
INNOVATION & TECHNOLOGY
SUMMIT
2017

REVISION 004 / UPDATED 26 APRIL 2017

DEFENDING THE ACADEMY FROM CYBER THREATS

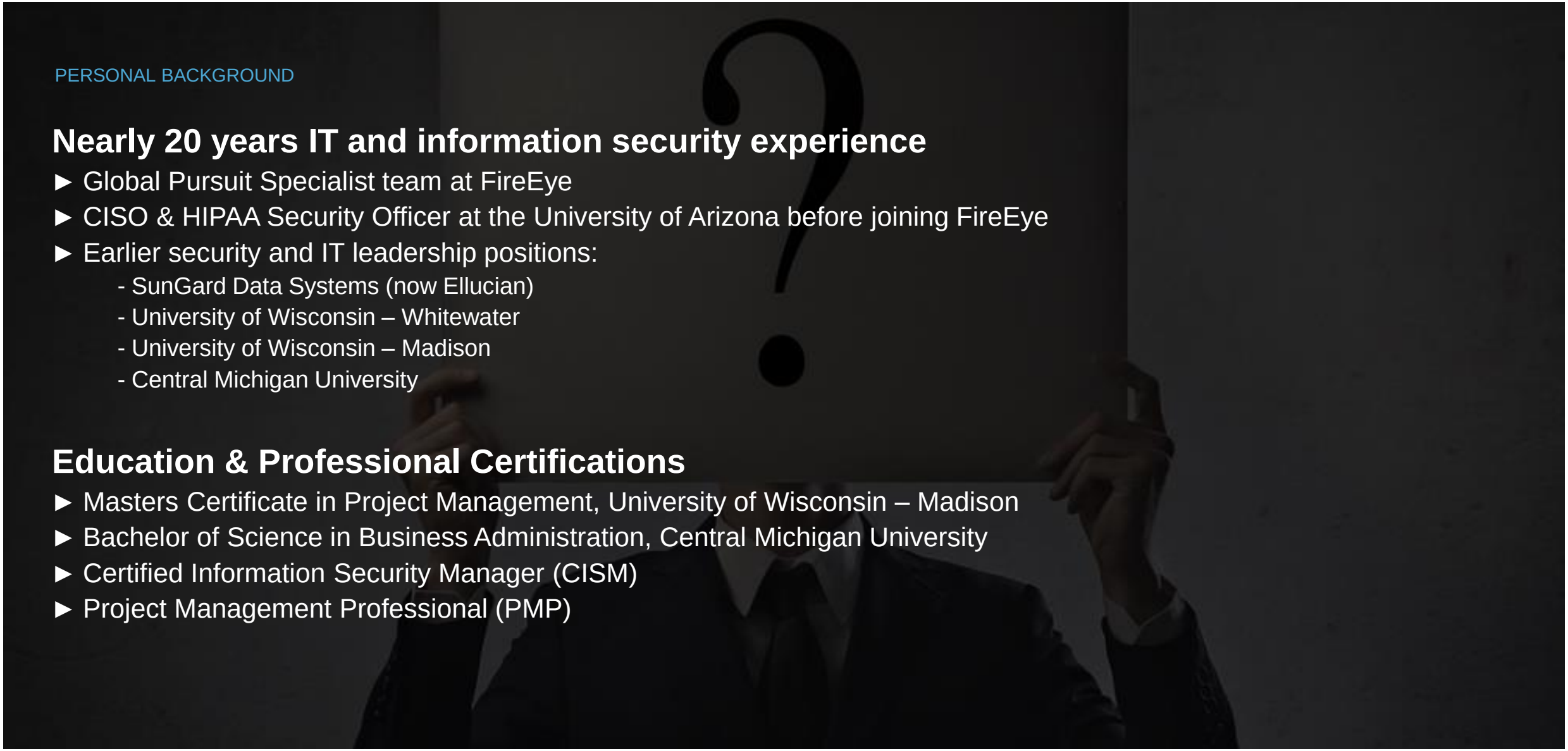
INNOVATION & TECHNOLOGY SUMMIT

UT DALLAS – 16 MAY 2017

Christian Schreiber, CISM, PMP

Consulting SE – Global Pursuit Specialist

FireEye
SECURITY REIMAGINED



PERSONAL BACKGROUND

Nearly 20 years IT and information security experience

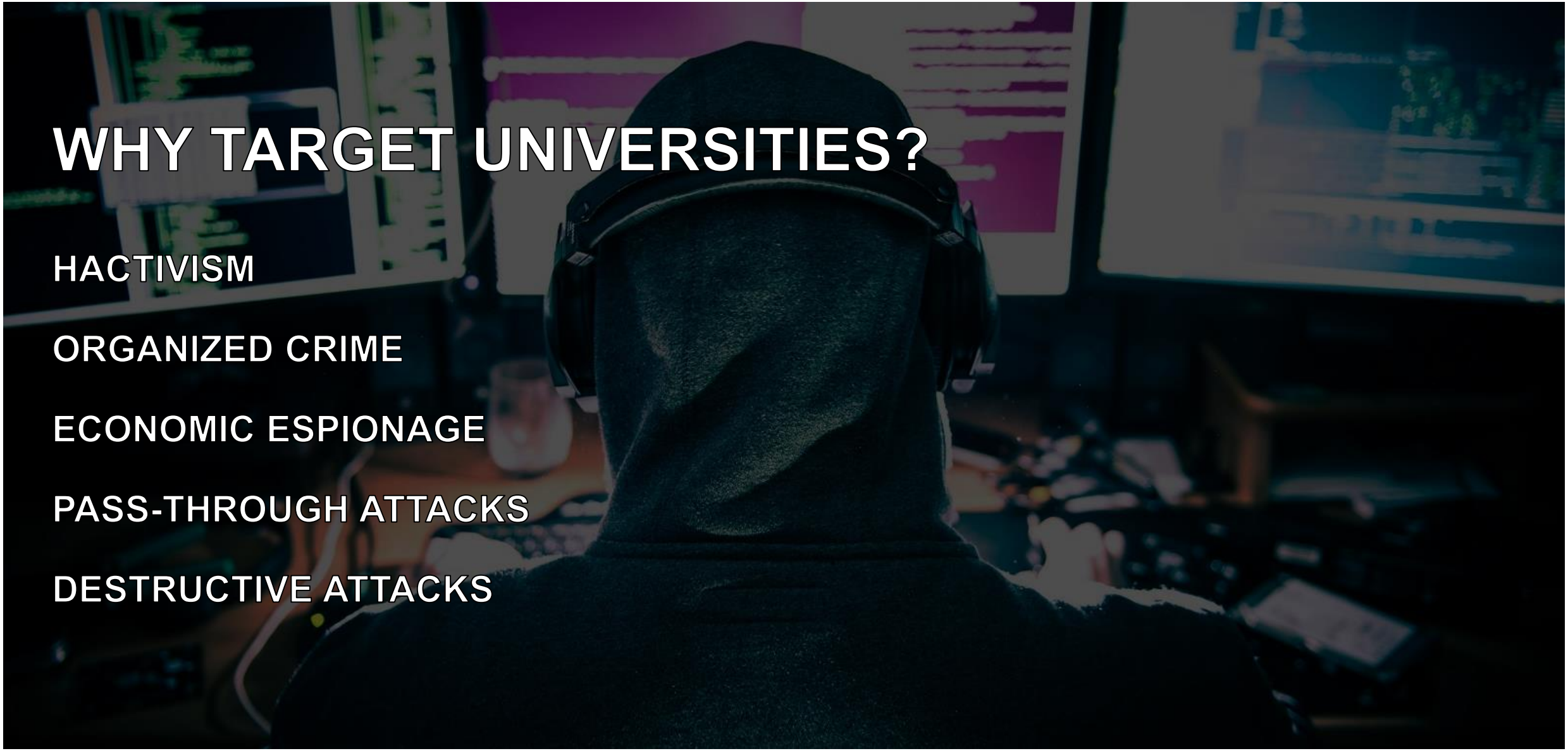
- Global Pursuit Specialist team at FireEye
- CISO & HIPAA Security Officer at the University of Arizona before joining FireEye
- Earlier security and IT leadership positions:
  - SunGard Data Systems (now Ellucian)
  - University of Wisconsin – Whitewater
  - University of Wisconsin – Madison
  - Central 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)

NON-IT LEADERS ARE BECOMING MORE AWARE OF CYBER THREATS

FireEye



WHY TARGET UNIVERSITIES?

