THREAT

MINISTRY OF SECURITY

HUNTING

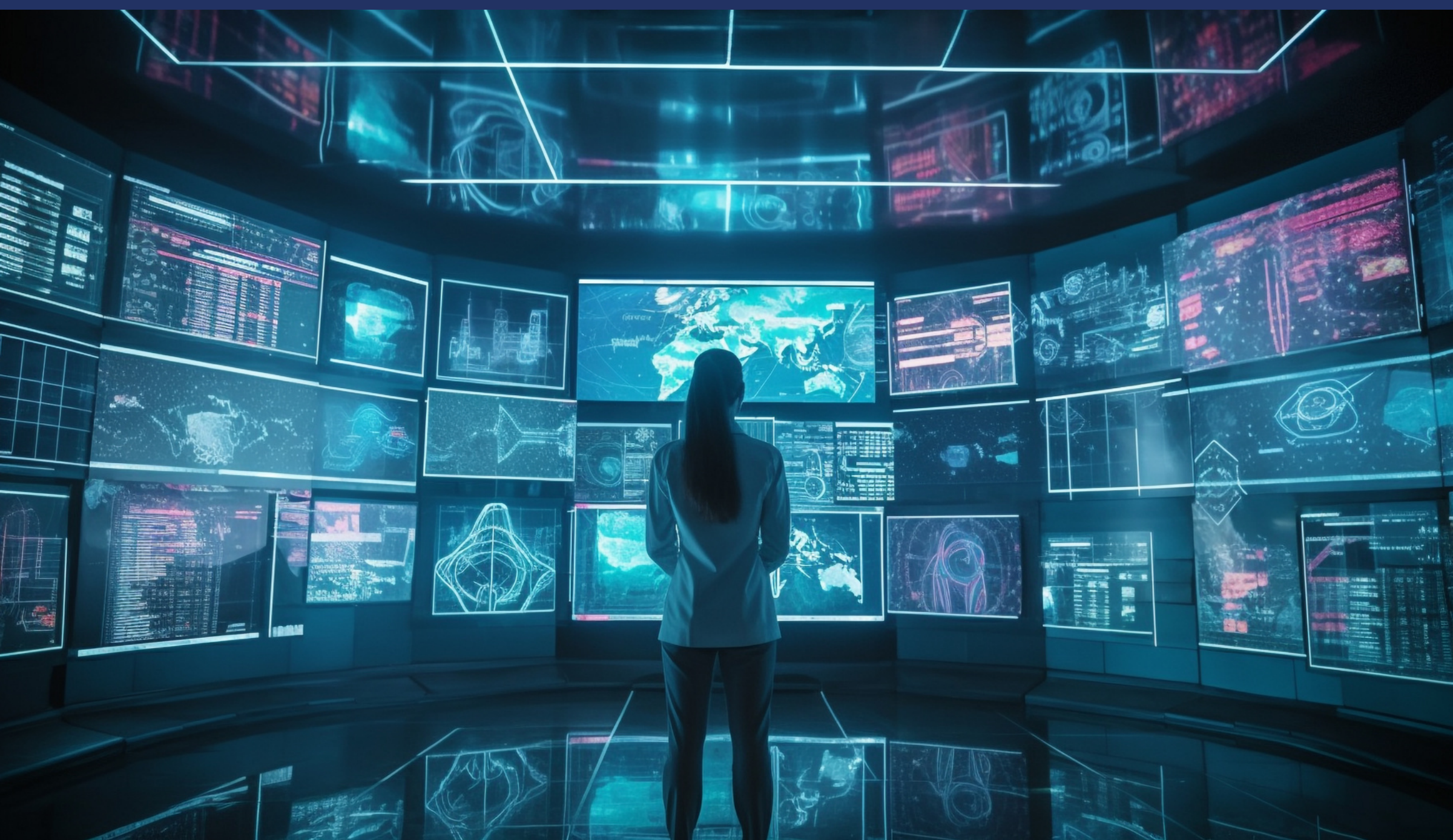
VS

ASSESSMENT

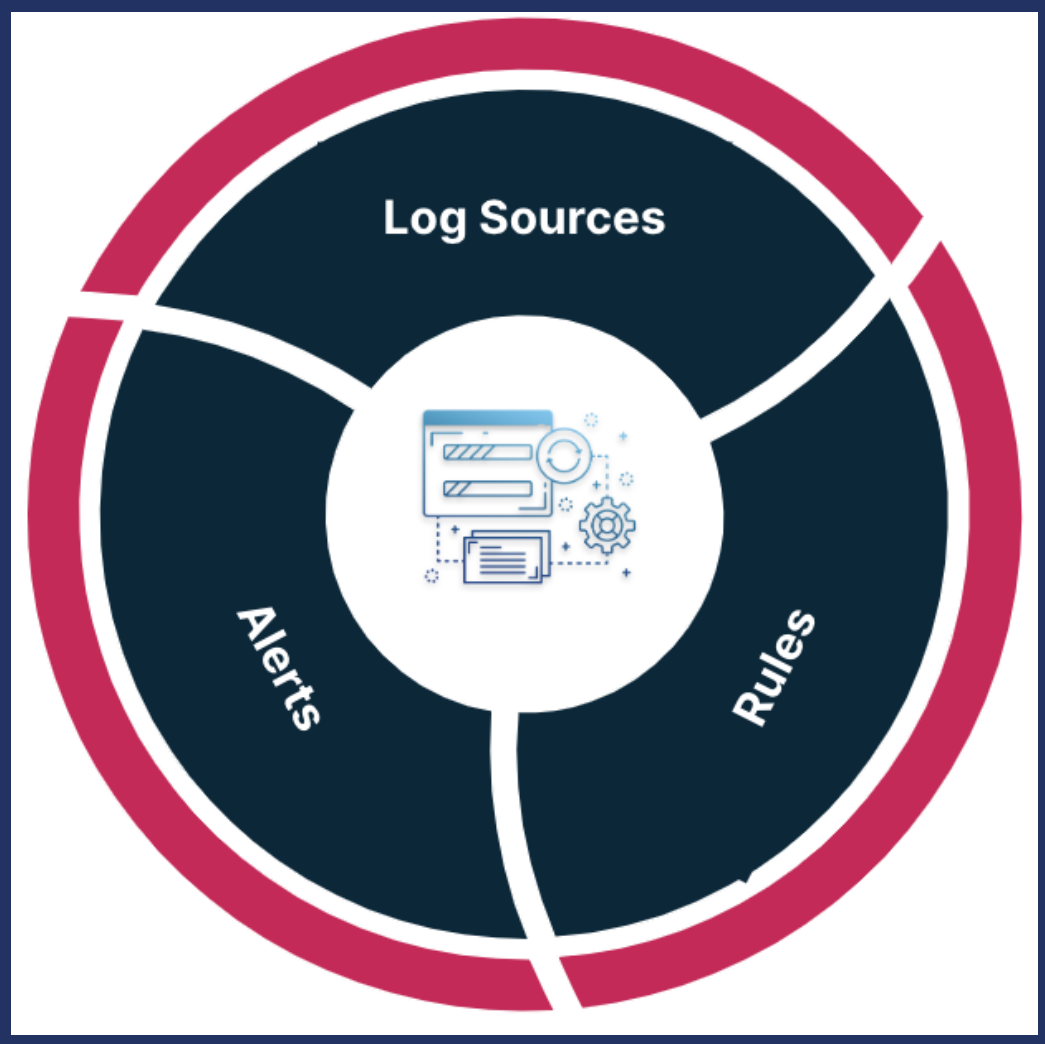
VS

MODELLING

INTELLIGENCE



PREFACE



We always get confused with various threat activities and relate them to threat detection alone.

Threat Detection involves monitoring and analyzing various sources of information, such as network traffic, system logs, user behavior, and physical security measures, to uncover signs of suspicious or anomalous activities.

It sets rules and conditions. Once a condition is met, an alert is triggered.

