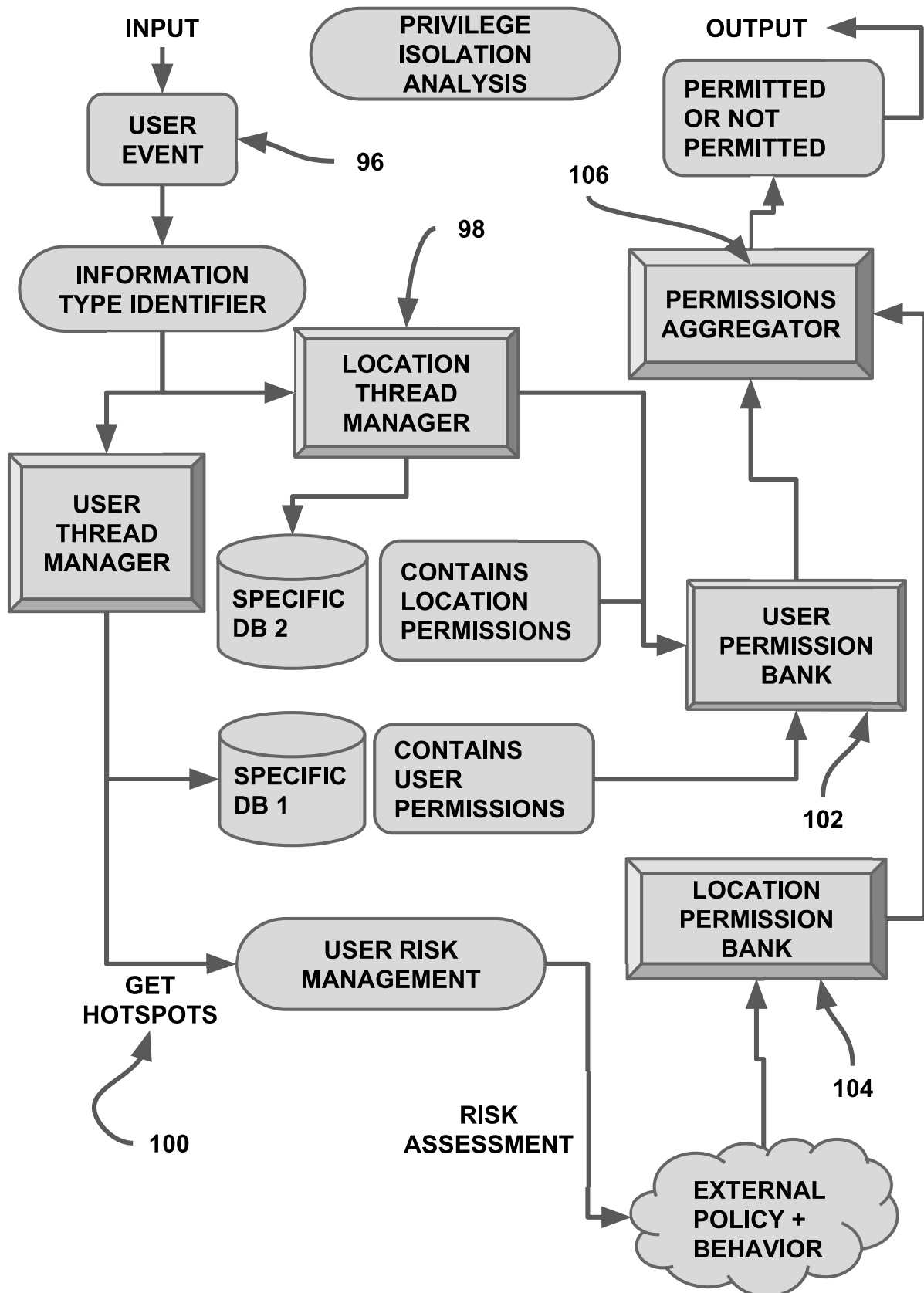


FIG. 16



FIG. 17

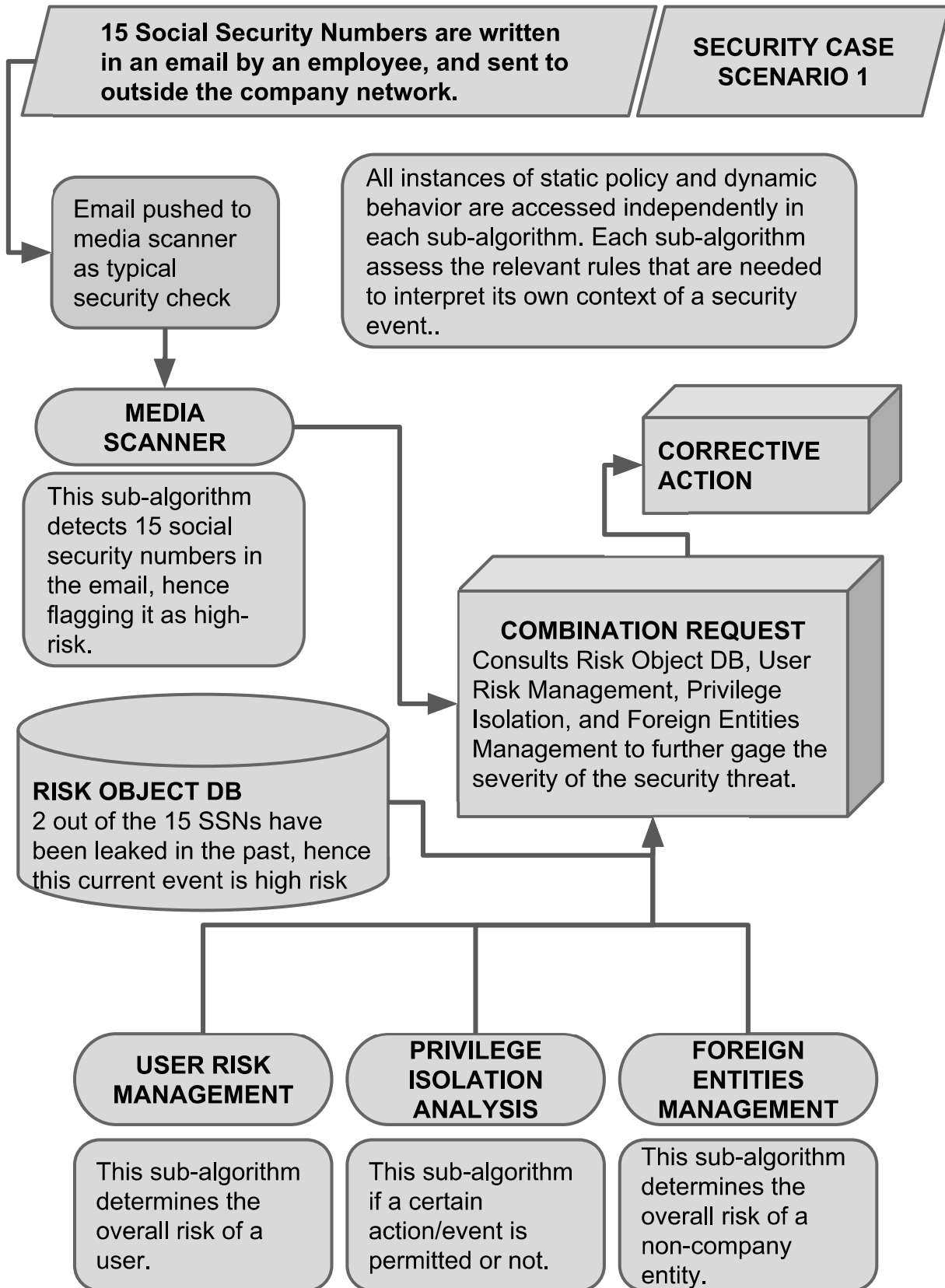


FIG. 18

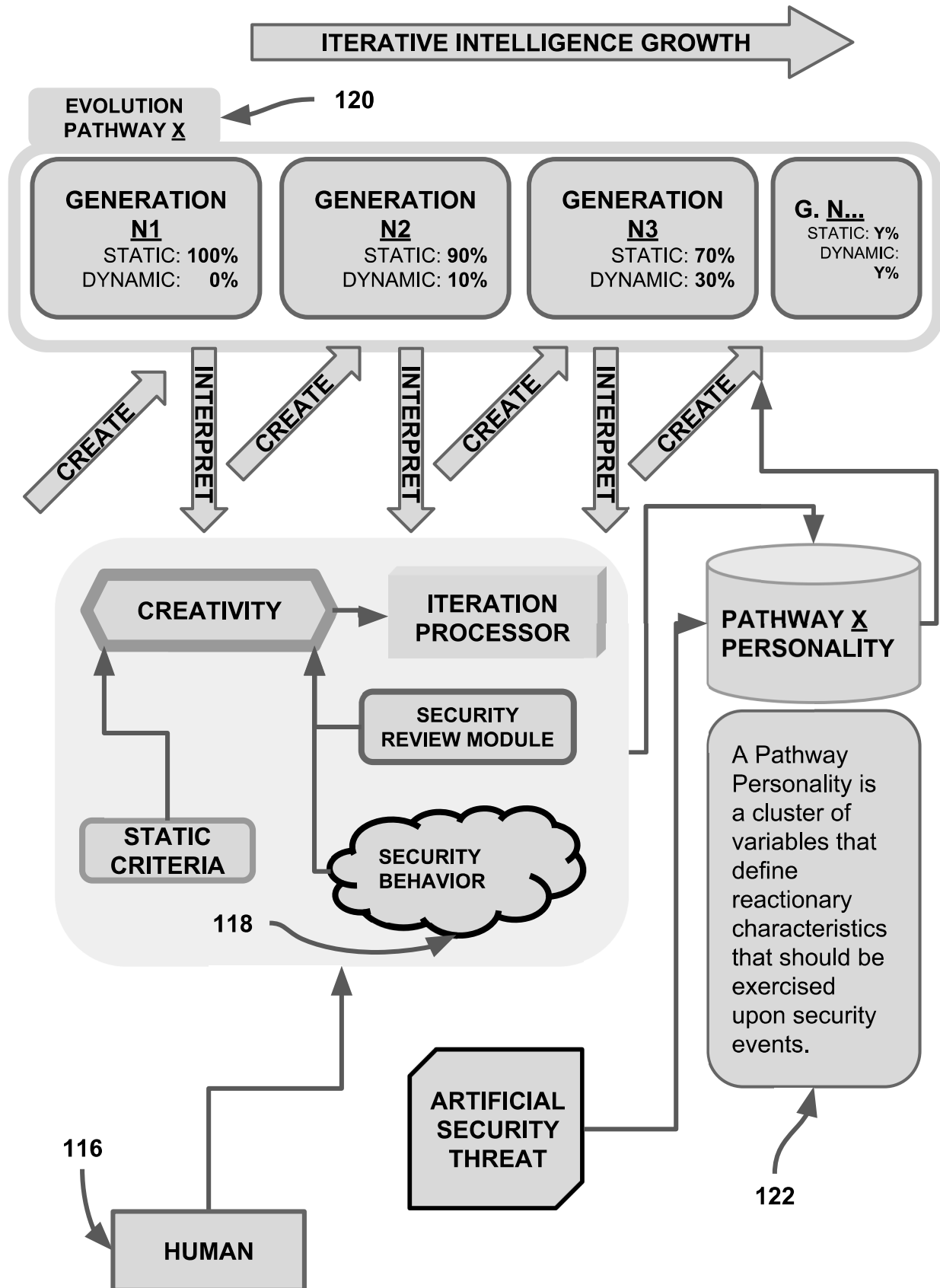


FIG. 19

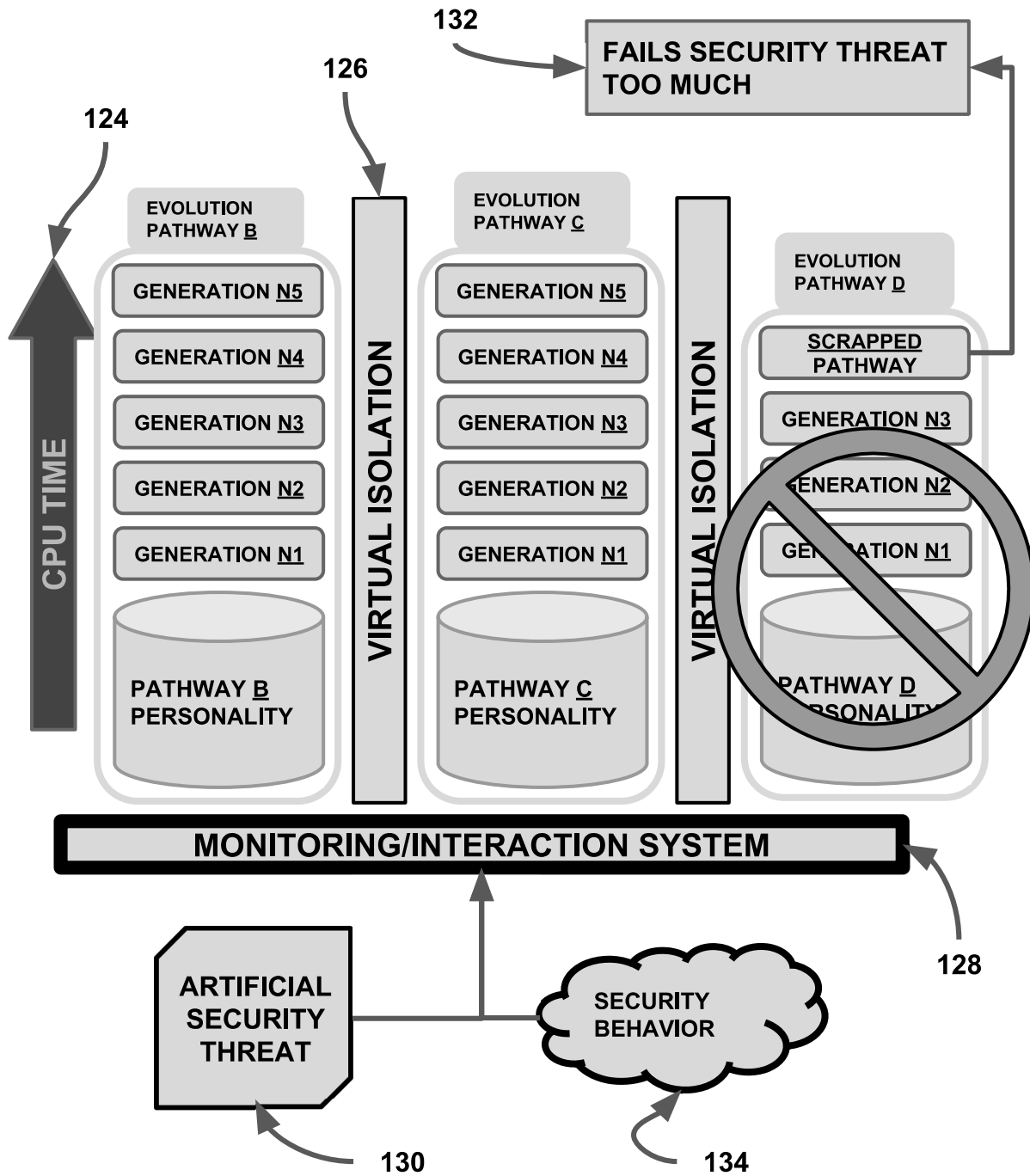


FIG. 20

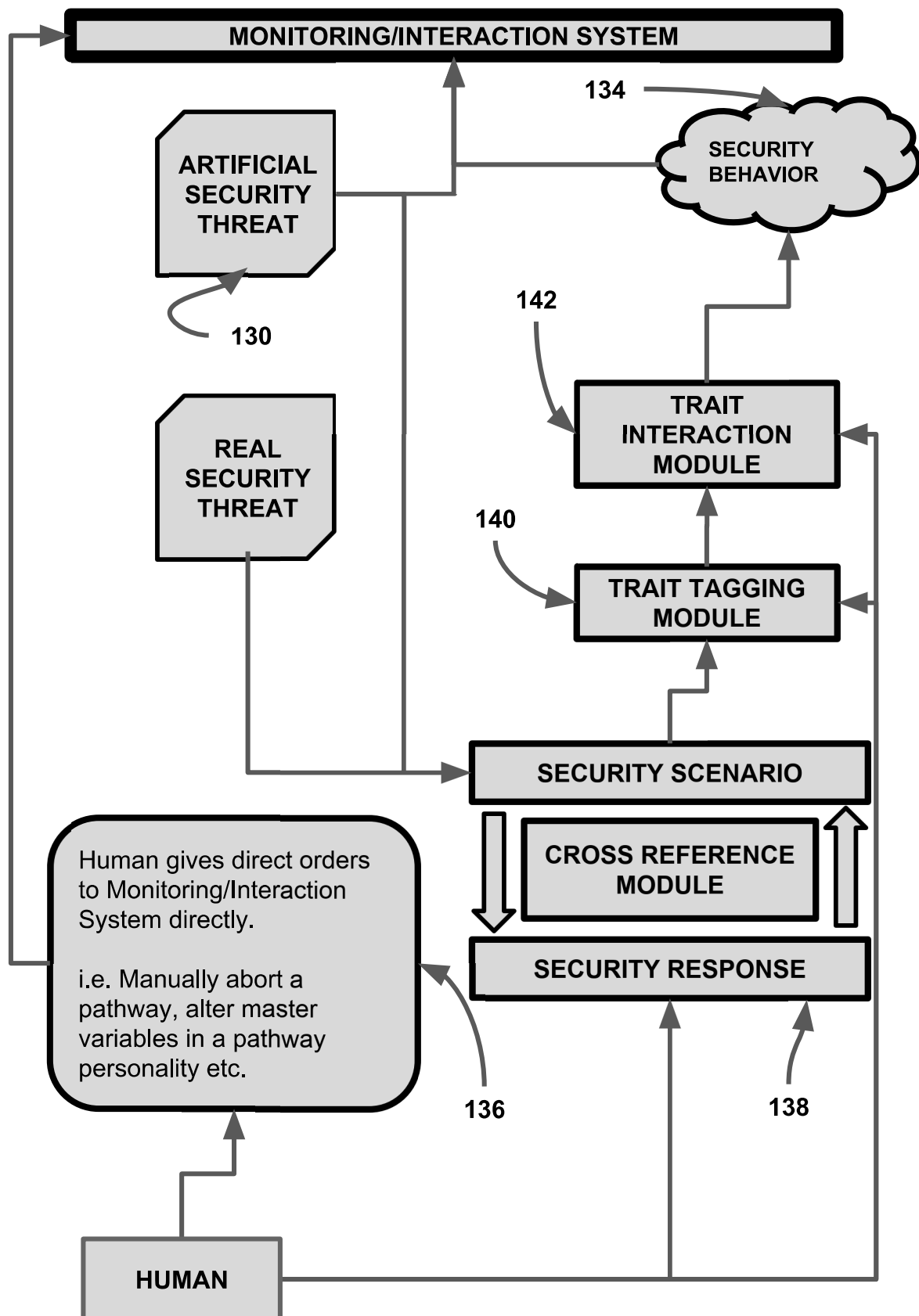


FIG. 21

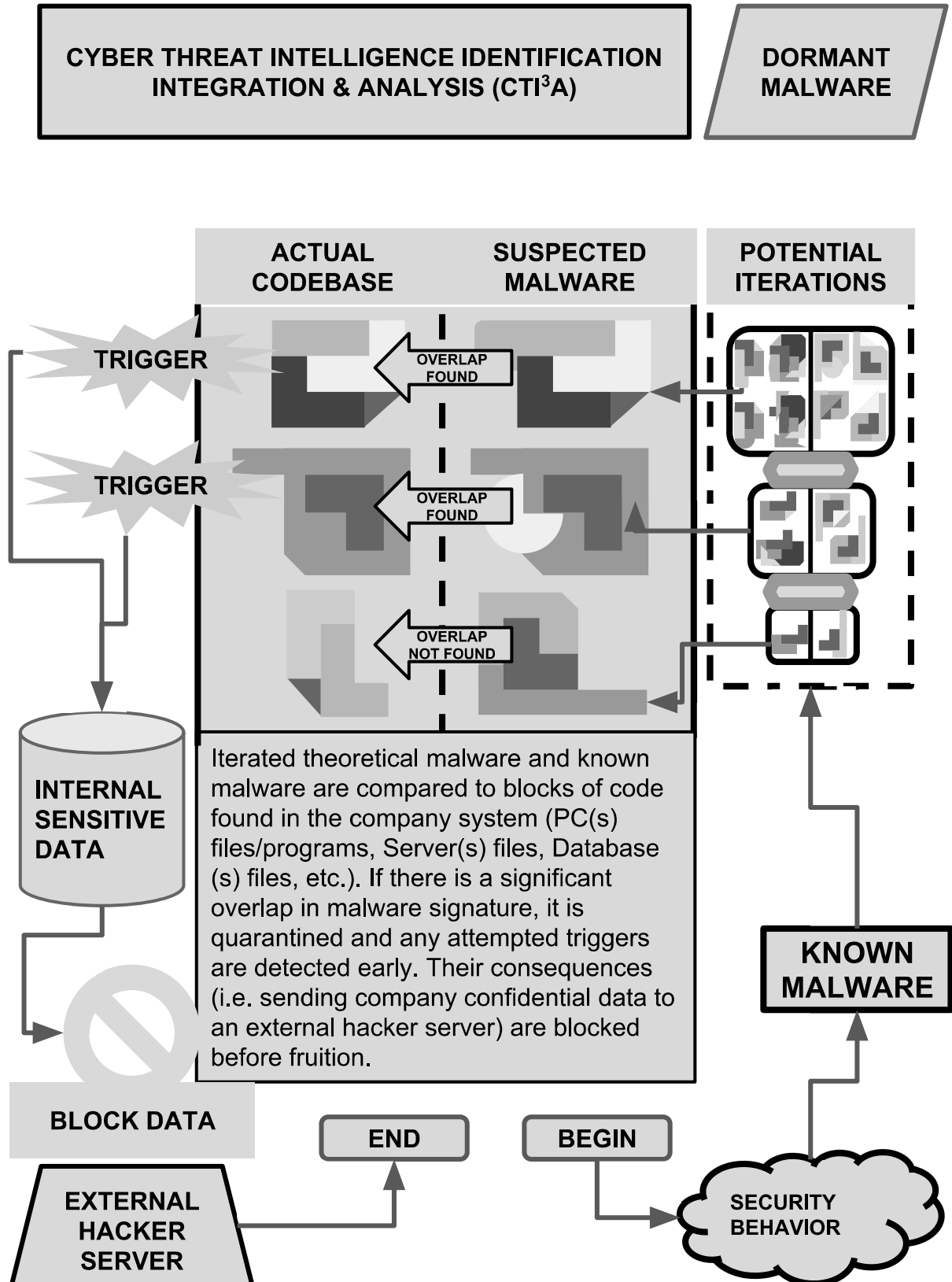


FIG. 22

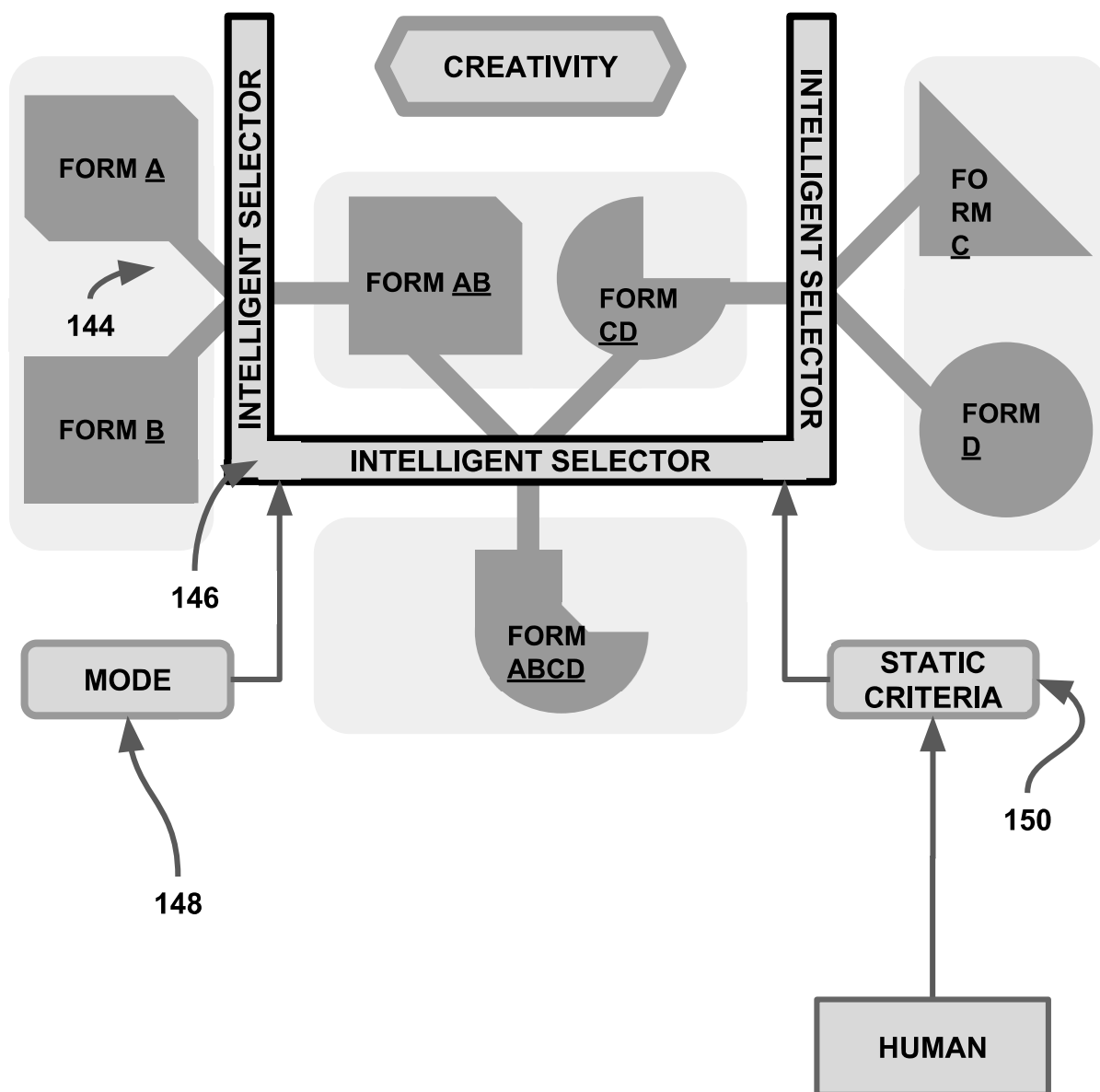


FIG. 23

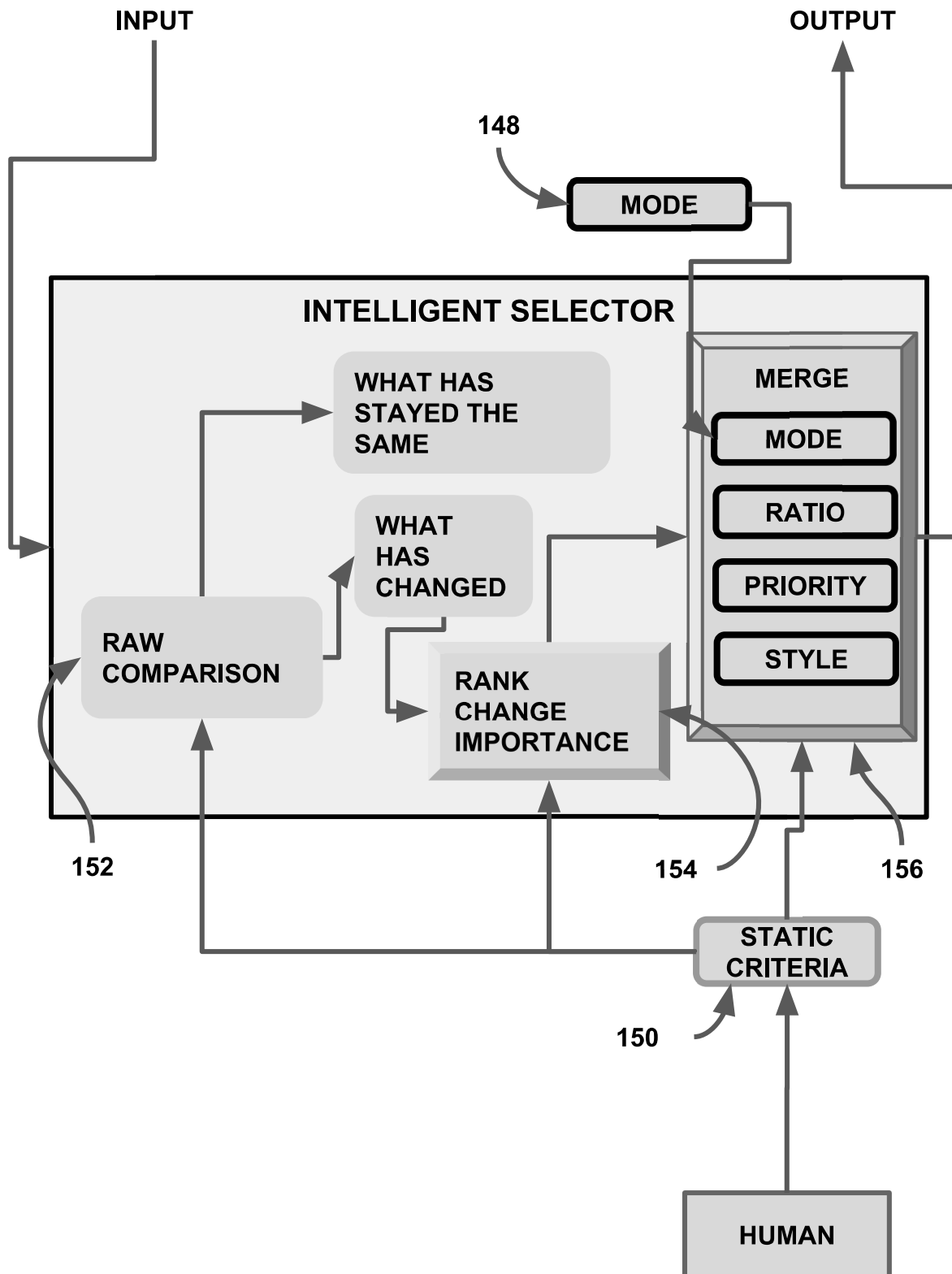


FIG. 24

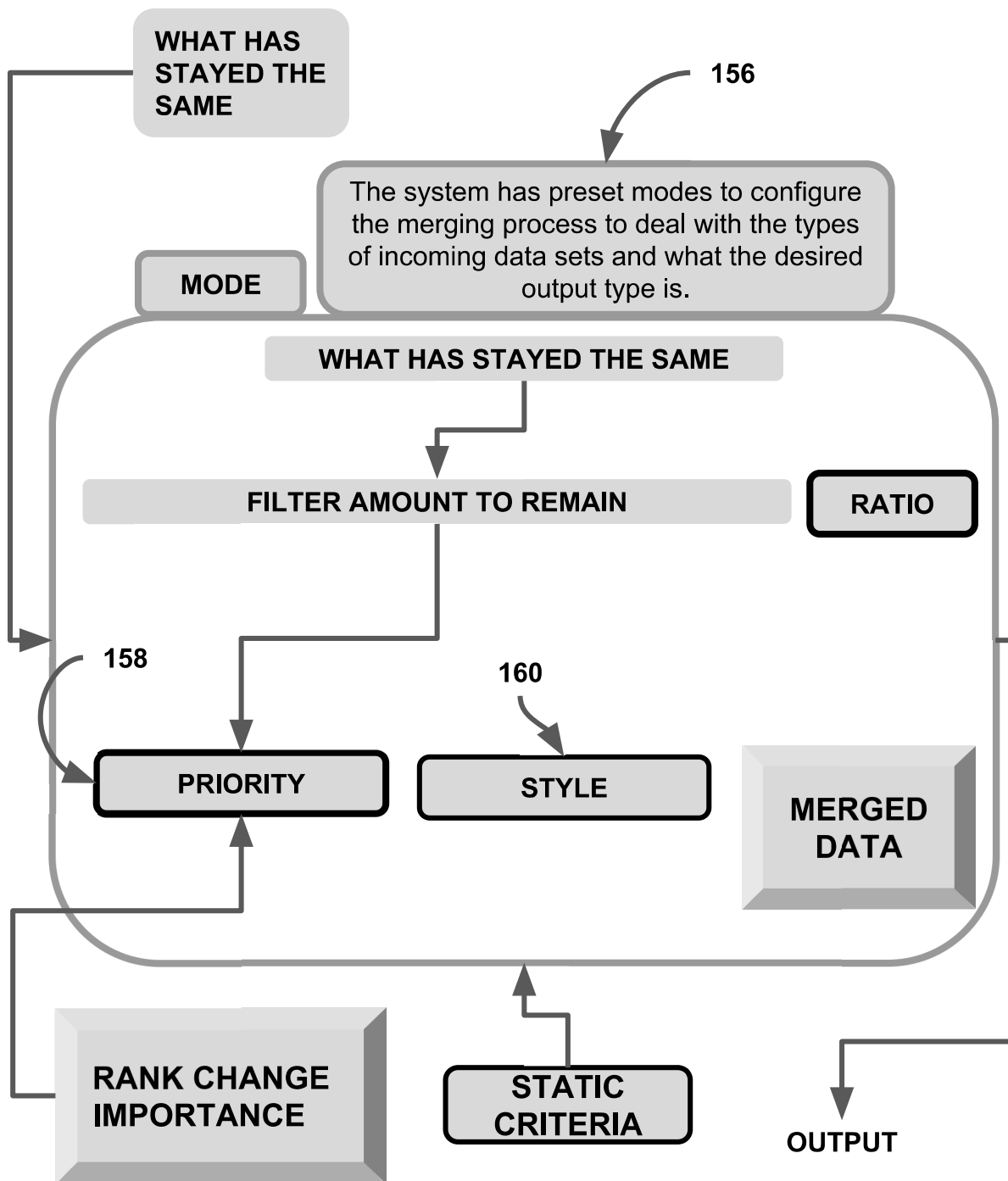