HACTIVISM

ORGANIZED CRIME

ECONOMIC ESPIONAGE

PASS-THROUGH ATTACKS

DESTRUCTIVE ATTACKS

FireEye

DEFENSE-IN-DEPTH AIMS TO PREVENT ATTACKS

FireEye

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

PREVENTION IS NOT ENOUGH

STUDIED 1600+ ORGANIZATIONS, INCLUDING MORE THAN 100 EDUCATION INSTITUTIONS

100% OF EDUCATION INSTITUTIONS COMPROMISED DURING TEST PERIOD

37% HAD EVIDENCE OF ADVANCED ATTACKS

YOU NEED TO HUNT FOR INTRUDERS THAT ARE ALREADY INSIDE

FireEye

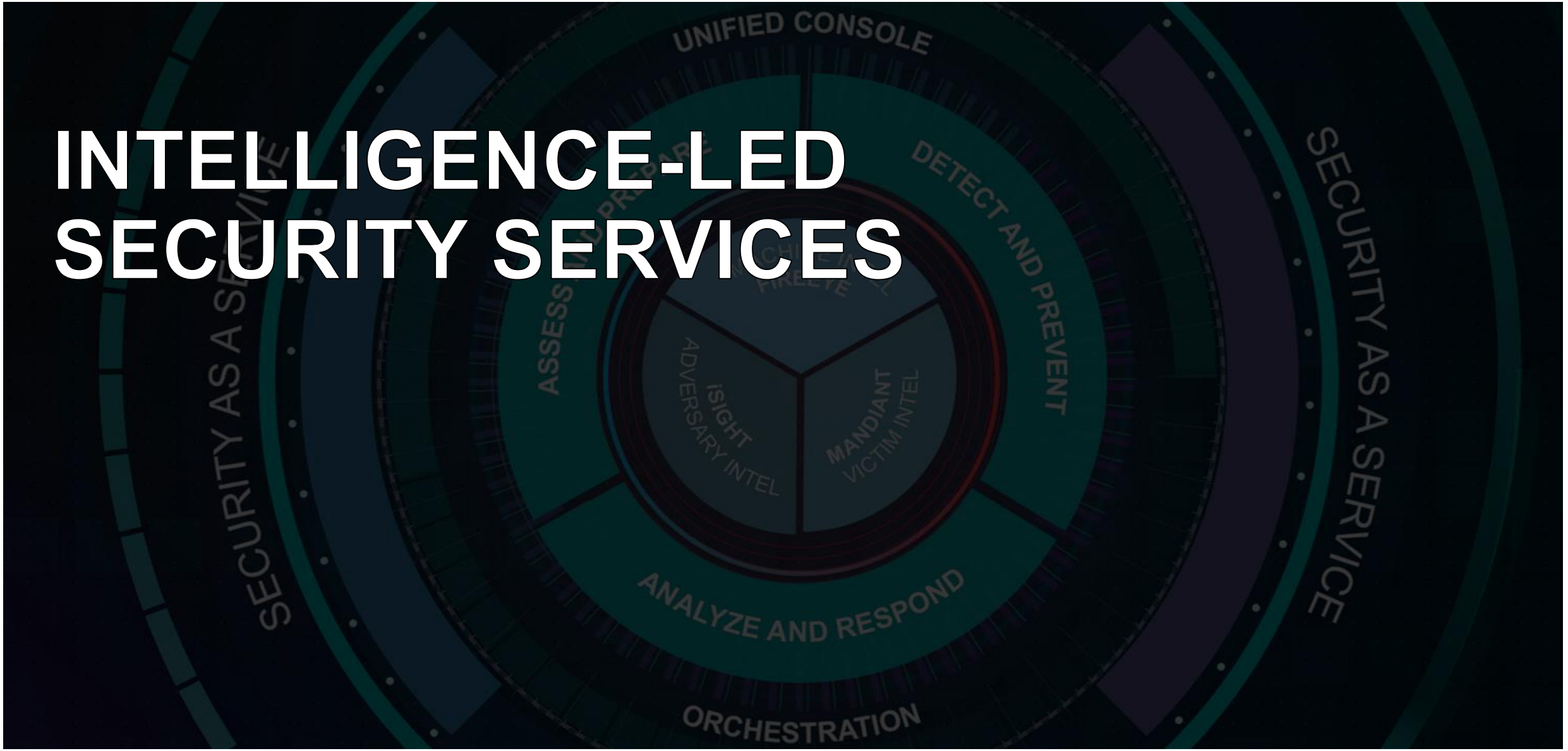
WHY? CYBERSECURITY THREATS ARE ASYMMETRIC

FireEye

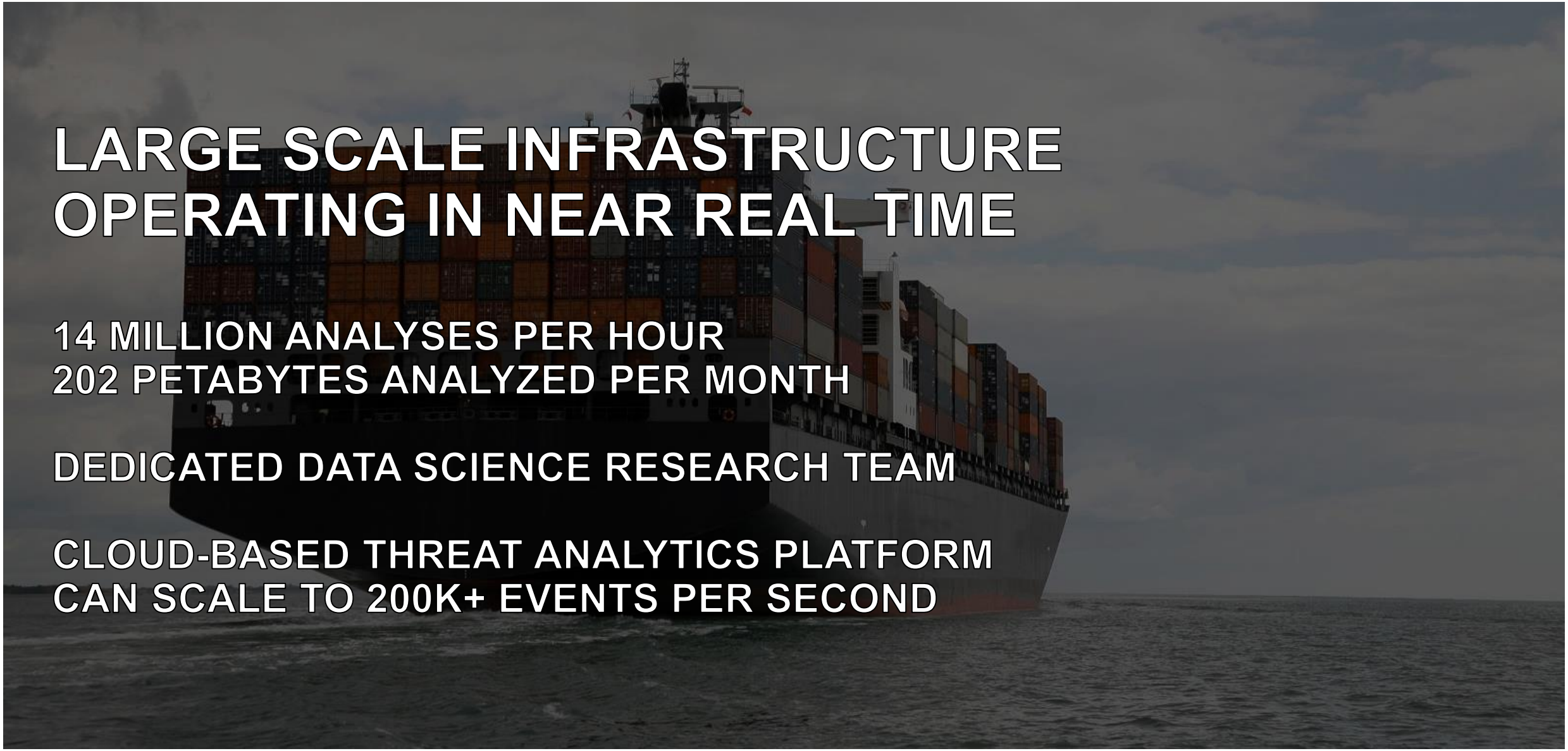
YOU NEED A STRATEGY THAT GOES BEYOND PREVENTING ATTACKS

