FINDING THE RIGHT NEEDLE IN A FIELD OF HAYSTACKS

ISSA PHOENIX - 2017 Q1 MEETING

PHOENIX, AZ – 10 JANUARY 2017

Christian Schreiber, CISM, PMP

PERSONAL BACKGROUND

Nearly 20 years IT and information security experience

- ► Senior consulting engineer at FireEye
- ► CISO & HIPAA Security Officer at the University of Arizona before joining FireEye
- ► Earlier security and IT leadership positions:
  - - SunGard Data Systems (now FIS)
  - - University of Wisconsin – Whitewater
  - - University of Wisconsin – Madison
  - - Central Michigan University

Education & Professional Certifications

- ► Masters Certificate in Project Management, University of Wisconsin – Madison
- ► Bachelor of Science in Business Administration, Central Michigan University
- ► Certified Information Security Manager (CISM)
- ► Project Management Professional (PMP)

SECURITY STRATEGIES ARE CHANGING TO COPE WITH EVOLVING THREATS

MANY ORGANIZATIONS RELY ON DEFENSE-IN-DEPTH TO KEEP ATTACKERS OUT

FIREEYE. MAGINOT REVISITED: MORE REAL-WORLD RESULTS FROM REAL-WORLD TESTS. 2015.

PREVENTION IS NOT ENOUGH

STUDIED 1600+ ORGANIZATIONS

96% COMPROMISED DURING TEST PERIOD

27% HAD EVIDENCE OF ADVANCED ATTACKS

CYBERSECURITY THREATS ARE ASYMMETRIC

YOU NEED TO HUNT FOR INTRUDERS THAT ARE ALREADY INSIDE

SECURITY TOOLS CAN ENABLE MORE EFFECTIVE HUNTING

MALWARE SANDBOXING, THREAT INTELLIGENCE, SIEM & DATA ANALYTICS

FIREEYE. MANDIANT M-TRENDS REPORT. 2015.

HUNTING HAS BECOME COMPLEX AND REQUIRES MORE DATA

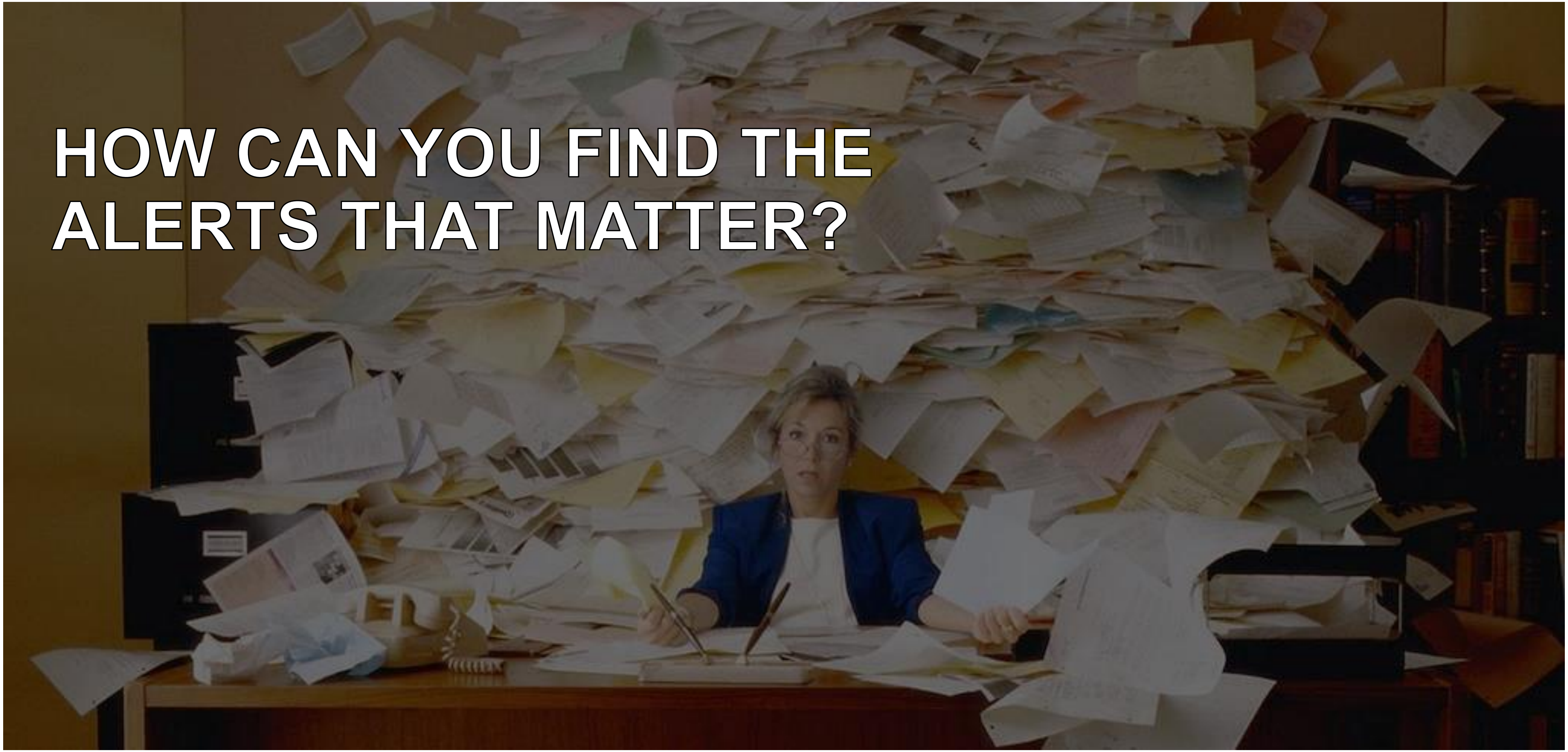
BYOD, CLOUD COMPUTING, IoT, PARTNERS,
GLOBAL & MOBILE WORKFORCE

