The Anatomy of a Data Breach

Andreas Fuhrmann
SKyPRO AG
andreas.fuhrmann@skypro.ch

John Waters
SailPoint
john.waters@sailpoint.com

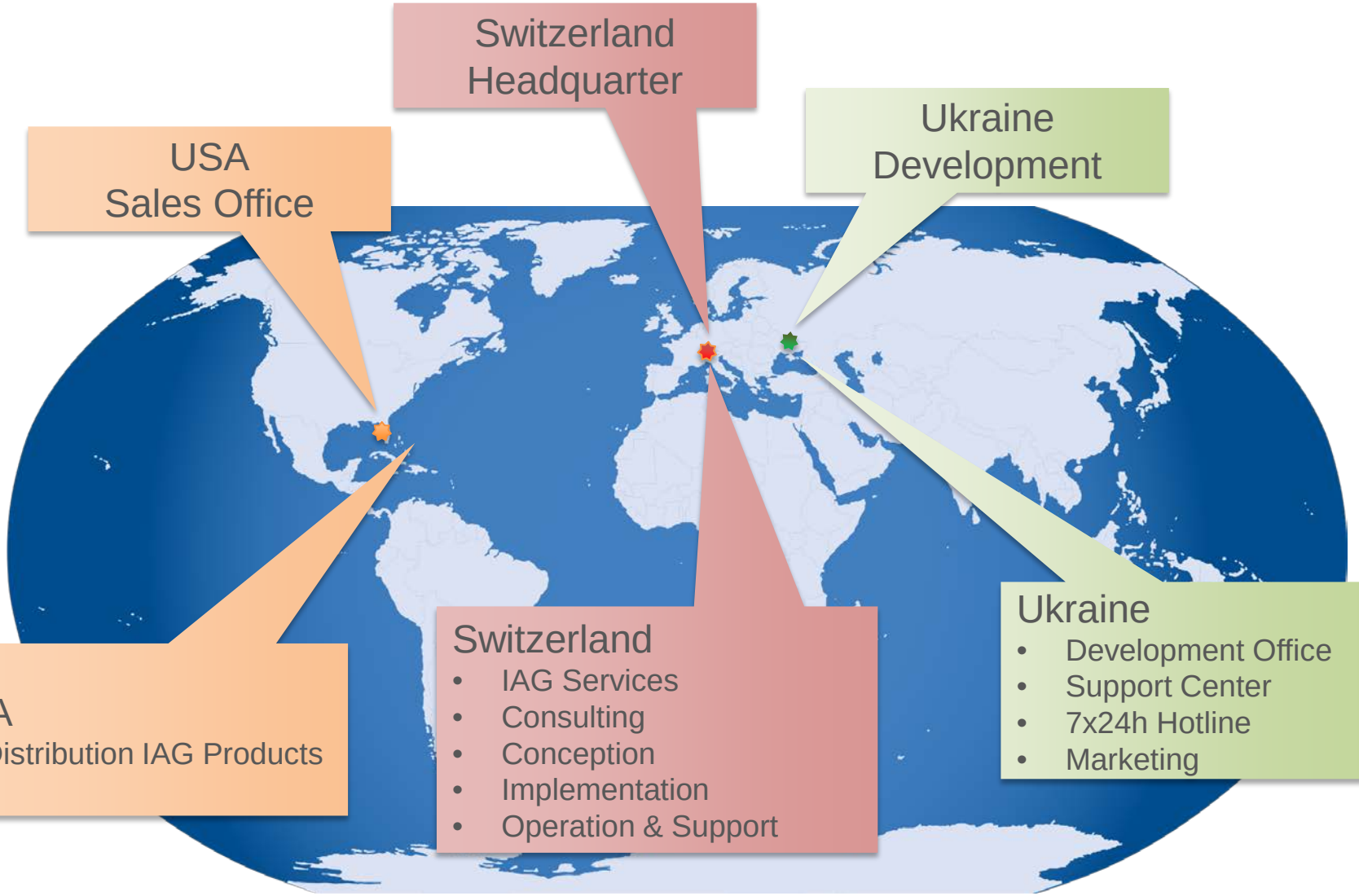
SKyPRO AG

Facts SKyPRO AG

- SKyPRO
  - founded April 1987
  - CHF 350‘000 AK
  - 50 employees
  - Headquarter in Cham
  - Development Office in the Ukraine
  - Sales Office in USA
  - CHF 7 Mio. Turnover

- we do
  - Identity & Access Governance (IAG) solution in Bank, Insurance, Industry, Government, Schools and Service Companies
  - Conulting, Conception, Implementation and Operation of IAG and security solutions
  - 30 years of experience as IT service company and over 15 years in IAG
  - SailPoint Partner

Facts SKyPRO AG



Learn from the past

Learn from the past

What can we learn from the past

FORENSICS AND POST BREACH ANALYSIS SHOWS

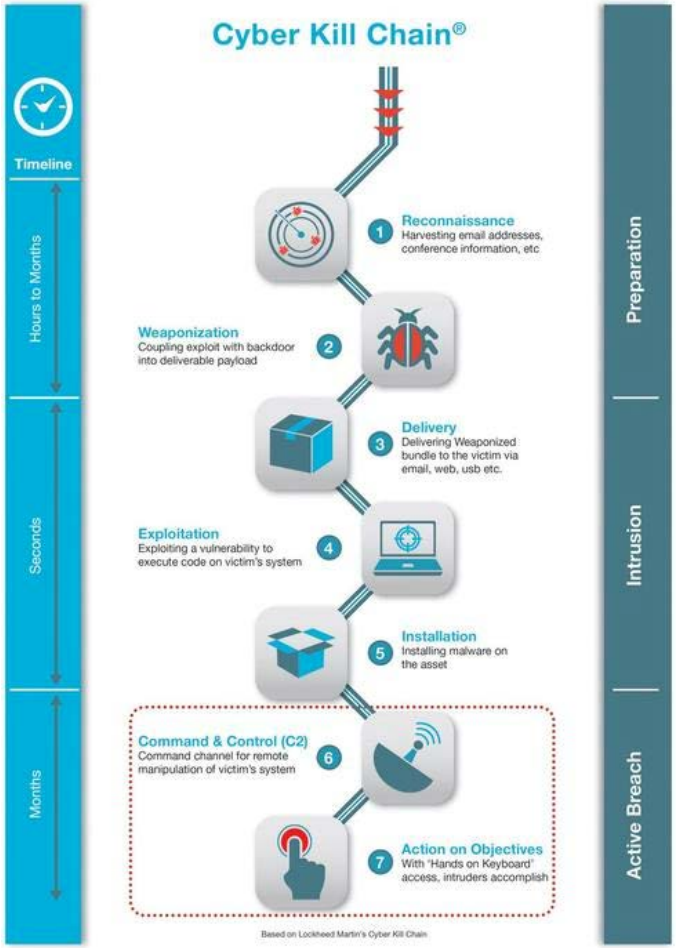
- Identity is a common weakness
- Entitlement and access is the attack target
- Files are responsible for 60% of breaches
- …..and are the most difficult to detect

SECURITY ERRORS AND WEAKNESSES ARE SPREAD OUT OVER A "CYBER KILL CHAIN"

- Poor account controls
- Weak passwords
- Orphan accounts
- Weak inventory and cataloging
- **Over assignment of user access**
- **Unstructured Data Insanity**

The Cyber Link Kill Chain

The Cyber Kill Chain



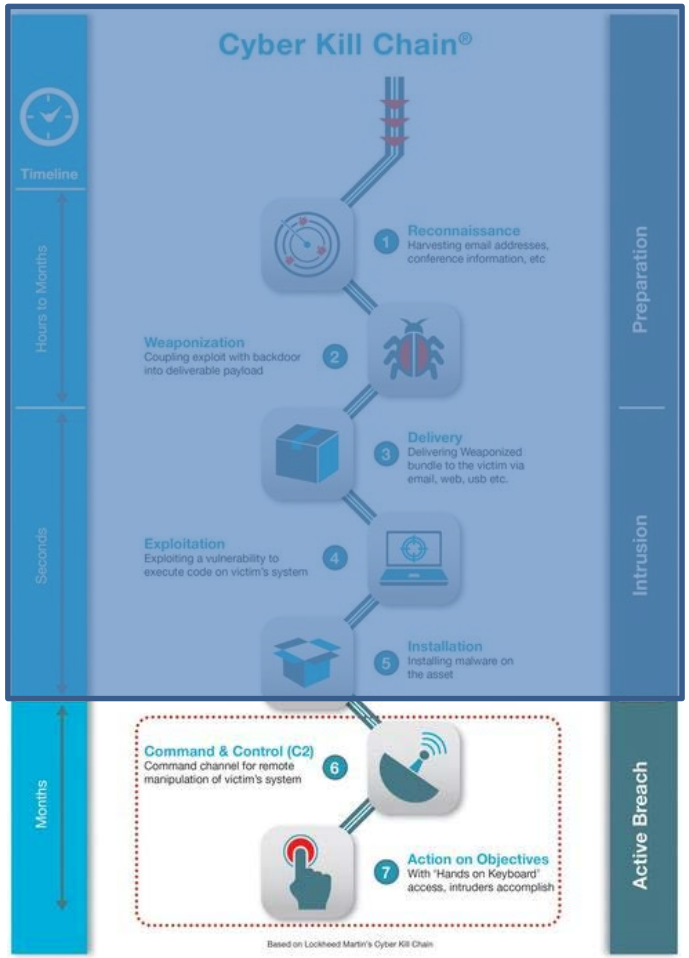
INTRODUCED BY LOCKHEED MARTIN '99

- Anatomy of a typical cyber breac
- Plots the path of an attack
- Reference model for cyber defense

PHASES OF ATTACK

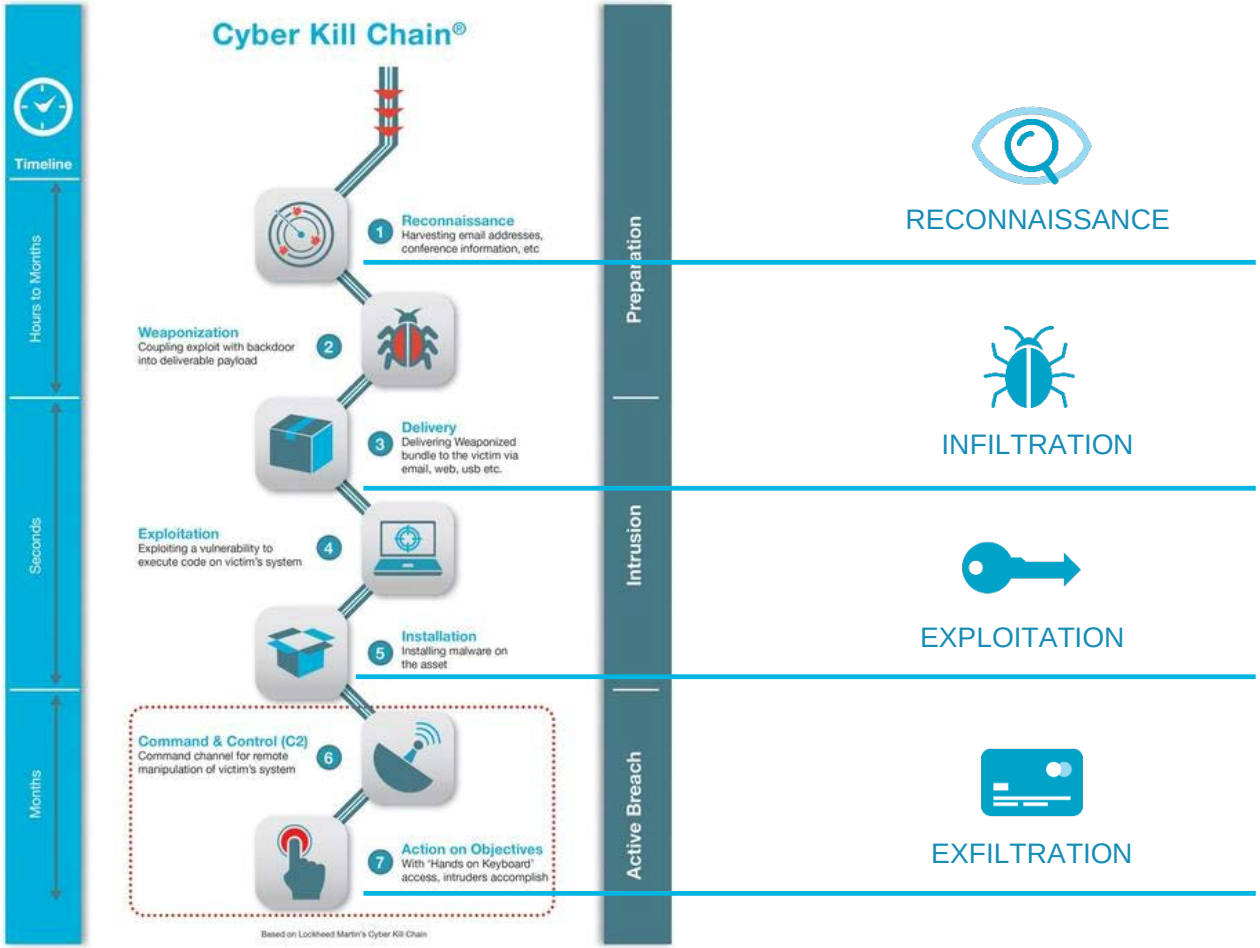
- Reconnaissance
- Weaponization
- Delivery
- Infiltration

