



The Anatomy of a Data Breach

Andreas Fuhrmann
SKyPRO AG
andreas.fuhrmann@skypro.ch

John Waters
SailPoint
john.waters@sailpoint.com

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

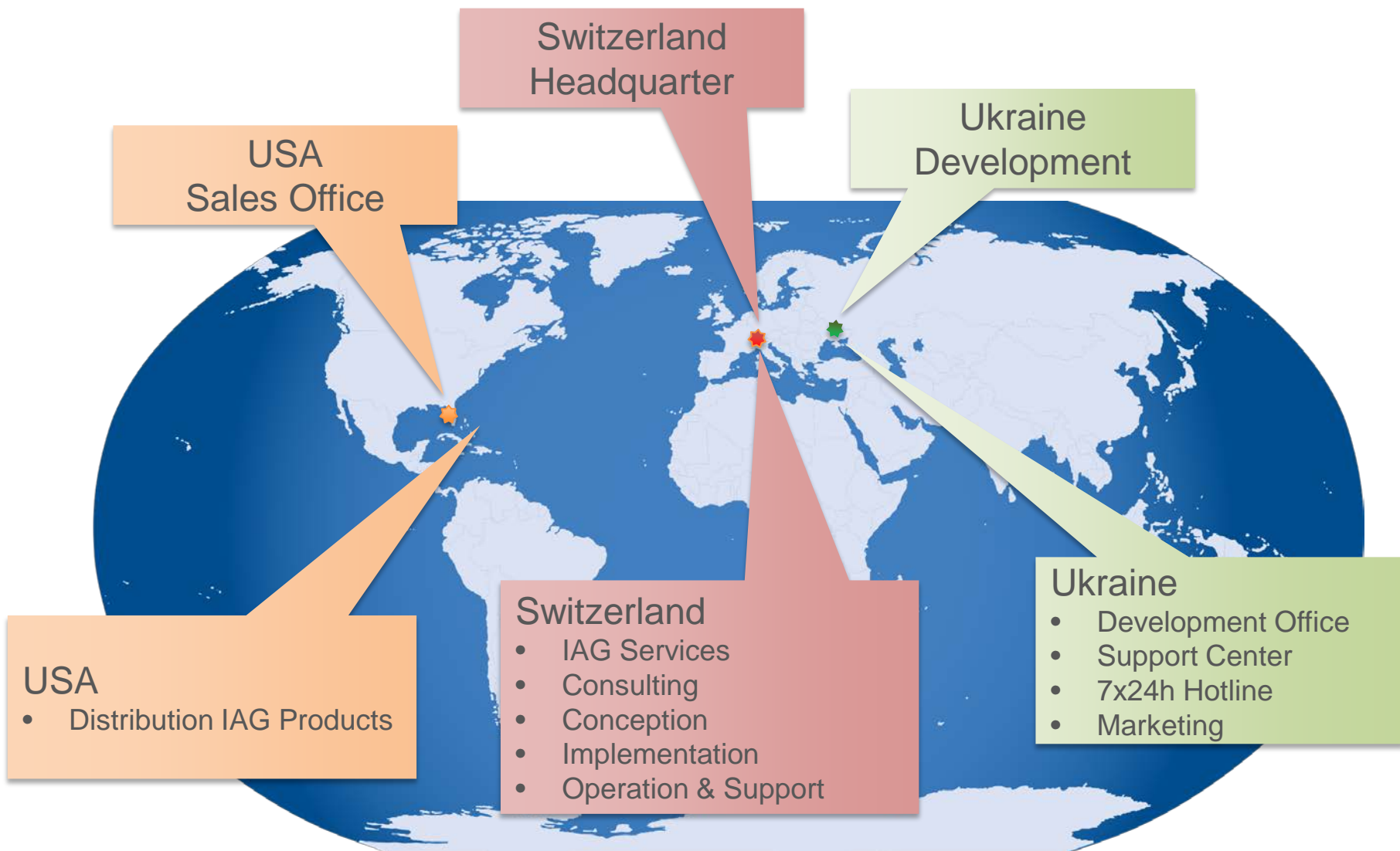


- we do

- Identity & Access Governance (IAG) solution in Bank, Insurance, Industry, Government, Schools and Service Companies
- Consulting, 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



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”

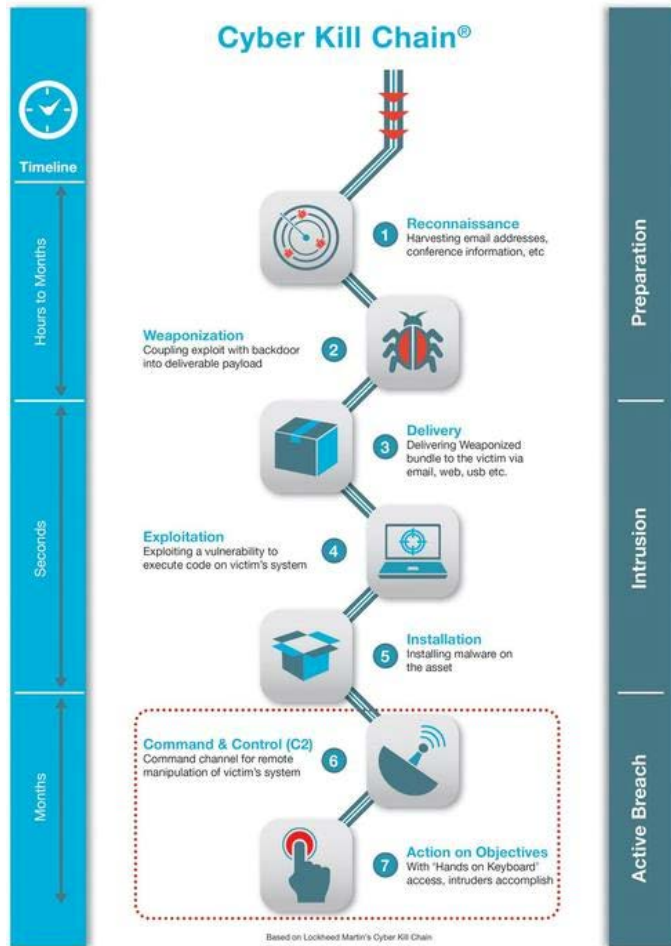
- Poor account controls
- Weak passwords
- Orphan accounts
- Weak inventory and cataloging
- **Over assignment of user access**
- **Unstructured Data Insanity**



The Cyber Link Kill Chain



The Cyber Kill Chain



INTRODUCED BY LOCKHEED MARTIN '99

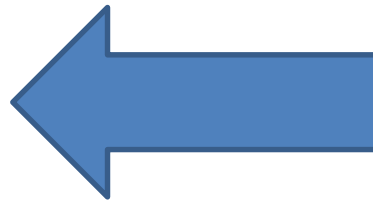
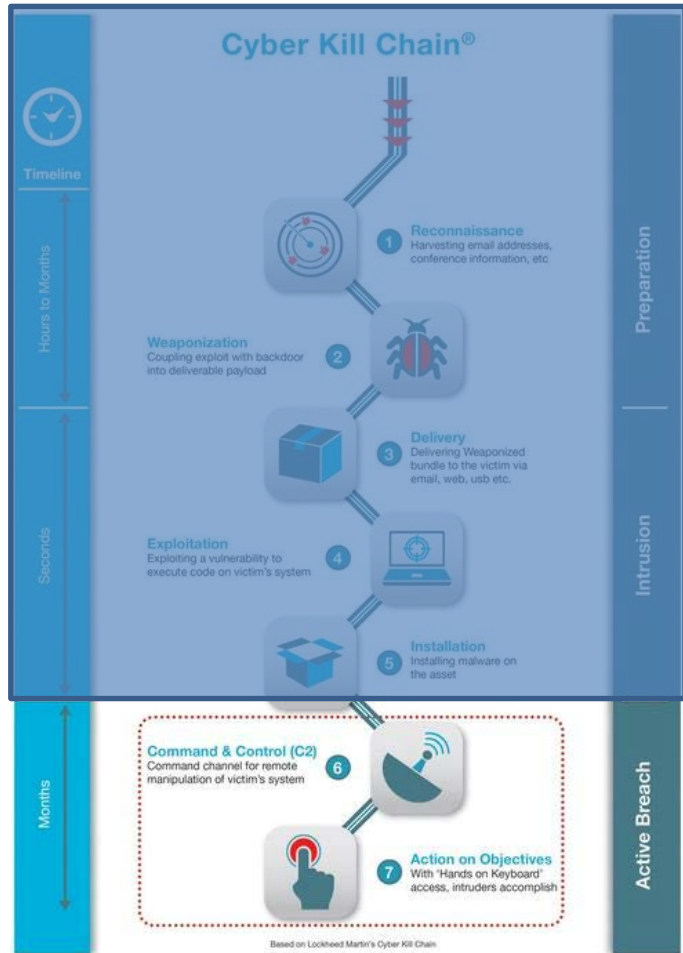
- Anatomy of a typical cyber breach
- Plots the path of an attack
- Reference model for cyber defense

