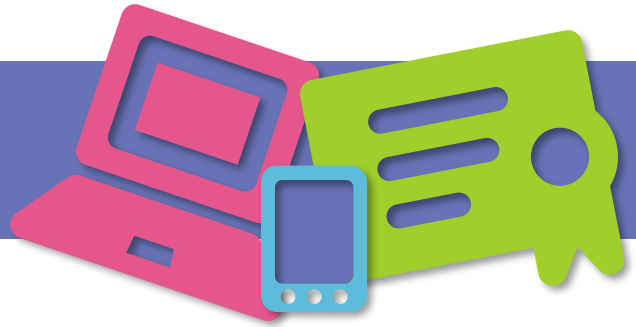
SECURITY 2015

23. ročník konference o bezpečnosti v ICT



Designing an Adaptive Defense Security Architecture

George Chiorescu

FireEye

Designing an Adaptive Security Architecture

- Key Challanges
  - Existing blocking and prevention capabilities are insufficient to protect against motivated, advanced attackers.
  - Most organizations continue to overly invest in prevention-only strategies.
  - Limited visibility in advanced attacks.
  - Because enterprise systems are under continuous attack and are continuously compromised, an ad hoc approach to "incident response" is the wrong mindset.

Source: Gartner's Report, Designing an Adaptive Security Architecture.
Available at https://www2.fireeye.com/GTM_ADV_RPT_Gartner-Designing-an-Adaptive-Security-Architecture.html

Designing an Adaptive Security Architecture

- Recommandations
  - Shift from „Incident response“ to „Continuous response“.
  - Adopt an adaptive security architecture.
  - Spend less on prevention; invest in detection, response and predictive capabilities.
  - Develop a security operations center that supports continuous monitoring.

Source: Gartner’s Report, Designing an Adaptive Security Architecture.
Available at https://www2.fireeye.com/GTM_ADV_RPT_Gartner-Designing-an-Adaptive-Security-Architecture.html

UNRESTANDING THE ATTACK

ABOUT THE ADVERSARY

IT'S A "WHO," NOT A "WHAT"

