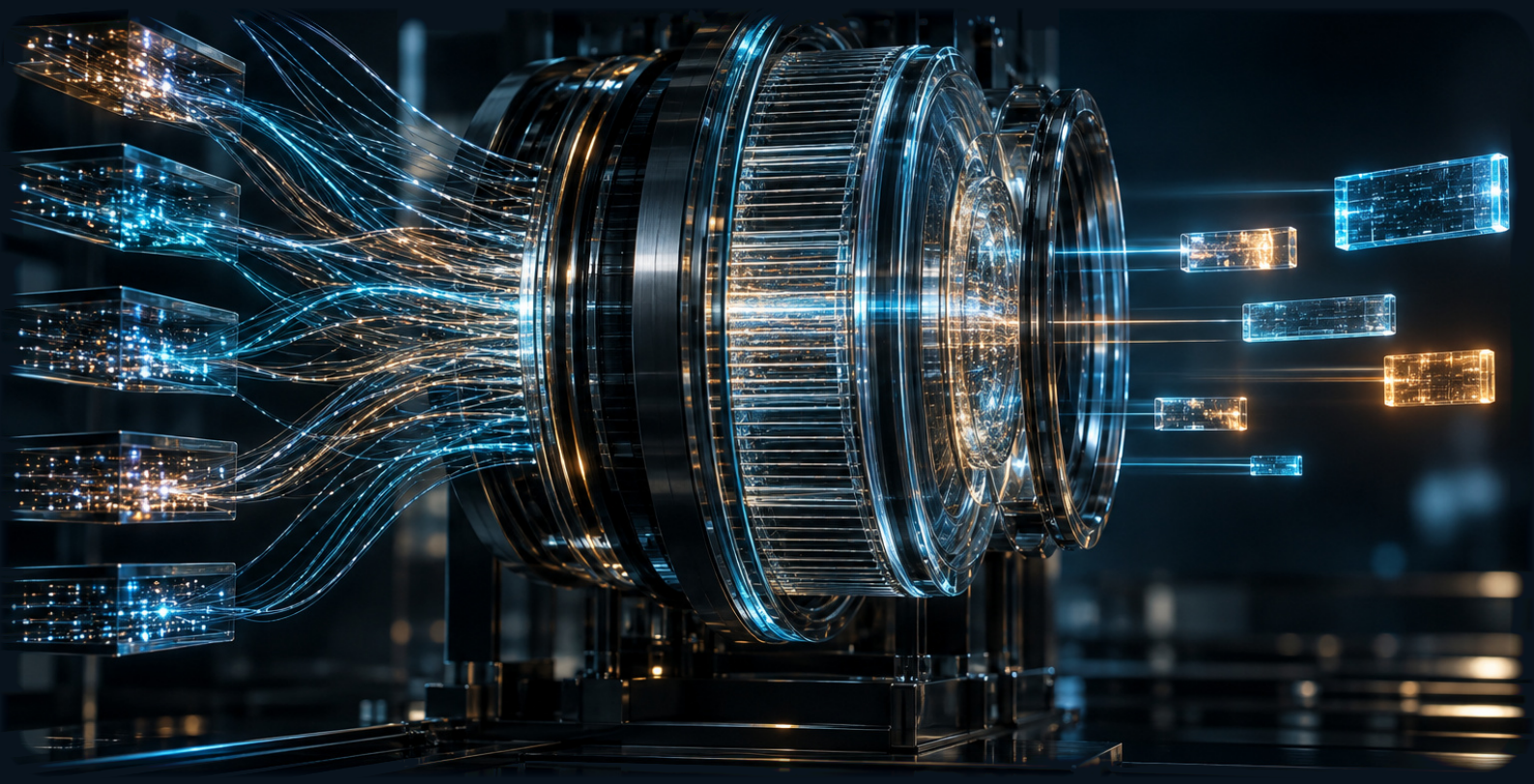
GNSAC

VIGIL

CYBER THREAT INTELLIGENCE / DIGITAL RISK MONITORING

See the threats aimed at your organisation.

From leaked accounts to brand impersonation: assess external risk with its source, its evidence and the response steps.



4.17 billion
intelligence records

190+
domain checks

24
alert categories

Intelligence volume as of 20 Sep 2026

BRING EXTERNAL RISK INTO ONE REVIEW

Your digital footprint. One workspace.

Vigil gathers account, brand, asset and supplier risk into a shared stream of findings. Your team decides which record concerns the organisation, and what happens next, on the same platform.

01 Accounts

Leaked credentials and infostealer records.

02 Brand

Look-alike domains, fake profiles and visual matches.

03 Digital assets

Exposed services, configurations and vulnerabilities.

04 Suppliers

Breach, infrastructure change and impersonation risk.

05 Key people

Exposure and reporting specific to VIPs.

06 Payment identifiers

MID, TID, BIN and payment-portal leaks.

A WORKFLOW THAT STARTS WITH A FINDING

01 Match

Isolate the signal that is yours.

02 Review

Open the source and evidence.

03 Prioritise

See severity and context.

04 Follow up

Manage the case and report.

The Dashboard, Findings and Alarms screens present source, severity, status and timing in a single workflow.

PRODUCT DATA AS OF 20 SEPTEMBER 2026

A large archive. Intelligence focused on you.

Records are collected on GNSAC's central infrastructure. The customer instance receives the intelligence relevant to its organisation by sync; review and response run in its own workspace.

93 million+

records processed in the last 7 days

- **3.49 billion credential records**
- Other intelligence records

1,754

registered intelligence sources

≈8,500

new IOC records per day

125,775

evidence pages archived over Tor

61,587

vulnerability (CVE) records

1.2 million+

phishing URL records

The 3.49 billion credential records are part of the 4.17 billion total. Volumes are the dated archive counts in the product documentation.

FROM SOURCE TO EVIDENCE THAT IS YOURS

Trace the leaked account.

Query the leak archive by domain or e-mail address. Review credentials, infostealer records and posts that mention your organisation, together with their source.

PASTE	TELEGRAM	RANSOMWARE	FORUM / GITHUB
5 min	10 min	15 min	30 min

See the source

Reach the relevant records through domain and e-mail indexes.

Review the evidence

Open the archived leak page in isolation, inside the panel.

Keep following

Track new findings, severity and alert status.

The intervals above are default source polling intervals, not end-to-end notification times. The image represents the matching flow.

FROM A VERIFIED DOMAIN TO A DETAILED REPORT

More than 190 checks. Review in 12 phases.

Verify your domain with a DNS TXT record. Discovery, exposure, relationship and risk analysis run in one scan pipeline, producing a baseline that later scans are compared against.

01 - 04

Discovery and exposure

Organisation profile, asset discovery, configuration, e-mail and brand.

05 - 08

Threats and dependencies

Leaks, vulnerabilities, actor / MITRE and third-party relationships.

09 - 12

Correlation and priority

IOC / reputation, attack path, risk / remediation and report.

13 minutes

Median duration across 29 measured scans. 27 of them completed in under half an hour.

Scheduled follow-up

Daily, weekly or monthly scans; expiry tracking for domain registrations and TLS certificates.

Scan duration varies with scope and domain. 13 minutes is the median of 29 scans, not a guaranteed completion time.

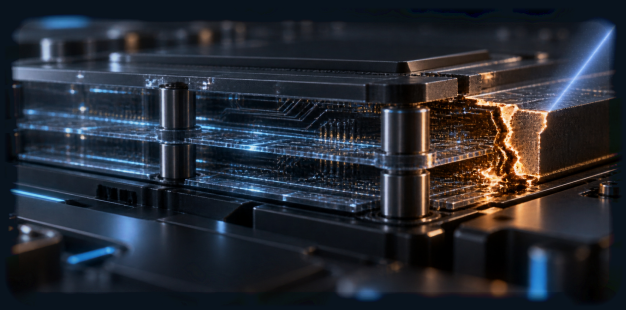
PUT EXPLOITATION CONTEXT NEXT TO SEVERITY

Which vulnerability should come first?

Assess a vulnerability by its technical score together with active exploitation, likelihood and published exploit information. See the related vendor and product record in the same review.

61,587
CVE records

149
KEV-flagged records



CVSS

Technical severity

Assess the theoretical impact and severity of the flaw.

EPSS

Exploitation likelihood

Review the probability estimate for the next 30 days.

KEV

Active exploitation

Separate records that the CISA catalogue lists as actively exploited.

EXPLOIT

Published method

See whether a public exploit exists.

ALERTS FOR VULNERABILITIES THAT MATCH A SUPPLIER

When a critical, high, KEV-flagged or exploit-published record names a monitored supplier, it enters the related alert stream.

CVE and KEV counts: product documentation dated 20 September 2026. CVSS, EPSS and KEV are different assessment dimensions.

REVIEW THE COPIED TRACES OF YOUR BRAND

Find the look-alike. Catch the visual copy.

Vigil lets you assess brand impersonation across domain, phishing, social-profile and application findings together. Logo and favicon comparisons add concrete grounds to the review.

1.2 million+

phishing URL records
20 September 2026

Exact file identity and perceptual-hash comparison help distinguish copied or resized logo and favicon files.

Look-alike domain | Fake social profile | Store application | Takedown case

The image represents the impersonation comparison. Access restrictions on social platforms may affect the scope of results.

RECORD THE STATUS AND EVERY STEP TAKEN

Turn detection into traceable response.

Takedown Center keeps the case, the notice, the reply and the evidence in one process. A notice counts as sent only once the mail server has accepted the message.

01

Case and contact

Record the target; collect registrar contact details and evidence.

02

Approved notice

Send from your organisation’s SMTP server; track delivery status.

03

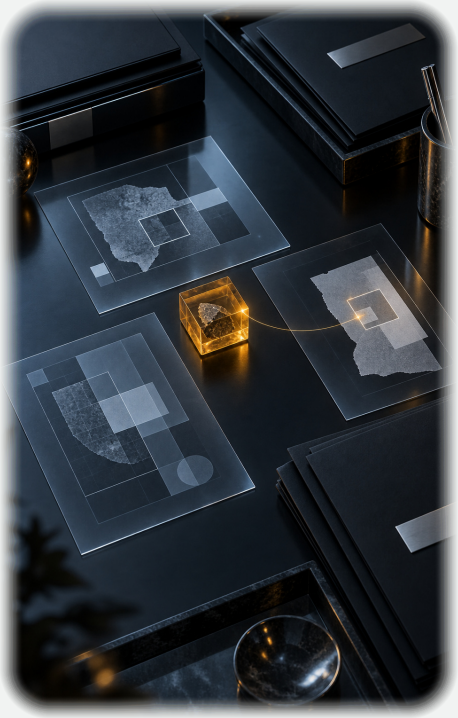
Reply and escalation

Record the other party’s reply; move to the next provider if needed.

04

Evidenced closure

Close with the removal or refusal outcome, notes and evidence.



12 hours

page evidence re-captured

7 days

follow-up for unanswered notices

14 days

delay tracking during escalation

6 ready-made playbooks: account leak, phishing, VIP, brand, supplier breach and manual review. Your team can also create its own.

Intervals are default follow-up settings. Notice and escalation are user decisions; the removal decision belongs to the provider or platform.

FROM BREACH SIGNALS TO INFRASTRUCTURE CHANGES

Watch supplier risk through eight signals.

Add a supplier by name and domain. The monitor compares against the previous state and routes new changes and new exposure to the related alert category.

01 **Ransomware record**

02 **Breach record**

03 **Infostealer finding**

04 **Look-alike domain**

05 **DNS change**

06 **Certificate change**

07 **E-mail spoofing risk**

08 **Supplier vulnerability**

30 minutes

Default monitoring cycle. Look-alike domain and certificate transparency checks run daily.

The supplier list is kept on the customer instance. Daily state snapshots form the basis for trend tracking.

MONITORING SPECIFIC TO PEOPLE AND PAYMENT IDENTIFIERS

Watch key people and payment identifiers.

Executive exposure and payment-identifier leaks are monitored as separate scopes. The related findings, sources and notifications arrive in your team's shared workspace.

VIP Protection

E-mail-based exposure scan for executives and key people.

- Leaked accounts and infostealer records.
- Dark web traces and publicly available exposure.
- Per-person PDF report in TR / EN.

POS & Payment

Leak monitoring for MID, TID, BIN and payment-portal logins.

- Trading-name and keyword matches.
- Payment-portal logins and historical record queries.
- Payment-themed look-alike domains.

Default monitoring: every 30 minutes

The VIP and payment monitors run on a schedule; manual query and scan options support the related review.

The payment module does not see or block card transactions; it monitors leaks of payment identifiers and logins.

REVEAL THE RELATIONSHIPS BETWEEN RECORDS

From one finding to a web of relationships.

Explore visually which account appears in which leak, which infrastructure a domain is tied to, and how IOCs connect to campaigns.

Credentials | Leaks | Threat actors | Domains | IP / IOC | Campaigns

Open the record

Move from a node to the actor or incident detail; review the source in context.

Assess locally

Produce trend, anomaly, risk and confidence assessments from the data inside your instance.

The graph is a conceptual example; node counts are not customer data. Insights are assessments derived from existing findings.

REGIONAL CONTEXT AND FILE INDICATORS

Take the review further.

Follow regional sources, the threat groups involved and sector distribution. Examine suspicious files with hash intelligence, YARA rules and local static analysis.

TR **Türkiye**
USOM and local sources

US **United States**
CISA KEV, FBI / CISA advisories

UK **United Kingdom**
NCSC sources

CA **Canada**
CCCS sources

AU **Australia**
ACSC advisories

RU **Russia**
Russian-language forum and channel sources

Hash lookup

Review engine verdicts, file metadata, family and tag information from VirusTotal and MalwareBazaar.

Local static analysis and YARA

Assess file type, entropy, readable strings and network indicators; match against the installed YARA rules. The uploaded file never leaves the instance and is not retained.

6 COUNTRY INTELLIGENCE MODULES

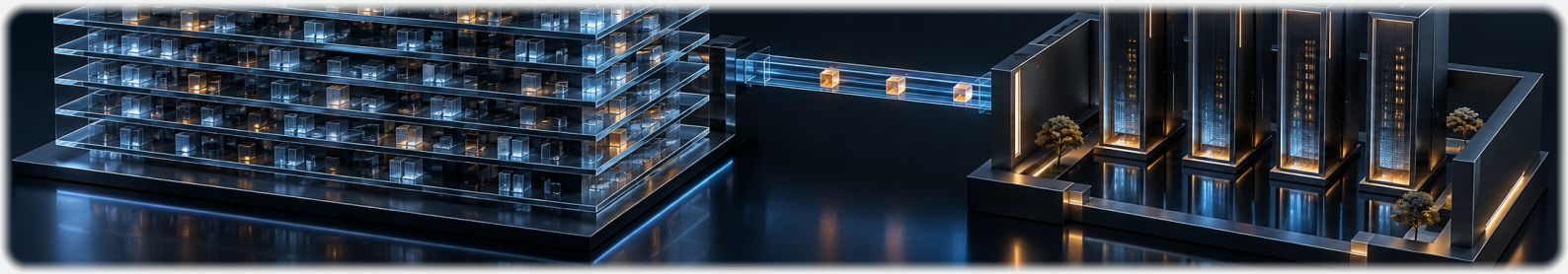
YARA MATCHING • REVIEW WITHOUT EXECUTION

Static review is not a sandbox service that executes the file. Regional data updates depend on the cadence of the respective sources.

CENTRAL COLLECTION, A SEPARATE INSTANCE PER CUSTOMER

Intelligence at the centre. Analysis on your instance.

Records concerning your organisation are delivered to a separate customer instance. The local analysis engine computes trends and correlation without sending data to external AI services.



GNSAC CENTRAL

Collection layer
Dark web, open sources, forums

Intelligence archive
Credentials, IOC, CVE, phishing

Evidence archiving
Page copies captured over Tor

CUSTOMER INSTANCE

Your assets
Domain, brand, VIP, supplier

Findings and alerts
Matching, severity, status, evidence

Analysis and output
Local analysis, playbooks, reports

Sync and query

BRING THE EVENT INTO YOUR TEAM'S CHANNEL

Slack	Microsoft Teams	Jira	Webhook / SOAR	STIX / TAXII

E-mail through your corporate SMTP; administrator / viewer role separation; two-step verification with TOTP. Shared intelligence is also available as a STIX 2.1 feed over TAXII 2.1.

Default central sync is every 15 minutes. Tor connectivity runs centrally; the customer instance never connects to leak sites directly.

CHOOSE WHAT TO WATCH AND WHEN TO BE TOLD

24 alert categories. Notifications your way.

Set the notification state, minimum severity and e-mail preference for each category. Critical and high findings appear in the in-product alert stream.

Credentials	3
Brand	7
Assets	2
VIP	1
Payments	1
Dark web	1
Platform	1
Supply chain	8

30 sec

alert check cycle for new records

9 feeds

under freshness watch

Controls that reduce notification noise for the same recurring event, and separate findings for stalled feeds, keep the state of the monitoring chain visible too.

30 seconds is the alert monitor's default check interval, not the total time from an event occurring to a notification.

TAKE THE SAME FINDING TO DIFFERENT DECISIONS

A summary for management. Detail for the technical team.

Produce six report types as PDF in Turkish and English. Deliver them to the right team by download, e-mail or scheduled delivery.

GNSAC VIGIL

Executive

Risk picture and priorities

TR / EN

GNSAC VIGIL

Technical

Finding and review details

TR / EN

GNSAC VIGIL

Compliance

Compliance / audit review

TR / EN

GNSAC VIGIL

VIP

Per-person exposure

TR / EN

GNSAC VIGIL

Vendor

Supplier intelligence

TR / EN

GNSAC VIGIL

Brand

Brand threats and findings

TR / EN

SCHEMATIC VIEW OF THE REPORT TYPES

Fix the period

Credential, leak, IOC, vulnerability and brand-threat counts at report time are stored.

Compare the change

The next report is compared with the previously stored period; the first report states the baseline scope.

Executive, Technical, Compliance, VIP, Vendor and Brand reports serve different review needs within one platform.

GNSAC

VIGIL

Evaluate it with your own organisation’s risk.

Start with your domain. Review a leak, a brand threat or a supplier finding together with its source and evidence.

01 Add and verify your domain.

02 Define the scan and monitoring scope.

03 Review a finding and move it into the response flow.

04 Report the outcome; compare it with the next period.

DEMO AND CONTACT

GNSAC Bilişim Teknolojileri Ltd. Şti.

gnsac.com.tr

info@gnsac.com.tr

+90 216 706 40 65

support@gnsac.com.tr

WhatsApp +90 532 203 32 89

ISTANBUL OFFICE

Şefikbey Sokak, Archerson Köşkü No:3
Oda No:301, Zühtüpaşa, Kadıköy
34724 Istanbul, Türkiye

DUBAI OFFICE

Levels 41 & 42, Emirates Towers
Sheikh Zayed Road, Dubai, UAE

Product scope: 2026.08.24.279 / Intelligence volumes: GNSAC Vigil product documentation dated 20 September 2026.