Biotech Startup Research Data Leak Investigation Report

1. Overview

On September 12, 2025, BioNext found a leak of confidential genetic research data. The investigation revealed combined insider misconduct and external hacking.

2. Incident Summary

- 07:30 UTC: Abnormal database queries detected.
- 08:10 UTC: Employee login from foreign IP.
- 09:00 UTC: Files copied to unauthorized cloud.
- 11:20 UTC: Breach confirmed, network isolated.

3. Root Cause

A staff member shared credentials with a hacker group, allowing internal exfiltration and external intrusion.

4. Impact

Exposure of key gene editing data, ~USD 5 million loss, potential regulatory penalties, reputation damage.

5. Measures

Revoke and reset credentials, enforce MFA, deploy continuous anomaly detection, perform insider risk audits, and strengthen security training.

6. Key Investigation Data

Item	Detail	Time	Note
Initial Detection	Abnormal database query	07:30 UTC	Alert triggered
Compromised Login	Foreign IP access	08:10 UTC	Credential misuse
Data Exfiltration	Unauthorized cloud upload	09:00 UTC	Core files copied
Containment	Network isolation	11:20 UTC	Leak stopped

o ¥ w / p o 9 Š < • î ò T µ , ‰ m

1.
2025 ï 9 " 12 Ã ¥ BioNext $ 8 ð • Ž @ š ó ÷ X Ê ¹ ‡ ê å , ‡ } · < ¾ . ‡
é £ L + ® Ê

2. E O 3
- 07:30 UTC: Ú ; • ' ß š ó ‡ ™ Ê
- 08:10 UTC: } · - O . IP ' ß E Ê
- 09:00 UTC: ž E ÿ * • • 0 ü < h Ê
- 11:20 UTC: µ ` ÷ X ð # § L Ê

3. •
´ M } · Q é • q ÷ X x Å X z ¥ + ® , ‡ . ÷ ¾ . ‡ £ ð Þ Ê

4. S »
¦ t ð • • á š ó X ¥ ì < 500 · ¼ ¥ H d × « (¬ ¾ # U ' ì Ê

5. ´
a V ð Õ ³ X z ¥ ´ 0 • ` z ¥ Ä [' ß Ú ; ¥ m Þ , ‡ °] ¥ ¨ ? } · ô ï
h Ê

6. ž ¶ 1 4 Ž

¸!	~	» ®	Î Õ
"Î ¨ t Z	Đ 9 Ž Ý 4	07:30 UTC	%U t%p ’
Đ 9 ×	IP ó ¬	08:10 UTC	i þ •"ø
Ž Ï	@ I ¿ ä ß	09:00 UTC	ž ¶ ¬ õ Ï Ž
i Ž ~	{ E Ý	11:20 UTC	(& Ï&7

ò õ å, ůy ËËð þ Èçí åø ÛâÚâöð åy

1. C > y A

12 • C 3 ë 2025 $ BioNext 7 & 8 7 =7 @ y • A $ C y 6 07 .$ | > C 8@ = + y) C y 3 | > $ $ < ') >$ [C y • ? ¸ 3 > : D >D-$]& 5 7 0 < 7 `‹

2. '. 7 C >

- 07:30 UTC: C < ¯ 0 . : úC > $ 8 3)? ‹
- 08:10 UTC: $ < ') >$ ~ @ 5IPAC ? # € & 7 ‹
- 09:00 UTC: N ? g 7 • 6 $ 3ù 0 8 >$ # 8 ‹
- 11:20 UTC: y ' 7 $ [8 ƒ, +7 . @ $? & ~ $ = & = ‹

3. $ > 2

$ A 6$ < ') >7 D $ < Þ ? # € & 7 7 $ >5, • + C C y 3 | > $ | > C @ : D > ' C 8 w ‹

