CYBERARK \ LABS

Okta Supply Chain Hack

2023 Edition

Lessons Learned and Mitigation Strategies

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.

Andy Thompson

Offensive Security Research Evangelist

- SSCP/CISSP
- GPEN
- Emcee of Dallas Hackers Association
- Travel Hacker
- Mentor

in andythompsoninfosec

Andy_Thompson

Andy.Thompson@CyberArk.com

Importance of this Discussion

- Identity is at the core.

Importance of this Discussion

- Identity is at the core.
- Pinpoint gaps in security.

Importance of this Discussion

- Identity is at the core.
- Pinpoint gaps in security.
- Don’t let happen to you!

Agenda

- Support portal compromise.

Agenda

- Support portal compromise.
- Downstream attacks.

Agenda

- Support portal compromise.
- Downstream attacks.
- Detection, Response, & Disclosure.

Agenda

- Support portal compromise.
- Downstream attacks.
- Detection, Response, & Disclosure.
- Prevention & mitigation strategies.

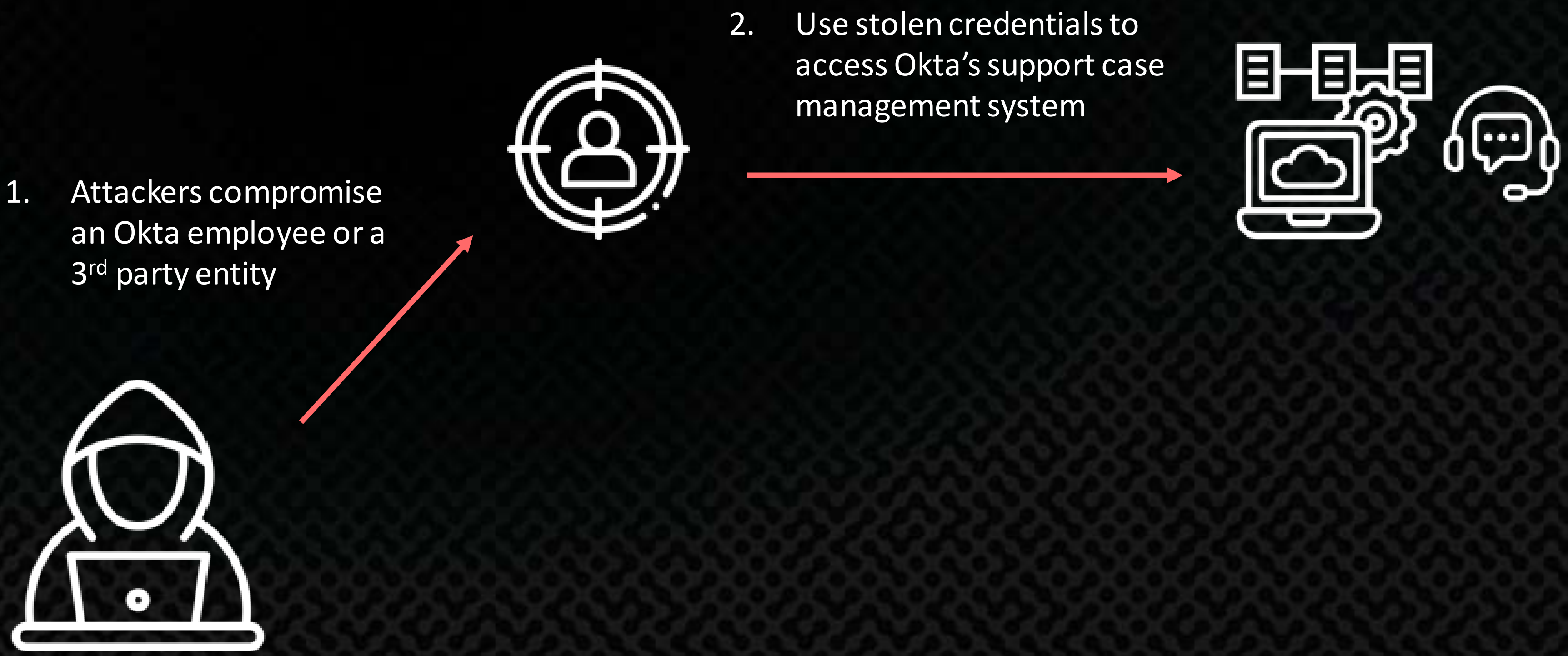
CyberArk Labs Analysis

Okta Breach Flow (November 2023)

1. Attackers compromise an Okta employee or a 3rd party entity

CyberArk Labs Analysis

Okta Breach Flow (November 2023)

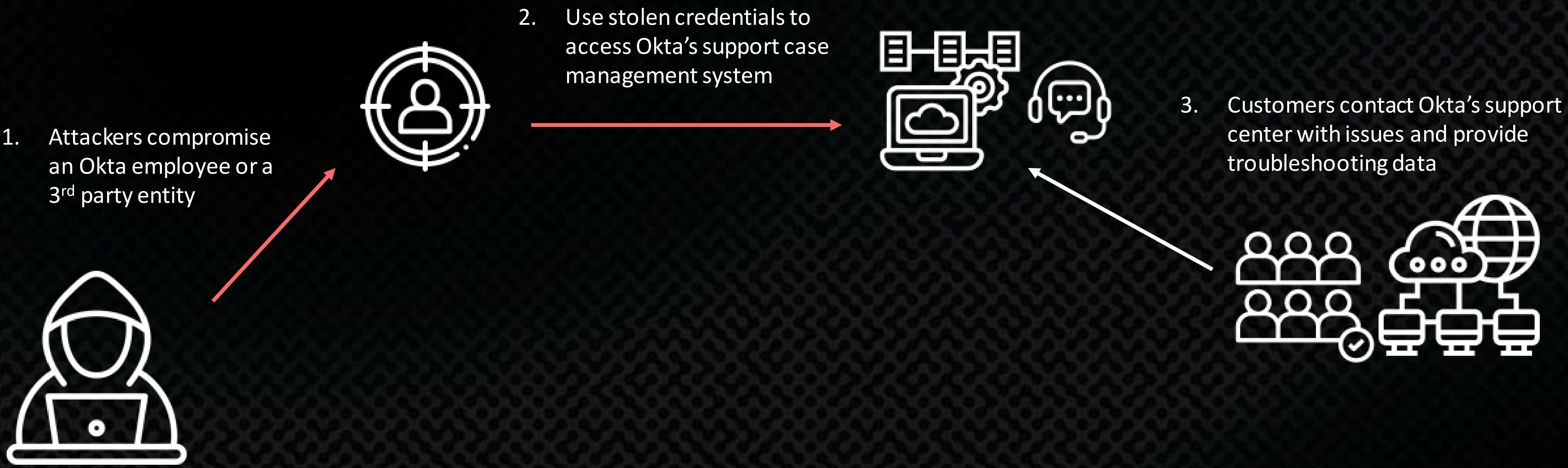


1. Attackers compromise an Okta employee or a 3rd party entity

2. Use stolen credentials to access Okta's support case management system

CyberArk Labs Analysis

Okta Breach Flow (November 2023)