FireEye

INTELLIGENCE-LED SECURITY SERVICES



FireEye



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 SCALE TO 200K+ EVENTS PER SECOND

GLOBAL VISIBILITY INTO MACHINE, VICTIM, AND ADVERSARY INTELLIGENCE

15 MILLION SENSORS IN 89 COUNTRIES
200,000+ INCIDENT RESPONSE HOURS PER YEAR
1000+ SECURITY AND INTELLIGENCE EXPERTS

PROTECT MORE THAN 65% OF THE FORTUNE 500 AND HUNDREDS OF GOVERNMENT, EDUCATION, AND NON-PROFITS

FireEye

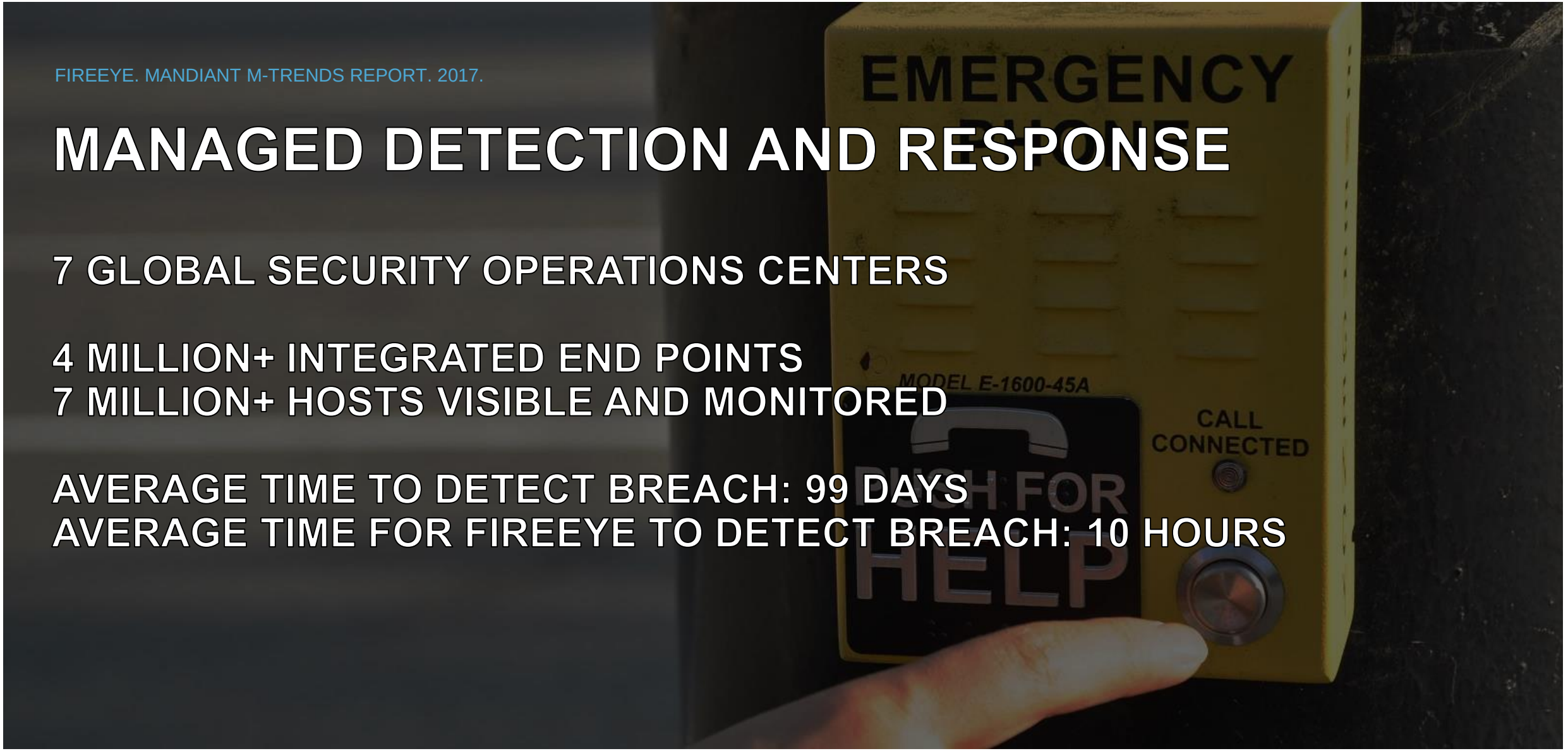
TIMELY & RELEVANT THREAT INTELLIGENCE

FIREEYE TRACKS MORE THAN 16,000 THREATS

174 MILLION NODE GRAPH DATABASE
583 MILLION CORRELATION RELATIONSHIPS

UPDATES DISTRIBUTED IN UNDER AN HOUR TO PROTECT ALL CUSTOMERS GLOBALLY

MANAGED DETECTION AND RESPONSE



7 GLOBAL SECURITY OPERATIONS CENTERS