ATTACKERS HIDE BEHIND LEGITIMATE SERVICES
46% OF COMPROMISES DON’T USE MALWARE

PONEMON INSTITUTE. THE COST OF MALWARE CONTAINMENT. JANUARY 2015.

ORGANIZATIONS RECEIVE THOUSANDS OF ALERTS

MOST SECURITY TEAMS CAN REVIEW ONLY 4%

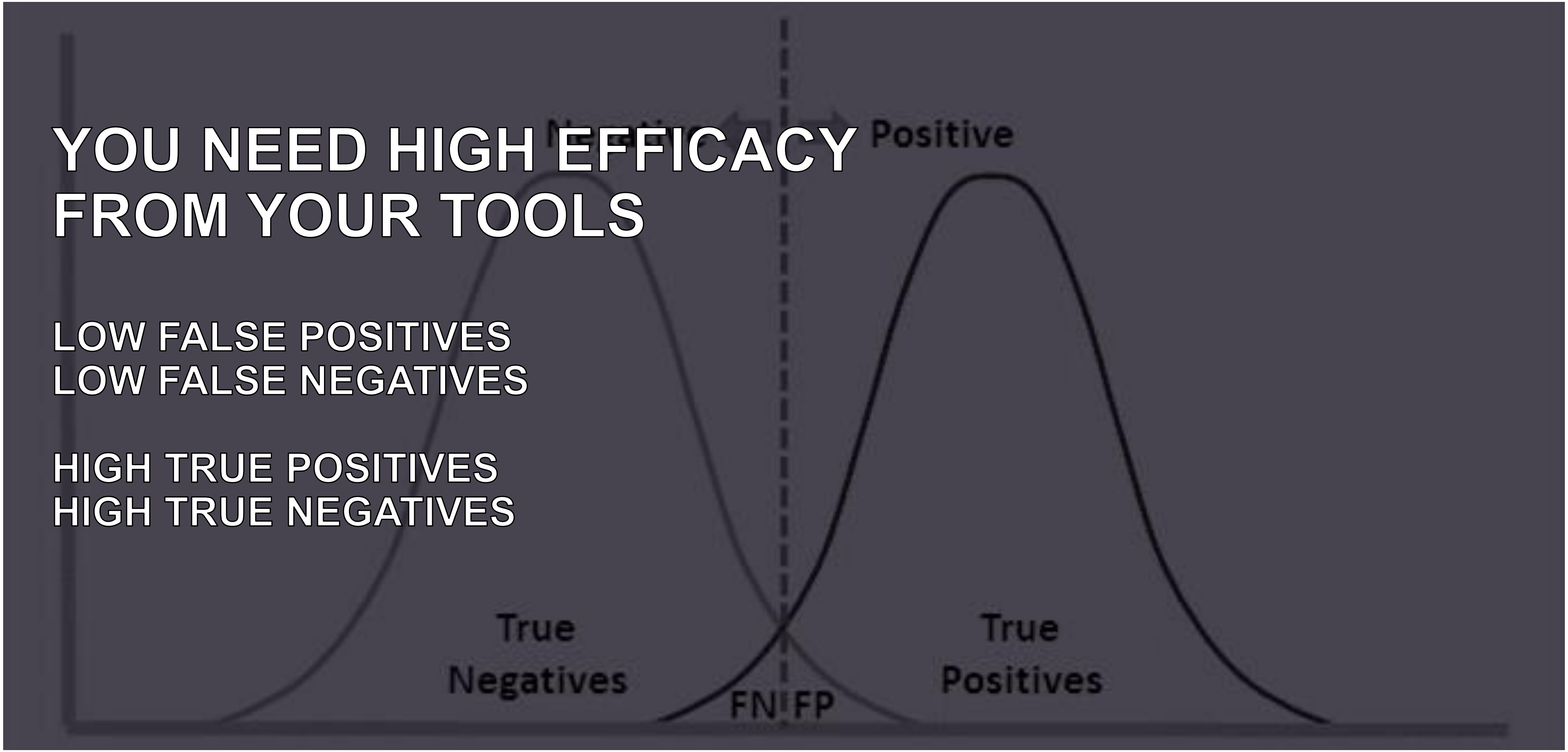


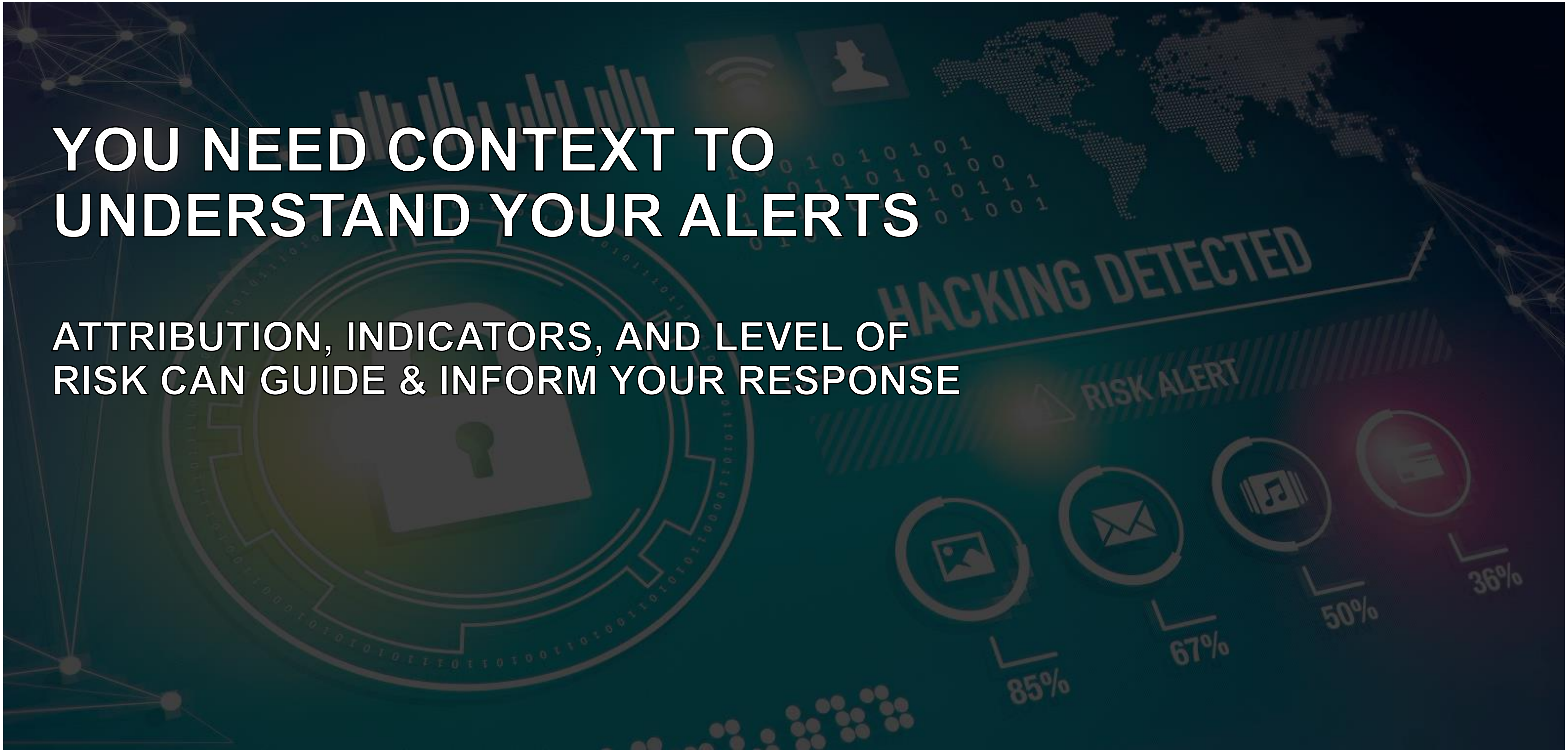
HOW CAN YOU FIND THE ALERTS THAT MATTER?