FIG. 25

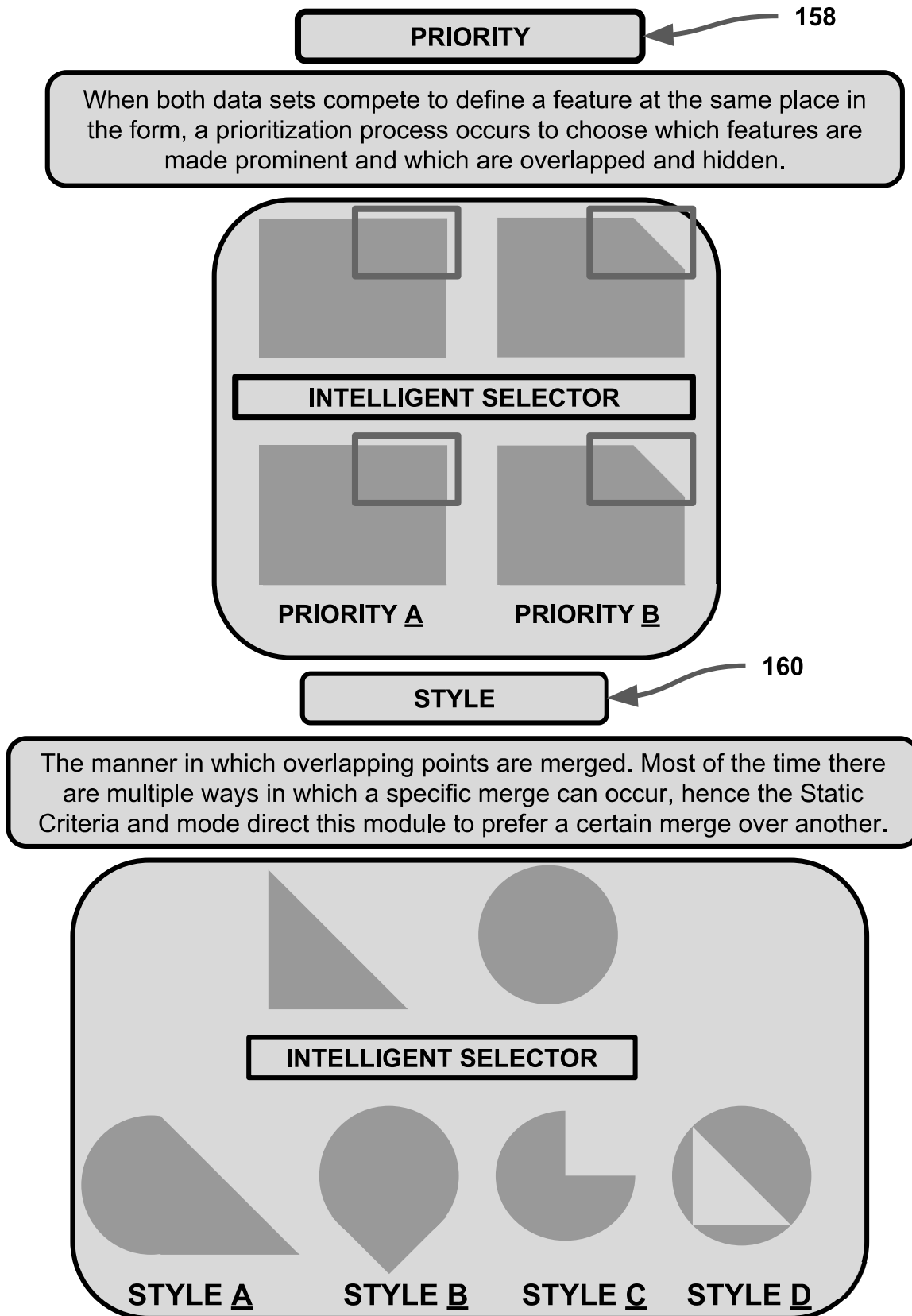


FIG. 26

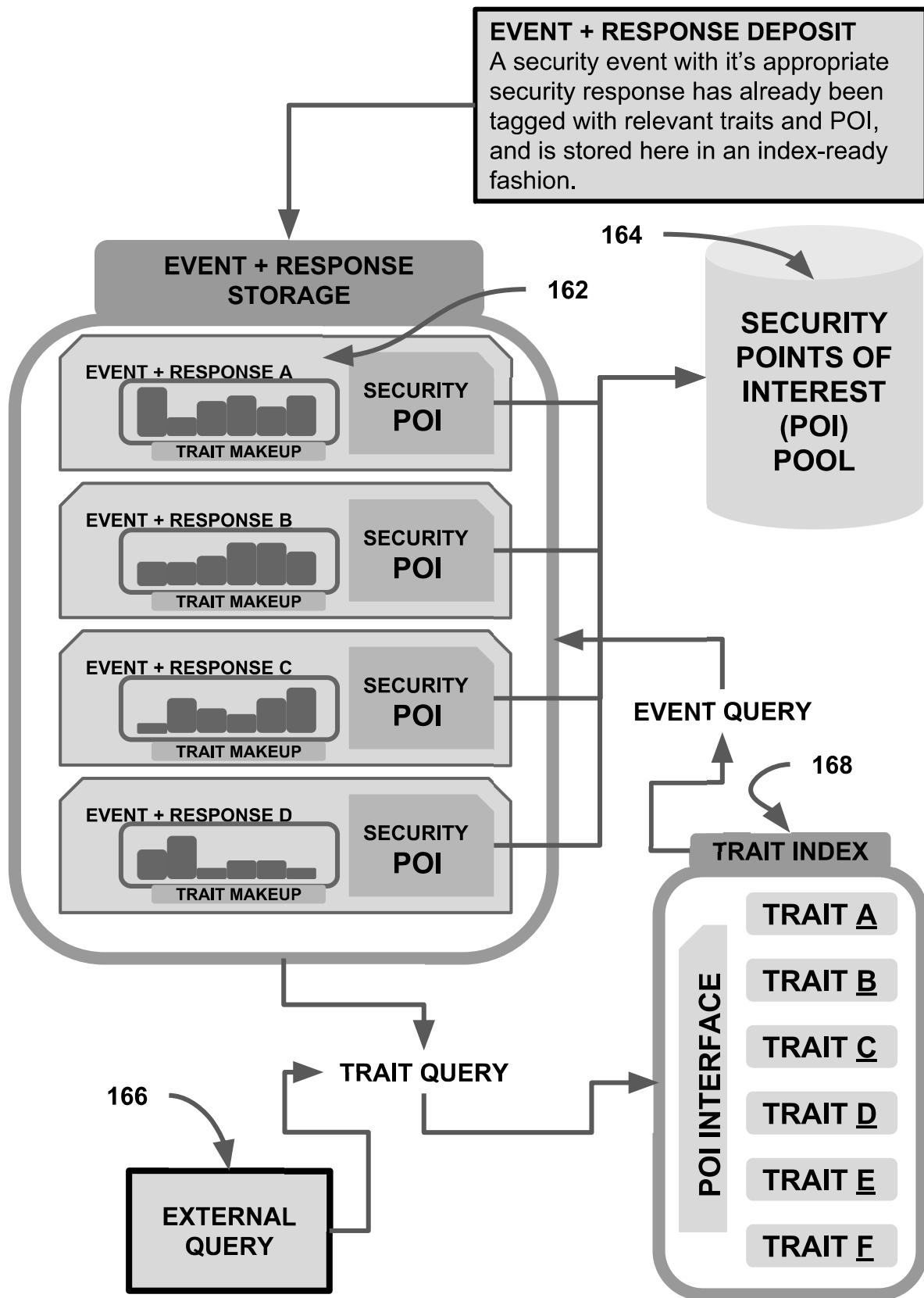


FIG. 27

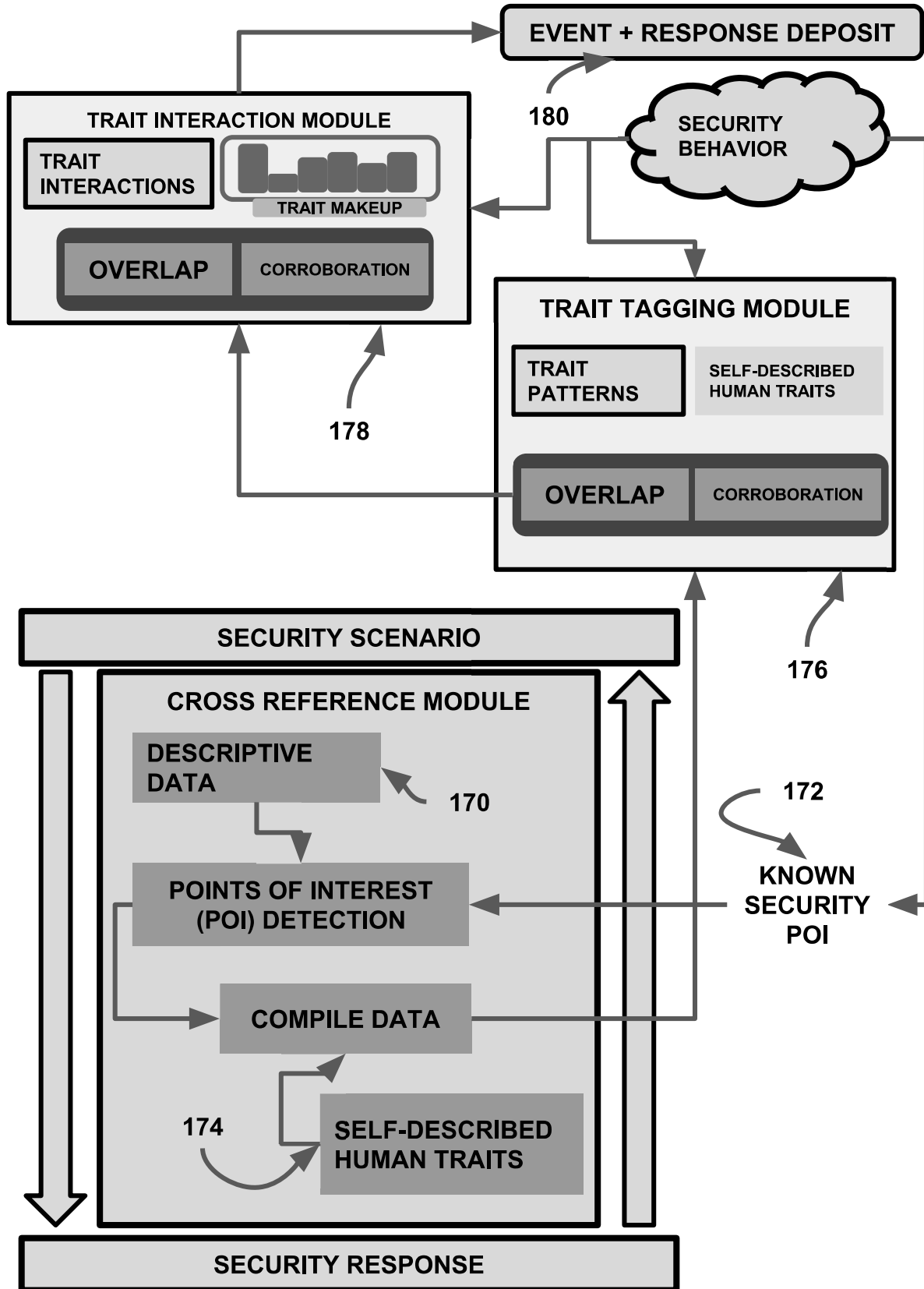


FIG. 28

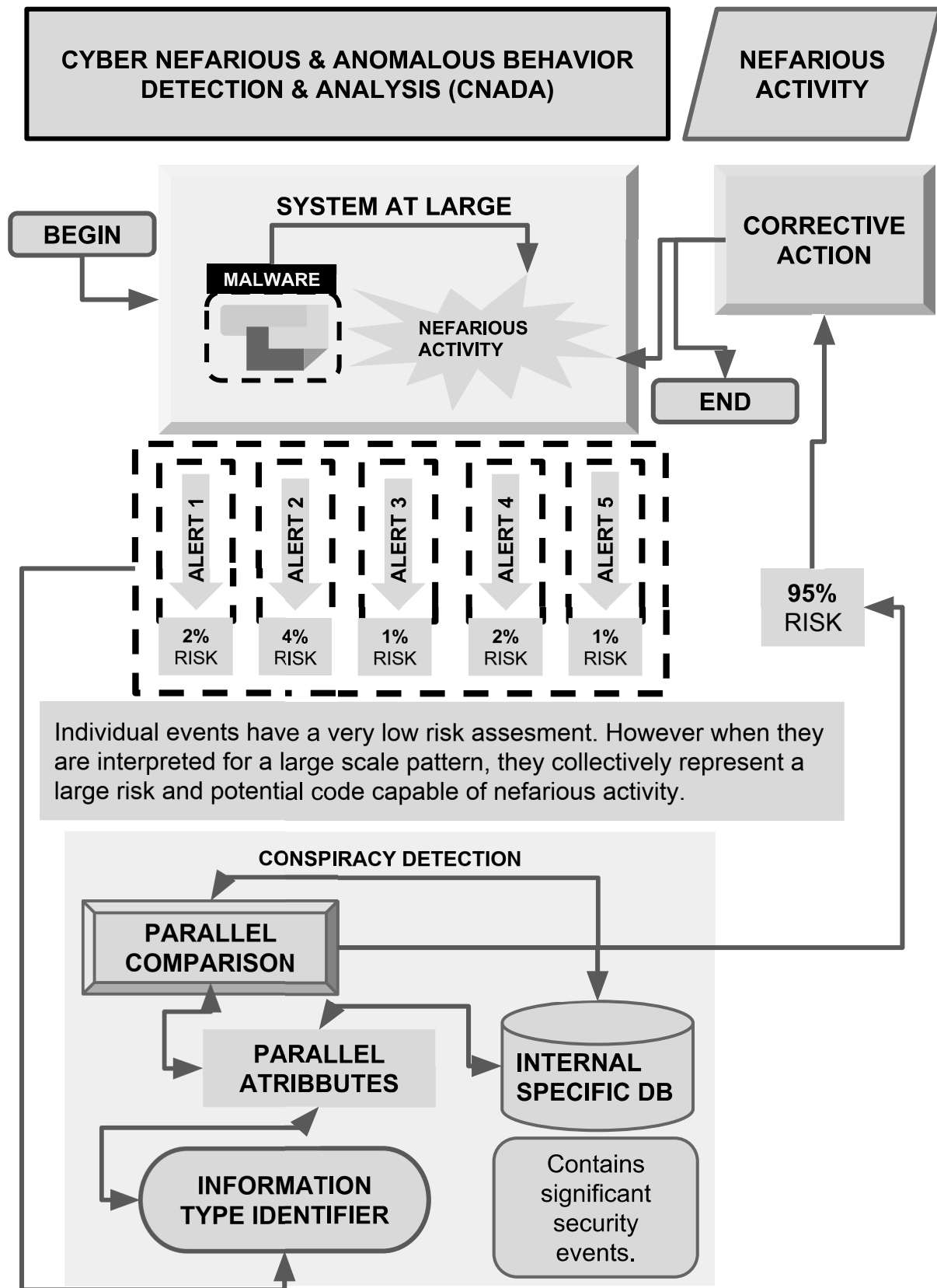


FIG. 29

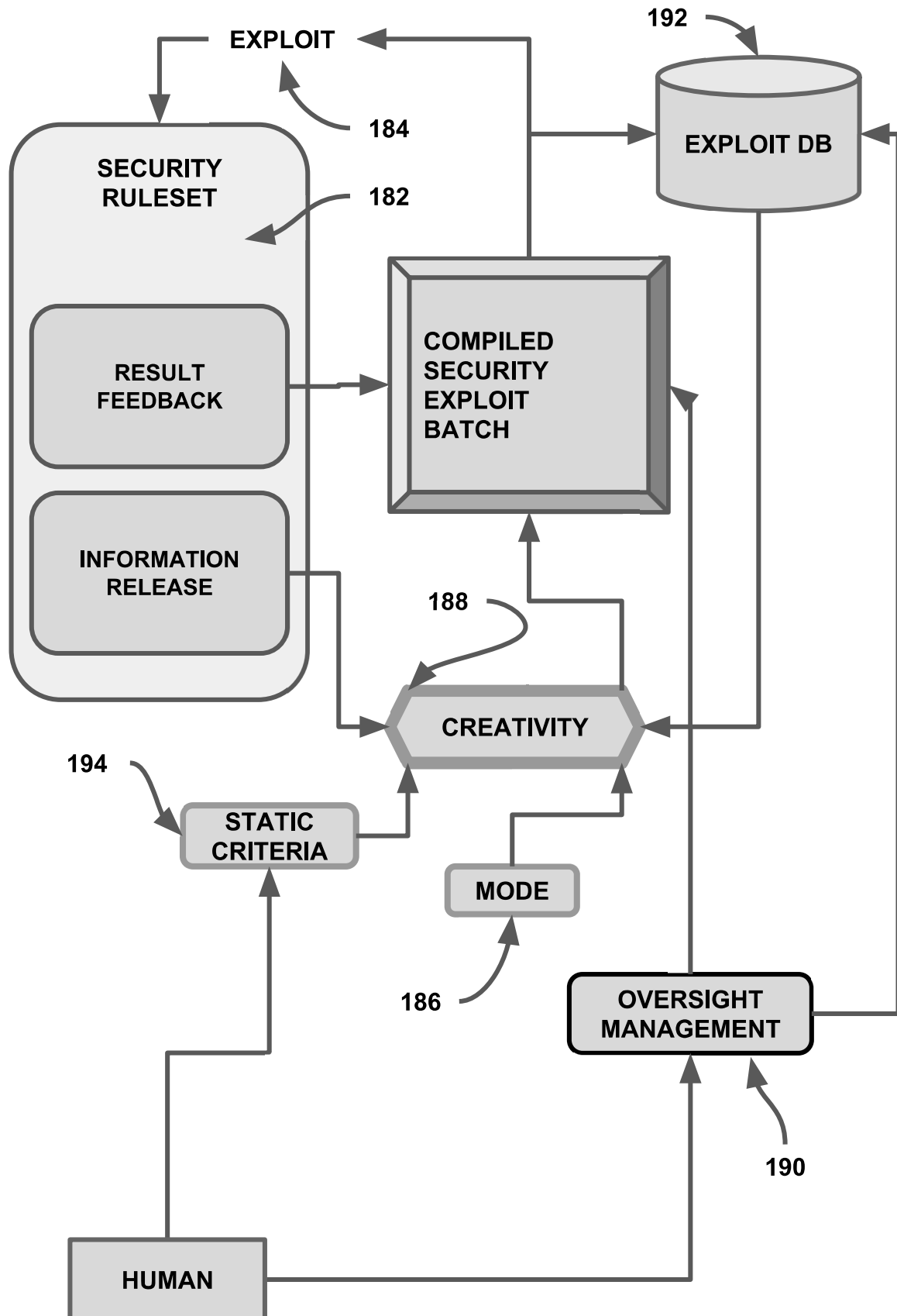


FIG. 30

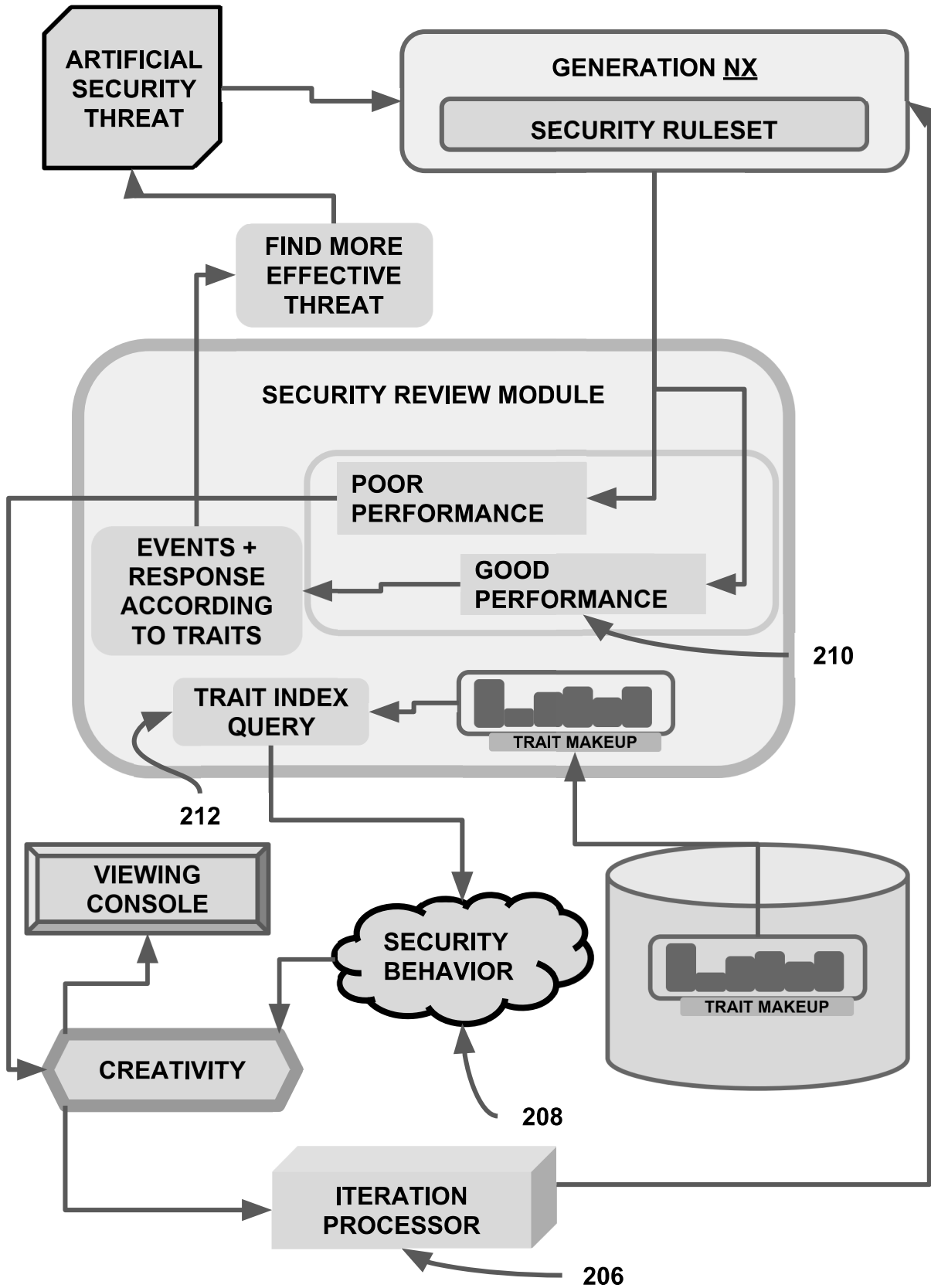


FIG. 32

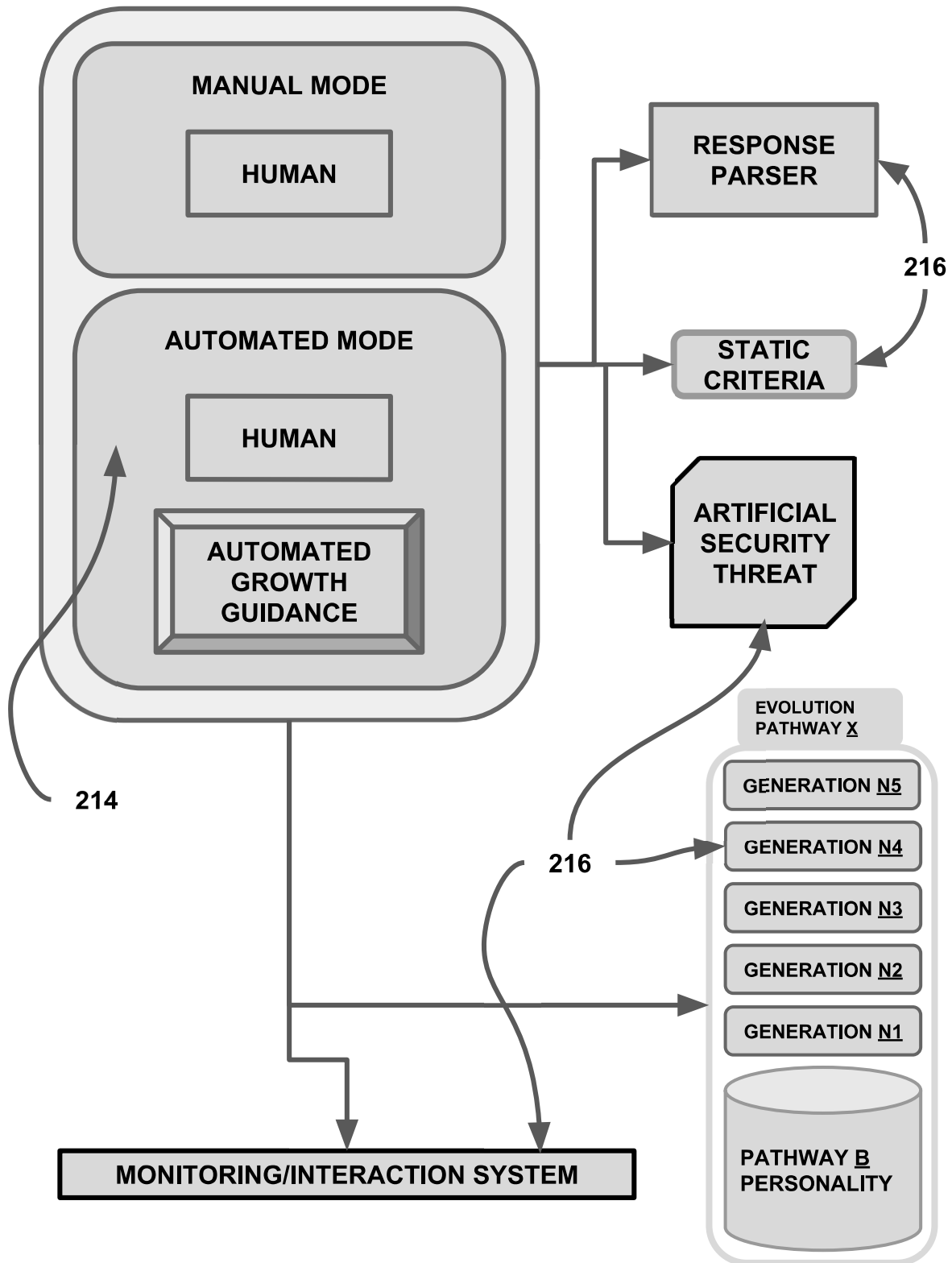


FIG. 33

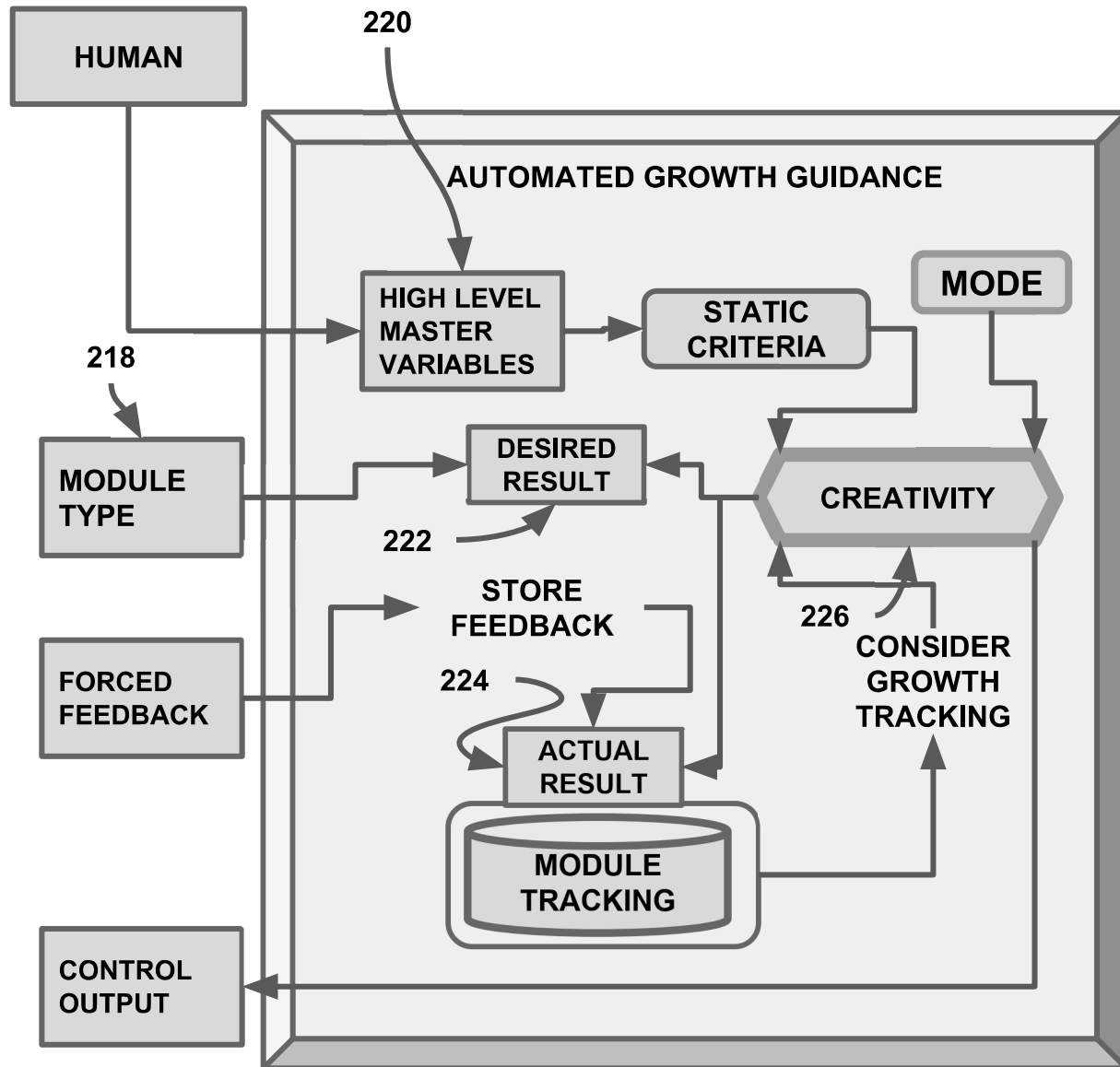


FIG. 34



