MENA Information Security Conference 2017

On the Verge :

Combating Cyber Threats leveraging Threat Intelligence, Faster Detection & Automated Response

Adaptive Security Strategy for SOC

Ramy AlDamati

Principle CyberSecurity Solution Architect

Kaspersky Lab Middle East Africa and Turkey

KASPERSKY lab

Global CyberThreats Landscape

KASPERSKY lab

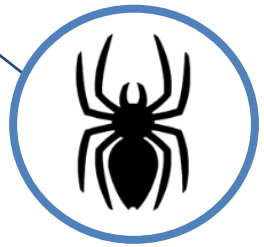
MALWARE EVOLUTION

Looking back at 25 years of malware development

1994

1

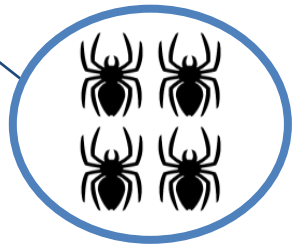
NEW VIRUS
EVERY HOUR



2006

1

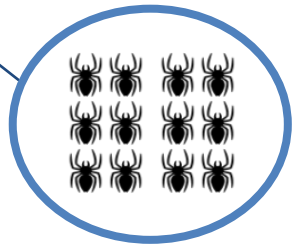
NEW VIRUS
EVERY MINUTE



2011

1

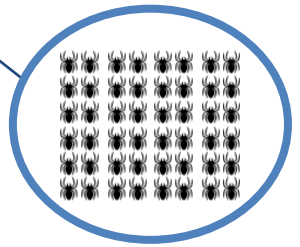
NEW VIRUS
EVERY SECOND



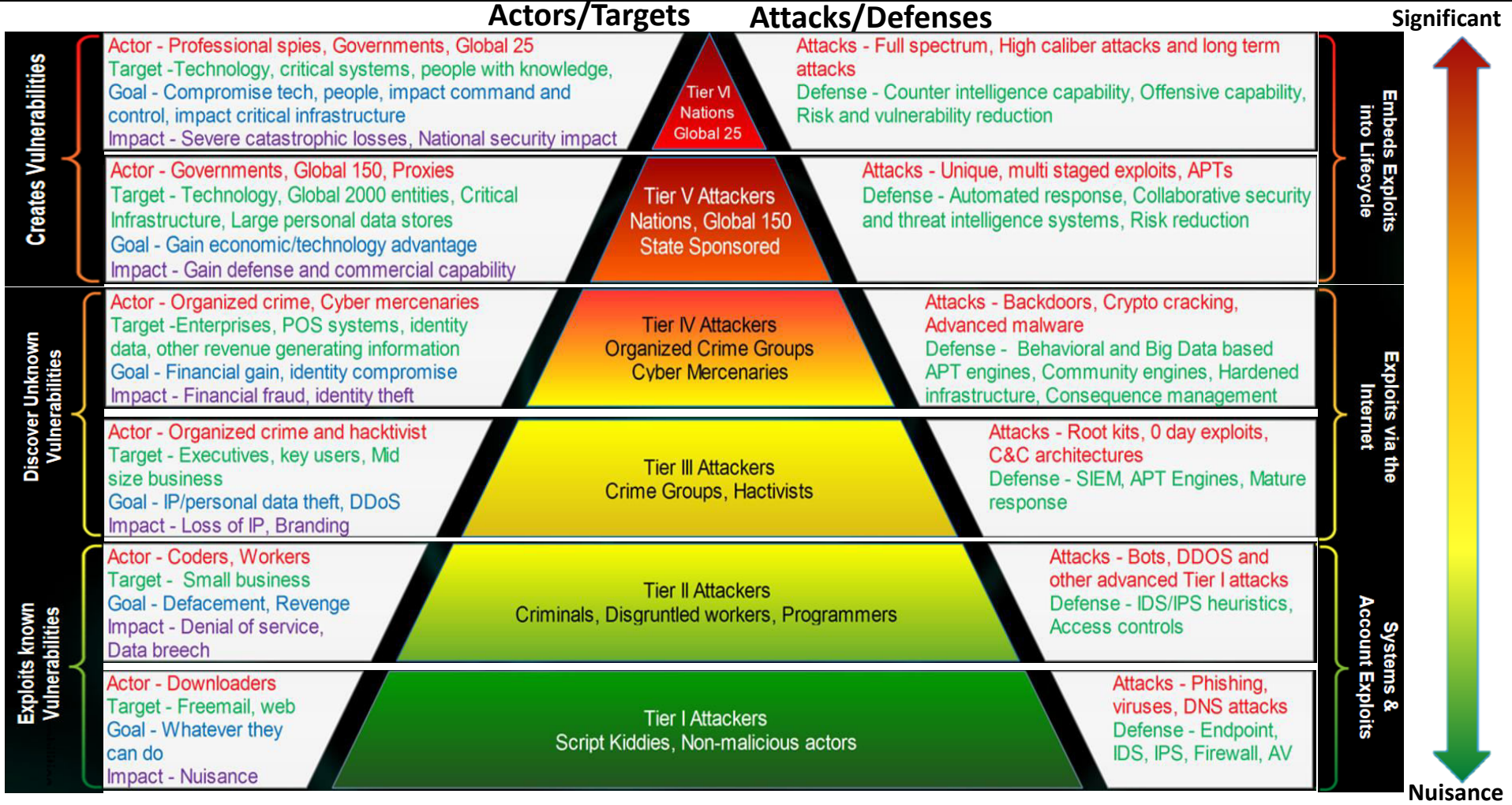
2017

323,000

NEW SAMPLES
EVERY DAY

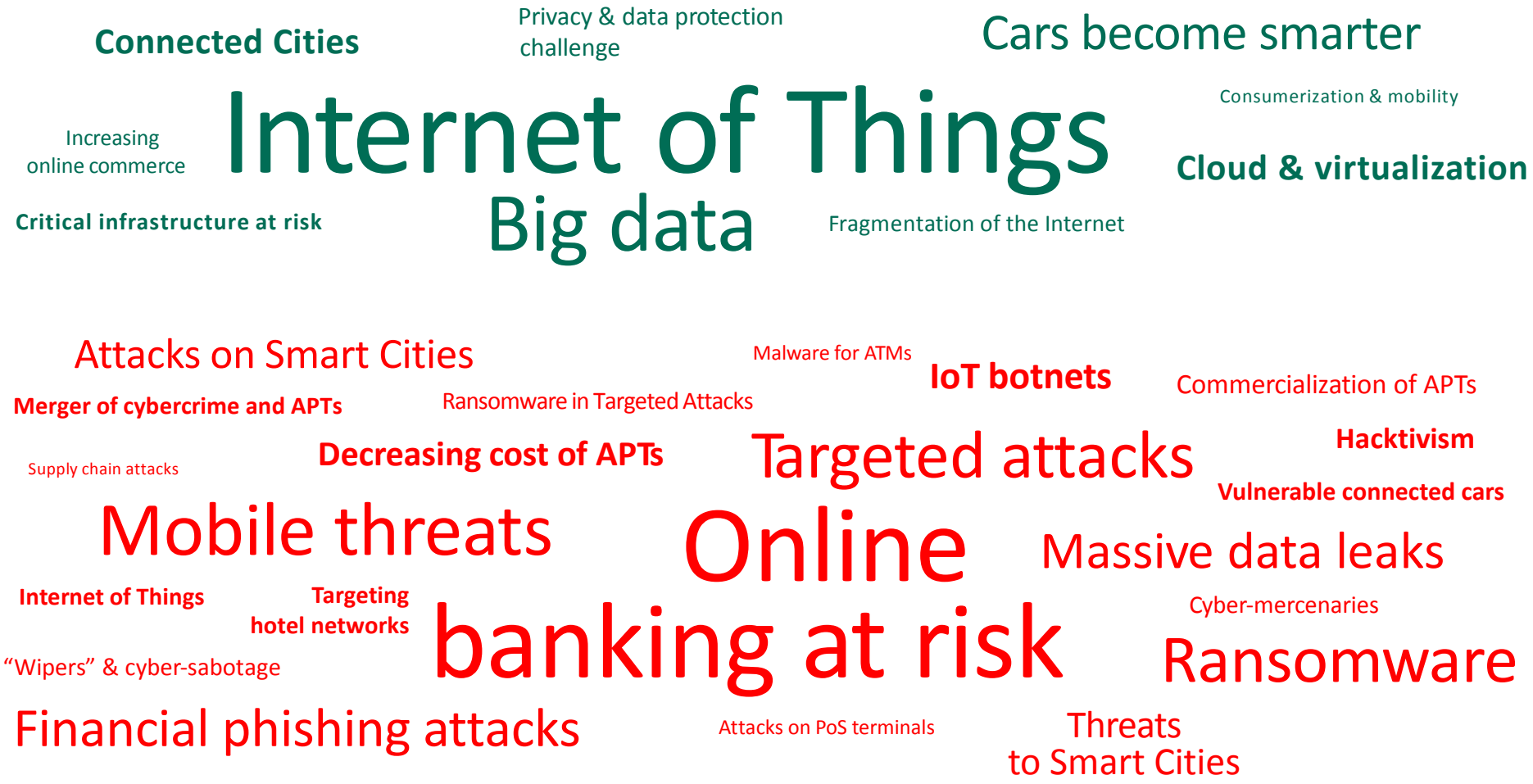


THREAT EVOLUTION



Trends and Threats

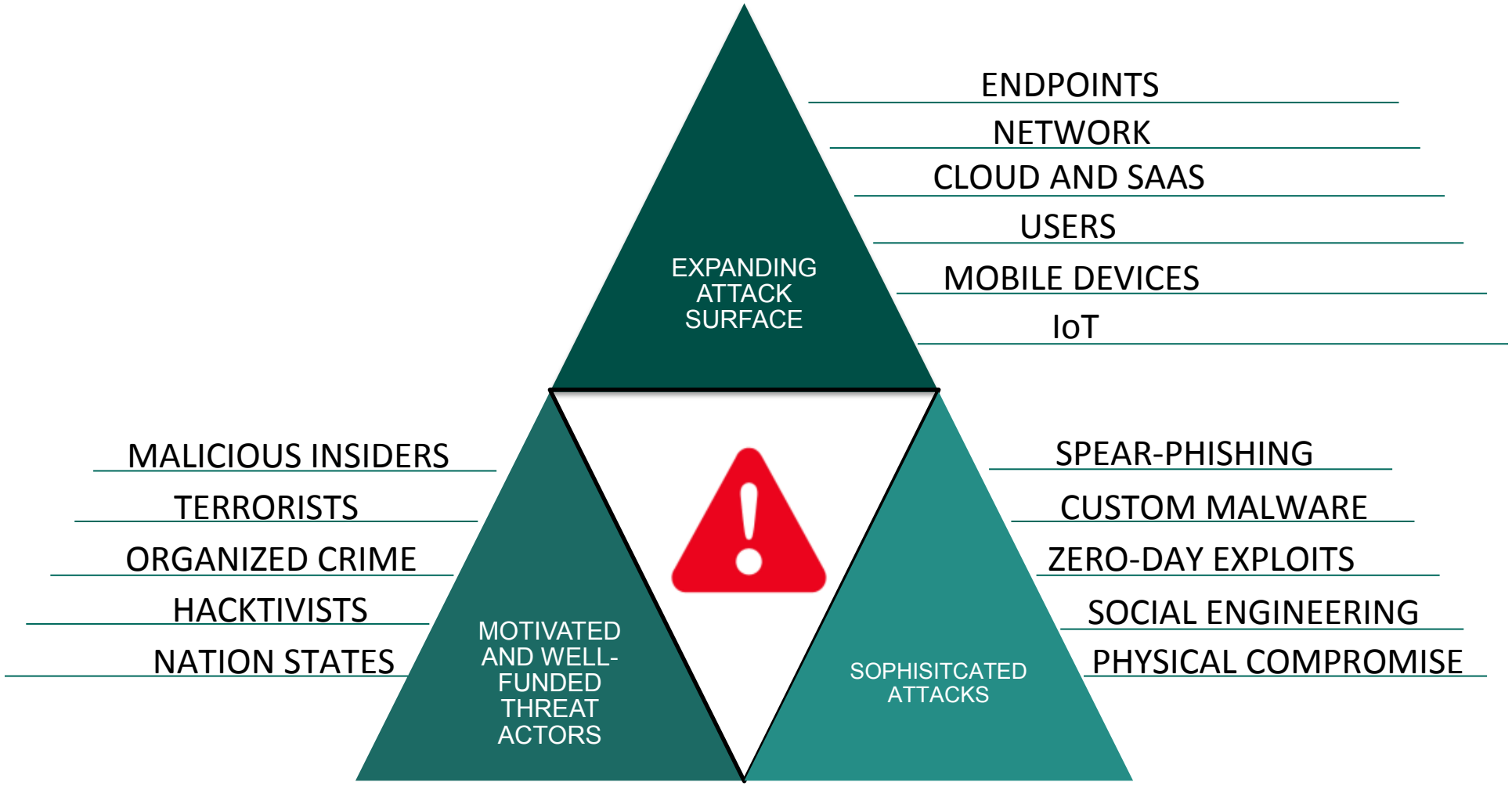