PHASES OF ATTACK

- Reconnaissance
- Weaponization
- Delivery
- Infiltration



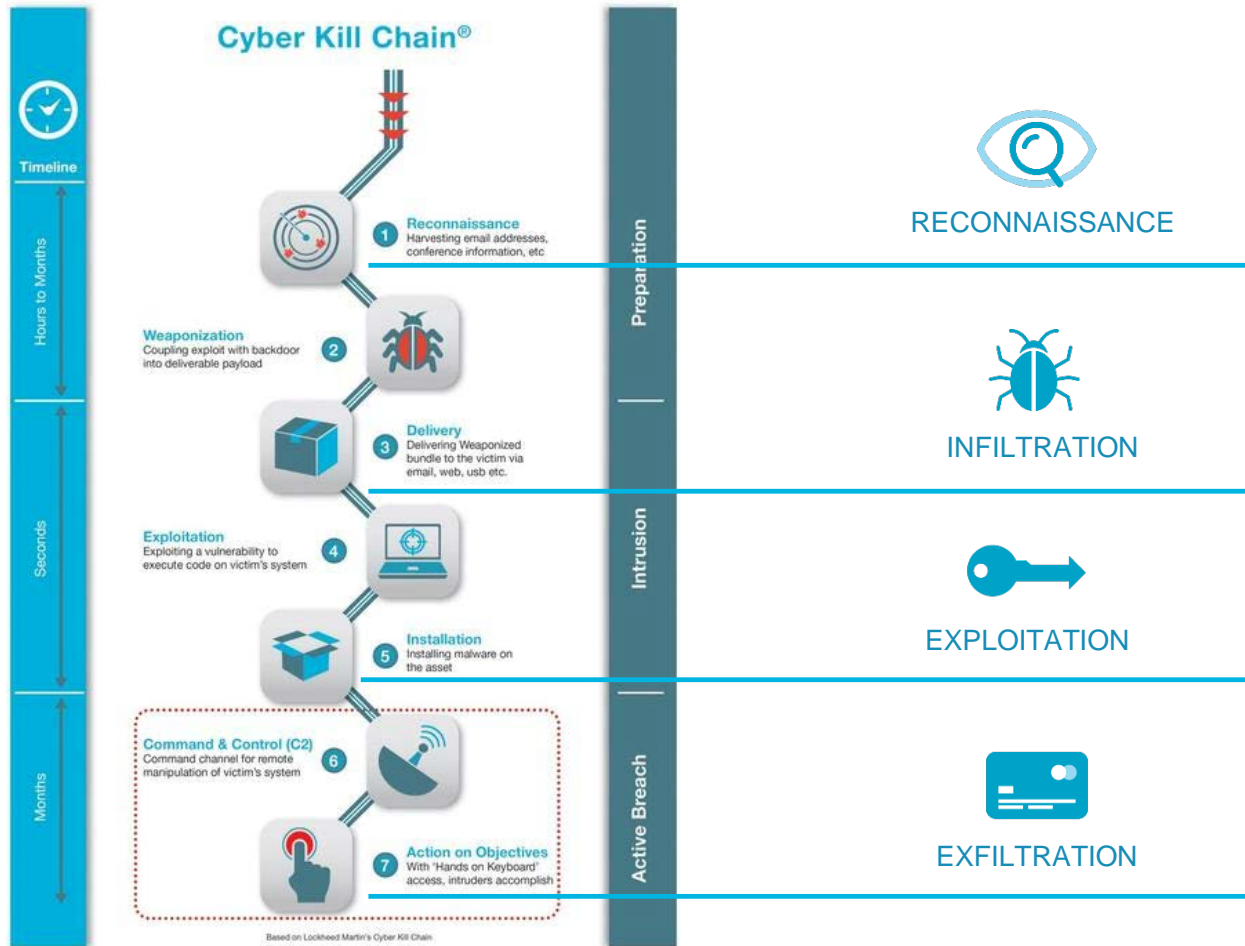
The Cyber Kill Chain



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



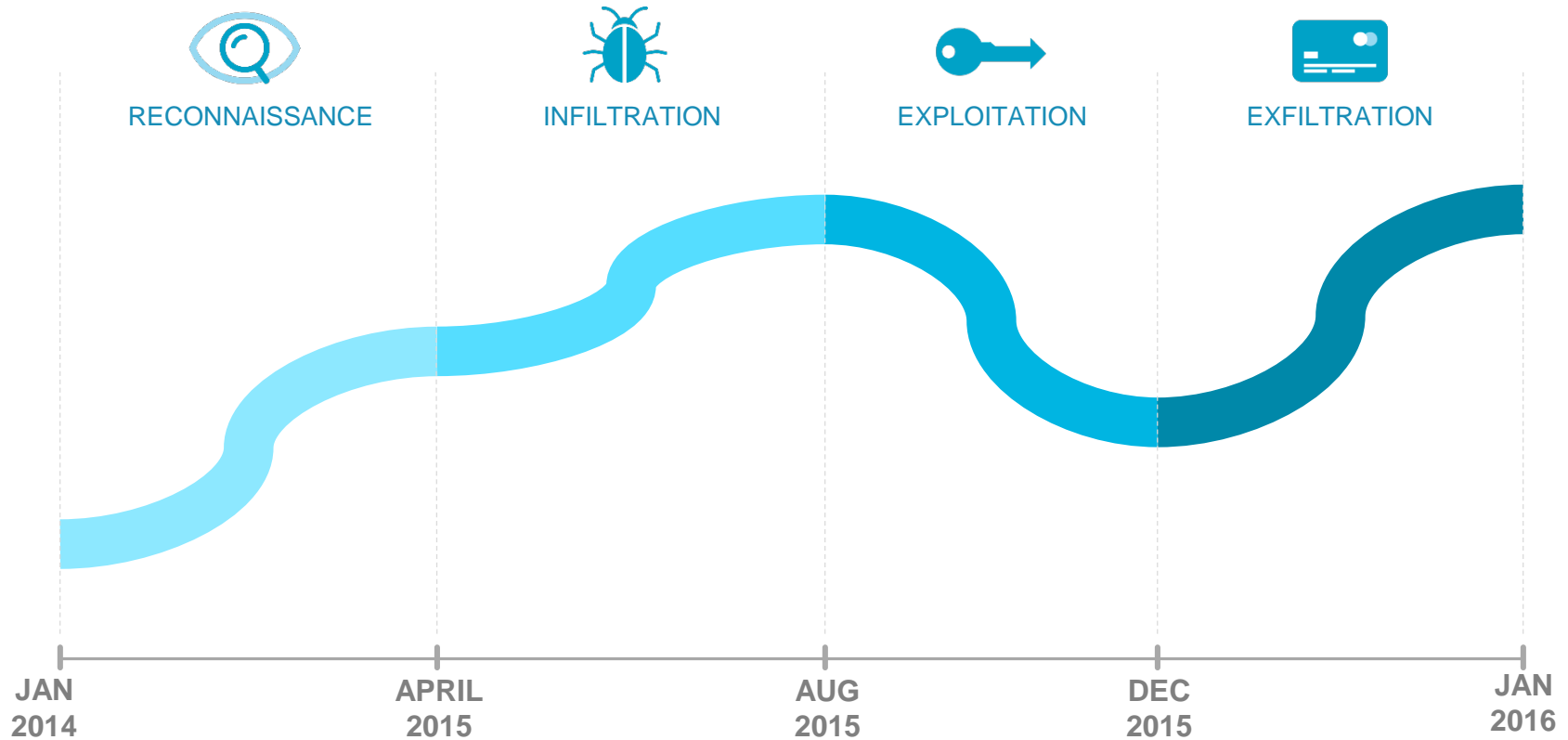
THE ATTACKER

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



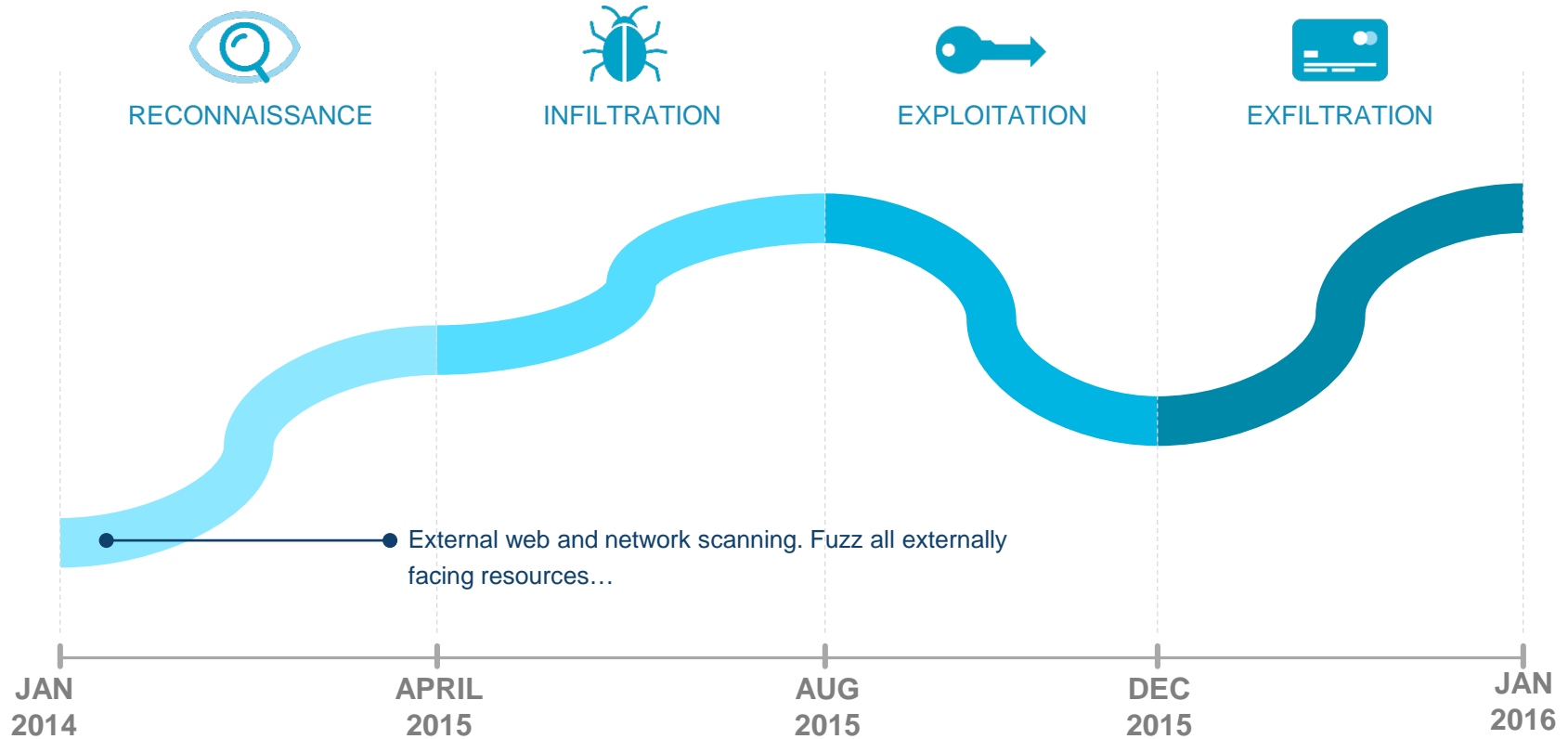
The Anatomy of a Data Breach

Timeline



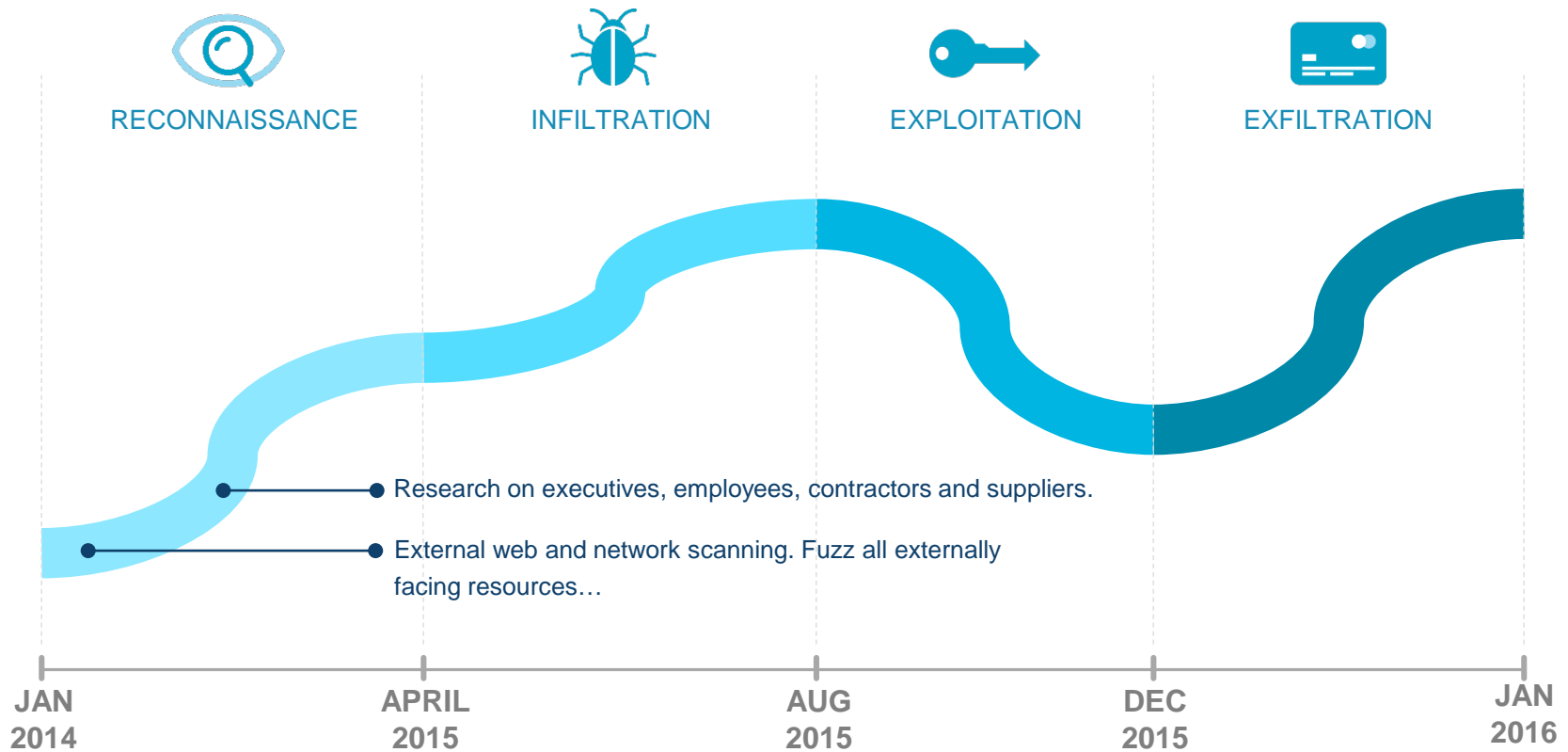
The Anatomy of a Data Breach

Reconnaissance