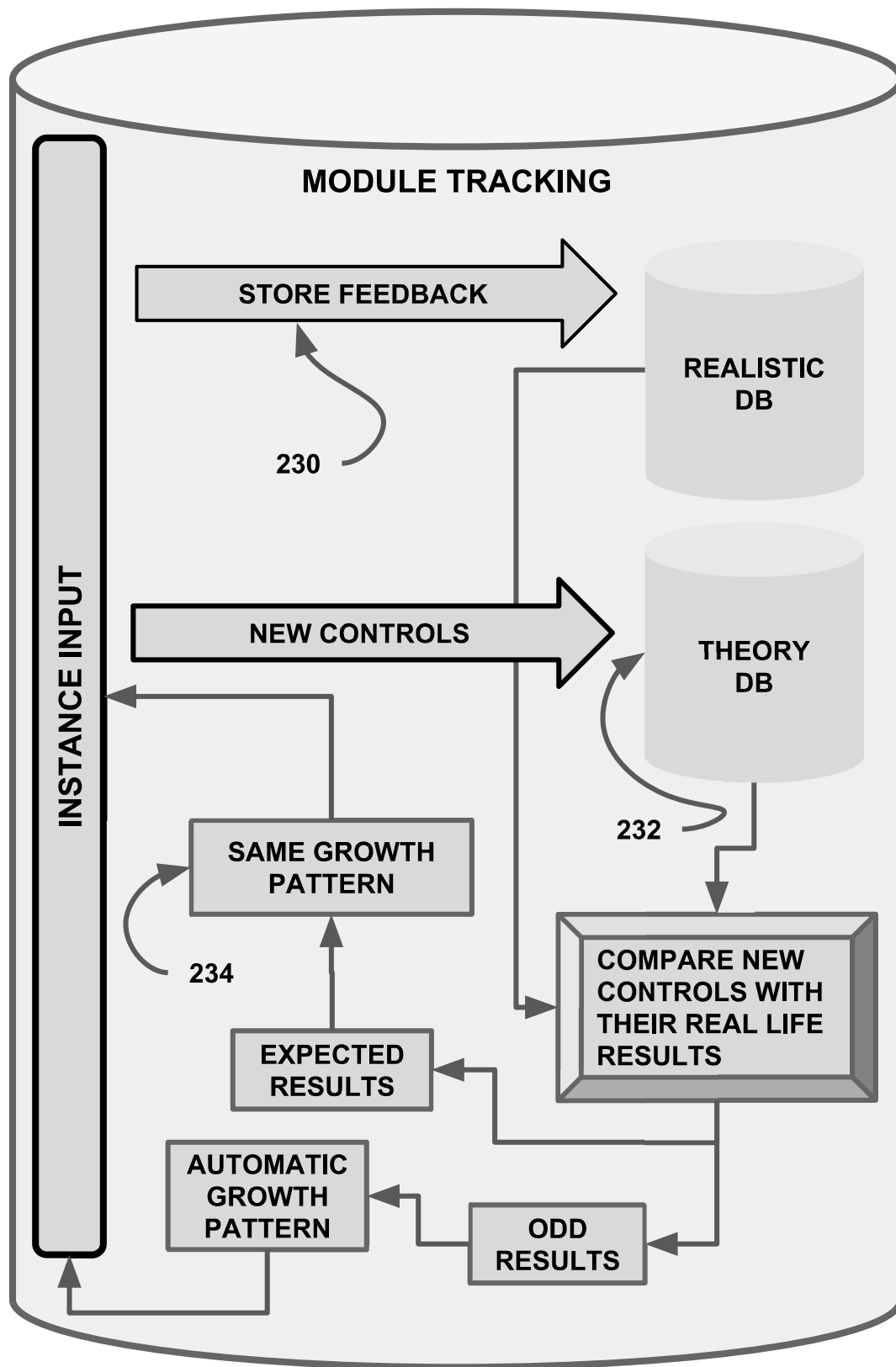


FIG. 36

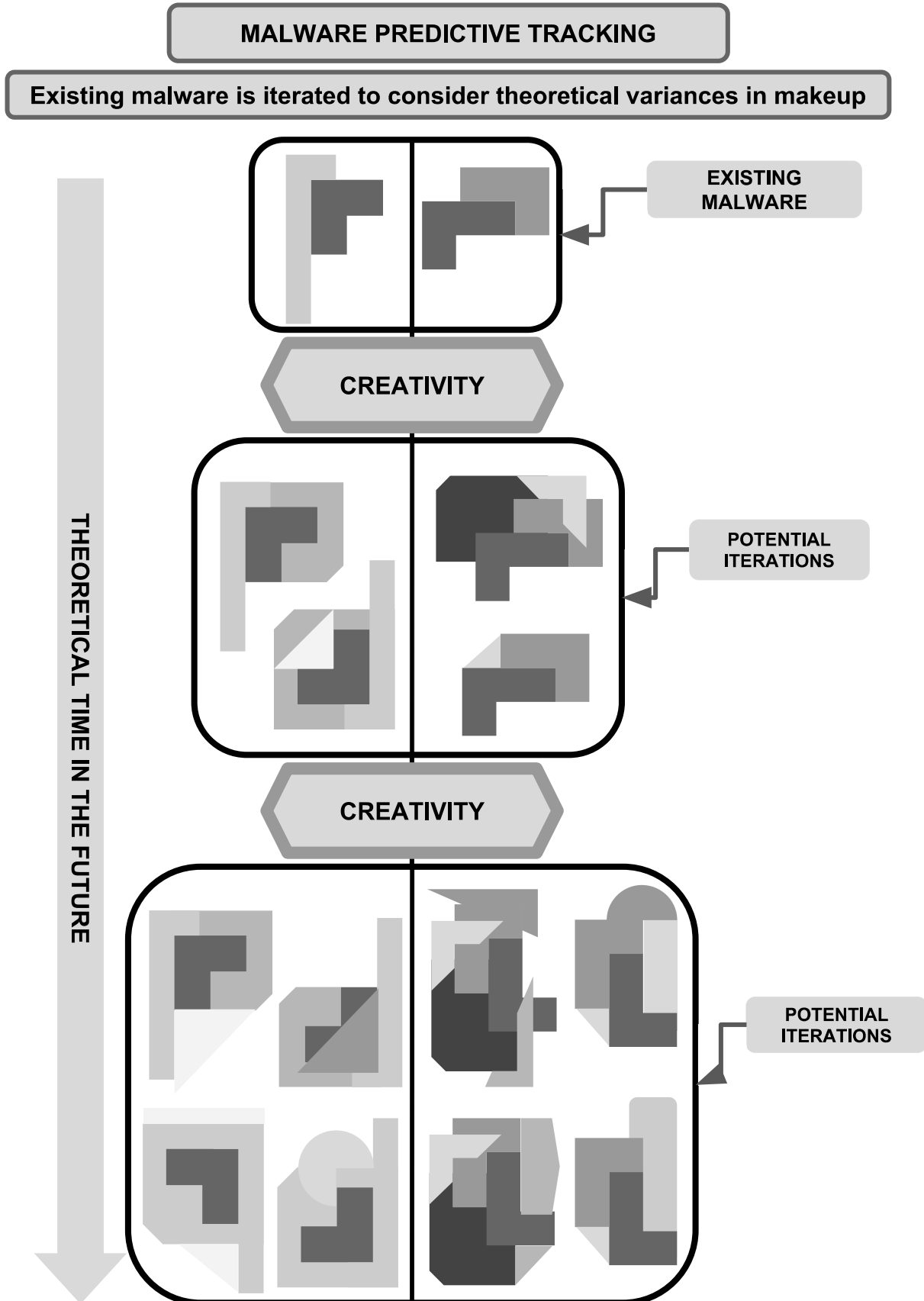


FIG. 37

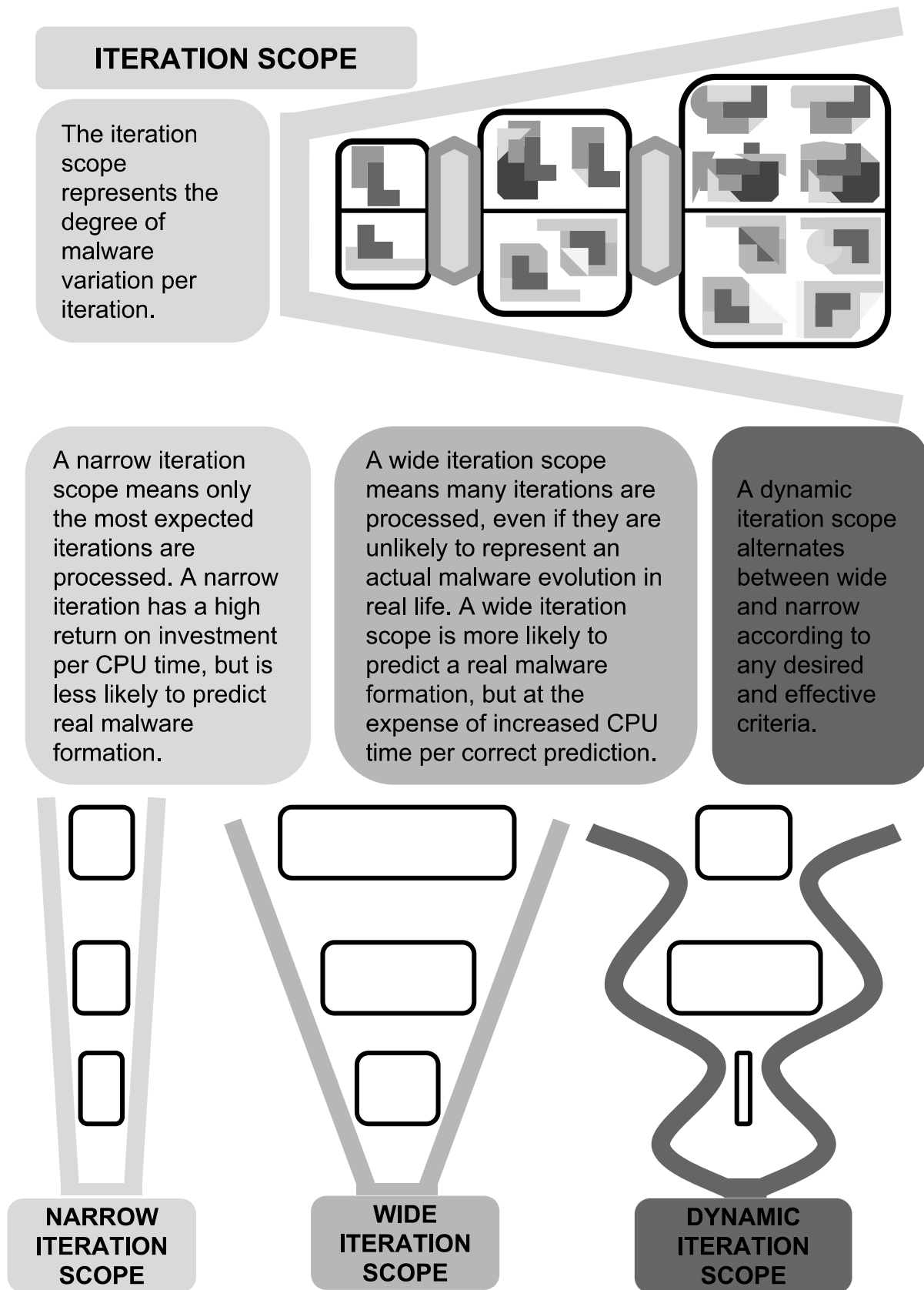


FIG. 38

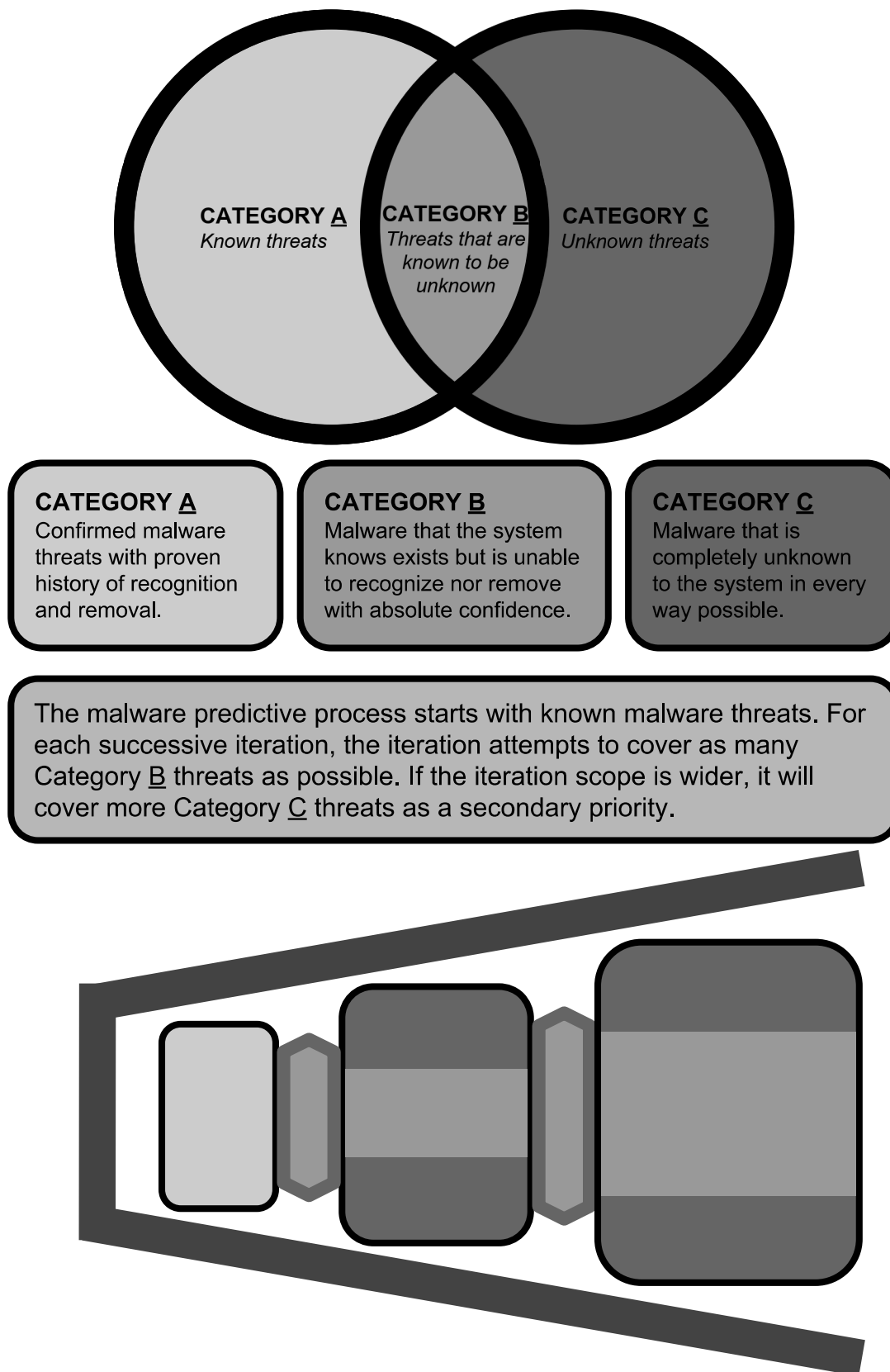


FIG. 39

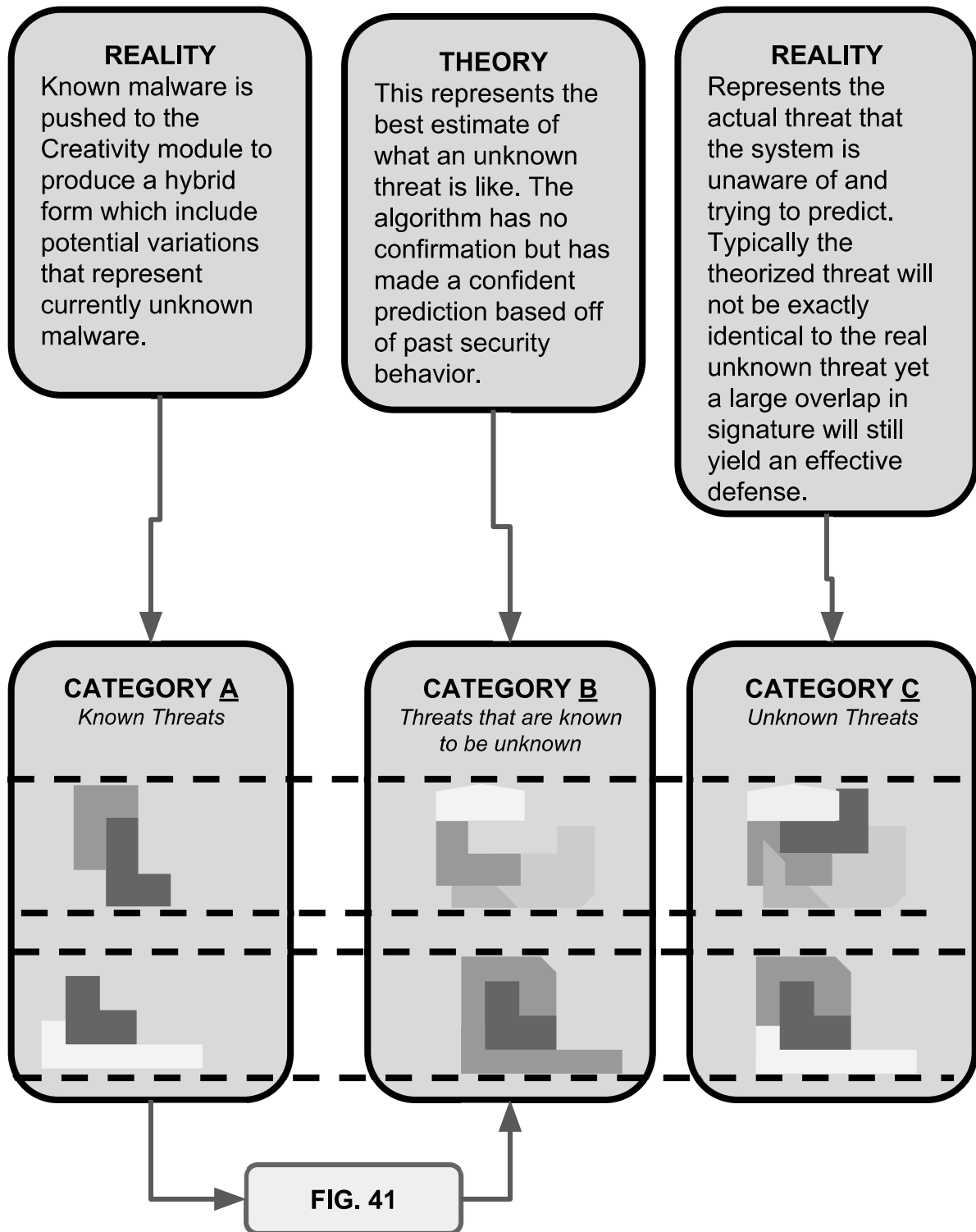


FIG. 40

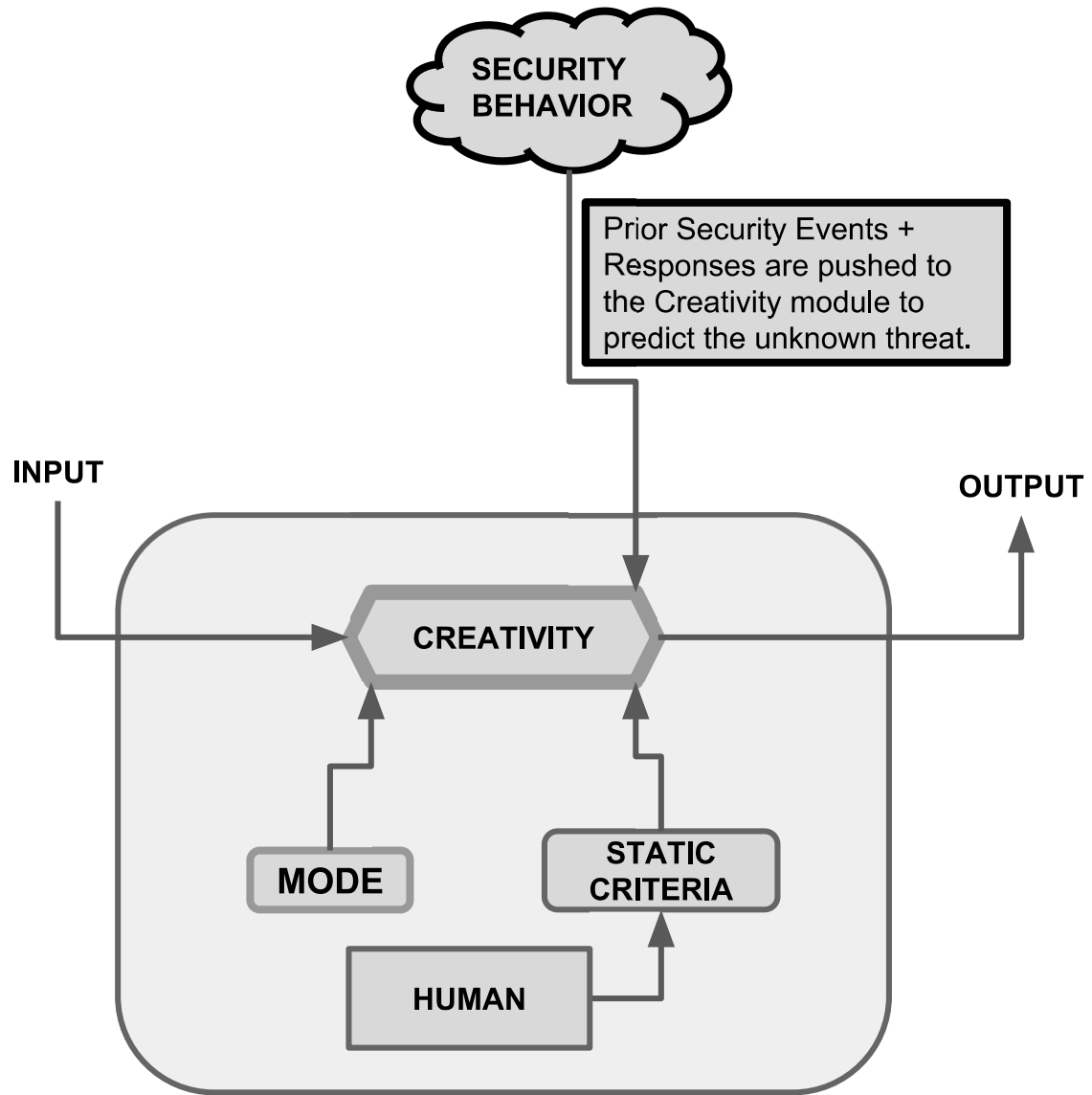


FIG. 41

A pattern is produced to represent the transition of a known and confirmed iteration. The transition pattern is then used to predict a currently unknown threat.

