

CORE FUNCTION BRIEF

Third-Party Add-ons Marketplace

A core function of the ClearSkies iSOC platform

A governed catalog of third-party connectors, monitored live and flagged before a feed goes dark.

Contents

1 Executive Summary

2 Why Ad Hoc Integration Falls Short

Integration built one connector at a time
Outages discovered after the blind spot opens
Breadth without depth, or depth without breadth
A flagged risk with nowhere to go
The cost of the workaround

3 How the Marketplace Works

The five stages
How a connector is judged

4 The Marketplace in the Platform

What it draws on, what it writes back, and what it does not do
A worked example
Delivery across many tenants

5 Schema and Ingestion Framework Alignment

6 Questions Raised in Evaluation

7 The Benefits

At a glance
What changes, and for whom
What sets it apart

8 Summary

SECTION 1

Executive Summary

IN ONE SENTENCE.

The Marketplace is the core function that catalogs, connects, monitors and flags the health of every third-party integration, so visibility grows through a governed, repeatable framework rather than one bespoke connector at a time.

A detection is only as good as the data behind it. Bringing a new tool into a security operation conventionally means bespoke engineering, an ad hoc script or a professional-services project for each source, so onboarding takes weeks and produces something only the person who built it can maintain. A feed can degrade or a credential can expire silently, and nobody notices until an incident review asks why a source went dark. And a wide catalog of connected-but-unused sources is integration sprawl, while a narrow, deep view misses whole categories of attacker path.

The Marketplace answers this with a five-stage mechanism. A catalog of more than 600 integrations is organized across nine categories, so an architect can see what is connectable and what it would add before committing engineering time. A connection is provisioned as a governed link, standardized to a common schema, authenticated with least-privilege credentials, and versioned, replacing one-off integration work. Every active connector carries a live health signal, and a failure-risk model flags a degrading connector before it fails rather than after.

Breadth and currency are always assessed as a pair, because a view that is wide but stale, or current but narrow, is still a blind spot. A Resource Center of guides, runbooks and reference material lets an administrator configure and troubleshoot a connector without depending on whoever originally set it up.

THE FUNCTION IS PRECISELY SCOPED.

The Marketplace catalogs, connects and monitors third-party integrations. It does not decide how urgent a security alert is, which is the Risk Scoring Formula. It does not execute a remediation such as renewing a credential or throttling traffic, which is SOAR or an administrator acting on a published flag. And it defines no commercial integration tier or price. Each of those is a separate decision or a separate core function.

Five stages

Discover, connect, monitor, predict, publish

600+ integrations

Cataloged across nine categories

Coverage and freshness

Assessed as a pair, never as a single number

Representative of the function's design. Which connectors are enabled, the remediation configured for a flag and the report cadence are set per tenant.

SECTION 2

Why Ad Hoc Integration Falls Short

Integration is underinvested relative to the rest of the security operation, and the consequences surface as a blind spot rather than as a single visible failure. Four failure modes explain why, and each is answered by a named stage of the mechanism in section 3.

2.1 Integration built one connector at a time

Each new source conventionally means bespoke engineering, an ad hoc script or a professional-services project, so bringing on a new tool takes weeks and produces something only its builder can maintain.

2.2 Outages discovered after the blind spot opens

A feed can degrade in volume or freshness, or a credential can silently expire, and nobody notices until an incident review asks why a source had no data for days.

2.3 Breadth without depth, or depth without breadth

A wide catalog of connected-but-unused sources is integration sprawl, cost and maintenance without security return, while a narrow, deep view of only a few tool categories leaves whole categories of attacker path unmonitored.

2.4 A flagged risk with nowhere to go

A connector approaching failure is only useful information if it reaches someone who can act on it. A risk noticed but not routed to an owner or a runbook is no better than no warning at all.

2.5 The cost of the workaround

The usual response is a dedicated integration engineer or a standing professional-services engagement whose job is to build and firefight connectors one at a time. Cost scales with the number of sources and the pace of vendor API changes, while the underlying problem, connections that are not standardized,

monitored or predicted, is untouched. The workaround also caps how far visibility can grow: adding a source means adding integration capacity in step, so the breadth of what a security operation can see is bounded by how fast it can build and maintain connectors rather than by what would be useful to watch.