YOU NEED HIGH EFFICACY FROM YOUR TOOLS

LOW FALSE POSITIVES
LOW FALSE NEGATIVES

HIGH TRUE POSITIVES
HIGH TRUE NEGATIVES





YOU NEED CONTEXT TO UNDERSTAND YOUR ALERTS

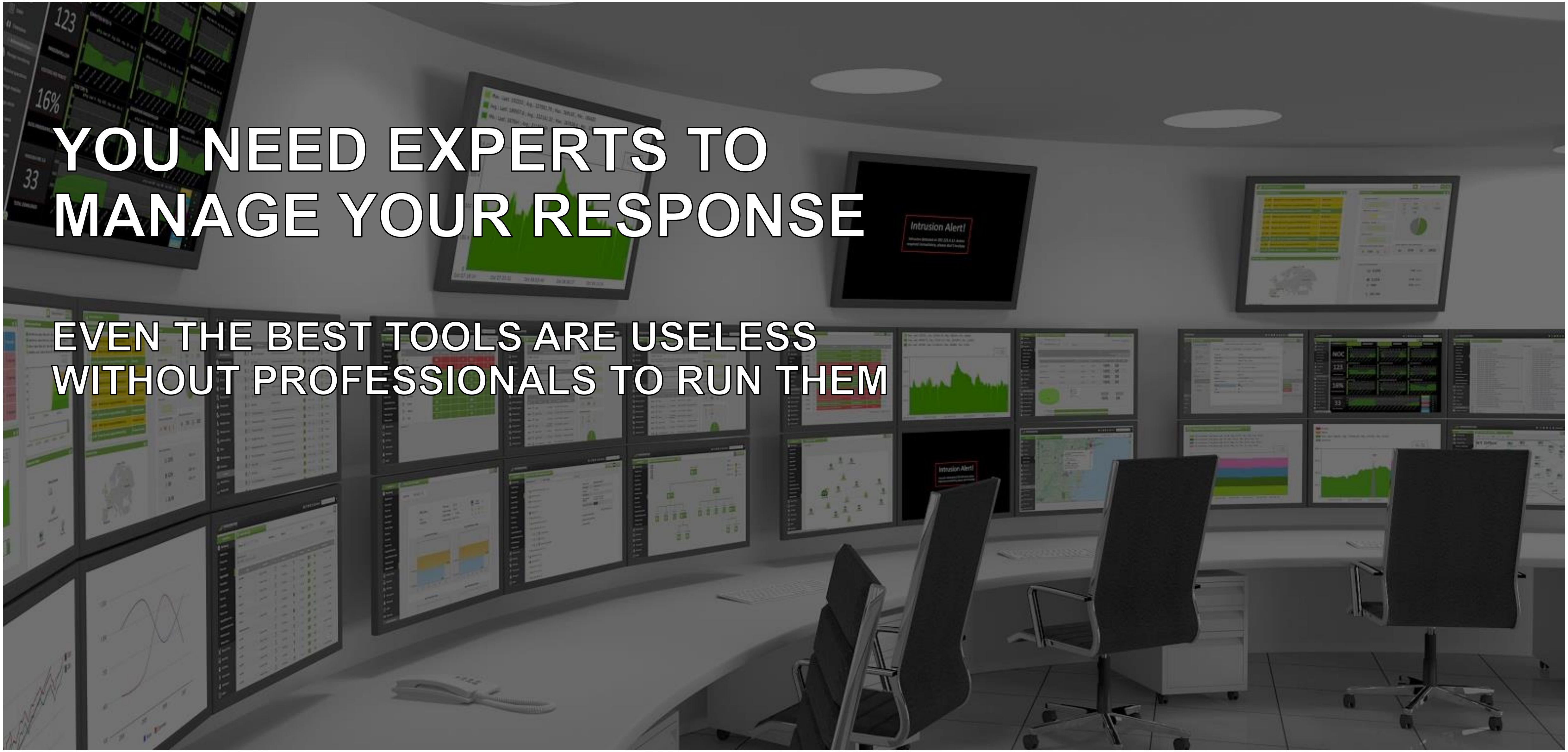
ATTRIBUTION, INDICATORS, AND LEVEL OF RISK CAN GUIDE & INFORM YOUR RESPONSE

YOU NEED VISIBILITY INTO BROADER PATTERNS

ARE SIMILAR EVENTS HAPPENING ELSEWHERE IN YOUR ORGANIZATION?

ACROSS YOUR INDUSTRY?