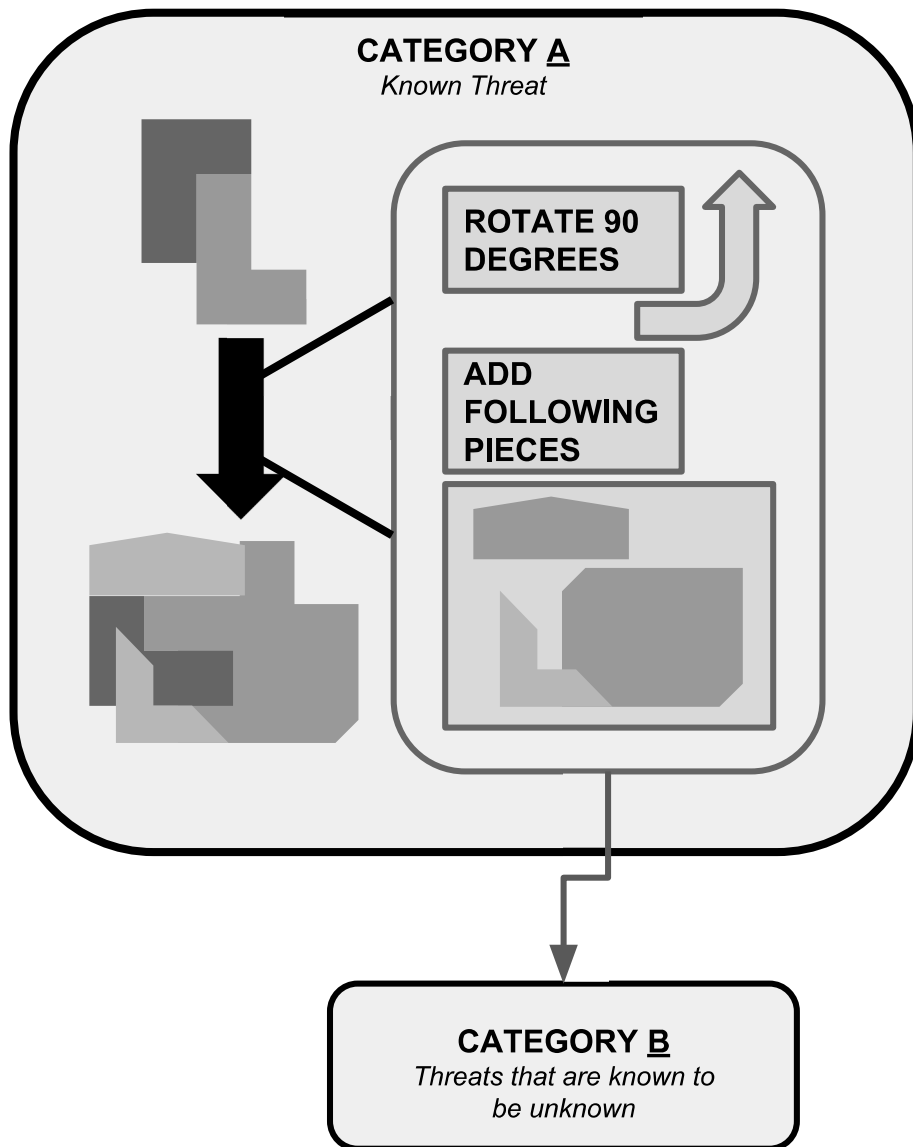
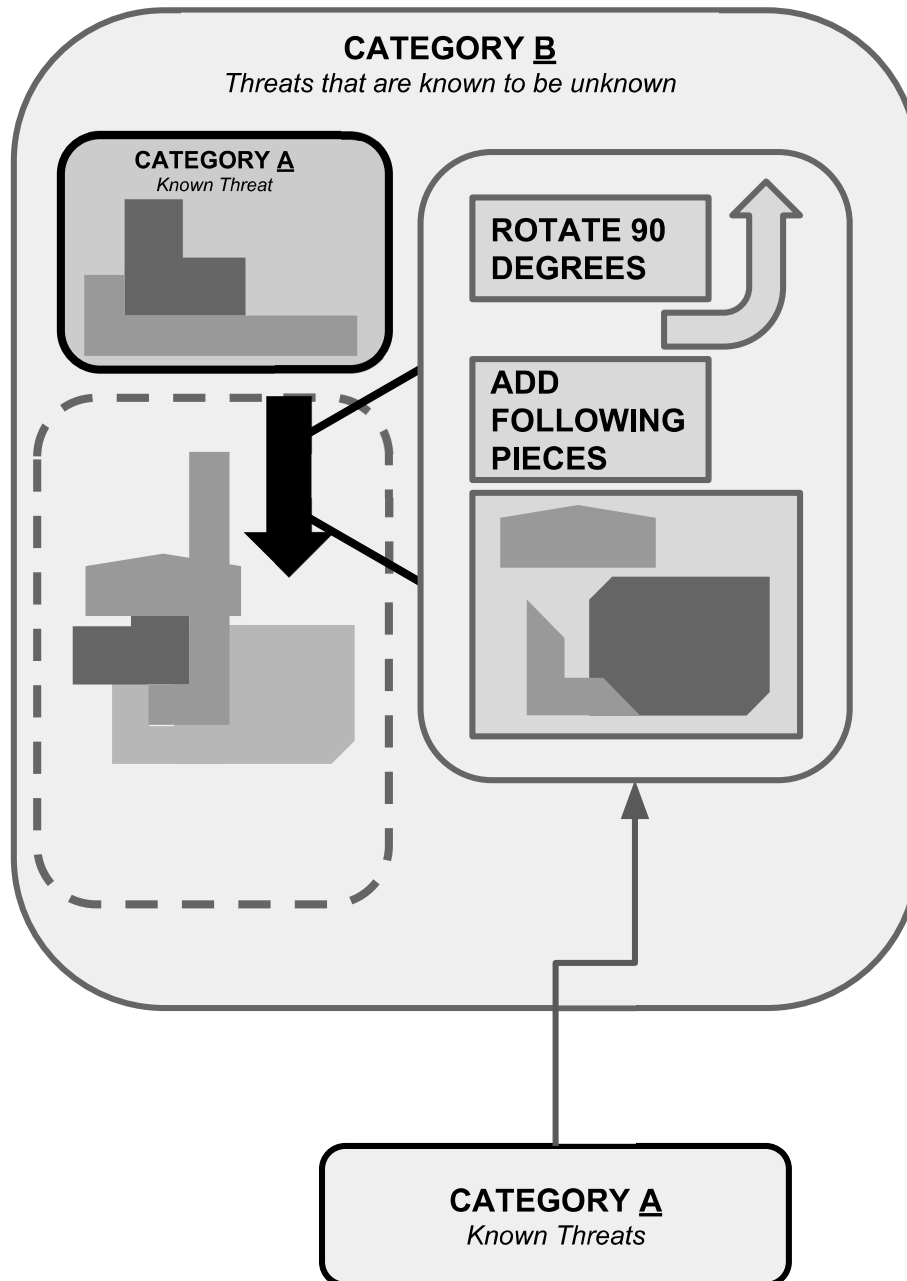


FIG. 42

The transition pattern is used to predict what a known malware might evolve into. The pieces added are not the exact same as those which were added in the known iteration, because this new color set matched the initial threat better. This means that the pattern iteration is dynamic and the iterative characteristics depends on the initial input.

**FIG. 43**

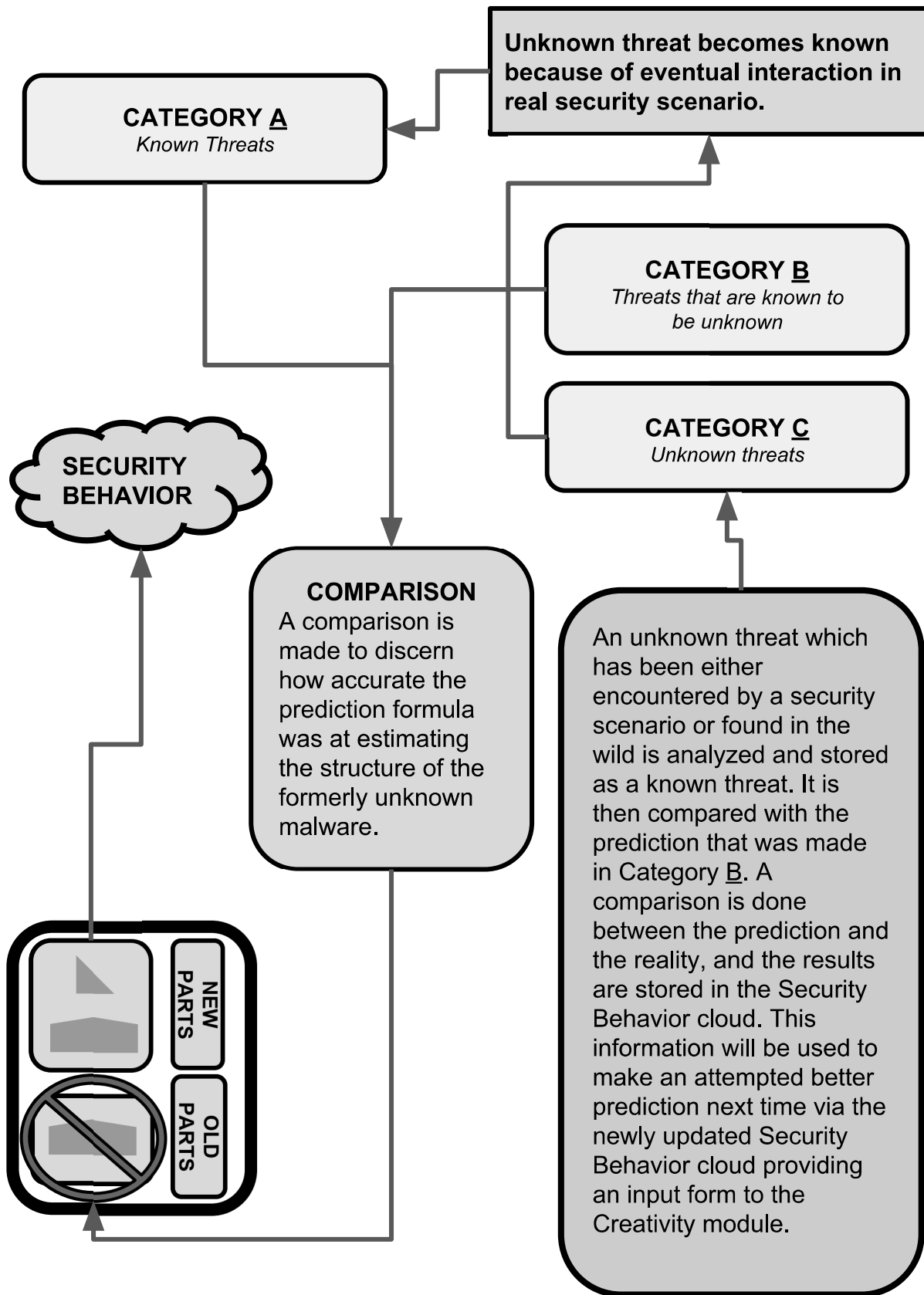


FIG. 44

These examples do not reflect the potentially more advanced correlation that can be made between shape/color/position and function/attribute.

GENOTYPE

A syntactic makeup of malware functions or attributes



A file transfer exploit that runs rogue code via the FTP protocol.

A file transfer exploit that runs rogue code via the SSH protocol.

A middleman intercept strategy. Malware pretends to be the intended target.

This malware pretends to be the intended file server target, and exploits the SSH protocol used to access files from the computer attempting to login.

PHENOTYPE

The descriptive and practical manifestation of malware functions or attributes

FIG. 45

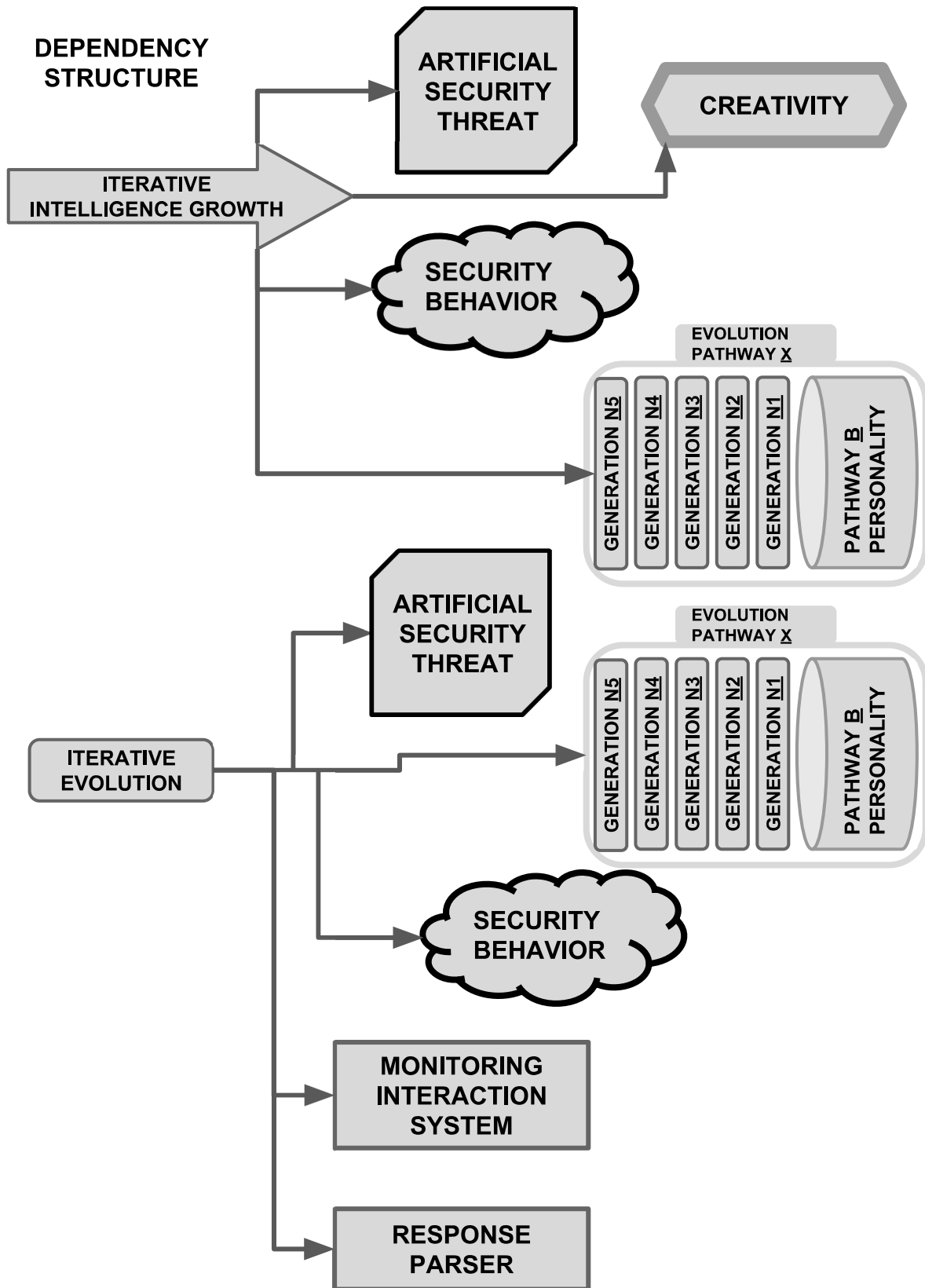


FIG. 46

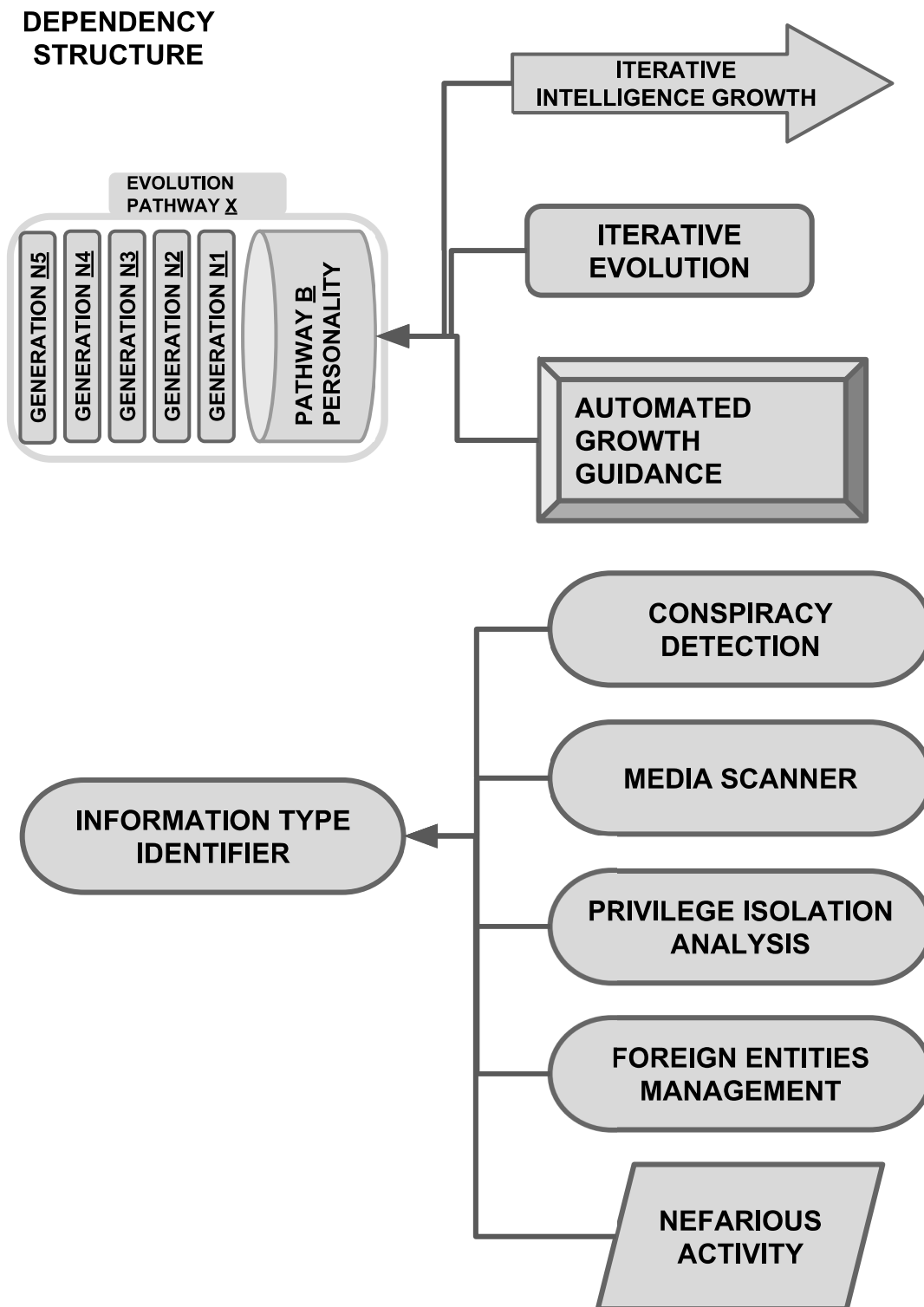


FIG. 47

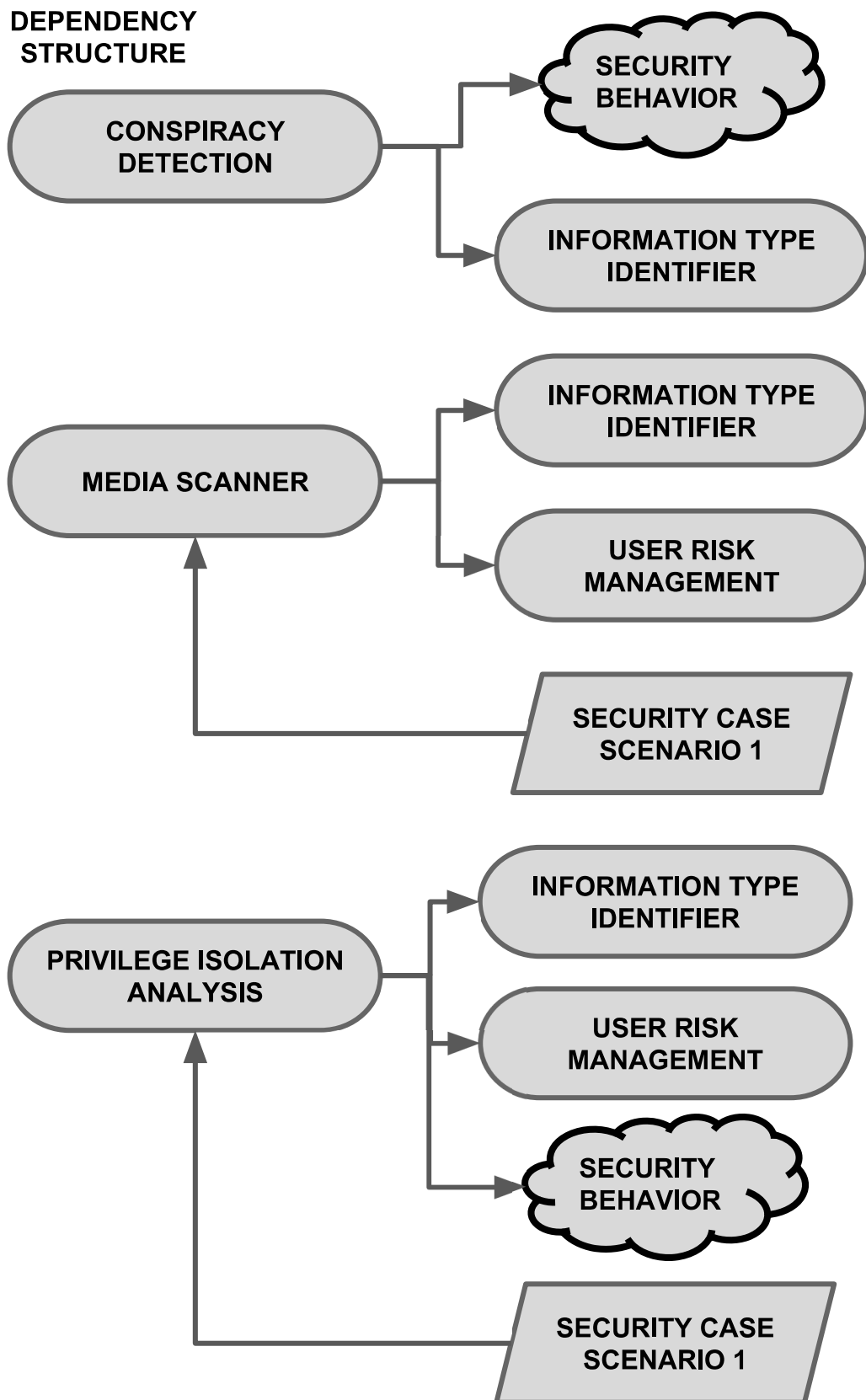
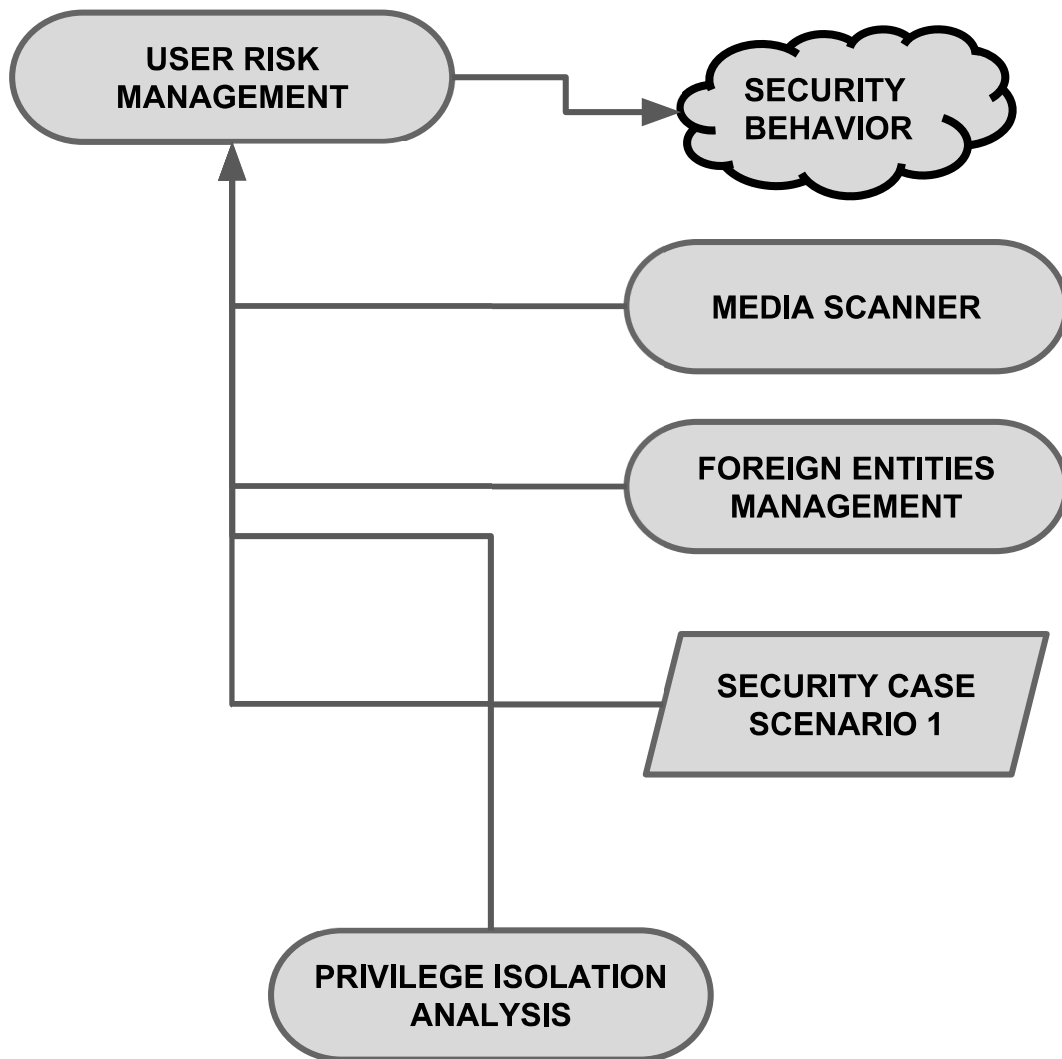


