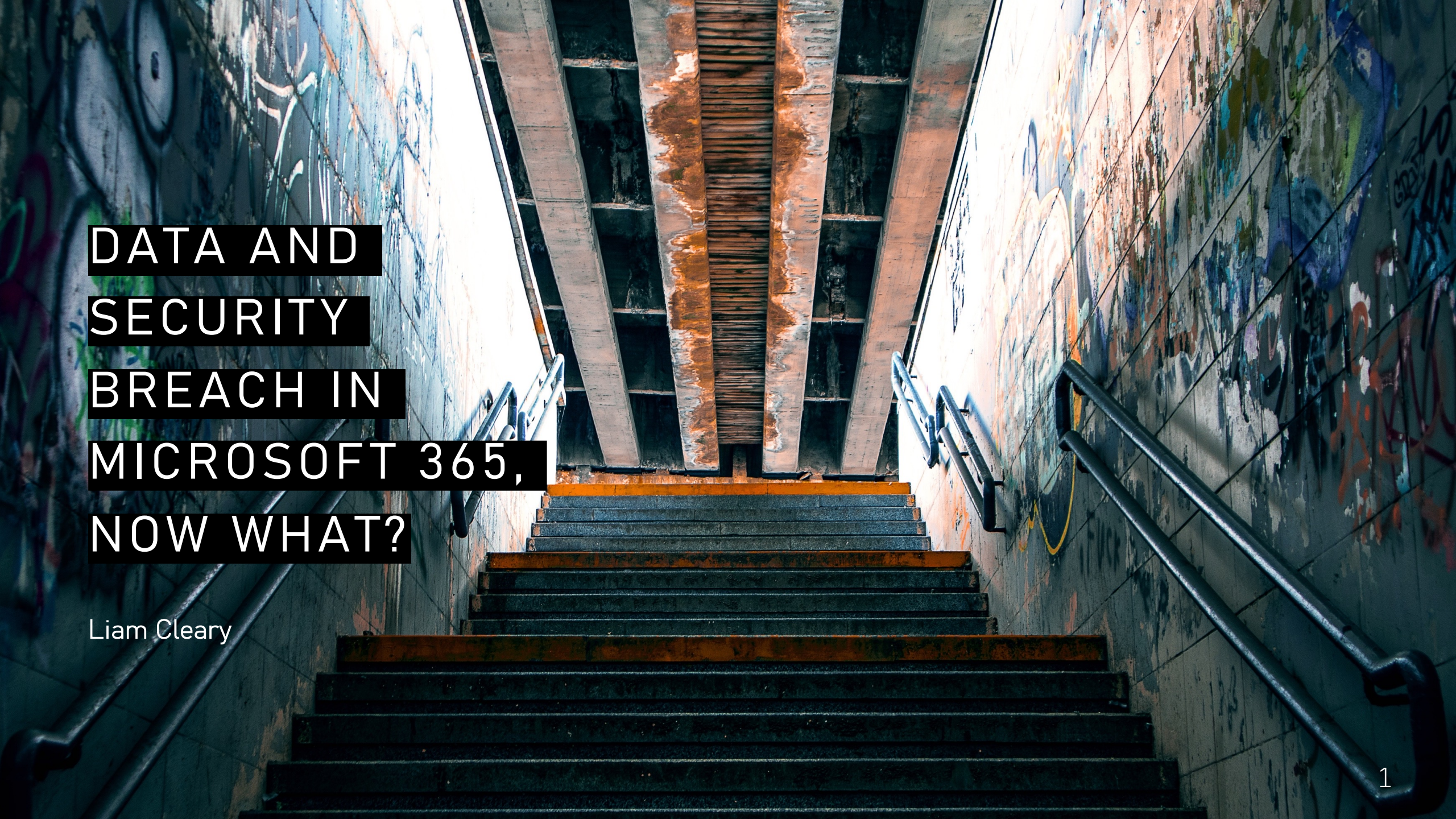


DATA AND SECURITY BREACH IN MICROSOFT 365, NOW WHAT?