The Cyber Kill Chain



Biggest area of weakness

The Cyber Kill Chain



The Anatomy of a Data Breach

The Anatomy of a Data Breach

The Players

THE VICTIM

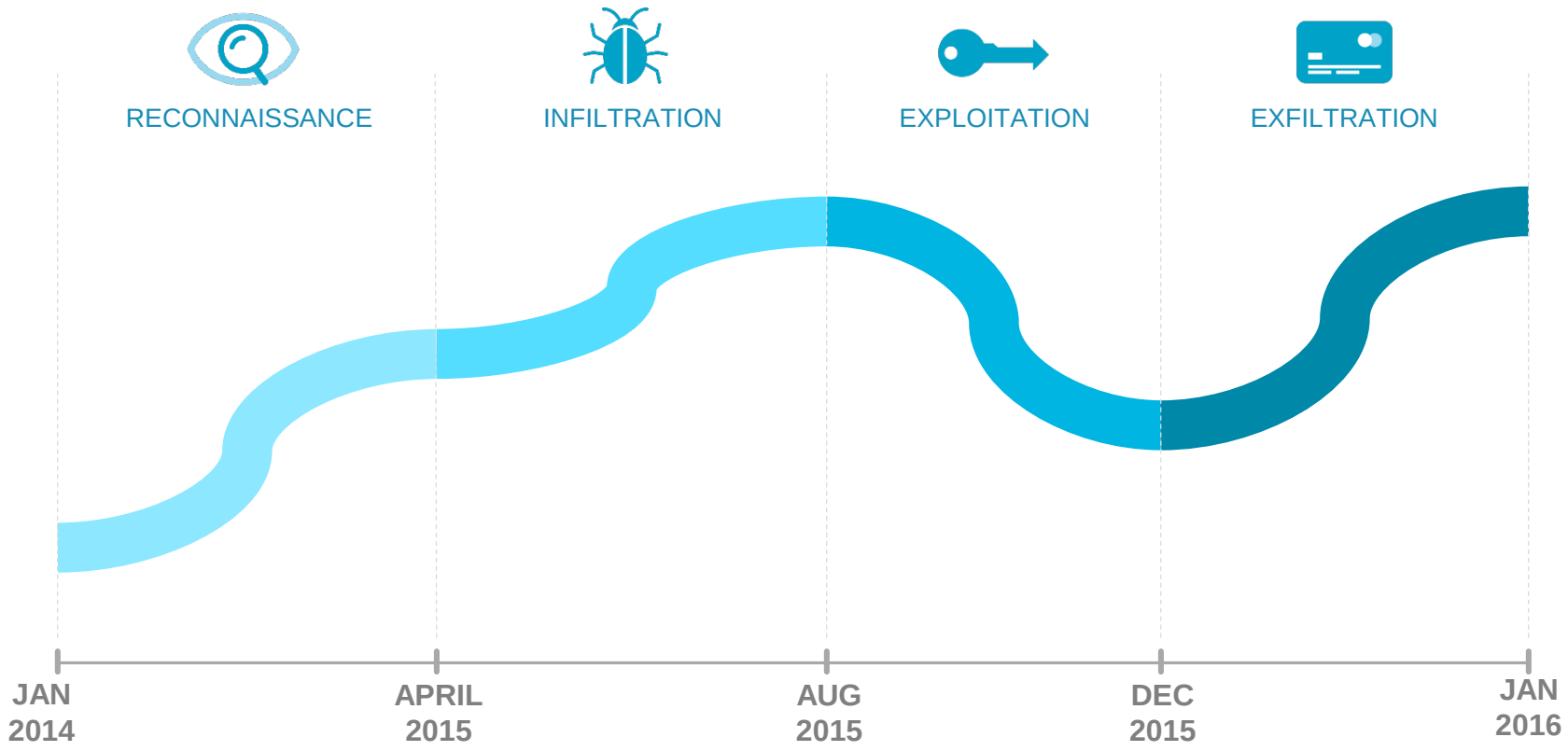
- A market leading manufacturing company with strong IP
- Big B2B and B2C presence on-line