FIG. 48

**DEPENDENCY
STRUCTURE****FIG. 49**

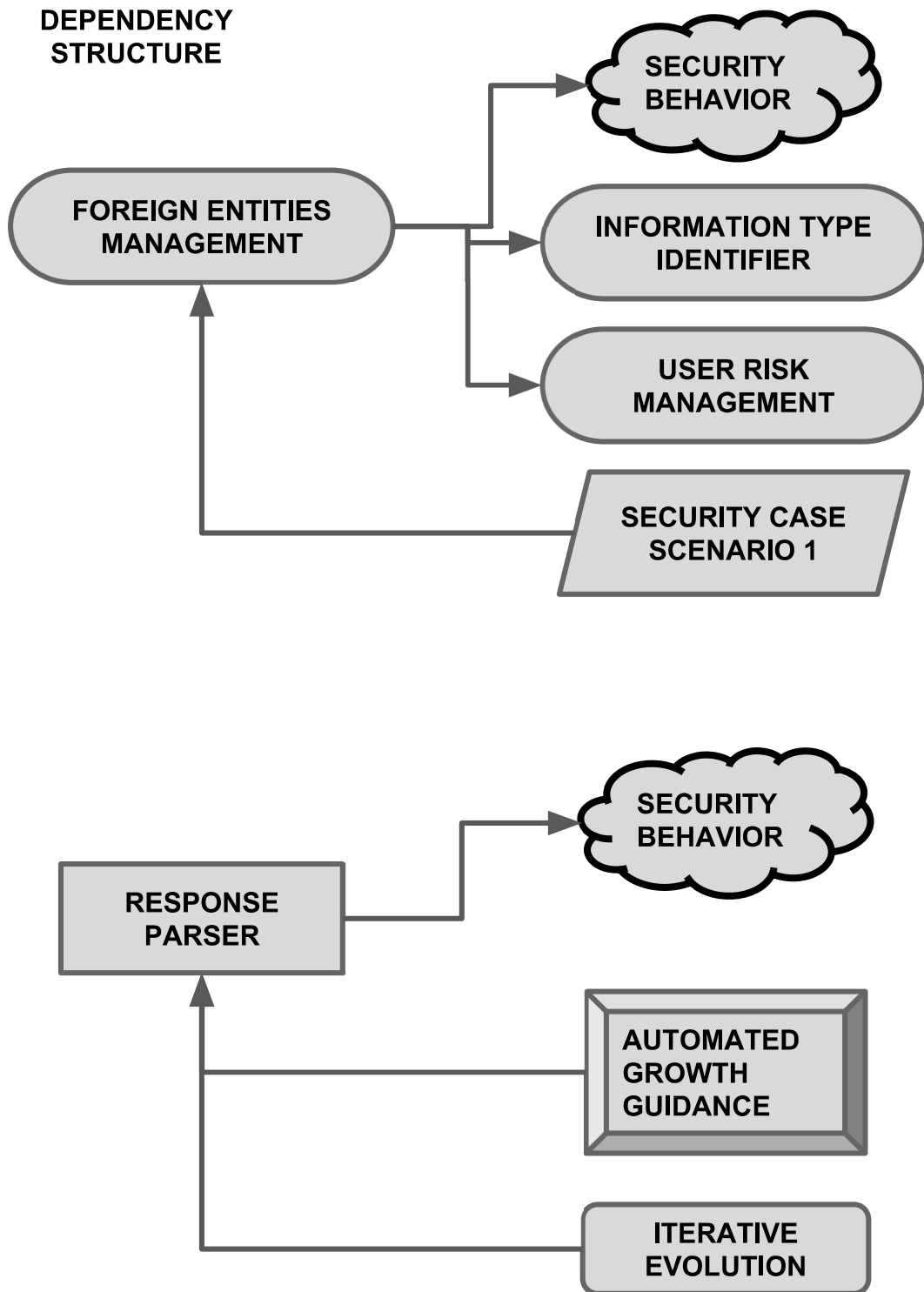


FIG. 50

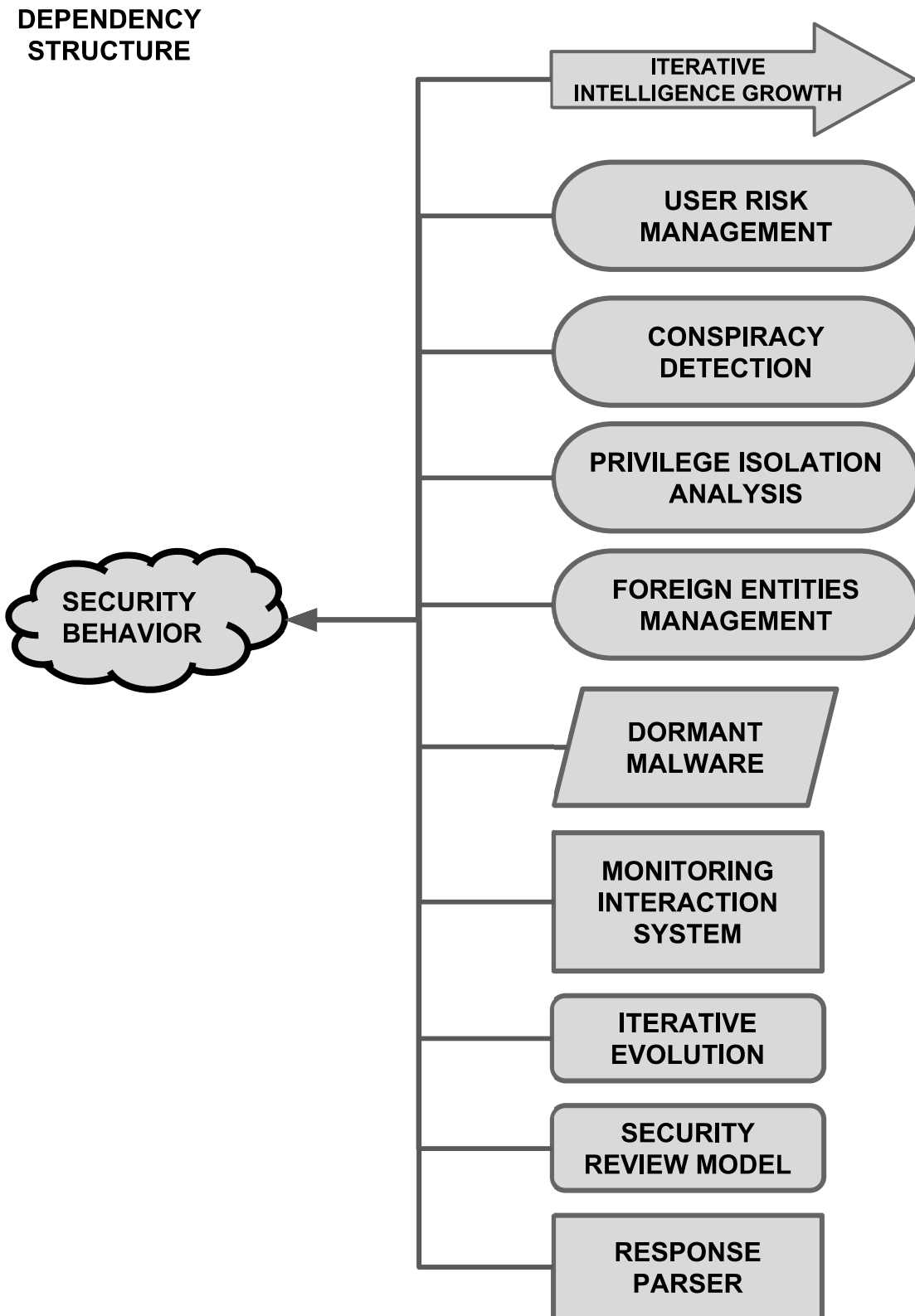


FIG. 51

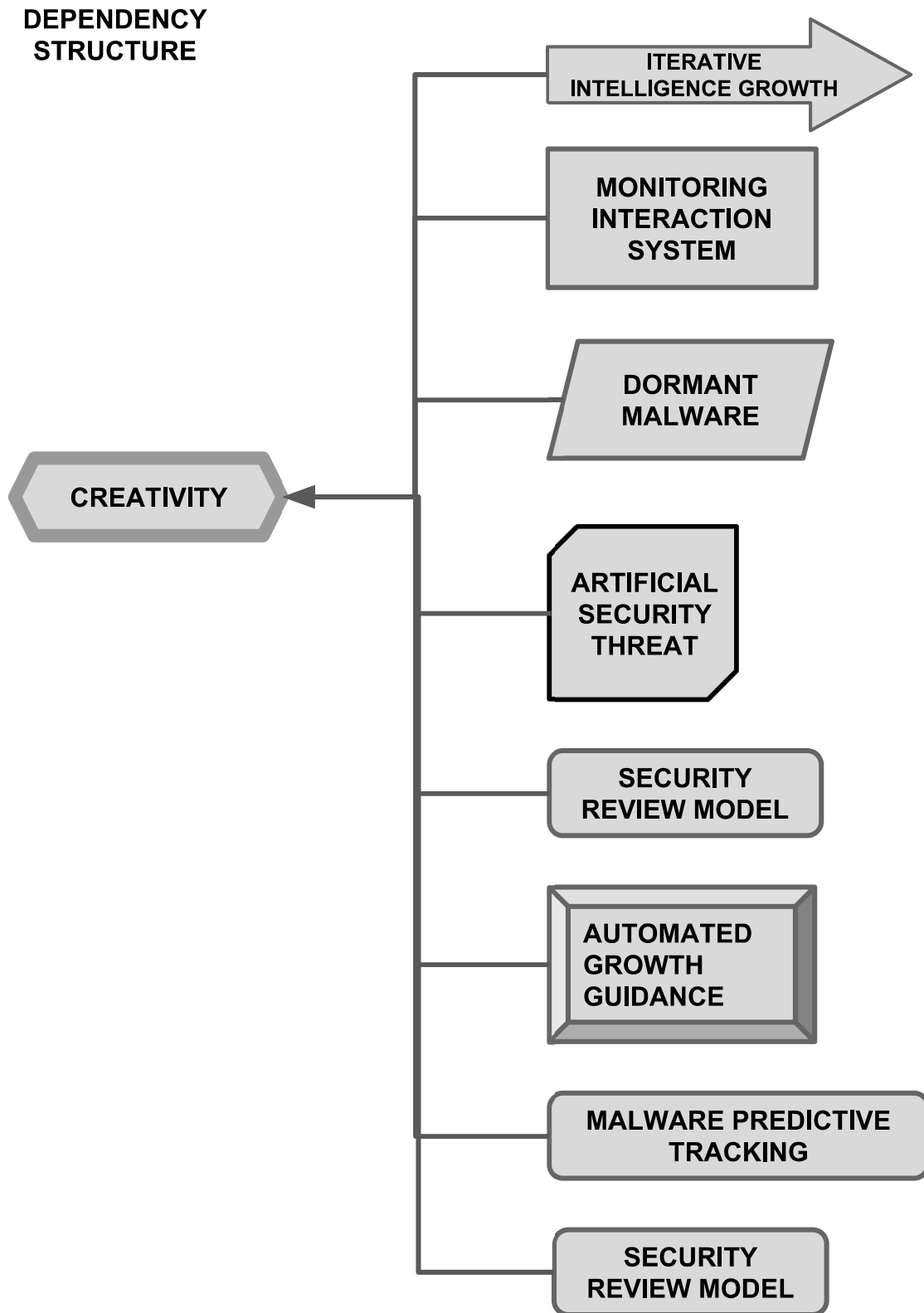
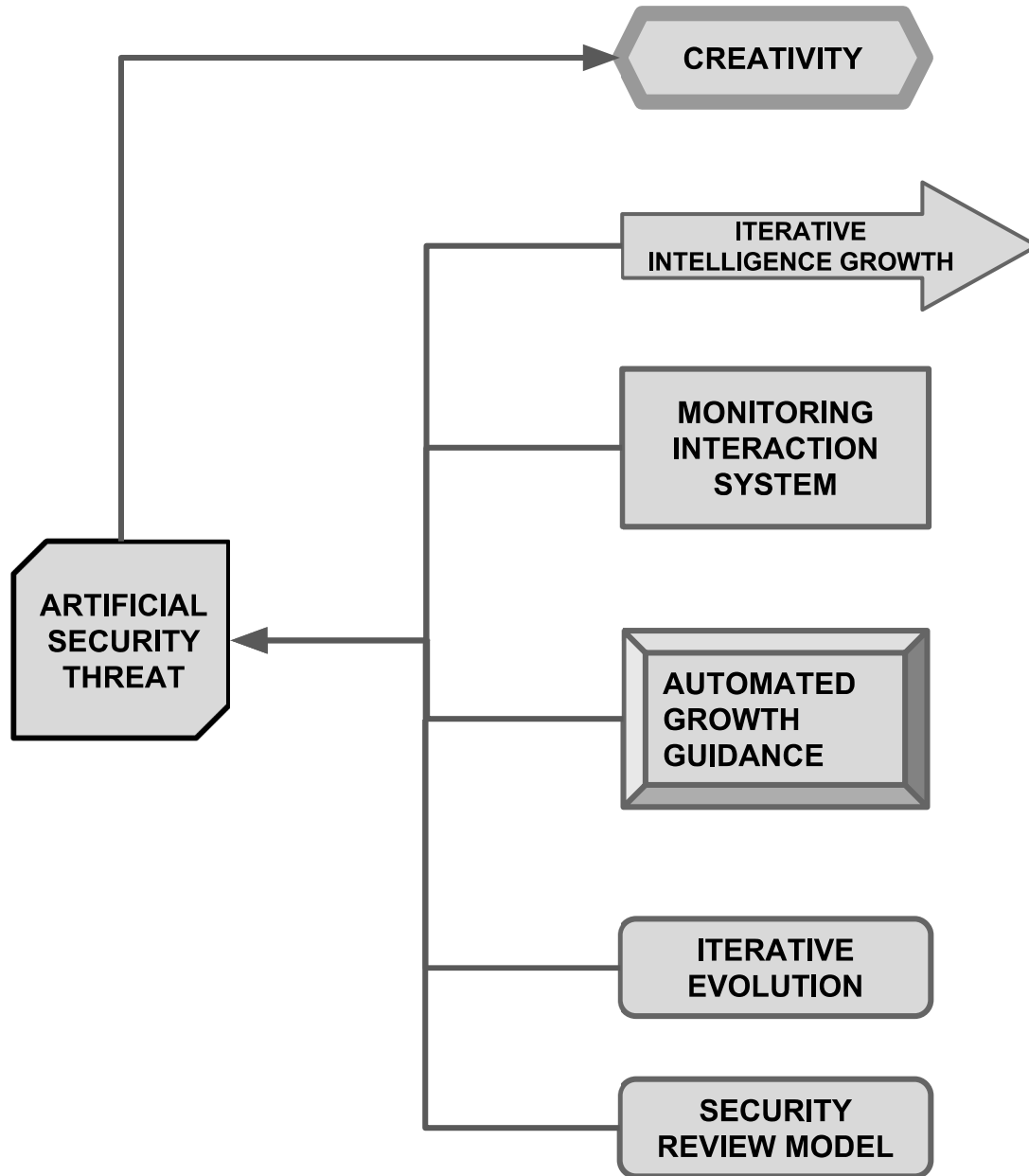
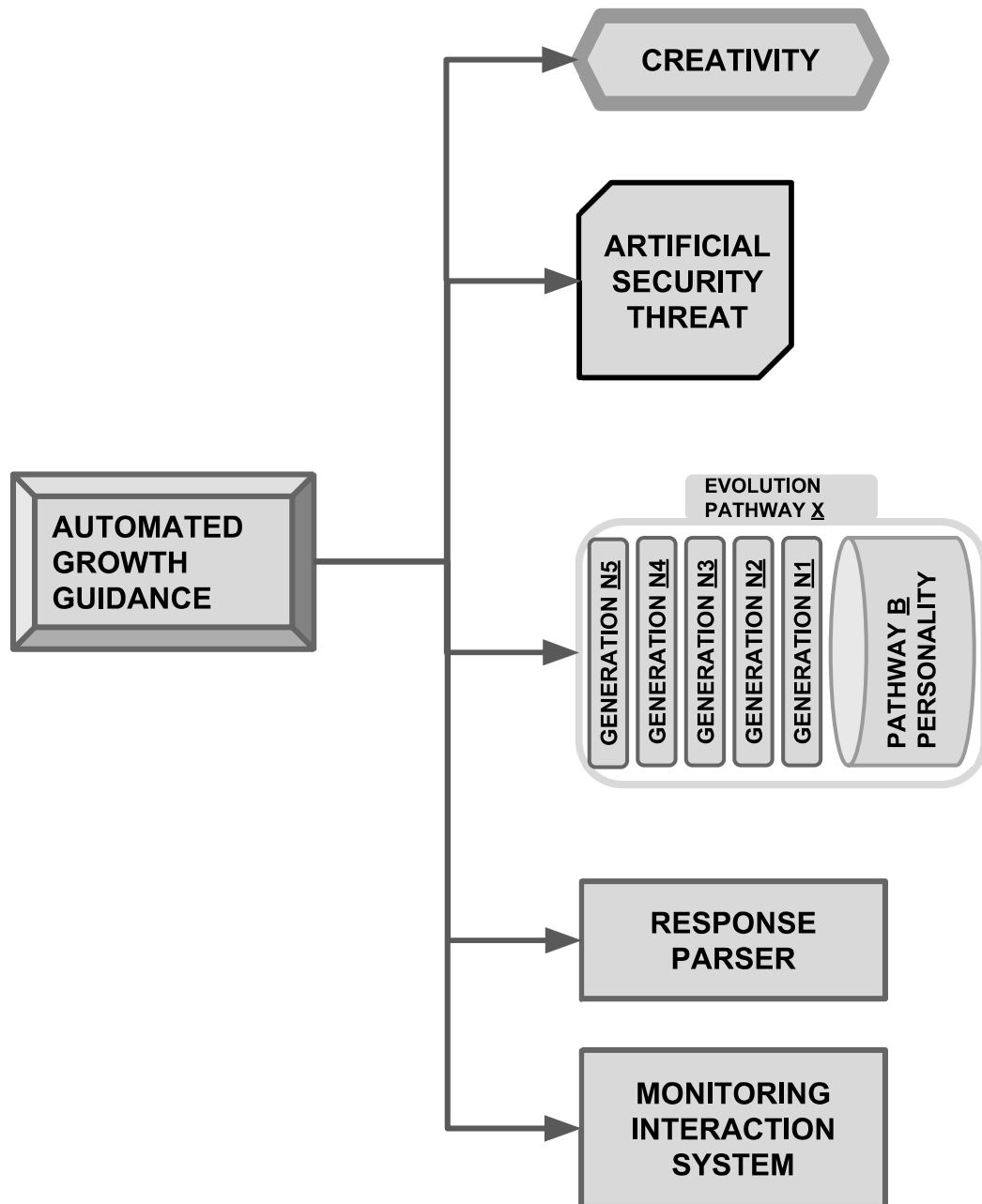
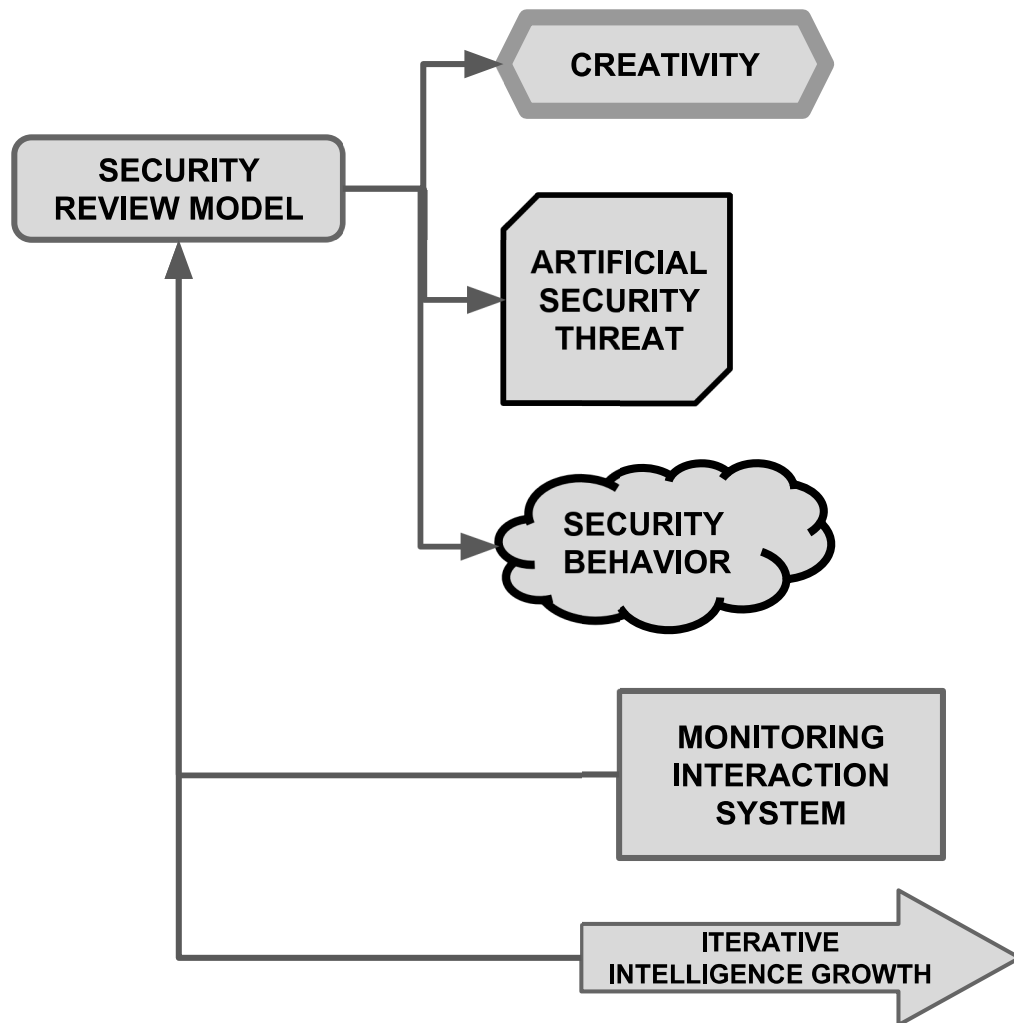
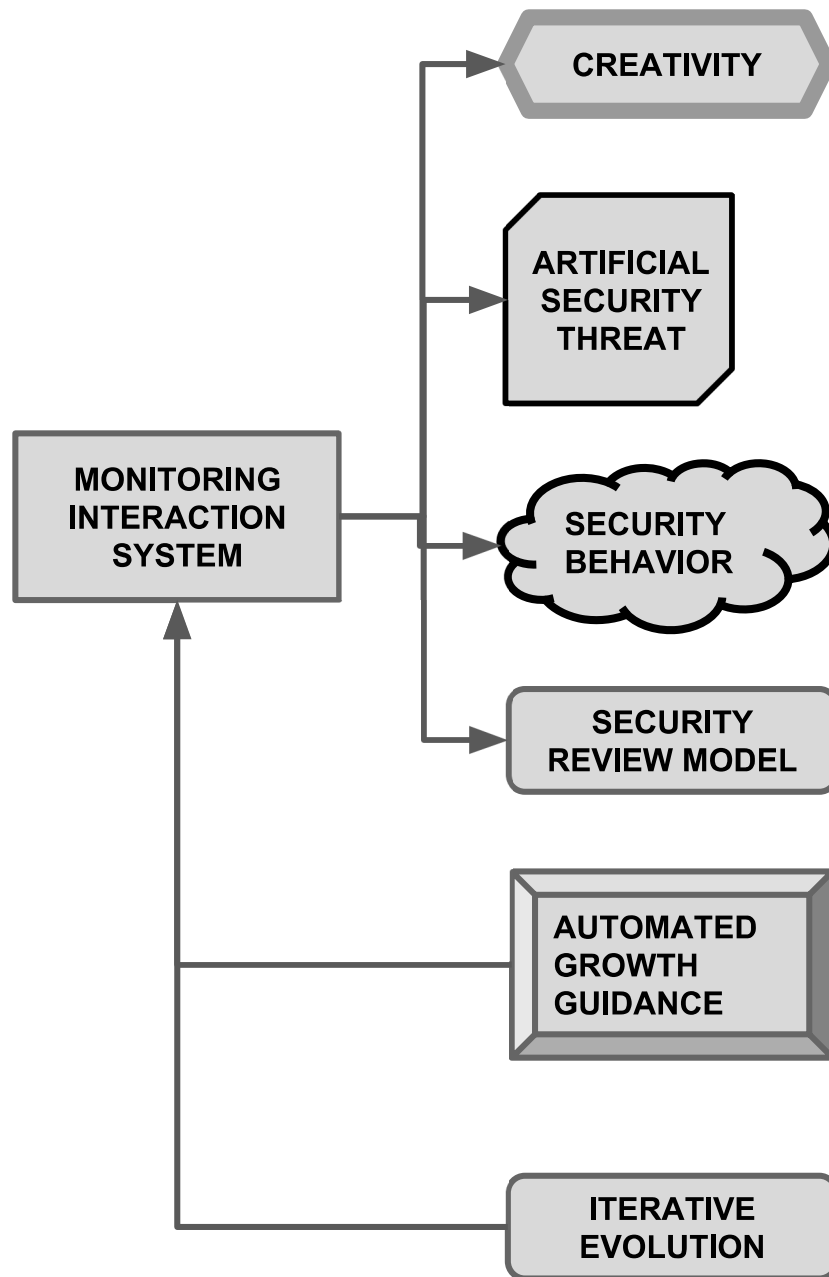


FIG. 52

**DEPENDENCY
STRUCTURE****FIG. 53**

**DEPENDENCY
STRUCTURE****FIG. 54**

**DEPENDENCY
STRUCTURE****FIG. 55**

**DEPENDENCY
STRUCTURE****FIG. 56**

**Critical Infrastructure Protection & Retribution (CIPR)
through Cloud & Tiered Information Security (CTIS)**

**CIPR
CTIS**

Who? is behind the malware/hack.