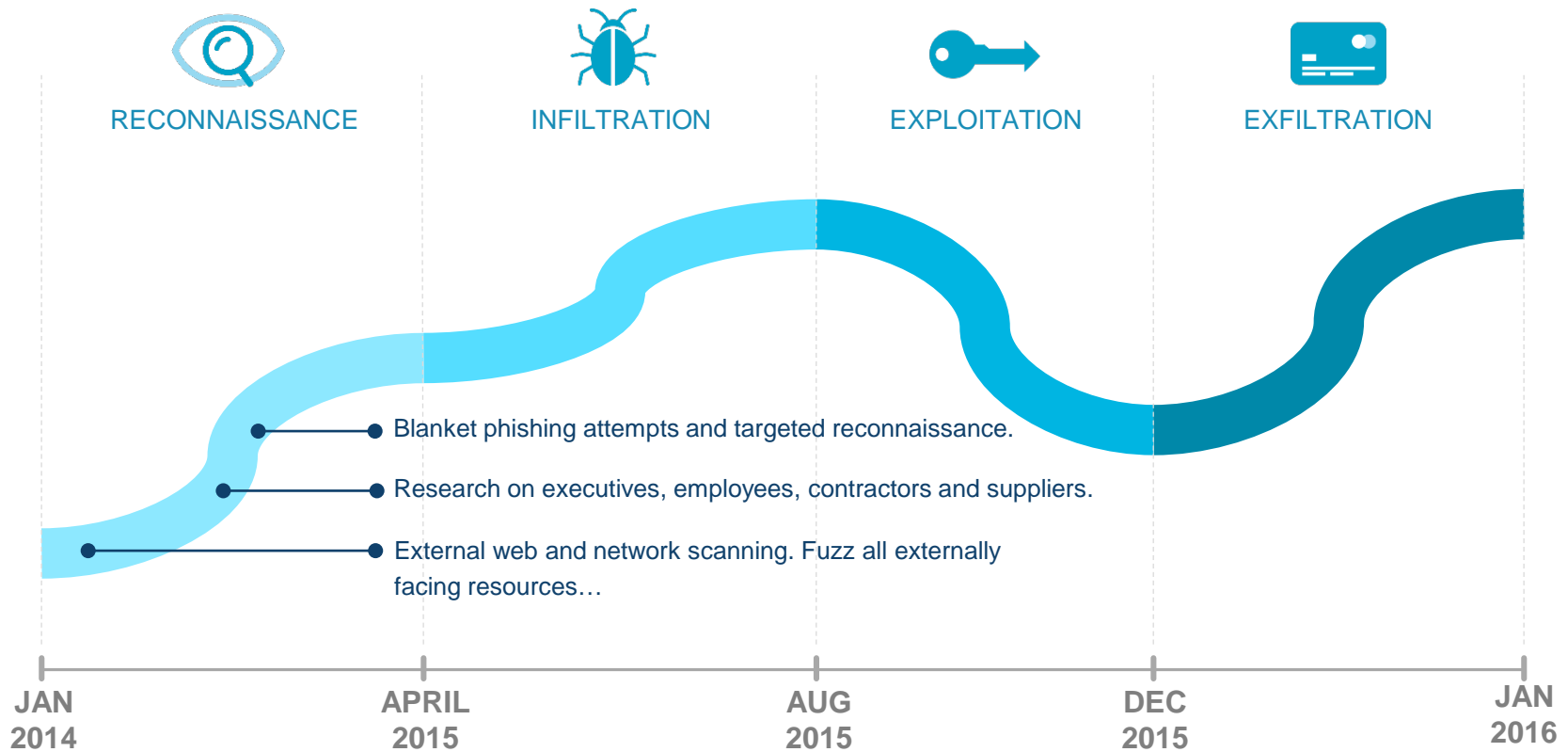
The Anatomy of a Data Breach

Reconnaissance



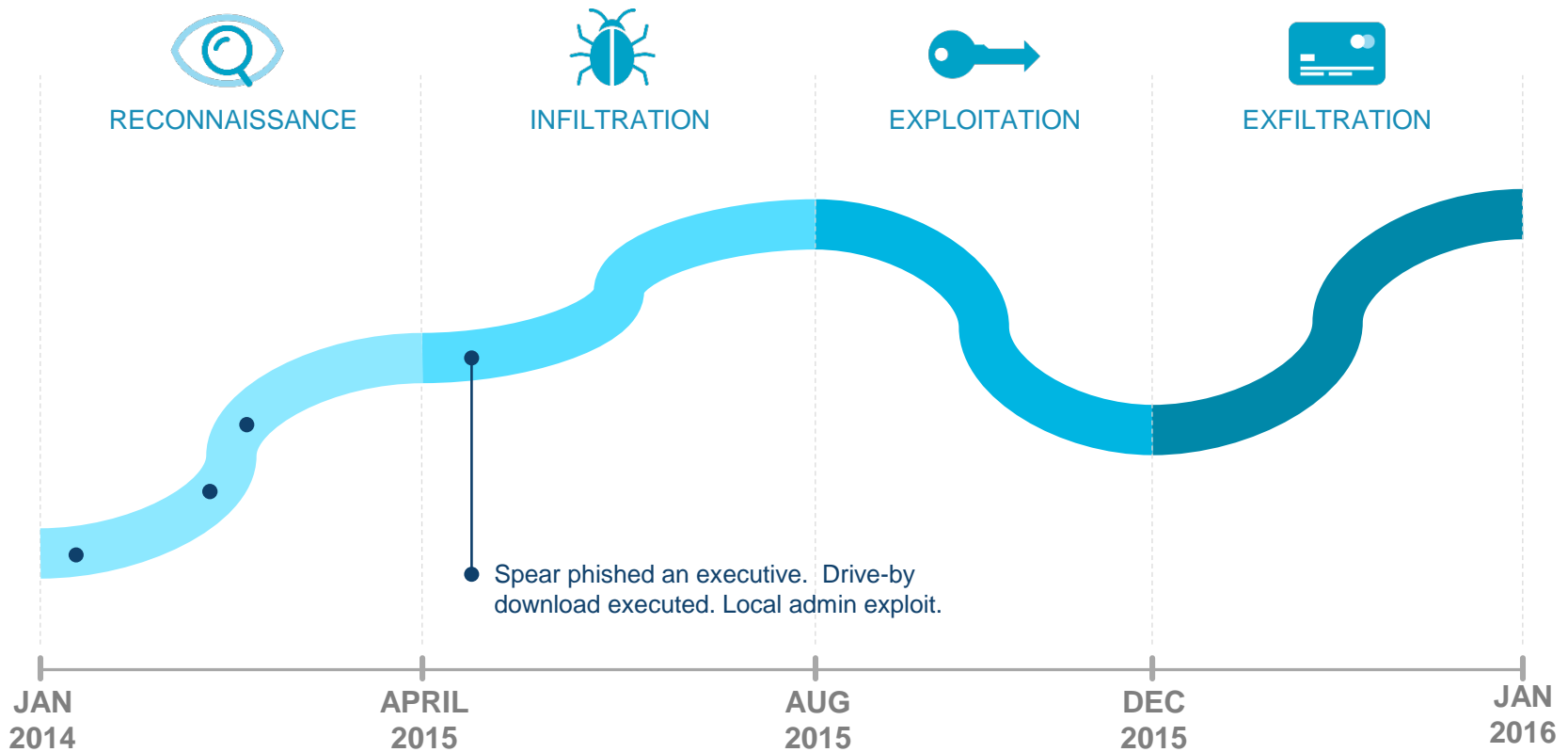
The Anatomy of a Data Breach

Reconnaissance



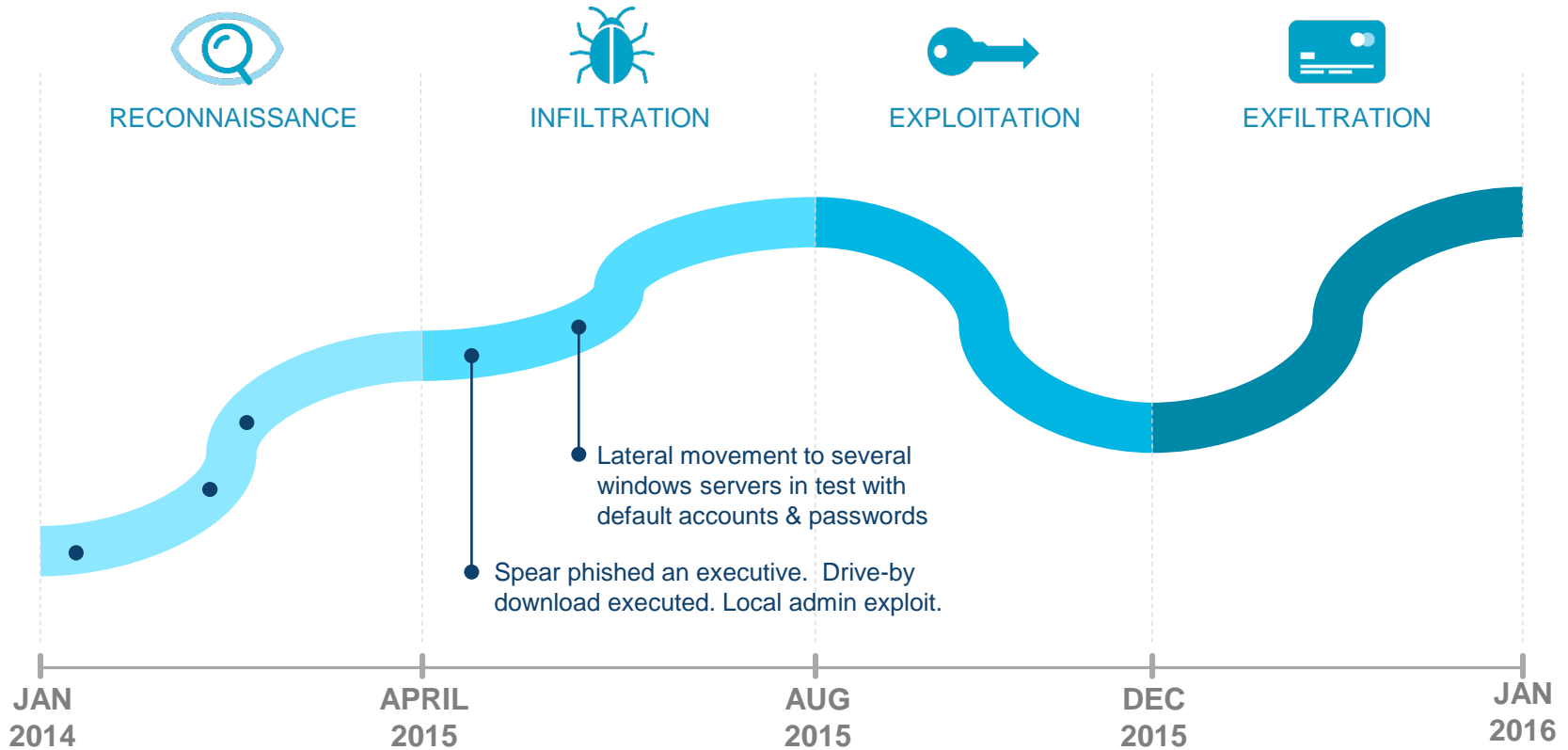
The Anatomy of a Data Breach

Infiltration



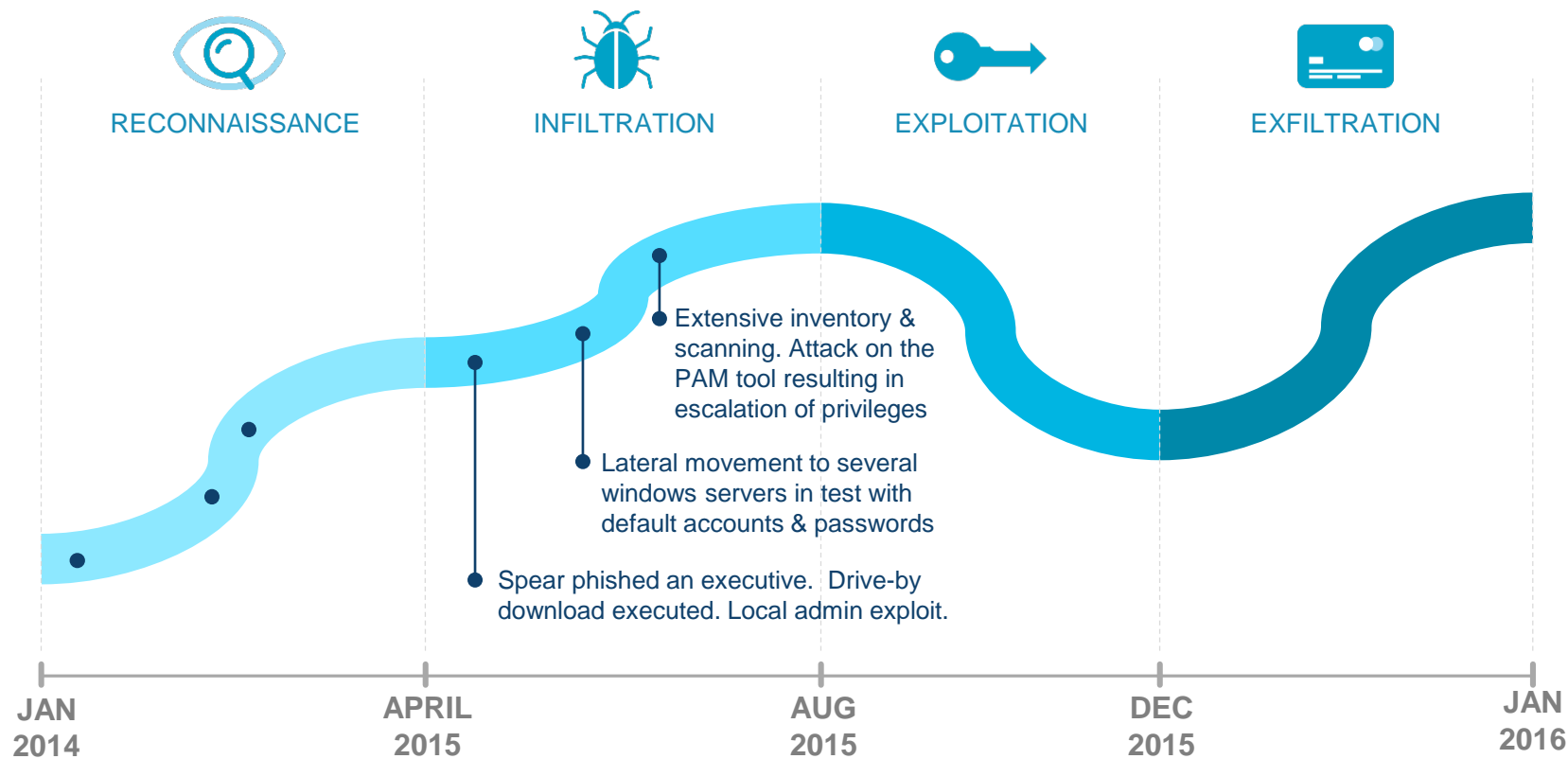
The Anatomy of a Data Breach

Infiltration



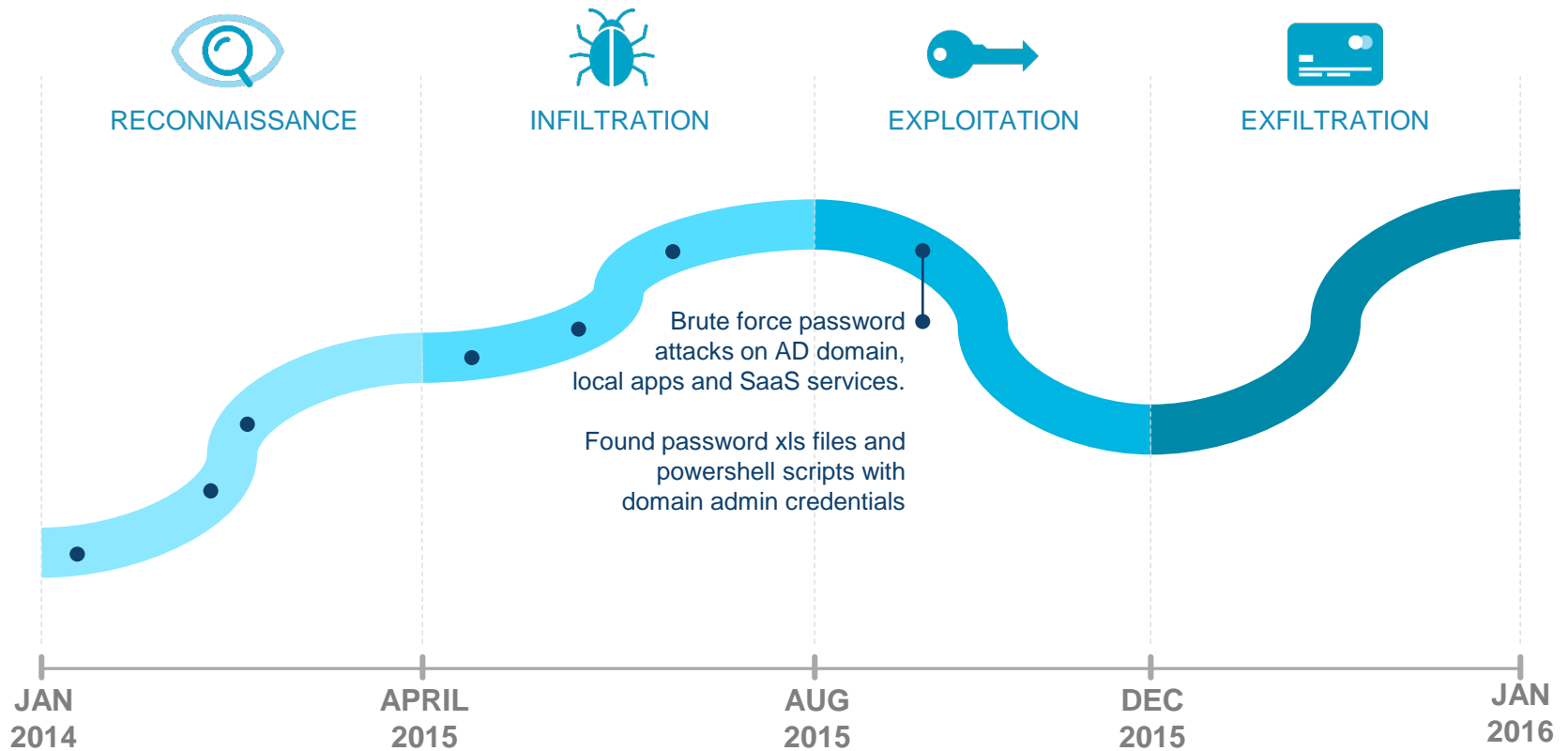
The Anatomy of a Data Breach

Infiltration



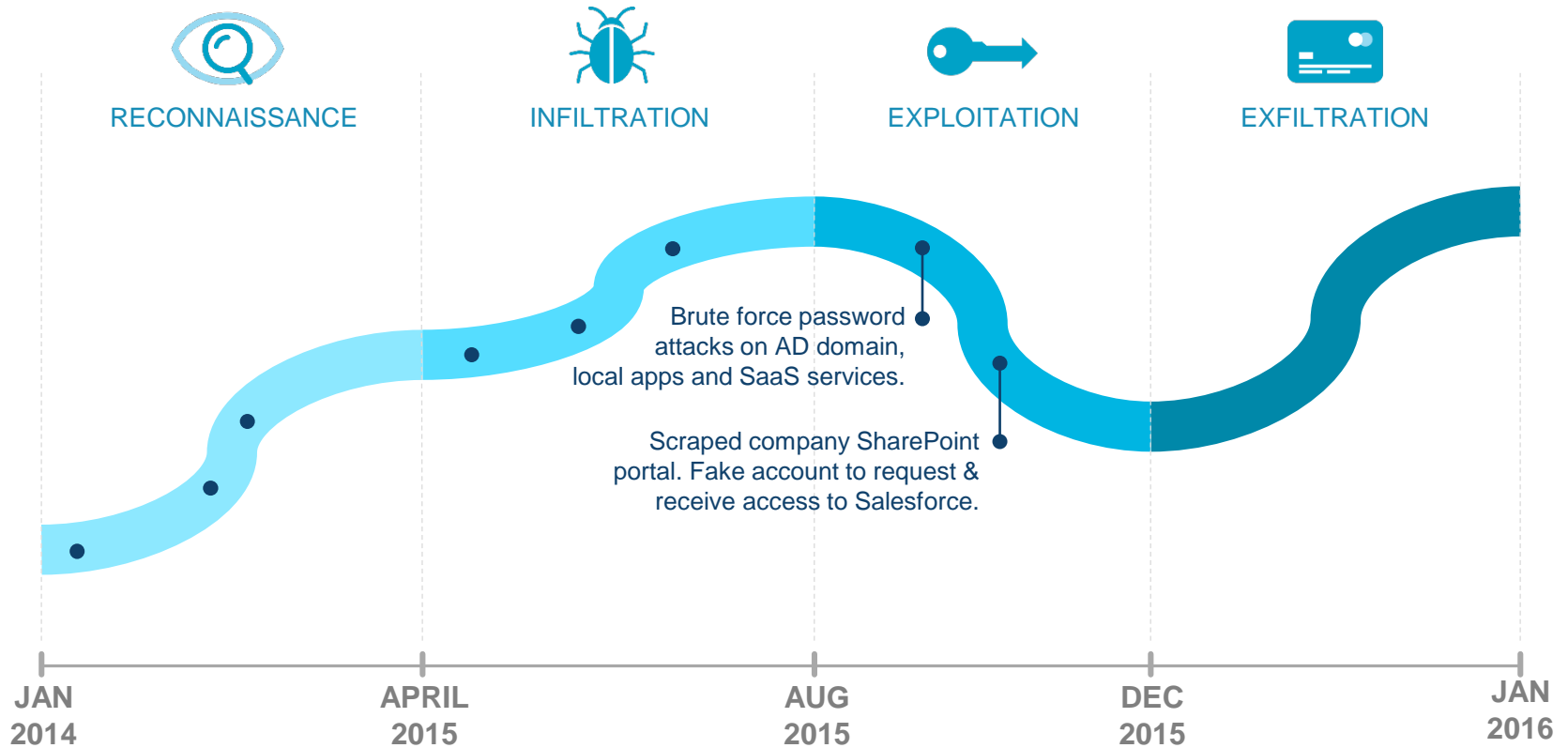