- THERE'S A HUMAN AT A KEYBOARD
- HIGHLY TAILORED AND CUSTOMIZED ATTACKS
- TARGETED SPECIFICALLY AT YOU

THEY ARE PROFESSIONAL, ORGANIZED AND WELL FUNDED

- NATION-STATE SPONSORED
- ESCALATE SOPHISTICATION OF TACTICS AS NEEDED
- RELENTLESSLY FOCUSED ON THEIR OBJECTIVE

IF YOU KICK THEM OUT THEY WILL RETURN

- THEY HAVE SPECIFIC OBJECTIVES
- THEIR GOAL IS LONG-TERM OCCUPATION
- PERSISTENCE TOOLS ENSURE ONGOING ACCESS

THE IMPACT OF THE TRADITIONAL MODEL

229 DAYS

MEDIAN NUMBER OF DAYS BEFORE DETECTION

32

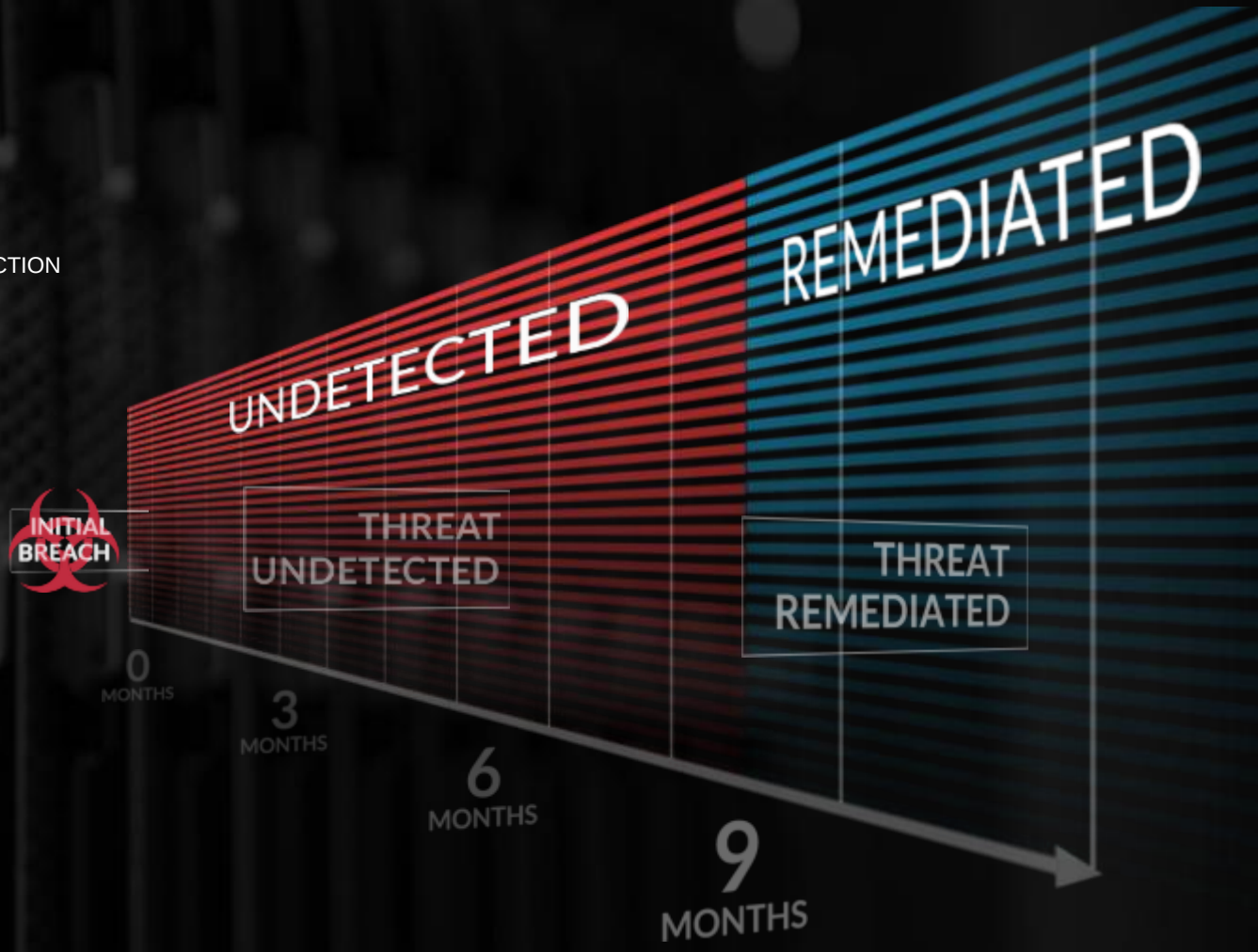
DAYS TO RESPOND TO A BREACH

67%

OF COMPANIES LEARNED THEY WERE BREACHED FROM AN EXTERNAL ENTITY

100%

OF VICTIMS HAD FIREWALLS OR UP-TO-DATE ANTI-VIRUS SIGNATURES



SOURCE: MANDIANT M-TRENDS REPORT, PONEMON COST OF DATA BREACH STUDY

THE IMPACT OF THE TRADITIONAL MODEL

THE IMPACT OF THE TRADITIONAL MODEL

Financial
18%

Government
16%

Chemical & Manufacturing
7%

High-Tech
7%

Consulting
7%

Energy
6%

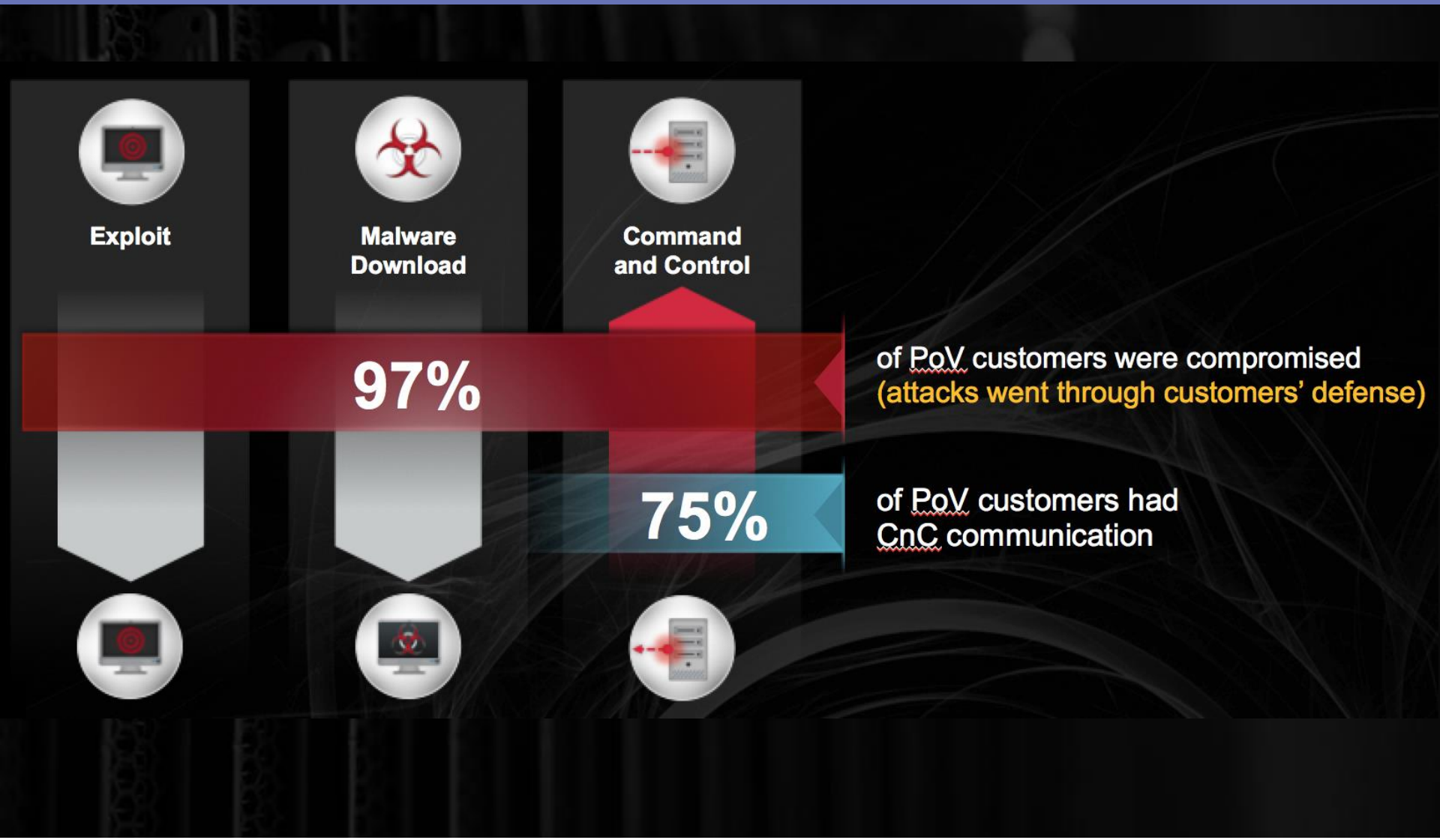
Retail
5%

Healthcare
4%

Others
(12+)