An established network of beacons and agents are used to form a map of aggressors and bad actors. When such a map/database is paired with sophisticated predictive algorithms, potential pre-crime threats emerge.

**Malware
Source**

I²GE leverages big data and malware signature recognition to determine who.

What? are the consequences/impact.

What assets are at risk, what potential damage can be done. e.g. A Hydroelectric dam can have all of it's floodgates opened which could eventually flood a nearby village and lead to loss of life and property.

**Infrastructure
DB**

**Infrastructure
Controls**

I²GE Security Behavior storage forms a precedent of security events, their impact, and the appropriate response. Such an appropriate response can be criticized by CTMP (Critical Thinking, Memory, Perception) as a supplemental layer of security.

When? is the potential/expected time of attack.

Traffic patterns are analyzed to highlight times of potential blind spots. Such attacks could be easily masked to blend with and underneath legitimate traffic. Are there are any political/financial/sporting/other events that may be a point of interest for bad actors.

24

**January,
2016**

The Trusted Platform's network of external agents report back hacker activity and preparation. Therefore attack timing can be estimated.

FIG. 57

**Critical Infrastructure Protection & Retribution (CIPR)
through Cloud & Tiered Information Security (CTIS)**

**CIPR
CTIS**

Where? is it likely to happen.

Who are the more vulnerable enterprises that might be targeted for an attack. What types of enterprises might be vulnerable in given geographic locations. What are their most vulnerable assets/controls and what are the best means of protecting them.

**Infrastructure
System**

The Trusted Platform's network of external agents report back hacker activity and preparation. Therefore attack location can be estimated.

Why? is it going to happen, and what are the motives.

What geopolitical, corporate, and financial pressures exist in the world to facilitate the funding and abetting of such an attack. Who would benefit and by how much.



The Trusted Platform's network of external agents report back hacker activity and preparation. Therefore attack motive can be estimated.

How? can it happen, and how can it be stopped.

What are potential points of exploits and hiding spots for malware. How can such blind spots and under-fortified points of access be used to compromise critical assets and points of infrastructure control.



LIZARD can derive purpose and functionality from foreign code, and hence block it upon presence of malicious intent or absence of legitimate cause. CTMP is able to think critically about block/approval decisions and acts as a supplemental layer of security.

FIG. 58

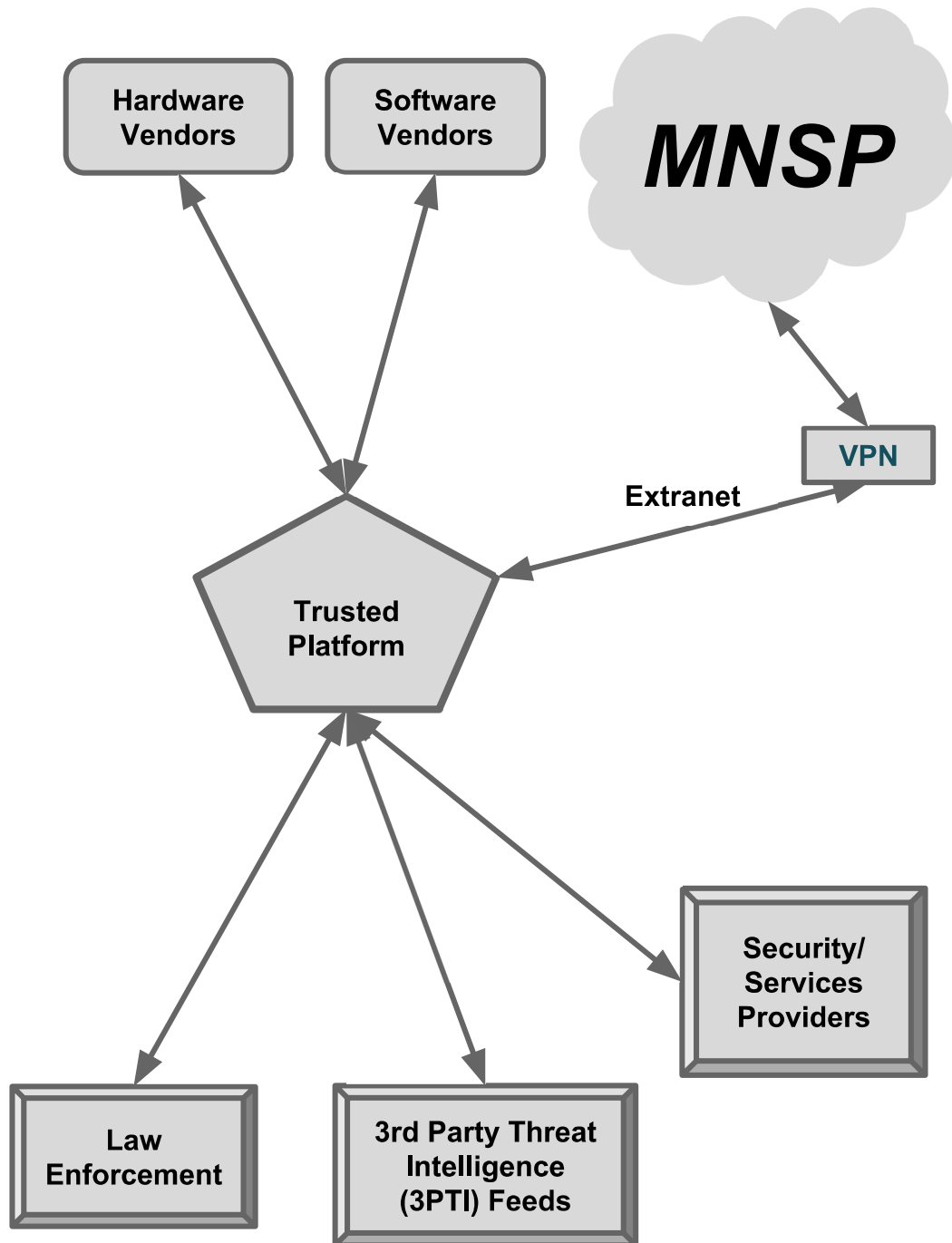


FIG. 59

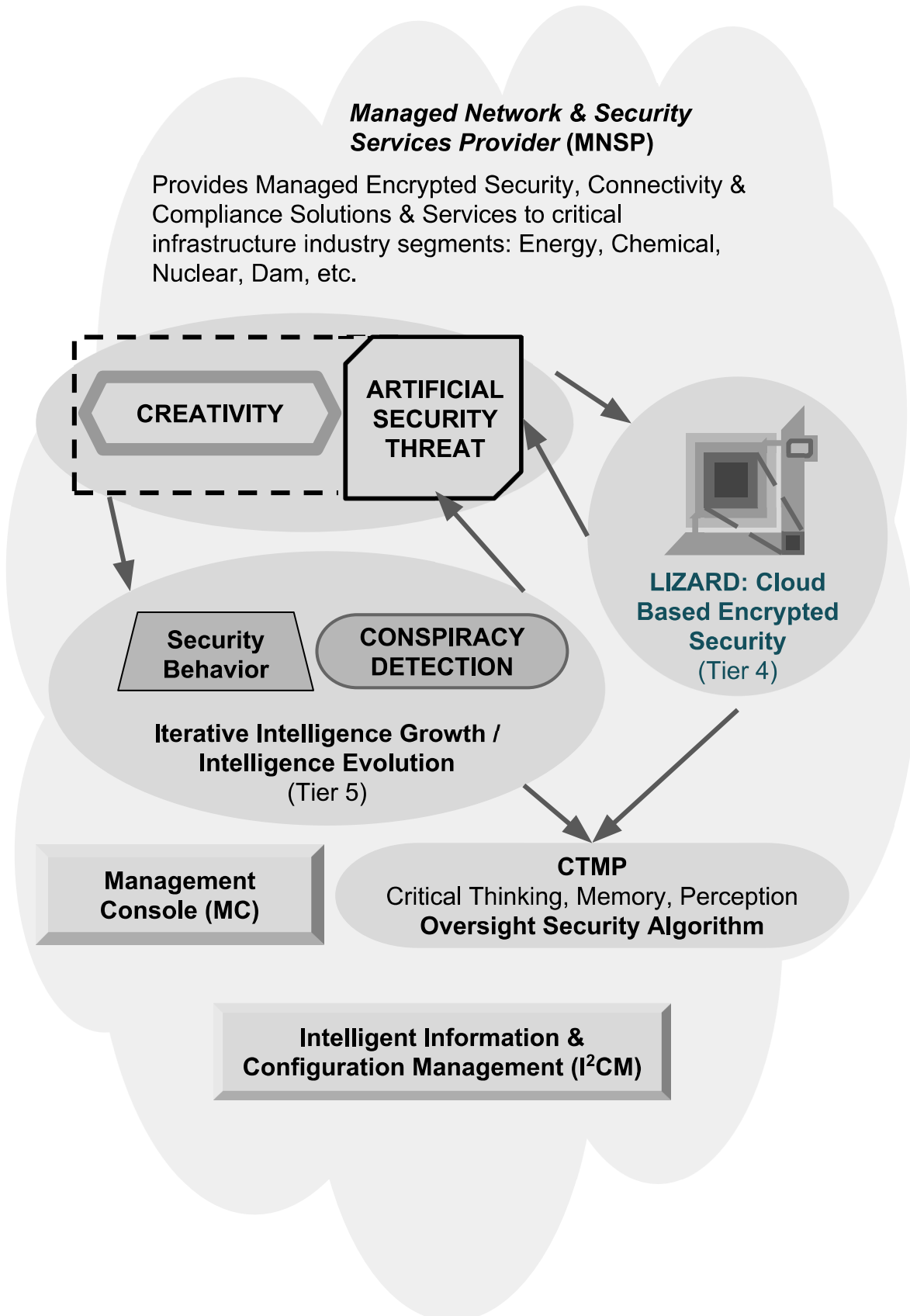


FIG. 60

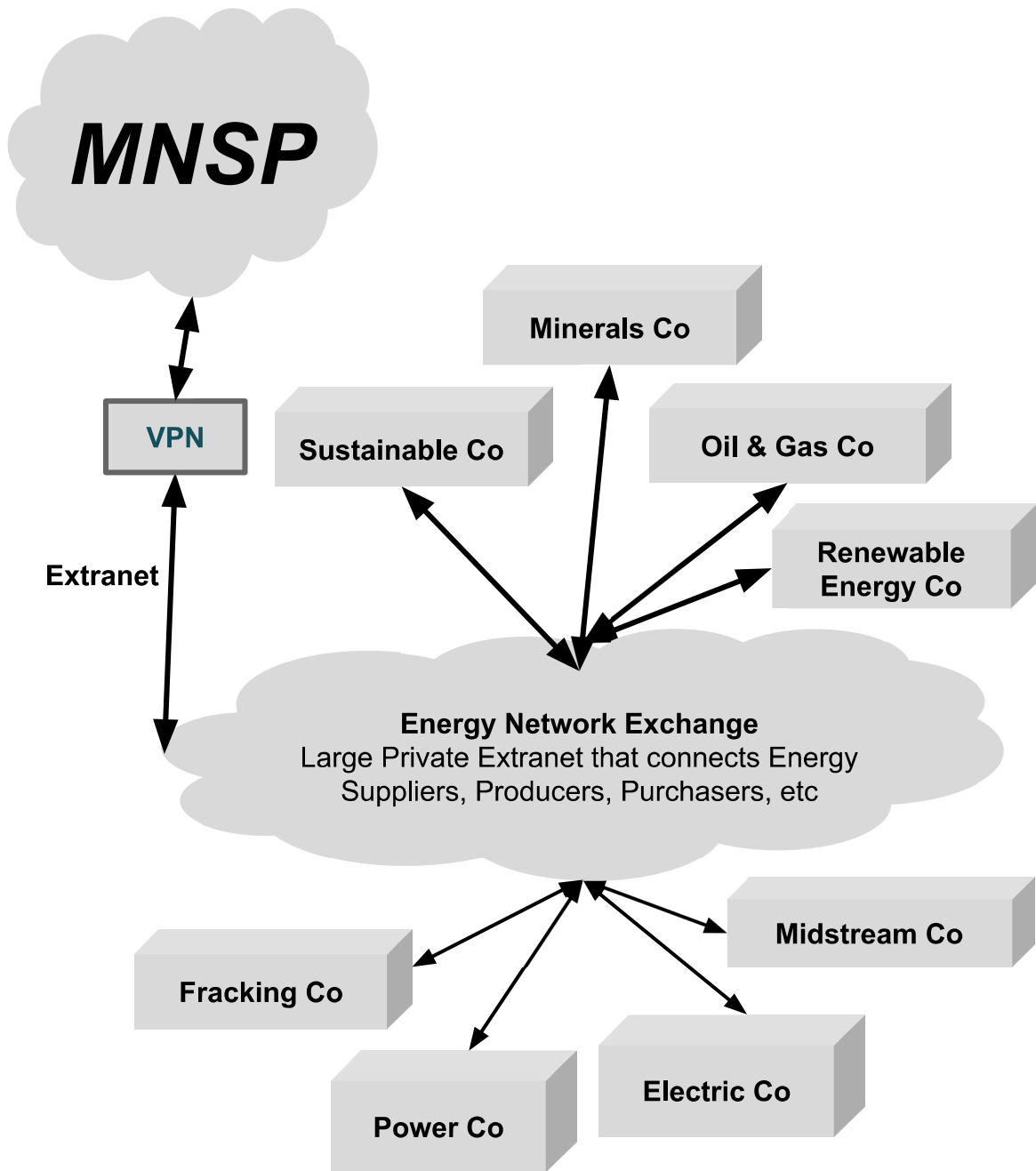


FIG. 61

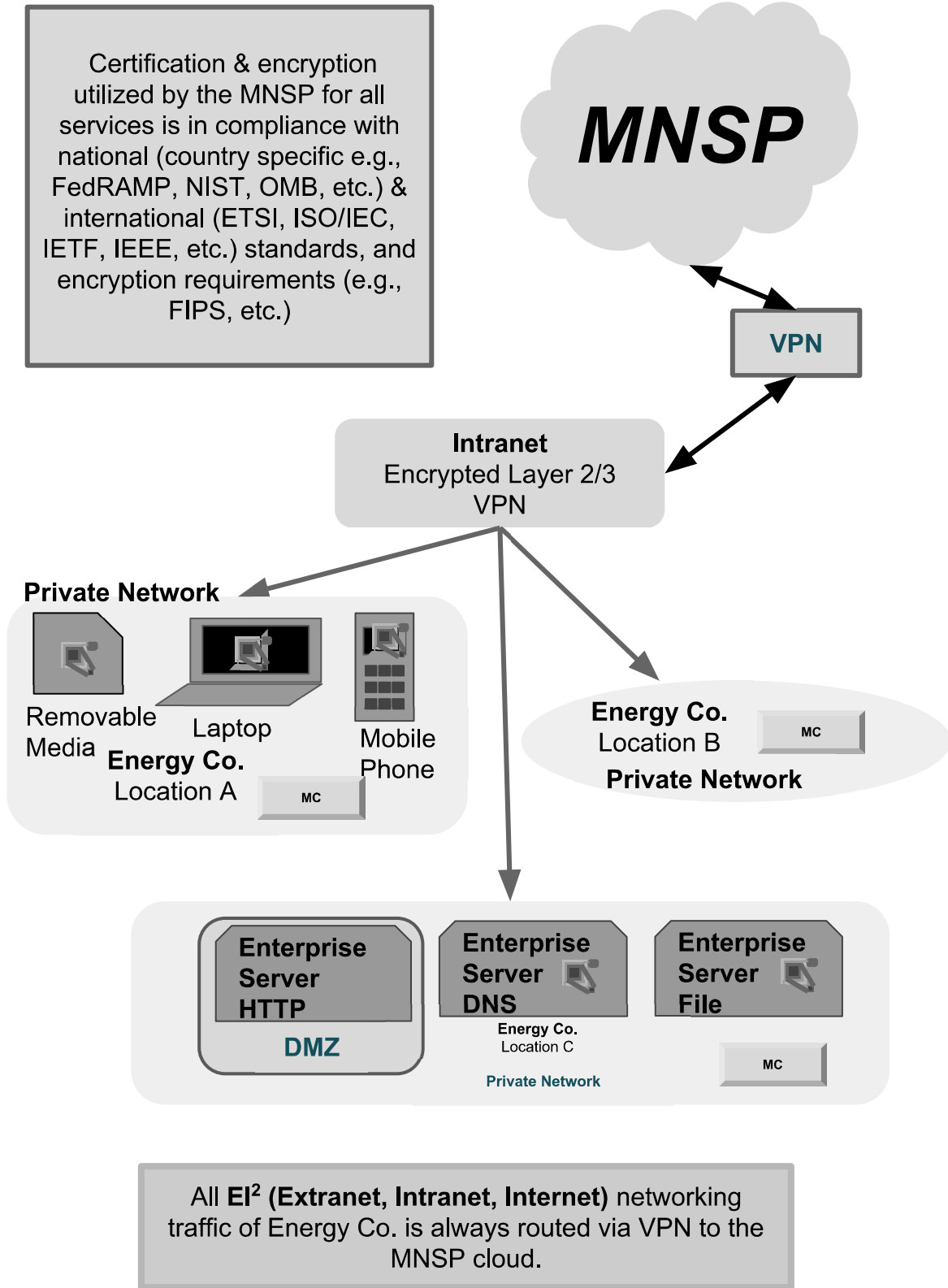
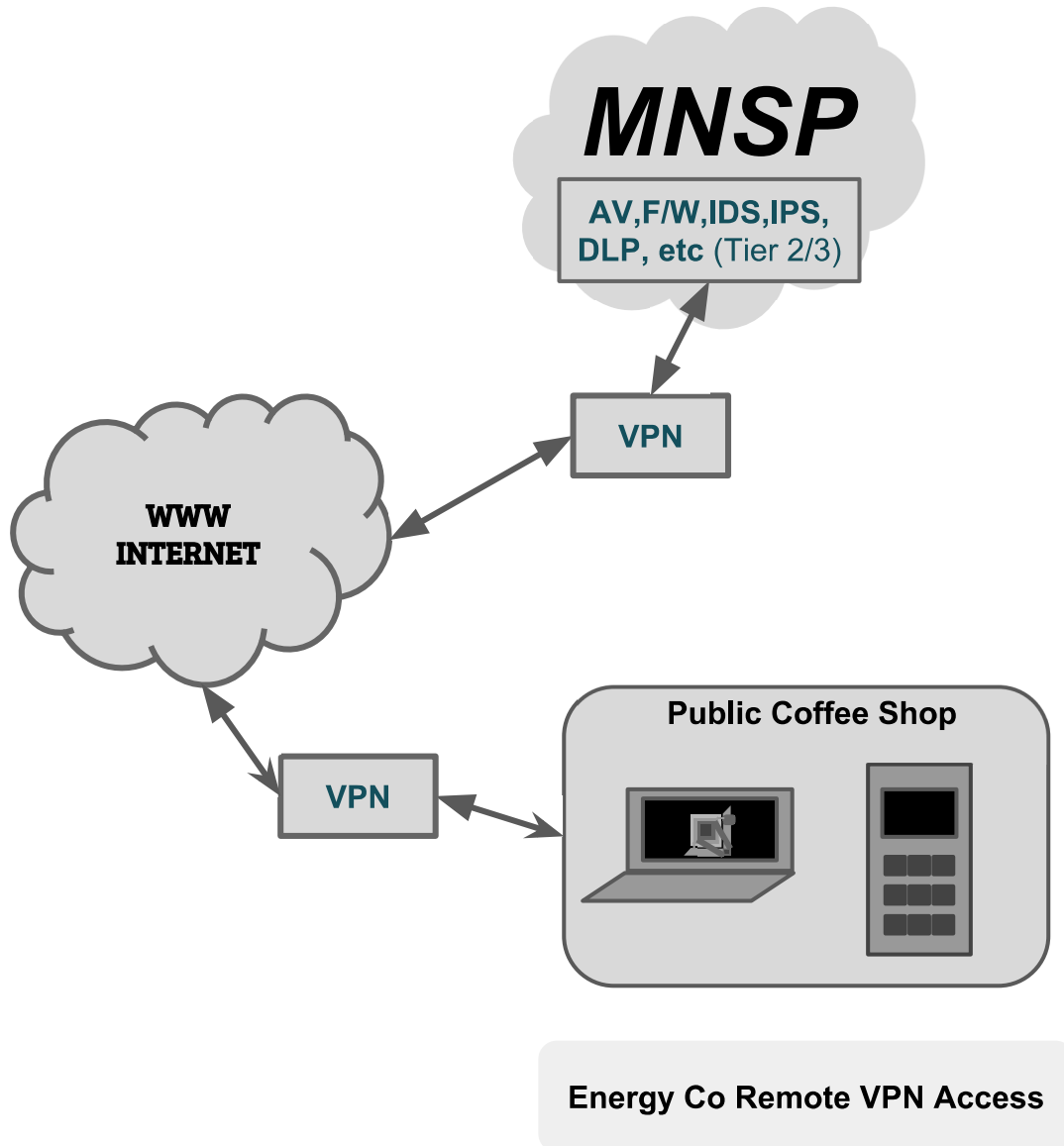