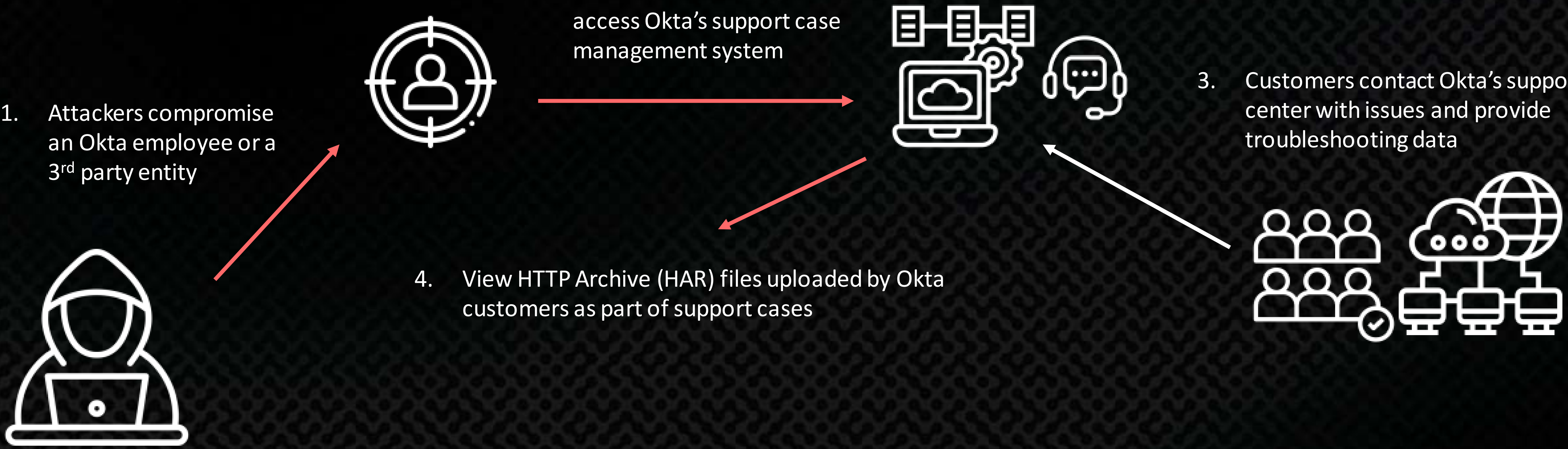


1. Attackers compromise an Okta employee or a 3rd party entity
2. Use stolen credentials to access Okta's support case management system
3. Customers contact Okta's support center with issues and provide troubleshooting data

HTTP Archive (HAR)

- Performance analysis.
- Debugging.
- Security.

Okta Breach Flow (November 2023)



1. Attackers compromise an Okta employee or a 3rd party entity

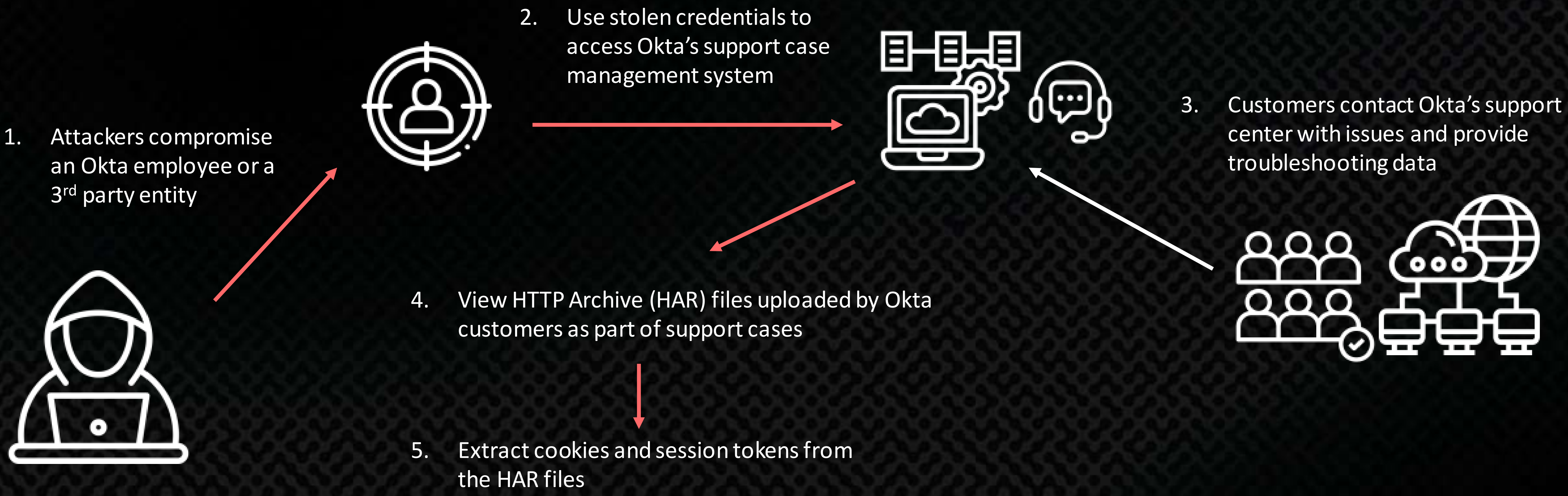
2. Use stolen credentials to access Okta's support case management system

3. Customers contact Okta's support center with issues and provide troubleshooting data

4. View HTTP Archive (HAR) files uploaded by Okta customers as part of support cases

CyberArk Labs Analysis

Okta Breach Flow (November 2023)