→

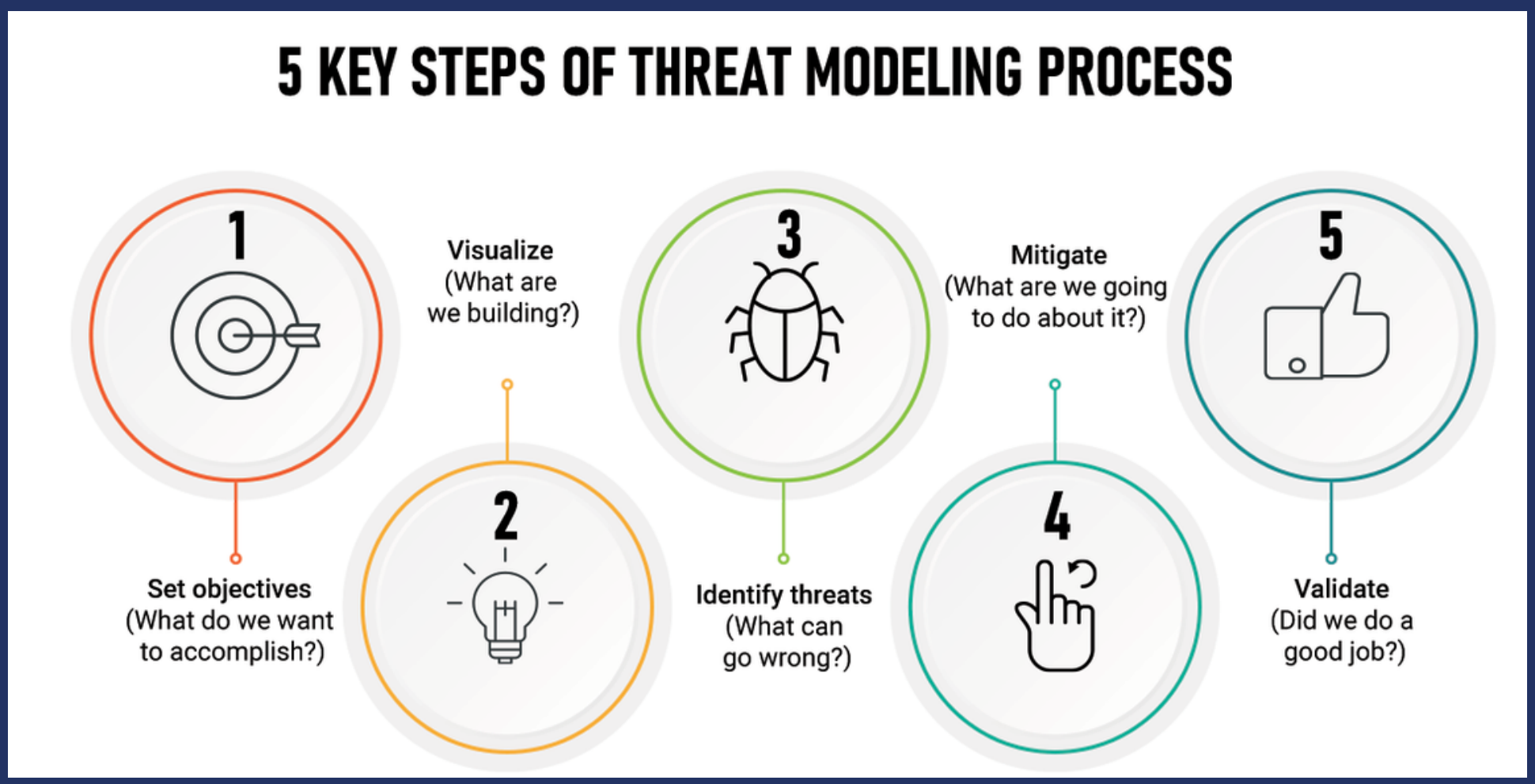
THREAT HUNTING

Threat hunting is a proactive approach aimed at actively searching for attacks (past and present) within an organization's networks, systems, or applications.

Based on suspicious activity, it formulates a hypothesis. These hypotheses are formulated by security experts using a creative and flexible methodology, then verified against a global log of events from endpoints around the world.

