

Kaspersky Enterprise Cybersecurity Services

Powered by HuMachine™ Intelligence

PENETRATION TESTING

TARGETED ATTACK DISCOVERY

DIGITAL FORENSICS

MALWARE ANALYSIS

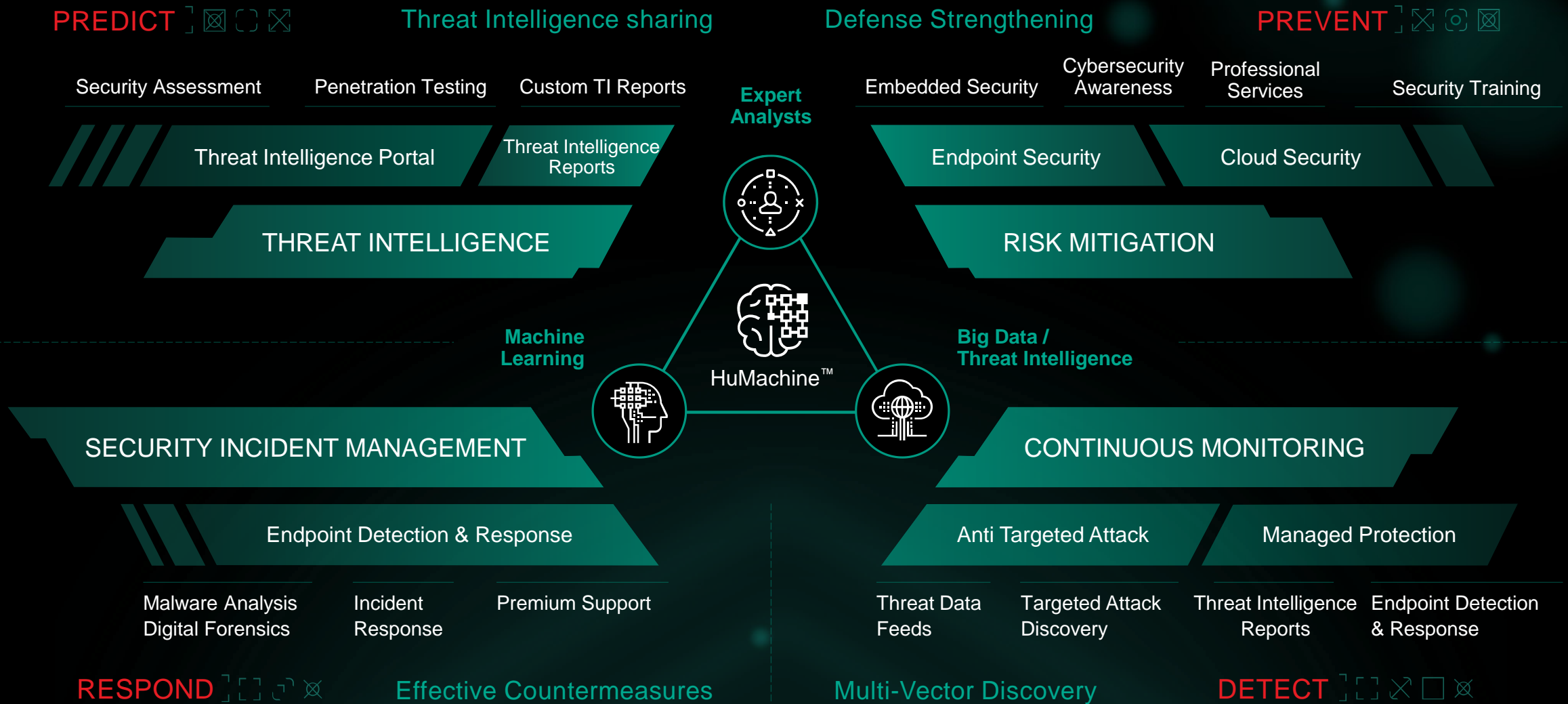
SECURITY TRAININGS



Proven.
Transparent.
Independent.