1. Attackers compromise an Okta employee or a 3rd party entity

2. Use stolen credentials to access Okta’s support case management system

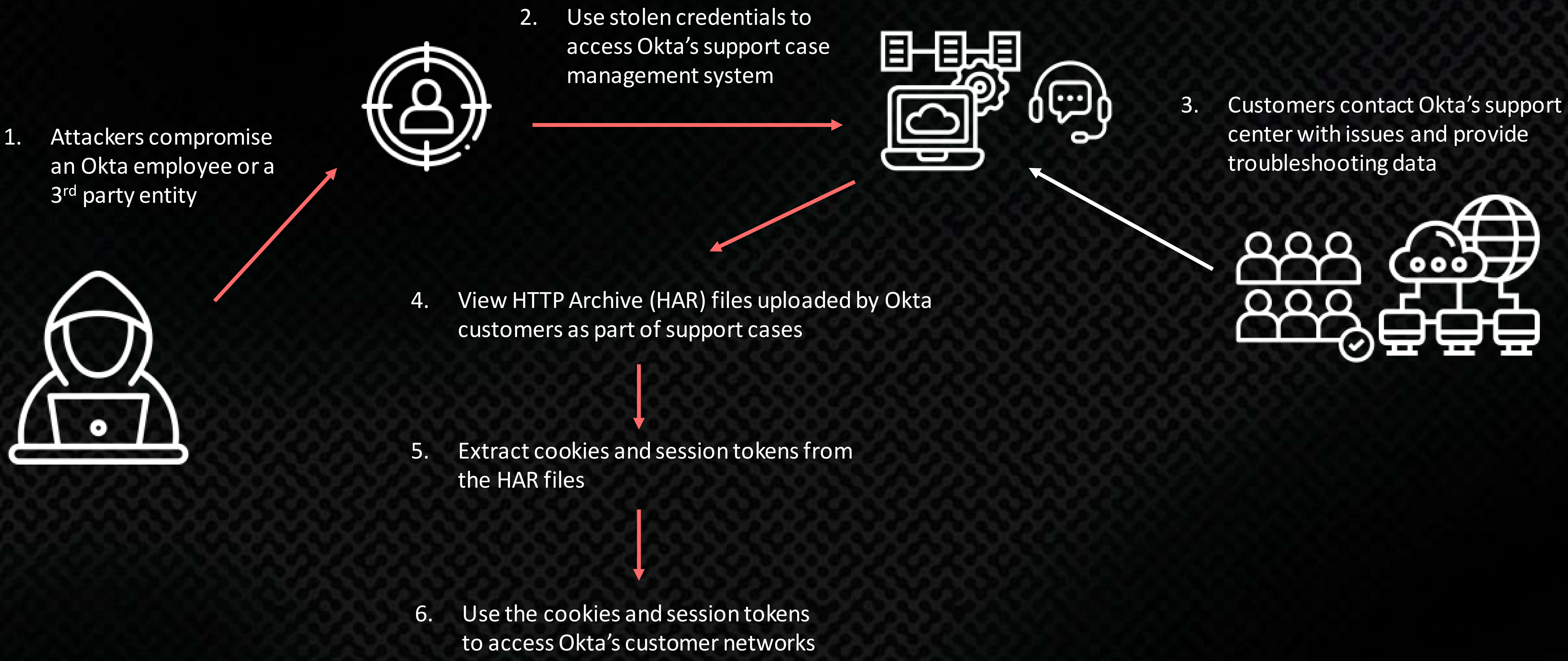
3. Customers contact Okta’s support center with issues and provide troubleshooting data

4. View HTTP Archive (HAR) files uploaded by Okta customers as part of support cases

5. Extract cookies and session tokens from the HAR files

CyberArk Labs Analysis

Okta Breach Flow (November 2023)



1. Attackers compromise an Okta employee or a 3rd party entity

2. Use stolen credentials to access Okta’s support case management system

3. Customers contact Okta’s support center with issues and provide troubleshooting data

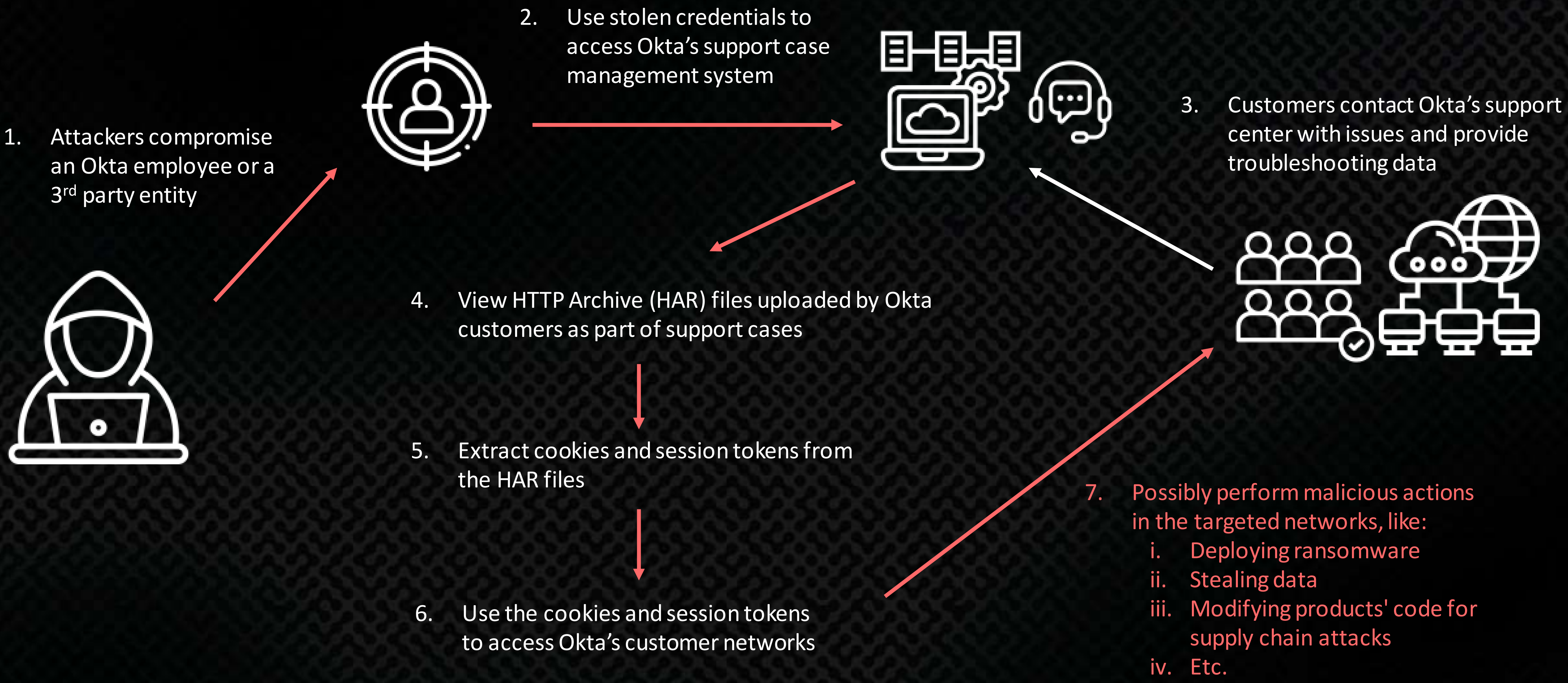
4. View HTTP Archive (HAR) files uploaded by Okta customers as part of support cases