→

THREAT MODELLING

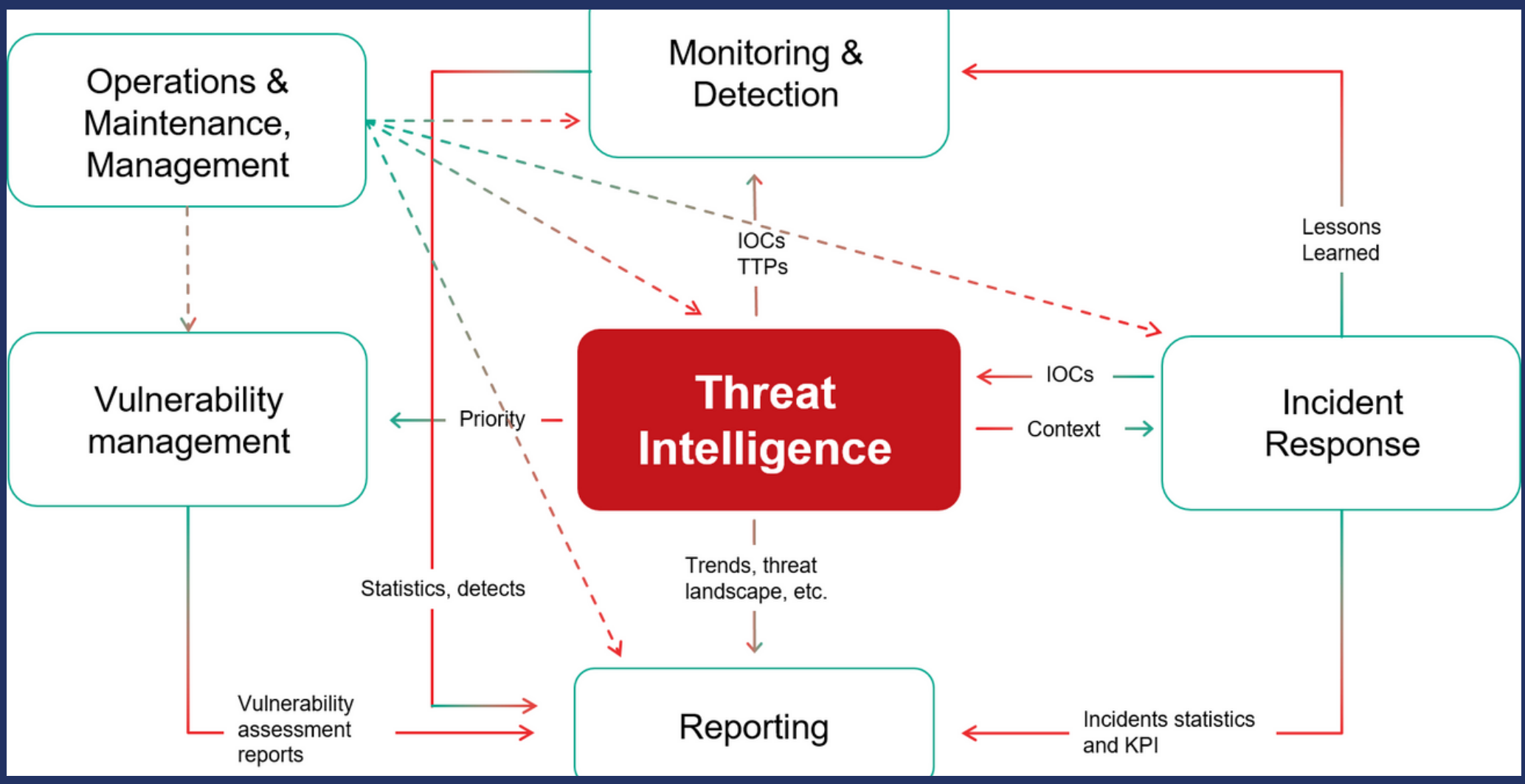


Threat modeling is defined as the process of proactively identifying and addressing potential threats to an organization's systems .

Typically, organizations conduct threat modeling during the design stage (but it can occur at other stages) of a new application to help developers find vulnerabilities and become aware of the security implications of their design, code, and configuration decisions.

