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*

٦ ۇ ξ ν ̔ ̂ ̂ ̂ ̂ p ɨ بخ کЧɵ

1.
2025 ᾰ 9 مج 12 بنæBioNext ǀ ثم ˘ ┌ Ὠ سكل ¨ يي شج ɫ Ẑ ᴎ ɟ Ѝ ₲
ɔ ק ӳ ′ ṟ ´ ¨

2. я Ҕ ئا
- 07:30 UTC: تجى ẟ ̋ ܠ سكل ȕ شج ¨
- 08:10 UTC: Ẑ ᴎ Ѽ ₲ IP ̋ ܠ Ա ¨
- 09:00 UTC: لج Ҕ ₮ ᵡ ẟ شمصيم є ¨
- 11:20 UTC: ᾰ ¨

3. Ḥ Ὠ
Ґ Ṡ Ẑ ᴎ Š ɔ Ὠ ǀ ᴸ æ´ ɫ ₲ Ѝ ₲ ק ӳ ᾰ ¨

4. Ч ő
شخ զ ┌ Ὠ عمسكل æ ذ ɟ 500 ǀ Ʊ æ بٍ Ц € Ѝ ₧ Ḻ ذ ¨

5. غ يج
ئم ᾰ ᴸ æ Ʊ يج ₴ Ὠ æ ḯ ̋ ܠ تجى æ چ ɫ ך æ ꝑ ` Ẑ ᴎ שׂ ך…
¨

6.

		07:30 UTC	
	IP	08:10 UTC	
	ني لجبَ	09:00 UTC	تجبَ
تجبَ		11:20 UTC	

Ȯşȳɋȣ ȣŷş Ȣ Ȯ ȉȎ ȁȎ ȥ ȿ ʔ ş ȵ Ȟ ȡȴȮȣw

1. ` 2 [2 ^

12 ˈ ` P ę [ 2025 A= BioNext T;C=UT4Z " T5 ˈ ^ A ! T5 S2T MK2 A2 "[ ` 2] U2Z2É H2F ` ; " P"[ A A YĐ2 [4 AB ` ˈ \ HuP2 . [W2a [4 a A C R=T ` 2Y T; " É

2. DKT2 ` 2[

- 07:30 UTC: ! ` 2Y2 ō MK2W; ` κ [4 A2 UP2 F \ 2É
- 08:10 UTC: A YĐ2 [4 A2 '] R;^4 IP ` ; \ @' C TÉ
- 09:00 UTC: k 2# \ T ' S A7P ķ 2%M U [A @U4É
- 11:20 UTC: % ɐ DT AB U5 ι , TK] AĐ! \ C ' A Z2 CZ2É

3. A2[O

+A ^=S A YĐ2 [4 T;a A [` Y A= \ @' C T H2T A2 [4 R4, ' H ` ` ; " P"[ A "[ ` 2] . [W2a [4 D5 U $É

4. ç X2]

Ya Ƶ U6ĐH4T ` U2RT MK2 %H2C [, \ C X C 5 ' Y ' \ Z T M@ \ [ AB c ' P, ` X2'] P ' T Z2Y A H5Y2Đ2, ç ' P ɭ 2 a2' TÉ

5. %U2Z

` X4 Ó MdZ Z \ [ I . [ [4 ` K A [W - A2 [A ç Y2O4 A [O \ 2C6A [PP ! ` 2Y2 ō P2 UaF2T, " P"[ A H= B Y 1 "MK, ` 5c2 ç ' ^ c O W j 2+É

6. ʍôĦ æŅÂĂŅ

ɨ ÌÀô	ņÛÛȑȆ	ṣôȒ	ŞÀ ȋ Ȅ
ʍŅȑŒǶ ȋèŅ	ɭ ṣŅôŅ Ȓ ÂĂŅòȘ ' ÛŤ	07:30 UTC	ɭ ȓ Àά
ṣôǾȒèŅ ȓ ǑǑÑȉ	ņÛêŨ IP ṣП ȷ Ấ	08:10 UTC	ʍôŅȄ êĦȋ ȒǑÑ
ÂĂŅŚȓ ṣŅÛ	ɭ ȉǑȊĦè ɳ ŅijÂ ɭ ȋ ȓ ǑÂ	09:00 UTC	ôĤȒ ȡŅİ ȓ ĦǑȋ
ĬȉȒǾȄ	ȉĂÛĦά ɭ ȓ ÑŅÛ	11:20 UTC	Śȓ ṣŅÛ ȓǑĦŅ

Informe de investigación de fuga de datos de investigación d' 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

Rapport dèenqu°te sur une fuite de donn®es de recherche ã BioNext

Ő ů ² ī Ú ÖϙÚĄĞÚ ă ÏýÚ

Le 12 septembre 2025, BioNext a découvert une fuite de données åÛĄÛĦíę ī ÚĞ ĐċĄäíÖÚĄĦíÚýýÚĞů [ϙÚĄę ī ÞĦÚ Â ĚÛĶÛýÛ ī ĄÚ Đċ ă ėýíĐíĦÛ íĄĦÚĚĄÚ et une intrusion externe.