Industry research on security operations consistently ties tool sprawl and integration complexity to operational cost, and separately finds a meaningful share of connected sources contributing nothing to detection, though the specific figures are not yet sourced for this brief.

SECTION 3

How the Marketplace Works

The Marketplace is one continuously operating mechanism native to the TDIR core, not a drawer of one-off integrations. A vendor API or telemetry source enters at one end, and a governed, monitored, self-documenting connection leaves at the other.

Figure 1. The five-stage catalog and connector mechanism.

3.1 The five stages

Each stage is named once here and referenced by name throughout the rest of this brief, paired with the failure mode from section 2 that it answers.

STAGE	WHAT HAPPENS	THE FAILURE MODE IT ANSWERS
Discover	The catalog is organized by category, network and firewall, endpoint and EDR, cloud and SaaS, identity, email, threat intelligence, posture, ticketing and notification, so an architect sees what is connectable before committing engineering time. That structure is what makes a gap visible as a gap rather than as an absence nobody thought to look for.	Breadth without depth, or depth without breadth
Connect	A connector is provisioned as a governed link: standardized to a common schema, authenticated with least-privilege credentials and key rotation, and versioned, replacing bespoke integration engineering.	Integration built one connector at a time
Monitor	Every active connector carries a live health signal, continuously comparing expected against actual data flow and volume.	Outages discovered after the blind spot opens

STAGE	WHAT HAPPENS	THE FAILURE MODE IT ANSWERS
Predict	A model scores each active connector for failure risk from flow metadata, credential state, capacity headroom and recent change context, flagging a connector before it degrades rather than after.	Outages discovered after the blind spot opens
Publish	Health, coverage, freshness and any at-risk flag are published into the shared model. This function does not itself renew a credential, throttle traffic or reconfigure a connector.	A flagged risk with nowhere to go

Predict hands off at the flag. What happens next, an automated renewal, a throttled poll or a routed troubleshooting task, is a decision SOAR or an administrator makes using the flag the Marketplace published.

3.2 How a connector is judged

Quality is measured rather than assumed, on definitions a provider can report and a customer can audit. The measures below are reported natively and per tenant, defined here because the same metric name is measured differently by different vendors. Target values are agreed per engagement rather than asserted.

MEASURE	THE DEFINITION USED	WHAT A POOR VALUE TRIGGERS
Coverage	Relevant tools and assets actively connected and feeding the platform, as a share of the in-scope catalog.	A prioritized onboarding review for the uncovered category.
Freshness	Average latency between an event occurring in a source and its normalized arrival.	A review of transport, moving a source from scheduled pull to streaming push.
Adoption rate	Connected sources actively contributing to detections, enrichment or response over a period, as a share of all connected sources.	A review of whether an unused source should be retired rather than maintained.
Prediction accuracy	Failure-risk predictions confirmed correct against the actual outcome, as a share of all predictions.	A retraining review of the model against recent misses.
Prediction lead time	Elapsed time between an at-risk flag and the connector's actual failure.	A review of whether the flag threshold fires early enough to be acted on.

MEASURE	THE DEFINITION USED	WHAT A POOR VALUE TRIGGERS
---------	---------------------	----------------------------

Wide but stale is still a blind spot. *Coverage and freshness are never read alone. A source that is connected but arrives with significant latency gives a false sense of visibility, and a current picture of two categories says nothing about the seven it does not cover.*

SECTION 4

The Marketplace in the Platform

4.1 What it draws on, what it writes back, and what it does not do

What it draws on. The third-party vendor's API or telemetry stream as the external source; the normalized entity model the Centric-AI Fabric carries, into which a connector's data is standardized; and each tenant's catalog of enabled integrations. Each is an input to a specific stage rather than a capability this function generates.

What it writes back. A connector's health, coverage and freshness status, and any at-risk flag, published into the shared model. SOAR consumes a flag where an automated remediation exists; otherwise an administrator acts on it through the Resource Center. The telemetry a connector delivers flows through the Centric-AI Fabric like any other source: this function's own contribution is the status of the connection, not the content it carries.