The Anatomy of a Data Breach

Exploitation



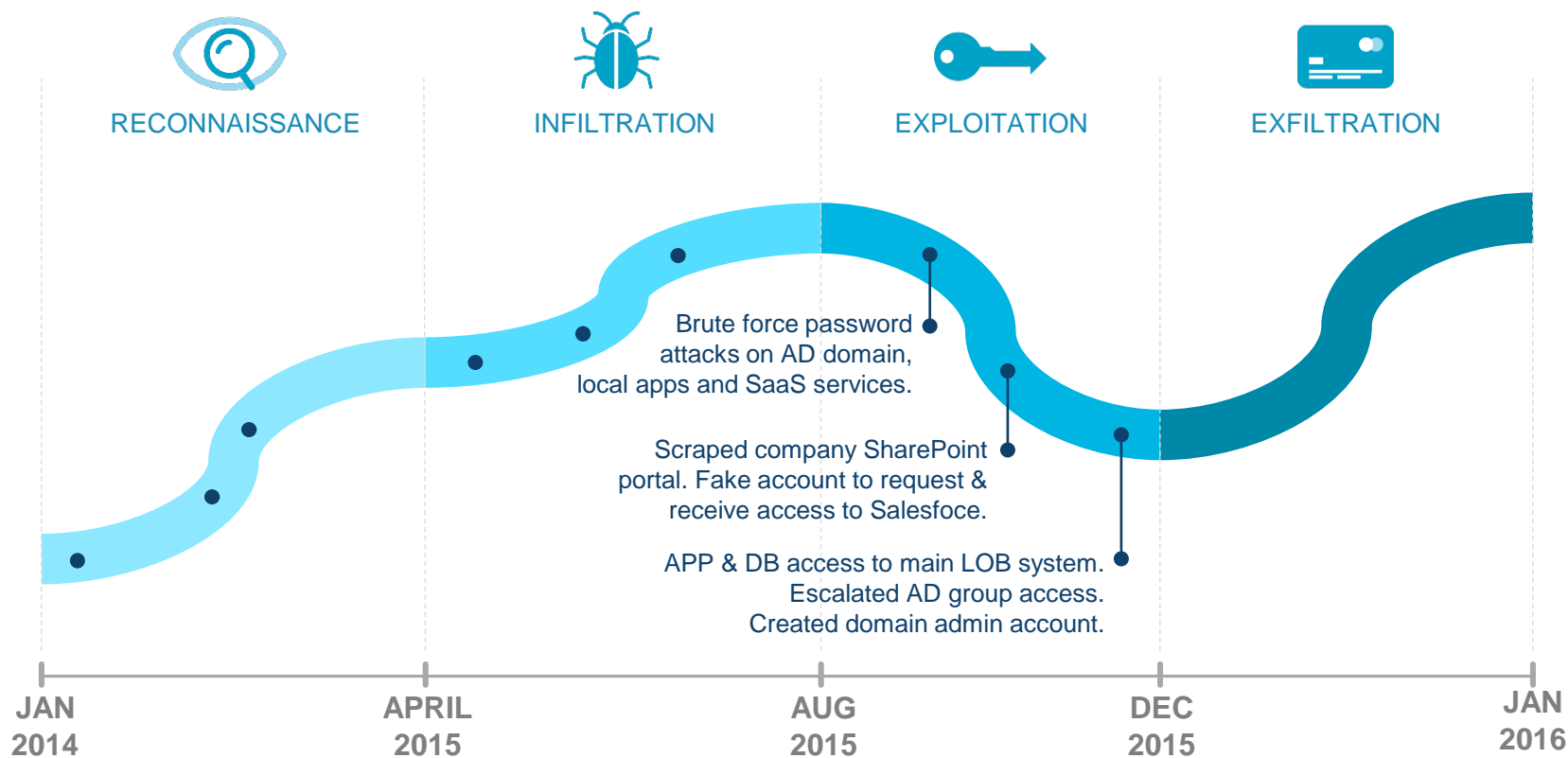
The Anatomy of a Data Breach

Exploitation



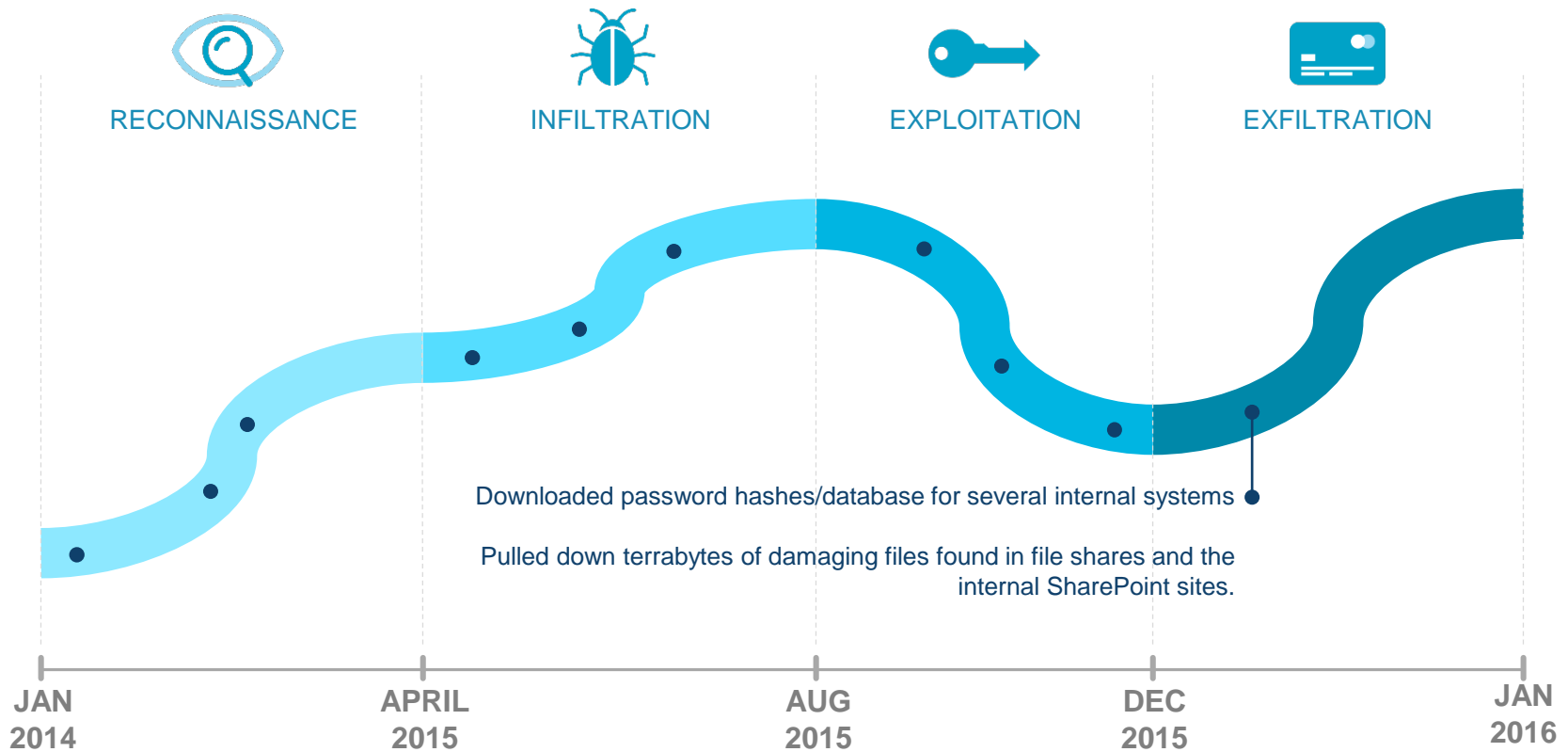
The Anatomy of a Data Breach

Exploitation



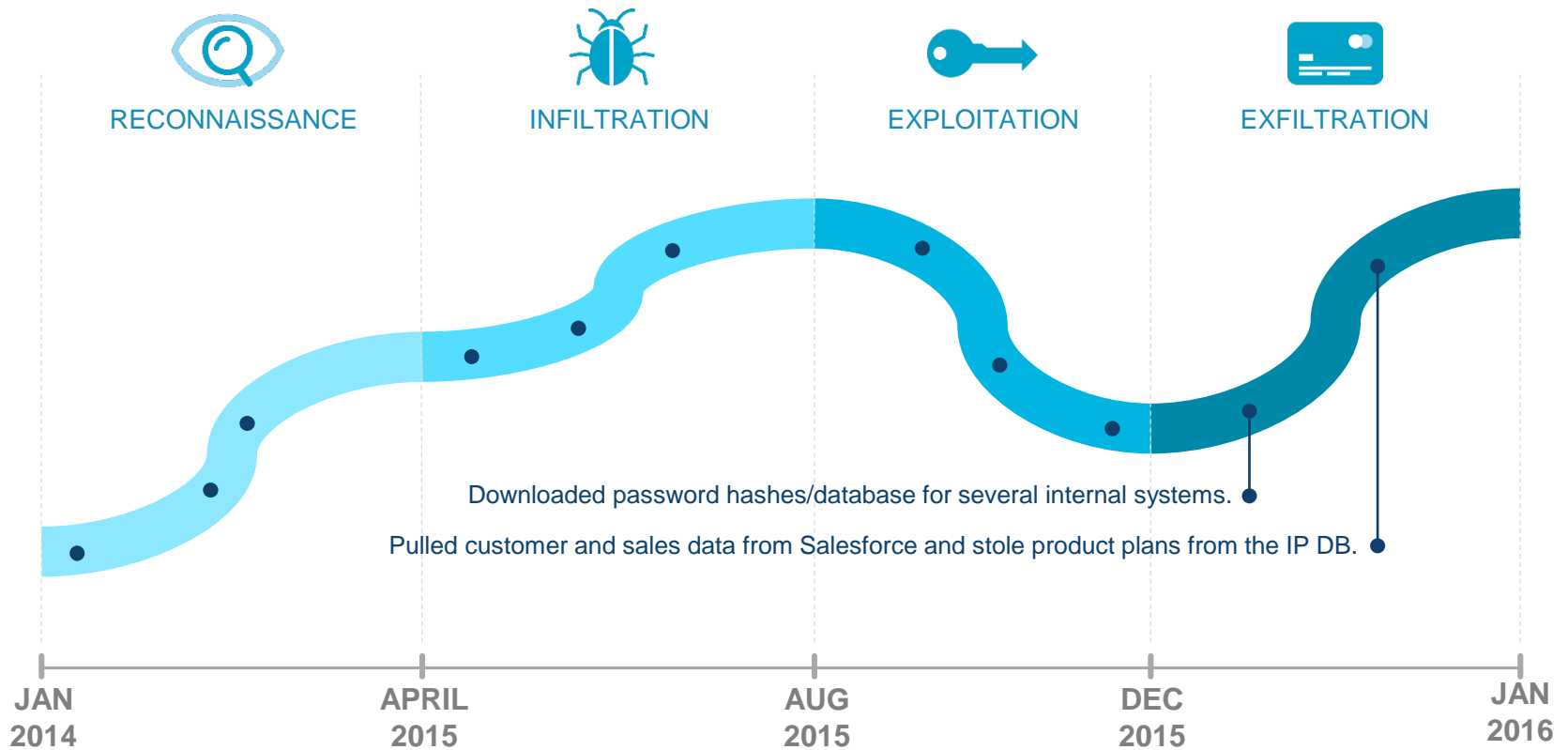
The Anatomy of a Data Breach

Exfiltration



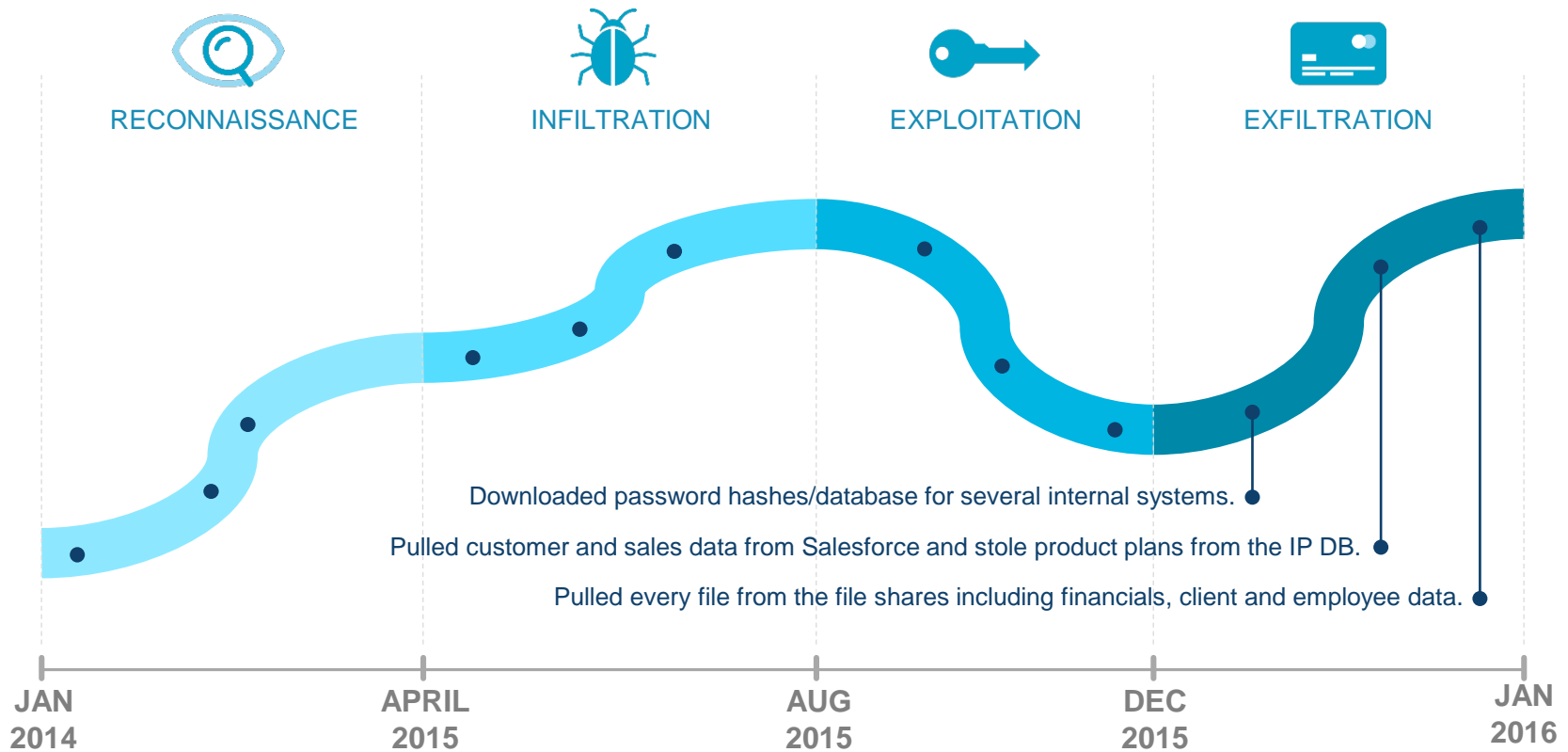
The Anatomy of a Data Breach

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

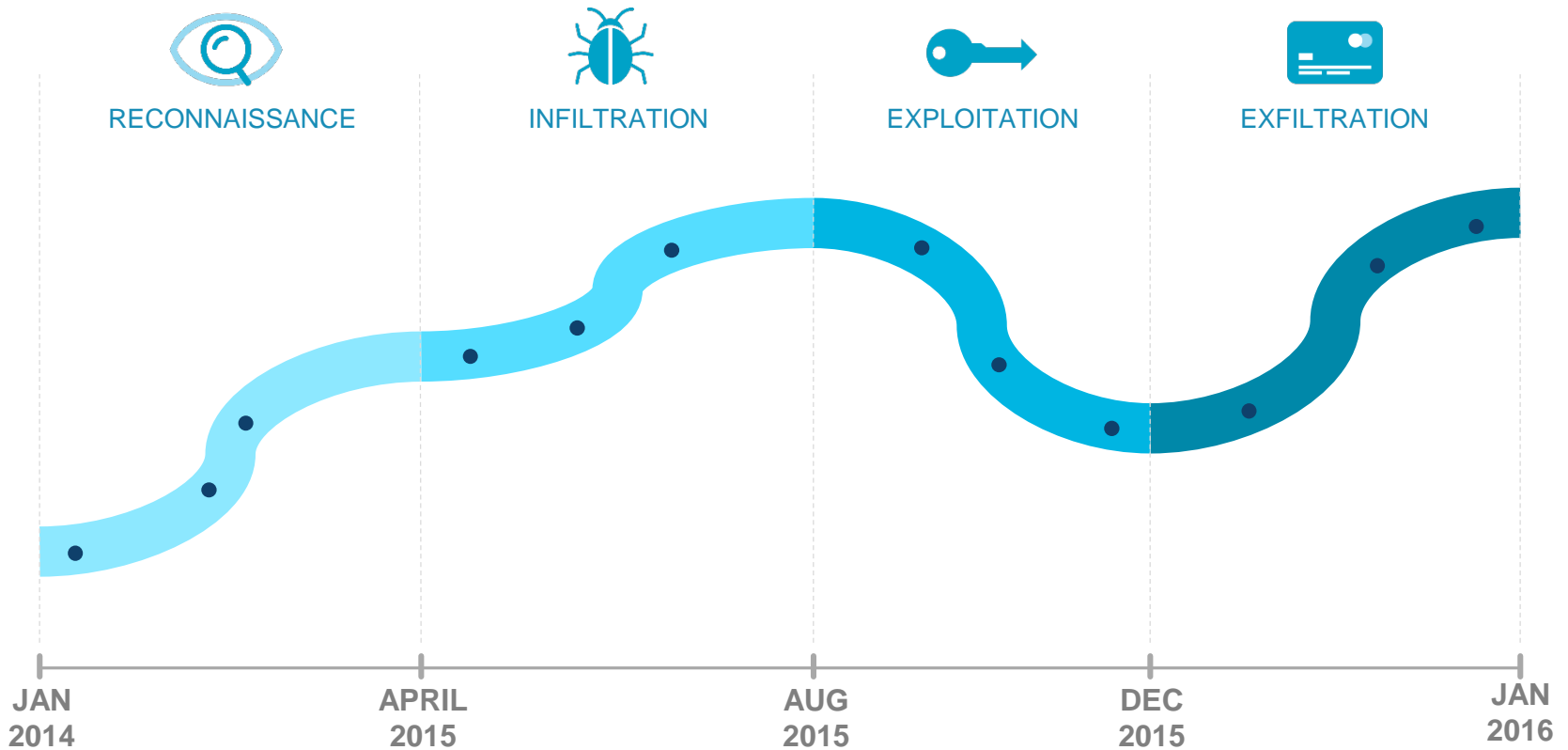