THE ATTACKER

- A known organized crime syndicate in China
- Money, time and resources

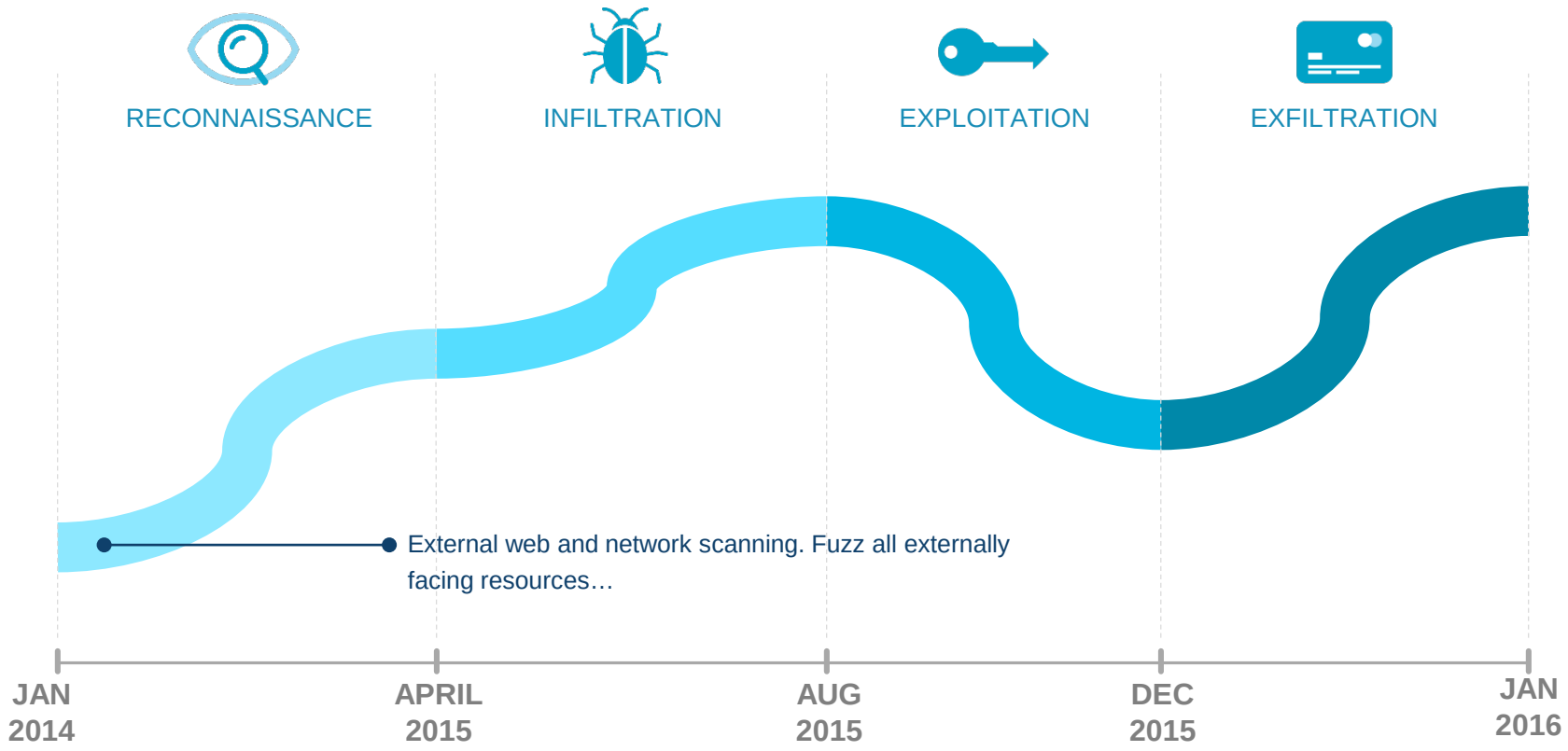
The Anatomy of a Data Breach

Timeline



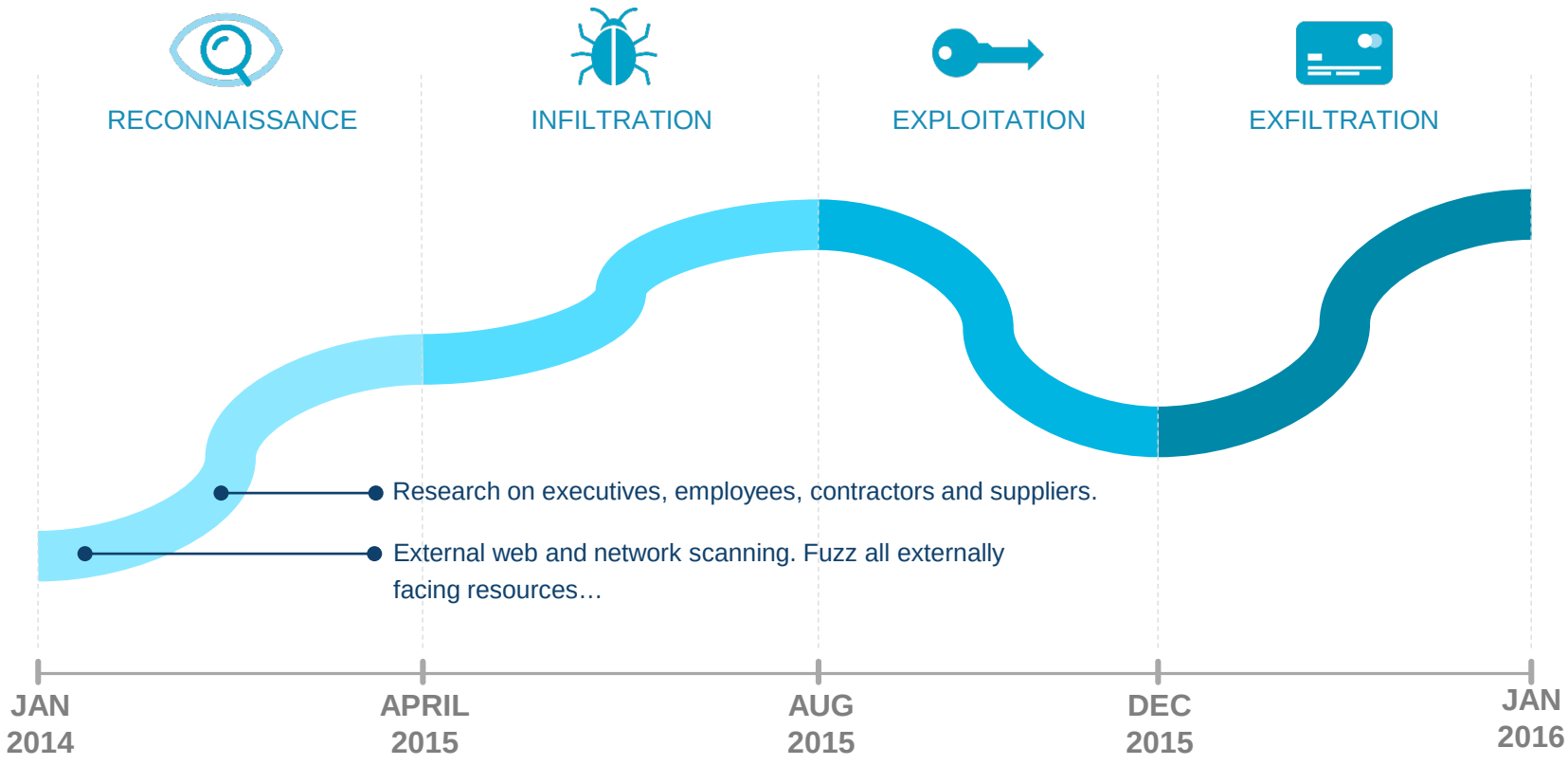
The Anatomy of a Data Breach

Reconnaissance



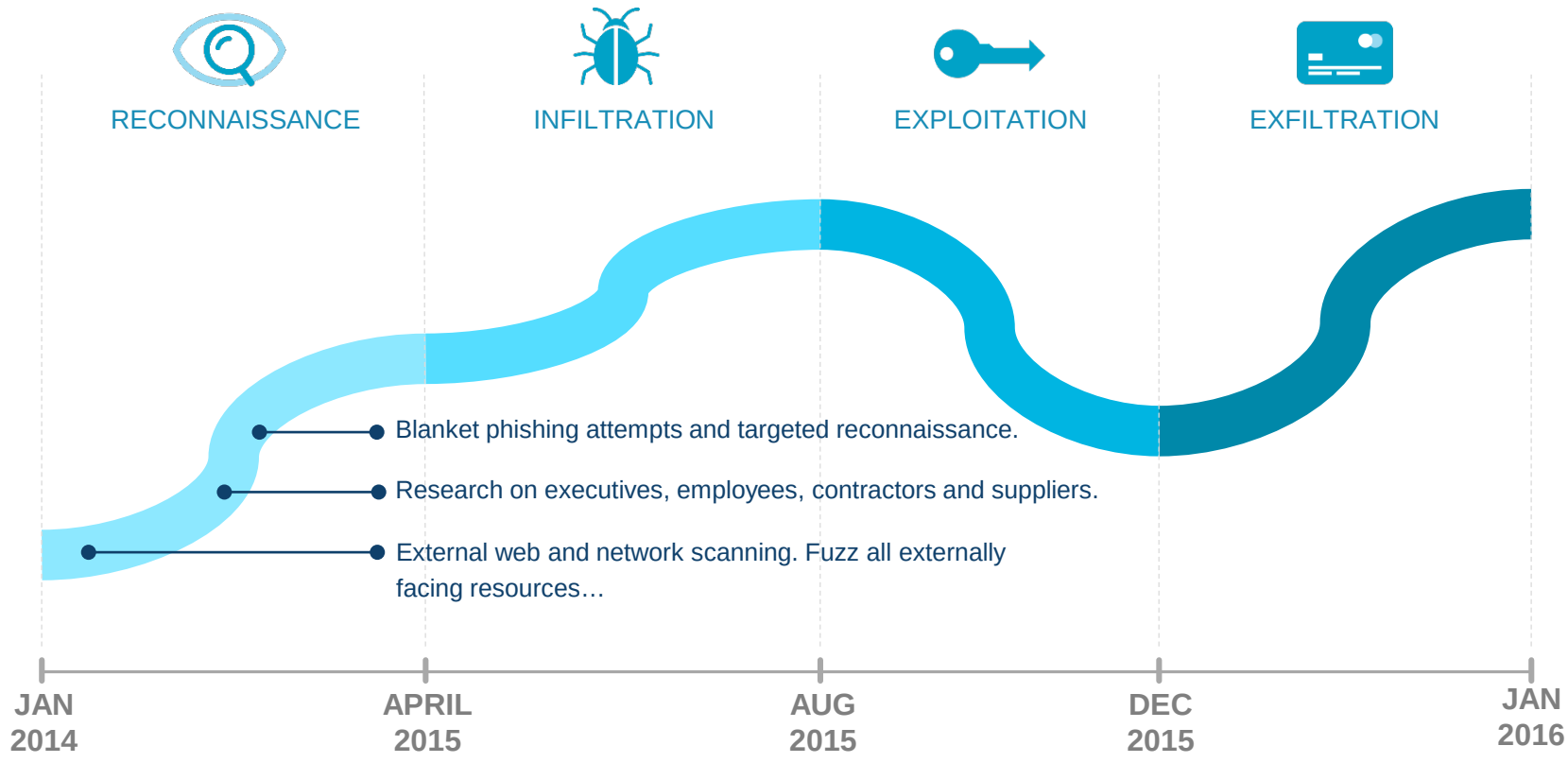
The Anatomy of a Data Breach

Reconnaissance



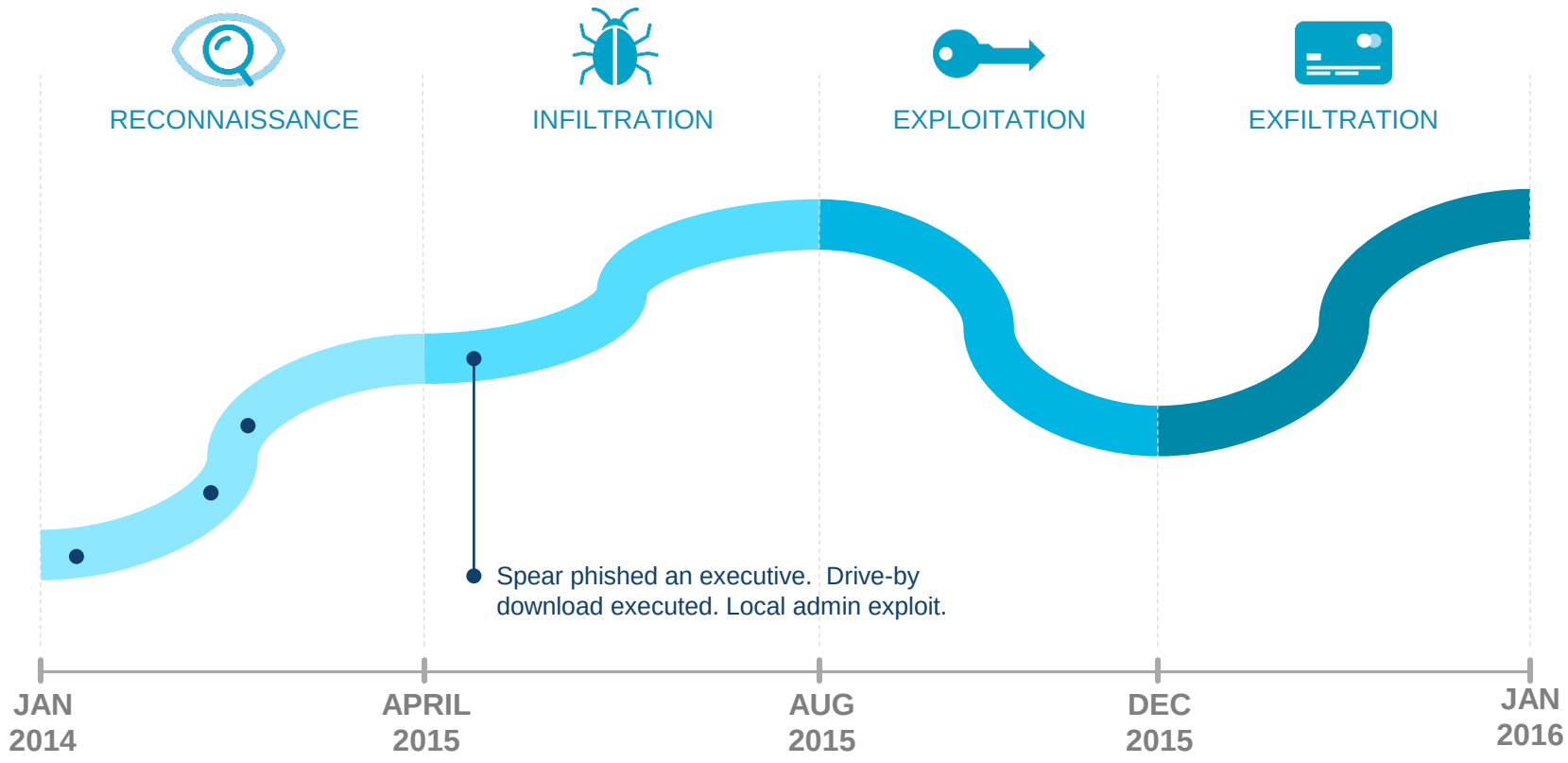
The Anatomy of a Data Breach

Reconnaissance



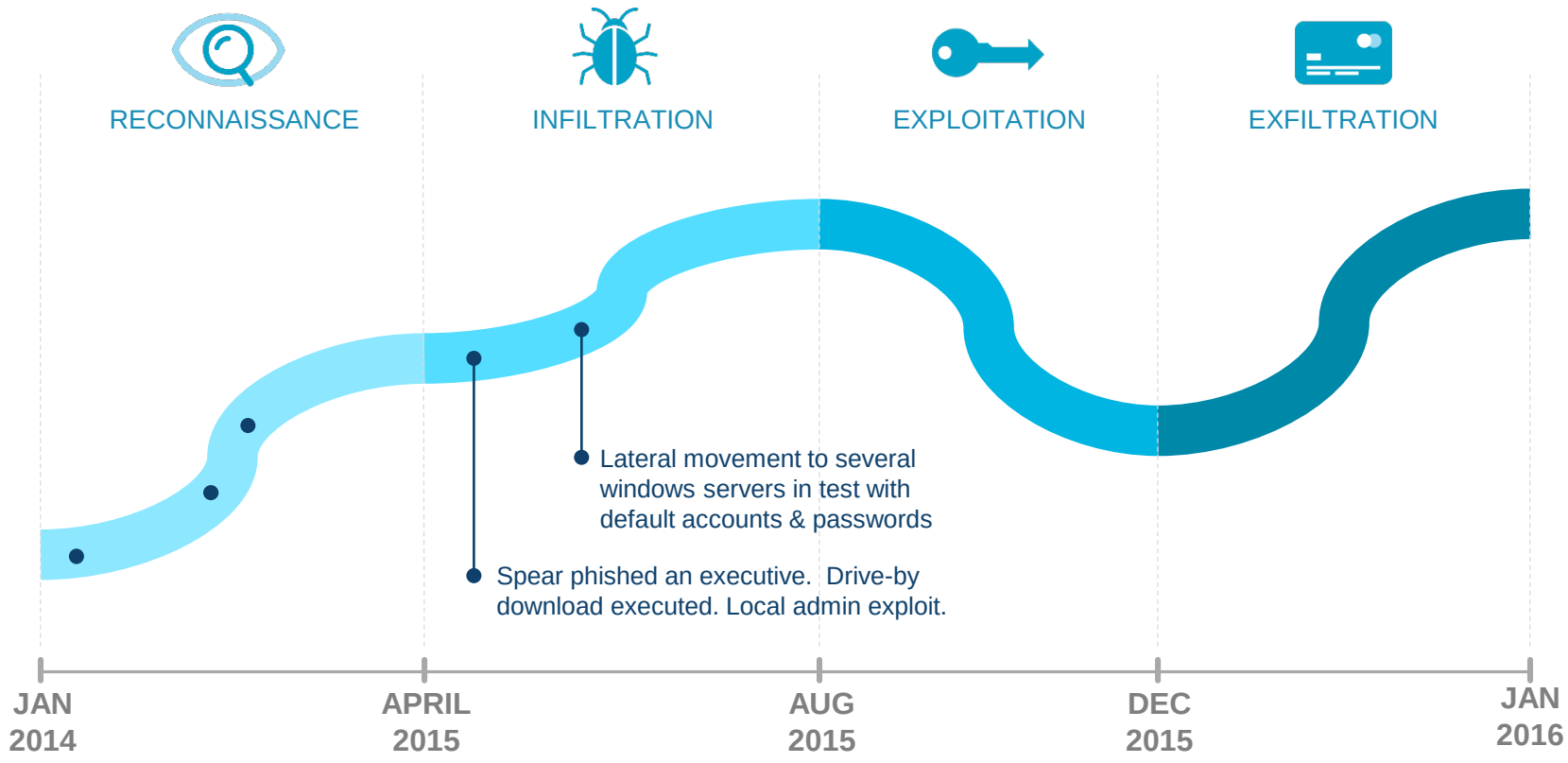
The Anatomy of a Data Breach

Infiltration