KASPERSKY Lab

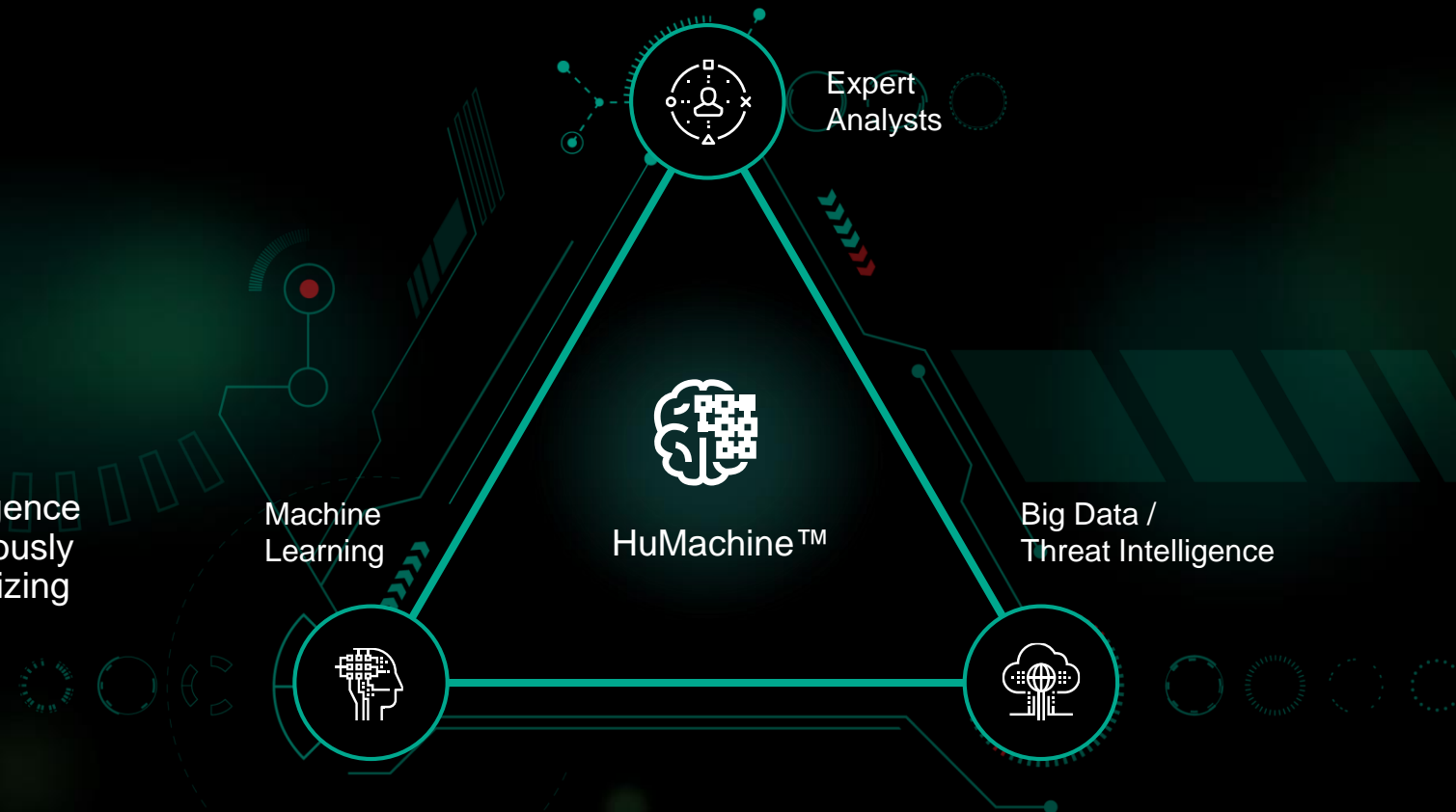
Kaspersky Adaptive Security Framework



True Cybersecurity

True cybersecurity doesn't just prevent cybersecurity incidents: it predicts, detects and responds to them – effectively, flexibly and reliably.

Our comprehensive portfolio of solutions achieves all this, thanks to our unique combination of HuMachine™ Intelligence and an Adaptive approach, protecting your business rigorously against Next-Gen and all other forms of threat, and minimizing the damage an incident could cause.



Reliable

For more than 20 years, we have developed the most tested, most awarded solutions and technologies that protect 400 million users worldwide

Efficient

Effective detection is achieved through our global cyber-brain combined with machine learning algorithms and powered by unequalled expertise

Adaptive

The whole product portfolio is built to help implement the architecture for a fully adaptive cycle of **Prediction, Prevention, Detection and Response**

AGILE

Our easy-to-use Next Gen solutions are able to adapt to our customers' needs, regardless of the size of business or the IT platforms used