5. Extract cookies and session tokens from the HAR files

6. Use the cookies and session tokens to access Okta’s customer networks

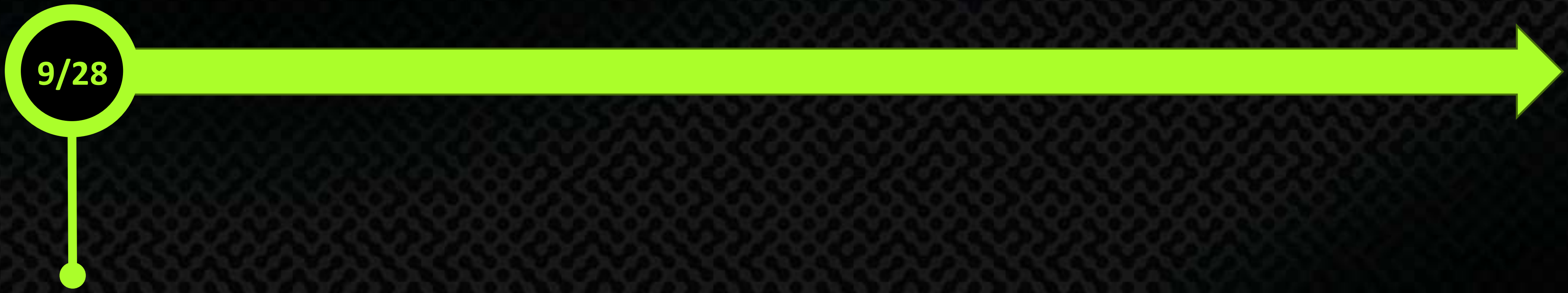
CyberArk Labs Analysis

Okta Breach Flow (November 2023)



1. Attackers compromise an Okta employee or a 3rd party entity
2. Use stolen credentials to access Okta’s support case management system
3. Customers contact Okta’s support center with issues and provide troubleshooting data
4. View HTTP Archive (HAR) files uploaded by Okta customers as part of support cases
5. Extract cookies and session tokens from the HAR files
6. Use the cookies and session tokens to access Okta’s customer networks
7. Possibly perform malicious actions in the targeted networks, like:
   i. Deploying ransomware
   ii. Stealing data
   iii. Modifying products' code for supply chain attacks
   iv. Etc.