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

AVERAGE TIME TO DETECT BREACH: 99 DAYS
AVERAGE TIME FOR FIREEYE TO DETECT BREACH: 10 HOURS

CUSTOMERS BENEFIT FROM INTELLIGENCE-LED SECURITY

CONFIDENCE WITH <1% FALSE POSITIVES

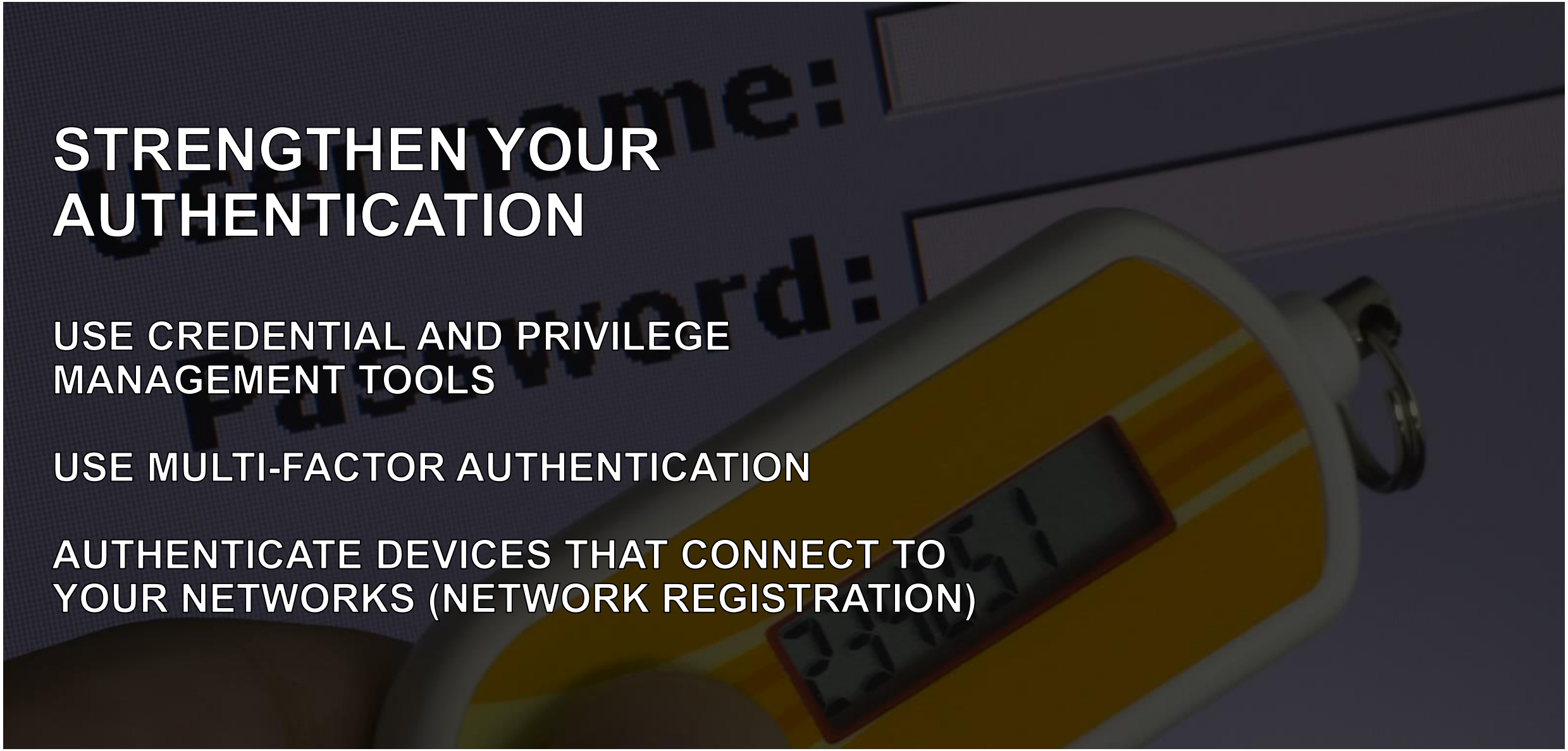
RESPONSE TIME REDUCED BY 95%

>90% CUSTOMER RENEWAL RATE

FireEye

HOW CAN YOU IMPROVE YOUR CYBER RESILIENCE?

FireEye



STRENGTHEN YOUR AUTHENTICATION

USE CREDENTIAL AND PRIVILEGE MANAGEMENT TOOLS

USE MULTI-FACTOR AUTHENTICATION

AUTHENTICATE DEVICES THAT CONNECT TO YOUR NETWORKS (NETWORK REGISTRATION)

STRENGTHEN YOUR ARCHITECTURE

SEPARATE WHAT'S TRULY PUBLIC FROM WHAT SHOULD BE INTERNAL

RISK-BASED NETWORK SEGMENTATION

ROLE-BASED DATA SEGREGATION

FireEye

