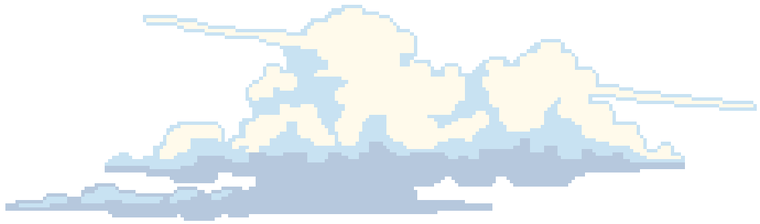
revolgy × vega

LIVE WEBINAR · REVOLGY + VEGA



Who set your retention window?



The same investigation on 30 days, 90 days and a year of logs, with a timer on screen

M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12

Months 1 to 9: deleted after 90 days in a typical SIEM

Months 10 to 12: what the SIEM still holds when the alert comes

Tuesday 3 November 2026 · 12:00 UK · 13:00 CET · 60 minutes

Marko Kirschner, Vega · Marius-Florin Cristian, CISSP, Cloud Security Lead, Revolgy

Keep the logs your risk calls for, without breaking the bank

Attacks run longer than the window

Breaches take 241 days on average to find and contain (IBM, 2025). In the demo, the theft started 147 days before the first alert.

A year of logs costs little to keep

One year at 100 GB a day costs about EUR 4,100 in object storage. The same year in Microsoft Sentinel costs about EUR 160,000 at list price.

A year of logs is fast to search

Vega answered the same question over 30 days, 90 days and a year, in 2 to 4 seconds each time.

Revolgy runs it around the clock

We bring order to scattered logs and alerts and watch them 24/7, so your teams keep shipping and the evidence is ready when an auditor asks.

The rest of the hour shows the evidence for each point. Ask questions in the chat at any time.

60 minutes with Vega and Revolgy

00-10	The problem with a 30 or 90-day window	Marius
10-30	Live in Vega: detect it, trace it back, then automate it	Marko and Marius
30-32	Your questions so far, and a poll	Marko and Marius
32-37	The cost of keeping a year of security data	Marius
37-47	The managed security service	Marius
47-52	The evidence auditors ask for, and how to start	Marius
52-60	Your questions	Marko and Marius



Marko Kirschner

System Engineer, Vega

Runs the investigation live in Vega.



Marius-Florin Cristian, CISSP

Cloud Security Lead, Revolgy

Practitioner and security programme lead. Former CISO; has taken B2B SaaS companies from pre-seed to exit.

Revolgy is a Google Cloud Premier Partner and a Vega partner.

Most teams can search 30 to 90 days of security data

30 days

of 365 days

Azure Log Analytics: default retention of analytics tables

90 days

of 365 days

Microsoft Sentinel: analytics retention included in the price

90 days

of 365 days

AWS CloudTrail Event History. A longer history needs a separate trail

180 days

of 365 days

Microsoft 365 and Google Workspace audit logs, default

In most companies the number came with the SIEM’s price per gigabyte.

POLL How many days of security logs can you search today? 30 90 180 a year or more

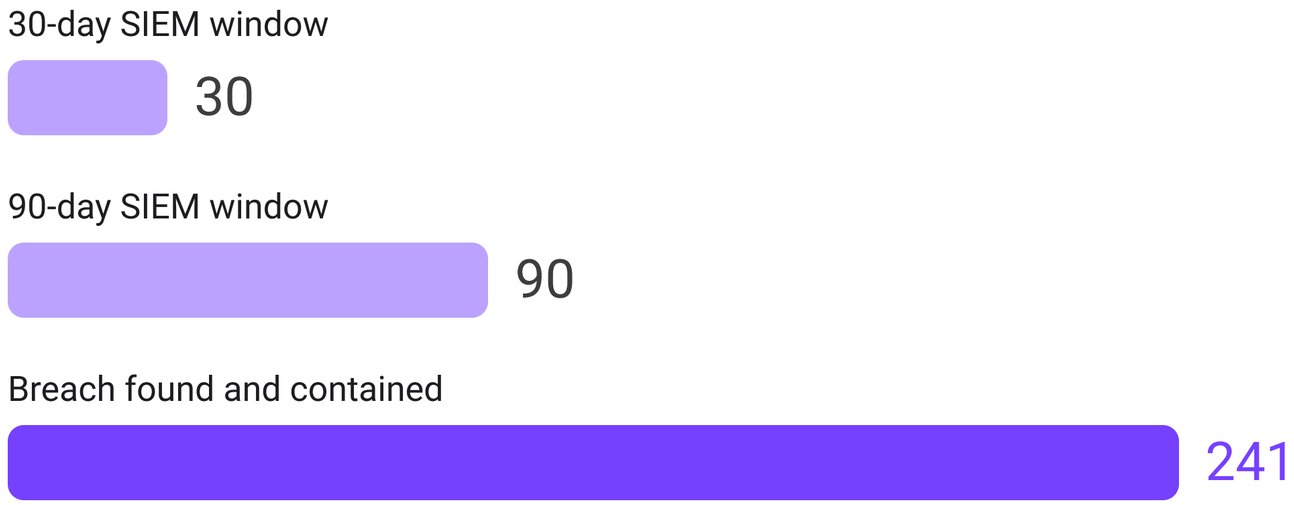
Vendor documentation: Azure Monitor Logs, Microsoft Sentinel pricing, AWS CloudTrail User Guide, Microsoft Purview Audit, Google Workspace Admin Help. Check current values before publishing.

Breaches take 241 days on average to find and contain

241 days

Mean time to identify (181 days) and contain (60 days) a breach.

When the alert fires, the start of the intrusion is often older than a 30 or 90-day window.



Source: IBM, Cost of a Data Breach Report 2025 (breaches from March 2024 to February 2025).

Regulators ask when it started and what was taken

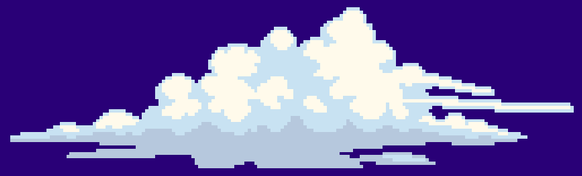
DORA	Major ICT incident: initial notice within 4 hours of classifying it as major, and no later than 24 hours after you became aware of it. Intermediate report within 72 hours. Final report within one month.
NIS2	Early warning within 24 hours. Incident notification within 72 hours. Final report within one month.
GDPR	Personal data breach: notify within 72 hours, with the approximate number of people and records concerned.

To classify and report the incident you need

- The date it started
- Which data, clients and transactions it touched
- Which accounts and systems were involved
- Whether it is still going on

“A supervisor, an insurer or a court will ask how you got to your numbers.”

DORA: Regulation (EU) 2022/2554; classification RTS (EU) 2024/1772; reporting time limits RTS (EU) 2025/301. NIS2: Directive (EU) 2022/2555, Art. 23. GDPR: Art. 33.



LIVE · 00:00

Detect it, trace it back, *then automate it*

Live in Vega, with a timer on screen

The alert: finance files leaving an S3 bucket

AWS GUARDDUTY

HIGH

`Exfiltration:S3/MaliciousIPCaller`

- First raised 13 October 2026, 00:35 UTC, then every night
- GetObject calls on the finance-exports bucket
- Made with the access key of a marketing user
- From a bulletproof-hosting address in Bulgaria

QUESTIONS THE INCIDENT MANAGER HAS TO ANSWER

Since when?

What was taken?

Which account, and where did the key come from?

Was anything else touched?

Is it still going on?

Same query, three windows: 450, 1,367 or 2,387 downloads

```
@CloudTrail
| where src_endpoint.ip == '45.142.213.99'
| summarize downloads = count(), first_seen = min(timestamp), last_seen = max(timestamp) by event_name, databucket.name
```

Last 30 days

a typical SIEM window

450

downloads of finance files

19% of the downloads

Earliest download seen: 24 Sep, the edge of the window

Last 90 days

the retention Sentinel includes

1,367

downloads of finance files

57% of the downloads

Earliest download seen: 26 Jul, the edge of the window

Last year

object storage, read by Vega

2,387

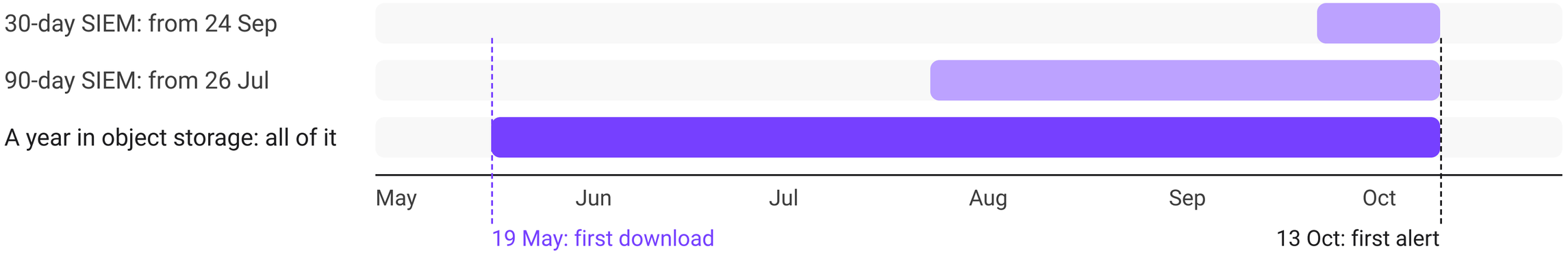
downloads of finance files

All of them, with the start date

First download: 19 May 2026, 10:59 UTC

All three runs in Vega on the same synthetic data, 23 October 2026. Each run took 2 to 4 seconds.

The theft started 147 days before the first alert



THE FULL YEAR SHOWS

- One access key, one IP address, one bucket. No other accounts or buckets touched
- The same 15 finance files, every night between 00:10 and 00:18 UTC
- The key belongs to a marketing manager with no business need for finance data

A year of logs gives the report its start date and scope. With 90 days, the report can only say the theft is ongoing.

The investigation was finished before anyone opened it

7 min 32 s

From incident created (01:07:27 UTC) to investigation complete (01:14:59 UTC), run by Vega's investigation agent.

Vega's published figures: triage from 25 minutes to under 3 at a Fortune 500 customer; 1 billion CloudTrail logs across 17 AWS regions searched in 41 seconds.

1. Identity: Entra ID profile of the key's owner
2. Baseline of the user's normal activity
3. The IP address and its hosting network
4. Everything the access key did
5. Everything the IP address did
6. Key creation and policy changes
7. Open posture issues in Wiz

Waiting for the analyst

VERDICT

Malicious, with 6 key findings

8 queries over 3 data sources: Entra ID, CloudTrail, Wiz

3 containment actions ready to approve:

- Disable the access key
- Block the IP address
- Disable the IAM user

Ask in plain language, keep a query an auditor can rerun

YOU TYPE

“Show me MFA fatigue attempts followed by a successful login”

VEGA WRITES AND RUNS

```
@Okta-System-Logs
| where _raw.eventType == 'user.mfa.okta_verify.deny_push'
| project deny_timestamp = timestamp, _raw.actor.alternateId,
    _raw.authenticationContext.externalSessionId
| join kind=inner ( @Okta-System-Logs
  | where _raw.eventType == 'user.authentication.auth_via_mfa'
    and _raw.outcome.result == 'SUCCESS' ... )
  on _raw.actor.alternateId, _raw.authenticationContext.externalSessionId
| where success_timestamp > deny_timestamp
```

Ask

A question in plain language, across every source

Confirm

The query and its results, saved in a notebook anyone can rerun

Detect

Promote it to a detection that runs on every new log

Other prompts in the sandbox: “Has anyone changed IAM roles or policies in the last 7 days?” · “Find impossible travel logins” · “Hunt for cloud actions taken from new source IPs by privileged users”

Query generated by Vega from the sentence above in the sandbox, 23 October 2026 (shortened for the slide).

Every verdict you approve tunes the detections

1

Alert

A detection fires on new logs

2

Vega investigates

7 min 32 s for the finance-bucket case, before anyone opened it

3

Your analyst approves

The verdict and the containment actions

4

Vega tunes the detection

Ruled-out noise is excluded, the rule is refined or a new one is proposed

The next alert like it is handled with what the team already learned

IN THE SANDBOX

- 129 skills for triage, investigation, hunting and tuning
- Tuning skills for service-account noise, admin-role duty noise and trusted infrastructure
- An engineer approves every change to a detection

The team does each analysis once. The detection keeps what it learned and applies it to every new log, around the clock.

Vega sandbox, agents and skills, 23 October 2026. Anthropic customer story on Vega: optimization skills update detections from approved verdicts, and engineers approve each change.

A new threat report becomes a detection the same day

Vega Threat Research, 8 October 2026: phishing through Google Drive share notices that installs a remote-access agent on the victim's machine.

62

indicators from the report, searched across the whole history: domains, IP addresses, file names, hashes

0

matches in the sandbox history, so the campaign has not reached it

8

detections for the campaign, mapped to MITRE ATT&CK, ready to switch on

- Library in the sandbox: 1,548 detections and 129 skills for triage, investigation, hunting and tuning
- Detections from your current SIEM can be imported
- The indicator search reads as far back as you keep logs, so a year of logs answers whether the campaign reached you this year

Vega sandbox, threat intel briefing and detections hub, 23 October 2026. The 8 detections were switched off in the sandbox, which Vega shows as 8 detection gaps.

Vega reads the logs where they are stored

WHERE YOUR DATA ALREADY LIVES

Your object storage
S3, Google Cloud Storage, Azure Blob

Your current SIEM
Microsoft Sentinel, Splunk, CrowdStrike NG-SIEM, Sumo Logic

Identity and endpoints
Entra ID, Okta, Google Workspace, CrowdStrike, Defender, SentinelOne

Posture and context
Wiz, Upwind, Axonius, Cyera, threat intelligence feeds

vega

Indexes the data where it is stored; nothing is copied into a SIEM

One schema across sources

Plain language or KQL

AI triage and investigation of every alert

Your bucket, your region: logs never cross borders

WHAT YOUR TEAM GETS

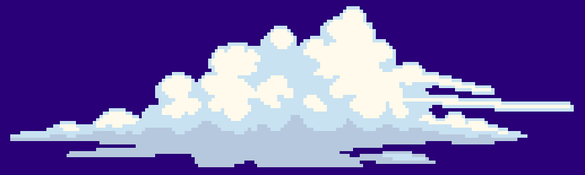
Incidents
each with a finished investigation and actions

Detections
mapped to MITRE ATT&CK, tested and tuned

Notebooks
queries anyone can rerun

Response
SOAR, ServiceNow, webhooks

In the sandbox: 29 event sources and 13 context sources connected, including CloudTrail, Okta, Palo Alto firewalls and Claude Code.



Questions so far

POLL

Who looks at a security alert at 3 am on a Sunday in your company?

- Nobody
- An on-call engineer
- Our SOC or MSSP
- Not sure

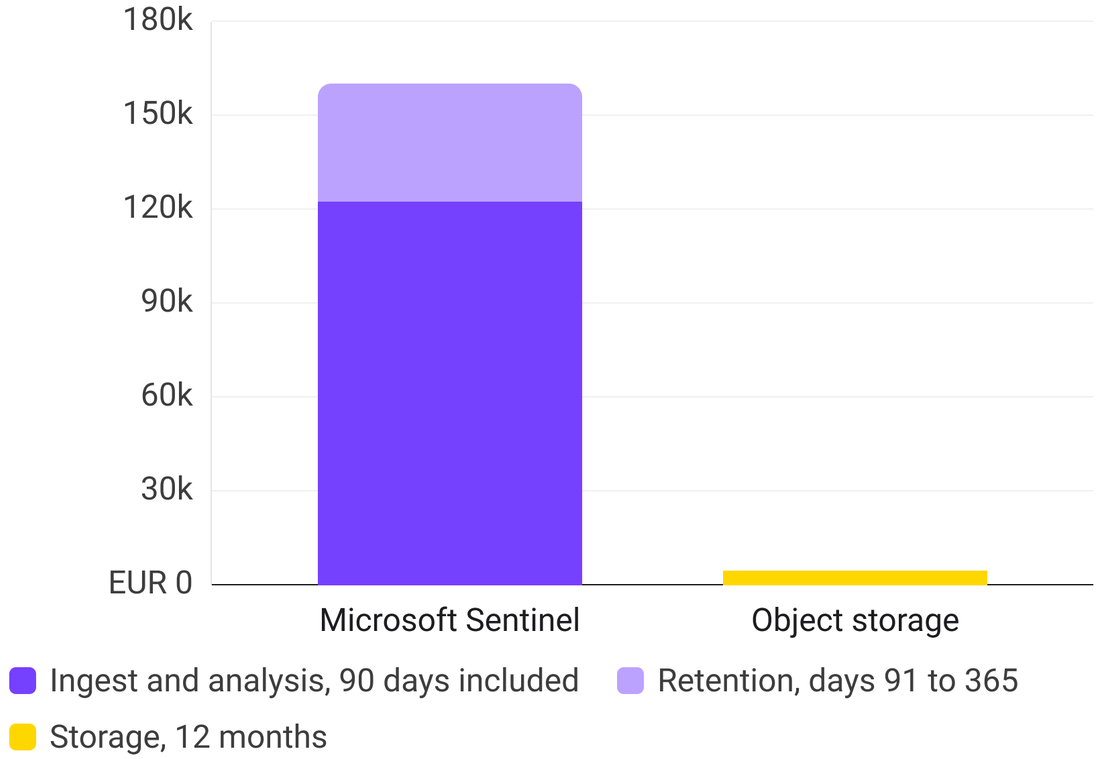
Join on Slido

Vote and ask questions

Next: the cost of keeping a year of data, and the service that runs it

Keeping a year of logs: storage is the cheap part

100 GB of logs a day, EU list prices, one year kept



about

EUR 160,000

a year in Microsoft Sentinel: EUR 122,775 for the 100 GB/day tier with 90 days, plus EUR 37,686 to keep days 91 to 365 searchable

about

EUR 4,100

a year in Azure Blob storage (30 days hot, 11 months cool), plus the Vega licence, which is priced per customer

Vega's figure: up to 82% lower cost than a legacy SIEM.

Azure Retail Prices API, West Europe, EUR, accessed 30 August 2026: Sentinel 100 GB/day tier EUR 336.37 a day; retention beyond 90 days EUR 0.1142 per GB-month; Blob LRS hot and cool tiers. Storage only, before compression. Vega figure: vega.io, method not published.

Keep your SIEM and add the logs it never sees

Your SIEM

keeps its rules, dashboards and contract

\+

Your object storage

takes the logs you drop today because of cost

=

Vega

one search and one set of detections across both

Day one

- Vega reads your SIEM through its connector
- Your SIEM detections are imported
- No migration project to start

Next

- Send the dropped logs to object storage first
- Move sources out of the SIEM when its contract allows
- Keep a year or more at storage prices

LOGS THAT RARELY REACH A SIEM TODAY

Firewall | WAF | Application | OpenTelemetry | VPC flow | Virtualization | CI/CD runners | SaaS audit

A managed security service keeps your business moving

Almost no friction for your teams

We set up security lean and run it for you, inside your release cycle, so your teams keep delivering without waiting on security.

Attacks are contained early, day and night

Every alert is triaged around the clock. Containment steps are agreed with you in advance.

You keep your customers' trust

When something happens, you can tell customers and the regulator what happened, with evidence.

A fractional CISO when a deal stalls

We join the call when a customer's security review holds up a deal, agree the risk level they need and what can wait, and keep the deal moving.

You go after new customers and markets. Revolgy keeps the risk in check and fixes what matters first.

Round-the-clock cover without hiring a five-person rota

BUILDING IT IN-HOUSE

EUR 109,000 to 121,000

a year for two mid-level security analysts in Czechia, fully loaded.

Two to four months to hire. Weekday cover only.

5 to 6 analysts plus a lead

for real 24/7 cover: 168 hours a week at 75 to 85% availability per person.

WITH VEGA AND REVOLGY

- Vega triages and investigates every alert as it arrives
- Revolgy analysts review, escalate and contain with you, around the clock
- One security engineer on your side is enough, or none: Revolgy covers the gap
- You choose the response tier, and the fee follows it

Our analysts start from finished investigations, so each analyst covers more clients, and the monthly fee reflects that.

Salaries: ISPV 2025, Czech Ministry of Labour wage statistics, private sector, plus 33.8% employer contributions. Rota: 168 hours a week at 40 hours per person.

Prevention and detection from one accountable team

Cloud and DevSecOps

Before an attack

- Posture and exposure with Wiz
- IAM drift and over-privileged accounts flagged to the SOC as soon as they change
- Exploitable versions of firmware, frameworks, container images and CI/CD runners
- Landing zone, logging and lifecycle policies

Application security

In your business domain

- Threat modelling of your business flows with STRIDE
- Findings mapped to MITRE ATT&CK, CVE and CWE
- Verified to OWASP ASVS Level 2 or 3, logging included
- Security fixes planned into your releases

Security operations

During and after an incident

- Vega triage and investigation of every alert
- Revolgy analysts 24/7, response times per tier
- Evidence packs for auditors and regulators

We tell you what to fix first, and our engineers fix it.

Check a company's logs before you buy it

1

Connect

Read-only access to the target's buckets or SIEM. No migration and no agents to roll out.

2

Find the gaps

Search their history and configuration before you sign.

3

Absorb it safely

Bring the acquired company under the same detections from day one.