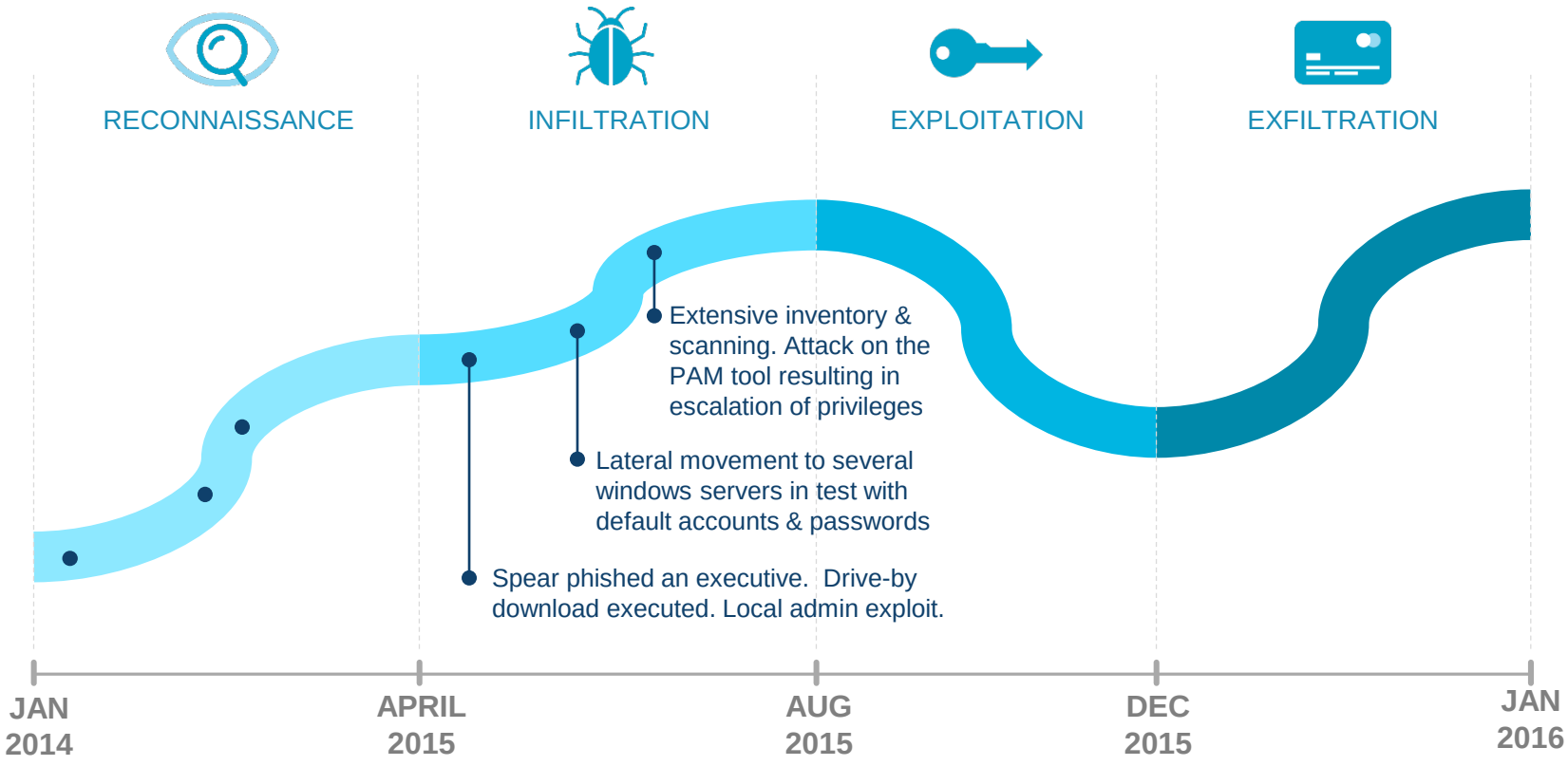
The Anatomy of a Data Breach

Infiltration



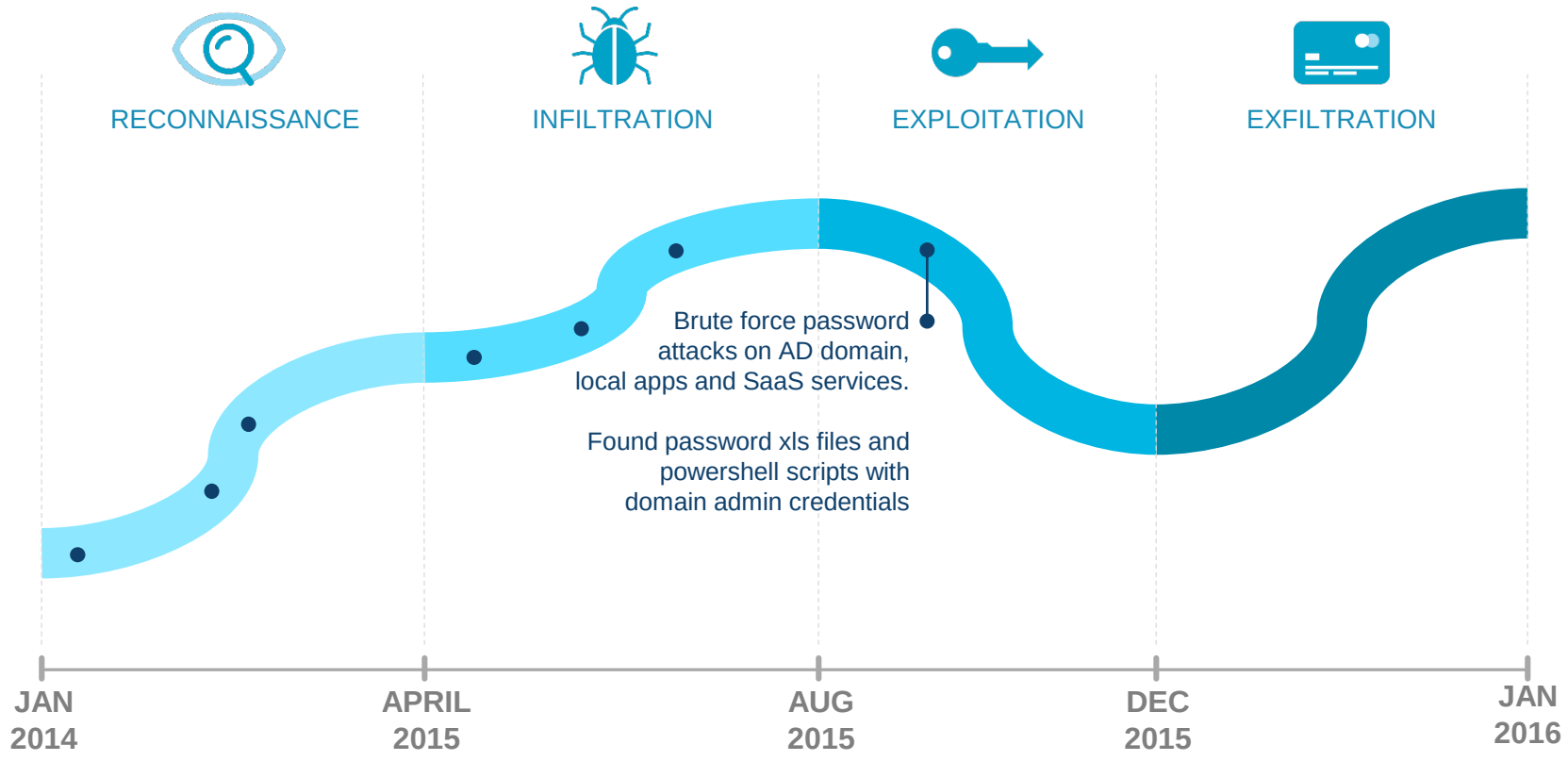
The Anatomy of a Data Breach

Infiltration



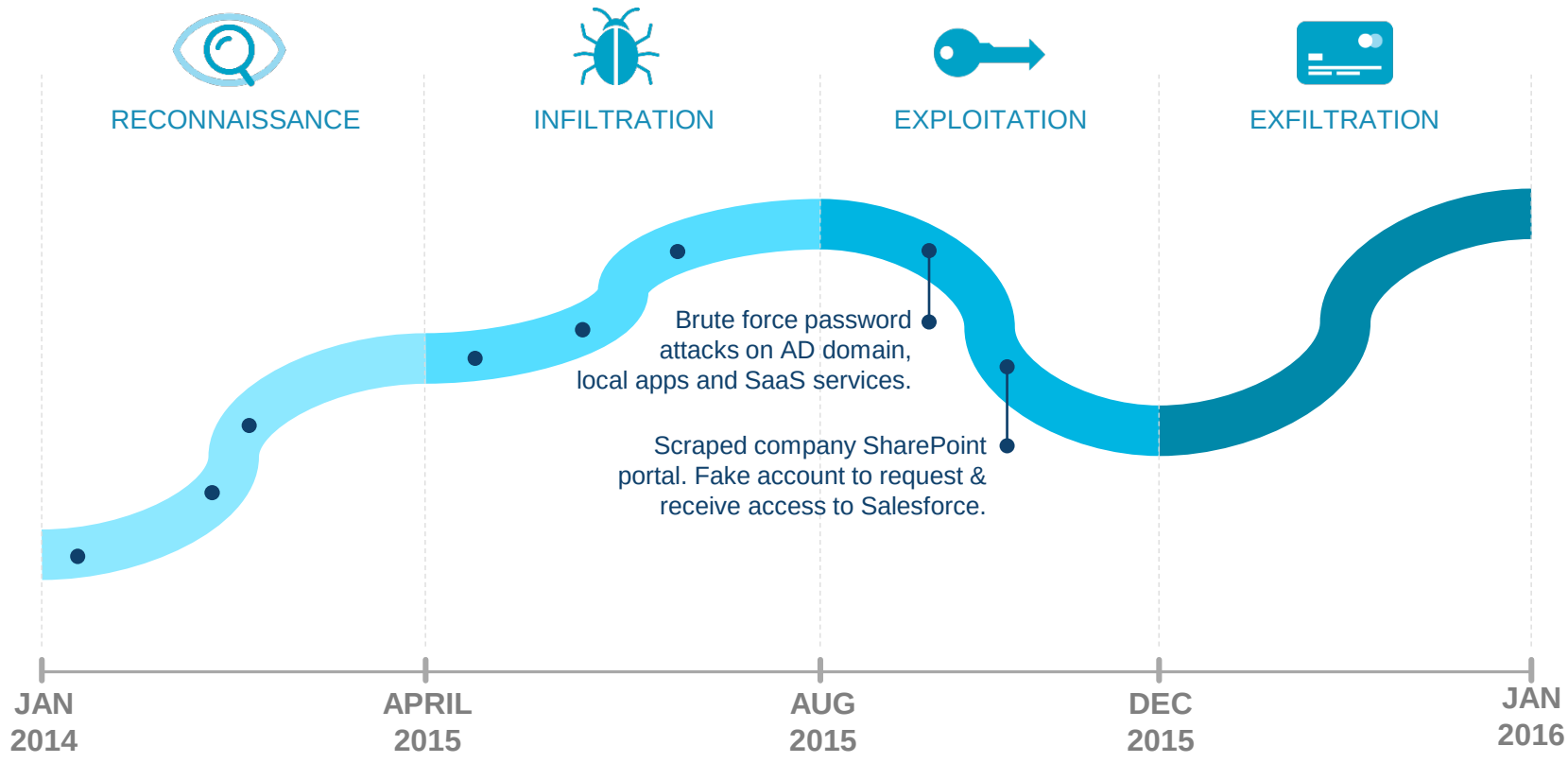
The Anatomy of a Data Breach

Exploitation



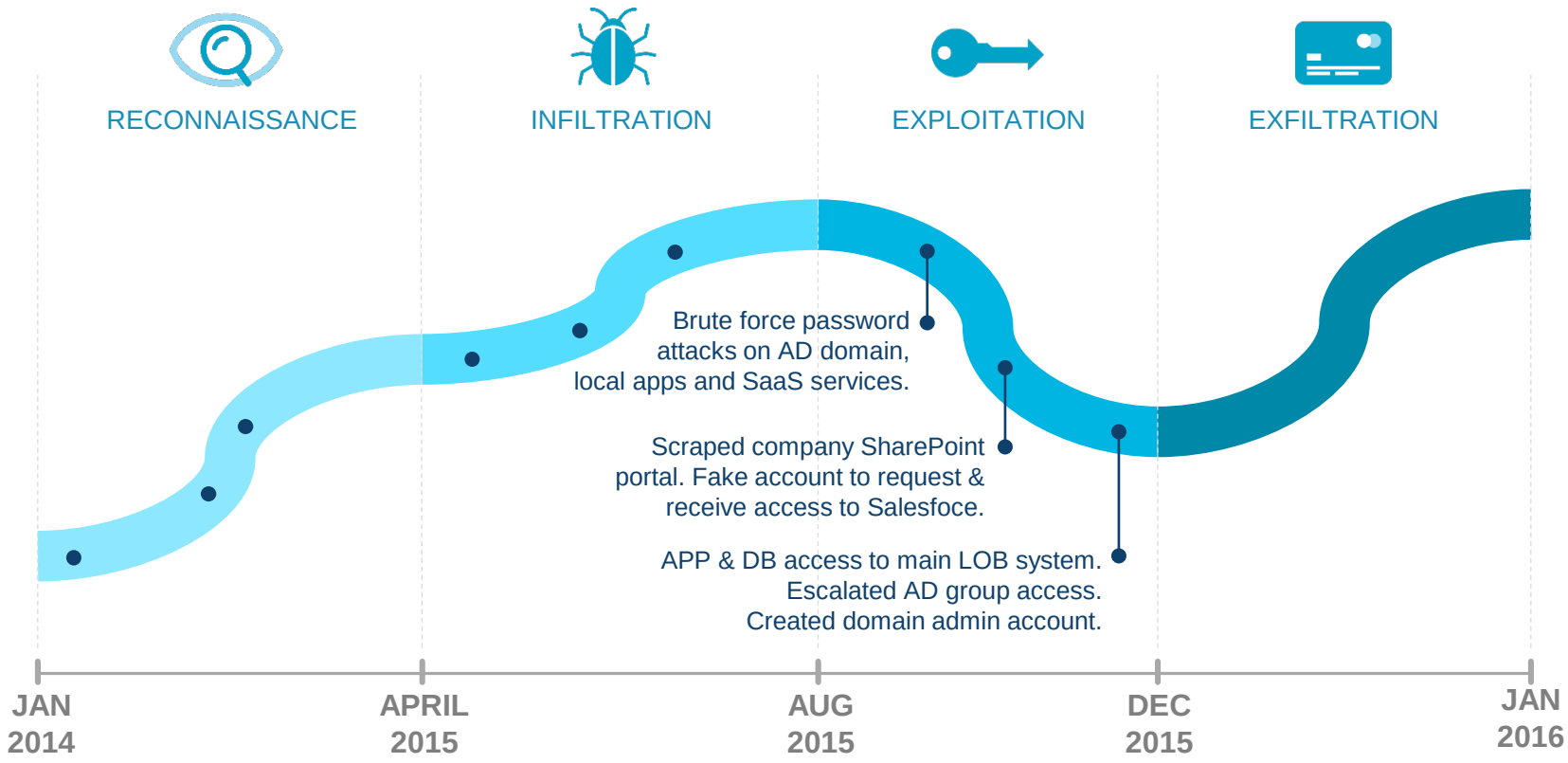
The Anatomy of a Data Breach

Exploitation



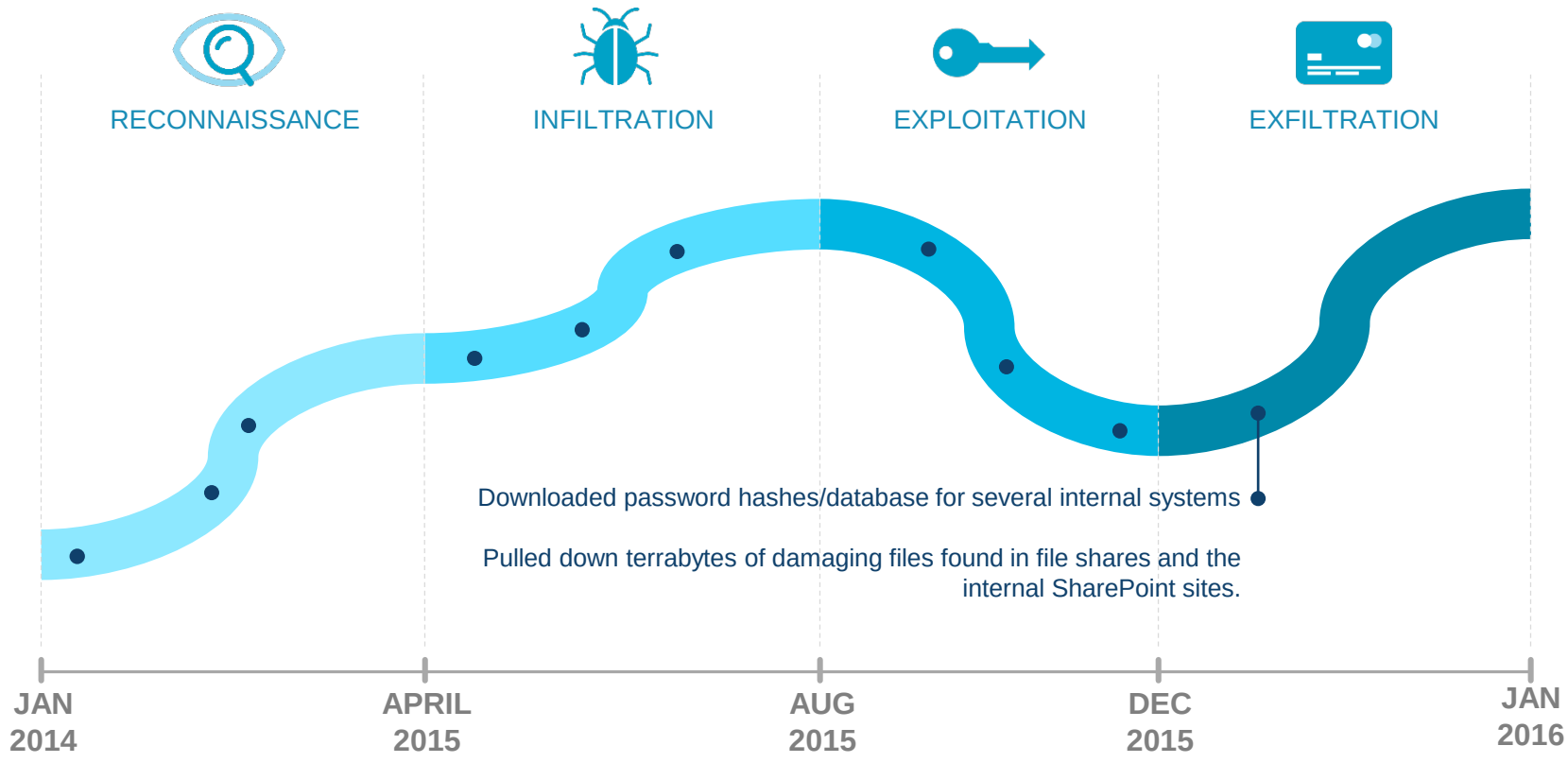
The Anatomy of a Data Breach

Exploitation



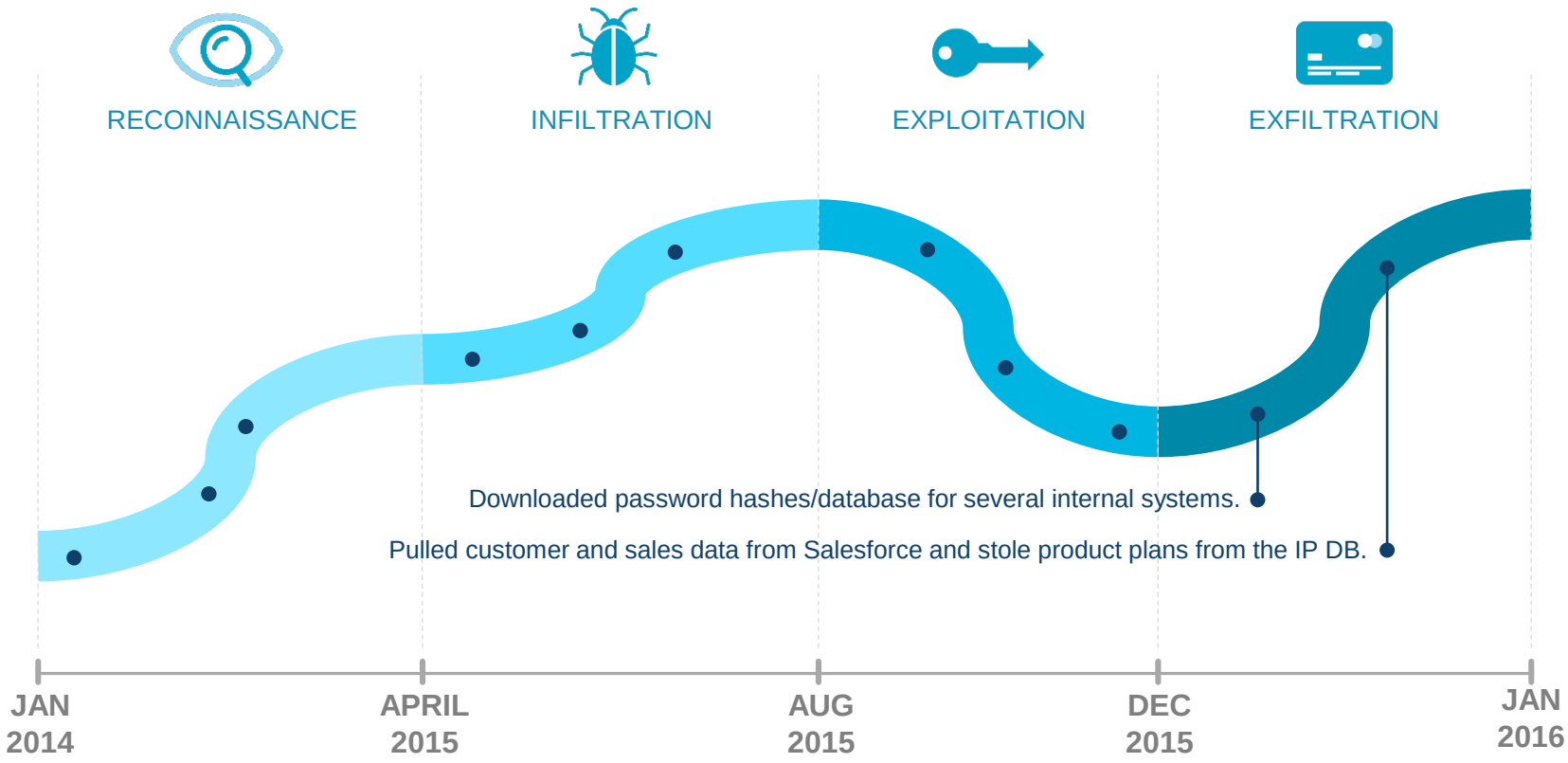
The Anatomy of a Data Breach

Exfiltration