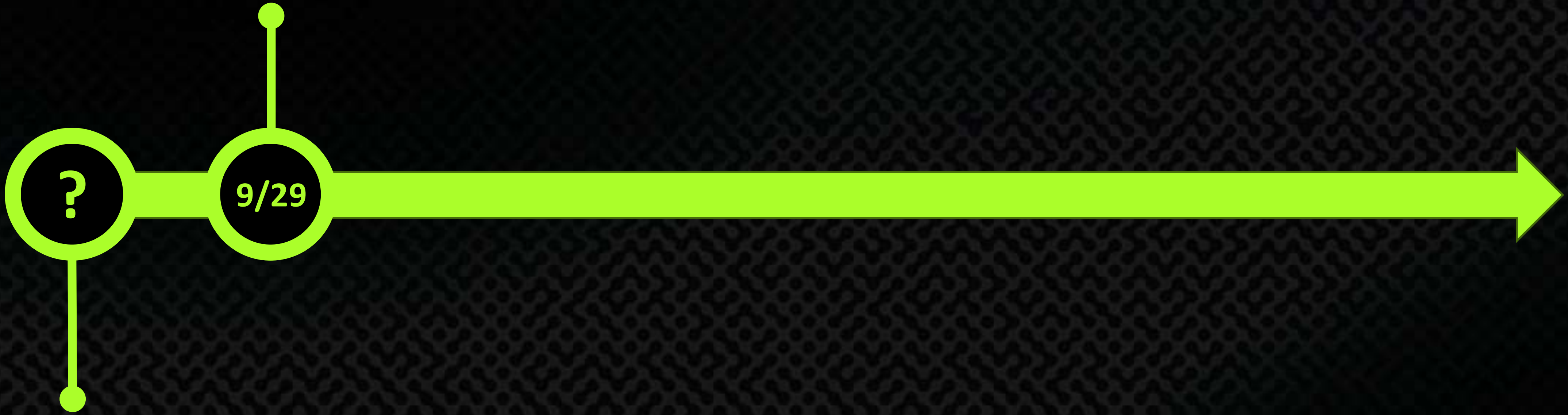
Breach Timeline



9/28

Initial Compromise

Breach Timeline



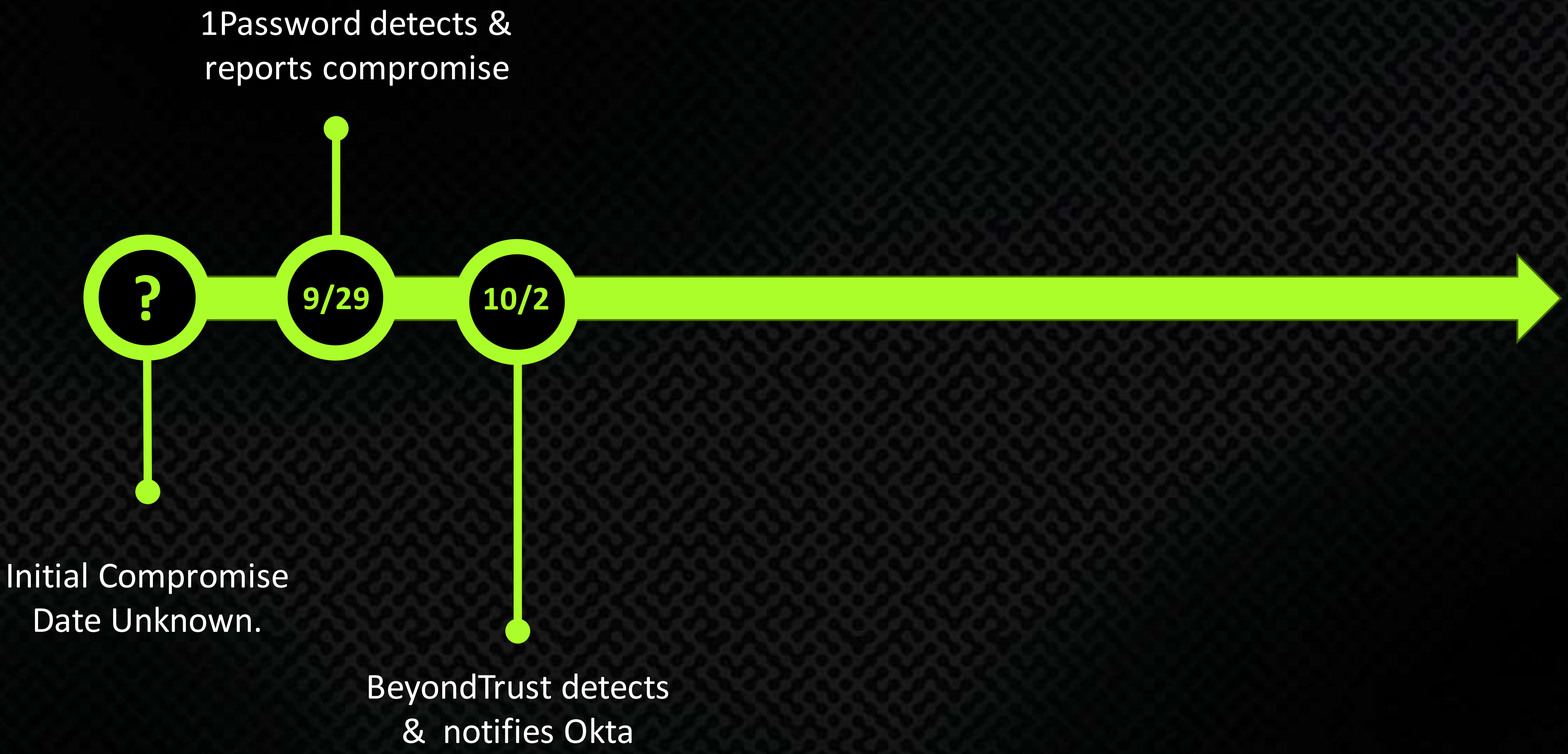
1Password detects & reports compromise

?

9/29

Initial Compromise Date Unknown.

Breach Timeline

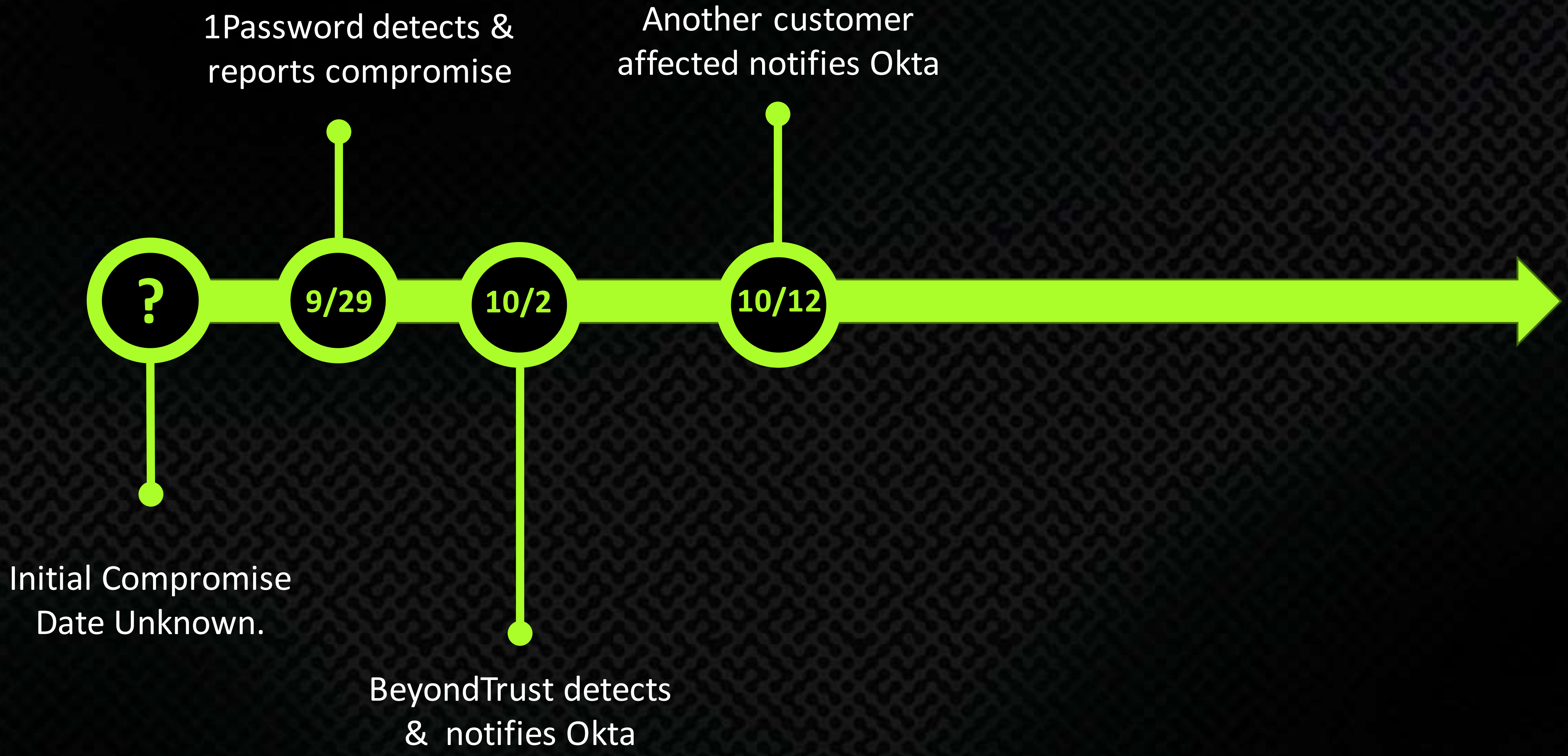


1Password detects & reports compromise

Initial Compromise Date Unknown.