Gaps worth finding before signing

- Accounts with no match in HR, and leavers who are still enabled
- Admins nobody owns, and a dormant admin that became active months before the deal
- Blind spots on the MITRE ATT&CK map, and exploitable versions in production

After the deal

- Redundancies done in HR while the accounts stay active
- Integration access that is never removed
- Past intrusions still in the target's history

The evidence auditors and regulators ask for

FRAMEWORK	AUDITORS CHECK	YOU SHOW
DORA	Log retention set in your logging procedures from your ICT risk assessment; major incidents reported at 4 hours, 72 hours and one month	The written derivation of your window and the full incident timeline
NIS2	Incident handling; reports at 24 hours, 72 hours and one month	The same timeline, from one source
SOC 2 Type 2	Monitoring that operated across the whole audit period	Logs and alert records for the 6 to 12-month period
ISO 27001:2022	Logging (8.15), monitoring (8.16), incident management (5.24 to 5.28)	The logging policy and the records behind it
OWASP ASVS 5.0, Level 2 and 3	A logging inventory that says how long logs are kept (V16.1.1); logs sent to a separate system for detection (V16.4.3); at Level 3, every authorization decision logged	The inventory, a separate log store and a searchable history

DORA RTS (EU) 2024/1774, Art. 12 (logging); NIS2 Directive (EU) 2022/2555, Art. 23; AICPA SOC 2; ISO/IEC 27001:2022 Annex A; OWASP ASVS 5.0.0 chapter V16. Legal check before publishing.

Invest for the risk you target and the maturity you have

1:1

30 MINUTES

Your data, your numbers: daily volume, retention window and a price for twelve months

Assess

FIXED FEE

Telemetry inventory, MITRE ATT&CK posture, business case

Implement

FIXED FEE, ONE-OFF

Landing zone, lifecycle policies, detection migration from your SIEM

Operate

MONTHLY

Managed detection and response, tiered by response time

Fits companies from about 150 people: financial firms under DORA; NIS2 entities and their suppliers; regulated online platforms with high transaction and log volumes; product teams verified to ASVS Level 2 or 3; acquirers checking a target.

Start with 30 minutes and grow into a managed service. Each step stands on its own, so the spend matches the risk you target today.

revolgy × vega



ONE-TO-ONE · 30 MINUTES

Your invoice picked your retention window. *Pick it back.*



Bring your daily log volume to a **revolgy** security expert. No slides, just your numbers.

WHAT YOU LEAVE WITH

- What is currently dark in your logs
- Whether your estate fits object storage
- A retention window you can defend, priced

Scan to book a 1:1

Everyone who registered gets the recording.

Your questions

Backup: the Sentinel data lake tier

- Microsoft’s low-cost tier for telemetry: about EUR 0.17 per GB to ingest and process, EUR 0.0211 per GB-month to store (billed at 6:1 compression)
- Queries are billed per GB scanned (EUR 0.0057) and run on a separate path from the analytics tier
- Vega indexes object storage for interactive search across all sources, and it reads Sentinel as well

The question to ask of any option: what does a 12-month search across all sources cost, and how long does it take?

Azure Retail Prices API, West Europe, accessed 30 August 2026.

Backup: data, models and residency

- Logs stay in your own object storage. Vega runs the indexing and the search compute
- EU control plane in Frankfurt
- AI inference through Amazon Bedrock with zero data retention and no training on customer data
- Vega holds ISO 27001:2022 and SOC 2 Type II reports (trust.vega.io)
- Vega’s own defense model runs beside general-purpose models

Anthropic customer story on Vega (claude.com/customers/vega); trust.vega.io. Vega to confirm the current model list, regions and settings before publishing.

Sources

IBM, Cost of a Data Breach Report 2025

Microsoft Azure Retail Prices API, West Europe, EUR, accessed 30 August 2026

Vega sandbox (**revolgy**-sandbox), synthetic data, queried 23 October 2026

Vega customer story, claude.com/customers/vega; vega.io cost reduction page

DORA: Regulation (EU) 2022/2554; RTS (EU) 2024/1774, 2024/1772 and 2025/301

NIS2: Directive (EU) 2022/2555, Art. 23. GDPR: Regulation (EU) 2016/679, Art. 33

OWASP ASVS 5.0.0, chapter V16. ISO/IEC 27001:2022, Annex A

ISPV 2025, Czech Ministry of Labour wage statistics

Vendor documentation on default retention: Azure Monitor, Microsoft Sentinel, AWS CloudTrail, Microsoft Purview Audit, Google Workspace

revolgy × vega





LIVE WEBINAR · REVOLGY + VEGA

Thank *you.*

The recording and the slides are on their way to everyone who registered.



Marko Kirschner
System Engineer, Vega



Marius-Florin Cristian, CISSP
Cloud Security Lead, **revolgy**

Scan to book a 1:1