IAG Protection & Detection



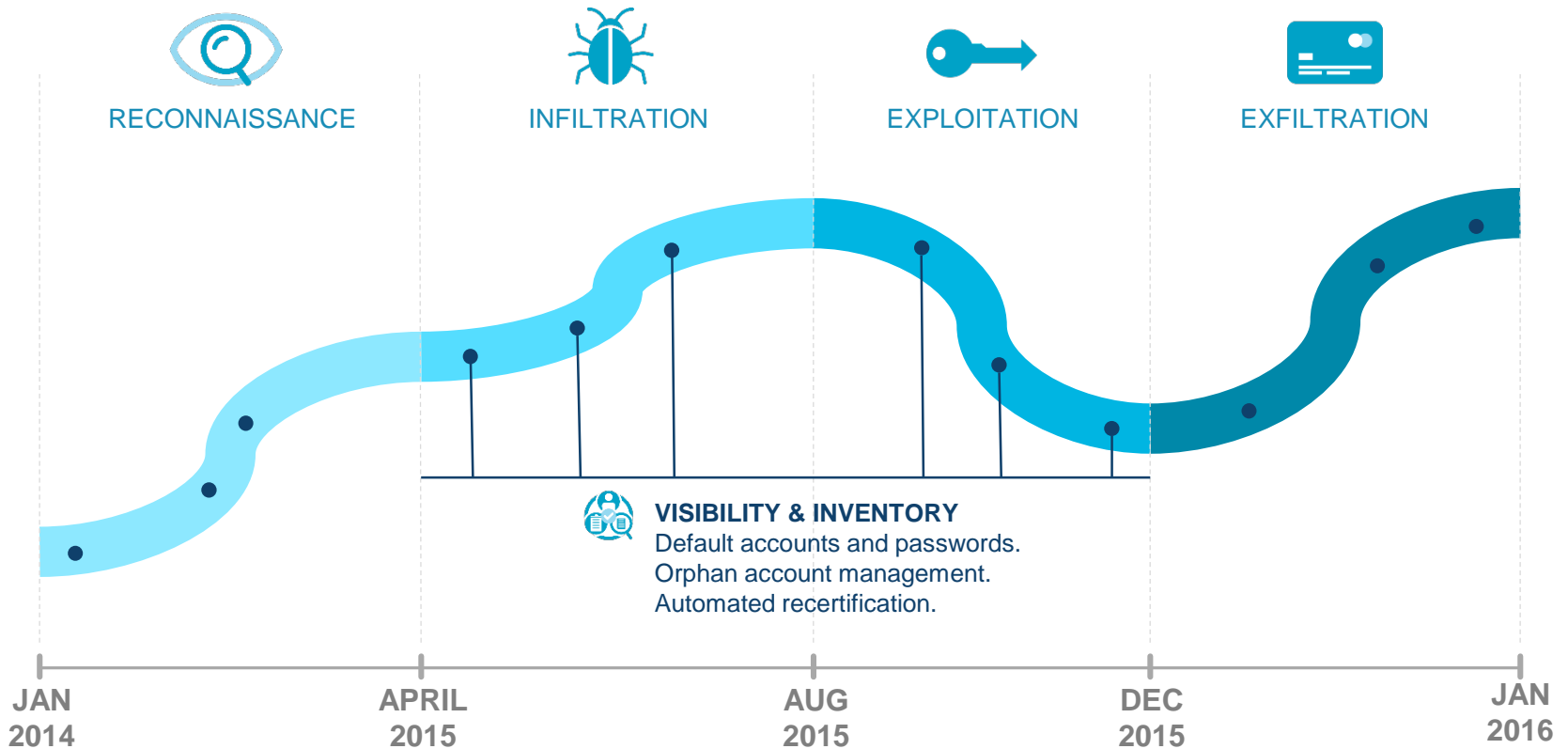
IAG Protection & Detection

The Anatomy of a Data Breach - Timeline



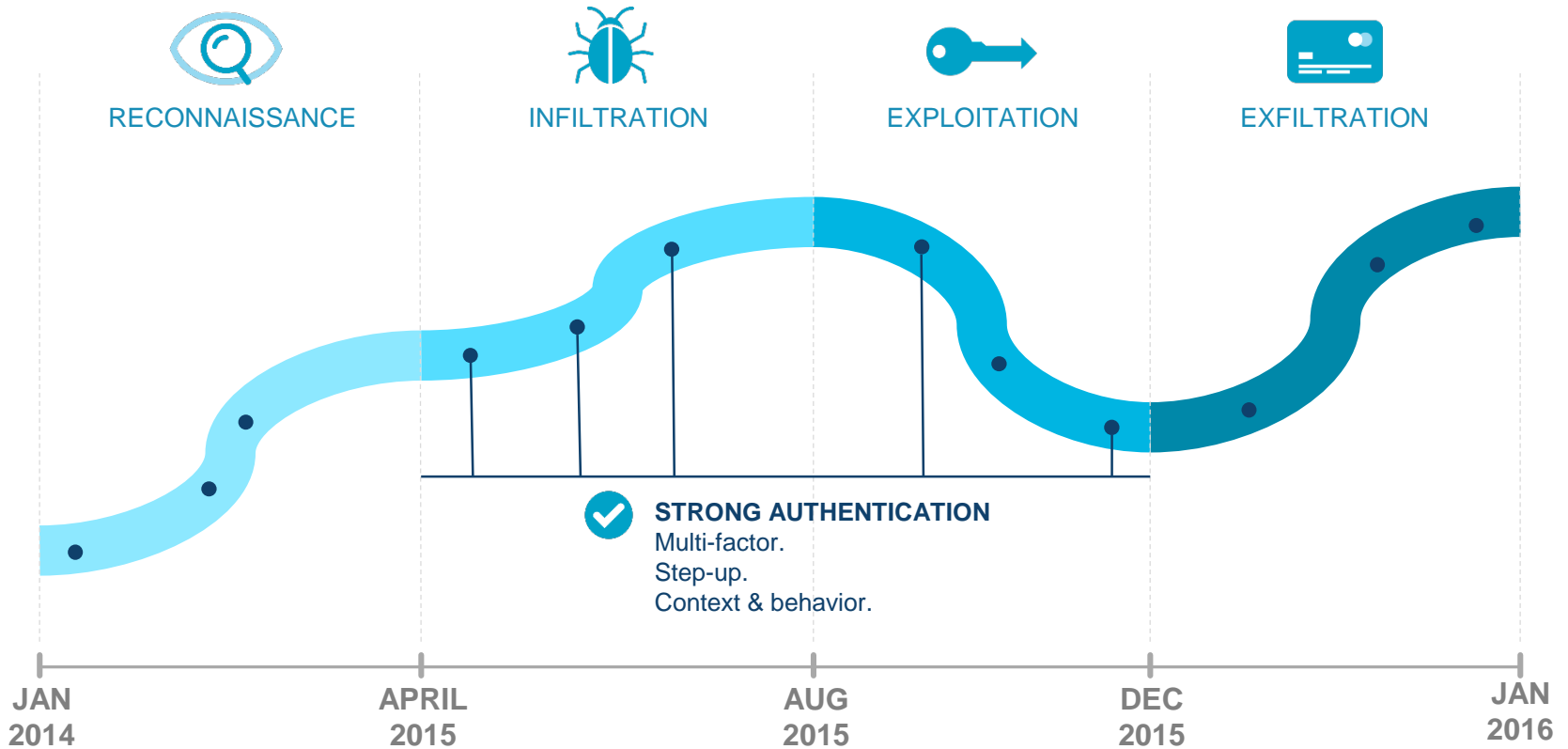
IAG Protection & Detection

Visibility & Inventory



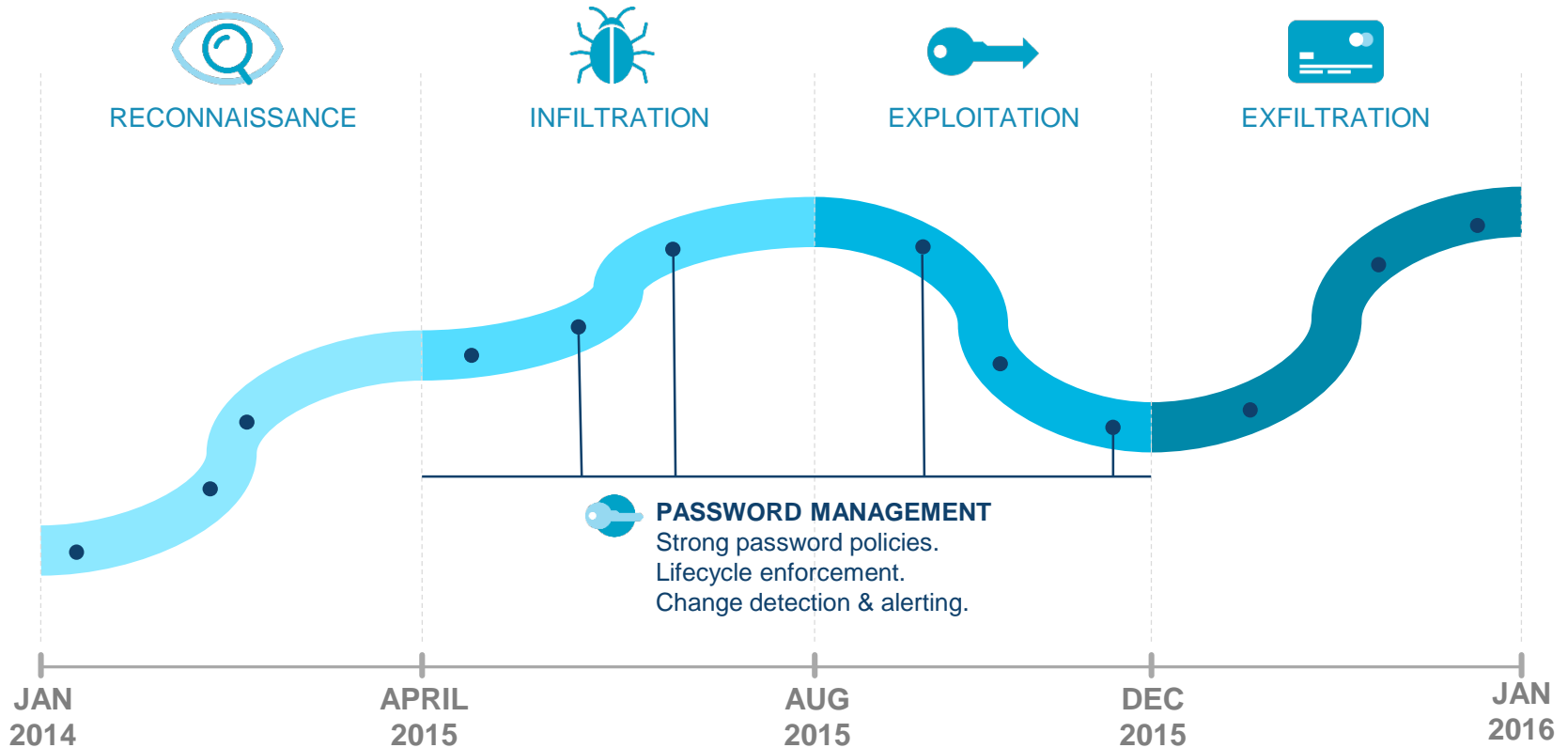
IAG Protection & Detection

Strong Authentication



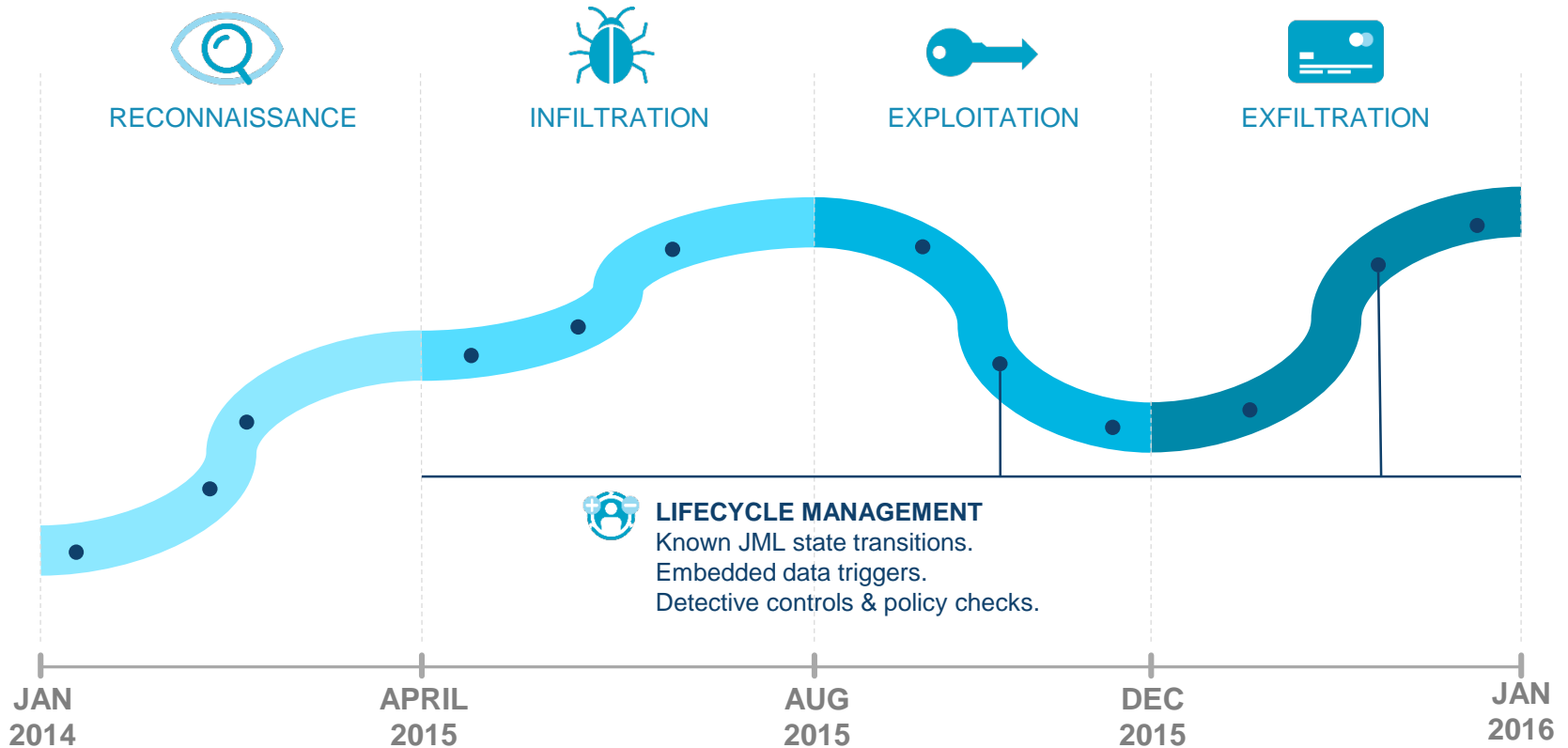
IAG Protection & Detection

Password Management



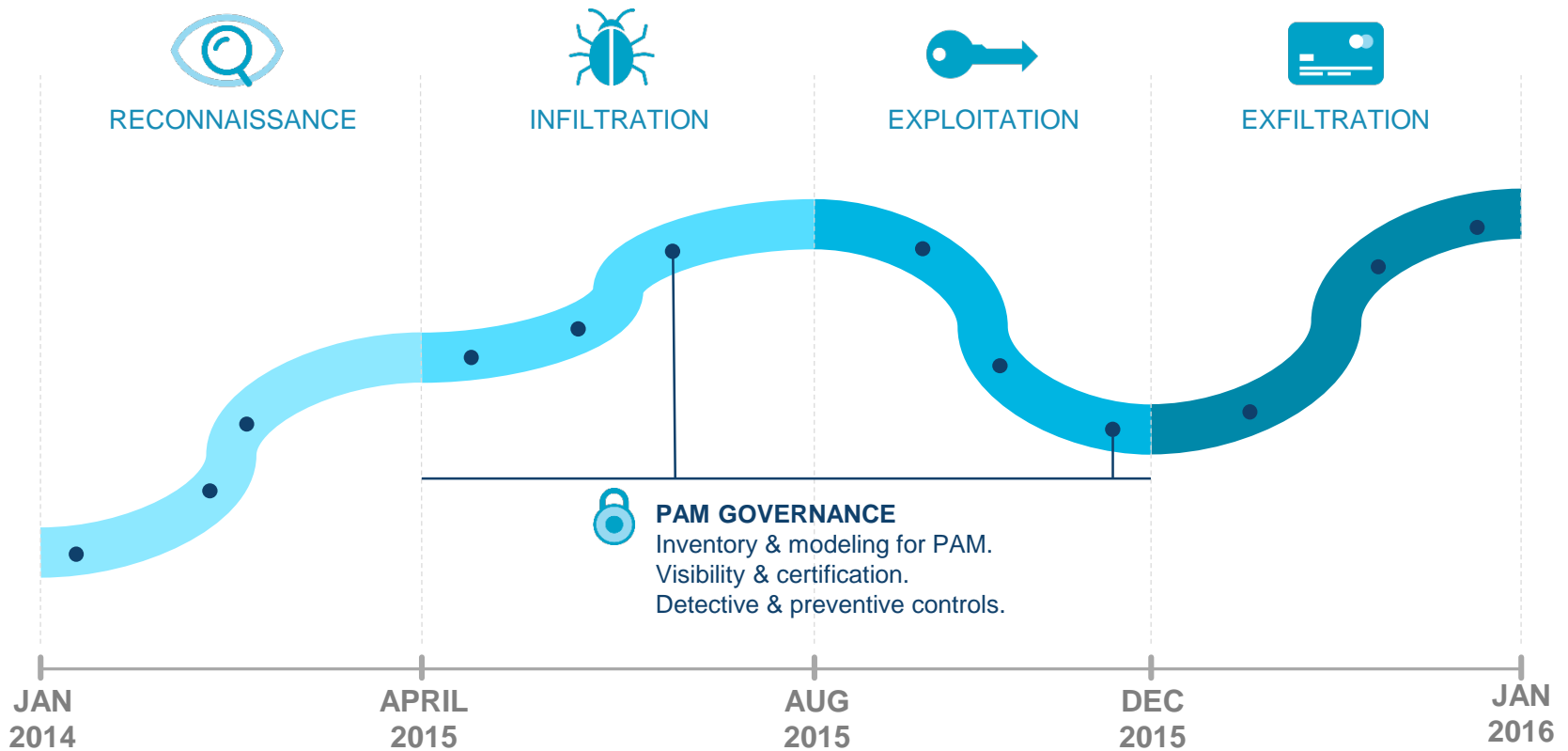
IAG Protection & Detection