4. © ; @

< D w 8 2 ' 7 C y 8 507 . + & ? & ; & 5 • < • ? = 70 # ? $ [F • 3 C y ; ~ @73 = < $ + < ', 7© • 3 / D • 7 ‹

5. 8 =

C ; • 0 g • A > ? > > C $ > g w $ > $ © < 2 $ > 2 & $ > g C 3 3 C < ¯ 3 8 D) ,7 y 3 | > $ + ƒ % < | 0 . , C > F © • A F 2 M z ‹

6. O Ñ ¿ ¹ [½ Ä Â

ñ ò Â Ñ	Ø Ø Ó Æ	Û Ñ Ò	Â “ Í Æ
O Ć Ð ¸ Í Ç	ð Û Ñ Ä Â ï Ê € Ø Ó	07:30 UTC	ð Õ Â^
Û Ñ À Õ “ º Ë	Ø É Ê IP Û $ t ¢	08:10 UTC	O Ñ É Æ Í Òº
Ä Â Ó Û Ø	ð Ë “ Ê ¸ Ł Ç õ Ä ð Í Õ Ä	09:00 UTC	Ñ J • ã Ò ò Õ Ţ Í
‘ Ë Ò 7 Æ	Ë Â Ø ¸ ^ð Õ º Ø	11:20 UTC	Ó Û Ó Ø ¸

Informe de investigación de fuga de datos de investigación Ñ BioNext

1. Resumen

El 12 de septiembre de 2025 BioNext detectó fuga de datos genéticos confidenciales. La investigación reveló complicidad interna y ataque externo.

2. Resumen del incidente

- 07:30 UTC: Consultas anormales en base de datos detectadas.
- 08:10 UTC: Inicio de sesión desde IP extranjera inusual.
- 09:00 UTC: Copia de archivos en nube no autorizada.
- 11:20 UTC: Fuga confirmada, red aislada.

3. Causa

Un empleado compartió credenciales con un grupo de hackers, permitiendo extracción de datos y acceso externo.

4. Impacto

Exposición de datos de edición genética, pérdidas de ~5 millones USD, posibles sanciones y daño reputacional.

5. Medidas

Revocar y cambiar credenciales, aplicar MFA, implementar detección continua de anomalías, auditoría interna y capacitación de seguridad.

6. Datos clave

Elemento	Detalle	Hora	Nota
Detección inicial	Consulta anormal en base de datos	07:30 UTC	Alerta
Inicio de sesión comprometido	Acceso desde IP extranjera	08:10 UTC	Mal uso de credenciales
Exfiltración de datos	Carga a nube no autorizada	09:00 UTC	Archivos críticos copiados
Contención	Aislamiento de red	11:20 UTC	Fuga detenida

5 D S S R U W G ª H Q T X r W H V X U X ¶ H I X L W H
BioNext

1 t í œ ˜ O œ Æ à œ Å ‘ ¿ œ

Le 12 septembre 2025, BioNext a dé couvert une fuite de donné es § • Æ • è ¯ Û í œ à ’ Í Æ ¦ ¯ ˜ œ Æ è ¯ œ ¿ ¿ œ à 1 > O œ Æ Û í è œ „ Ü • ø • ¿ • í Æ œ ’ Í Å Ù ¿ et une intrusion externe.

1 Z • à í Å • ˜ œ ¿ O ¯ Æ ’ ¯ ˜ œ Æ è

- 07:30 UTC : Requê tes de base de donné es anormales dé tecté es.
- * i d * Í Æ Æ œ þ ¯ Í Æ ˜ O í Æ œ Å Ù ¿ Í ÿ • ˜ œ Ù í ¯ à í Æ œ / W • è Ü „ Æ § £ Ü œ inhabituelle.
- 09:00 UTC : Copie de fichiers vers un cloud non autorisé .
- 11:20 UTC : Fuite confirmé e, ré seau isolé .

3. Cause

Un employé a partagé ses identifiants avec un groupe de pirates, permettant extraction interne et intrusion externe.

