Securing organizations against large scale identity-based attacks

Priti Patil

IAM Analytics Architect

IBM

Jose Rodriguez

Chief Product Architect, IAM

IBM

Identities are being exploited in a majority of attacks ...

84%

Organizations have experienced an identity-related attack in the past year

https://www.idsalliance.org/white-paper/2022-trends-in-securing-digital-identities/

19%

Stolen or compromised credentials are the most common cause of data breach

$4.5 M

Average cost of breaches caused by stolen or compromised credentials

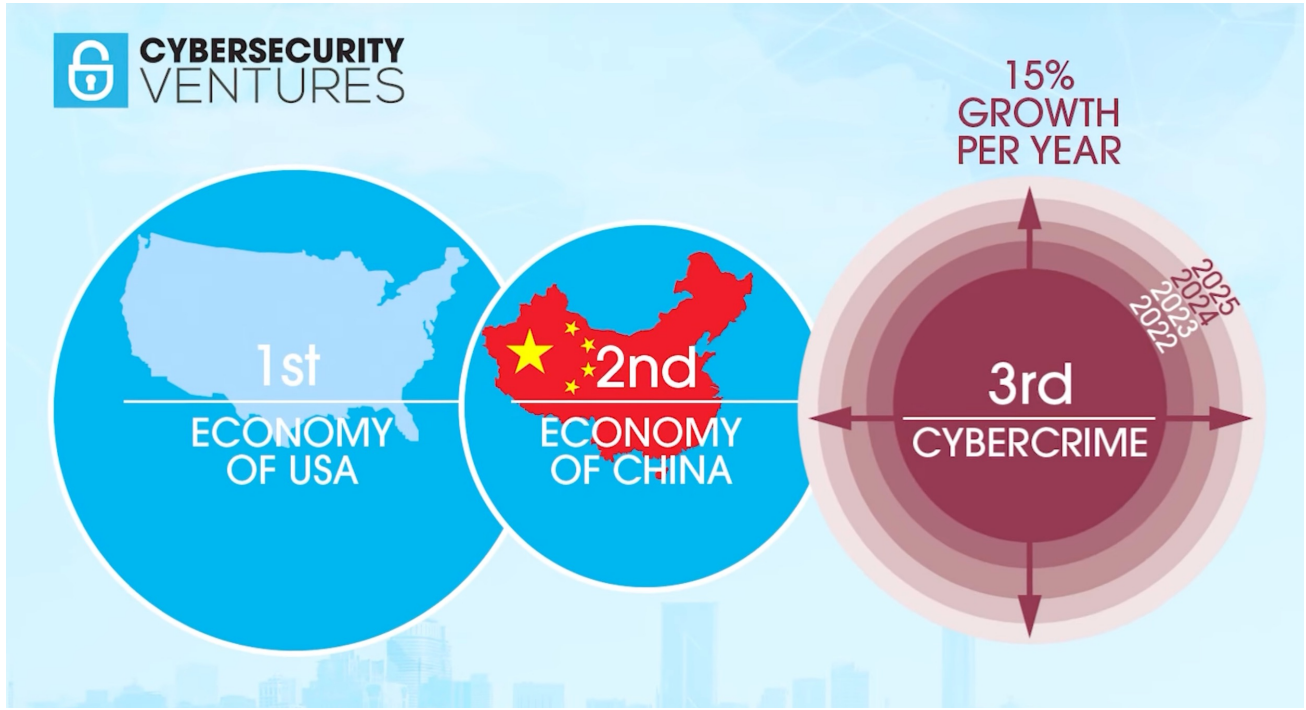
https://www.ibm.com/reports/data-breach

Which is world's third largest economy after US and China?

