IBM Security

Threat Intelligence to enhance Cyber Resiliency

KEVIN ALBANO
GLOBAL THREAT INTELLIGENCE LEAD
IBM X-FORCE INCIDENT RESPONSE AND INTELLIGENCE SERVICES

IBM

Agenda

Welcome

Threat Intelligence EcoSystem

Cyber Resiliency Life Cycle

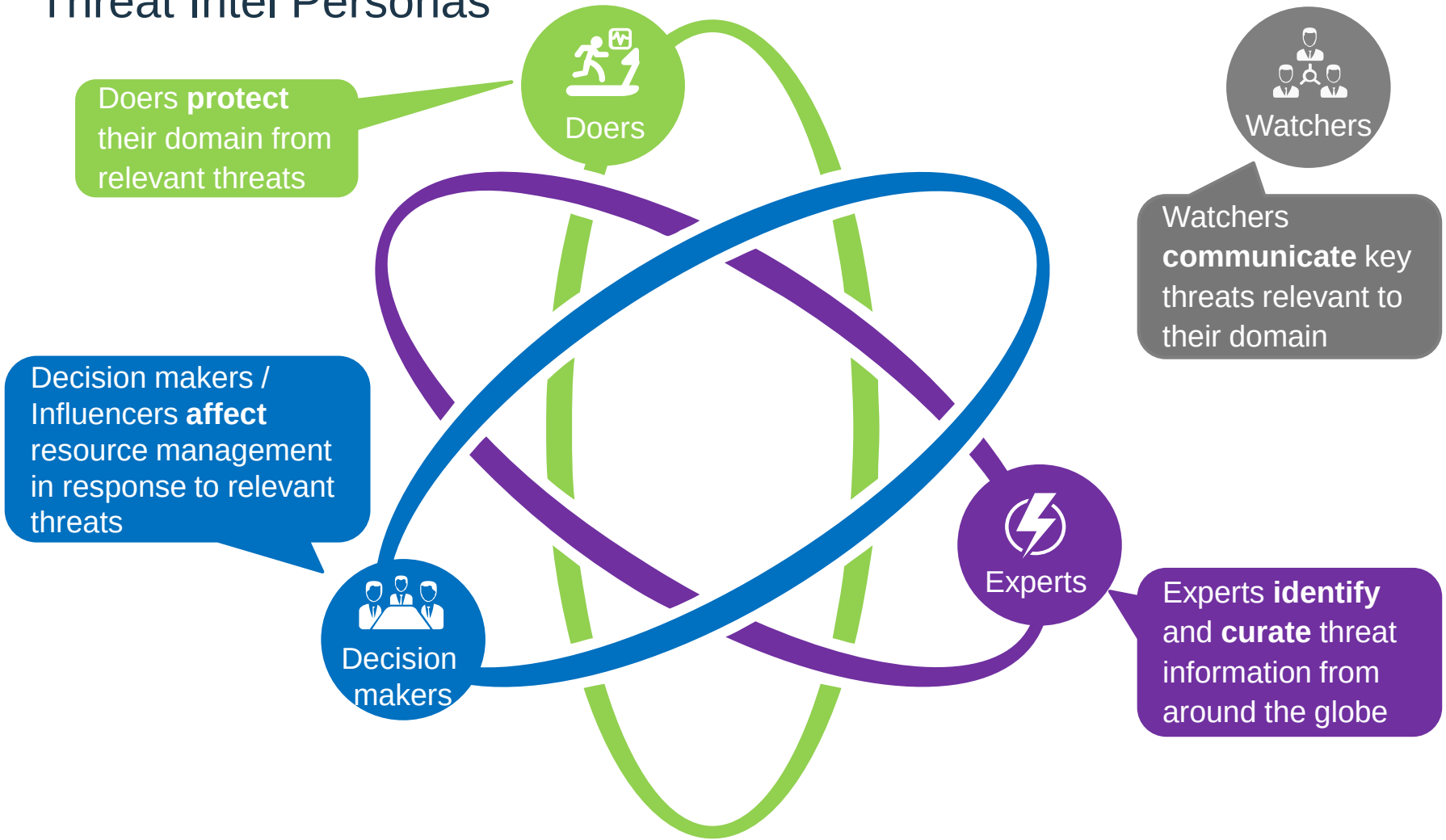
Questions

Exploits have an average life span of

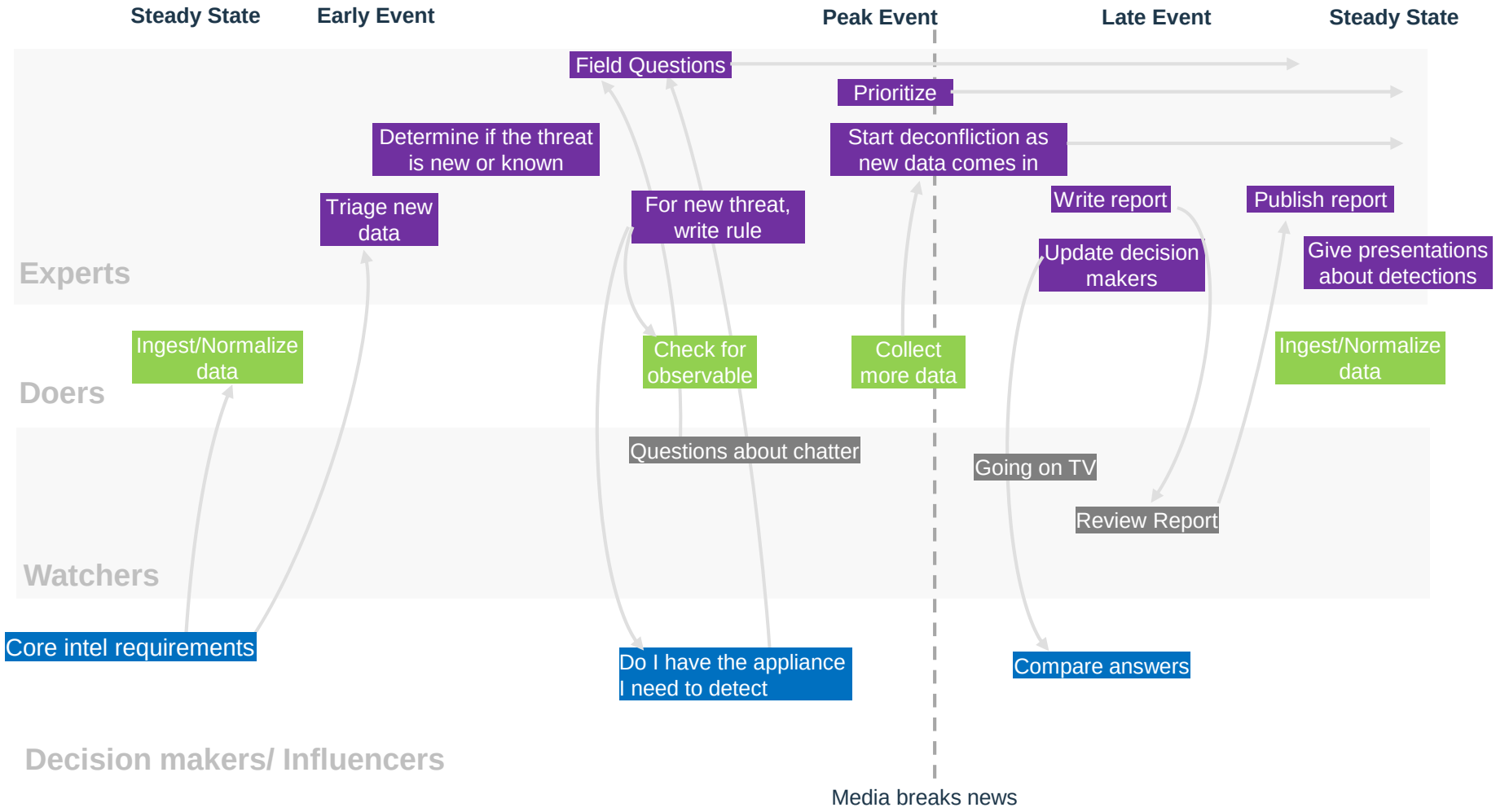
A. 2 years
B. 175 days
C. 6.9 years
D. 9.5 years