What it does not do. It does not decide how urgent a security alert is or who investigates it, and it does not renew a credential, throttle traffic or reconfigure a connector on its own authority. SOAR or an administrator makes that decision from the flag it publishes. It defines no commercial integration tier or price.

THE ONE DOCUMENTED EXCEPTION TO ONE-WAY REPORTING.

Where a third-party vendor exposes a response API, the connector the Marketplace governs can accept an instruction back from SOAR as well as send telemetry forward, unlike a native add-on's strict one-way relationship. The capacity belongs to the connector; the decision to use it belongs to SOAR.

4.2 A worked example

The chain below is illustrative and technically representative rather than drawn from a named engagement. A cloud connector approaches its API rate limit during a traffic spike, and its access token is due to expire within days. Monitor shows volume nearing the expected ceiling, Predict combines the rate-limit headroom, the token's age and the recent traffic pattern into a high failure-likelihood score,

and Publish surfaces the flag. Because this tenant has an automated renewal remediation configured, SOAR reads the flag and invokes it, throttling a lower-priority polling job to protect headroom. Without that remediation, the same flag routes to an administrator through the Resource Center with the guide for that connector attached. Both branches begin with the same flag, and the function's work ends there either way.

4.3 Delivery across many tenants

The catalog, the connector framework and the Resource Center serve every tenant from the same governed structure, so onboarding a source is repeatable rather than a bespoke build per customer, and a vendor API change is absorbed once in the connector version rather than separately in every tenant using that source. What travels between tenants is the catalog and the framework; what never travels is one tenant's credentials, telemetry or connector configuration.

Because the function is switched on with the platform rather than deployed separately, time to value is a matter of connecting sources rather than an onboarding project. In the first week, the catalog is available for review and the first connectors in a tenant's priority categories begin feeding the platform. Through the first month, coverage becomes visible and Predict accumulates enough flow history to be meaningful for that tenant's own sources. At steady state, prediction accuracy and adoption rate are tracked as ongoing measures.

SECTION 5

Schema and Ingestion Framework Alignment

The Marketplace does not map detection content and does not compute technique relevance, so MITRE ATT&CK plays no direct role for this subject and is not given a row below. The frameworks that matter here are the ones governing how a third-party source is standardized and ingested, which is what the Connect stage does.

FRAMEWORK OR STANDARD	ITS ROLE IN THE MARKETPLACE
OCSF	The common schema every connector standardizes to at the Connect stage. The platform's normalized model aligns to it rather than being it, which is a distinction an architect will ask about.
Syslog, CEF, LEEF and REST API	General collection formats supported across the catalog, together with the position on custom and AI-assisted parsers.
OpenTelemetry	Application and infrastructure telemetry ingestion, for the subset of the catalog built on it.

FRAMEWORK OR
STANDARD

ITS ROLE IN THE MARKETPLACE

STIX and TAXII

The connector format for the threat-intelligence category of the catalog. What happens to the content afterward, its curation and rating, belongs to the Threat Intelligence brief.

Support for a format is not compliance with an obligation. The platform states which schemas and transports a connector supports. It never states that supporting one makes an organization compliant with anything, and control-level framework mapping is held by the Regulatory Frameworks core function.

SECTION 6

Questions Raised in Evaluation

The questions below recur in buyer evaluations, each answered directly against the mechanism described in section 3.

QUESTION, AS A
BUYER ASKS IT

ANSWER

Does the Marketplace decide how urgent a degraded connector is, or route it to an analyst?

No. Connector health carries its own status model. An at-risk flag is consumed by SOAR where an automated remediation exists, or by an administrator through the Resource Center.

Does the Marketplace execute remediation itself, such as renewing a credential or throttling traffic?

No. It publishes the flag. SOAR or an administrator decides and acts.

Can a third-party integration receive instructions from the platform, or only send data?

Both are possible, depending on the connector. Sending telemetry is universal, and where a vendor exposes a response API the connector can also accept an instruction back from SOAR. This is the one documented exception to the platform's native add-on architecture.

Does the Marketplace define what a customer pays for different levels of integration?

No. Catalog depth available at a given platform tier is a commercial decision made elsewhere. This function governs and measures whatever connectors are enabled.

QUESTION, AS A
BUYER ASKS IT

ANSWER

How is a connected-but-unused source identified?

Adoption rate, defined in section 3.2, tracks the share of connected sources actively contributing to detections, enrichment or response, surfacing candidates for review or retirement.

What happens when a vendor changes its API?

The change is absorbed once in the connector version rather than separately in every tenant that uses that source, which is what the Connect stage's versioning exists for.

Can a tenant configure its own connectors, or must a provider do it?

The Resource Center's configuration guides support self-service setup. The same governed connector framework applies whether a tenant or a provider configures it.

SECTION 7

The Benefits

Integration is where a security operation either grows what it can see or spends its engineering budget keeping what it already has alive. The outcomes are countable: how much of the in-scope catalog is connected and current, how many degrading connectors were caught before a feed went dark, and how much of that took bespoke work.

7.1 At a glance

BENEFIT

WHAT PRODUCES IT

A new source is provisioned rather than engineered

Connect standardizes, authenticates and versions the link, replacing one-off integration work.

A blind spot is prevented rather than explained afterward

Predict scores a degrading connector and Publish surfaces the flag while there is still time to act.

A gap is visible as a gap

Discover organizes the catalog into nine categories, so an unmonitored category is a named absence.

A wide view cannot pass for a current one

Coverage and freshness, defined in section 3.2, are read as a pair and never as a single number.

BENEFIT	WHAT PRODUCES IT
A connector outlives the person who built it	The Resource Center carries the guides and runbooks that a bespoke integration kept in one engineer's head.
Visibility scales with the catalog, not with headcount	The same catalog and connector framework serve every tenant, and a vendor API change is absorbed once.

7.2 What changes, and for whom

A governed, monitored connector framework changes what each role spends time on, and what each role can rely on being current.

ROLE	WHAT CHANGES
Security architect	Sees what is connectable and what it would add before committing engineering time, rather than scoping a bespoke project to find out.
SOC analyst	Works from a live, current picture rather than discovering a blind spot in the middle of an incident.
Administrator	Self-serves setup and troubleshooting from the Resource Center rather than depending on whoever originally configured a connector.
Service provider practice lead	Repeatable onboarding and one console scale across every tenant, without bespoke integration engineering per customer.

7.3 What sets it apart

- **Governed, not bespoke.** Every connector is standardized, authenticated and versioned, so integration becomes a provisioning step rather than an engineering project with a single owner.
- **Failure flagged before it happens.** Predict surfaces a degrading connector while there is still time to fix it, so a blind spot is prevented rather than explained afterward in an incident review.
- **Breadth and depth measured together.** The two measures are read as a pair, so a wide-but-stale or narrow-but-current view is never mistaken for good visibility.
- **Self-service by design.** The Resource Center gives an administrator what a bespoke integration would otherwise need professional services for, so knowledge of a connector does not leave with the person who configured it.

The value in one line. Ad hoc integration buys visibility one connector at a time and pays for it forever. A governed catalog turns the same visibility into something that is provisioned, measured, and warned about before it fails.

SECTION 8

Summary

The Marketplace is how the platform turns a heterogeneous, third-party technology stack into governed, monitored visibility. It is one core function among twelve, scoped to a five-stage mechanism that runs continuously inside the TDIR core rather than as a drawer of bespoke, one-off connectors.

- ▶ Discover, connect, monitor, predict and publish replace ad hoc, one-connector-at-a-time integration.
- ▶ Every connector is standardized, authenticated and versioned, and its health is tracked live.
- ▶ Failure risk is flagged before a feed goes dark, and the function publishes the flag rather than acting on it unilaterally.
- ▶ Breadth and currency are assessed together, and a Resource Center supports self-service configuration and troubleshooting.
- ▶ The function catalogs, connects and monitors third-party integrations, and leaves security urgency, response and commercial structure to the functions and decisions built for them.

Forward-looking statement: any statement about future capability is forward-looking and non-binding, and capability described in the present tense is capability available at the publication date, subject to the deployment configuration in force. Catalog scale and parser coverage change as vendors and formats change.