Liam Cleary

LIAM CLEARY | CEO @ SHAREPLICITY

MICROSOFT MVP (16 YEARS)
MICROSOFT CERTIFIED TRAINER

FOCUS ON MICROSOFT 365 AND AZURE ARCHITECTURE, SECURITY AND COMPLIANCE, AND DEVELOPMENT

CREATE ONLINE TRAINING COURSES AT PLURALSIGHT, AND LINKEDIN LEARNING, AS WELL AS TEACHING ONLINE CERTIFICATION COURSES

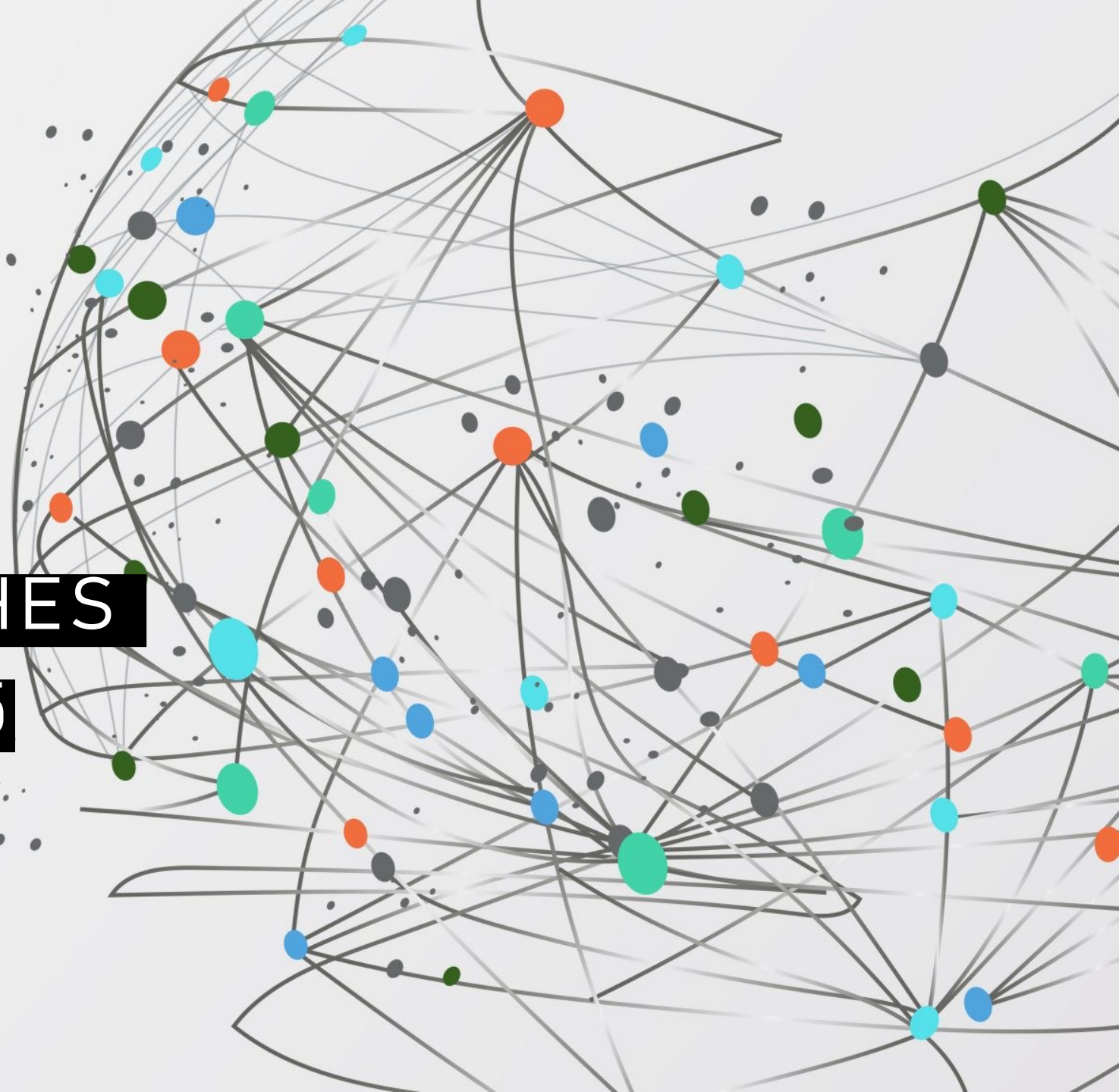
I LIKE TO RUN, MOUNTAIN BIKE, AND I COACH BOYS U12 SOCCER

www.helloitsliam.com www.linkedin.com/in/liamcleary twitter.com/helloitsliam

AGENDA

1. TYPES OF DATA SECURITY BREACHES IN MICROSOFT 365
2. IMPACT OF MICROSOFT 365 DATA SECURITY BREACHES
3. RESPONDING TO A DATA SECURITY BREACH IN MICROSOFT 365
4. PREVENTING DATA SECURITY BREACHES WITHIN MICROSOFT 365

TYPES OF DATA SECURITY BREACHES IN MICROSOFT 365



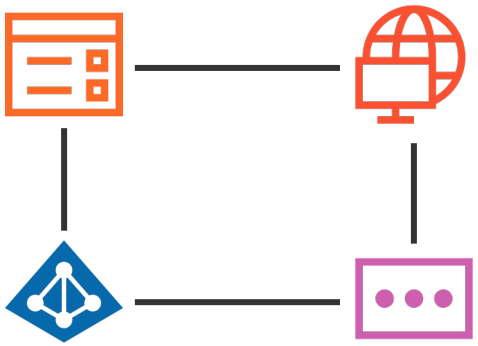
TYPES

- PHISHING ATTACKS
- MALWARE INFECTIONS
- INSIDER THREATS
- MISCONFIGURATION
- PASSWORD ATTACKS
- APPLICATION VULNERABILITIES
- DATA LEAKAGE
- MAN-IN-THE-MIDDLE (MITM) ATTACKS
- ACCOUNT TAKEOVERS