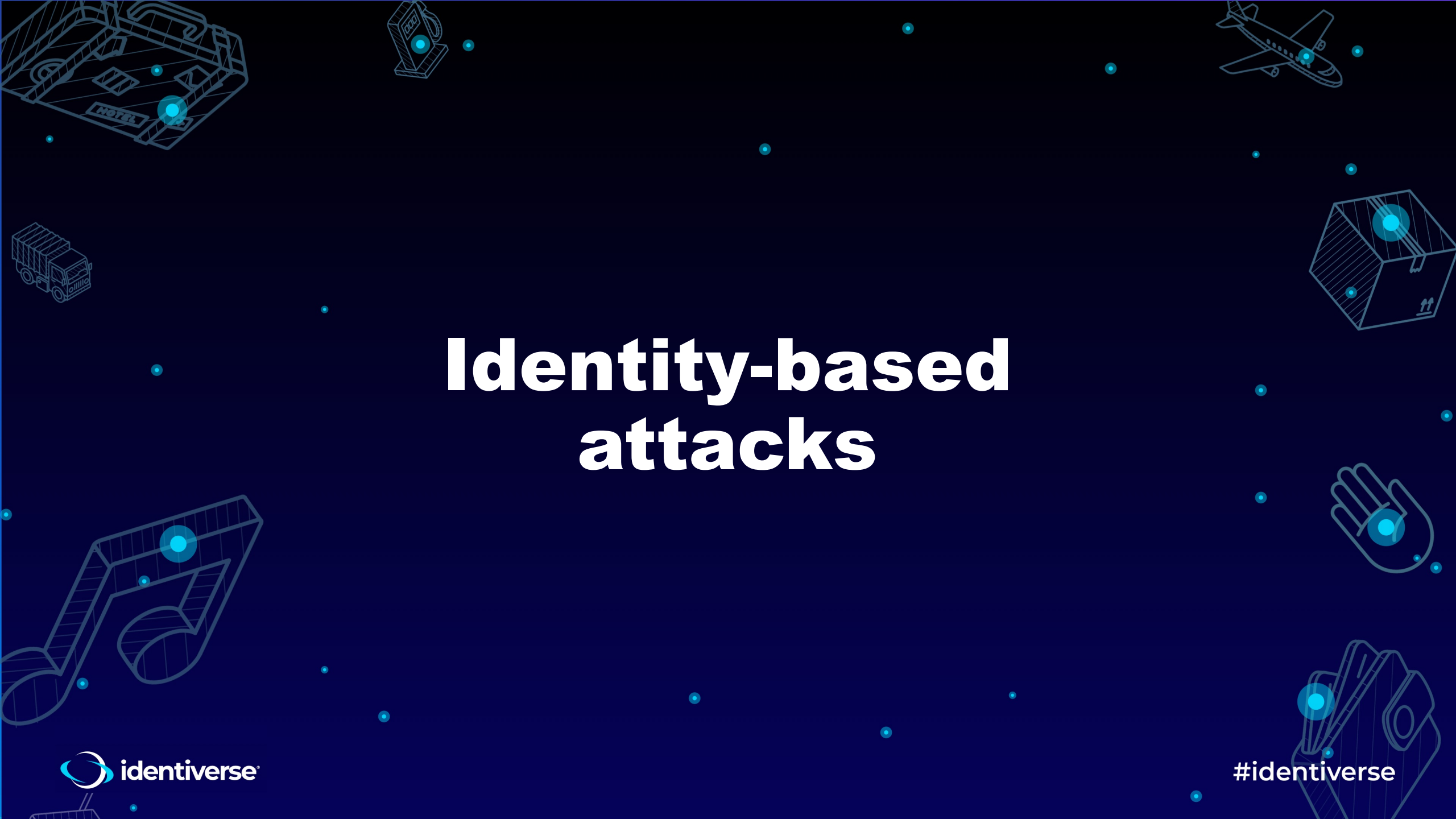
If it were measured as a country, then cybercrime would be the world's third largest economy after the U.S. and China

$8 trillion USD a Year.
$667 billion a Month.
$154 billion a Week.
$21.9 billion a Day.
$913 million an Hour.
$15.2 million a Minute.
$255,000 a Second.