KEVIN ALBANO
IBM X-FORCE IRIS
Global Threat Intelligence Leader

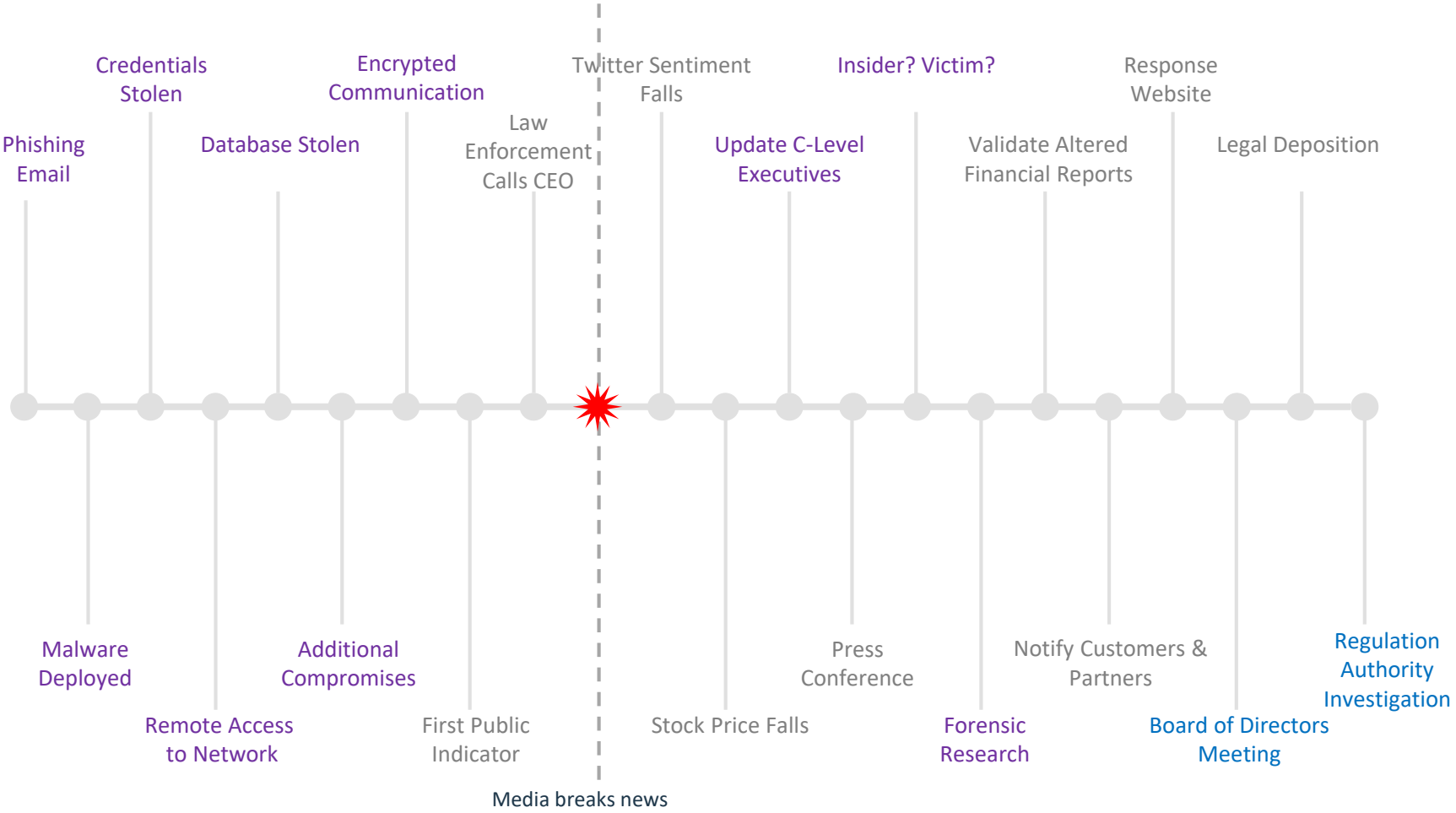
Threat Intel Personas



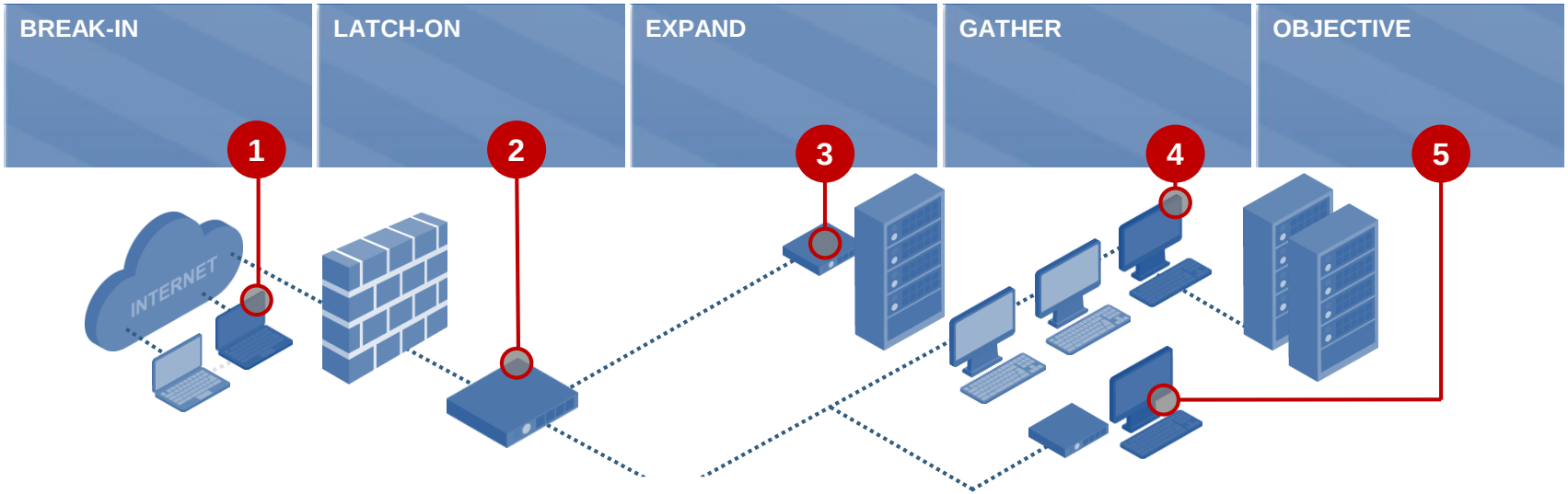
Responsibility Timeline



Reality Timeline



The Attack Chain



PEOPLE

- The right level of expertise to handle advanced attacks
- Respond quickly and efficiently; onsite and / or remotely
- Understand business process and security requirements
- Focused on protecting a clients intellectual property

PROCESS

- Controlled standards-based incident response plans
- Intelligence and malware analysis and reportin

TECHNOLOGY

- Endpoint event analysis in near real-time
- Watson for Cybersecurity bringing cognitive

Common Threat Vectors – Zero-Day Attacks

- RAND Study – Zero-Days, Thousands of Nights
  - Exploits have an average life of 6.9 years
  - 25% will not survive a year
  - 25% will survive more than 9.5 years
  - The median time to develop an exploit is 22 days from vulnerability discovery
  - For organizations that stockpile vulnerabilities, approximately 5.7 percent have been discovered and disclosed by others within 1 year

- How Would You Respond?

Ablon, Lillian and Timothy Bogart, Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits, Santa Monica, Calif.: RAND Corporation, RR-1751-RC, 2017.

