
FireEye
SECURITY REIMAGINED
COMBATTING
CYBER THREATS
PRESENTED BY
President, FireEye, Inc

YEAR IN REVIEW

~ 500 INVESTIGATIONS

FireEye
SECURITY REIMAGINED

~17 COUNTRIES

FireEye
SECURITY REIMAGINED

CONCLUSIONS

AGENDA

SO WHAT DO WE DO?

FIVE YEARS OUT

THERE ARE **FEW RISKS**
REPERCUSSIONS
FOR THE ATTACKERS

FireEye
SECURITY REIMAGINED

ATTACKERS CONTINUE TO
EXPLOIT **HUMAN TRUST**

FireEye
SECURITY REIMAGINED

Attacks Will Continue to Reflect Geopolitical Conditions

CYBER-CRIME TRADECRAFT HAS **IMPROVED DRASTICALLY**

EXTORTION IN CYBERSPACE IS RISING (BACK?)

DISCLOSURE IS MORE PROBABLE

FireEye
SECURITY REIMAGINED

DETECTION EFFICACY IS **WEAKER** IN **LATER** **STAGES** OF THE KILL CHAIN

FireEye
SECURITY REIMAGINED

ZERO DAYS DEPLOYED BY **NATION STATES**

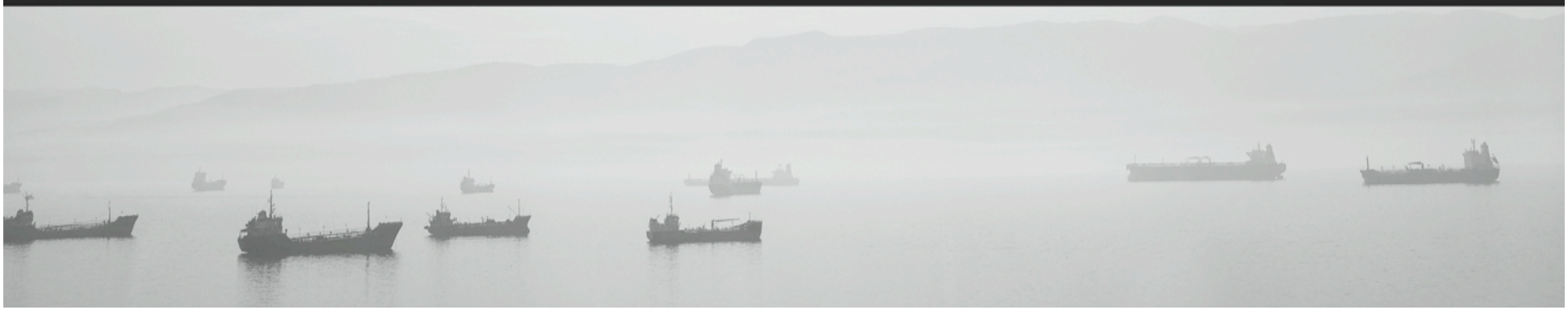
FireEye
SECURITY REIMAGINED

ATTRIBUTION IS GETTING HARDER

ACCURATE AND TIMELY ATTRIBUTION IS CRITICAL
FOR
DETERRENCE & LIABILITY

KEY WEAKNESSES

- Failure to detect spear phishing or malicious attacks
- Poor Credential Management
- Lack of Network Segmentation
- Single factor access to VPN or OWA
- Security safeguards not armed from privileged accounts
- Critical data for response not being collected



