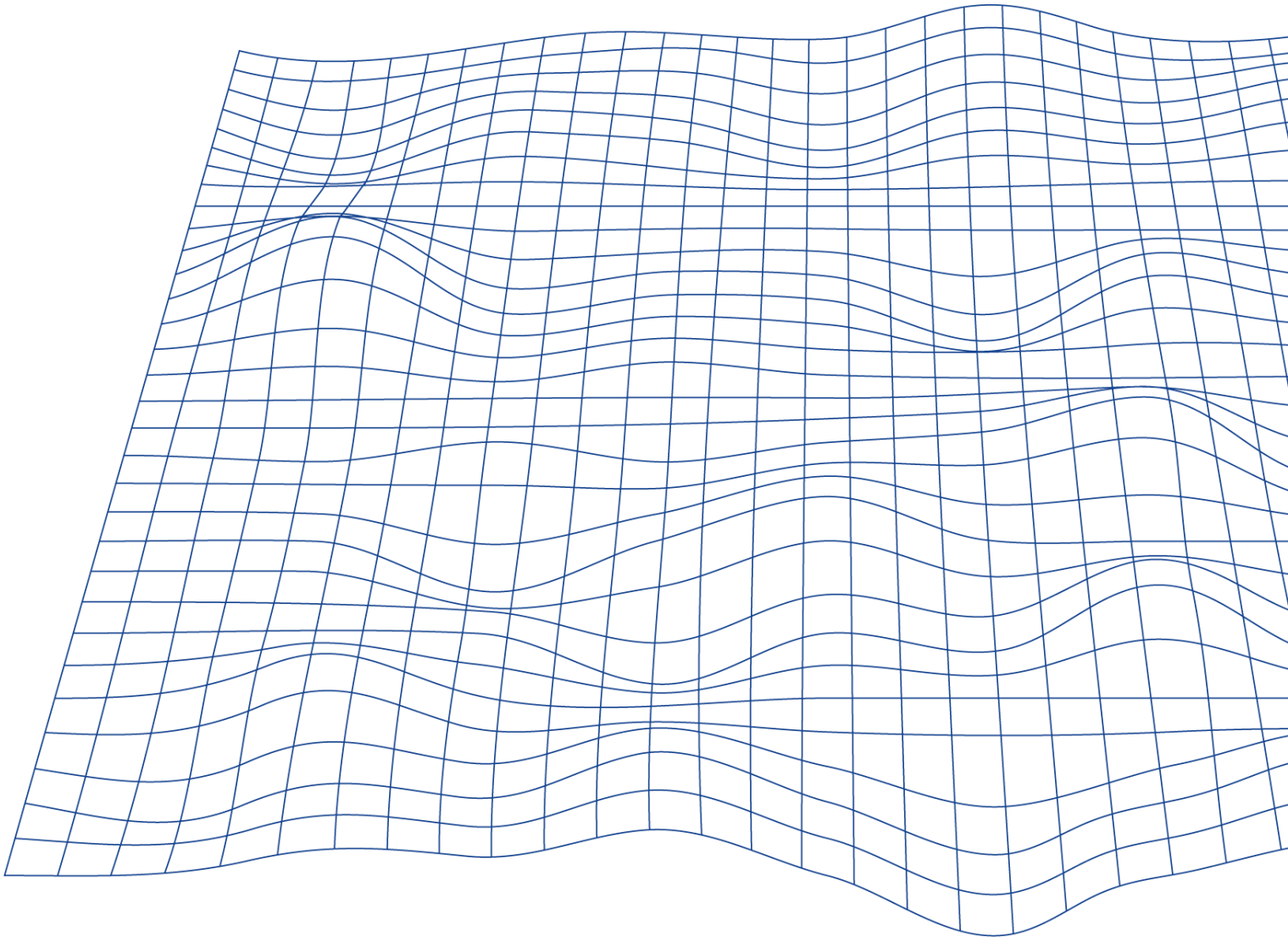
SecAlliance

G-Cloud 15

ThreatMatch

Service Definition



1. Introduction

This document defines the ThreatMatch service provided by SecAlliance. It describes the scope of the service, how it is delivered and supported, the underlying technical and security controls, as well as service levels, constraints, and exit arrangements.

The intended audience is customer security, procurement, risk management and IT teams who require a clear understanding of how ThreatMatch operates and how it integrates into their environment.