Main GOAL: to understand global **IT Trends** and the **Threats** they bring



MENA INFORMATION SECURITY CONFERENCE 2017

KASPERSKY lab

THE MODERN CYBERTHREAT LANDSCAPE

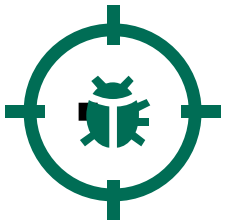


Cybersecurity challenges of «nearest future»

Endpoints Essential

Compliance

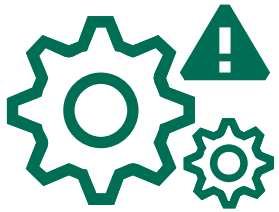
Skills Demand



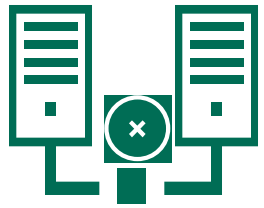
Malware focus

Manual Work

Multiple solutions issue



Advanced Security Complexity



Lack of integration

Security Expert Yesterday – Today – Tomorrow

Role: Security Engineer
Responsibility: building protection
Goal: Prevent the external threats

5 - 10 years ago

Role: Security Analyst
Responsibility: monitor and react
Goal: Unify the processes and automate routine

Today

Role: Threat Hunter
Responsibility: discover threats and manage advanced engines
Goal: Protect the business

Tomorrow???