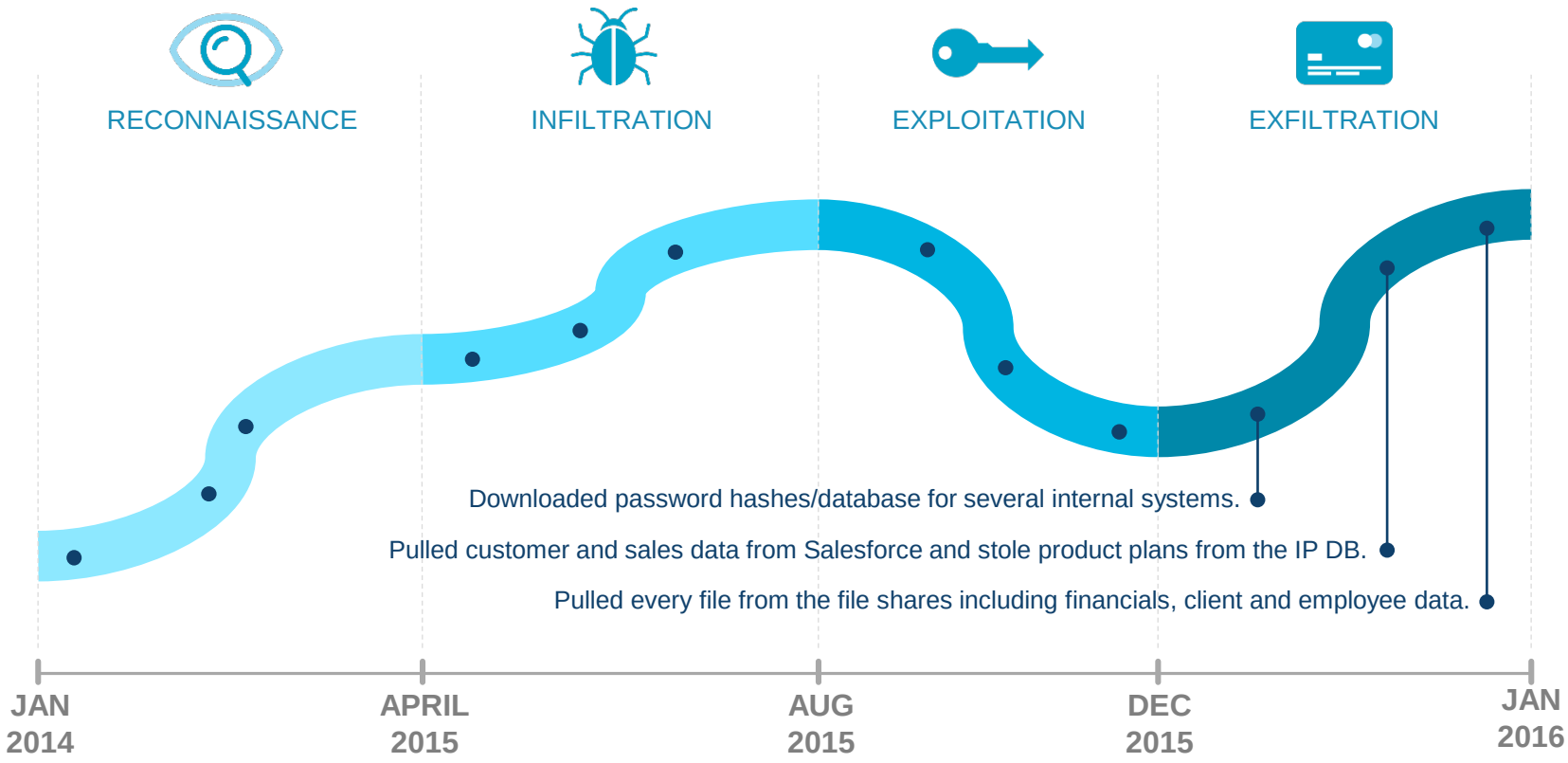
The Anatomy of a Data Breach

Exfiltration



The Anatomy of a Data Breach

Exfiltration



The Anatomy of a Data Breach

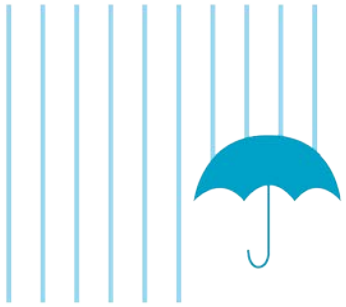
Damage Assessment

- **COMPANY FINANCIALS EXPOSED**
- **EMPLOYEE DATA SOLD ON THE DARK WEB**
- **COMPANY IN CHINA OPENS SELLING A DUPLICATE PRODUCT**
- **REPUTATIONAL DAMAGE**
- **LOSS OF PARTNERS AND CUSTOMERS**
- **EMPLOYEE DISSATISFACTION**
- **RESIGNATION OF THE CISO**

The Anatomy of a Data Breach

What went wrong?