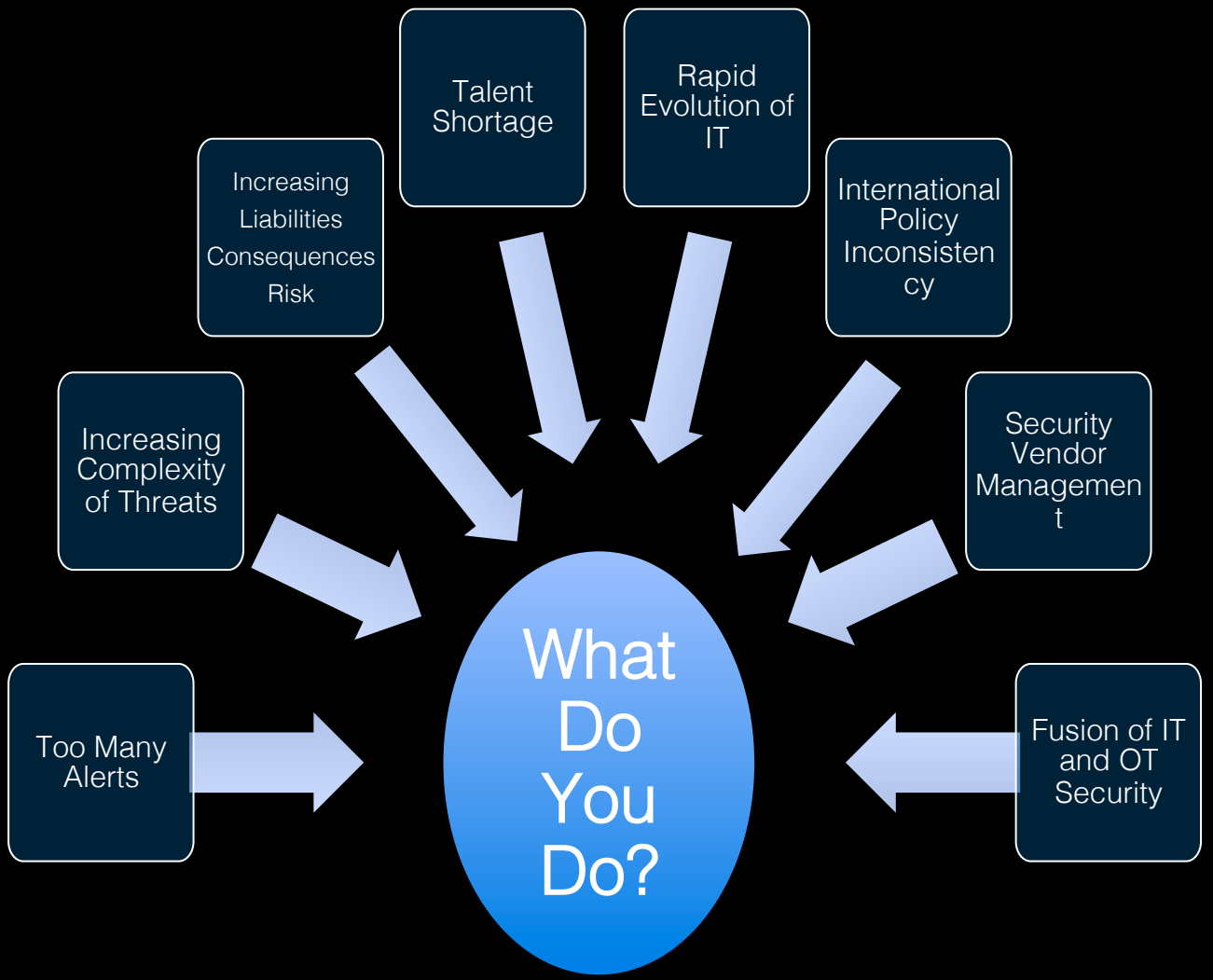
AGENDA

CONCLUSIONS

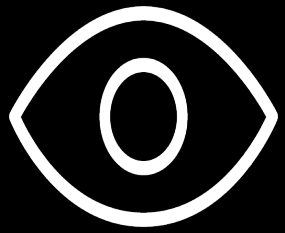
SO WHAT DO WE DO?

FIVE YEARS OUT

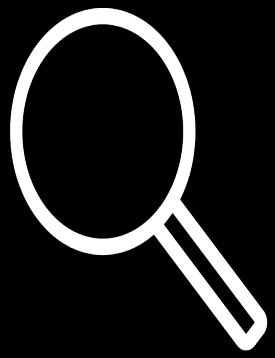
The CISO Dilemma …



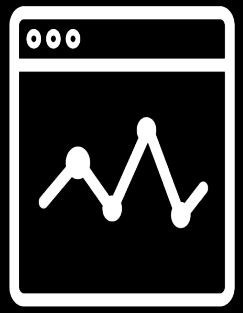
Talent Shortage Addressed by Increased Automation



Higher Fidelity



Threat Data



Analytics / ML

PROTECT THE NETWORK
TO
PROTECT THE DATA

- SECURE ENCLAVES
- NETWORK SEGMENTATION
- CLOUD MIGRATION

FireEye
SECURITY REIMAGINED

PERIMETER PROTECTION
TO
COMPREHENSIVE PROTECTION

- NETWORK
- ENDPOINT
- CLOUD

- EXPLOIT
- MALWARE
- C2
- LATERAL MOVEMENT
- EXFIL
- TTPs

FireEye
SECURITY REIMAGINED

LOG MANAGEMENT
TO
SECURITY ANALYTICS

- FILTER THE NOISE
- ANOMALY DETECTION

FireEye
SECURITY REIMAGINED

REACT
TO
PROACTIVE HUNTING

- THREAT DATA FEED
- THREAT INTELLIGENCE
(WHO)
- DETECT THE KNOWNS

FireEye
SECURITY REIMAGINED

VULNERABILITY ASSESSMENT

COMPROMISE ASSESSMENT

Penetration Testing → Red Teaming

Penetration Testing

Red Teaming

FireEye

Emergence of Security Orchestration (Consolidation / Integration / Automation)

What Is Working

- Create Secure Enclaves
- Credential Management
- “Dry Runs” of Incident Response Plan
- Focus on Phishing Prevention
- Require Two-Factor Authentication for Remote Access
- Only Permit Authorized Programs to Run on Servers
- Use New Technology to Block Advanced Malware
- Promote a “Security Culture”

FIVE YEARS OUT

ALL CONFLICT WILL HAVE A CYBER COMPONENT

FireEye
SECURITY REIMAGINED

ESTABLISHING INTERNATIONAL RULES OF ENGAGEMENT

PRIVACY AND ANONYMITY

Assess Your Team

How would you compromise our company?
If an attack was successful, how would we detect it?
If we had a security breach today, what is the worst-case scenario? Who would you disclose the details to?

THANK YOU