4. Impact

þ Ù Í à ¯ è ¯ Í Æ ˜ œ ˜ Í Æ Æ • œ à ˜ O • ˜ ¯ è ¯ Í Æ § • Æ • è ¯ Û í œ + Ù œ Ü è œ à œ à è ¯ Å • risques de sanctions et atteinte à la ré putation.

5. Mesures

Ré voquer et renouveler les identifiants, appliquer MFA, dé tection continue des anomalies, audit interne, formation sé curité renforcé e.

6. Données clés

É lément	Détail	Heure	Remarque
Détection initiale	Requête anormale en base de données	07:30 UTC	Alerte
Connexion compromise	Accès depuis IP étrangère	08:10 UTC	Identifiants abusés
Exfiltration de données	Envoi vers cloud non autorisé	09:00 UTC	Fichiers copiés
Confinement	Isolement du réseau	11:20 UTC	Fuite stoppée

ß Ä í ÖÛÇÄ GÓÄøXÿÖW - X . í Þø Y ø³ BÞoNext

1. î T » Ž µ ó

× Ž ¡ l Ã Ÿ m × S 2025 Ž e í m e › 12 Ä BioNext Ž ú ¶ W Ž › r S • k T ó T f c Ž ™ n T Ã z • T † Ã y û T Ã ã † S $ Ã ² S n Ð Ñ • m è S

2. o ‡ T • è S ¤ … ã î

- 07:30 UTC: k T ó T e è S ˆ » T Ò Ä ¹ e ² Ž À k T î) ¹ m › S Á T Ÿ m × S
- 08:10 UTC: ñ î á † ‡ â y ™ n IP ‡ T m ¹ î Ž À e ò z W
- 09:00 UTC: T ú f • Ž ¥ î Ž À f T • › è Y k T Ã ã î „ ™ ó
- 11:20 UTC: Õ e Ÿ è S á ‘ » c Ž ™ m è S × X n

3. d e ™ è S

ã † S ‡ w S • … m › T € í › T î ò § S • Ò » í y î ¸ î á † ˆ è S k T ó T f Â ¶ î Ó • T ¡ z • T † â ã ™ n

4. Ž r * S

k T î S • À á T í m ‚ S • (‡ ñ) î 5 c • T Ñ n Ž T ™ † ò z â ˆ ¹ n k T ó T f Â Ÿ × ¹ í › ð S ˆ Ñ Ä

5. Ž f S ˆ m è S

‰ Š ¡ Â Ÿ × â î S ¹ è S ‡ ˆ ¹ m î Ò ‡ T ¥ î Ð e ± n á † ˆ è S k T ó T f Ž ¾ n R T ¿ è Y ñ Ã ¶ í ã è ò î W d • ˆ n ã † S ‡ Ž ² T … î Ð Ò ˆ n Ž í m ™ î

6. { À • w • þ w · w À y

‹ ¸ z ± û	° À – w © ~ ± û	‖ « ¼ ± û	{ † È ´
¾ ± Ãw û ” ~ ® Ç û	þ w · w ýÀ ¢ y w ‹ È £ ~ • û ¾ £ À z À e ¥	07:30 UTC	¹ À z ¸ }
• ~ Š ´ ¼ ‰ ° À „ ‘ }	¶ ´ ¼ – IP ¾ z ¸ ƒ ÷	08:10 UTC	þ w · w À ¢ y Š ~ • õ û ¼ • ¼ ‰ ‹ ± û
þ w · w ù À • z } ‡ û	• À ¥ y w ‡ ½ ± ° ù À µ ‡ } w » y — ´	09:00 UTC	{ • w ‘ † þ w © ² ˆ ‘ ·
õ û ¼ ~ † Ç û	{ ¯ z ” ± ú Ž ¢	11:20 UTC	ü • ‘ ~ ± û w ¬ ¿ ù