GNSAC Vigil

External Threat Intelligence and Digital Risk Protection

Investigate credential exposure, underground activity, phishing infrastructure, brand abuse and externally observable technology risk in the context of your organisation.

Managed SaaS and on-premises deployment options, subject to agreed scope, architecture and security review.

- **Credential exposure**
- **Underground sources**
- **Phishing and brand**
- **External exposure**

External signals need organisational context.

Security teams already have extensive internal telemetry. Vigil adds an external intelligence layer for signals that may appear beyond the customer perimeter and correlates them with an authorised organisational scope.

1 Exposed identities

Collected stealer-log, combolist and breach data may contain corporate identities, passwords, tokens or session context that warrants investigation.

2 Underground activity

Selected forums, marketplaces, lawfully accessible messaging communities and leak sites may surface access offers, data-sale claims or relevant actor discussion.

3 Phishing and brand abuse

Certificate records, look-alike domains, phishing URLs and fake pages can provide evidence of infrastructure that imitates an organisation or its services.

4 External technology and third parties

Internet-facing assets, observed technologies, vulnerability context and supplier references can supplement internal inventories and periodic assurance reviews.

Relationship to the SOC / CSIRT

Vigil supplements existing security operations; it does not replace them. Internal logs and events remain with the customer SOC / CSIRT. Vigil contributes external findings and available source context through supported investigation and integration workflows.

From external signal to a reviewable finding.

Collection volume is not the outcome. The operating model is designed to preserve source context, apply the customer-approved scope and route prioritised findings into a repeatable investigation process.

1 Collect

Ingest selected external sources and intelligence feeds under defined legal, ethical and operational controls.

2 Match

Correlate observed records with authorised domains, identities, brands, executives, suppliers and assets.

3 Prioritise

Use freshness, privilege, session context, infrastructure evidence and customer relevance to support triage.

4 Deliver

Present findings with available timestamps, source context and investigation history; route them through supported integrations.

Operating principles

Authorised scope

Customer-specific checks begin only after the monitored scope and authority are confirmed.

Evidence before assertion

Findings retain the context available from the source and indicate processing or review status.

Analyst review

Automated correlation supports triage; customer teams remain responsible for validation and response decisions.

Measured coverage

Coverage and alert timing depend on source availability, collection conditions, processing status and routing rules.

Six capabilities in one investigation workflow.

Each capability addresses a different external-risk domain while using shared watchlists, correlation, evidence review, case context and reporting.

1 Credential intelligence

Investigate exposed identities across collected stealer-log, combolist and breach datasets, including available source and session context.

2 Underground-source intelligence

Monitor selected underground sources and lawfully accessible messaging communities for relevant organisational references.

3 Phishing and brand protection

Review look-alike domains, certificate activity, phishing infrastructure, fake pages and available registration or hosting evidence.

4 External risk assessment

Run structured discovery and intelligence checks against customer-authorised domains and review prioritised remediation guidance.

5 Supply-chain and VIP monitoring

Use supplier, executive and brand watchlists to investigate relevant exposure and third-party references.

6 Reporting and workflows

Produce technical and management outputs from the same finding set and route supported alerts to operational tools.

Outputs

Finding records, technical reports, management summaries, indicators and supported API / workflow integrations. Exact outputs depend on the selected licence and agreed scope.

Deployment choices with documented controls.

Deployment, connectivity and data flows should be evaluated as part of the customer security review. The applicable order form and technical design define the selected model.

1 On-premises

Vigil can be deployed as an OVF / OVA appliance in a customer-controlled virtualisation environment. Monitored assets, findings and user activity are held in a customer-isolated database within that environment. Required connectivity and intelligence synchronisation are documented for review.

2 Managed SaaS

Vigil can be provided as a managed SaaS service where appropriate. Data location, retention, access, connectivity and support requirements are agreed during commercial and security scoping.

Control set for review

- Two-factor authentication and role-based access control
- Auditable user activity and investigation history
- Customer isolation appropriate to the selected deployment
- Architecture, connectivity and data-flow documentation
- Supported REST API, webhook and operational integrations where licensed
- Defined support and escalation arrangements in the applicable contract

Data-governance position

These controls can support data-governance, supplier-assurance and audit processes. Regulatory compliance depends on each organisation's implementation, policies, processing activities and legal obligations.

A controlled path into operational use.

Implementation is scoped around the customer environment, authorised watchlists, integrations, alert priorities and operating responsibilities. Timing depends on infrastructure readiness, approvals and complexity.

1 Scope and authorise

Confirm domains, identities, brands, executives, suppliers, source requirements and permitted assessment activities.

2 Review architecture

Agree deployment model, data location, connectivity, access controls, retention and security-review evidence.

3 Deploy and configure

Install or provision the service, create roles, import watchlists and configure collection and matching rules.

4 Tune and integrate

Set severity and routing rules, review representative findings and connect supported SIEM, SOAR, ticketing or collaboration tools.

5 Hand over operations

Confirm ownership, escalation paths, reporting cadence, training and acceptance criteria.

A buyer should confirm

- Which sources and regions are relevant to our requirements?
- What evidence is retained for each finding?
- Which data enters or leaves the selected deployment?
- Which integrations and API functions are included in our licence?
- What support hours, response targets and escalation paths are contracted?
- How will coverage, false-positive handling and operational outcomes be measured?

Evaluate Vigil against your environment.

A focused product session should show the current interface, representative evidence, investigation workflow, deployment choices, supported integrations and the commercial scope relevant to your organisation.

1 Product review

Walk through current modules and representative alert, investigation and reporting workflows.

2 Methodology review

Examine source context, matching logic, prioritisation factors and the limits of available evidence.

3 Technical review

Discuss deployment, connectivity, access control, data location, retention and supported integrations.

4 Commercial scope

Confirm monitored entities, users, scans, reports, API access, support and any customer-specific work in the quote and order form.

Important limitation

No cybersecurity platform can guarantee that every threat, exposure or incident will be detected or prevented. Product coverage and timing depend on the contracted scope, source availability, processing status, selected deployment and configured routing rules.

Request a product session

Customer-domain assessments are performed only after scope and authorisation are confirmed.

sales@gnsac.com.tr

support@gnsac.com.tr

+90 216 706 40 65

https://gnsac.com.tr