Cybercrime is predicted to cost the world $8 trillion USD in 2023



https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

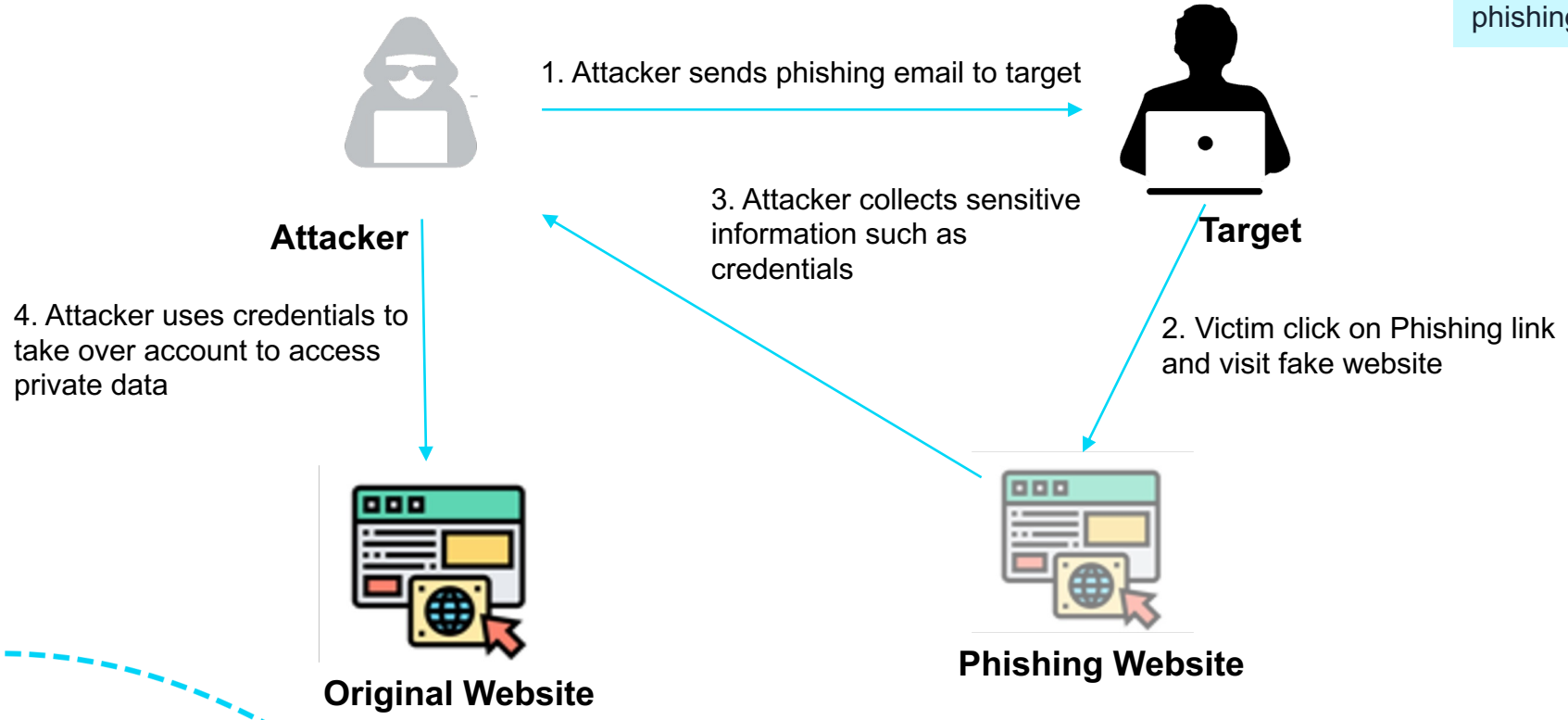


Identity-based attacks

Phishing

41%

Percentage of incidents involving phishing for initial access



Brute Force Attack

In Brute Force Attack, a cyber criminal uses trial and error to try and break into device, network or website.

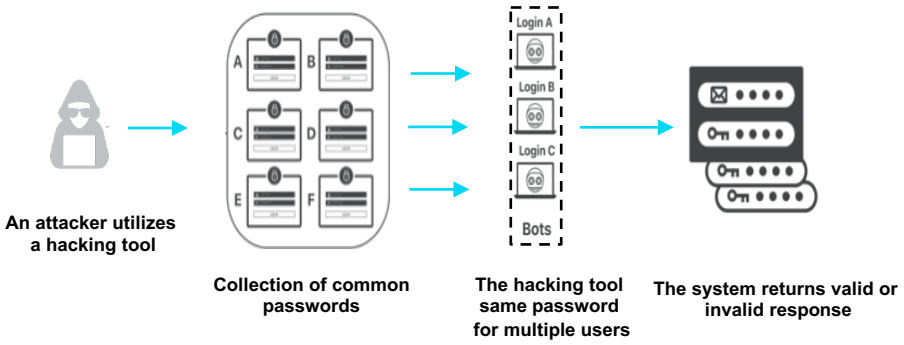
15 B

Stolen credentials from 100,000 Breaches based on dark web audit[1]

