THE NEW CHALLENGE CYBER CHALLENGES

Serge Bertini, VP Sales and GM Canada
TODAY’S THREAT OUTLOOK IS BLURRY
BLURRED LINES

ADVERSARY TYPES
2018 Targeted State-Sponsored Intrusions by Region

- China
  - Targeting Big Sectors
  - Many Countries (US too!)

- North Korea
  - Currency Generation

- Iran
  - New Adversaries & TTPs Evolving

- Russia
  - DNC Actor Very Active
  - Updating its Toolkit
BLURRED LINES
ATTACK TYPES

DESTRUCTIVE ATTACK
SELF-REPLICATION
RANSOMWARE
LEAKED ZERO-DAY
BLURRED LINES
ATTACK TYPES

- Destructive Attack
- Self-Replication
- Leaked Zero-Day
- Ransomware
BLURRED LINES

GEOGRAPHIC BOUNDARIES ARE NONEXISTENT
BLURRED LINES

RED TAPE & REGULATIONS

- PCI DSS
- FFIEC
- FISMA
- CSA STAR
- HIPAA COMPLIANT
- AICPA SOC 2
- NIST
- NIST
- NATIONAL SECURITY AGENCY
- GDPR
“DEFENSE IN DEPTH”
INDEFENSIBLE
Defense in Depth has failed.
SO WHAT CAN WE DO ABOUT THIS?
THE NEW PILLAR OF CYBER ATTACKS

- IP THEFT
- ESPIONAGE
- DISRUPTION
- eCRIME
THE NEW PILLAR OF CYBER ATTACKS

- IP THEFT
- ESPIONAGE
- DISRUPTION
- eCRIME
- INFORMATION WEAPONIZATION
THE NEW DIMENSION: DEFENSE IN BREADTH
"A planned, systematic (approach) to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle."

— NIST DEFINITION OF "DEFENSE IN BREADTH"
SPEED IS EVERYTHING
BREAKOUT TIME

1 HOUR

58 MINUTES

SOURCE: CROWDSTRIKE’S 2018 GLOBAL THREAT REPORT
AVERAGE TIME TO REMEDIATE

63 HOURS

SOURCE: CROWDSTRIKE 2018 GLOBAL SUPPLY CHAIN ATTACKS SURVEY
BREAKOUT TIME BY ADVERSARY FOR 2018

BEAR 00:18:49

CHOLLIMA 02:20:14

PANDA 04:00:26

KITTEN 05:09:04

SPIDER 09:42:23
SO WHAT CAN WE DO ABOUT THIS?
SURVIVAL OF THE FASTEST:

THE 1-10-60 RULE

1 MINUTE
TIME TO DETECT

10 MINUTES
TIME TO INVESTIGATE

60 MINUTES
TIME TO REMEDIATE & CONTAIN
TIME TO INVESTIGATE

10 MINUTES

ENDPOINT DETECTION & RESPONSE

THREAT INTELLIGENCE

MANAGED HUNTING

REMOTE FORENSIC INVESTIGATIONS
60 MINUTES

TIME TO REMEDIATE & CONTAIN

- CLOUD-BASED REMOTE DEVICE MANAGEMENT
- PROACTIVE PLANNING & PREP
- GOOD BUSINESS PROCESSES
- EFFICIENT COMMUNICATION
ACHIEVING DEFENSE IN BREADTH:

So what’s next?