SECURITY OPERATION CENTER
Dublin & Cork, Ireland
Netherlands
Germany
Ukraine
SECURITY OPERATION CENTER
Reston, VA
Idaho Falls, ID
London, UK
Spain
Romania
Salt Lake City, UT
Chantilly, VA
Cyprus
SECURITY OPERATION CENTER
Dubai, UAE
HEADQUARTERS
Milpitas, CA
Pune, India
China
SECURITY OPERATIONS CENTER
Osaka, Japan
JAPAN HQ
Tokyo, Japan
Taiwan
Philippines
Bengalaru, India
Malaysia
SECURITY OPERATIONS CENTER
Singapore
Brazil
Argentina
SECURITY OPERATIONS CENTER
Sydney, Australia
New Zealand
FireEye
SECURITY REIMAGINED



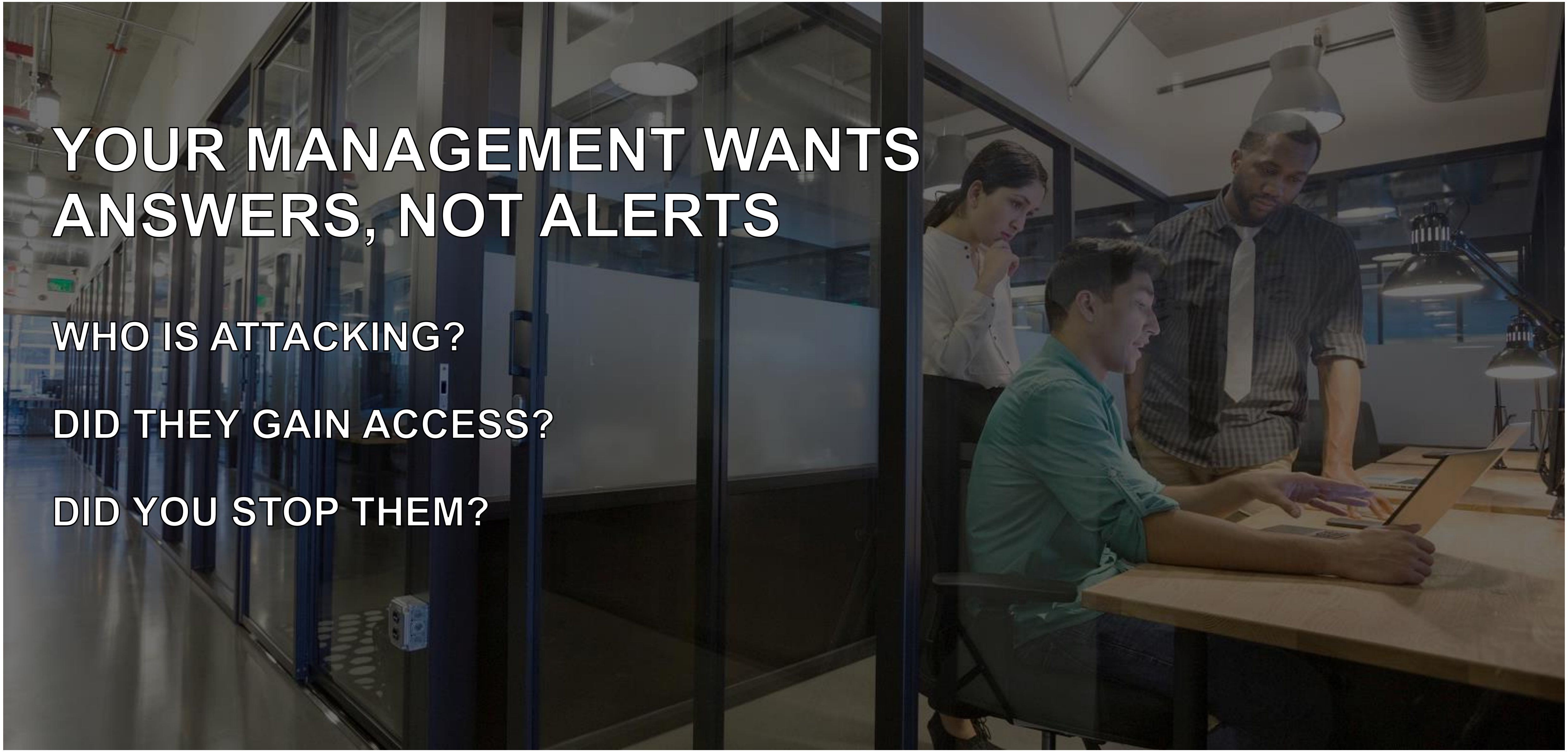
YOU NEED EXPERTS TO MANAGE YOUR RESPONSE