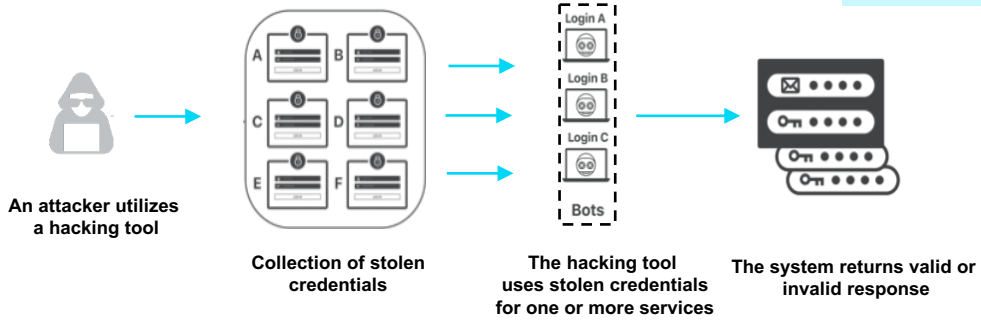
51%

Of people use the same password for work and personal accounts[2]

Password Spray Attack

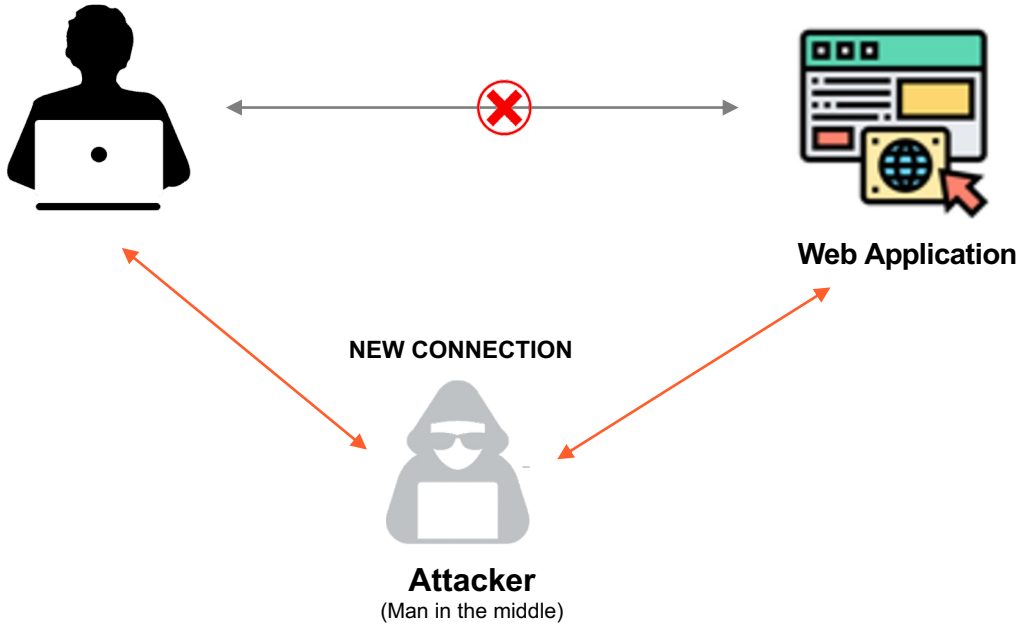


Credential Stuffing Attack



1. https://www.forbes.com/sites/daveywinder/2020/07/08/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime/?sh=34914ea180fb
2. https://dataprot.net/statistics/password-statistics/

Man in the middle attack



35%

of exploitation activity involves man-in-the-middle attacks.

How to secure organizations against Identity-based attacks

What our customers are asking ...

01

Prevention

What are preventive measures against Identity-based attacks?

02

Detection

Can we get visibility into suspicious traffic indicating identity-based attacks?

03

Remediation

How can I take proactive remediation actions to prevent further attack?

Preventive measures are required but not sufficient

	Advantages	Challenges
Single Sign on (SSO)	➢ Reduces password fatigue. ➢ Simplifies username and password management.	➢ Extra-strong passwords must be enforced ➢ If a hacker breaches your identity provider user account, all your linked systems could be open to attack.
Multi-factor Authentication (MFA)	➢ Provides increased security ➢ Reduces impact due to stolen credentials ➢ Addresses regulatory compliance	➢ Increases friction for end user ➢ Hackers can still bypass MFA by exploiting MFA configurations or by triggering MFA Fatigue for a user
Adaptive Multi-Factor Authentication (MFA)	➢ Reduces friction for legitimate users in low risk sessions ➢ Mitigate risk by requesting MFA, or blocking access, when suspicious device or activity is detected	➢ Hackers can still bypass MFA by exploiting MFA configurations or by triggering MFA Fatigue for a user

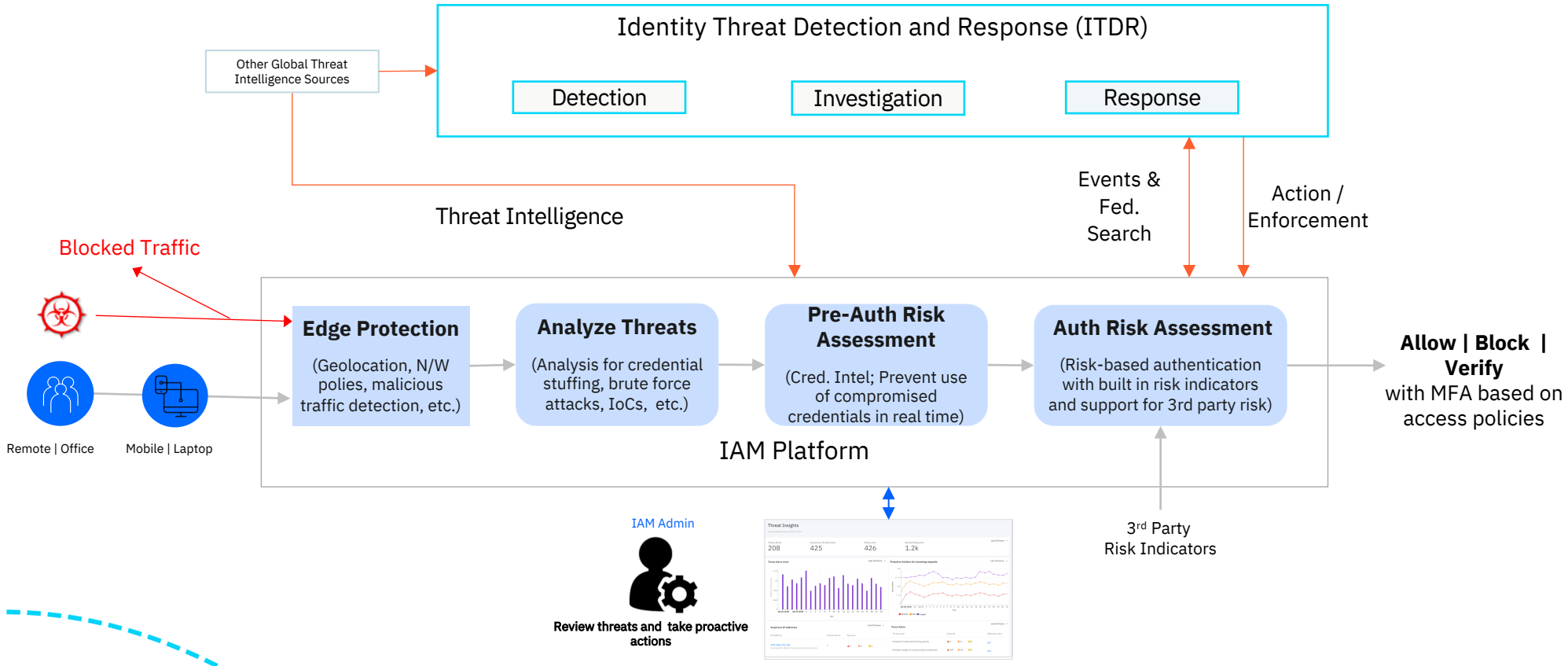
Detection of Identity-based attacks using AI/ML

Indicators of an attack →

Known IoCs	Brute force attack	Credential stuffing attack	Password spray attack	Real time detection of suspicious traffic using ML
✓ Botnet Command and Control Server ✓ Bots ✓ Malware ✓ Scanning IPs	✓ Multiple failed logins from risky IP address ✓ Multiple usage username/password failures.	✓ Multiple usage username/password failures. ✓ Multiple usage of compromised credentials	✓ Same password being used for multiple usernames	✓ ML model based on historical data including attack data to predict if incoming request is suspicious
Apply actionable threat intelligence	**Detect behavior anomalies**	**Credential intelligence**	**Pattern recognition**	**Classification and Deep learning**

Threat detection capability so that customers can get threat events for further investigation. For more details refer to blog.

