SYMBEEO

PUBLIC

DESIGN STUDY

SIEM and observability on Splunk for a 24×7 operations floor

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Security	Global Service Providers	Managed service provider
DOCUMENT	VERSION	DATE
SEC-004	1.3	Oct 10, 2026

WRITTEN BY

David Morgan, Principal Security Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	SEC-004	Version	1.3
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.2, Sep 27, 2026
Capability	Security	Industry	Global Service Providers
Author	David Morgan	Role	Principal Security Architect
Credentials	CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP, Adopting Zero Trust (Forrester)		
Approval	Approved by Edwin Ozer, Founder, Oct 10, 2026. Issued by Symbeeo, Oct 10, 2026. Design study: every figure is vendor-published, a design target or a marked assumption.		
Sign-off	"An engagement under this design is signed by the practice lead before any build proceeds."		

Contents

1 · Scope 3
1c · Public implementations this design follows 4
2 · Requirements register 4
3 · Architecture overview 5
4 · Design by subsystem 6
5 · Failure behavior 7
6 · Limits 7
7 · Lessons learned 7
8 · The author 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure read from the vendor's own current page on Sep 18, 2026 · [S*] figure from the vendor's page summary where the page itself could not be opened · [A] design assumption for the typical buyer, to be confirmed by the signing engineer · [T] design target taken from the design's stated outcome or derived from it. Every figure carries one tag. No figure comes from any prior engagement, file or asset. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

Table 1. Revision history

Date	Version	Change
Sep 18, 2026	1.0	First issue.
Sep 20, 2026	1.1	Public implementations added; figures reconciled with published sources.
Sep 27, 2026	1.2	Figures and platform details rechecked against published sources.
Oct 10, 2026	1.3	Approval line now reads: approved by the Founder, issued by Symbeeo. David Morgan remains the author.

1 · Scope

Who it is for. The head of the SOC at a managed service provider whose analysts work three shifts across a floor, who needs one platform for detections and one view of the network path to every customer-facing service, sized for the next two years of customer growth.

Typical buyer [A]. A managed service provider running a 24×7 SOC for 60 customers, 14 analysts across three shifts, 3.2 TB/day of security log today growing to a 4 TB/day design point, 40 customer-facing services (portals, APIs, hosted desktops) delivered from two data centers and one public cloud region.

What is in. Splunk Enterprise indexing tier sized for 4 TB/day; Splunk Enterprise Security 8 with detection content mapped to MITRE ATT&CK; the analyst queue and case workflow; ThousandEyes Enterprise and Cloud Agents for every customer-facing service; alert routing from ThousandEyes into the SOC queue. **What is out.** Log source onboarding for each customer beyond the standard set; SOAR playbook authoring beyond the starter set; the ticketing system.

Assumptions. Splunk Enterprise on-premises in the provider's data centers [A]; Enterprise Security Premier edition for native SOAR and UEBA [A]. ThousandEyes is the path-visibility vendor [A]. Retention 90 days searchable, 365 days archived [A].

Related documents, read Sep 18, 2026. Splunk Enterprise reference hardware (Splunk Enterprise 10.0), https://help.splunk.com/en/splunk-enterprise/get-started/deployment-capacity-manual/10.0/performance-reference/reference-hardware · Splunk Enterprise Security editions, https://help.splunk.com/en/splunk-enterprise-security-8/enterprise-security-editions · About Splunk Enterprise Security 8.1, https://help.splunk.com/en/splunk-enterprise-security-8/user-guide/8.1/introduction/about-splunk-enterprise-security · ThousandEyes Path Visualization, https://docs.thousandeyes.com/product-documentation/internet-and-wan-monitoring/path-visualization · ThousandEyes Enterprise Agents, https://www.thousandeyes.com/product/enterprise-agents · Splunk Validated Architectures, Distributed Clustered Deployment with SHC, Multisite (M4/M14) (Dec 10, 2024), read Sep 20, 2026, https://docs.splunk.com/Documentation/SVA/current/Architectures/M4M14 · Splunk for the MSSP: Technical Architecture white paper (PDF dated Aug 16, 2018, © 2018, WP-Splunk-MSSP-104), read Sep 20, 2026 and Sep 27, 2026, https://www.splunk.com/en_us/pdfs/white-paper/splunk-for-managed-security-service-providers-technical-architecture.pdf · ThousandEyes blog, a software-as-a-service company's network team on Enterprise Agents and Path Visualization (September 2018), read Sep 20, 2026, https://www.thousandeyes.com/blog/how-thousandeyes-saved-sanity-atlassian-network-team.

© 2026 Symbeeo. All rights reserved. · Public

1c · Public implementations this design follows

Deployment rows are real public deployments, each dated. Where no public deployment matches, the row is Vendor documentation: the vendor's document that this design, Symbeeo's own, is built on.

Table 2. Public implementations this design follows

Implementation	Who published it · date	What it settles for this design	URL
Vendor documentation. Splunk Validated Architecture M4/M14: multisite indexer cluster with search affinity and a search head cluster spanning two or more sites, under a cluster manager; ES on a search head cluster follows the vendor's SHC guidance	Splunk · Dec 10, 2024	R15 and §3: the indexer cluster plus three-member search head cluster across two data centers is the vendor's validated topology for strict availability, not this document's invention; the vendor recommends its own services for ES in this category	`https://docs.splunk.com/Documentation/SVA/current/Architectures/M4M14`
Vendor documentation. Splunk for the MSSP technical architecture: one dedicated index set per customer, customer-prefixed index names, sizing in reference indexers of about 300 GB/day under a stated search load	Splunk · Aug 16, 2018 (white paper PDF date)	R7, R8 and §4.6: per-customer indexes for attributable ingest are the vendor's MSSP model; the reference-indexer figure is the ceiling above this document's 150 GB/day assumption under ES search load	`https://www.splunk.com/en_us/pdfs/white-paper/splunk-for-managed-security-service-providers-technical-architecture.pdf`
Deployment. A software-as-a-service company placed Enterprise Agents (virtual appliance, Linux package, Docker) in every office, data center, PoP and cloud availability zone across 200+ VPCs and fed metrics by API into its correlation engine, using Path Visualization to locate loss	ThousandEyes · 2018-09	R12, R13 and §4.5: Docker Enterprise Agents at each provider location plus API and webhook export into a central tool is a published deployment on the same platform, at larger scale than 6 agents	`https://www.thousandeyes.com/blog/how-thousandeyes-saved-sanity-atlassian-network-team`

The vendor's 300 GB/day reference indexer sits above R7's 150 GB/day assumption, so R7 is conservative, not contradicted.

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Daily ingest design point	4 TB/day	[T]
R2	Ingest today and growth	3.2 TB/day; 4 TB/day reached in 18 months	[A]
R3	Detection content mapping	every enabled detection annotated to a MITRE ATT&CK technique	[T]
R4	Path visibility	every one of 40 customer-facing services under a ThousandEyes test with Path Visualization	[T]

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R5	Indexer reference hardware, high-performance	48 physical cores or 96 vCPU at 2 GHz+, 128 GB RAM, SSD hot/warm at 800+ sustained IOPS	[S] Splunk reference hardware
R6	Search head reference hardware, minimum	16 physical cores or 32 vCPU, 12 GB RAM, 300 GB dedicated storage	[S] Splunk reference hardware
R7	Ingest per indexer with ES searching	150 GB/day per indexer at the high-performance spec	[A]
R8	Indexer count	27 indexers for 4 TB/day at R7, plus 3 spare (replication headroom and burst margin) = 30	[A] derived from R1, R7
R9	ES edition and version	Enterprise Security Premier; ES 8.x, 8.6 or later on Splunk Enterprise, exact release set at staging	[S] ES editions; [S] ES 8.6 release notes `https://help.splunk.com/en/splunk-enterprise-security-8/release-notes-and-resources/8.6/splunk-enterprise-security-release-notes/release-notes-for-splunk-enterprise-security`, read Sep 26, 2026
R10	ES capabilities used	risk-based alerting, finding groups aligned to security frameworks, analyst queue in Mission Control, Splunk SOAR actions and playbooks, UEBA	[S] About ES 8
R11	Searchable retention	90 days hot/warm; 365 days archived	[A]
R12	Path tests	agent-to-server test per service from 6 Enterprise Agents and 6 Cloud Agents; a minimum of three tests per agent underlies Path Visualization	[S] Path Visualization, [A] agent counts
R13	Enterprise Agent placement	Docker on Linux in each data center and the cloud region; Catalyst 9300 hosting at the two largest customer edges	[S] deployment options, [A] placement
R14	Alert to queue	ThousandEyes alerts arrive in the ES analyst queue within 60 s	[A]
R15	Availability	search head cluster of 3; indexer cluster replication factor 2, search factor 2	[A]

Fifteen rows; six carry a vendor figure, six are design assumptions, three are design targets.