BeyondTrust detects & notifies Okta

Breach Timeline



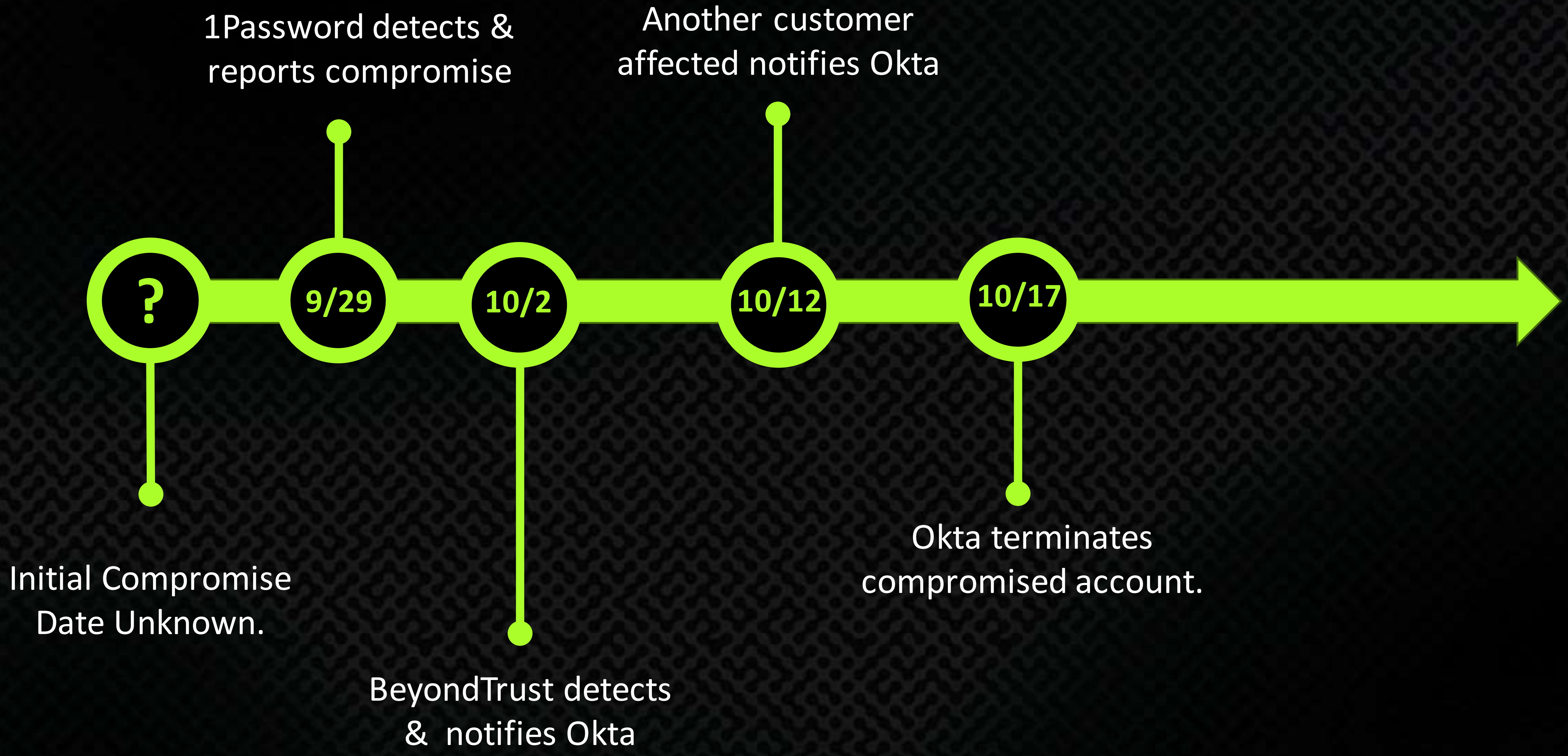
Initial Compromise Date Unknown.

1Password detects & reports compromise

BeyondTrust detects & notifies Okta

Another customer affected notifies Okta

Breach Timeline



?

Initial Compromise
Date Unknown.

9/29

1Password detects &
reports compromise

10/2

BeyondTrust detects
& notifies Okta

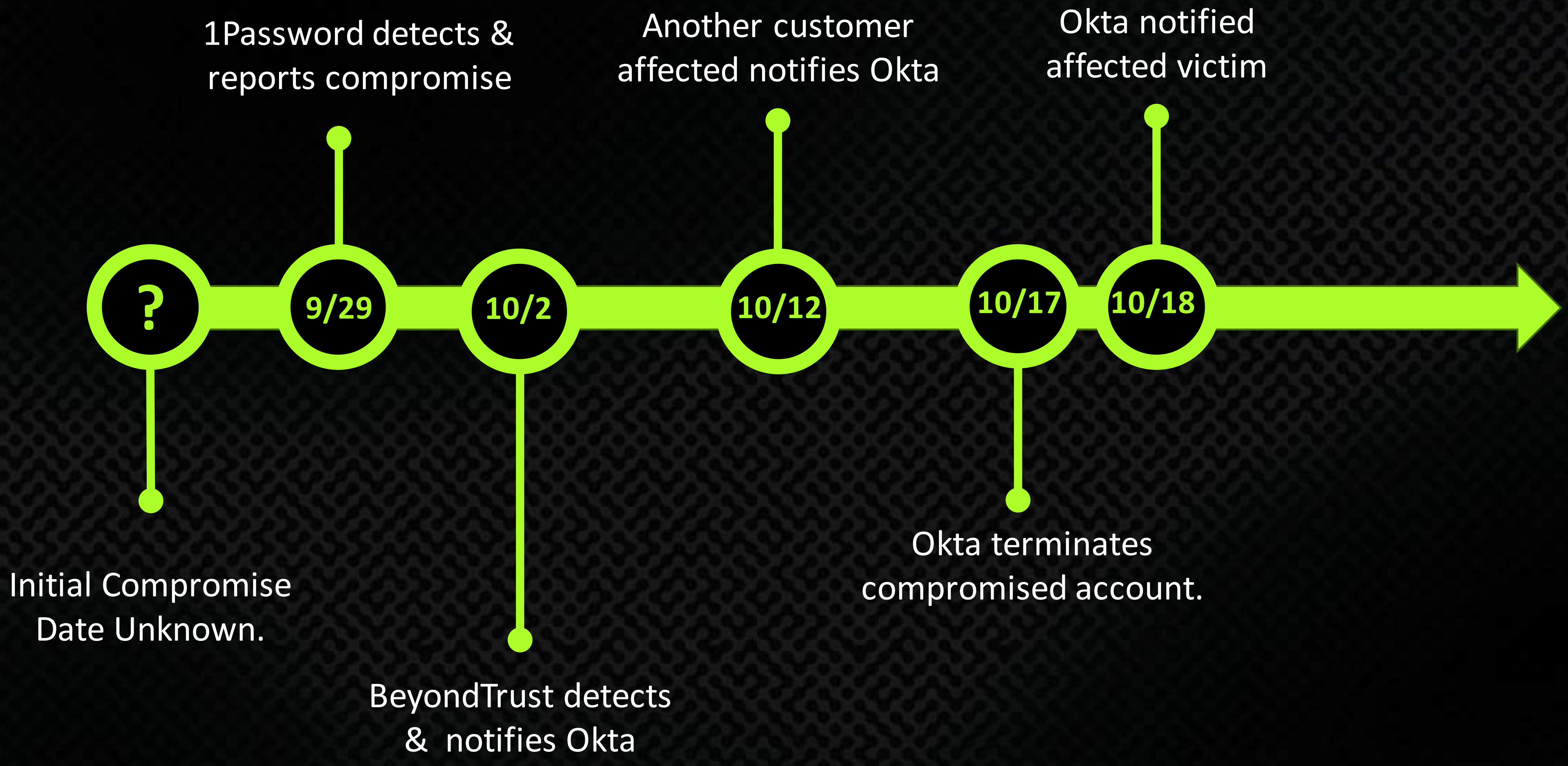
10/12

Another customer
affected notifies Okta

10/17

Okta terminates
compromised account.

Breach Timeline



?