As of September 30, 2017: https://www.rand.org/pubs/research_reports/RR1751.html

The Cyber Resiliency Life Cycle and Organizations Today

Detect unknown threats with advanced analytics

- See attacks across the enterprise
- Investigate active threats hiding inside the enterprise
- Detect attacks coming from outside the enterprise

Protect against attacks by discovering vulnerabilities before they are exploited

- Disrupt malware and exploits
- Discover and patch systems
- Automatically fix vulnerabilities
- Zero Trust as a guiding principle of your network policy

Respond to cyber outbreaks

- Engage cyber incident responders leveraging threat intelligence to repel the attackers
- Remediate the attack damage by restoring systems and closing vulnerabilities
- Utilize network resource to defend against outside threats

Recover access to critical data and applications

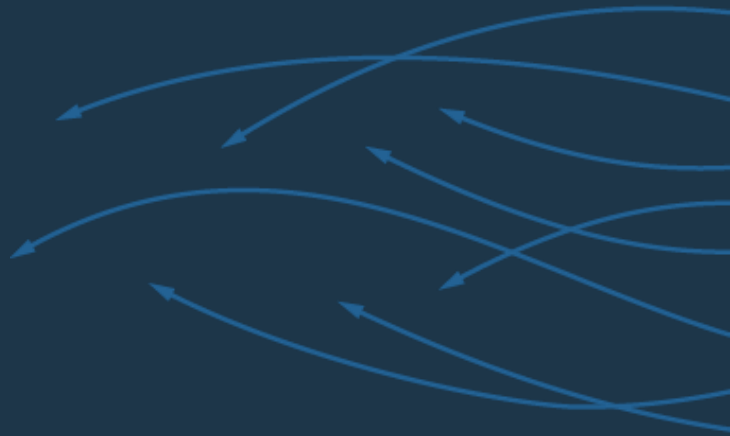
- Rebuild mission-critical business applications
- Restore data from back up
- Prioritize network resources to speed recovery

Prepare a cyber resiliency plan

- Assess cyber resiliency readiness, process and posture
- Orchestrate and automate recovery workflow

ASK AWAY!

Questions?



IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM