Exposure statement

Signed record of the facts concerning one legal entity found in circulation on deep and dark web sources during the period stated.

REFERENCE	sample-escalation-en
ISSUED	04 May 2026
PERIOD	01 Feb 2026 → 30 Apr 2026
PRODUCT	surveillance

ENTITY

SitinCloud SAS

SIREN 807 841 069 · SAS

DECLARED PERIMETER

The SitinCloud and OwlyScan names, the sitincloud.com and owlyscan.com domains, and the corporate mail addresses attached to them.

VERDICT

Confirmed findings

Findings recorded: 3 · 1 high · 1 medium · 1 low

FINDINGS IN CIRCULATION

#	CLASS	CONFIDENCE	SOURCE	OBSERVED	REFERENCE
01	Credentials on a corporate domain	■ HIGH	credentials in circulation	11 Mar 2026	DOC-2603-0231
02	Documents citing the entity in a third-party corpus	◧ MEDIUM	third-party corpus	02 Apr 2026 → 21 Apr 2026	DOC-2604-0118
03	Scraped public directory data	□ LOW	public directory	03 Feb 2026 → 28 Apr 2026	DOC-2601-0009

Annex A sets out each finding in full: the observation, the risk it creates, the question that would settle it, and what follows if it is confirmed.

SIGNATURE

CONTENT HASH (SHA-256)

09a8f3a6 18ec9697 f3e33483 34d093c0 96a1782b 87fa16a7 d650e124 901d1fd2

SIGNATURE LEVEL	stub-advanced
TIMESTAMP	stub-ts-sample-escalation
ARCHIVED UNTIL	01 Aug 2032
PREVIOUS STATEMENT	90d3d865 6273f7fd 0144ac27 439c33dc 7492bc7f d453df50 4ac88e19 e07efdb9

This series of exposure statements constitutes evidence of monitoring of the entity's mentions across deep and dark web sources, relevant to the threat-monitoring obligations under NIS2, DORA and applicable contractual security requirements. It attests continuous monitoring since 01 Aug 2025, the date of the first statement in the chain referenced above.

Issued by SitinCloud SAS. Verify this statement, no account required.

This signature attests that SitinCloud issued this content on this date about this entity. It does not attest exhaustiveness of collection, which is contractually excluded.

ANNEX A

Findings in detail

One entry per finding in the register on page 1, in the same order. Each entry states what was observed, what an attacker could do with it, the closed question that would confirm or dismiss it, and where the observation came from.

01 Credentials on a corporate domain

■ HIGH

FACT	A credential set pairing a corporate address on the sitincloud.com domain with a cleartext password is circulating on a resale channel. The record carries a March 2026 collection date and a machine identifier, both markers of an information-stealer rather than of an aged compilation.
RISK	Credentials that can be replayed against any login accepting these identifiers.
IF CONFIRMED	Credential exposure on corporate domains; forced reset and session review recommended.

ARTEFACT	SOURCE	OBSERVED	REFERENCES
credentials	credentials in circulation	11 Mar 2026	DOC-2603-0231

02 Documents citing the entity in a third-party corpus

◧ MEDIUM

FACT	A supplier tracking spreadsheet citing the entity and two of its named contacts appears in a corpus published after an incident at a client. The file carries direct contact details and order references.
RISK	Documents citing the entity are in circulation on darknet source categories, usable as context for social engineering.
TO VERIFY	Is the cited entity the legal entity SitinCloud SAS (SIREN 807841069)?
IF CONFIRMED	Material usable for targeted social engineering against contacts named in the documents.

ARTEFACT	SOURCE	OBSERVED	REFERENCES
documents	third-party corpus	02 Apr 2026 → 21 Apr 2026	DOC-2604-0118

03 Scraped public directory data

□ LOW

FACT	The entity's registry identity is still carried by the same business directories as in the previous quarter. No internal data is added to it.
RISK	A targeting lead only. No internal data is in circulation.
IF CONFIRMED	No distinct client consequence beyond ordinary vigilance.

ARTEFACT	SOURCE	OBSERVED	REFERENCES
directory	public directory	03 Feb 2026 → 28 Apr 2026	DOC-2601-0009

ANNEX B

Method and coverage

What was watched, how an observation becomes a finding, and how confidence is assigned. This annex is part of every statement, including one that records nothing: an assurance that nothing is in circulation means little without the scope behind it.

Source categories

Every finding is attributed to one category. The category describes where the material was observed, not who put it there.

credentials in circulation	Sets of identifiers, most often address and password pairs, republished across collection and resale channels.
documents in circulation	Files published after an incident affecting the organisation that held them, indexed at document level rather than as an archive.
third-party corpus	Material published after an incident at a supplier, a client or a partner, in which the entity appears without being the subject of the incident.
claim site	Pages on which a group names the organisations it claims to have compromised, together with any material it publishes in support.
forum	Discussion boards and channels where access, data and targets are offered, negotiated or simply mentioned.
public directory	Openly published registers and directories collected in bulk and republished elsewhere, including company registries and staff listings.

How a finding is written

Every finding carries the same four fields, in the same order, so that two findings can be compared and so that no observation is reported as a conclusion.

Fact	What is in circulation, phrased as an observation and nothing more. It never asserts that the entity was compromised.
Risk	What the material lets an attacker do. Stated independently of the entity's own systems, which are never examined.
To verify	A closed question only the entity can answer, present when confidence is low or medium. Answering it settles the finding.
If confirmed	What follows for the entity if the validation question comes back confirmed. A conditional, never a diagnosis.

Confidence scale

Confidence describes how firmly the material is tied to this legal entity. It says nothing about how severe the finding is.

high	The material carries an identifier belonging to the entity alone, such as a domain it controls or its registration number.
medium	The attribution rests on several converging elements, none of which is conclusive on its own.

low	The name matches, and nothing further distinguishes the entity from an organisation with a similar name.

Limits of this statement

- Collection is not exhaustive, and exhaustiveness is contractually excluded. Sources appear and disappear, and no watch sees all of them.
- No system belonging to the entity is accessed, scanned or tested at any point. Everything reported here was observed on third-party sources.
- A finding is not an incident. It reports material in circulation, which may predate the period, may concern a namesake, or may already be known to the entity.
- This document is a statement of observation. It is not a security audit, not a certification, and not an opinion on the entity's security posture.

ANNEX C

Verification and glossary

This document is meant to be checked by someone who did not receive it from us. Anyone holding a copy can confirm it is the document SitinCloud issued, without an account and without contacting us.

Checking this document

1. Open owlyscan.com/verify in any browser.
2. Enter the content hash printed below, exactly as it appears. Spaces are ignored.
3. The register answers with the entity, the period and the issue date recorded against that hash. If any of the three differs from this document, the copy in your hands is not the one that was issued.

CONTENT HASH (SHA-256)

`09a8f3a6 18ec9697 f3e33483 34d093c0 96a1782b 87fa16a7 d650e124 901d1fd2`

What the signature attests

IT DOES ATTEST

- that SitinCloud issued this content,
- on the date printed on page 1,
- concerning the legal entity named on page 1.

IT DOES NOT ATTEST

- that collection was exhaustive,
- that the entity was, or was not, compromised,
- anything about the entity's security measures.

Glossary

Exposure statement	The document itself: a dated, signed record of what was in circulation about one legal entity during one period.
Legal entity	The subject of the statement, identified by its registration number so that a group, a brand and a subsidiary are never confused.
Finding	One observation of material in circulation, qualified by the four fields set out in Annex B.
Content hash	A fingerprint computed from the statement's content. Changing a single character of the document produces a different fingerprint, which is what makes tampering visible.
Chain	Each statement in a surveillance series records the fingerprint of the one before it, so the series can be shown to be continuous and complete.
Timestamp	Independent proof of the date, so the issue date rests on more than our own word.
Verdict	The one-line result for the period: nothing in circulation, findings awaiting validation, or confirmed findings.