Others
30%

THE IMPACT OF THE TRADITIONAL MODEL



Today's Malware is Highly Targeted

208,184

Malware Download

124,289

Unique Malware

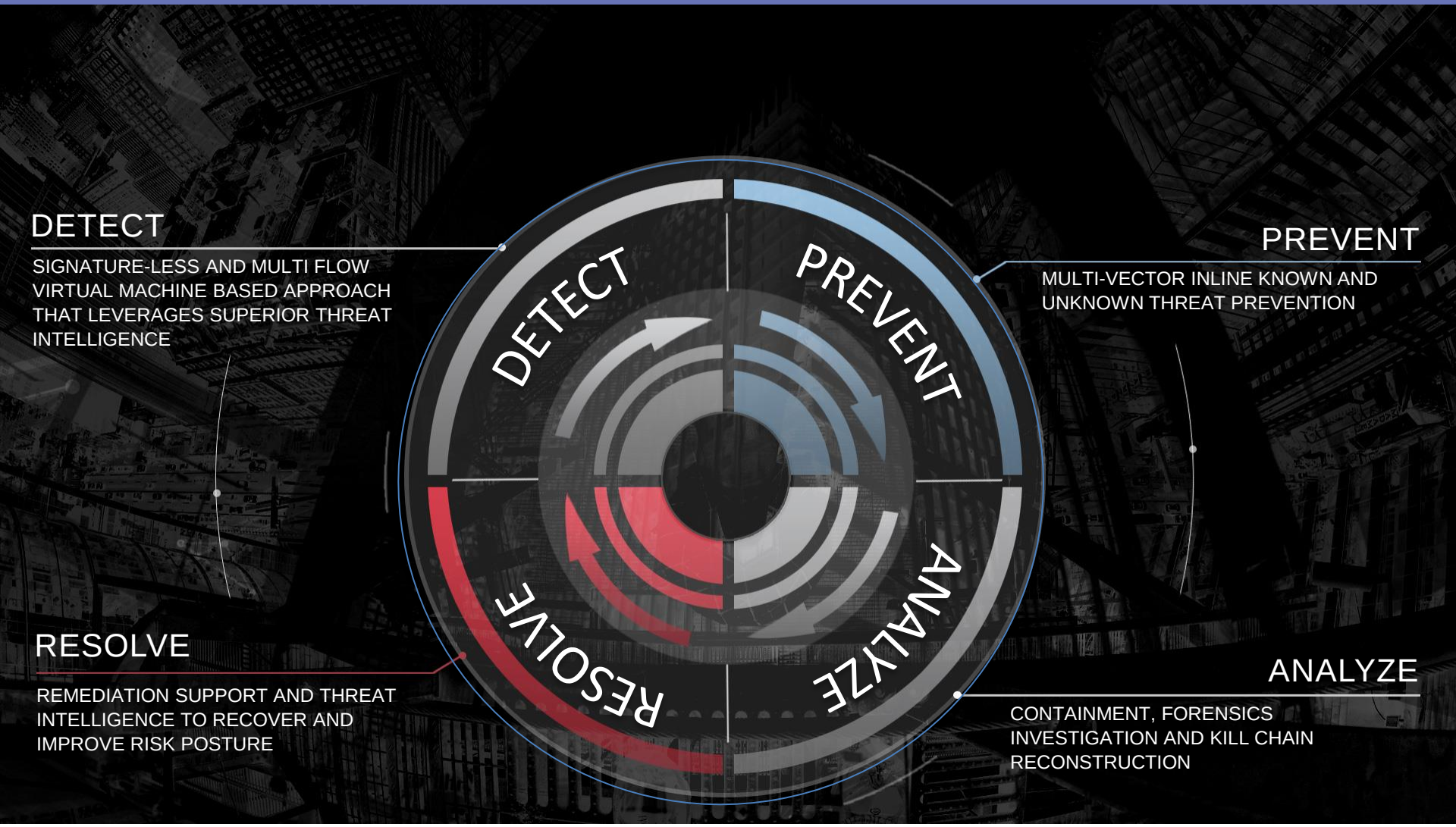
93,755

Malware Seen ONCE

75%

of all the unique malware detected was seen **ONCE**

The Adaptive Defense Security Model



The Adaptive Defense Security Model

The Adaptive Defense Security Model

The Adaptive Defense Security Model

ENDPOINT SECURITY ARCHITECTURE MUST BE AGILE, FLEXIBLE, AND DEEPLY INTEGRATED.