WRONG



MISSED PROTECTIONS

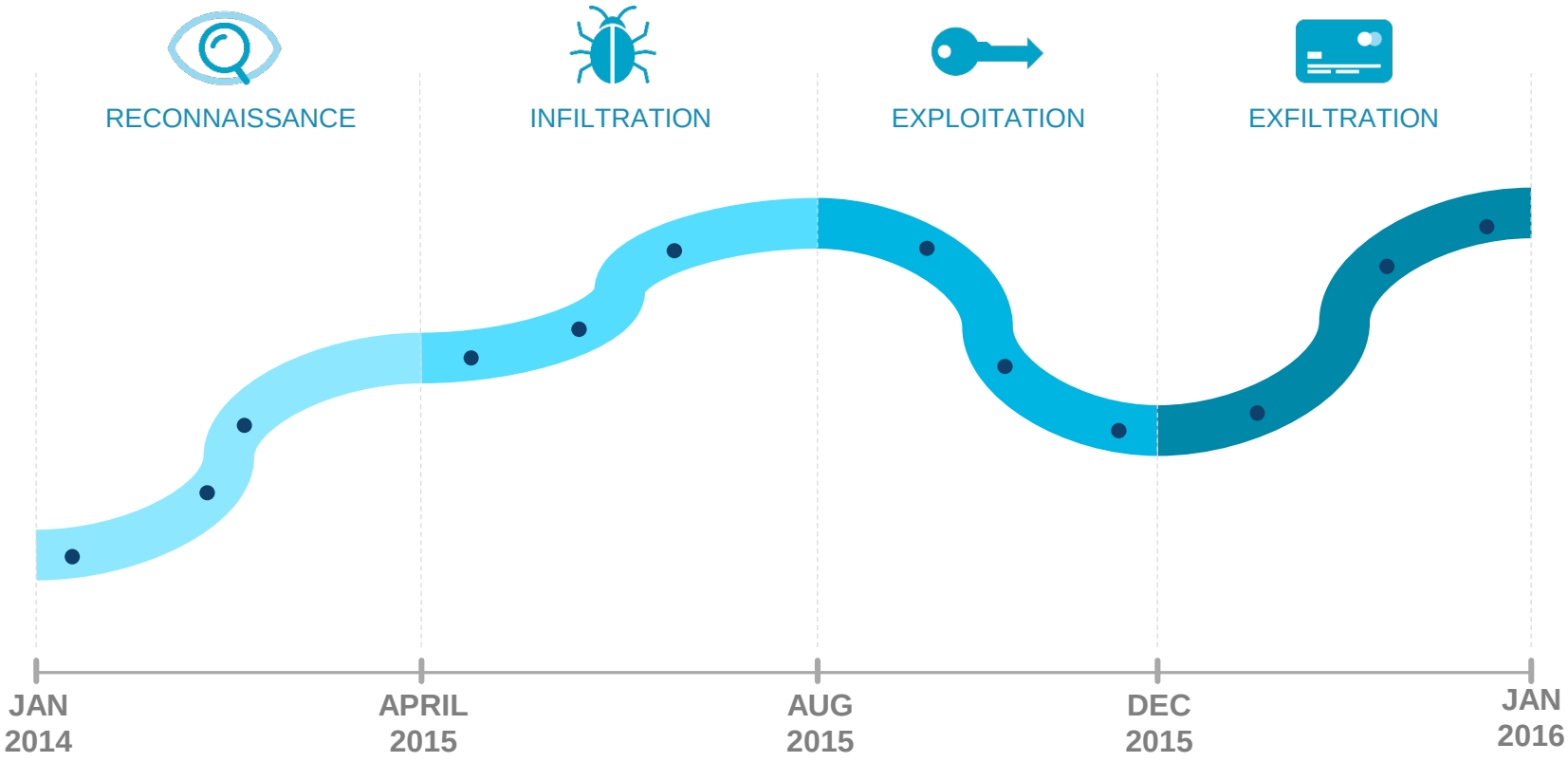
MISSED DETECTIONS

IAG Protection & Detection

IAG Protection & Detection

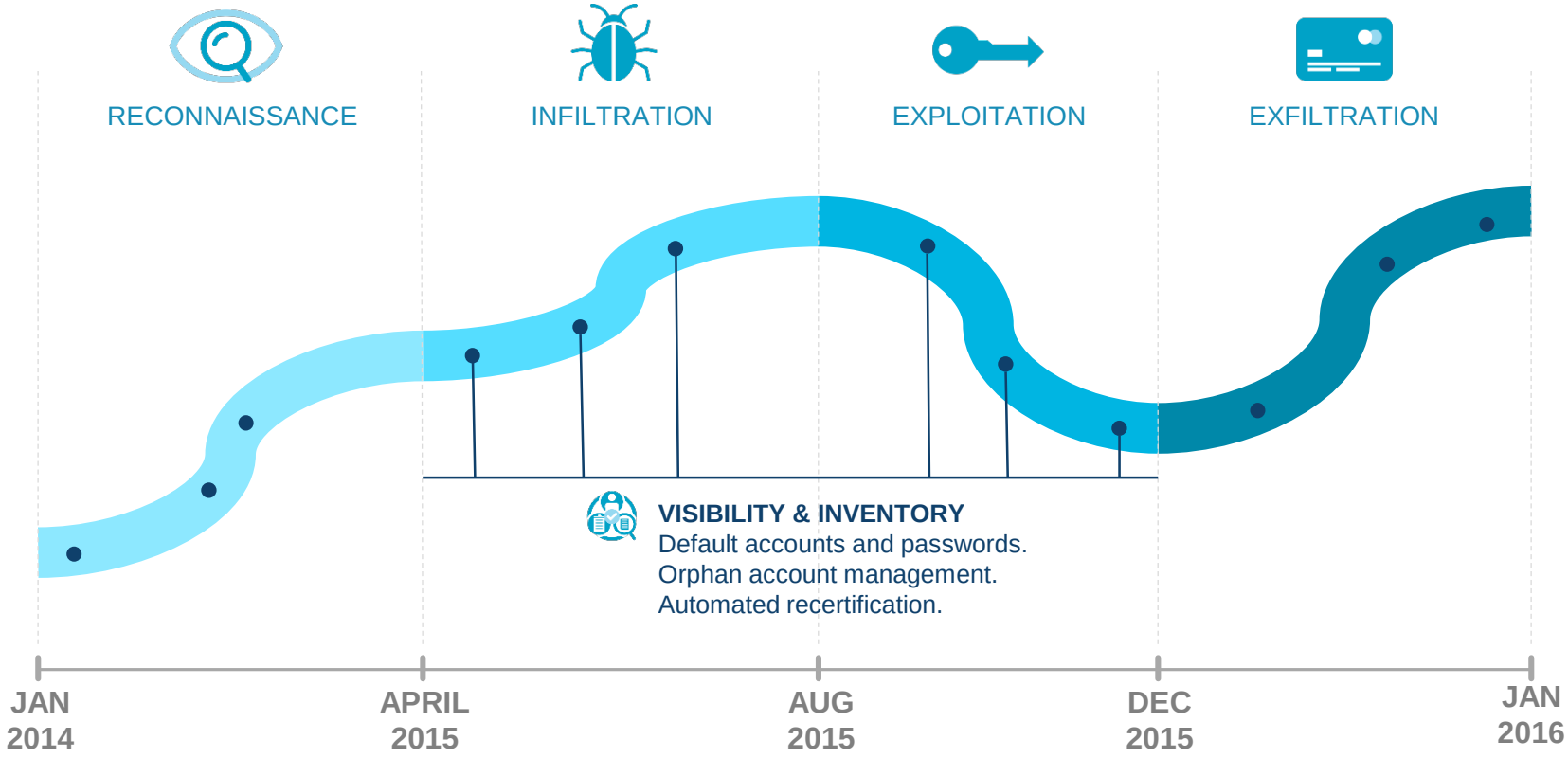
IAG Protection & Detection

The Anatomy of a Data Breach - Timeline



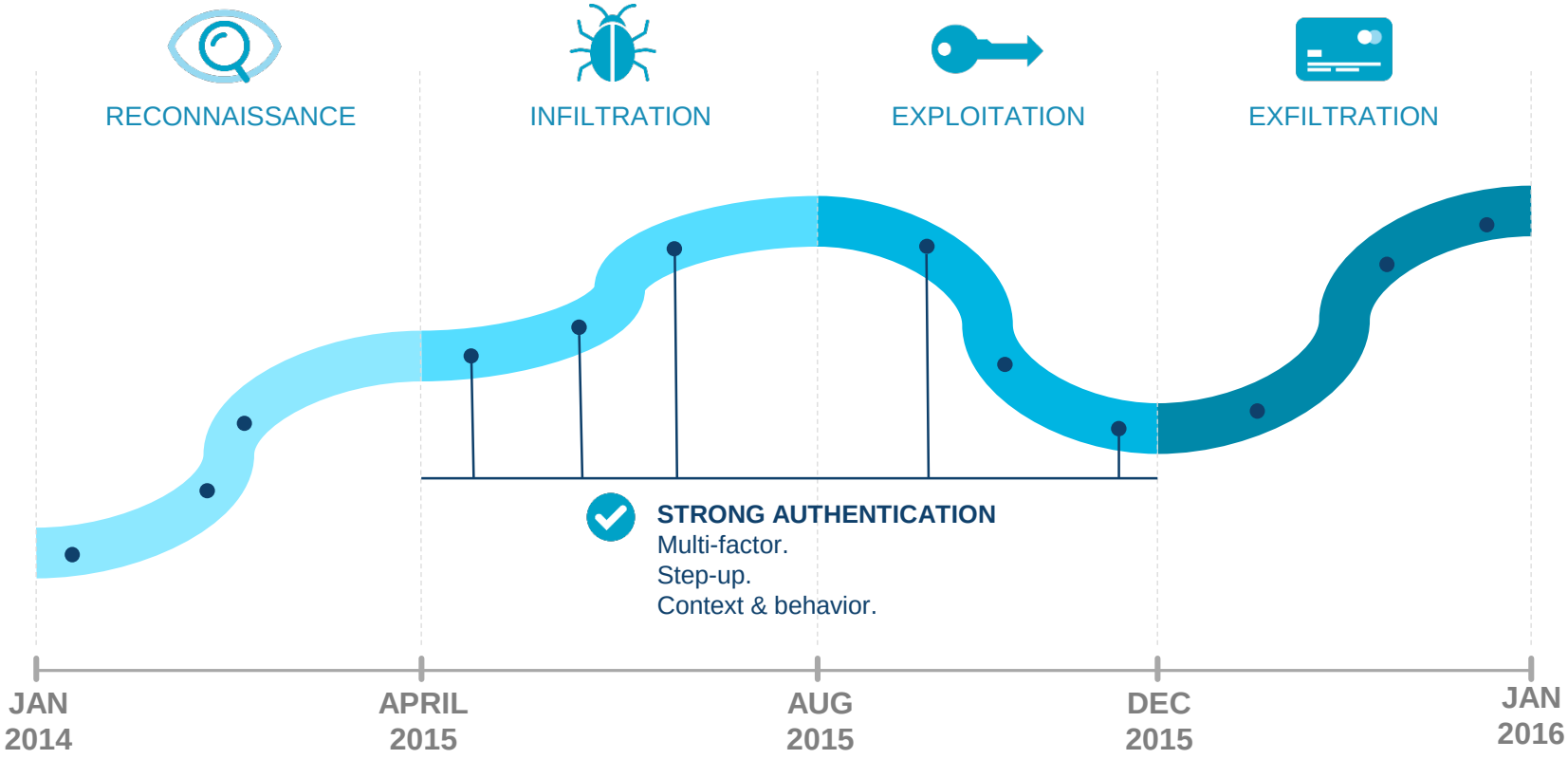
IAG Protection & Detection

Visibility & Inventory



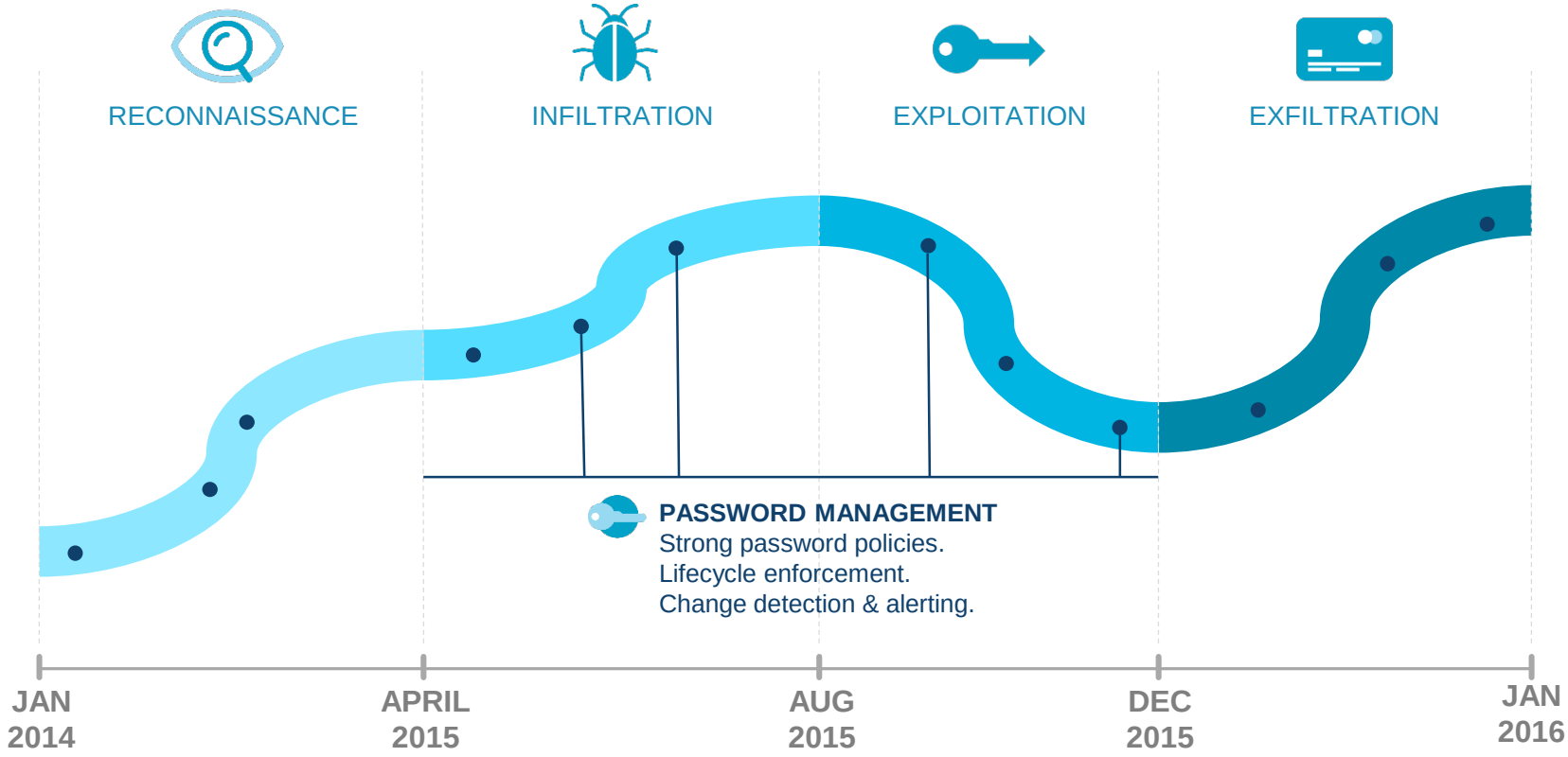
IAG Protection & Detection

Strong Authentication



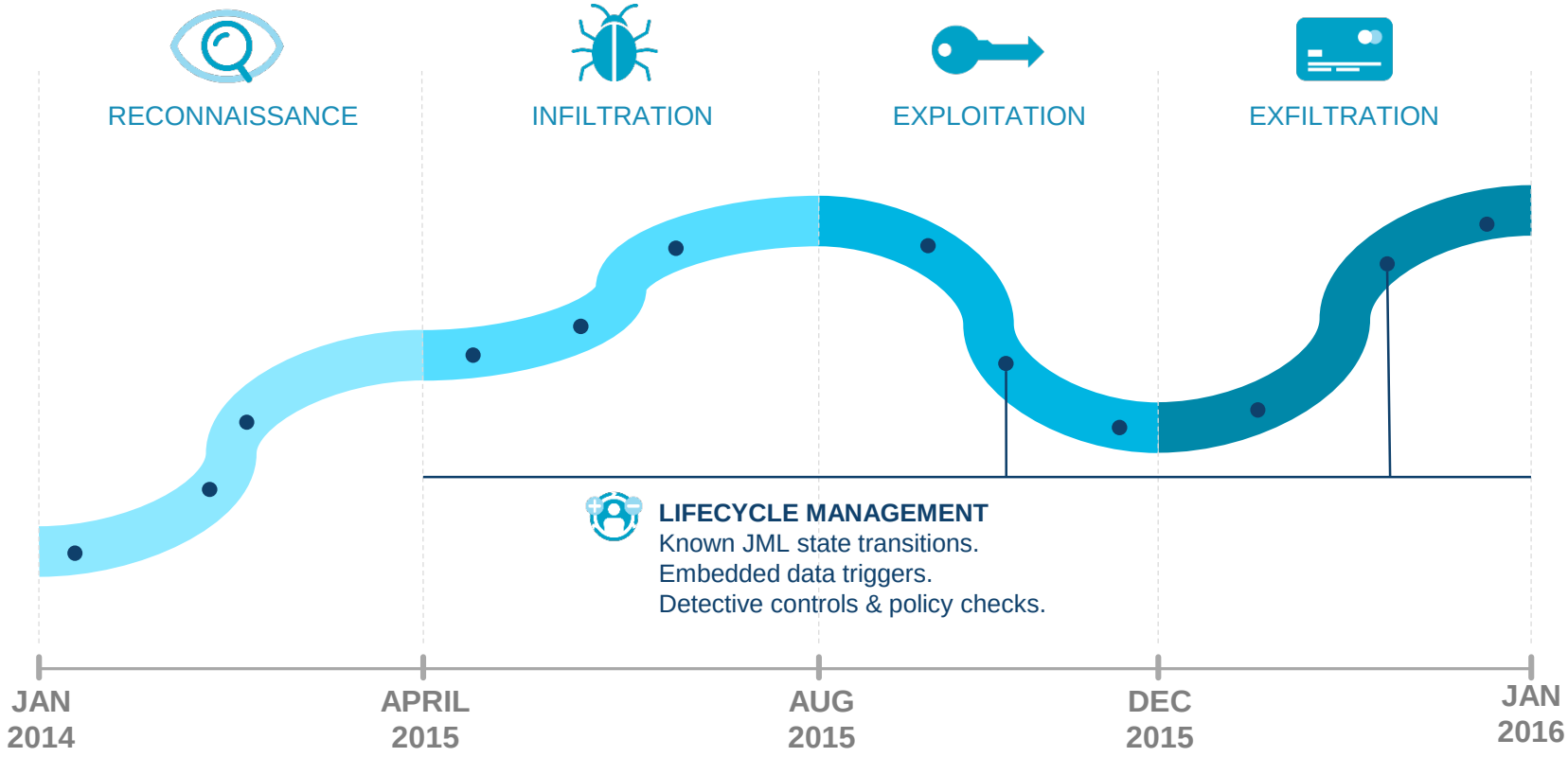
IAG Protection & Detection