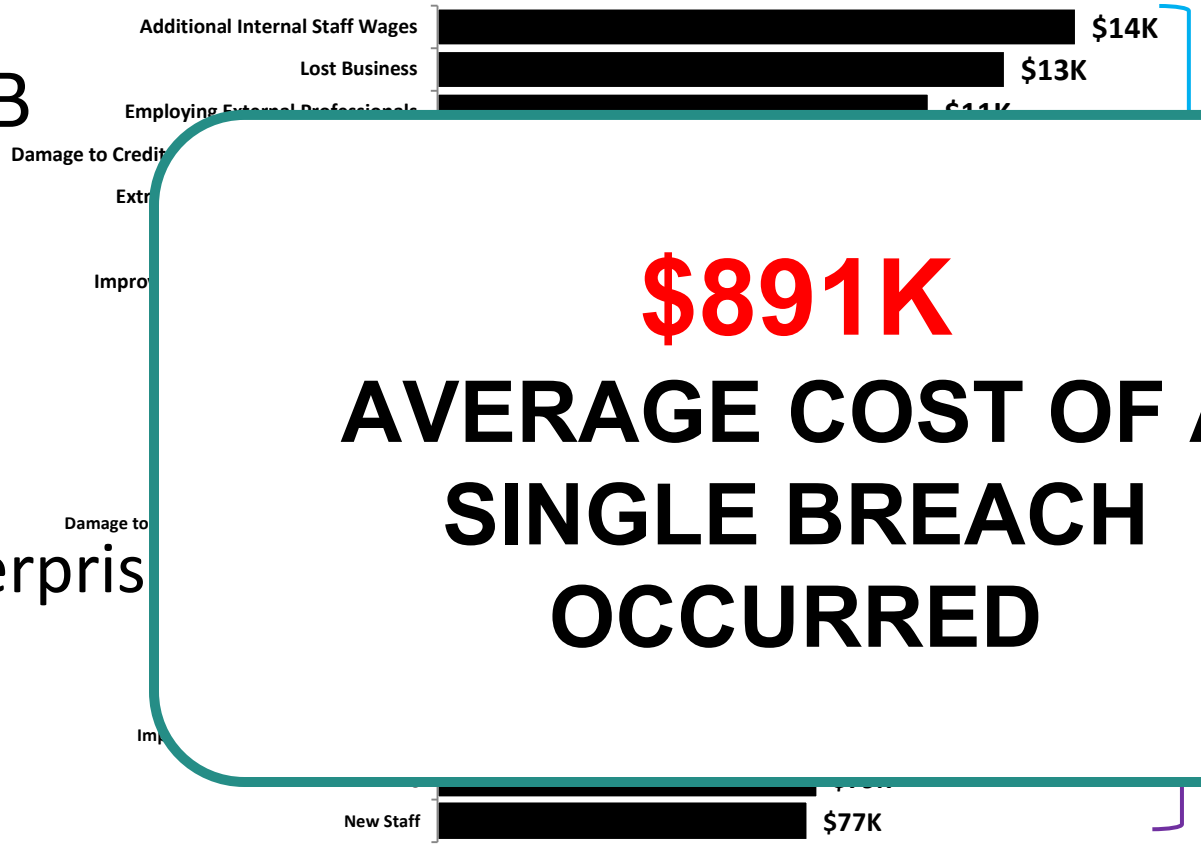
Enterprise Security Trends

KASPERSKY lab

THE AVERAGE FINANCIAL IMPACT OF A BREACH

SMB

Average Total
mpact:
86.5k



$891K

AVERAGE COST OF A SINGLE BREACH OCCURRED

Enterpris

age Total
mpact:
$891k

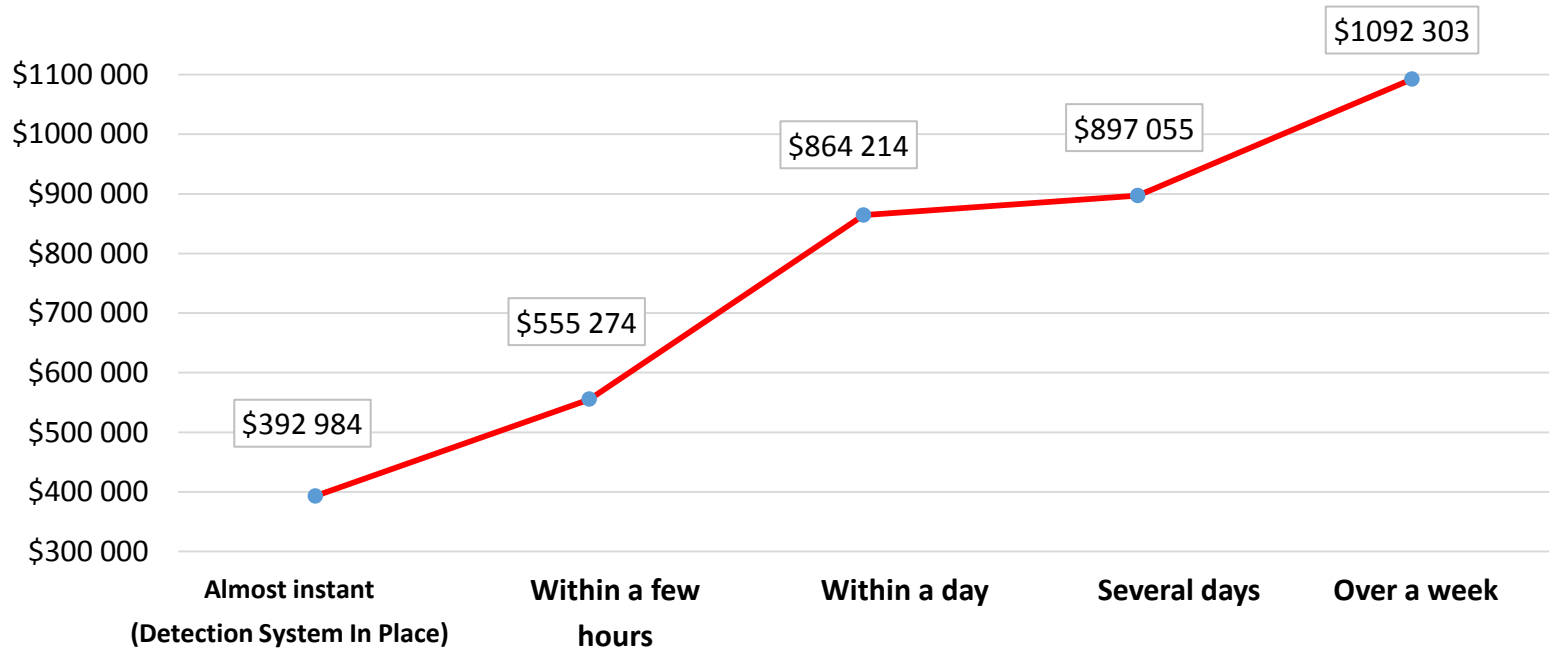
The reallocation of IT staff time represents the single largest source of additional cost for both SMBs and Enterprises

Results from Kaspersky Lab's Corporate IT Security Risks. Survey 2016, conducted worldwide by Kaspersky Lab

Base: 926 SMBs/ 590 Enterprises *Suffering At Least One Data Breach*

Financial impact of security incident

200% **growth of the recovery cost during the first week of discovering a security breach for Enterprises**



***Cost of recovery vs. time needed to discover a security breach for enterprises**

Enterprise Security Trends: External Factors

Most advanced threats using basic vulnerabilities and human factor

Availability and lowering prices leading to Cybercrime-as-a-Service

Attacks on third-party: SMBs can become a part of an attack chain

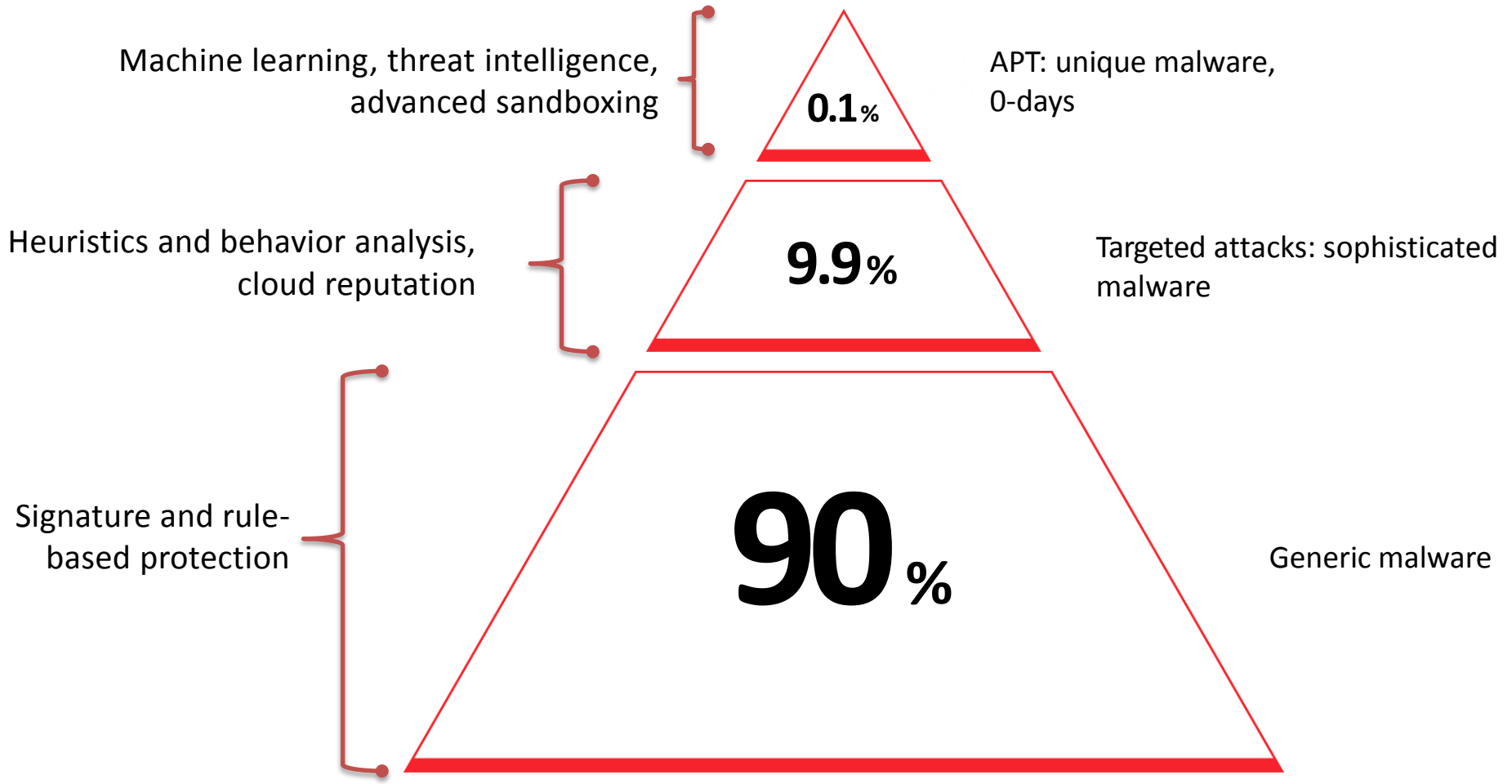
Enterprise Security Trends: Internal Factors

Growing IT sophistication results in visibility gap and lack of operational information