ADAPTIVE DEFENSE

DETECT AND PREVENT

- Advanced Threat Detection (Signature-Less, Tamper resistant)
- Threat Prevention Across All Endpoints

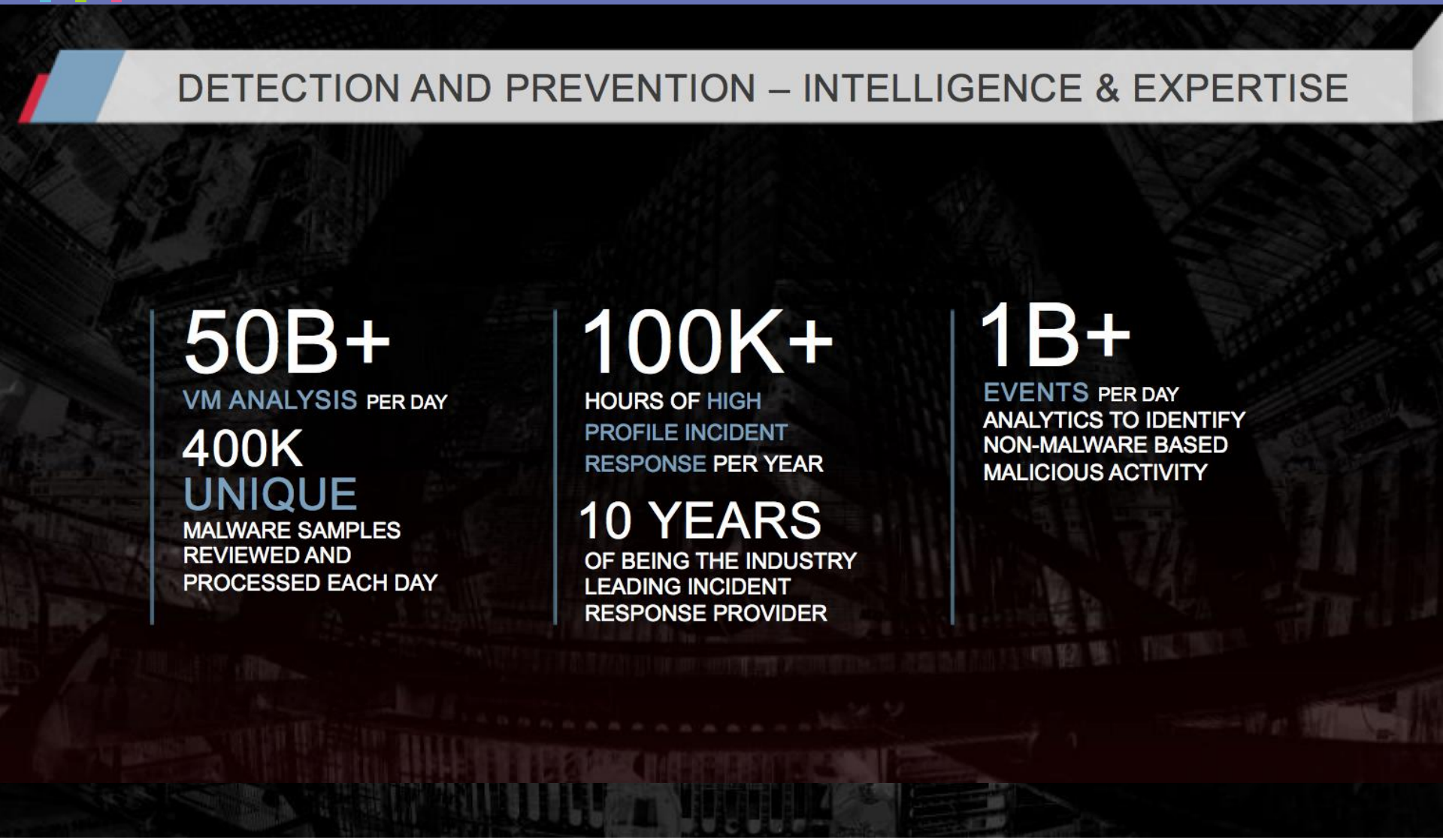
ANALYZE AND RESPOND

- Threat Intel (Network, Cloud)
- Endpoint Live Response (Validate, Contain, Search, Sweep)