EVEN THE BEST TOOLS ARE USELESS WITHOUT PROFESSIONALS TO RUN THEM

YOU NEED EFFICIENCY FROM SECURITY INVESTMENTS

SECURITY TOOLS NEED TO FUNCTION TOGETHER SEAMLESSLY

SECURITY TEAMS NEED TO SPEND LESS TIME ON LOW VALUE TASKS

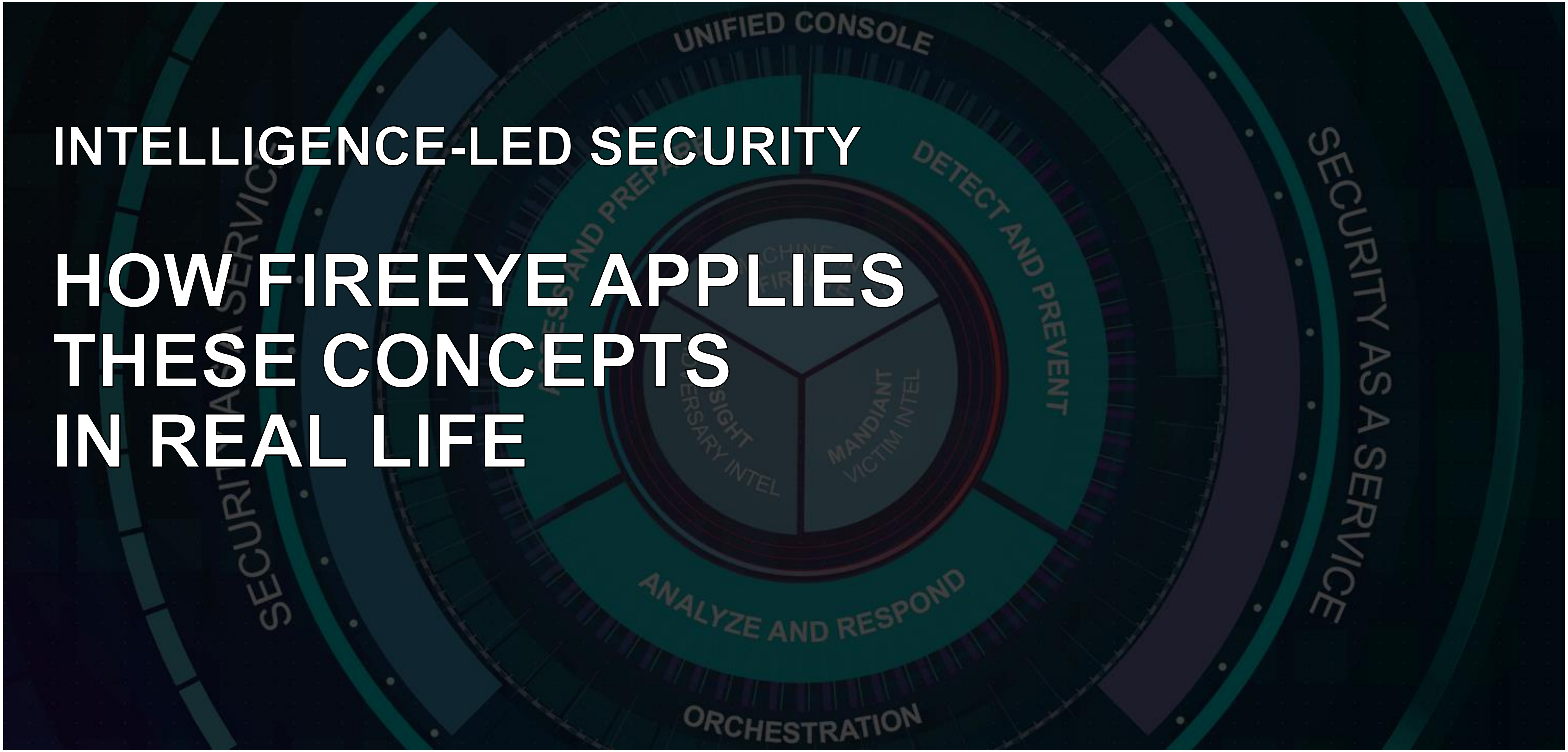


YOUR MANAGEMENT WANTS ANSWERS, NOT ALERTS

WHO IS ATTACKING?