An average targeted attack stays undetected for more than 214 days

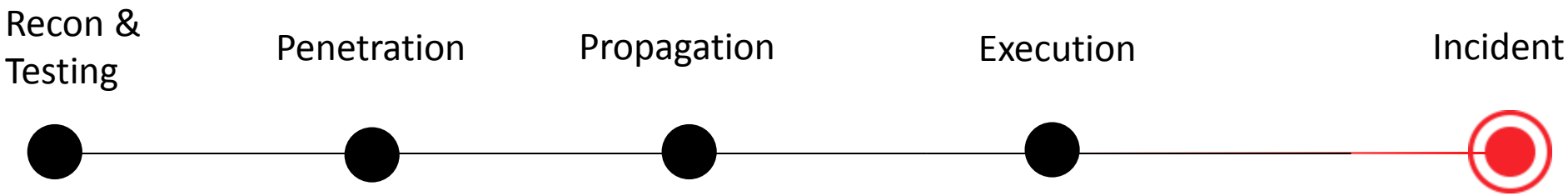
Perimeter security is overestimated

The smallest percentage of threats creates the highest risk



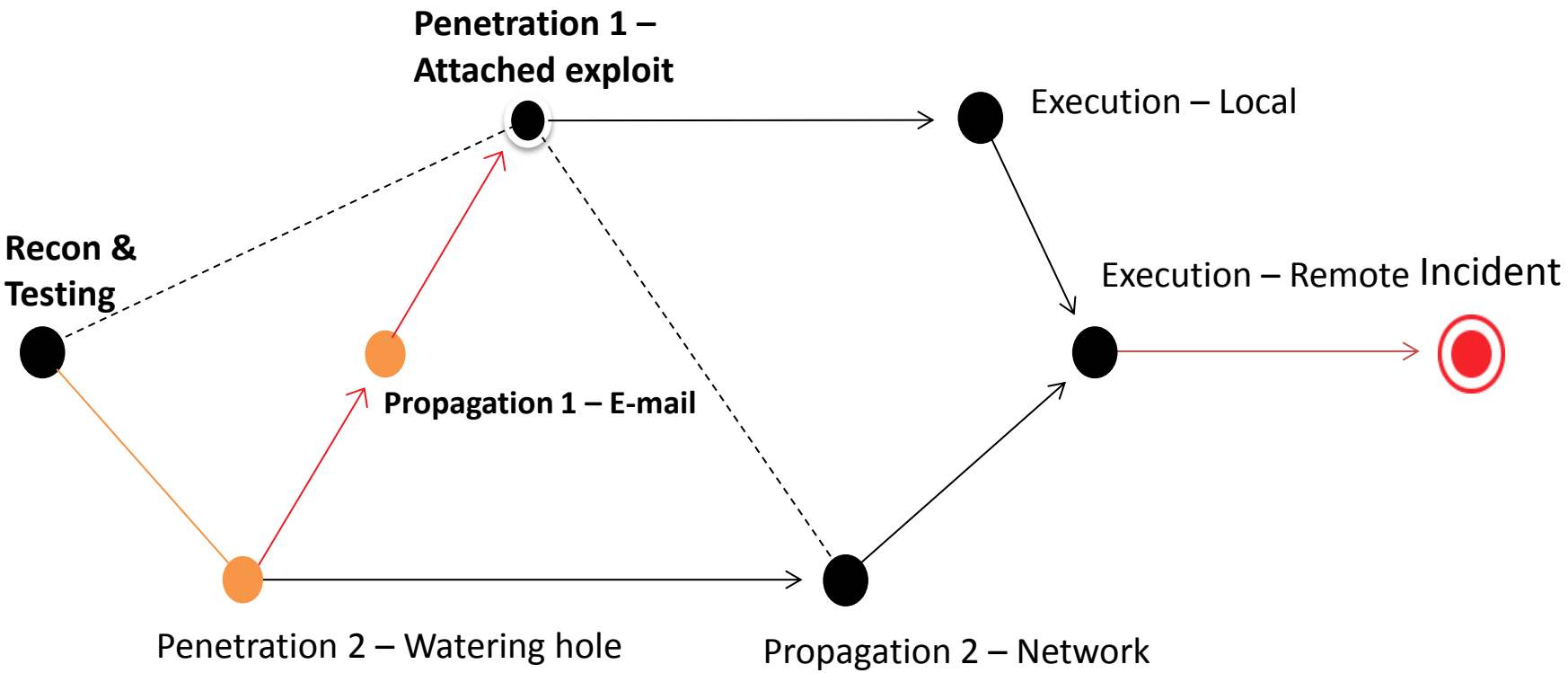
TARGETED ATTACK KILL CHAIN: THEORY VS REALITY

- **In theory… pretty straightforward:**

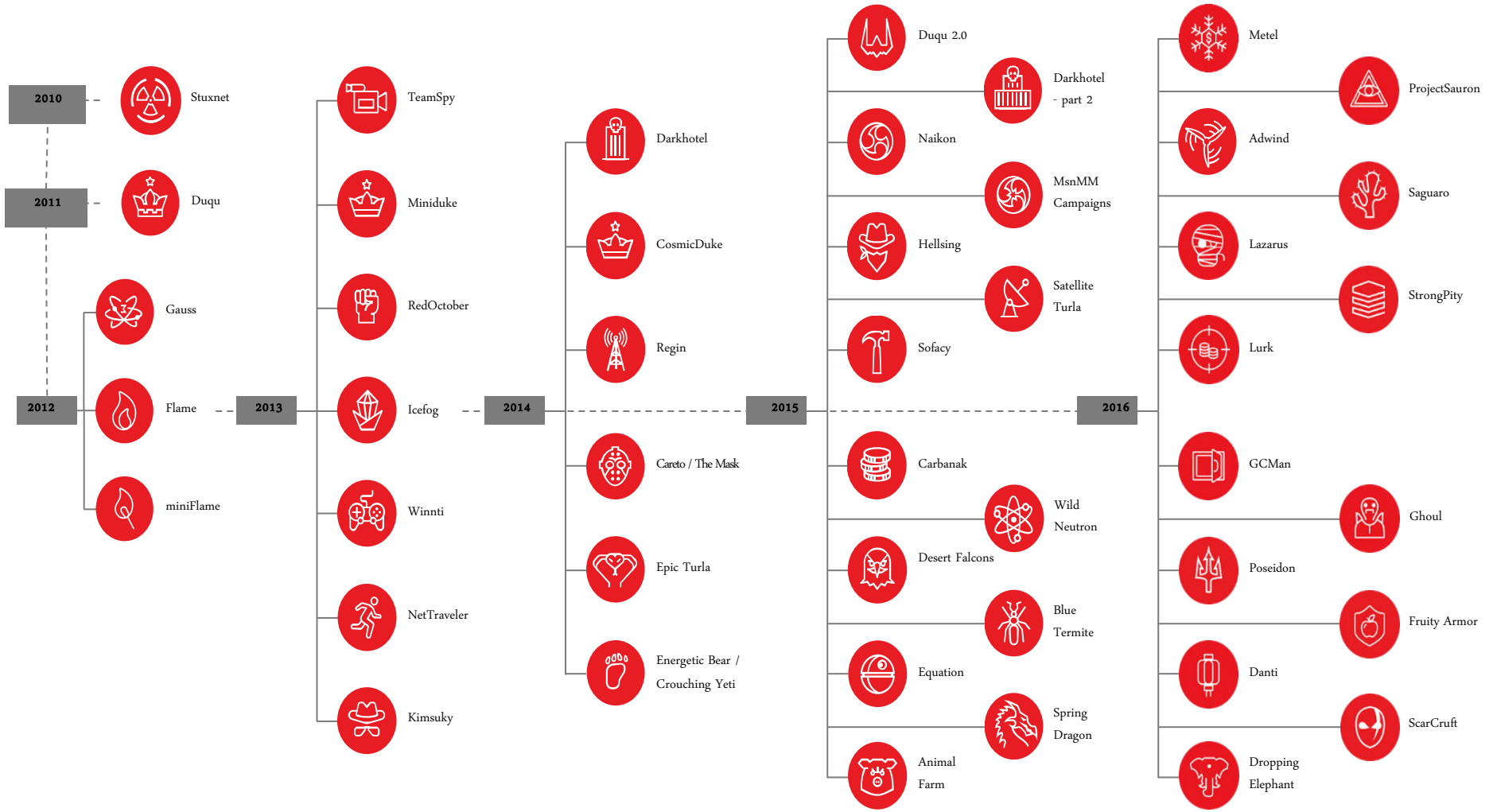


TARGETED ATTACK KILL CHAIN: THEORY VS REALITY

- **In reality… sophisticated and nonlinear ☹**



Targeted Attack Groups rapidly increased



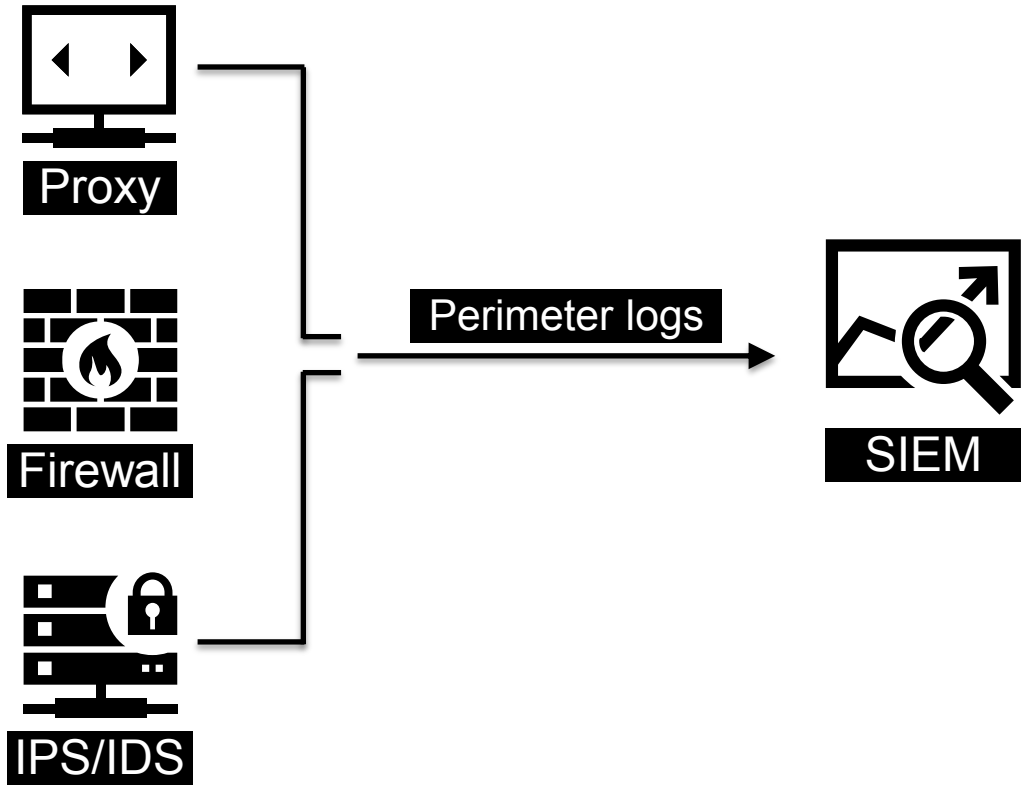
MENA INFORMATION SECURITY CONFERENCE 2017