őů wÛĞ ī ă Û ÖÚ ýϙíĄĐíÖÚĄĦ

- 07:30 UTC : Requêtes de base de données anormales détectées.
- ő ŗÛŐő § ¢ / Ů / ċĄĄÚ ļ íċĄ ÖϙīĄ Ú ă ėýċĽÛ ÖÚė ī íĞ ī ĄÚ Lt ÛĦĚÂĄåáĚÚ inhabituelle.
- 09:00 UTC : Copie de fichiers vers un cloud non autorisé.
- 11:20 UTC : Fuite confirmée, réseau isolé.

3. Cause

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

4. Impact

9 ļ ėċĞíĦíċĄ ÖÚ ÖċĄĄÛÚĞ ÖϙÛÖíĦíċĄ åÛĄÛĦíę ī Úũ ėÚĚĦÚĞ ÚĞĦí ă ÛÚĞ Ç Ŕ a § { 5ũ risques de sanctions et atteinte à la réputation.

5. Mesures

Révoquer et renouveler les identifiants, appliquer MFA, détection continue des anomalies, audit interne, formation sécurité renforcée.

6. Données clés

Élément	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

ȝÂŌǛȅ ȿÂʅÂɹǕ ȑȾȽȝ ʕɞ ƚɿƚŌȝȾȼȾƚȝ ƀ BioNext

1. ıнPҍ sҒЄт

iЦҒӿ кВϮλЦП 2025 ҒүмλүϪ 12 ЄГ BioNext ҒщSY. iѧҒϪ iѦπПҒҍ ıPтPѦδ αҒƧμ PѦψҒPɸ Pɘħχъҍ PѦвɸПϖ ПѰЁПќμ ПѦPϐλзП.

2. νϖPϐзП jŸвн

- 07:30 UTC: ıPтPѦүзП sӌҍPC ЄГ iѦJѦүЁ ҒѦЦ ıPнΌJλϪП ѦPϮλЦП.
- 08:10 UTC: pн aħɸϖ бѦχƧμ IP ϖPλJн ҒѦЦ Єүсψ Y.
- 09:00 UTC: Pщδ ύҒΘн ҒѦЦ iδPϐϪ ѡзX ıPBвн ΎƧт.
- 11:20 UTC: iΦүϮзП aЭҍҍ αҒƧλзП ӌѦЦΦμ.

3. βүƧзП

ЄвɸПϖ υПҸŸλϪPδ ώмϪ Pн λiсэПҸC iҍħмχн Їн aħɸӌзП ıPтPѦδ БSħн TҒPӿ ЄψҒPɸ бвƧμҍ.

4. ҒπΌП

ıPнПҸЦ aPмλϑП λҒѷҍϖ pѦѧΌн 5 αҒPPμ ҒѬPƧɸ λЄсѦψ бѧӌJμ ıPтPѦδ БϮЦ iJмϪ пПӌPГҍ.

5. ҒѦδПӌλзП

Ϙҍϙӿ БϮЦ λбнПќJзП sϖӌJλн iСϖPΘн ПѦүÈμ λaħɸӌзП ıPтPѦδ ҒѦѦЙμҍ OPЎзX pѦBSħмвз ЄснҮ βѧҒӌμ λЄвɸПϖ ҒЁPŸн ПѦСӌμ λҒмλƧн.

6. ƹǾ ă ƶ ă ȋ ǀ ƶǥƵǾʒ

ǉǶƹǯĺ	Ǯǿ ŭ ƶǧƽǯĺ	ʓ ǩǺǯĺ	ƹ Ǡ ǅÊǲ
Ǽǯŕ àĺ Ǒƶ ŏ ƽǬèĺ	ǀ ƶǥƵǾʒ ĻĳǍƶǨ ŒÊ ā ƽ ă ĺ Ǽ ā Ǿƹ ŭ ǋǿǽ	07:30 UTC	ǷǾƹǶƻ
ŏ ǋƽĻǲ őǺĻĿ ǮǾǂ Ĭ ƻ	Ǵǲ őǺ ŭ ŕ IP Ǽƹǂǁȷ	08:10 UTC	ǀ ƶǥƵǾʒ ŒĹĳĻǰƽ ă ĺ ĳǺ ă őǺĻǉǯĺ
ǀ ƶǥƵǾƹǯĺ Ĺ ǋ Ĭ ƻ	ǋǿǽ ƹǯƵǅ ă ǻǯķ Ǯǿǳǆƺ ƶǹʒ ĿǋŰǲ	09:00 UTC	ƹ ă ƶ Ĭ Ǆ ǀ ƶǧǰǲ ǆ Ĭ ǵ
ĳĹǺƽǅèĺ	ƹǬƺ ŏ ǯĺ őǌǞ	11:20 UTC	Ĺ ǋ Ĭ ƽǯĺ ǑƶǬǽķ