COMMON

PHISHING

LOGIN

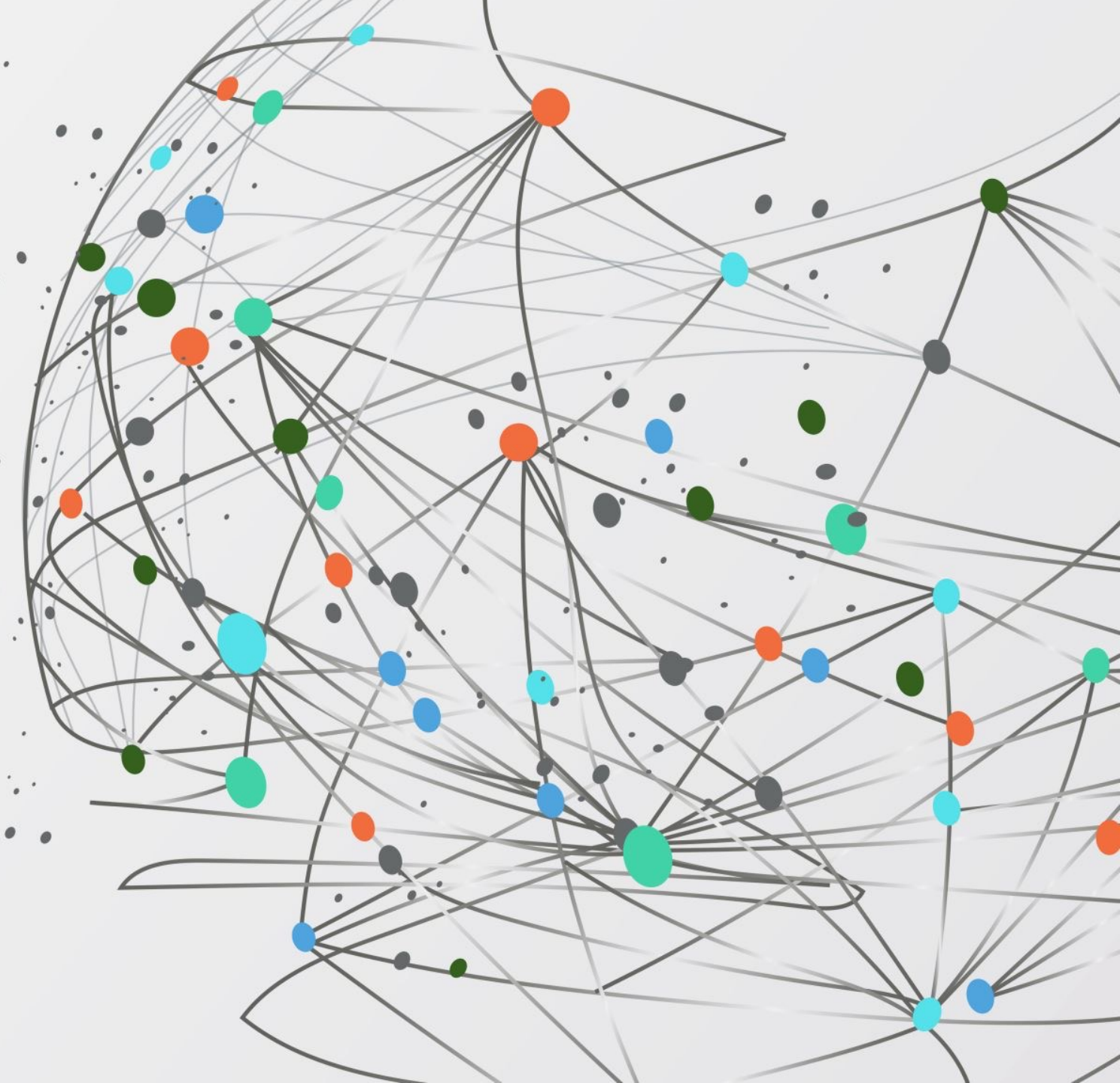


FORWARD

APP

DELETE

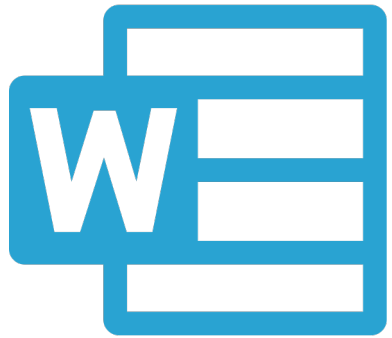
IMPACT OF MICROSOFT 365 DATA SECURITY BREACHES



IMPACT

277 Days

Log in



Microsoft Office

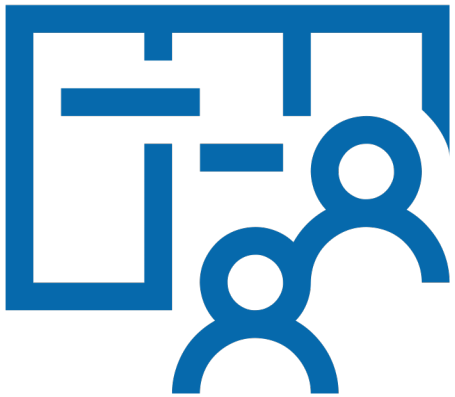
IMPACT

1. FINANCIAL LOSS
2. OPERATIONAL DISRUPTION
3. LOSS OF SENSITIVE INFORMATION
4. REPUTATIONAL DAMAGE
5. LEGAL CONSEQUENCES
6. HIGHER CYBERSECURITY COSTS