KASPERSKY lab

The New Era of SOC

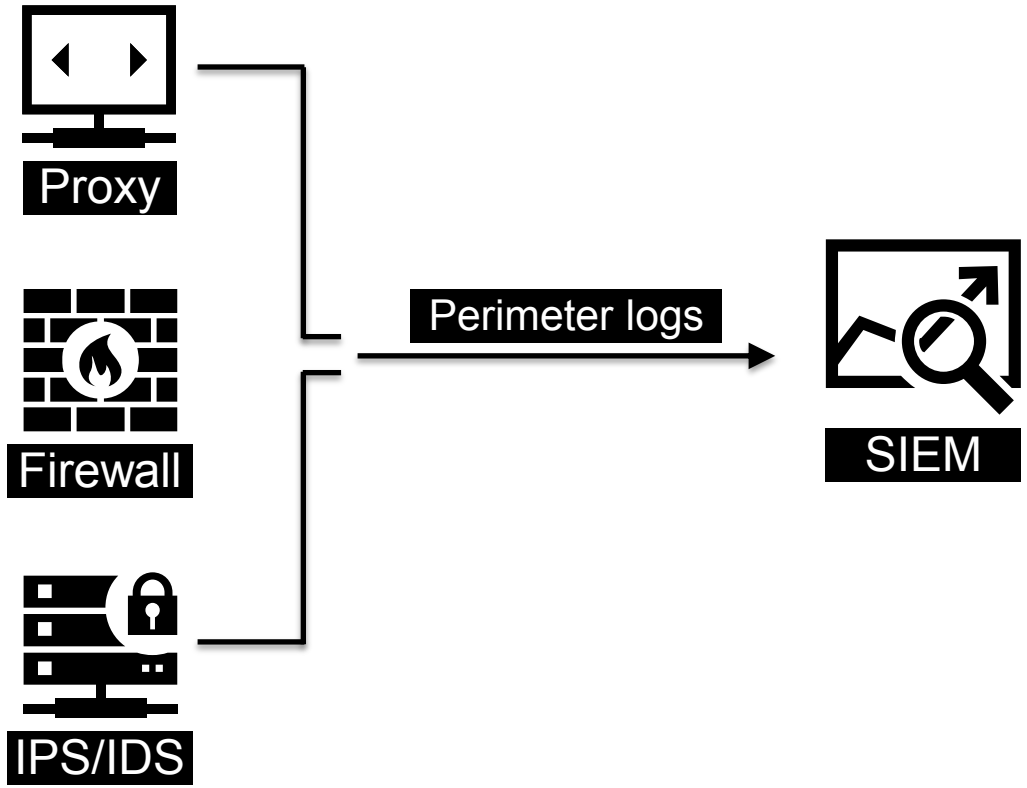
KASPERSKY lab

TRADITIONAL SOC – Functionality



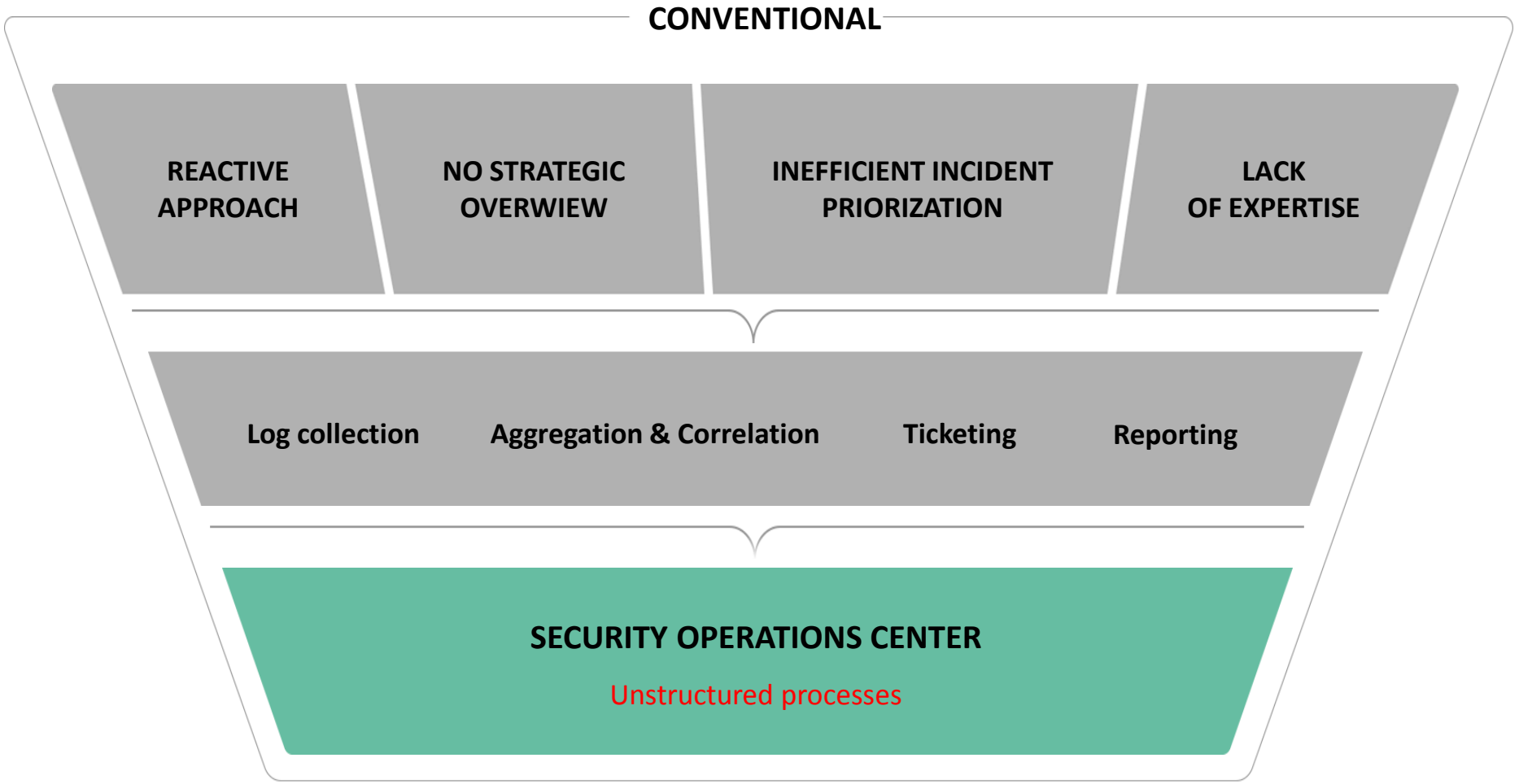
- SECURITY DEVICE MANAGEMENT AND PERIMETER MAINTENANCE
- SECURITY EVENT MONITORING THROUGH SIEM
- INCIDENT FORENSICS AND REMEDIATION
- INTERNAL OR REGULATORY COMPLIANCE SUPPORT (e.g. PCI-DSS)

TRADITIONAL SOC – RISK



- LACK OF A COMPREHENSIVE THREAT OVERVIEW, IMPEDING EFFICIENT SECURITY PROGRAM DEVELOPMENT
- POOR PRIORITIZATION OF DETECTED THREATS
- UNDISCOVERED THREATS STILL ACTIVE WITHIN THE ORGANIZATION
- LACK OF IN-HOUSE EXPERTISE AND SHORTAGE OF SKILLED PROFESSIONALS ON THE MARKET
- INEFFICIENT INCIDENT RESPONSE PROCEDURES LEADING TO HIGH RECOVERY COSTS

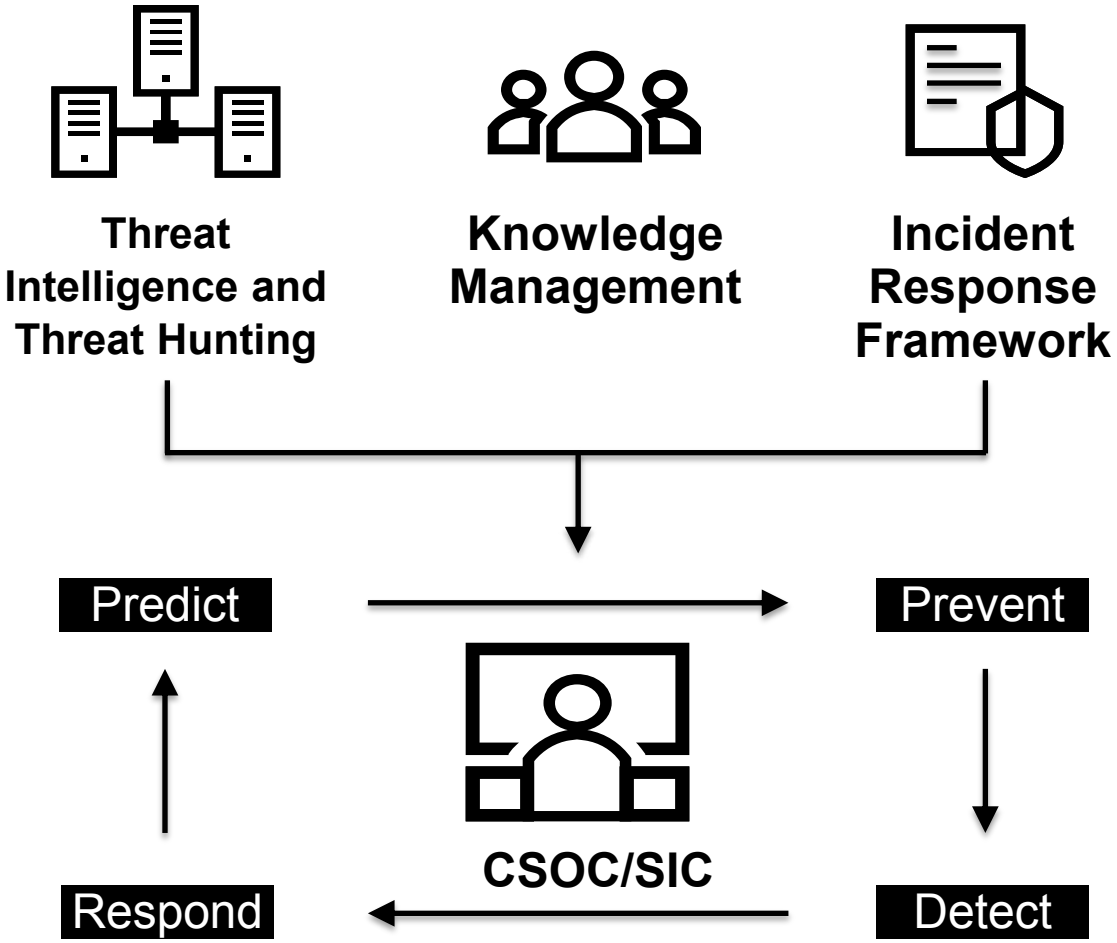
Traditional SOC Required REDISIGN



Ice-climbing requires
trusted teamwork and
agility to continually
detect and respond to
hidden dangers in a
challenging and ever changing
landscape, by utilizing the proper tools
in same harmony.

so does your SOC ?!