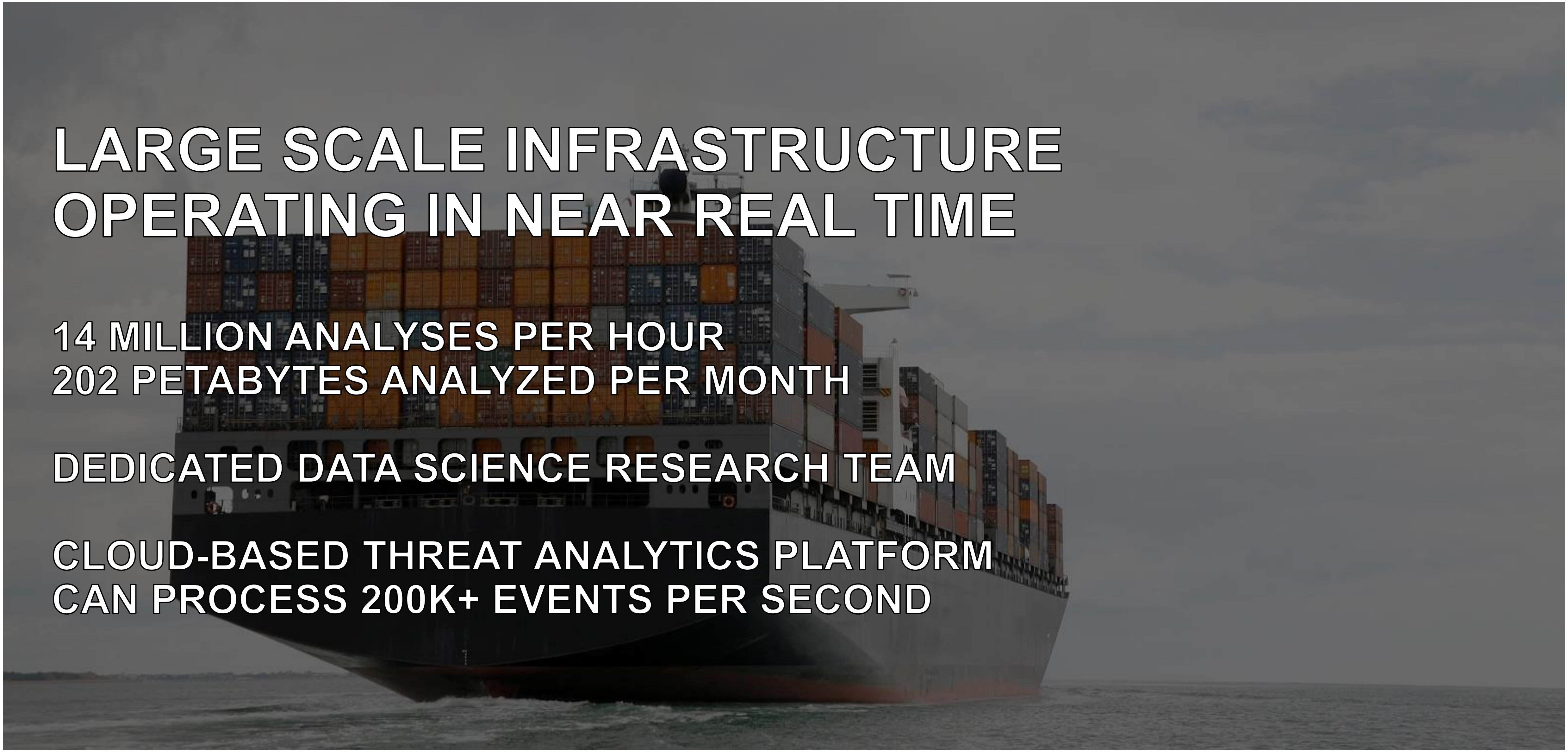
DID THEY GAIN ACCESS?

DID YOU STOP THEM?