FIG. 62

**FIG. 63**

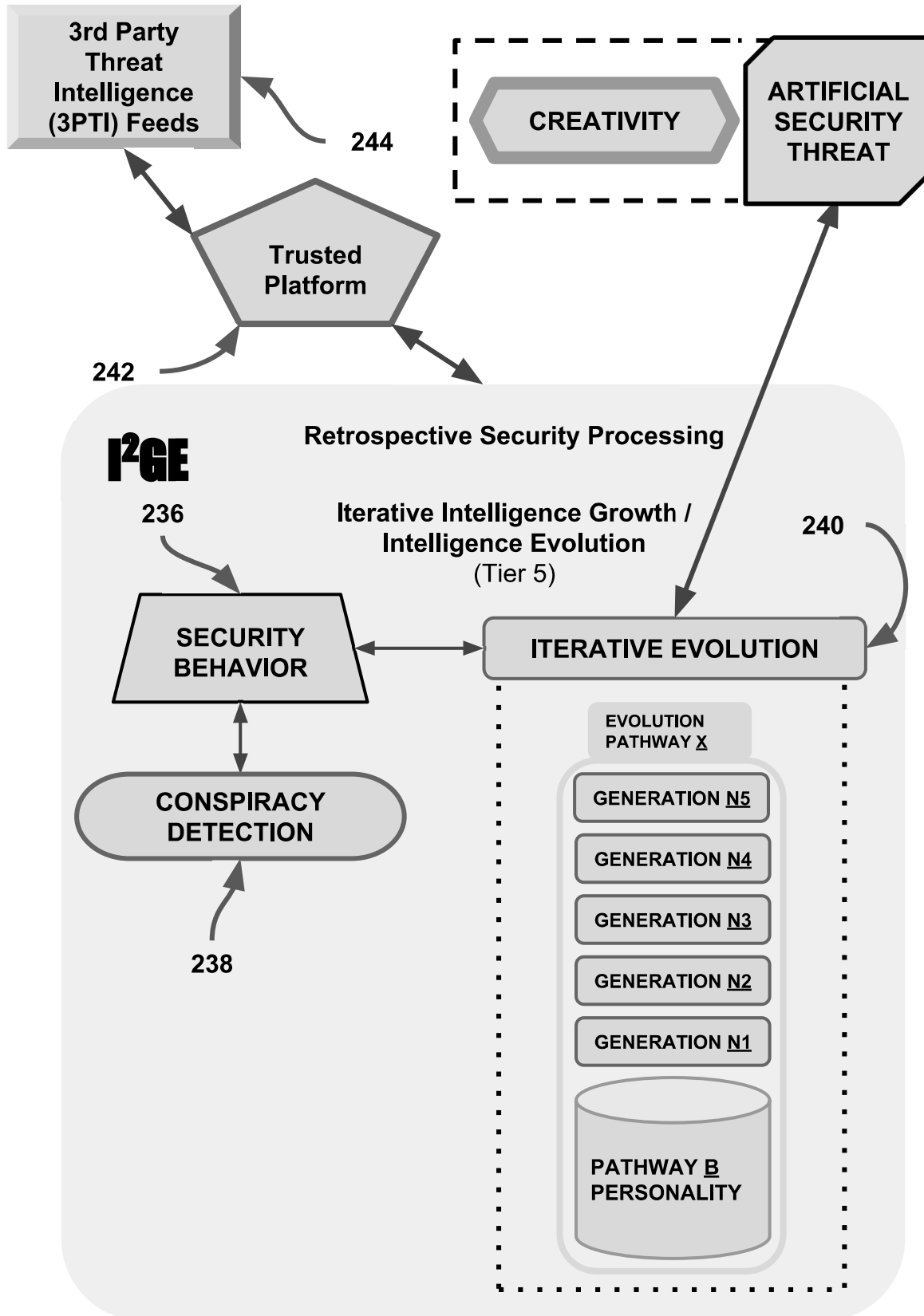


FIG. 64

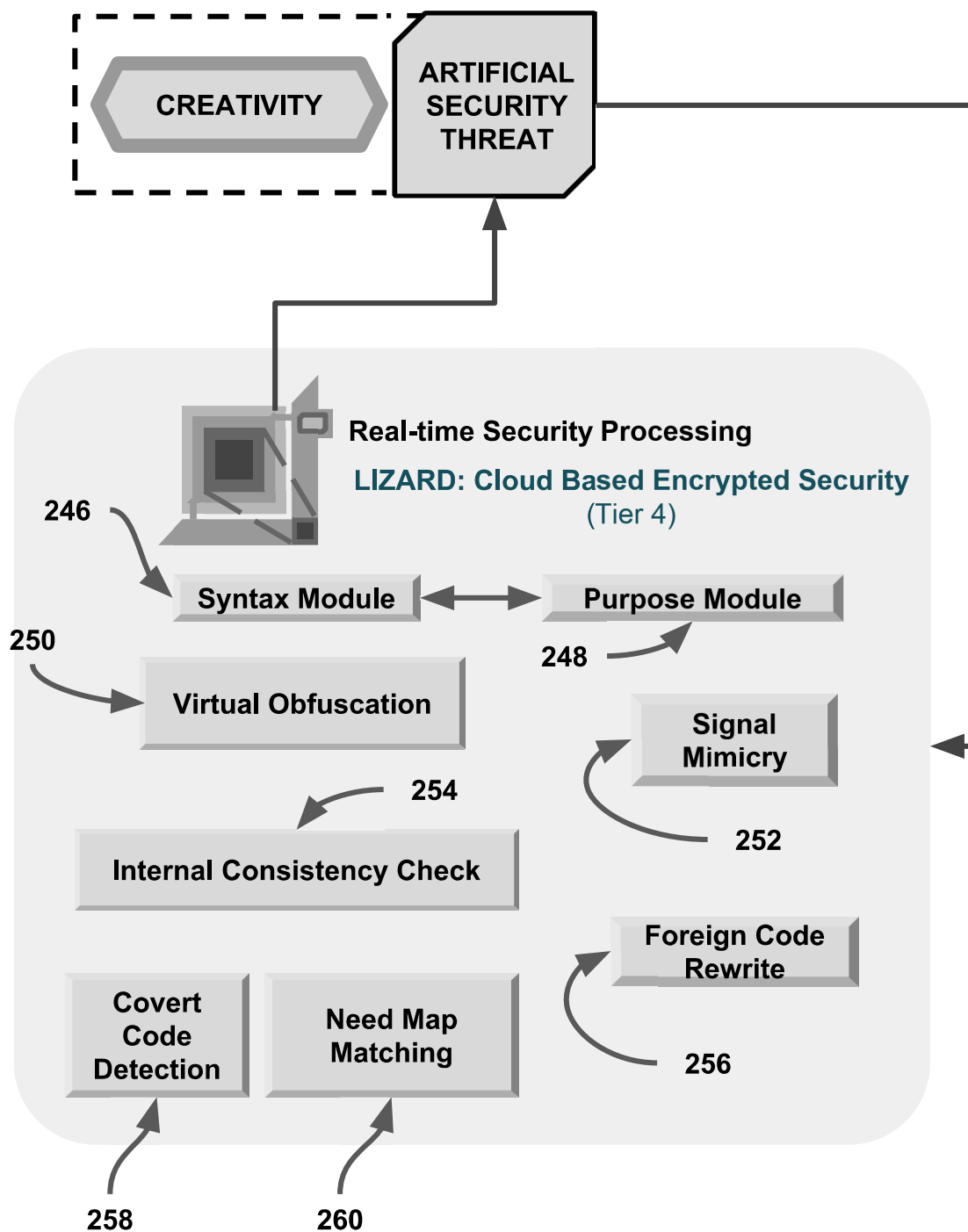


FIG. 65

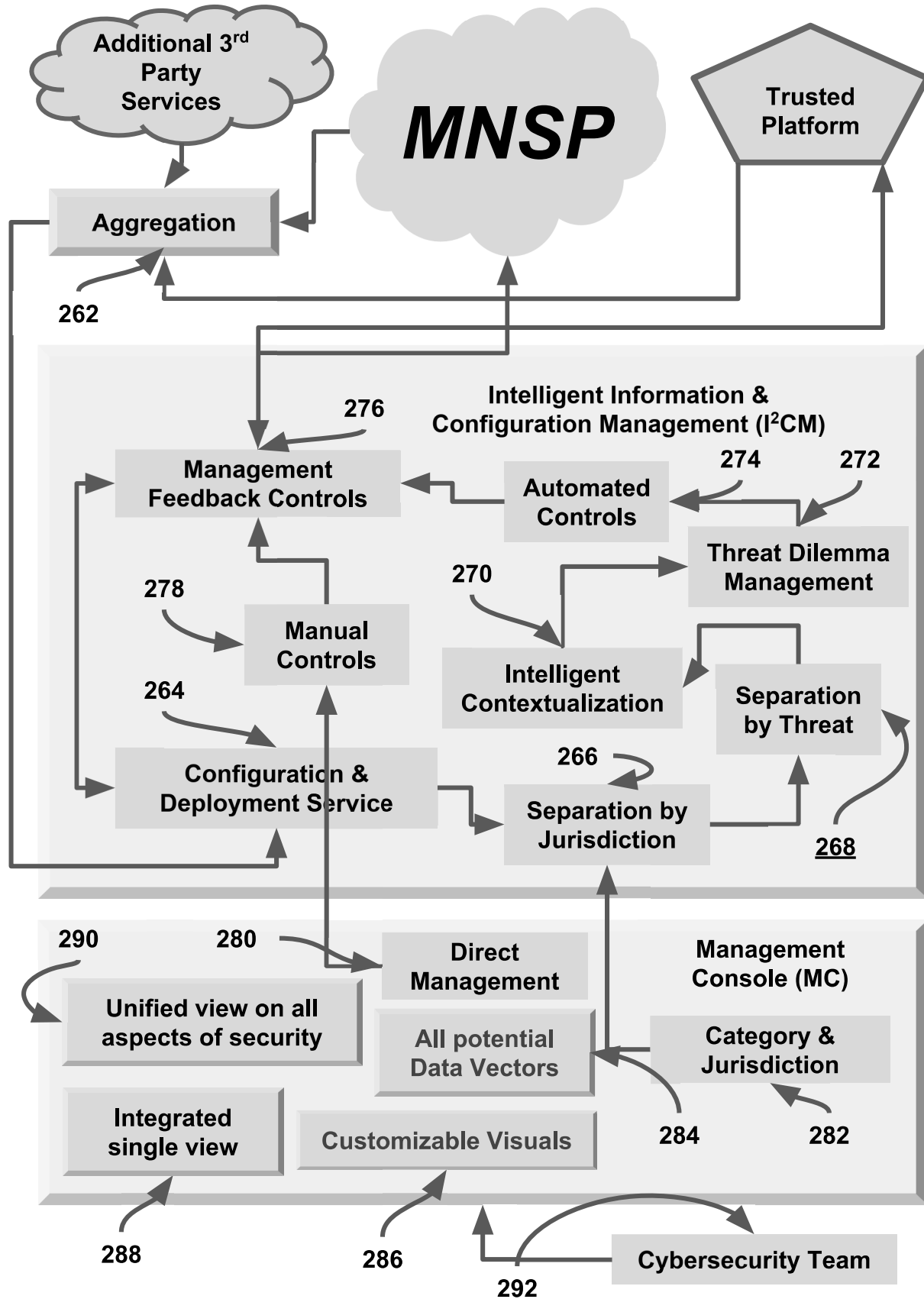


FIG. 66

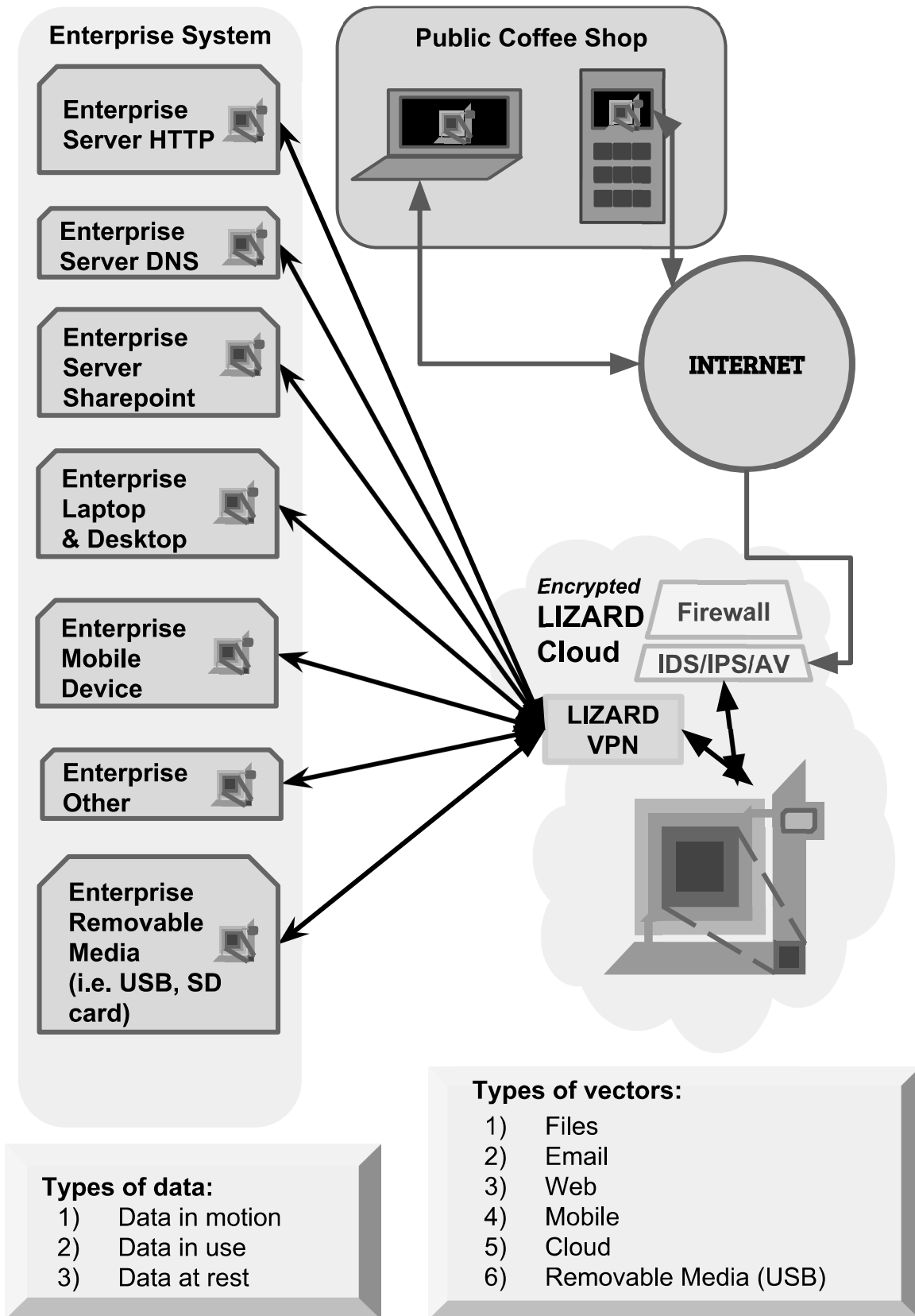


FIG. 67

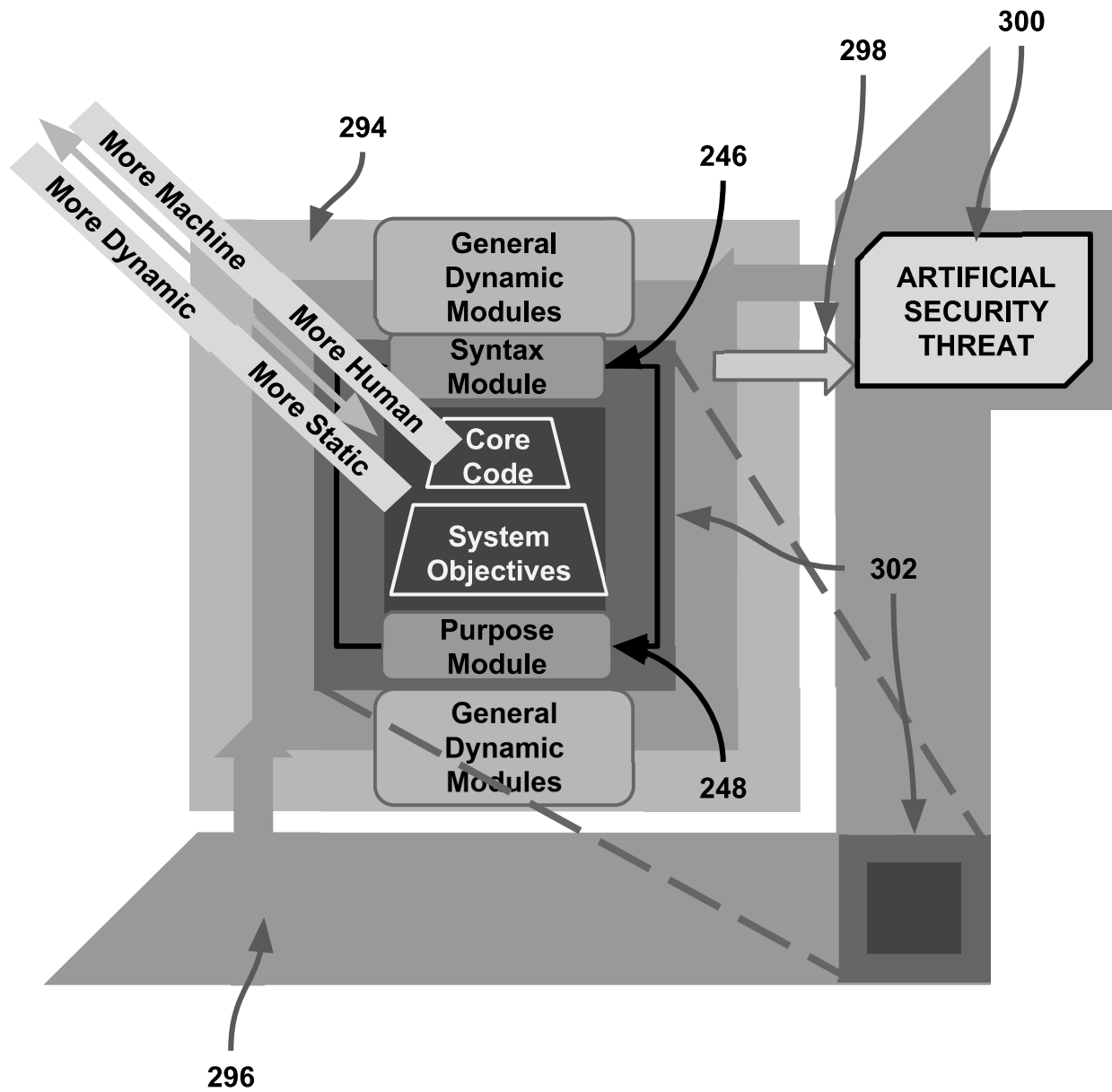


FIG. 68

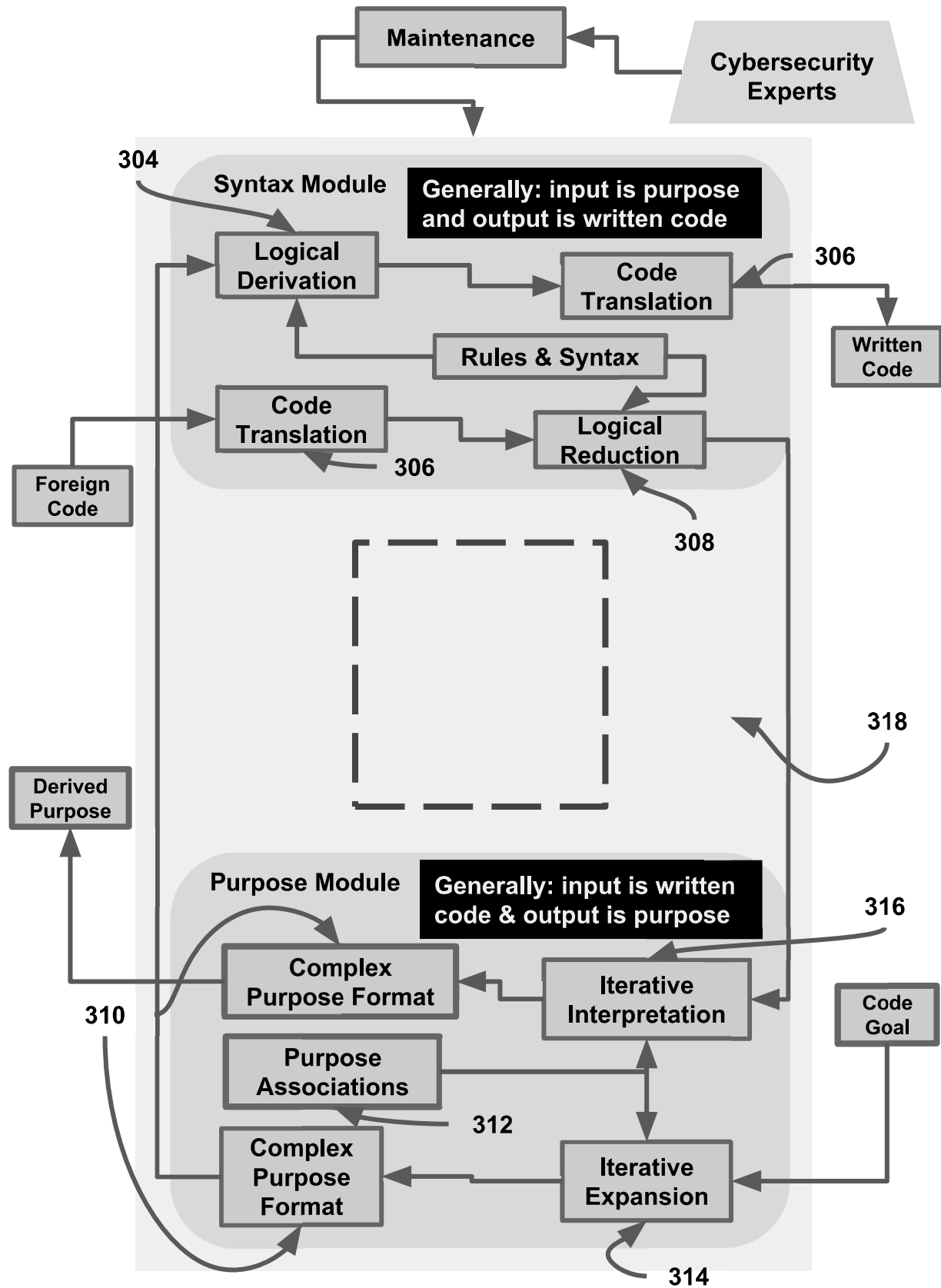


FIG. 69

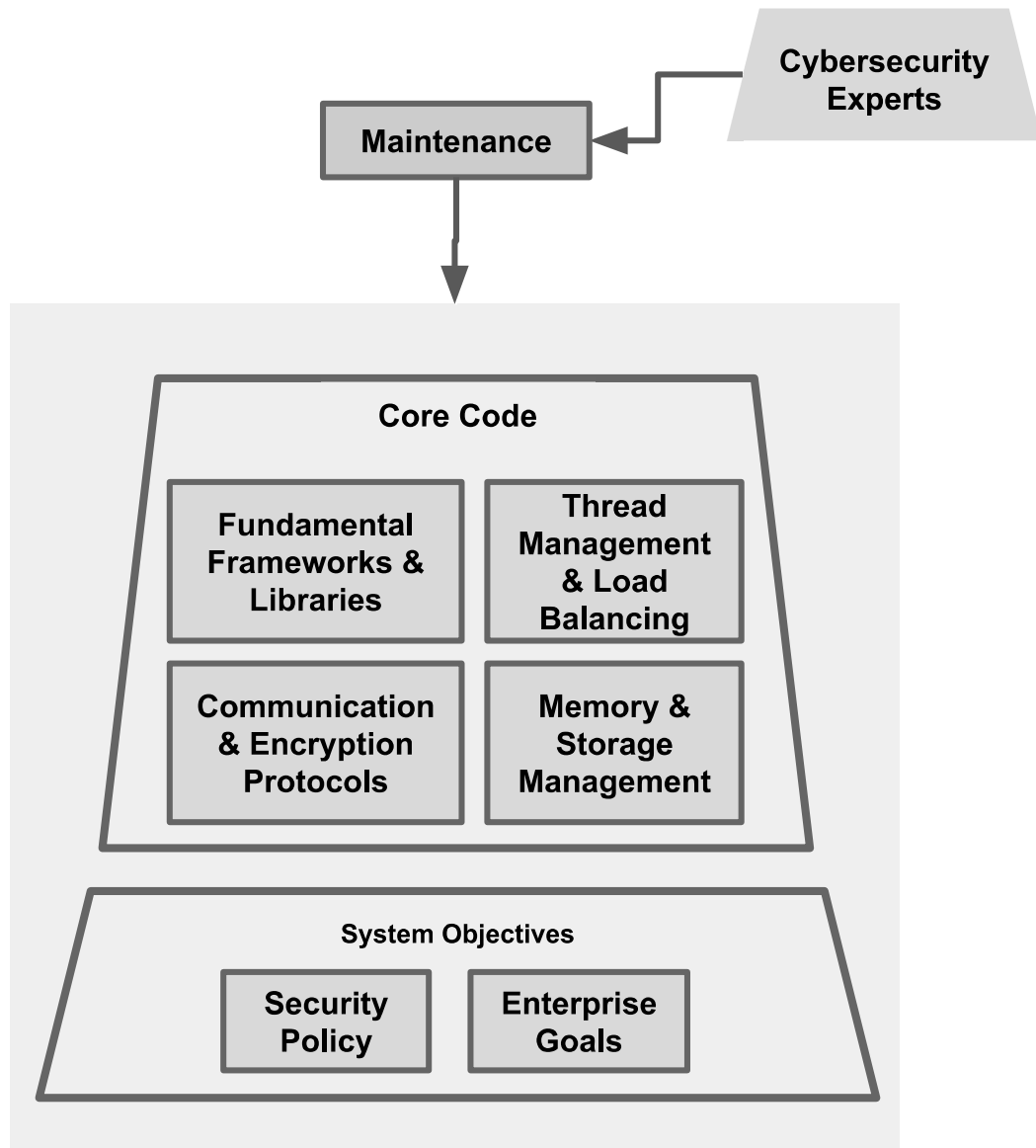


FIG. 70

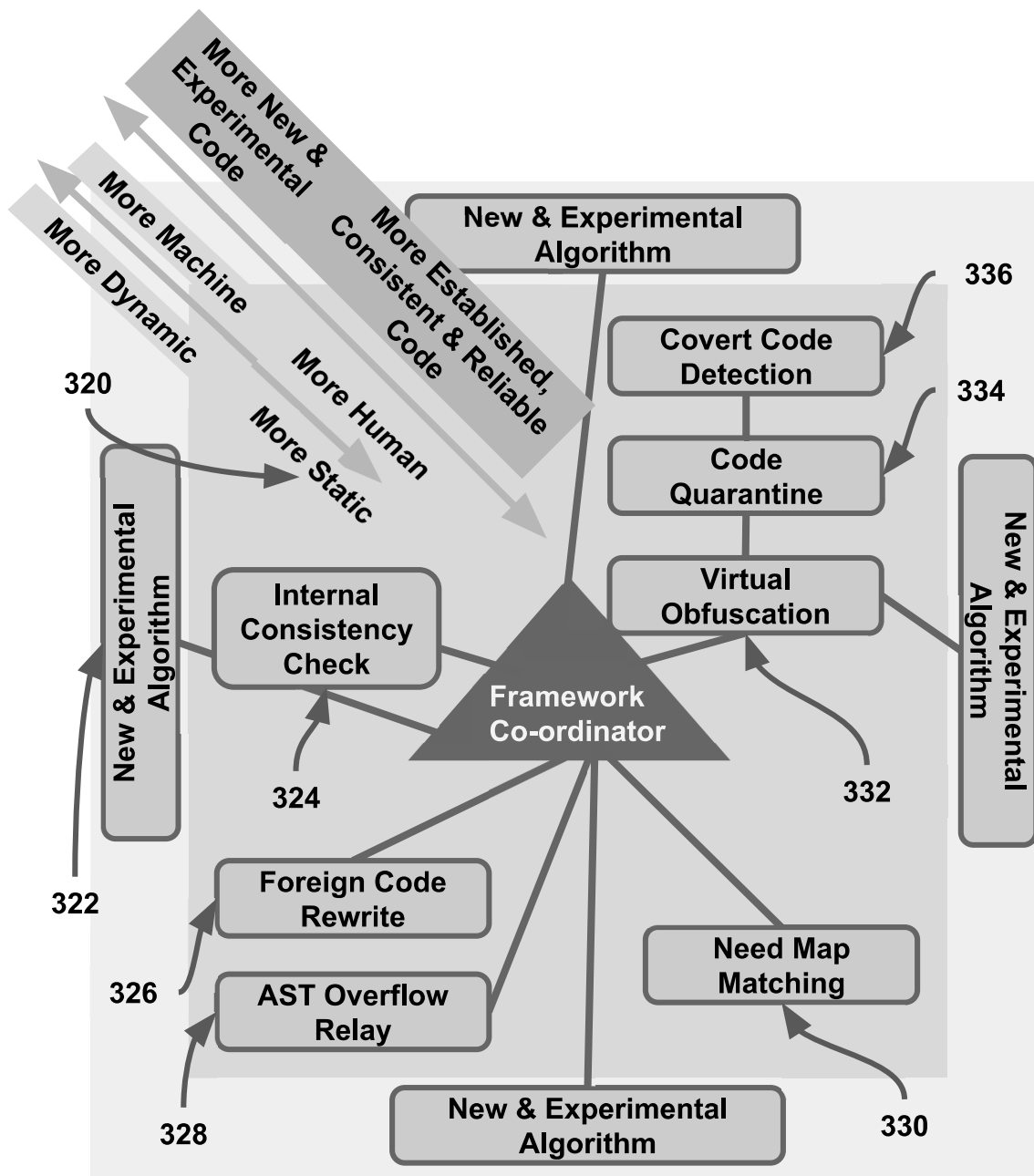


FIG. 71