MAIN FOUR KEY ELEMENTS FOR INTELLIGENCE-DRIVEN APPROACH



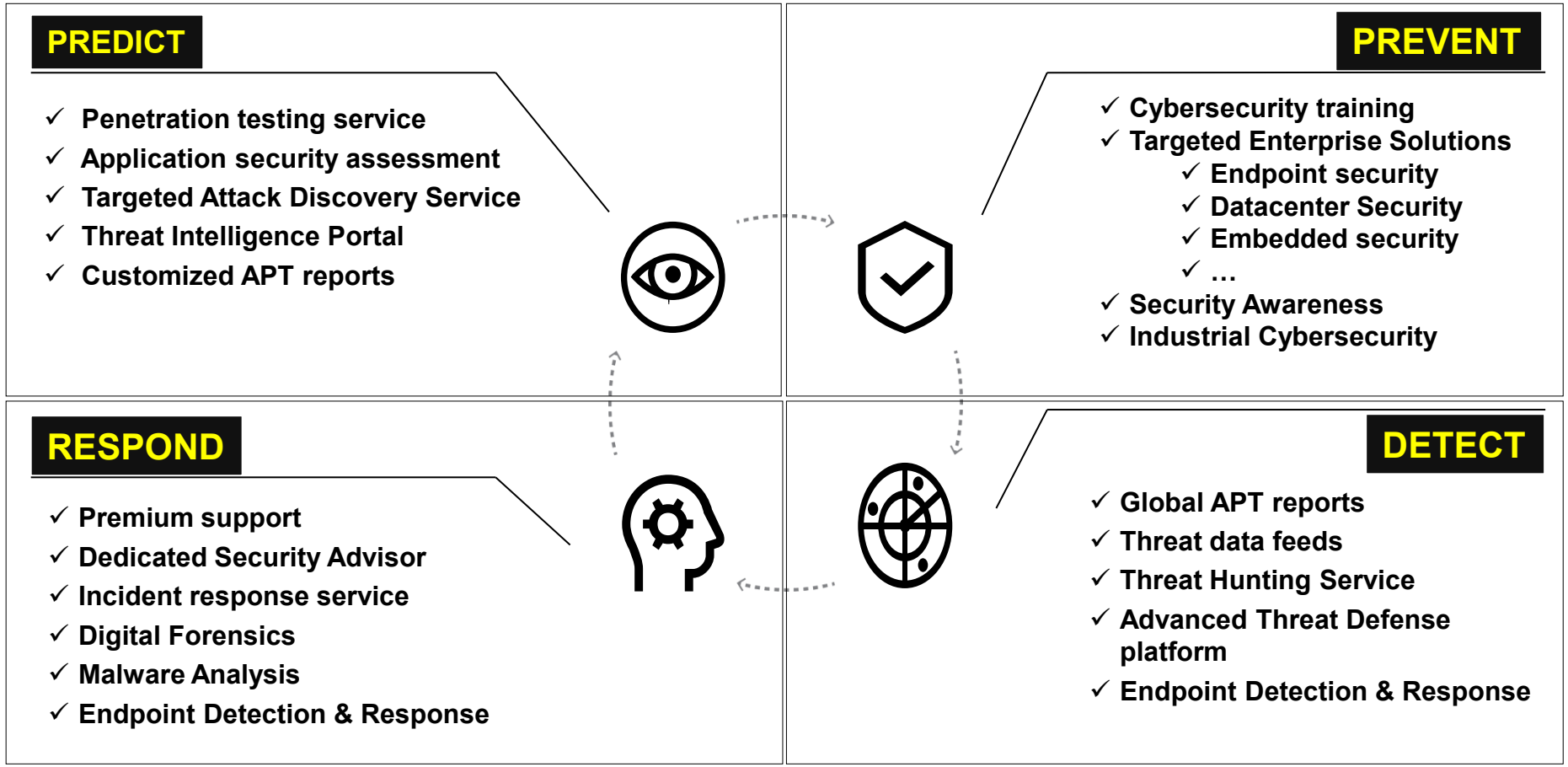
THREAT INTELLIGENCE FROM MANY DIFFERENT SOURCES IS ESSENTIAL TO THE TIMELY DETECTION OF EMERGED THREATS

THREAT HUNTING PROACTIVELY SEARCHES FOR THREATS REMAINING UNDETECTED BY TRADITIONAL SECURITY SYSTEMS

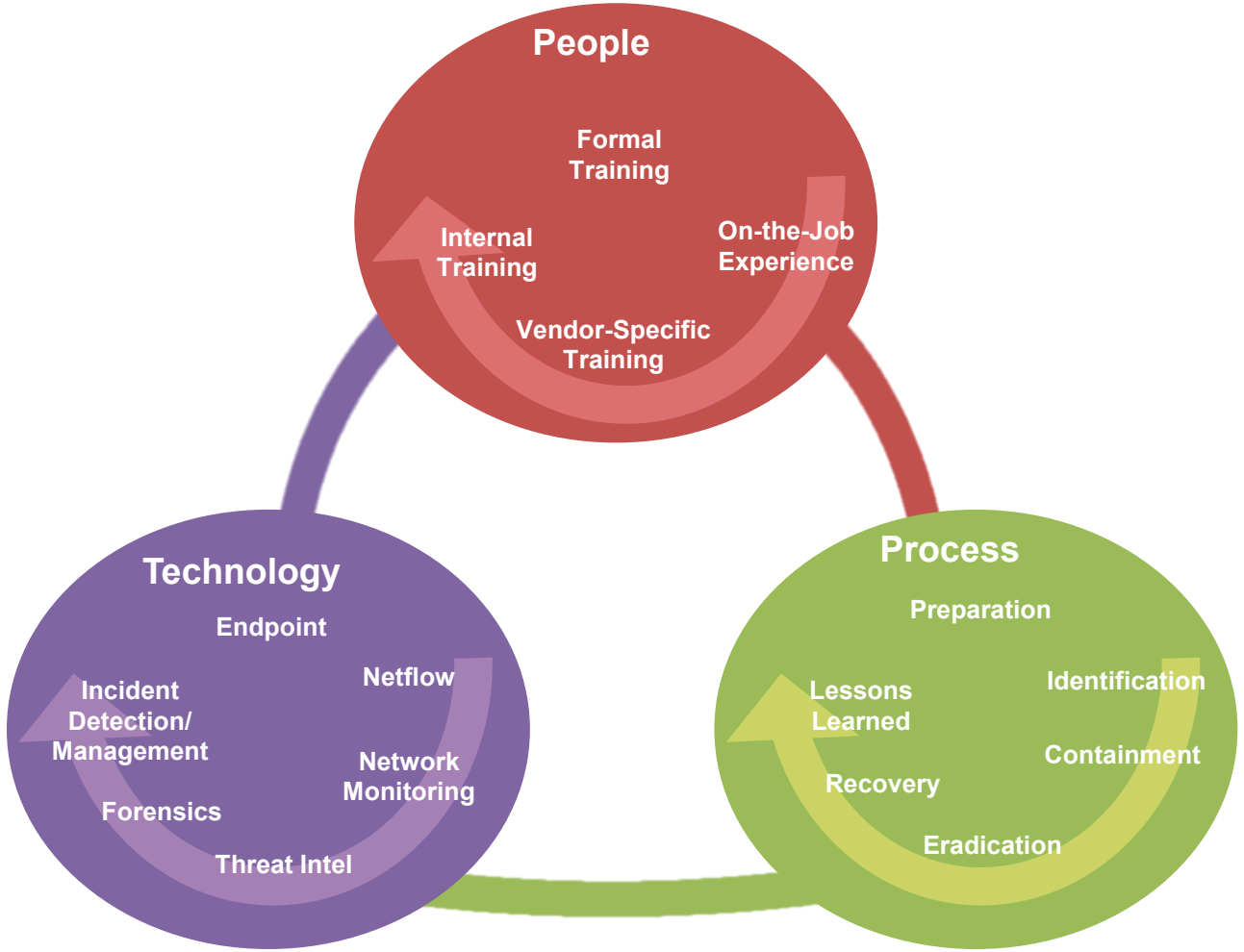
KNOWLEDGE MANAGEMENT PREVENTS AND RESPONDS TO INCREASINGLY SOPHISTICATED ATTACKS