Password Management



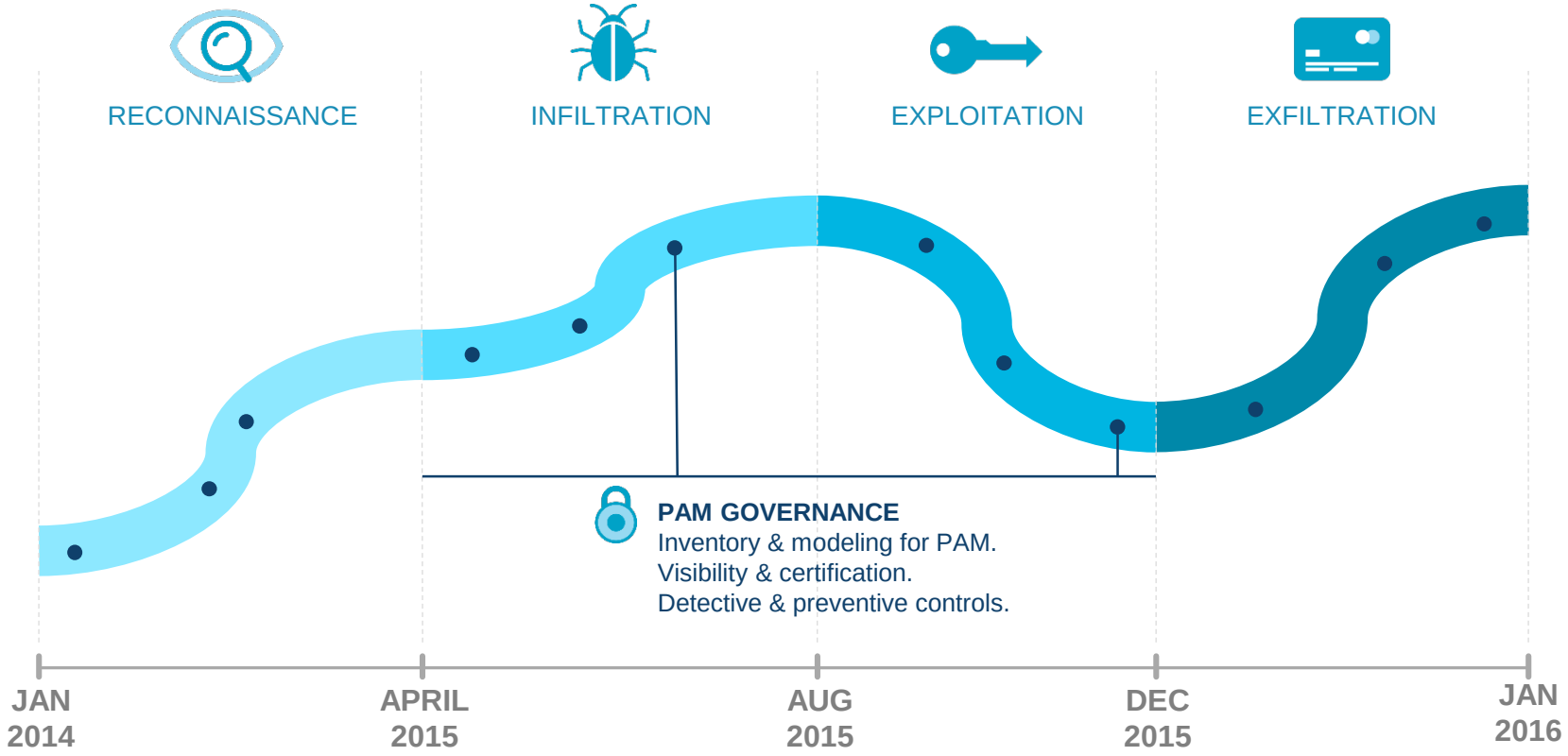
IAG Protection & Detection

Lifecycle Management



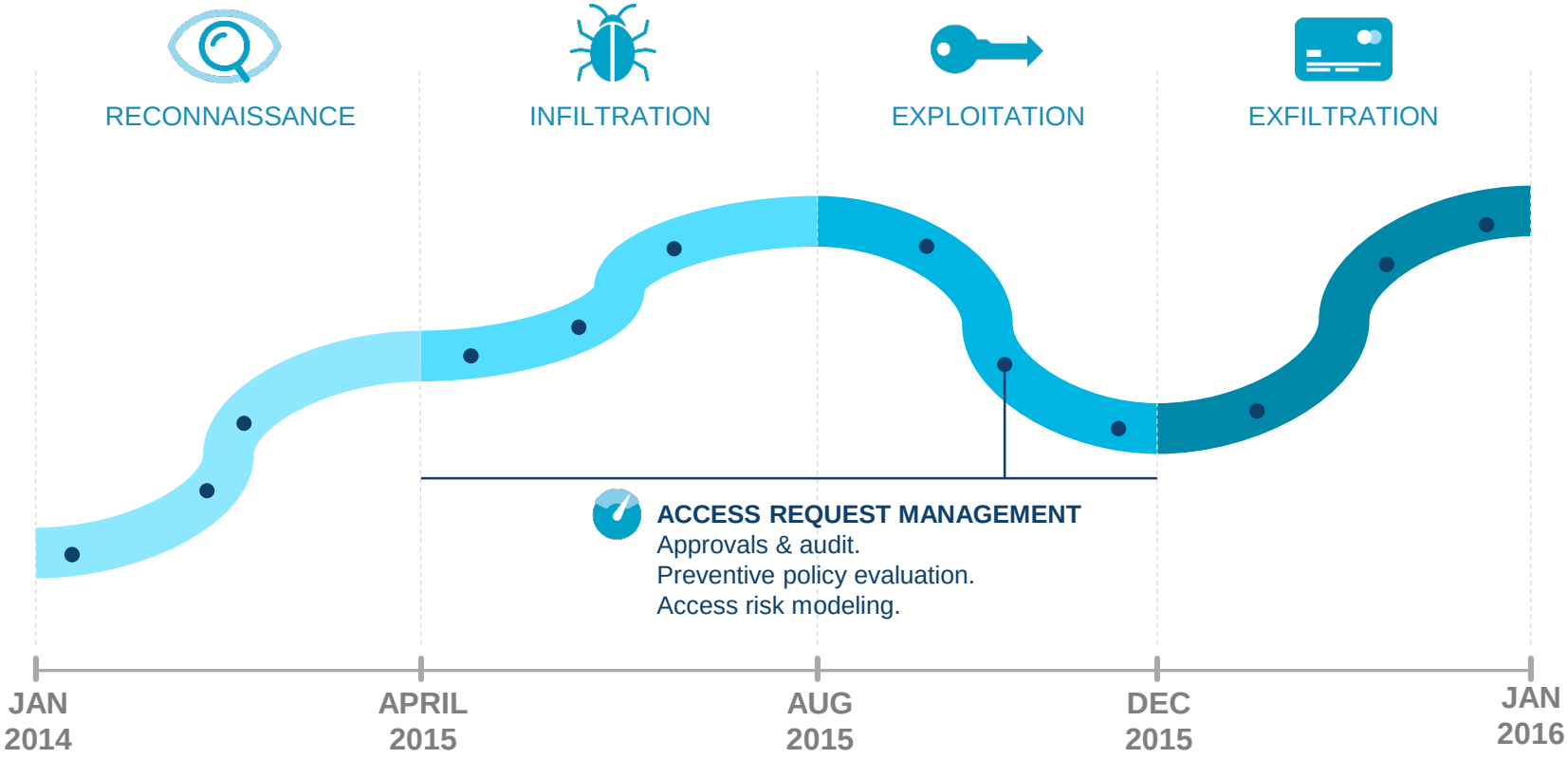
IAG Protection & Detection

PAM Governance



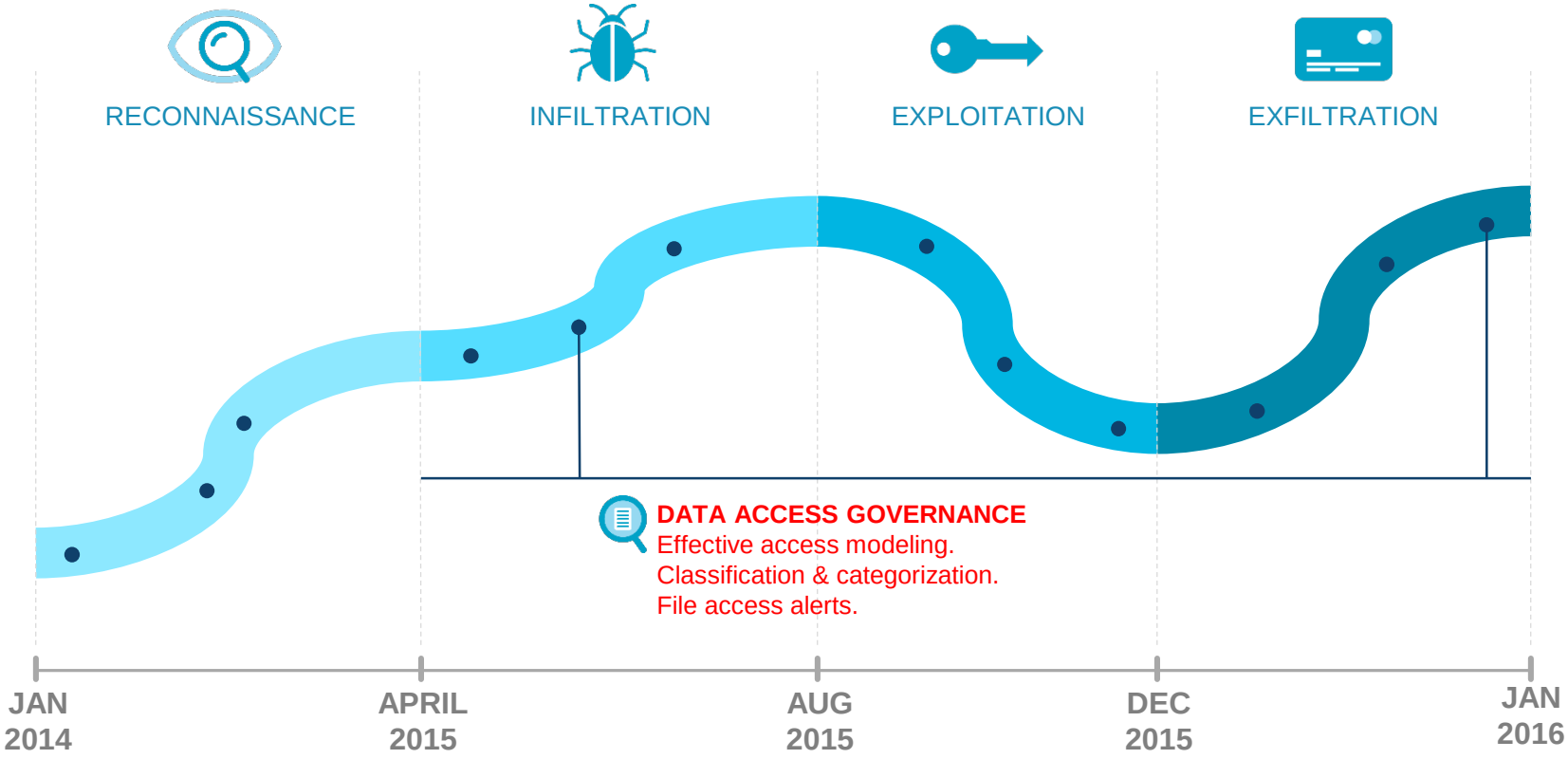
IAG Protection & Detection

Access Request Management



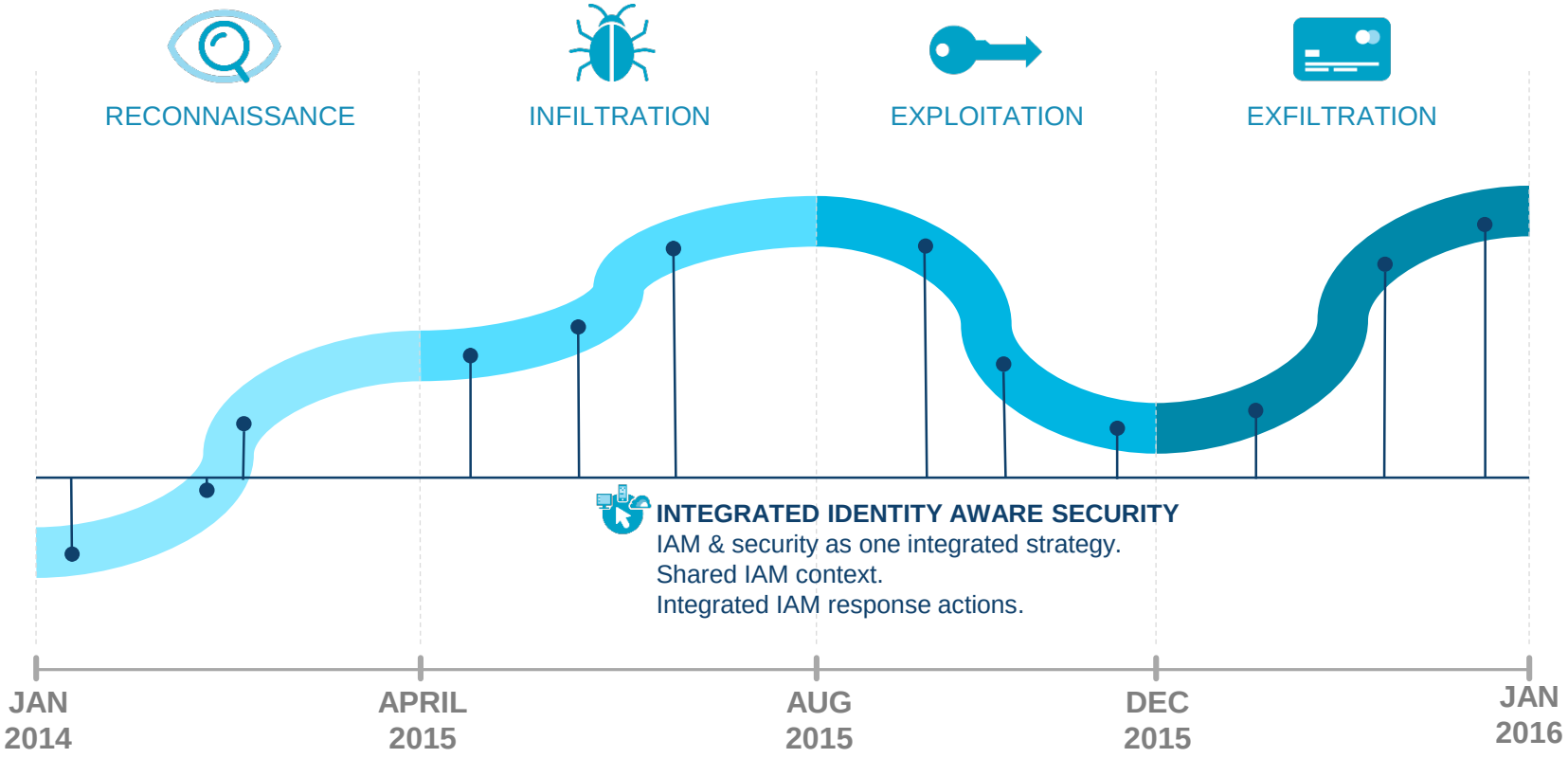
IAG Protection & Detection

Data Access Governance



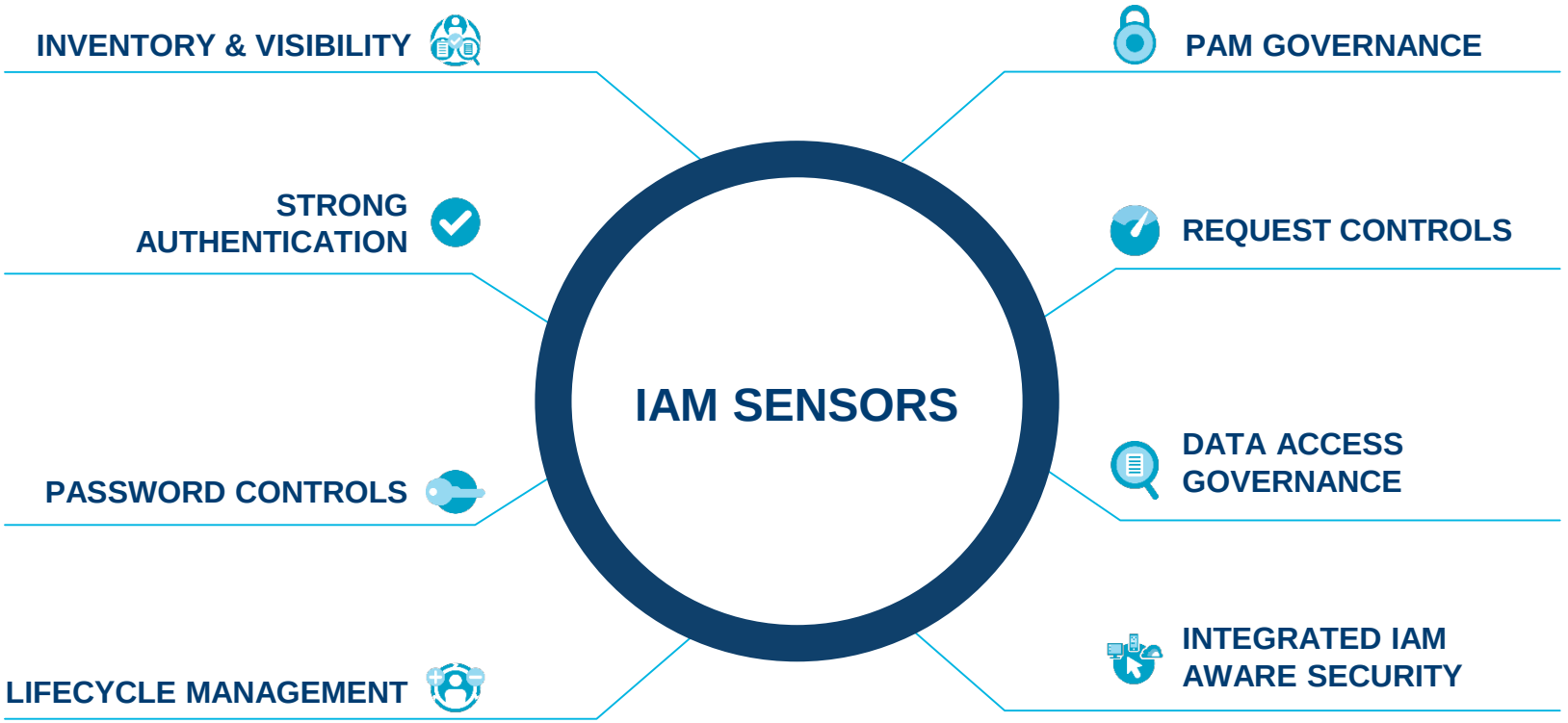
IAG Protection & Detection

Integrated Identity Aware Security



IAG Protection & Detection

IAG Protection & Detection



IAG Sensors

IAG Sensors

Detecting Attacks

ACCOUNT “HONEY POTS”

- Fake accounts with login alerts
- Deliberately weak passwords
- Automatically created and managed
- Spread out over apps and infrastructure

FILE & FOLDER “TRIP WIRES”

- Fake files and folders
- Appealing names and content
- Pre-set file access alerts
- Spread out over cloud and on-premises file shares

Q & A

Andreas Fuhrmann
SKyPRO AG
andreas.fuhrmann@skypro.ch

John Waters
SailPoint
john.waters@sailpoint.com