Proactive remediation of Identity-based attacks

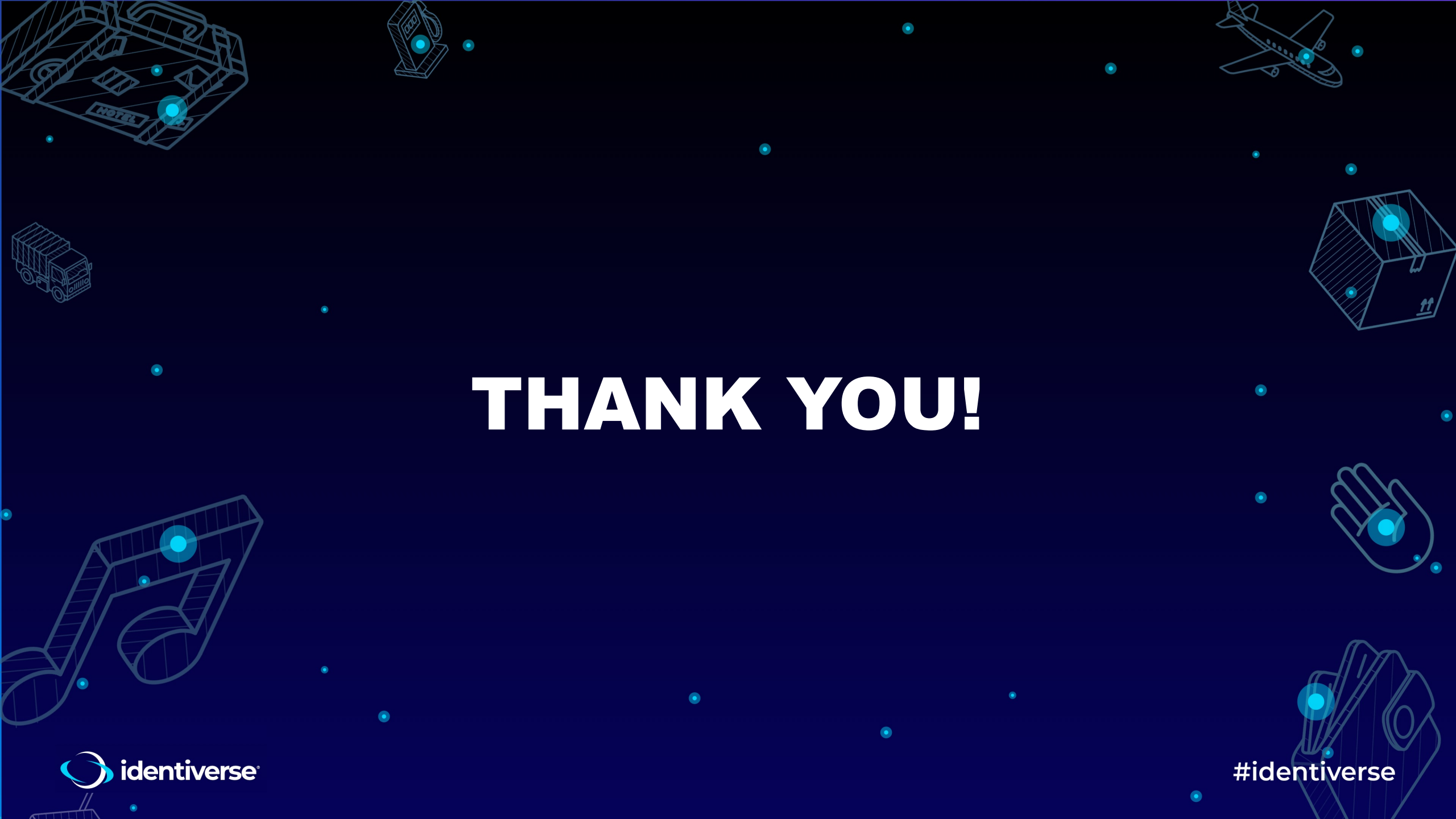


identiverse®

#identiverse

Key takeaways

- Regularly review and update password policies to encourage strong, unique passwords
- Adopt phishing resistant password less technologies like FIDO
- Leverage adaptive authentication and multi-factor authentication (MFA) to secure critical systems and applications
- Detect indicators of an attack in identity tool to detect suspicious traffic to perform real time proactive remediations
- Integrate identity tool with Identity Threat Detection and Response (ITDR) tools by providing threat insights for extended threat detection and response.


THANK YOU!
identiverse
#identiverse