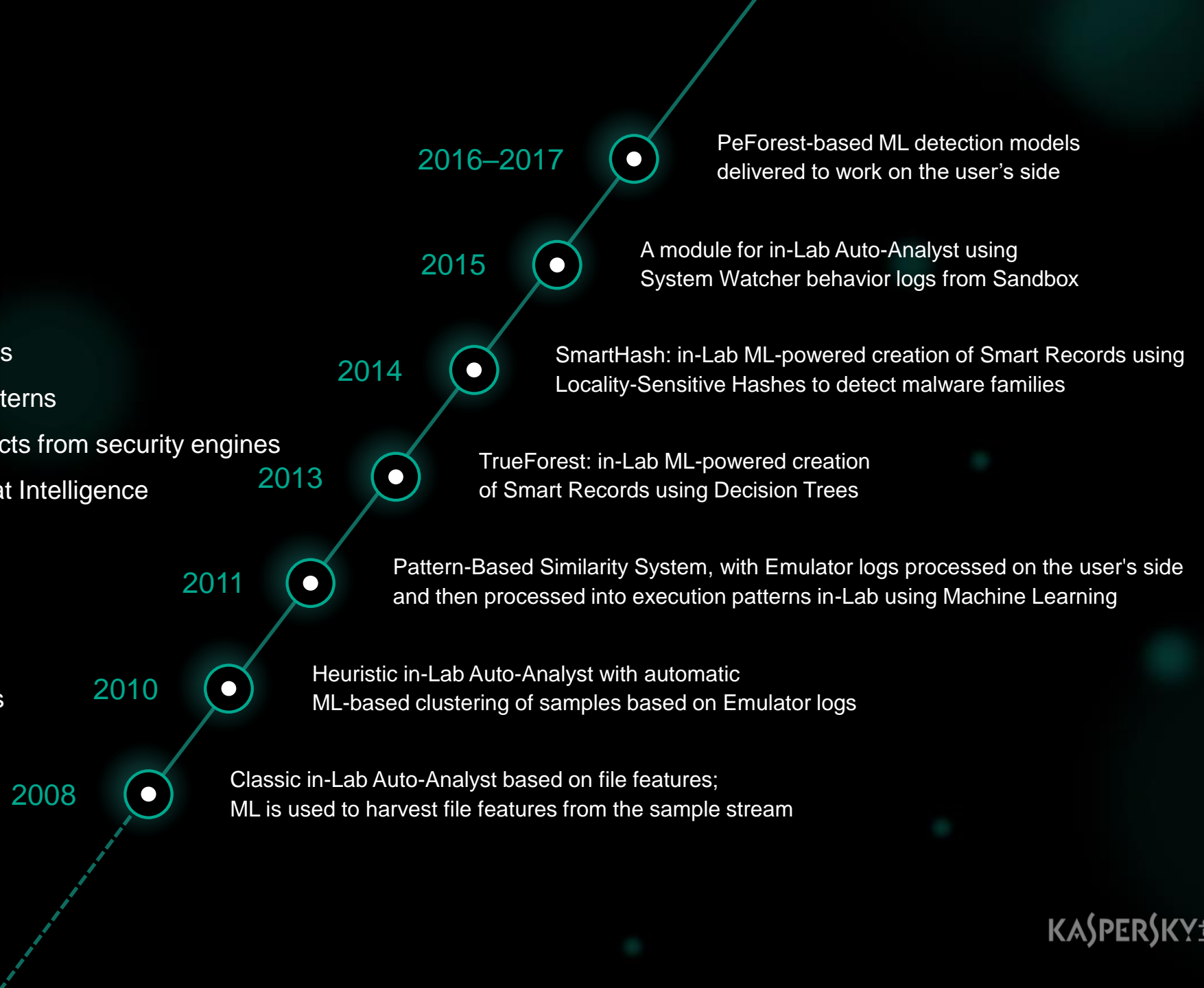
Machine learning in Kaspersky Lab solutions

Anomaly Detection:

- Catches deviations beyond thresholds
- Finds suspicious peaks in normal patterns
- Correlates activity patterns with verdicts from security engines
- Correlates events with external Threat Intelligence

Adaptive Thresholding:

- Establishes baselines
- Recognizes normal behavior patterns
- Adapts these patterns over time



Threat Intelligence Services



Kaspersky®
Threat Intelligence



FINANCIAL THREAT INTELLIGENCE REPORTING

Focuses on threats specifically targeting financial institutions, and tools developed or sold by cybercriminals to attack banks, payment processing companies, ATMs and POS systems



APT INTELLIGENCE REPORTING

Exclusive access to descriptions of high-profile cyber-espionage campaigns, including Indicators of Compromise (IOCs) and YARA rules



TAILORED THREAT INTELLIGENCE REPORTING

A snapshot of current and anticipated threats to the specific organization or country within the reporting time-frame



CLOUD SANDBOX

Allowing customers to 'detonate' suspicious files in a virtual sandbox environment, with a full report on the file's activities. Comprehensive and deep investigations can be run, based on tight integration with Kaspersky Threat Lookup.



THREAT LOOKUP

Web portal providing access to all Kaspersky Lab's knowledge on specific Indicators of Compromise (hashes, URLs or domains, IPs and threat names)



THREAT DATA FEEDS

- IP reputation
- URLs and domains
- Malware hashes
- P-sms trojans
- Mobile botnet C&Cs
- Ransomware URL
- APT IOCs

KASPERSKY®

Threat Hunting Services



**Kaspersky®
Threat Hunting**



KASPERSKY MANAGED PROTECTION

Proactive monitoring and detection of both known and unknown threats, for organizations with Kaspersky Endpoint Security and/or Kaspersky Anti Targeted Attack Platform already in operation



TARGETED ATTACK DISCOVERY

Proactive identification of any present or historical signs of compromise, and a comprehensive response to attacks previously missed:

- Threat intelligence
- Automated vulnerability assessment
- Incident investigation

Let's Talk?

Kaspersky Lab

Paseo del Club Deportivo nº1, Edificio 11, Planta 1, Izquierda 1

Parque empresarial La Finca, Pozuelo de Alarcón, 28223

Tel.: 91 398 37 52

www.kaspersky.es

KASPERSKY



Proven.
Transparent.
Independent.