RESPONDING TO A DATA SECURITY BREACH IN MICROSOFT 365

RESPONDING

REQUIRES A WELL-COORDINATED AND STRUCTURED APPROACH



UTILIZE AN INCIDENT RESPONSE PLAN (IRP)

RESPONDING

DETECTION AND IDENTIFICATION

CONTAINMENT

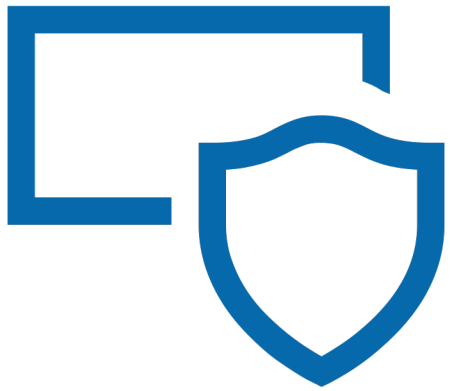
NOTIFICATION AND COMMUNICATION

ASSESSMENT AND INVESTIGATION

REMEDIATION AND RECOVERY

RESPONDING TOOLS

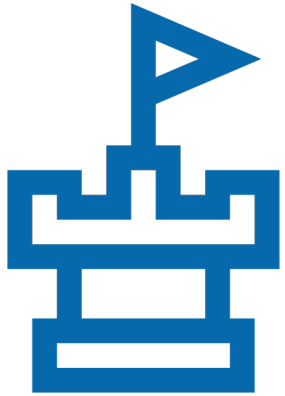
MICROSOFT INCIDENT RESPONSE



MICROSOFT 365 SECURITY CENTER

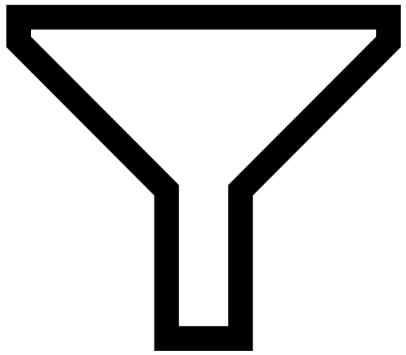
MICROSOFT 365 COMPLIANCE CENTER

MICROSOFT 365 SECURITY CENTER



MICROSOFT DEFENDER

ALERTS



ADVANCED HUNTING

SECURE SCORE

MICROSOFT 365 COMPLIANCE CENTER

Audit Logs

Insider Risk Management

Communication Compliance

Advanced eDiscovery

WHAT TO LOOK FOR?

- UNUSUAL SIGN-IN LOCATIONS
- SIGN-INS FROM UNFAMILIAR DEVICES
- SIGN-INS OUTSIDE WORKING HOURS
- FAILED SIGN-IN ATTEMPTS
- SIGN-INS WITH LEGACY AUTHENTICATION
- IMPOSSIBLE TRAVEL
- PASSWORD RESET EVENTS
- PRIVILEGED ACCOUNT SIGN-INS
- CONDITIONAL ACCESS POLICY BYPASS
- SIGN-INS FROM ANONYMOUS IP ADDRESSES

SEARCHING USER ERROR CODES

```
# Advanced Hunting Query
AADSignInEventsBeta
| where Timestamp > ago(30d)
| where ErrorCode != 0
| where AccountUpn == nestorw@msdx878906.onmicrosoft.com
| summarize UnusualSignInCount = count() by ErrorCode, AccountUpn, Country
```

ERROR CODE CHECKING

YOU CAN USE THE MICROSOFT ERROR PAGE TO EITHER SUBMIT AN ERROR CODE OR PASS IT AS PART OF THE URL.

https://login.microsoftonline.com/error

https://login.microsoftonline.com/error?code=50053

https://learn.microsoft.com/en-us/azure/active-directory/develop/reference-error-codes#aadsts-error-codes