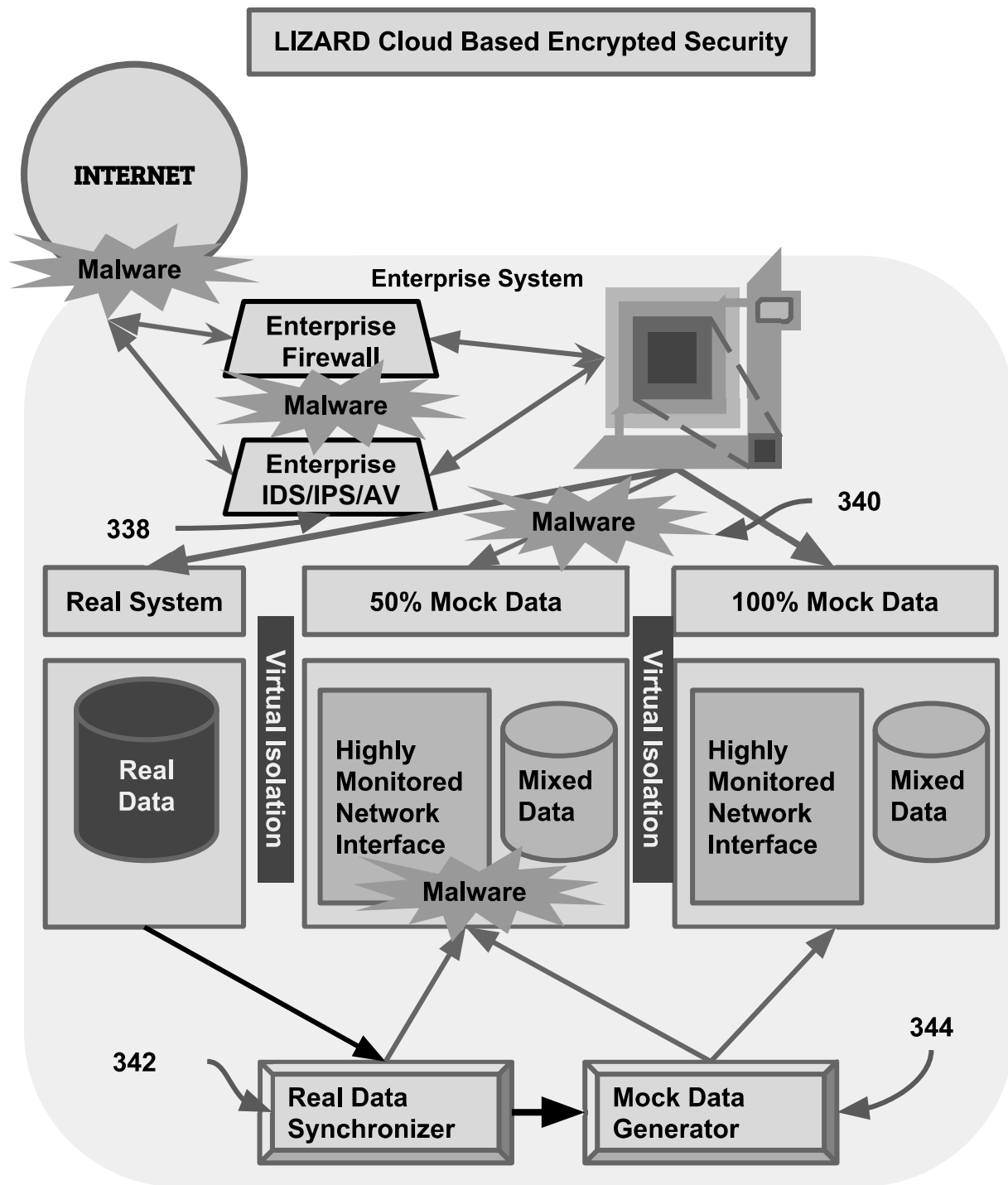


FIG. 72

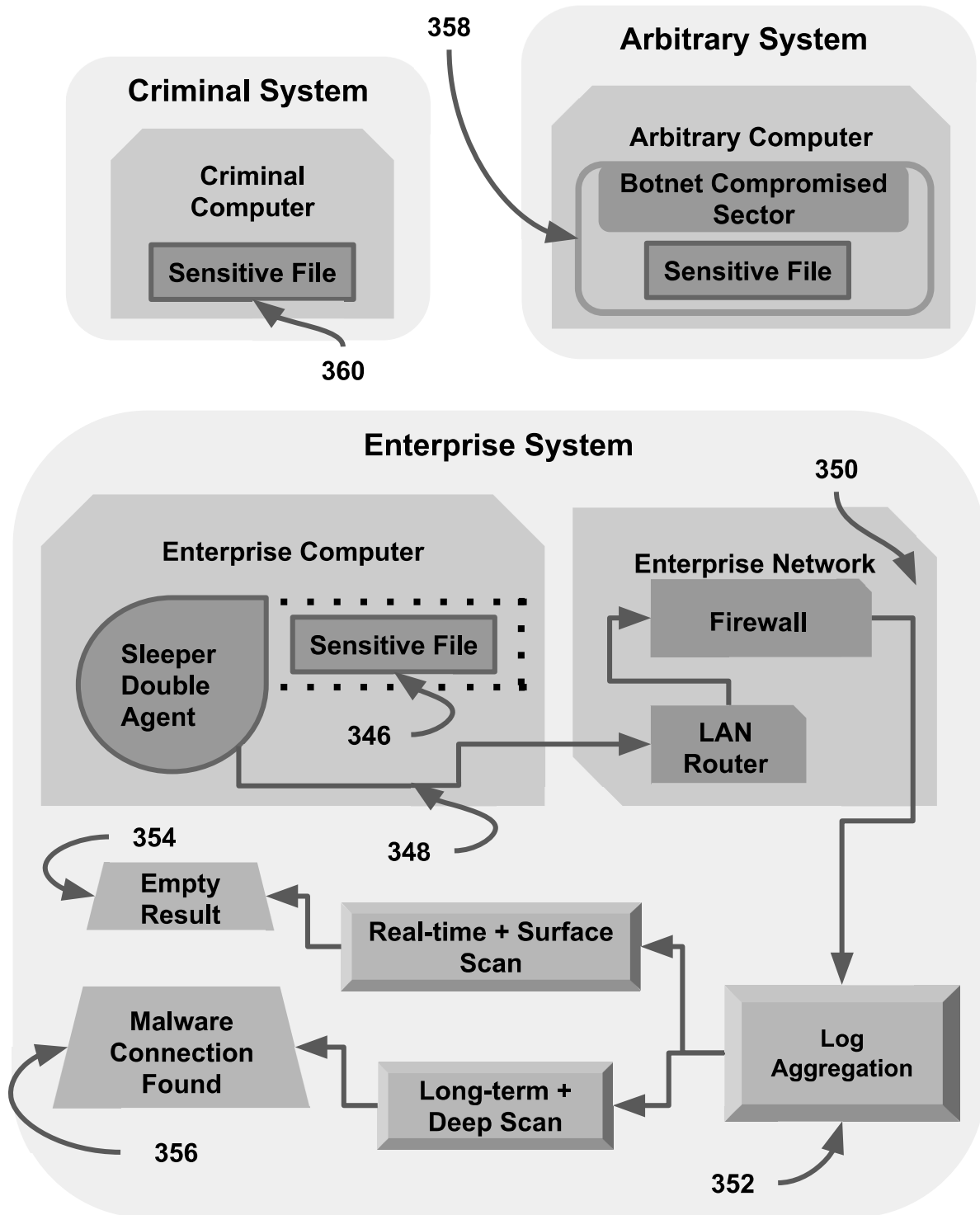


FIG. 73

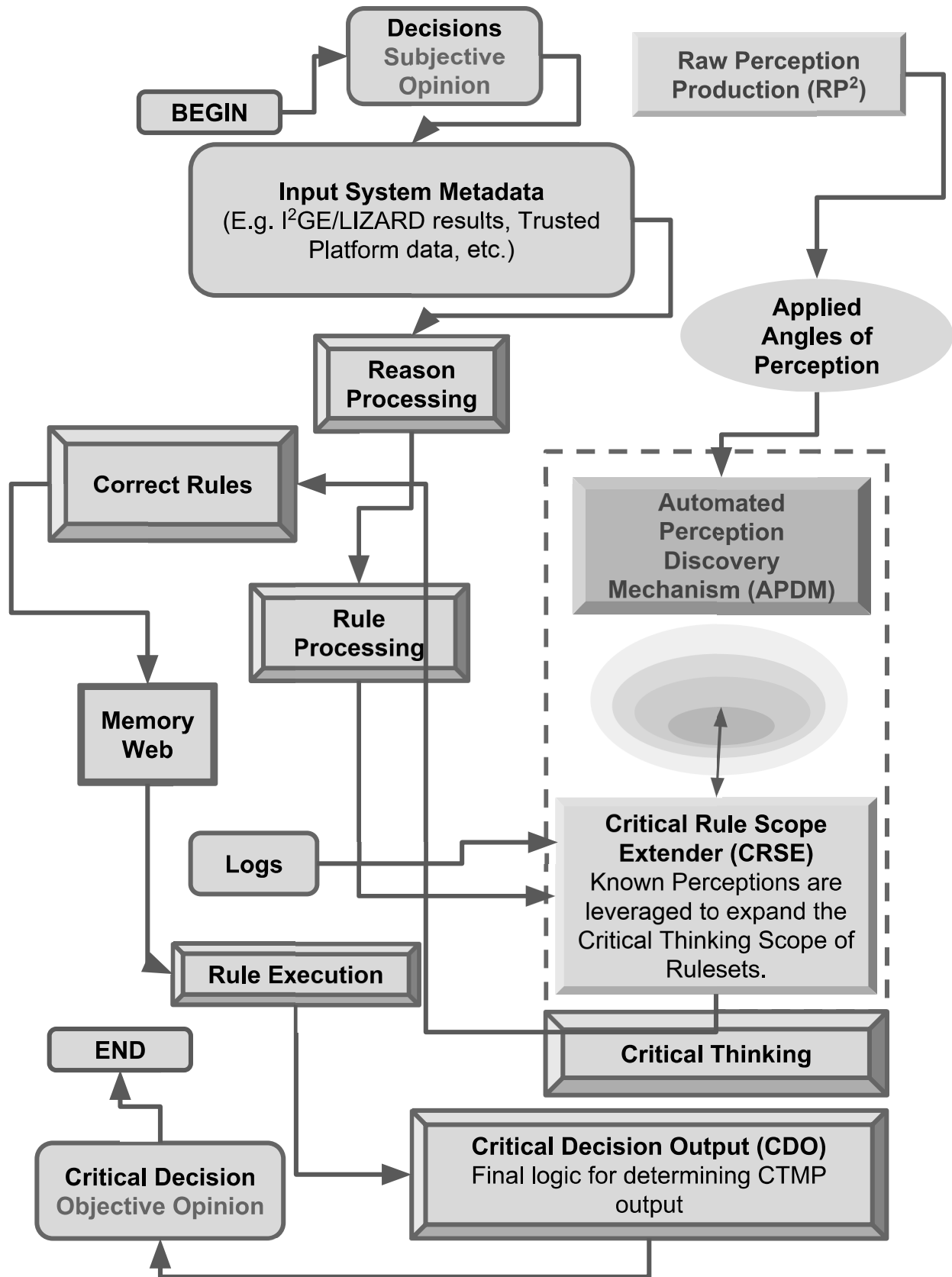


FIG. 74

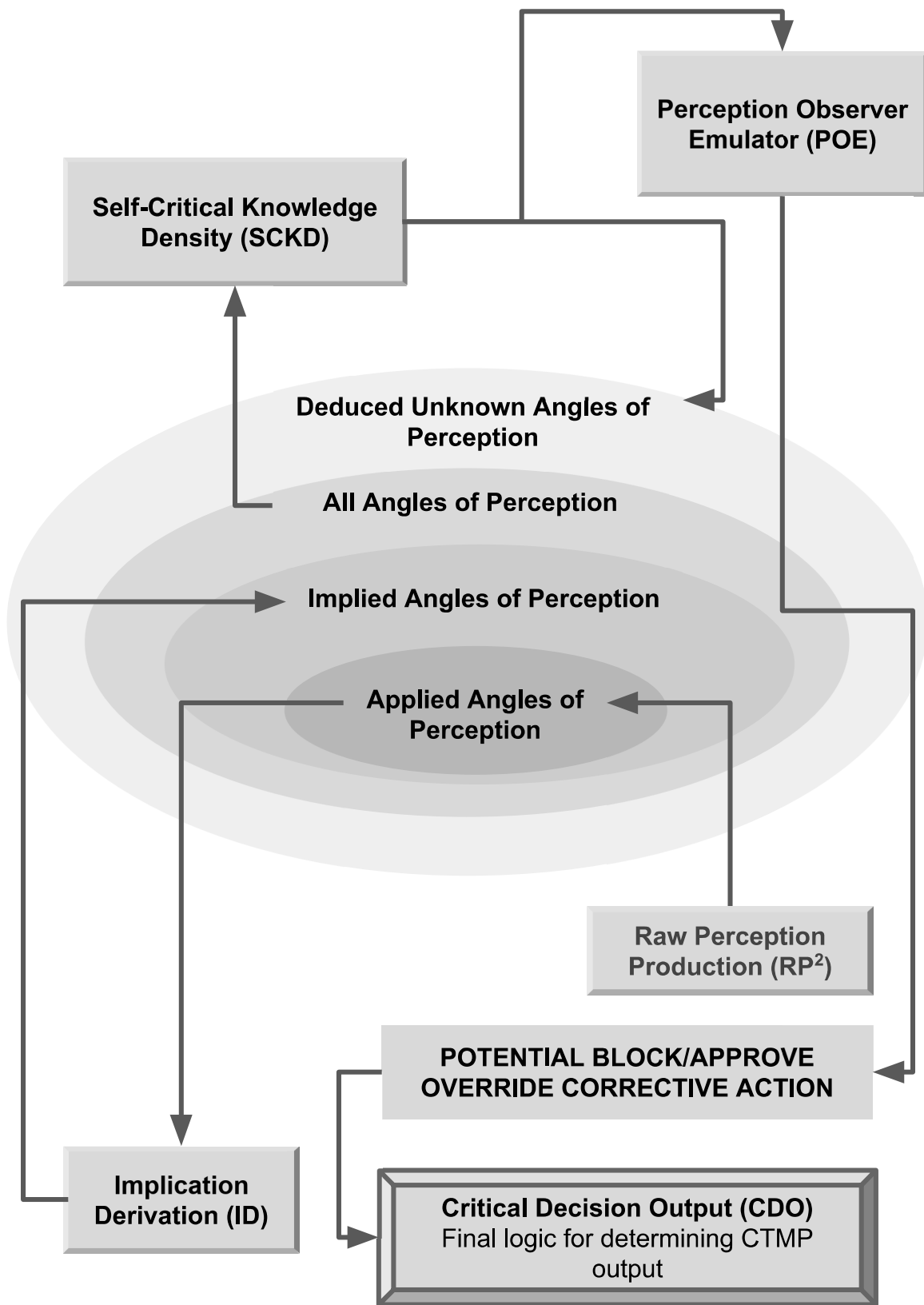


FIG. 75

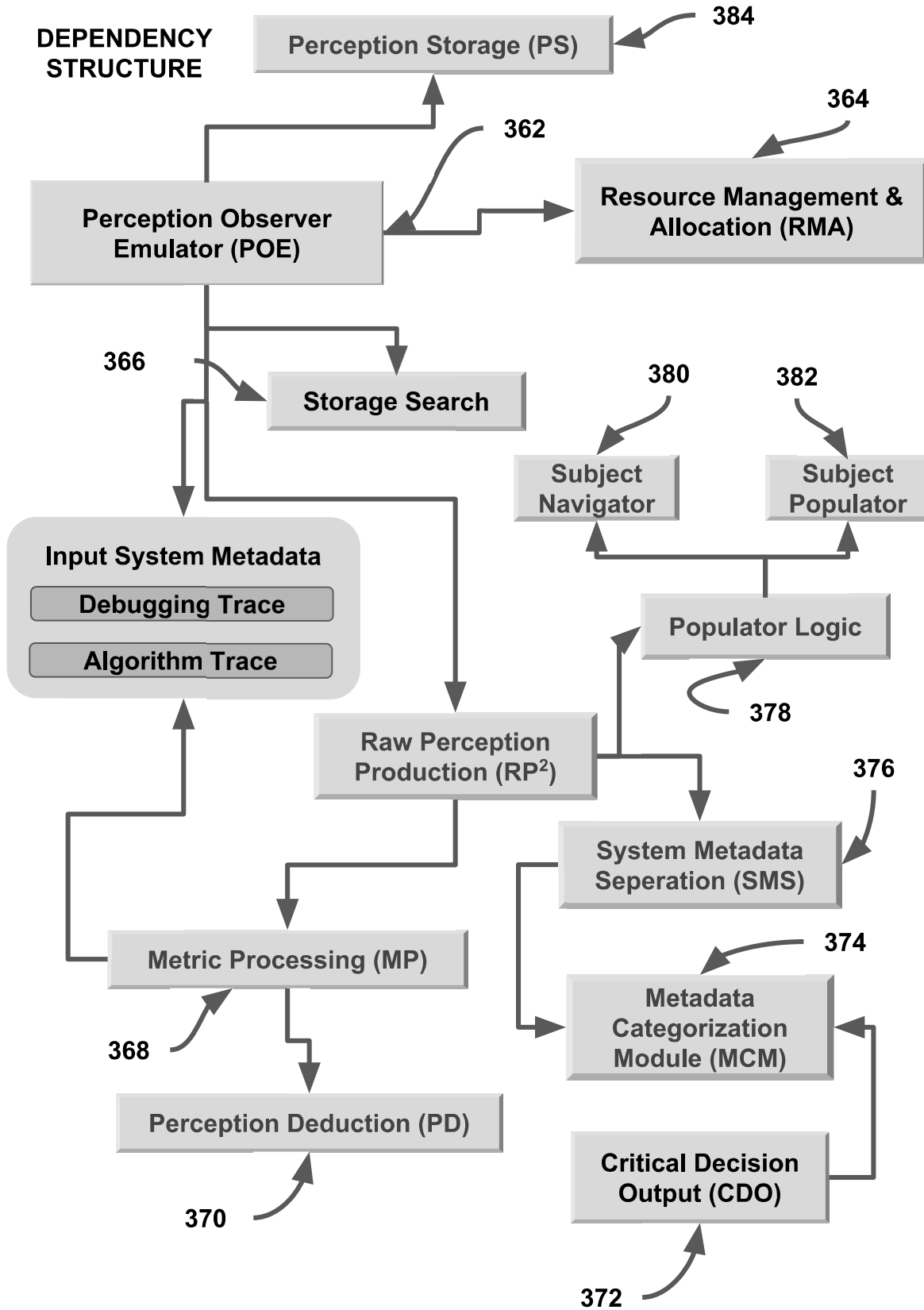


FIG. 76



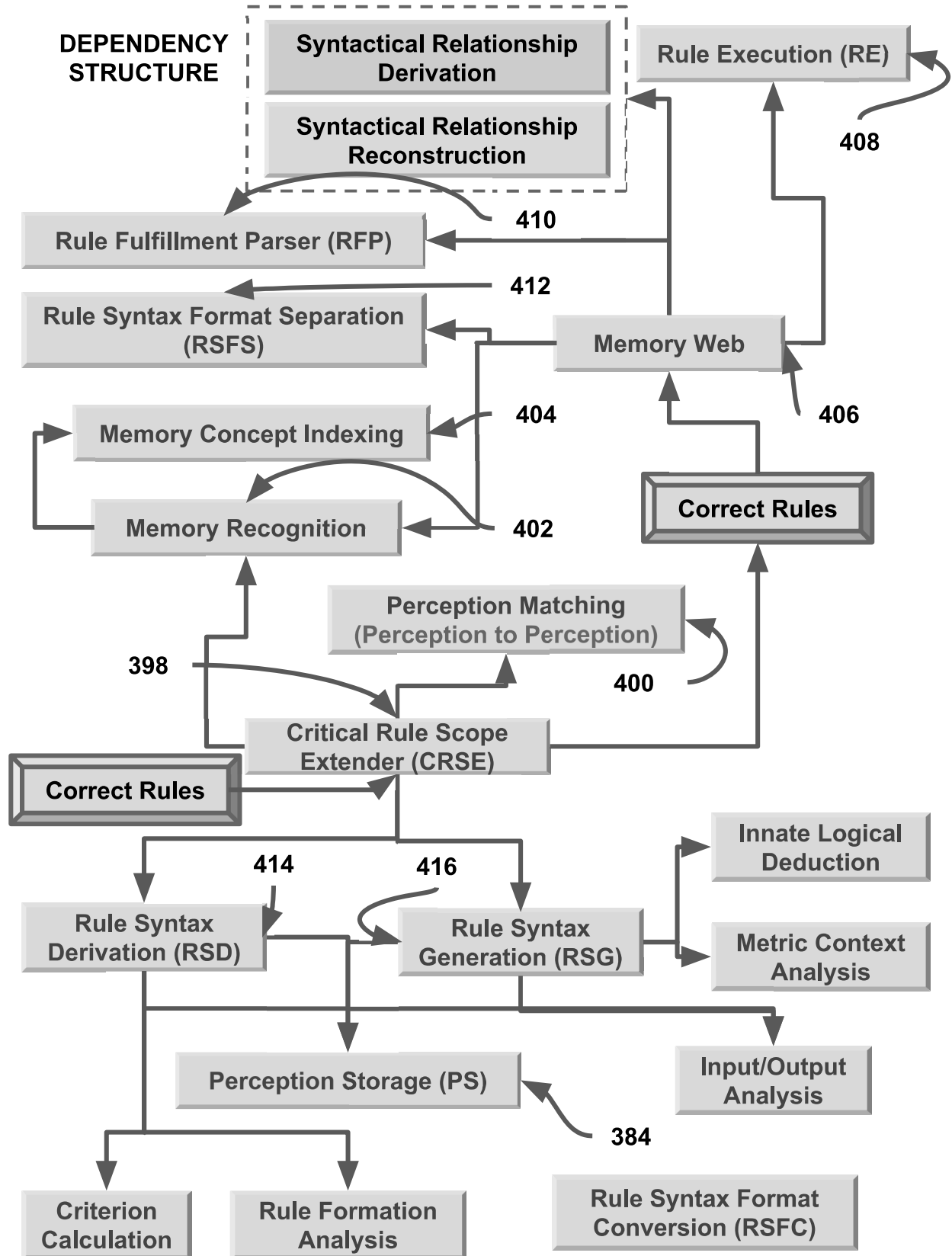


FIG. 78

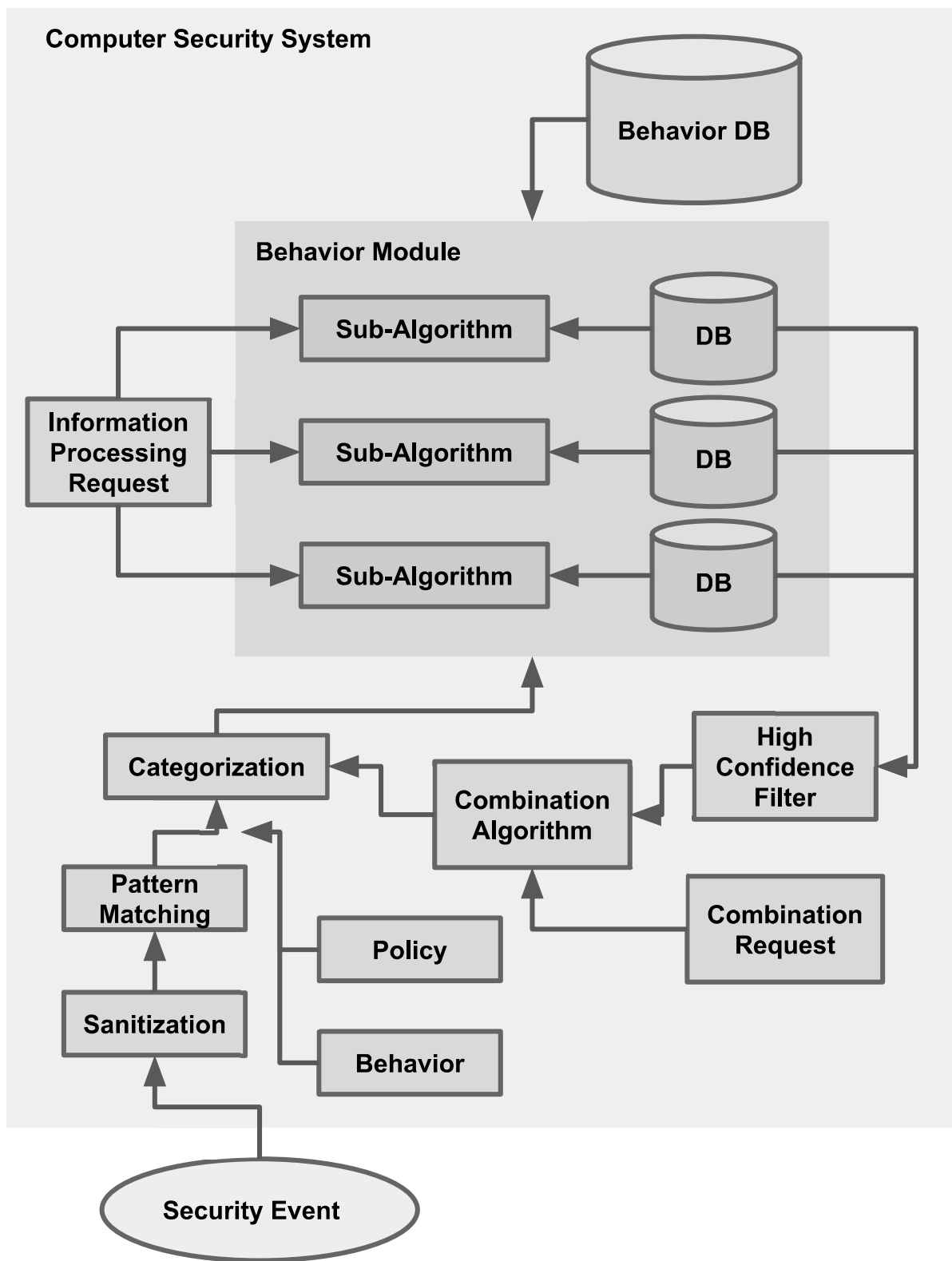
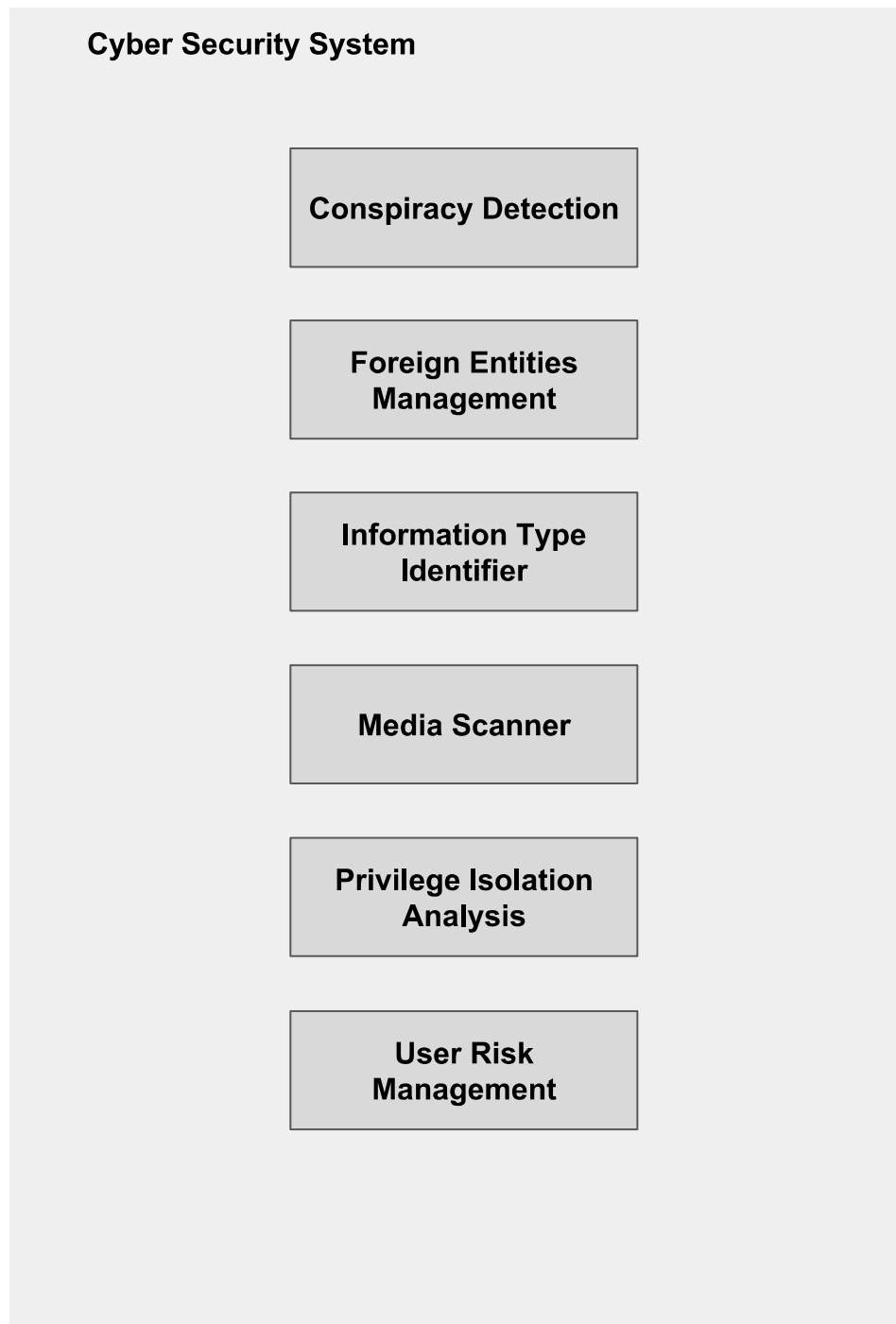


FIG. 79

**FIG. 80**

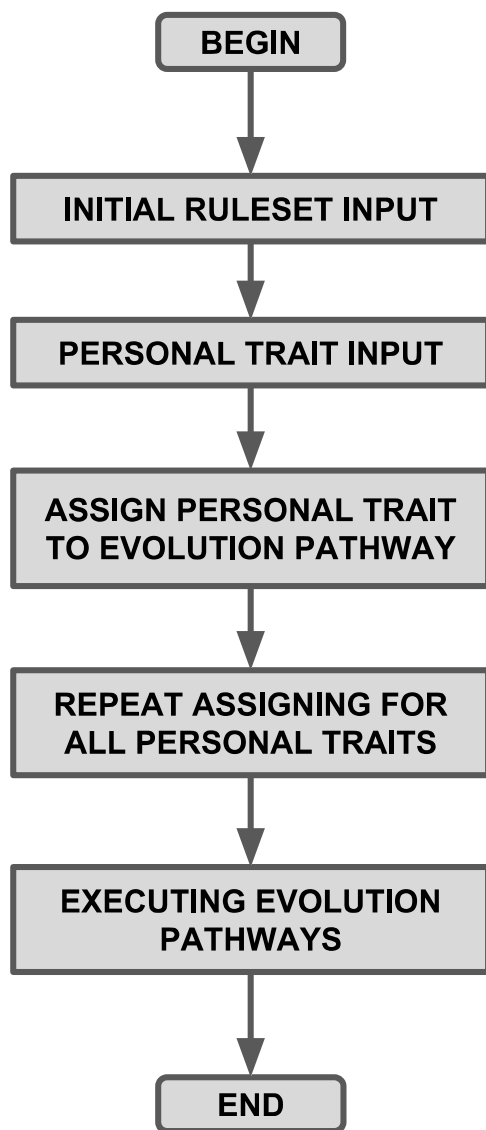


FIG. 81