2. Service Overview

2.1 Service Description

ThreatMatch is SecAlliance's cloud-based secure threat intelligence platform used to deliver finished intelligence products, provide access to live data feeds, facilitate customer support requests, and support information sharing through management of community groups. ThreatMatch is provided as a multi-tenant Software-as-a-Service (SaaS) platform.

2.2 Core Components

ThreatMatch consists of the following key features:

Threat Alerts – Curated, ranked by severity, and mapped to your Intelligence Requirements. Supports incident response and helps improve defences over time by learning from past attacks.

MITRE ATT&CK® Integration – All content aligned with MITRE techniques, tactics, and sub-techniques.

Control & Sharing – Decide what to share, with whom, and when.

Collaboration Tools – Ask the Analyst, comments, chat, and forums for direct interaction.

Profiles & Scenarios – In-depth actor profiles, malware, incidents, and attack scenarios.

Reports – Regular threat intelligence and bespoke client reporting.

Custom Content – Create and share your own alerts, profiles, or incidents.

IOCs – integrated into each alert, and available as block lists and research lists via API

Asset Registry – keep your assets and key words up to date - anytime

Integrations – API access with STIX 2.1, MISP, TAXII Server and JSON feeds.

2.3 Service Modules Delivered via ThreatMatch

ThreatMatch is the primary delivery channel for the following service modules (where purchased by the customer):

Digital Risk Protection Services (DRPS)
Protects against credential exposure, dark web threats, code leaks, data loss and monitors the organization's digital footprint.

- Dark Web Coverage - Monitors forums, marketplaces, and telegram communities for threats targeting your organization
- Data Leak Detection - Detects unauthorized exposure of proprietary code and intellectual property
- Compromised Credentials - Credentials related directly to customer-base or employees
- Supply Chain Breach Alerts - Monitors for attacks, breaches or vulnerabilities in your supply chain

Continuous monitoring of surface, deep and dark web sources for:

- Compromised credentials (employees and customers where applicable)
- Data leaks and exposure of proprietary code or sensitive data
- Brand abuse, phishing and impersonation infrastructure

External Attack Surface Management (EASM)
Provides continuous alerting into an organization's external digital footprint, helping security teams prioritize and remediate risks.

- Assessment & Prioritization - Enables organizations to secure their digital perimeter and minimize attack vectors
- Prioritization - Evaluates vulnerabilities and exposure and provides threat severity scoring to inform decision making

Domain & Brand Intelligence
Monitoring and take down of domains, social media or app stores that either infringe on the brand of an entity or are used as attack infrastructure against it.

- Domain & Brand Monitoring Service - Detects domain abuse, typo squatting, brand impersonation, phishing threats in real time, and identifies fake websites, social media accounts and unauthorized brand usage
- Take Down - Global Coverage - we coordinate with local authorities and registrars that have the legal authority to enforce takedowns

Cyber Threat Intelligence

Delivers sector focused intelligence, indicator of compromise (IOC) feeds, geopolitical reporting, and threat actor and malware profiling.

Cyber Defence Feed
Delivery of high-confidence and comprehensive indicator feeds (IP, domain, URL, etc.) suitable for use in security tools for blocking, alerting and investigation.

Payment Fraud Intelligence
Advanced intelligence feed providing real-time data on identified compromised

payment cards. Enables financial institutions to proactively block fraud and support investigations.

Analyst as a Service (AaaS)

Provides an Intelligence function with surge capability to directly ask short or long form questions of our intelligence team and consultancy as well as request bespoke monthly intelligence reports.

- Requests for Intelligence (RFI) - The RFI service allows customers to request research or investigative work directly from our team. RFIs are based on a token-based subscription, allowing organizations to request tailored intelligence products based on their specific needs.
- Bespoke Monthly Reports – Allows customers to directly dictate the required format and content for intelligence reports tailored to their organisation.
- Intelligence as a Service (IaaS) – A force multiplier that enables customers to request and utilise dedicated and highly skilled analysts to support or enhance their existing internal Cyber Threat Intelligence (CTI) capability.

Vulnerability Intelligence

Continuous tracking and analysis of vulnerabilities, prioritising them based on real-world exploitation and risk impact. Customers receive tailored alerts and mitigation guidance through automated feeds and expert analysis.

- Alerts - Real-time updates on vulnerabilities, exploit techniques, threat actor campaigns and mitigation strategies
- Threat Actor Monitoring – Tracking of active exploitation trends and determining if threats are coming from known actors
- Mitigation Strategy - Providing security teams with tailored guidance based on their technology stack

Physical Intelligence

A continuous intelligence feed covering physical security threats, including crime, and protest activity. Provides real-time monitoring of executive safety, group dynamics, and individual sentiment analysis.

- Physical Monitoring - Monitors organised crime, violent incidents, and mass disruption events affecting operations. Tracks conventional crime, extremist threats, and potential terror activities
- Protest Activity Analysis - Monitors demonstrations, activist movements and trends
- Sentiment Monitoring - Identifying online or social media campaigns that could have a negative impact on the organisation, associated brands or senior executives. Also includes disinformation monitoring and alerting
- Executive Monitoring - Continuous executive risk analysis including travel related threats. Also provides the option of standalone point in time executive vulnerability assessments (EVA) that enable baseline visibility into online executive exposure

Requests for Intelligence (RFI)
On-demand short- and long-form intelligence tasks submitted via ThreatMatch to SecAlliance's analyst team, with delivery through the portal as structured reports or briefings.

The modules active for a given customer are defined in the customer's order form or statement of work.

3. Service Boundaries and Customer Responsibilities

3.1 In-Scope

ThreatMatch service includes:

- Provision and operation of the ThreatMatch platform and underlying infrastructure
- Configuration and operation of subscribed monitoring and intelligence modules
- Ingestion, processing and enrichment of data from OSINT, technical and other sources
- Delivery of alerts, reports, feeds and other outputs via the portal and agreed channels
- User management interfaces and, where applicable, integration with customer identity providers
- Support, incident handling and platform maintenance as described in this document

3.2 Out-of-Scope

Unless explicitly contracted, ThreatMatch does not include:

- On-site incident response or hands-on-keyboard compromise remediation
- Operation or tuning of customer-owned security tools (SIEM, SOAR, EDR, etc.)
- Changes to customer infrastructure, networks or endpoints
- Legal, HR or regulatory advisory services beyond the intelligence content itself
- Custom software development or bespoke integrations outside standard interfaces

3.3 Customer Responsibilities

Customers are responsible for:

- Designating primary and backup points of contact for operational and security communications
- Providing and maintaining up-to-date monitoring scopes (domains, IP ranges, brands, suppliers, BINs, etc.)
- Maintaining their own internal processes to triage and act on ThreatMatch alerts and reports

- Ensuring network and security controls allow access to ThreatMatch (e.g., allowlisting required domains/IPs)
- Managing their own user accounts and access rights within agreed governance, where self-service is enabled
- Meeting their own regulatory and policy obligations when using intelligence produced via ThreatMatch

4. Service Architecture, Hosting and Locations

4.1 Hosting Model

ThreatMatch is delivered as a cloud-hosted SaaS platform deployed in secure data centres operated by third-party cloud providers. The platform uses high-availability configurations and load-balanced services to provide resilience against component failures and to support scaling under increased demand.

4.2 Data Location

Customer data is stored and processed in designated regions aligned with contractual and regulatory requirements. Specific region(s) applicable to each customer are documented in the relevant agreement or order form.

4.3 Resilience and High Availability

ThreatMatch is architected with:

- Redundant instances for critical components to avoid single points of failure
- Automated health checks and failover mechanisms to maintain service continuity
- Autoscaling capabilities (where supported) to handle load spikes, e.g., during major security incidents

System uptime target for the platform is a minimum of **99.7%** per year, including planned maintenance.

5. Data Management, Backup and Disaster Recovery

5.1 Data Types

ThreatMatch processes and stores, as applicable:

- Customer account and user profile data
- Configuration data (watchlists, monitoring scopes, rules)
- Intelligence outputs (alerts, reports, artefacts, indicators)

- Operational logs and audit trails
- Supporting reference data used in intelligence production

5.2 Backup

ThreatMatch uses regular automated backups for critical data stores, including:

- Scheduled database and configuration backups
- Backups of stored intelligence artefacts and files
- Integrity checks to detect backup corruption

Backup retention is aligned with internal data retention and regulatory requirements. Backups are stored securely and protected with appropriate access controls and encryption.

5.3 Restore and Disaster Recovery

In the event of data corruption or infrastructure failure:

- Data is restored from the most recent valid backup consistent with the Recovery Point Objective (RPO) defined in internal procedures.
- The ThreatMatch platform is recovered in accordance with the organisation's disaster recovery plan.

The **Recovery Time Objective (RTO)** for restoring customer access to the ThreatMatch portal following a major incident that renders it unavailable is **within 4 hours**.