→

THREAT INTELLIGENCE

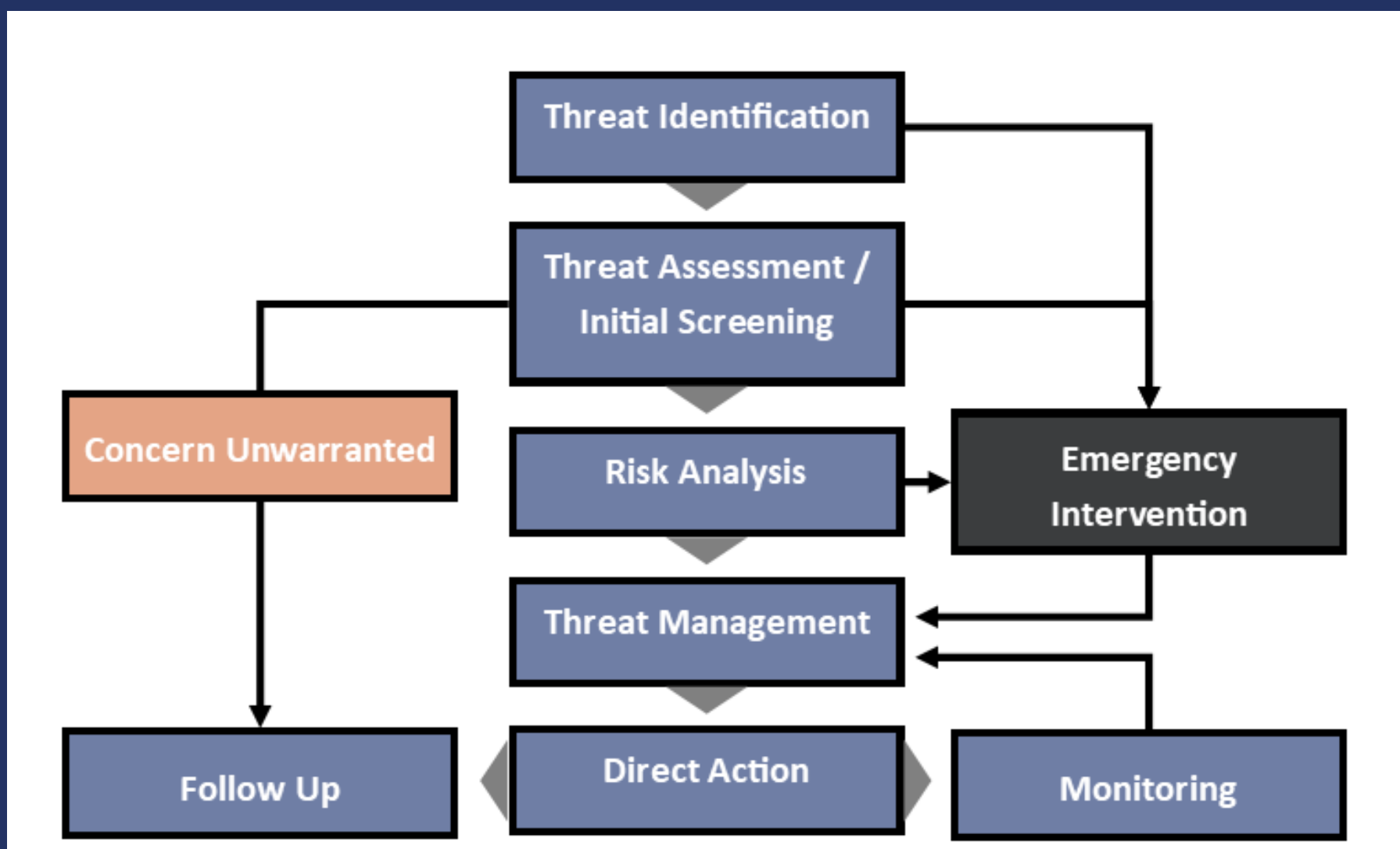


Threat intelligence refers to the collection, analysis, of information about the threat landscape, including the tactics, techniques, and procedures (TTPs) employed by cybercriminals and threat actors.

It involves gathering data from various sources, such as security vendors, open-source intelligence, dark web monitoring, and internal logs, and then processing and analyzing that data to extract actionable insights.

→

THREAT ASSESSMENT



Threat assessment refers to the process of identifying, evaluating, and analyzing potential threats or risks to individuals, organizations, or systems and enhance security

It involves gathering information, conducting assessments, and making informed judgments about the severity and likelihood of specific threats.

DID YOU LIKE OUR PLAYBOOK
AND IF YOU NEED MORE FREE

TRAININGS | CHECKLISTS
WHITEPAPERS | TEMPLATES

FOLLOW US ON

MINISTRY OF SECURITY

SECURITY & PRIVACY
MADE EASY