Initial Compromise Date Unknown.

9/29

1Password detects & reports compromise

10/2

BeyondTrust detects & notifies Okta

10/12

Another customer affected notifies Okta

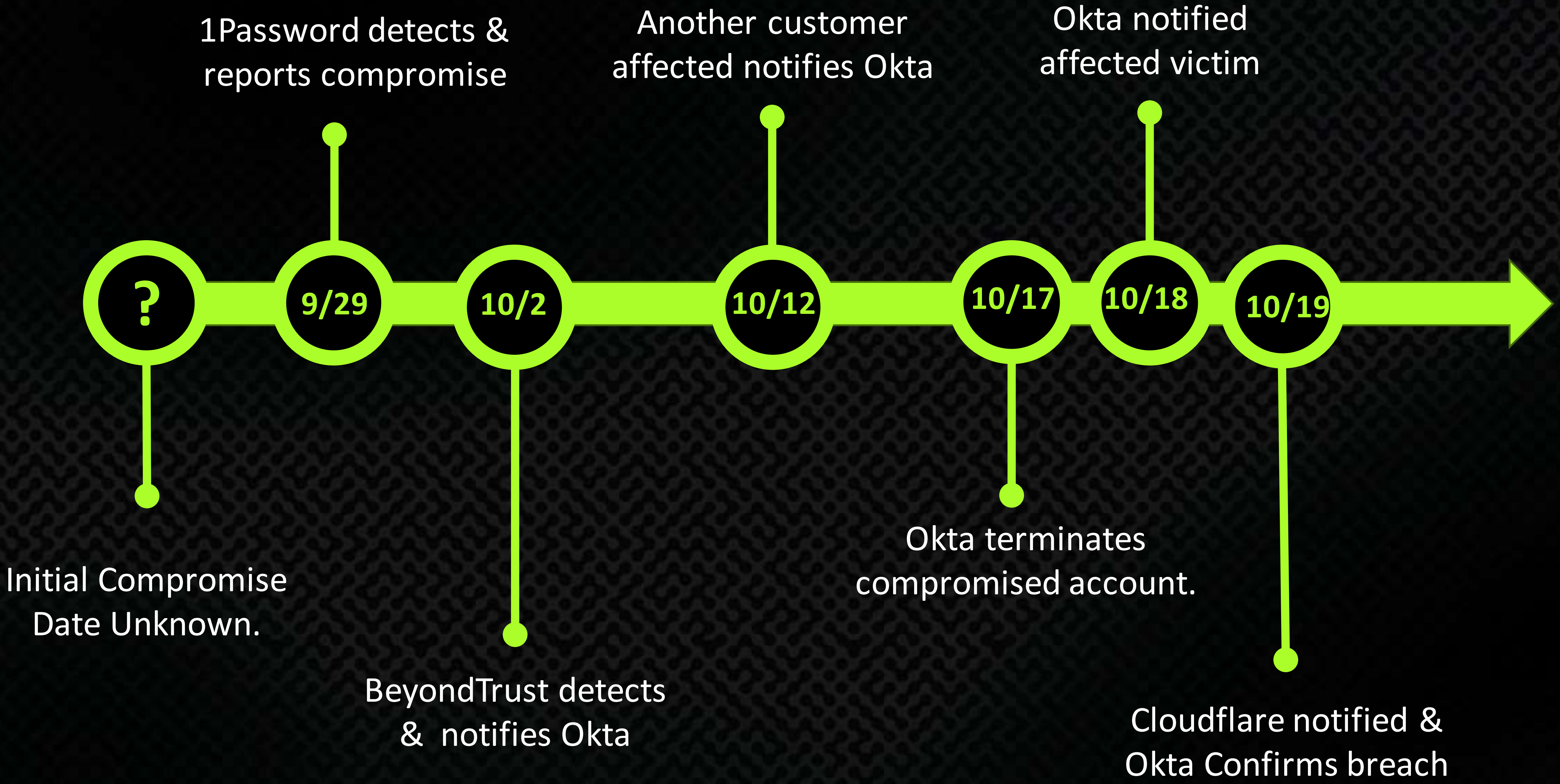
10/17

Okta terminates compromised account.

10/18

Okta notified affected victim

Breach Timeline



?

Initial Compromise
Date Unknown.

9/29

1Password detects &
reports compromise

10/2

BeyondTrust detects
& notifies Okta

10/12

Another customer
affected notifies Okta

10/17

Okta terminates
compromised account.