Critical functions and recovery procedures are periodically tested as part of the wider business continuity and disaster recovery programme.

6. Onboarding and Offboarding Support

6.1 Onboarding

Standard onboarding for a new ThreatMatch customer includes:

1. **Kick-off and Planning**
   - Confirming scope, modules, use cases and points of contact.
   - Agreeing timelines and responsibilities.
2. **Technical Setup**
   - Provisioning the tenant, initial administrator accounts and access controls.
   - Configuring SSO/identity integration where applicable.
   - Support for setting up API or feed integrations to customer systems (e.g., SIEM/SOAR/email).
3. **Monitoring Scope Configuration**
   - Collation of technology stack details for inclusion on a customer specific asset registry. Includes: domains, IP ranges, technologies (types and versions), brands, suppliers, payment card BINs and other assets that are to be monitored as part of the service.

- Defining alerting preferences, severity thresholds and escalation contacts.

4. **Validation and Go-Live**
   - Conducting basic user and organisation functional checks and sample alert validations.
   - Confirming customer satisfaction prior to agreed ‘go-live’ date
5. **Training and Handover**
   - Providing user training and/or documentation.
   - Handing over to business-as-usual operations and support.

A typical onboarding timeframe is agreed per customer based on complexity and modules purchased.

6.2 Offboarding

On termination or non-renewal:

1. **Access Wind-Down**
   - Coordinated disabling of user access at or shortly after contract end date.
2. **Data Export**
   - Provision of reasonable assistance to export customer data (alerts, reports, watchlists and relevant configuration) in commonly-used formats (e.g., CSV, JSON, PDF), via the portal or through a managed export.
3. **Data Retention and Deletion**
   - Retention of customer data for a defined period after termination to allow export (as specified in agreement), followed by deletion in line with internal policies and legal requirements.
   - Backups containing customer data are expired and deleted on their normal lifecycle schedule.

Confirmation of data deletion can be provided upon request where appropriate.

7. Service Constraints, Service Levels and Support

7.1 Service Constraints

- ThreatMatch is a multi-tenant SaaS platform; deep customisation of core workflows, data models or UI is not supported.
- Configuration is available via standard options (e.g., watchlists, alert thresholds, dashboards) rather than bespoke code changes.
- Certain advanced features or integrations may require separate scoping and agreement.

- Use of the service is subject to fair usage principles; excessive or abusive API or data usage may be subject to rate limiting or additional terms.

7.2 Maintenance Windows

- Planned maintenance is scheduled during predefined maintenance windows, typically outside standard business hours in the relevant region to minimise impact.
- Planned maintenance that is expected to significantly impact availability or functionality is communicated to customers in advance through agreed channels (e.g., email, portal notifications).
- Short maintenance activities that do not materially affect service may be performed without prior notice.

7.3 Availability

- Target platform uptime is **99.7%** per year, including planned maintenance windows.
- Where internal or external incidents undermine this target, incident and post-incident processes are triggered to restore service and prevent recurrence.

7.4 Performance

ThreatMatch is designed to:

- Handle at least **1,000** simultaneous user sessions without degradation of core portal functionality under normal operating conditions.
- Provide responsive UI performance and timely alert and report delivery under typical workloads.

Performance may vary depending on customer network conditions, integrations and workload characteristics.

7.5 Support Hours and Contact Channels

Support for ThreatMatch includes:

- A central support contact (e.g., ticketing system/email) for incident reporting and service requests.
- Defined support hours and any extended or on-call arrangements as agreed in the contract or service schedule.
- Clear incident severity classification and handling procedures.

Specific hours (e.g., business hours vs. 24/7 for critical incidents) are set out in the customer's agreement or service schedule and may vary by region and service tier.

7.6 Incident Management

Incidents affecting ThreatMatch are classified by severity, for example:

Severity 1 – Critical business impact

- Complete unavailability of the ThreatMatch portal for all customers.
- Incidents leading to confirmed or suspected severe data exposure.

Severity 2 – Some business impact

- Degraded performance or partial loss of functionality affecting multiple customers but with workaround available.

Severity 3 – Limited impact

- Issues affecting a single customer or minor non-service-critical defects.
- For Severity 1 and Severity 2 incidents:

An incident manager is appointed and incident handling follows a defined response, communication and escalation process.

Customers are kept informed at regular intervals until resolution.

A post-incident review may be produced for significant events.

8. Security

8.1 Security Governance

ThreatMatch is operated within a formal information security management framework aligned with recognised standards. Security controls cover people, processes and technology and are regularly reviewed.