INCIDENT RESPONSE FRAMEWORK LIMITS DAMAGE AND REDUCES REMEDIATION COSTS

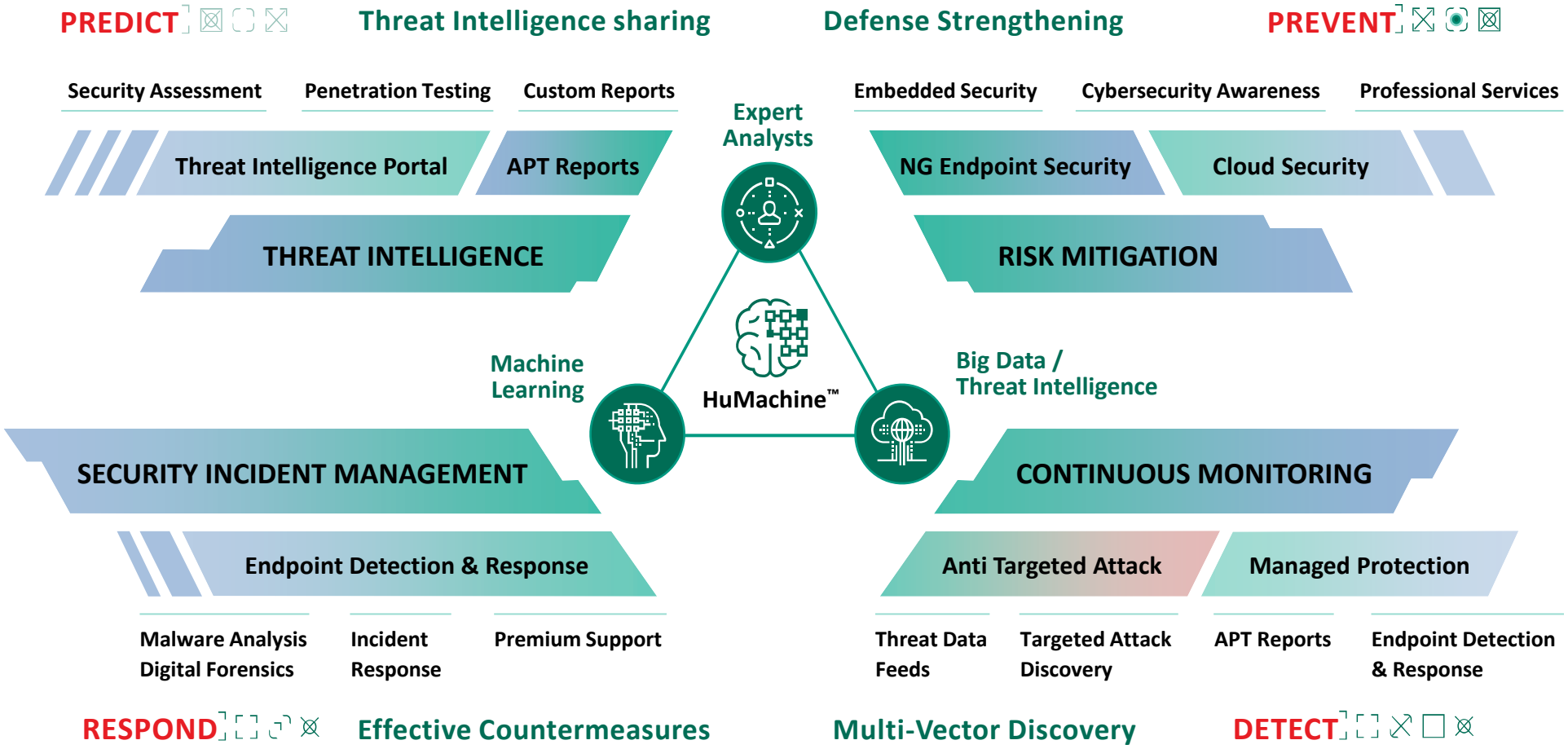
The role of an Adaptive Security Strategy



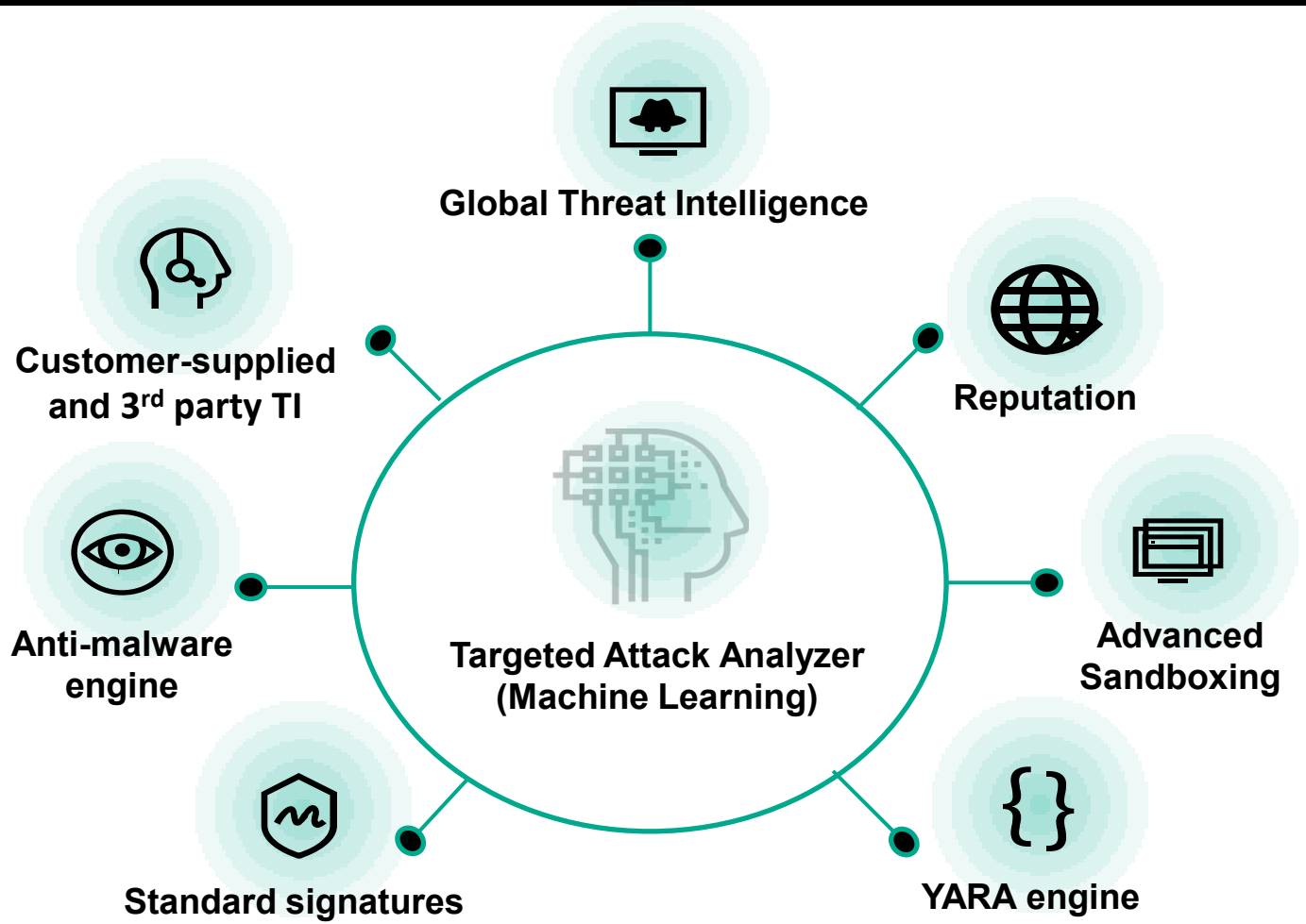
Security Operations framework rely on Three key functions