Lifecycle Management



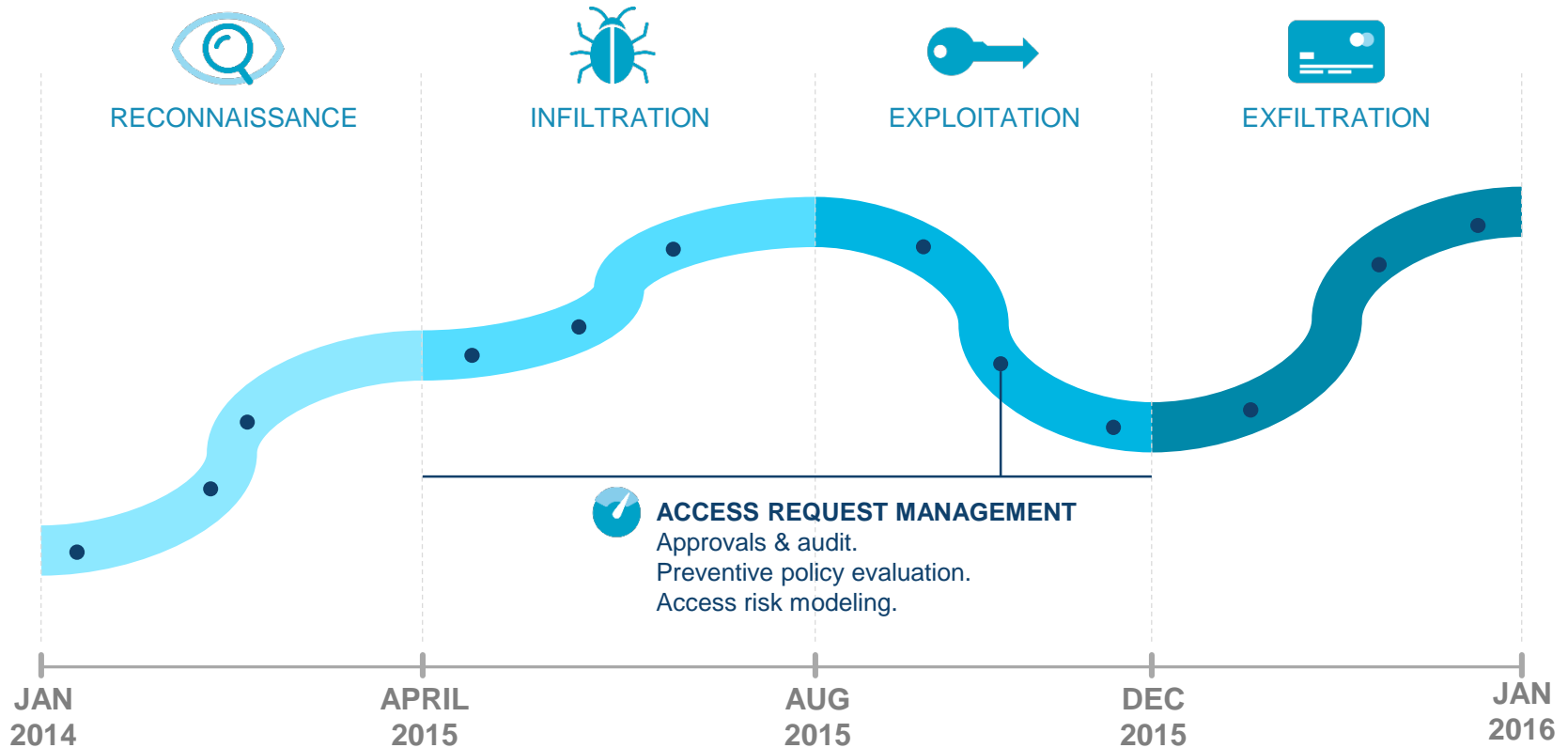
IAG Protection & Detection

PAM Governance



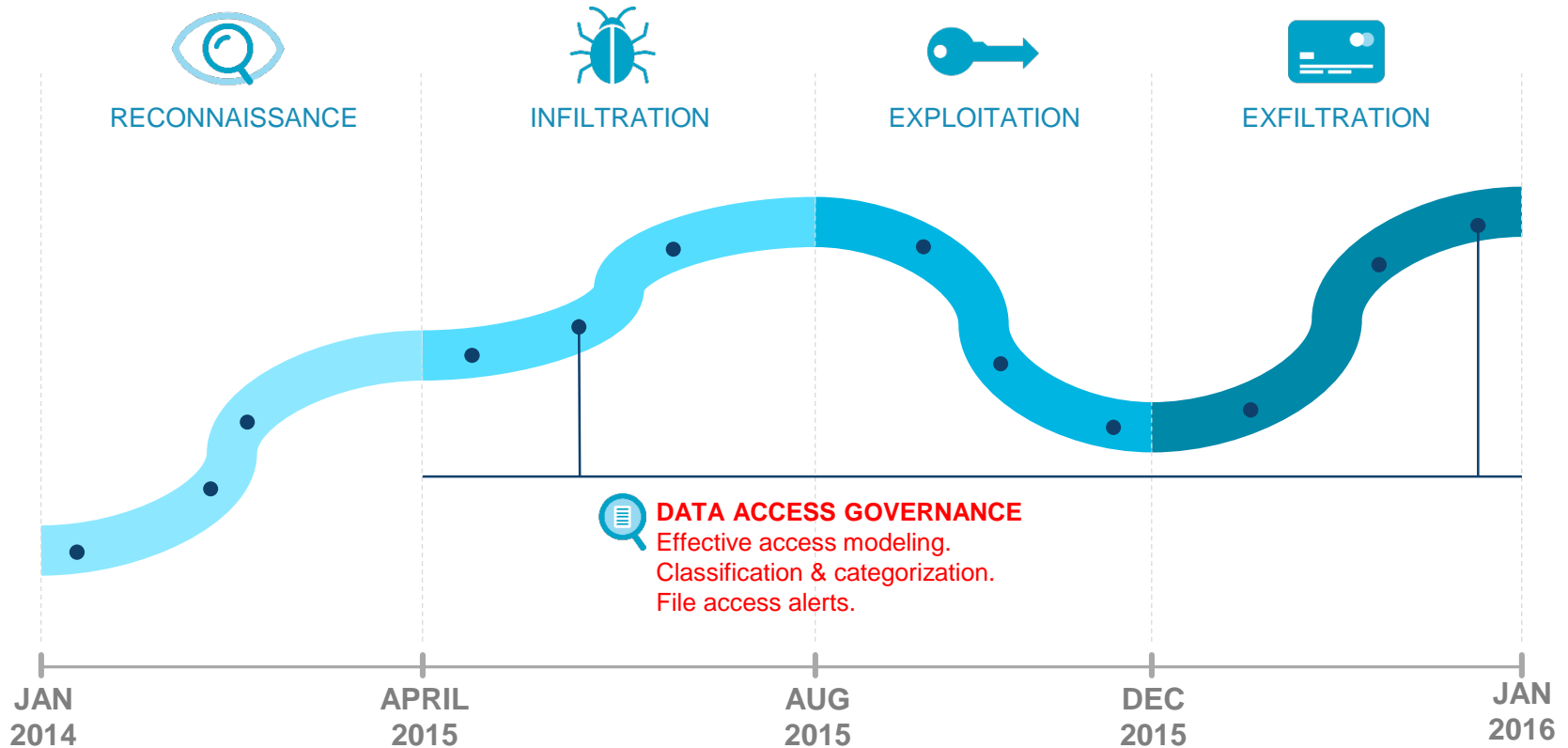
IAG Protection & Detection

Access Request Management



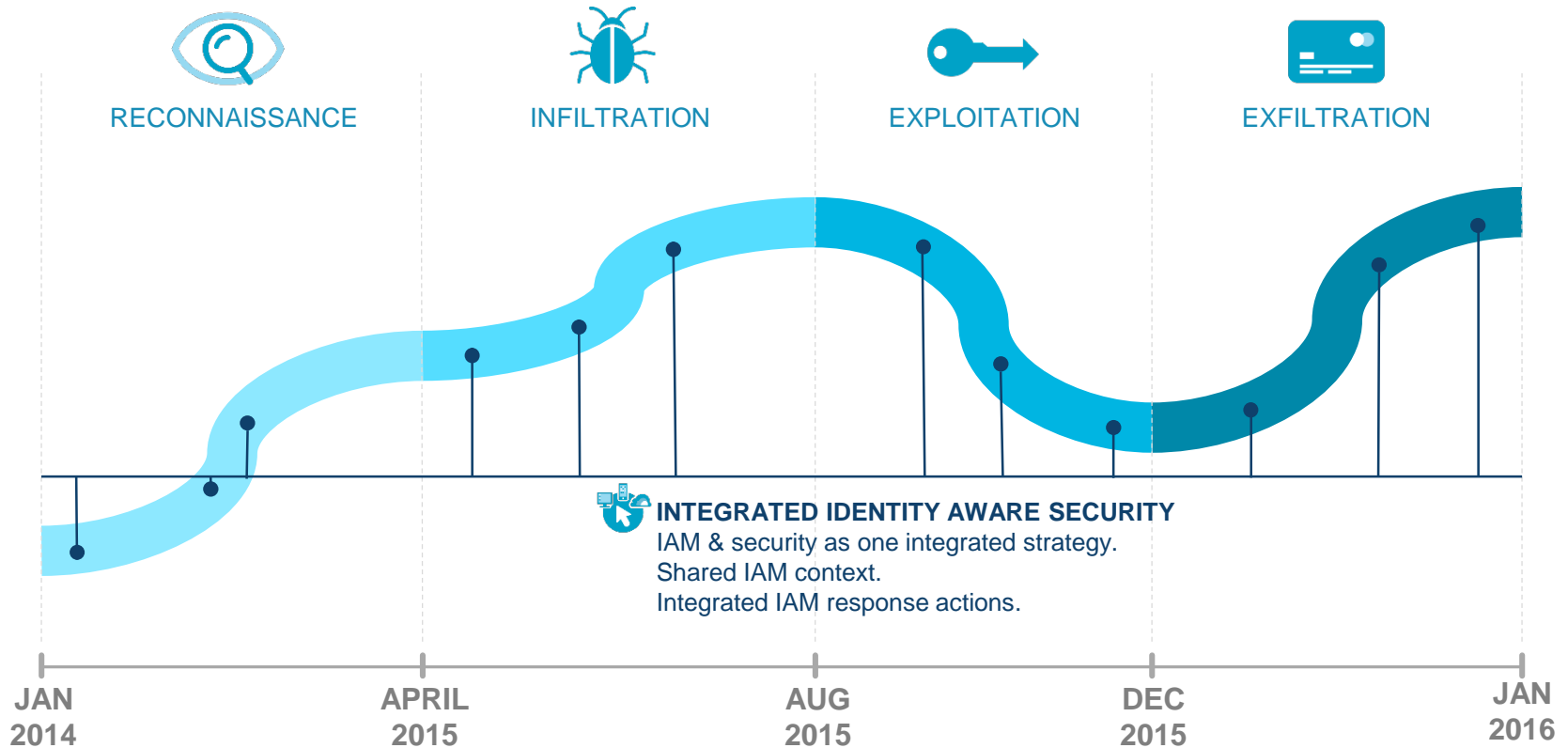
IAG Protection & Detection

Data Access Governance



IAG Protection & Detection

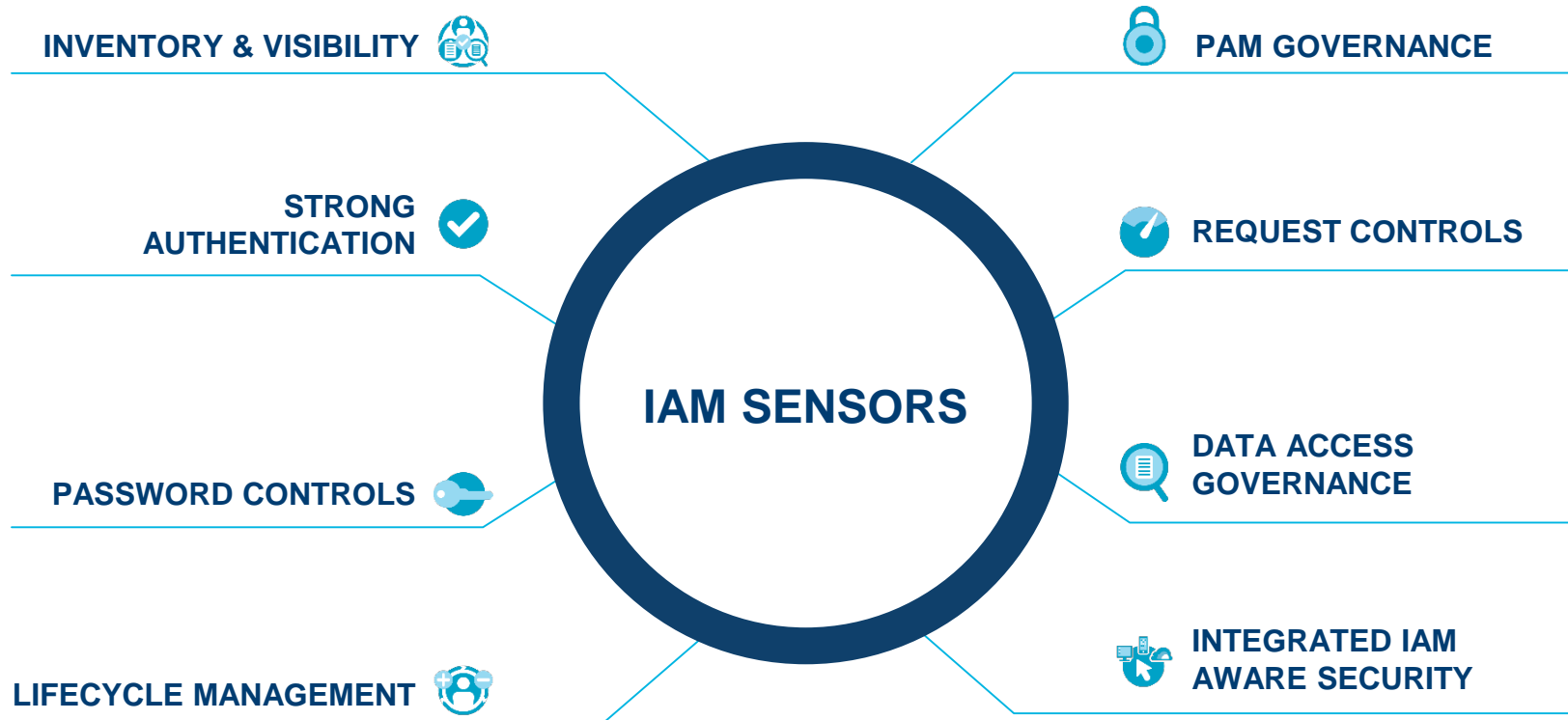
Integrated Identity Aware Security



IAG Protection & Detection



IAG Protection & Detection



IAG Sensors



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



Andreas Fuhrmann
SKyPRO AG
andreas.fuhrmann@skypro.ch

John Waters
SailPoint
john.waters@sailpoint.com



Unpublished Work of SKyPRO, All Rights Reserved.

This work is an unpublished work and contains confidential, proprietary, and trade secret information of SKyPRO. Access to this work is restricted to SKyPRO employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of SKyPRO. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

General Disclaimer

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. SKyPRO makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for SKyPRO products remains at the sole discretion of SKyPRO. Further, SKyPRO reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All SKyPRO marks referenced in this presentation are trademarks or registered trademarks of SKyPRO in Switzerland and other countries. All third-party trademarks are the property of their respective owners.