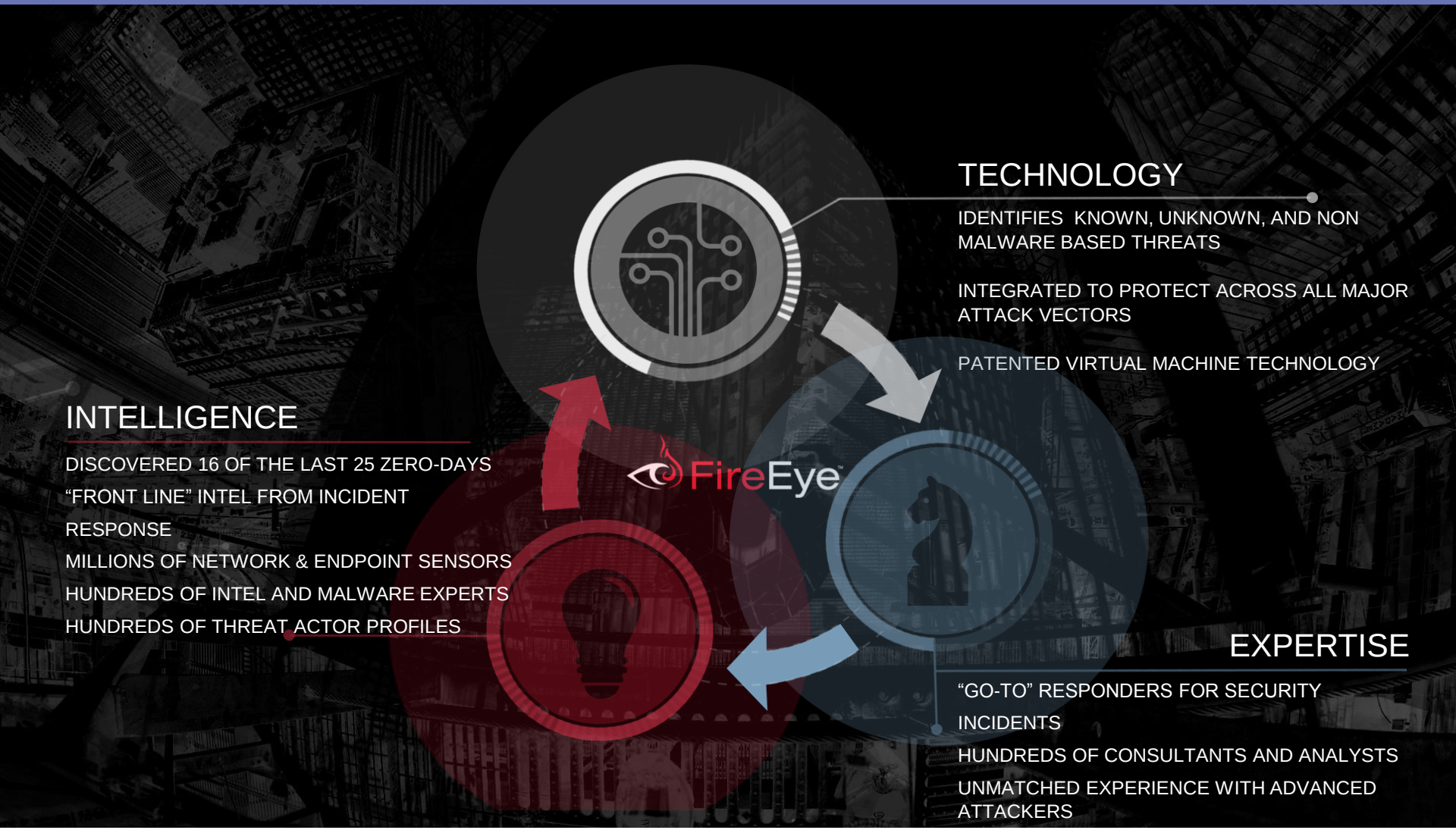
NEXT GENERATION ENDPOINT SOLUTION REQUIREMENTS

- DETECTION TO RESPONSE: detection, validation, containment, and remediation
- PROACTIVE AND ADAPTIVE: searching, sweeping, and advanced detection of unknown threats
- COMPREHENSIVE ENDPOINTS: on premise, remote and Mobile endpoints
- REAL-TIME INTELLIGENCE: real-time intelligence feeds from cloud and network alerts

The Adaptive Defense Security Model



The Adaptive Defense Security Model



SECURITY 2015

23. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

George Chiorescu

FireEye

George.Chiorescu@FireEye.com