DEMO

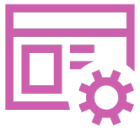
QUERYING MICROSOFT 365

PREVENTING DATA SECURITY BREACHES WITHIN MICROSOFT 365

PREVENTION

MULTI-FACTOR AUTHENTICATION (MFA) POLICY

DATA LOSS PREVENTION (DLP) POLICY



CONDITIONAL ACCESS POLICY

RETENTION POLICY

ANTI-PHISHING POLICY

ADVANCED PREVENTION

MICROSOFT DEFENDER
FOR OFFICE 365

MICROSOFT DEFENDER
FOR IDENTITY

PRIVILEGED IDENTITY
MANAGEMENT (PIM)

POLICIES

REQUIRE MULTIFACTOR AUTHENTICATION (MFA)

ENABLE SAFE LINKS PROTECTION

ENABLE SAFE ATTACHMENTS

ENABLE COMMON ATTACHMENTS FILTER

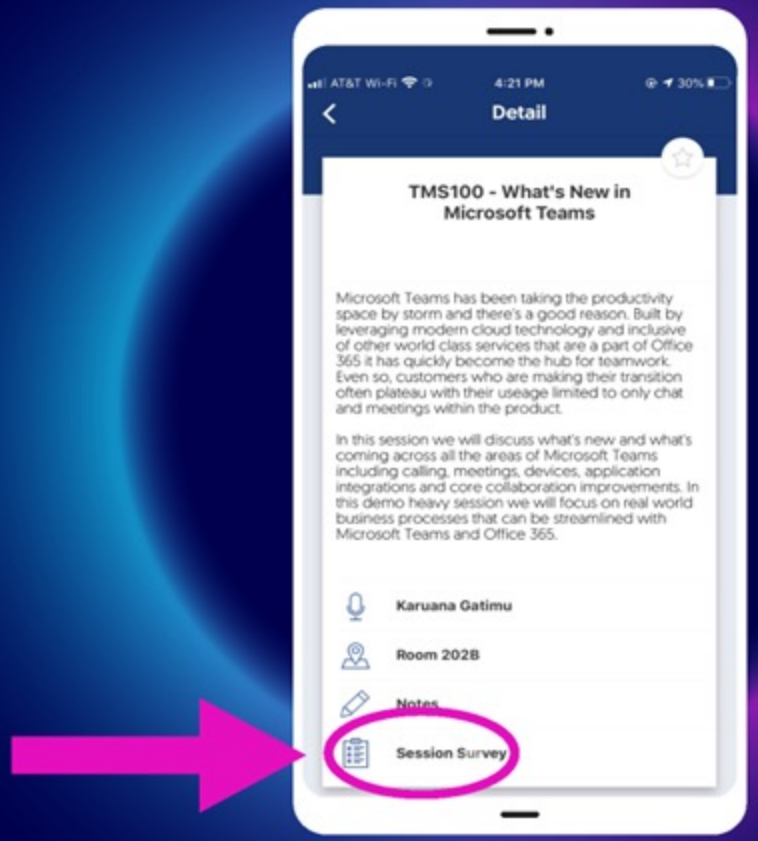
BLOCK GRANT CONSENT TO APPLICATIONS

ENABLE IMPERSONATION PROTECTION

CONCLUSION

CONCLUSION

1. ASSUMED BREACH
2. IMPLEMENT BASE ACCOUNT PROTECTIONS
3. UTILIZE CONDITIONAL ACCESS CONTROLS
4. ENABLE LOGGING (LOG ANALYTICS)
5. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)



How was the session?

Search for **365 EduCon** in the App Store or Google Play

Fill out the Session Surveys in the **365 EduCon App** and be eligible to win **PRIZES!**

365 EduCon
Microsoft 365 Conference

LIAM CLEARY

www.helloitsliam.com

www.linkedin.com/in/liamcleary

twitter.com/helloitsliam