8.2 Secure Development and Change Management

ThreatMatch is developed and maintained following a documented secure software development lifecycle.

Secure coding practices, code reviews, and testing (including security and vulnerability testing where appropriate) are carried out.

Changes are managed through a formal change management process including impact assessment, testing, approval and, where needed, rollback planning.

8.3 Access Control and Authentication

- Logical access to ThreatMatch is restricted based on the principle of least privilege.
- Authentication is required for all users; multi-factor authentication (MFA) is supported or can be enforced where available.
- Integration with customer identity providers (e.g., SSO using standard protocols) is supported where agreed.
- Role-based access controls within ThreatMatch are used to assign appropriate permissions (e.g., administrators, analysts, read-only users).

8.4 Data Protection and Privacy

- Data in transit between customers and ThreatMatch is protected using strong encryption (e.g., TLS).
- Data at rest is stored using appropriate encryption and secure storage mechanisms.

- Personal data and sensitive information are processed in accordance with applicable data protection laws and internal data protection policies, including data minimisation and purpose limitation.
- Data retention schedules are applied in line with contractual, legal and operational requirements.

8.5 Infrastructure and Operations Security

- Production environments are segregated from development and test environments.
- Infrastructure is hardened following secure configuration baselines.
- Protection mechanisms are in place to detect and mitigate malware and malicious code.
- Logging and monitoring are implemented to detect anomalous activities; security events are handled via defined incident management procedures.

8.6 Vulnerability and Patch Management

- Regular vulnerability scanning and security assessments are performed on relevant components.
- Identified vulnerabilities are triaged and remediated in accordance with defined risk-based timelines.
- Patches and updates are deployed through controlled procedures to minimise service impact.

8.7 Resilience to Attacks

- DDoS mitigation, rate limiting and other controls help protect ThreatMatch from large-scale denial-of-service attacks and abusive use of APIs.
- Privacy-by-design and data anonymisation techniques are applied where appropriate to protect user and customer data.

9. Outage and Maintenance Management

9.1 Detection and Response

- Continuous monitoring of key ThreatMatch components and services is in place.
- Alerts from monitoring systems trigger investigation and response by operations personnel.
- For outages or significant performance degradation, incident processes are initiated according to severity classification.

9.2 Communication During Incidents

- For significant incidents, customers are informed via agreed channels (e.g., email notifications, portal banners or a status page).
- Communications include initial notification, periodic updates and notice of service restoration.
- For major incidents, a summary or post-incident report may be provided.

9.3 Post-Incident Activities

- Root cause analysis is performed for major incidents.
- Lessons learned are used to improve processes, monitoring and controls and to reduce the risk of recurrence.

10. Access to Data and Exit Management

10.1 Data Access During Contract Term

- Customers may export their data through self-service functionality or via a managed export process within a defined period.
- Data is provided in commonly used formats suitable for ingestion into customer systems.

10.2 Data Export at Exit

Upon termination or expiry of the service:

- Customers may export their data through self-service functionality or via a managed export process within a defined period.
- Data is provided in commonly used formats suitable for ingestion into customer systems.

10.3 Data Deletion

- After the export window, customer data is deleted from active systems in line with data retention and deletion procedures.
- Residual data in backups is removed as backups reach the end of their retention period.
- Deletion processes are designed so that customer data is no longer accessible beyond justified technical residuals.

11. Technical Requirements

11.1 Client Requirements

Use of supported, up-to-date web browser versions (e.g., current and prior major releases of mainstream browsers).

Reliable internet connectivity with sufficient bandwidth and acceptable latency for web application usage.

Configuration of local security controls (proxy, firewall, endpoint protection) to allow access to ThreatMatch endpoints.

11.2 Network and Integration Requirements

Allowlisting of ThreatMatch domains/IP ranges and ports as communicated during onboarding.

For feed/API integrations, the ability to consume data in supported formats and protocols (e.g., HTTPS-based APIs or standard feed formats).

Secure management of any credentials, keys or certificates used to integrate with ThreatMatch.

11.3 Identity and Access Integration

Where SSO is configured, integration with the customer's identity provider using supported protocols and standards.

Provisioning and deprovisioning of users according to agreed processes (manual or automated, where available).

12. Document Governance

This service definition is reviewed periodically to ensure it remains accurate and aligned with the ThreatMatch service, internal policies and regulatory requirements.

Material changes to the service that affect customers will result in an updated version of this document being made available.