IMPLEMENT PROCESSES AND TOOLS TO HUNT FOR THREATS

MALWARE SANDBOXING, CYBER THREAT INTELLIGENCE, SIEM & DATA ANALYTICS

FireEye

FIREEYE. MANDIANT M-TRENDS REPORT. 2015.

EXTEND YOUR VISIBILITY

46% OF COMPROMISES DON'T USE MALWARE

COLLECT DATA TO ENABLE BETTER MONITORING, ALERTING, AND INVESTIGATION

UNDERSTAND WHAT SYSTEMS, APPLICATIONS, AND DATA ARE CRITICAL

FireEye

ADOPT “CONTINUOUS IMPROVEMENT” MINDSET

ALLOCATE TIME TO BRAINSTORM, UNDERSTAND YOUR DATA, AND IMPROVE

HUNTING INTRUDERS IS AN ONGOING ACTIVITY, NOT A ONE TIME “BREAK GLASS”

FireEye

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

MOST SECURITY TEAMS CAN ONLY REVIEW 4% OF ALERTS

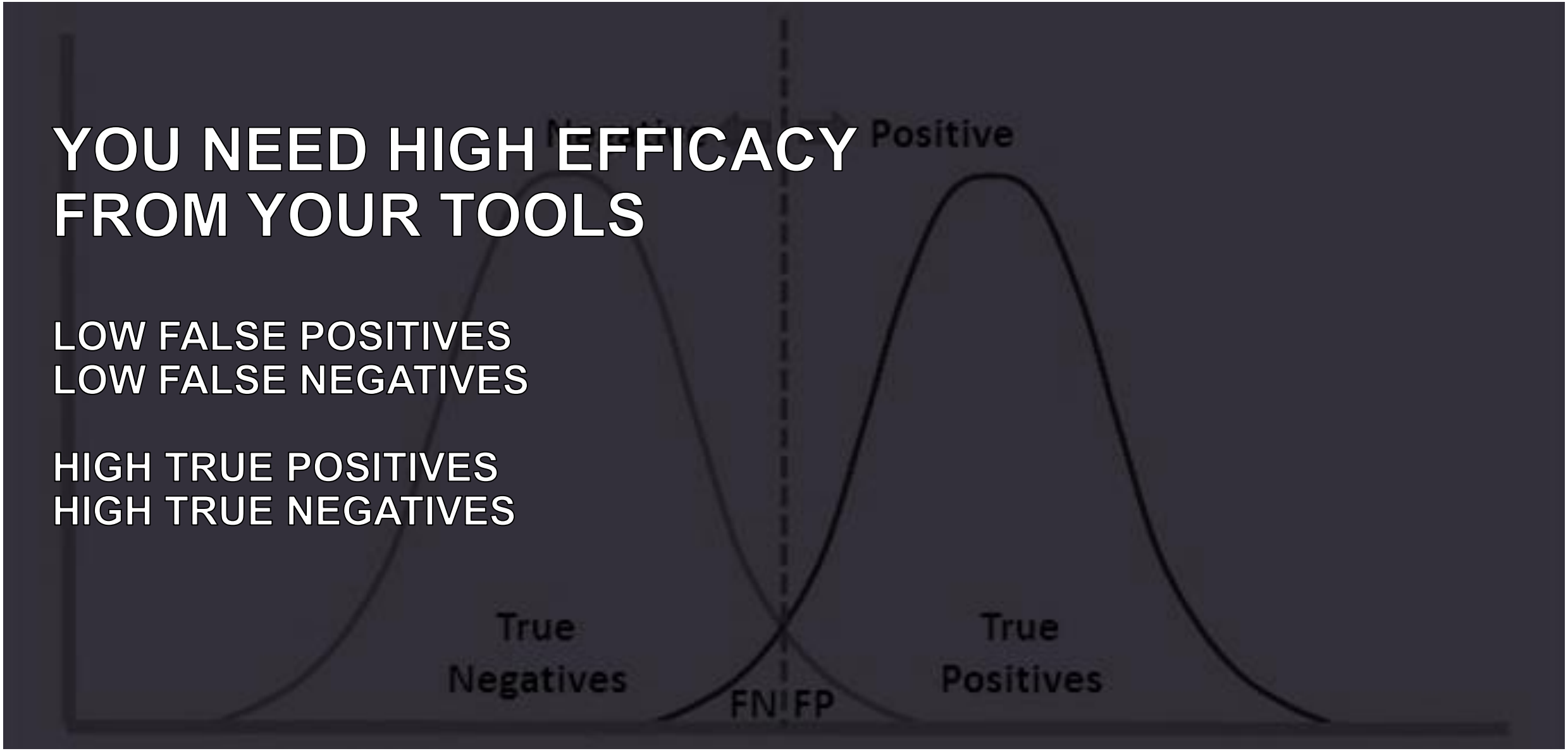
ARE YOUR SECURITY INVESTMENTS HELPING YOU FIND THE ALERTS THAT MATTER?