INTELLIGENCE-LED SECURITY

HOW FIREEYE APPLIES THESE CONCEPTS IN REAL LIFE



LARGE SCALE INFRASTRUCTURE OPERATING IN NEAR REAL TIME

14 MILLION ANALYSES PER HOUR
202 PETABYTES ANALYZED PER MONTH

DEDICATED DATA SCIENCE RESEARCH TEAM

CLOUD-BASED THREAT ANALYTICS PLATFORM
CAN PROCESS 200K+ EVENTS PER SECOND

GLOBAL VISIBILITY INTO MACHINE, VICTIM, AND ADVERSARY INTELLIGENCE

15 MILLION SENSORS IN 89 COUNTRIES
100,000+ INCIDENT RESPONSE HOURS PER YEAR
1000+ SECURITY AND INTELLIGENCE EXPERTS

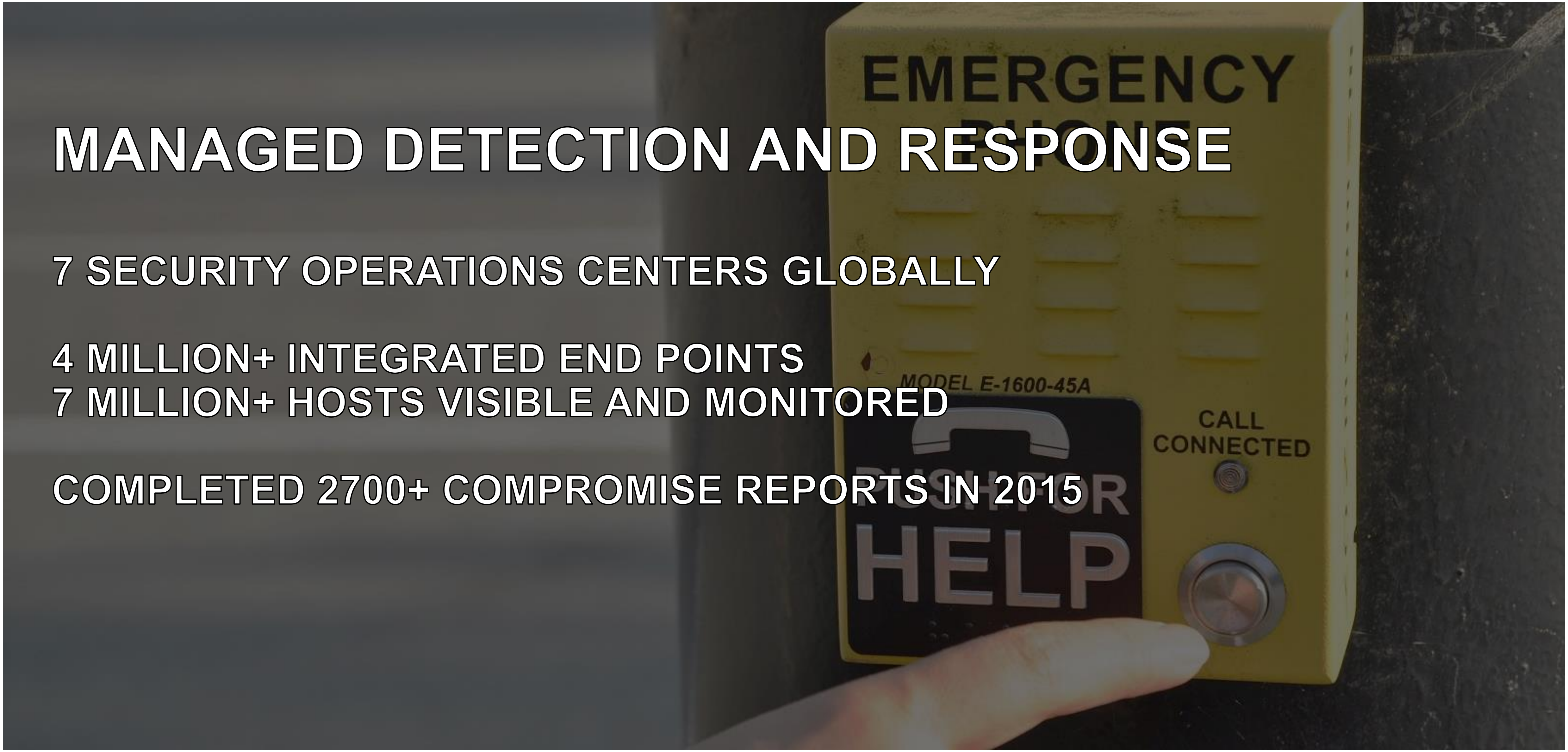
PROTECT MORE THAN 65% OF THE FORTUNE 500 AND HUNDREDS OF GOVERNMENT AND NON-PROFIT ORGANIZATIONS

TIMELY & RELEVANT THREAT INTELLIGENCE

FIREEYE TRACKS MORE THAN 16,000 THREATS

174 MILLION NODE GRAPH DATABASE
583 MILLION CORRELATION RELATIONSHIPS

UPDATES DISTRIBUTED TO ALL CUSTOMERS GLOBALLY IN LESS THAN AN HOUR



MANAGED DETECTION AND RESPONSE

7 SECURITY OPERATIONS CENTERS GLOBALLY

4 MILLION+ INTEGRATED END POINTS
7 MILLION+ HOSTS VISIBLE AND MONITORED

COMPLETED 2700+ COMPROMISE REPORTS IN 2015

INTELLIGENCE-LED SECURITY BENEFITS FOR CUSTOMERS

CONFIDENCE WITH <1% FALSE POSITIVES

RESPONSE TIME REDUCED BY 95%

>90% CUSTOMER RENEWAL RATE

THANK YOU!

Christian Schreiber, CISM, PMP
christian.schreiber@FireEye.com