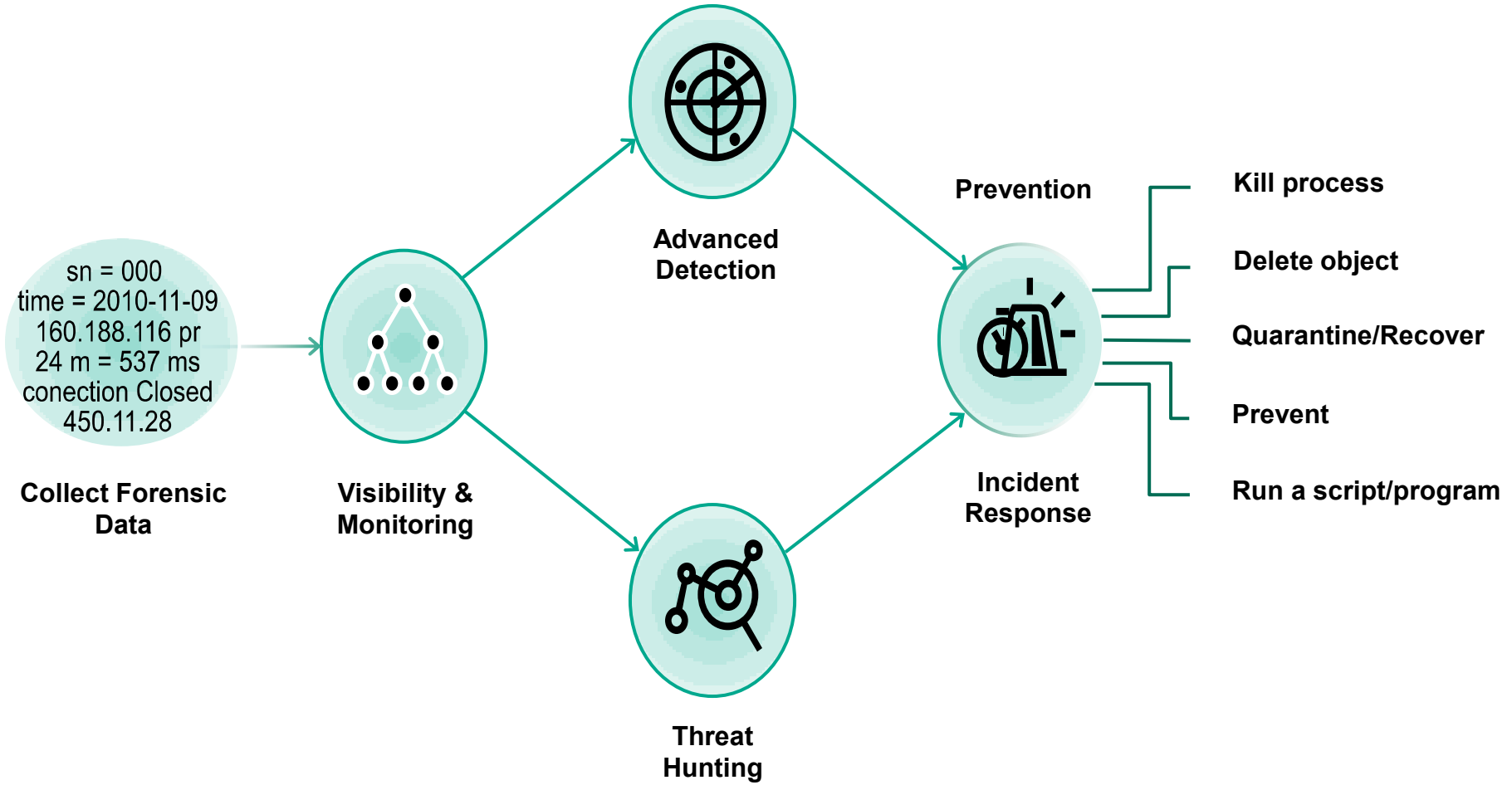
Kaspersky Adaptive Security Framework



Advanced Detection with Machine Learning

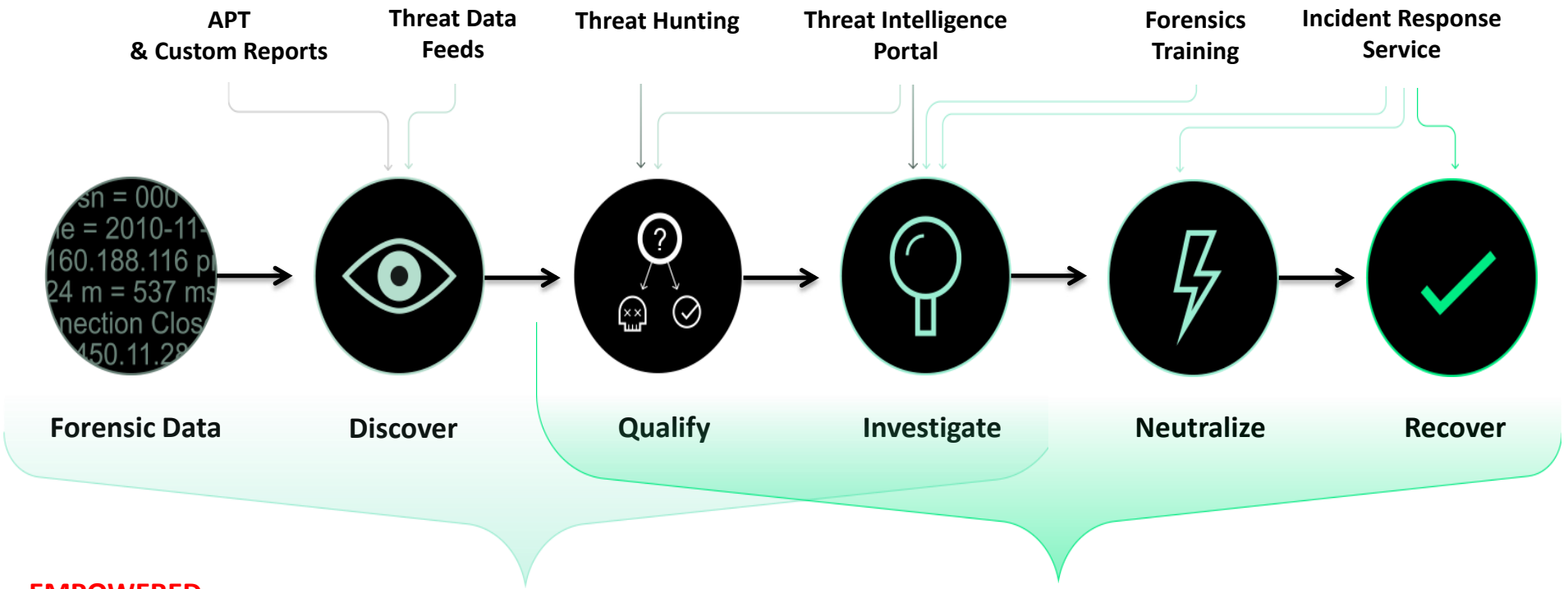


Adaptive Threat Response - Automation

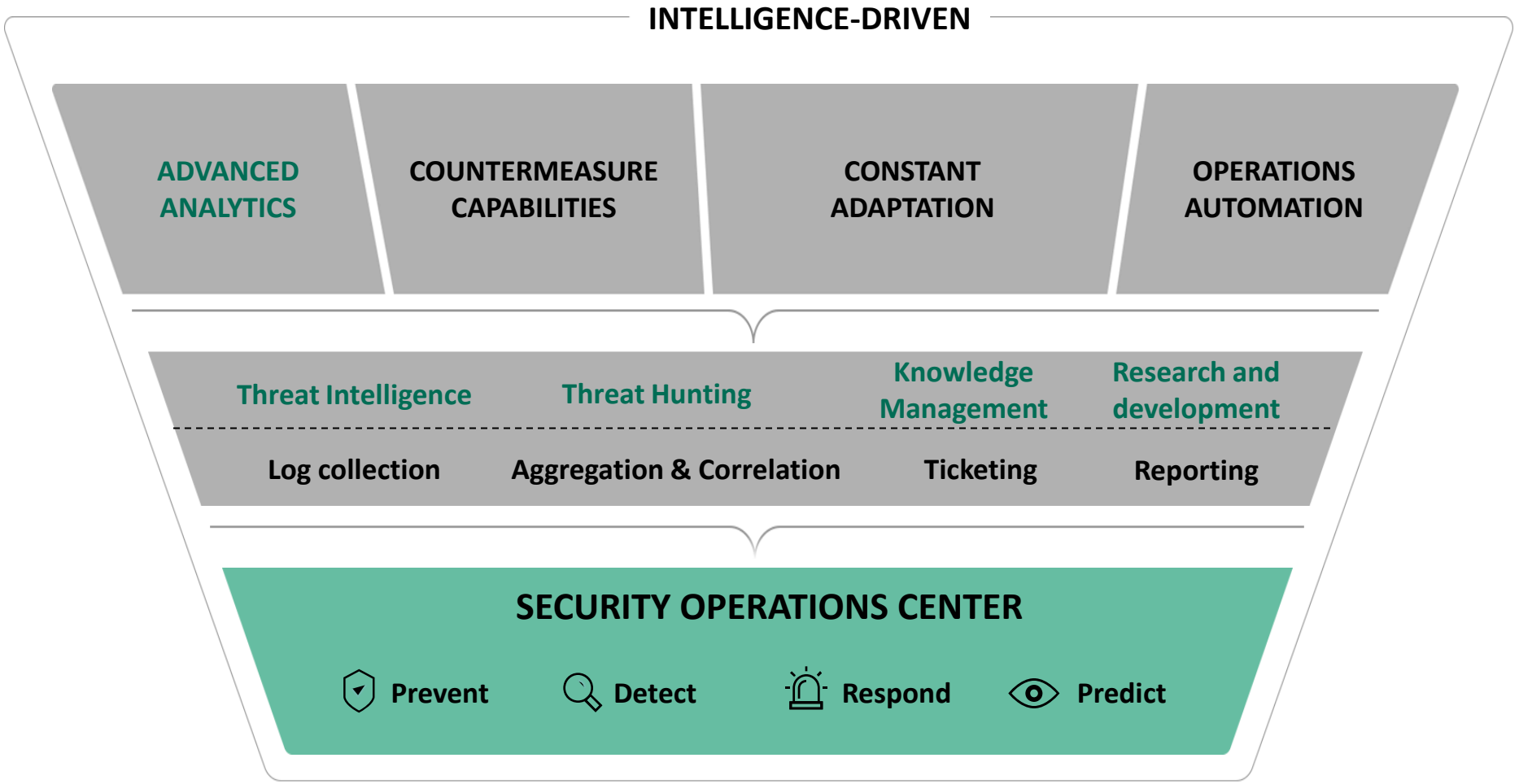


EMPOWERING THE PROCESS :
FROM DETECTION AUTOMATION TO RESPONSE

DRIVEN BY INTELLIGENCE



IT IS THE RIGHT TIME FOR:
INTELLIGENCE DRIVEN SOC



SAVING
THE WORLD
FOR 20 YEARS

WE PROTECT WHAT MATTERS MOST

KASPERSKY lab THE POWER OF PROTECTION

THANK YOU