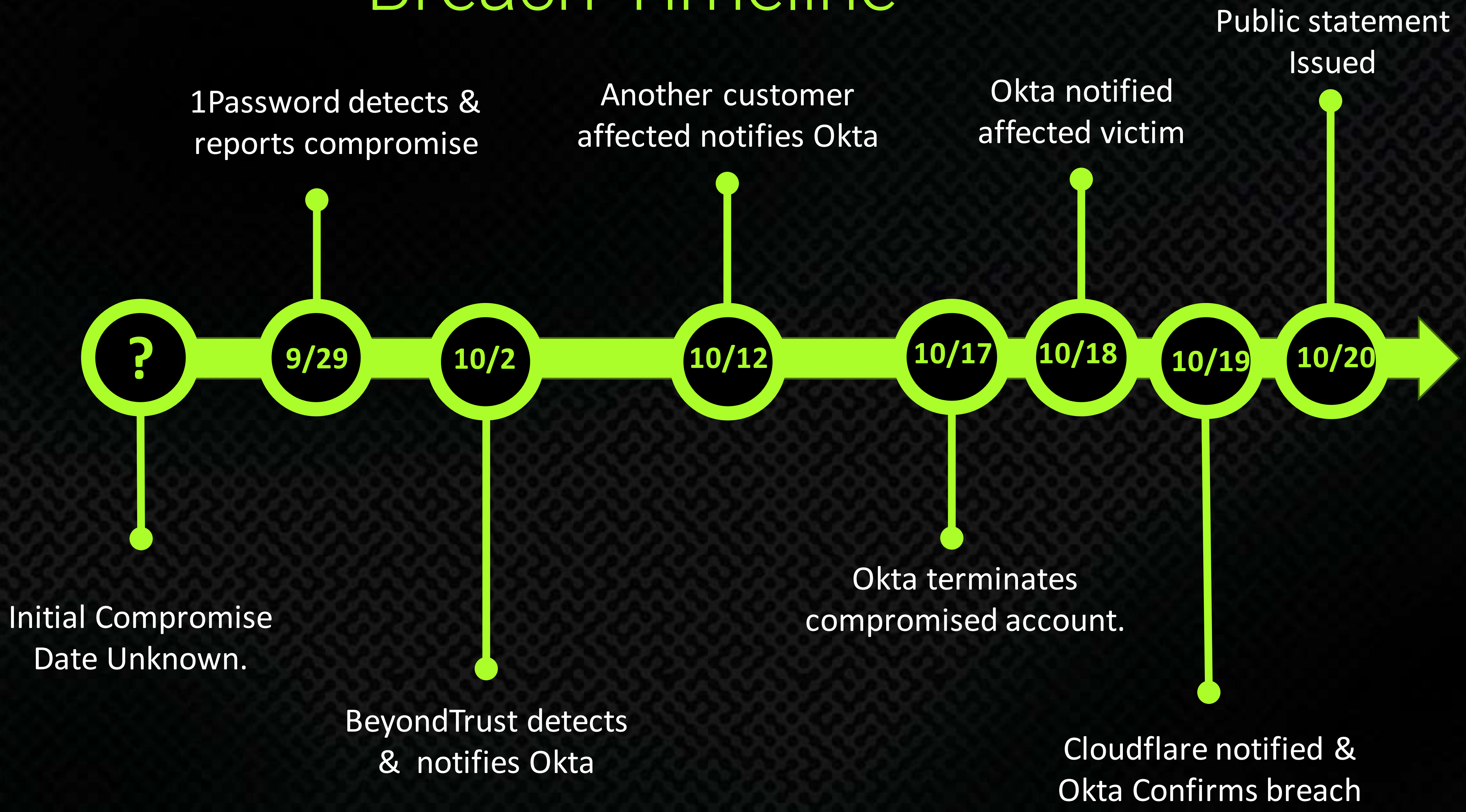
10/18

Okta notified
affected victim

10/19

Cloudflare notified &
Okta Confirms breach

Breach Timeline



? Initial Compromise Date Unknown.

9/29 1Password detects & reports compromise

10/2 BeyondTrust detects & notifies Okta

10/12 Another customer affected notifies Okta

10/17 Okta terminates compromised account.

10/18 Okta notified affected victim

10/19 Cloudflare notified & Okta Confirms breach

10/20 Public statement Issued

Prevention & Mitigation

- Review your ITDR.

Prevention & Mitigation

- Review your ITDR.
- Strengthen MFA policies.

Prevention & Mitigation

- Review your ITDR.
- Strengthen MFA policies.
- Restrict access.

Prevention & Mitigation

- Review your ITDR.
- Strengthen MFA policies.
- Restrict access.
- Harden the OS.

Prevention & Mitigation

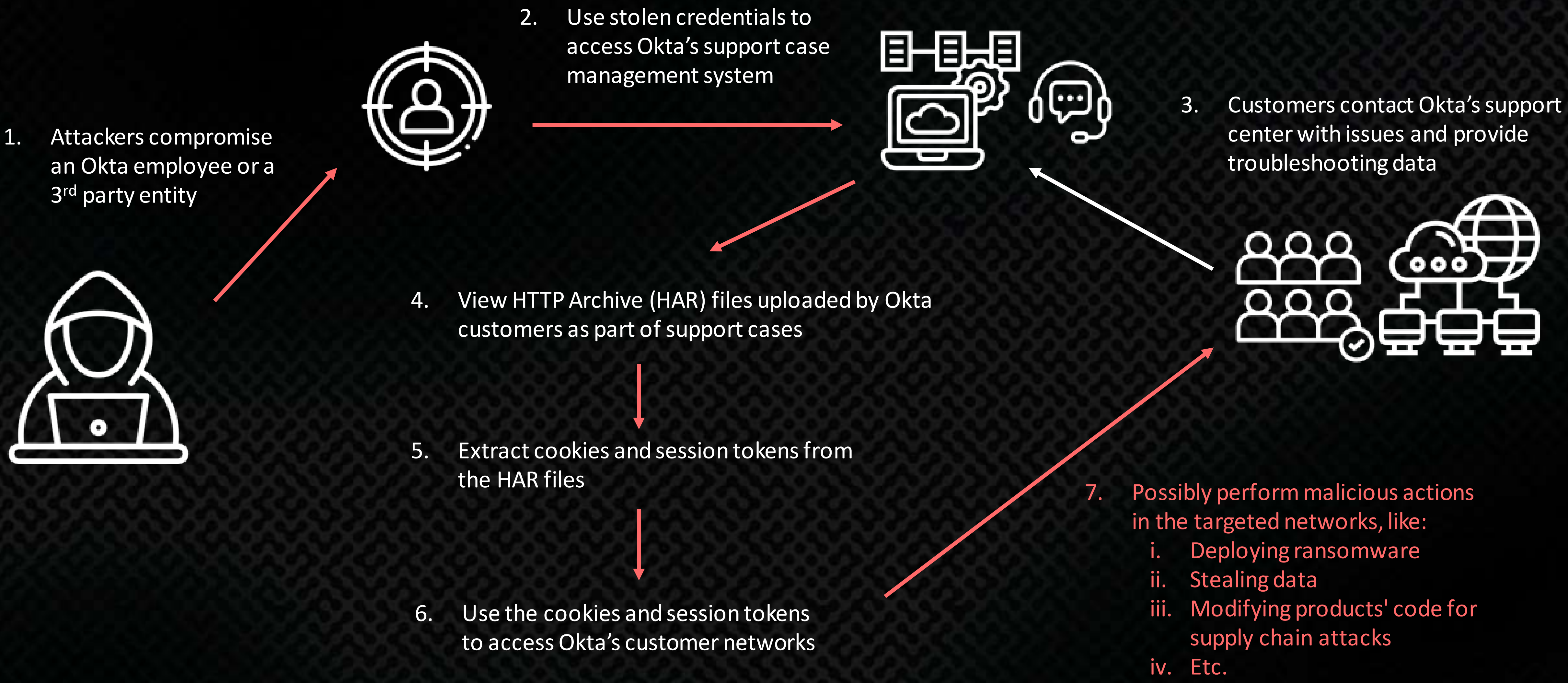
- Review your ITDR
- Strengthen MFA policies
- Restrict access
- Harden the OS
- Sanitize HAR files

Prevention & Mitigation

- Review your ITDR
- Strengthen MFA policies
- Restrict access
- Harden the OS
- Sanitize HAR files
- Secure storage of privileged identities

CyberArk Labs Analysis

Okta Breach Flow (November 2023)



1. Attackers compromise an Okta employee or a 3rd party entity
2. Use stolen credentials to access Okta's support case management system
3. Customers contact Okta's support center with issues and provide troubleshooting data
4. View HTTP Archive (HAR) files uploaded by Okta customers as part of support cases
5. Extract cookies and session tokens from the HAR files
6. Use the cookies and session tokens to access Okta's customer networks
7. Possibly perform malicious actions in the targeted networks, like:
   1. Deploying ransomware
   2. Stealing data
   3. Modifying products' code for supply chain attacks
   4. Etc.

Thank you!