FireEye

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

FireEye

YOU NEED VISIBILITY INTO BROADER PATTERNS

ARE SIMILAR EVENTS HAPPENING ELSEWHERE IN YOUR ORGANIZATION?

ACROSS YOUR INDUSTRY?

FireEye

YOU NEED EFFICIENCY FROM SECURITY INVESTMENTS

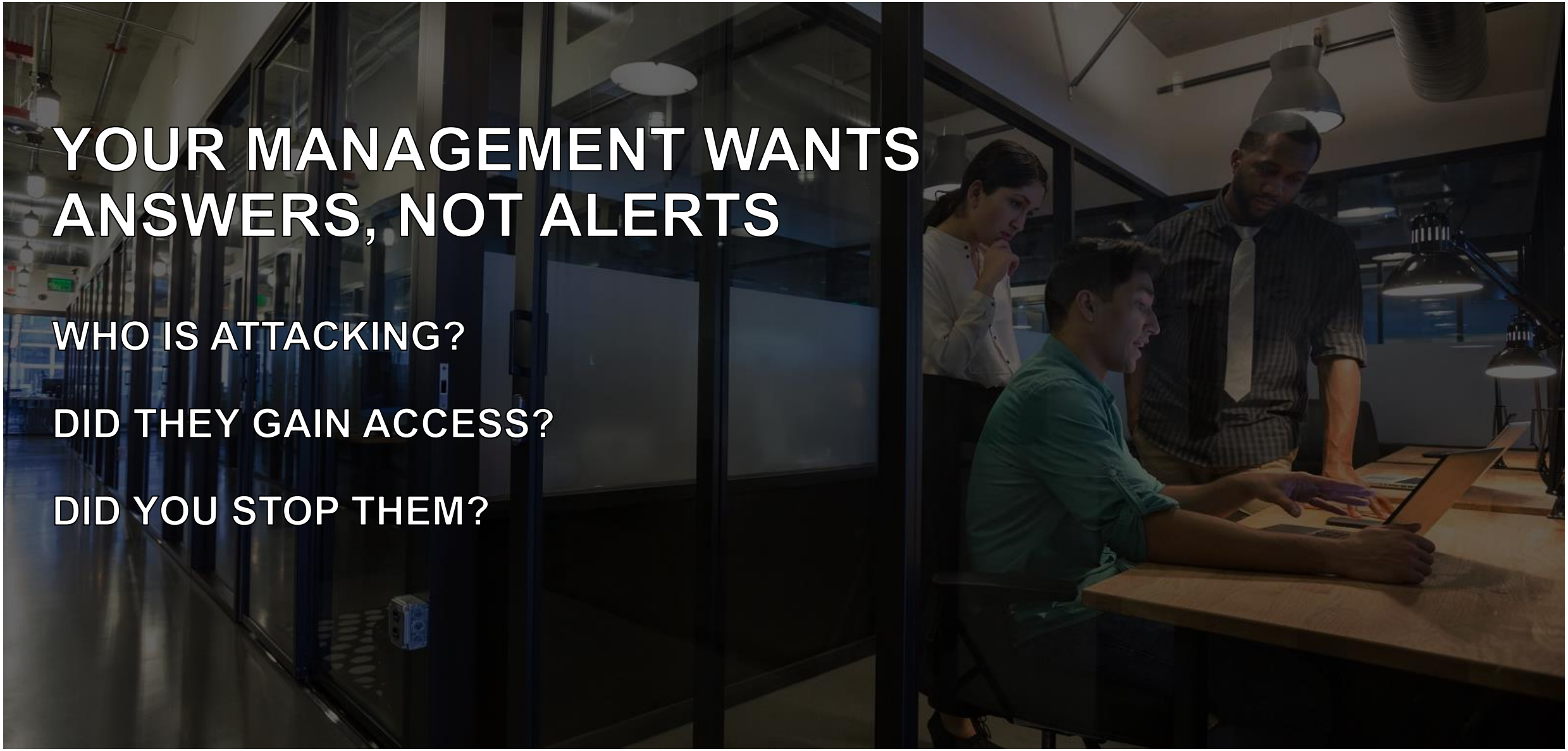
SECURITY TOOLS NEED TO FUNCTION TOGETHER SEAMLESSLY

SECURITY TEAMS NEED TO SPEND LESS TIME ON LOW VALUE TASKS

YOU NEED EXPERTS TO MANAGE YOUR RESPONSE

EVEN THE BEST TOOLS ARE USELESS WITHOUT PROFESSIONALS TO RUN THEM

FireEye



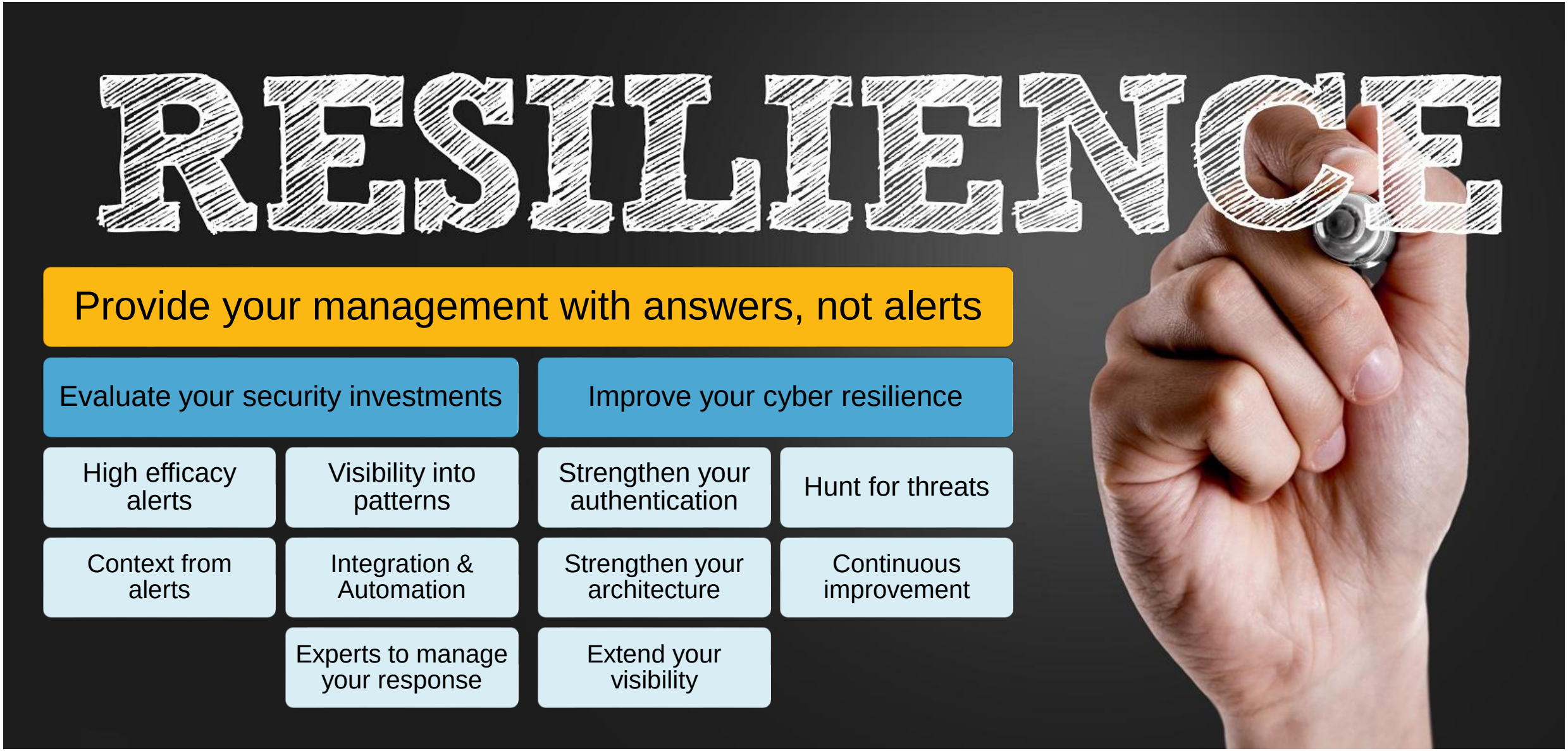
YOUR MANAGEMENT WANTS ANSWERS, NOT ALERTS

WHO IS ATTACKING?

DID THEY GAIN ACCESS?

DID YOU STOP THEM?

FireEye



Provide your management with answers, not alerts

Evaluate your security investments

- High efficacy alerts
- Visibility into patterns
- Context from alerts
- Integration & Automation
- Experts to manage your response

Improve your cyber resilience

- Strengthen your authentication
- Hunt for threats
- Strengthen your architecture
- Continuous improvement
- Extend your visibility

FireEye

THANK YOU!

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

FireEye
SECURITY REIMAGINED