3 · Architecture overview

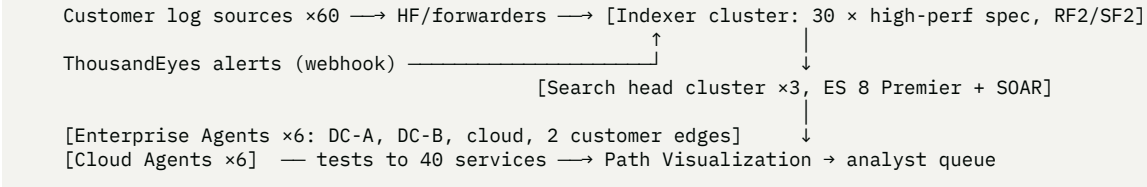


Figure 1. SIEM and service tests

© 2026 Symbeeo. All rights reserved. · Public

One indexer cluster sized to 4 TB/day, one search head cluster running ES 8 Premier, and a ThousandEyes test per customer-facing service whose alerts land in the same queue.

Table 4. Architecture overview

Role	Product (exact model)	Qty	Capacity used	Why this unit
Indexer	Splunk Enterprise indexer on the high-performance reference spec (48 cores / 128 GB / SSD 800+ IOPS)	30	4 TB/day ÷ 27 = 148 GB/day per indexer against R7; 3 spare	Vendor reference hardware [S]; per-indexer ingest assumed [A]
Search head	Splunk Enterprise search head, ES 8	3 (cluster)	14 analysts, 60 customer dashboards [A]	Vendor minimum plus headroom for ES [S]/[A]
SIEM application	Splunk Enterprise Security Premier, ES 8.x (8.6 or later)	1 license	4 TB/day	Native SOAR and UEBA in the edition [S]
Path visibility, provider side	ThousandEyes Enterprise Agent (Docker)	4	40 services × agent-to-server tests	Docker deployment option [S]
Path visibility, customer edge	ThousandEyes Enterprise Agent on Cisco Catalyst 9300	2	tests to the same 40 services	Catalyst 9300 hosting listed by the vendor [S]
Path visibility, outside-in	ThousandEyes Cloud Agents	6	40 services	1,085 vantage points in 276 cities available [S]

4 · Design by subsystem

4.1 Indexing tier.

30 indexers on the high-performance reference spec [S], indexer cluster with replication factor 2 and search factor 2 [A]. Hot/warm on local SSD at 800+ sustained IOPS [S]; cold to object storage after 90 days (R11). Rejected: mid-range spec (24 cores / 64 GB [S]) at twice the count — more chassis to run for the same ingest, and ES search load favors the larger node [A].

4.2 Search tier and ES 8.

Three-member search head cluster [A] running ES 8 Premier. The analyst queue in Mission Control replaces the older incident review page [S]; findings are grouped by rules aligned to common security frameworks [S], which is how R3 is met: every detection carries an ATT&CK technique annotation before it is enabled, and a detection without one fails the content review [A]. Risk-based alerting is the default alerting path [S]; raw notable-per-detection is off.

4.3 Detection content.

Starter set: Splunk-supplied content enabled per customer tier, then provider-authored detections in the same annotated format [A]. Detection review monthly; a detection with no true positive in 90 days is tuned or retired [A].

4.4 SOAR and UEBA.

Splunk SOAR actions and playbooks from the search head [S]; starter playbooks: enrichment, containment request to the customer's firewall team, case close [A]. UEBA on the identity sources of the 20 largest customers first [A].

4.5 ThousandEyes tests.

For each of the 40 services: an HTTP server or agent-to-server test from the 6 Enterprise Agents and 6 Cloud Agents, with Path Visualization on, so the SOC sees every node and link between agent and target and can separate forwarding

© 2026 Symbeeo. All rights reserved. · Public

loss from terminal loss [S]. Every service has a named owner and an alert rule; alerts post by webhook into ES as a finding source (R14).

4.6 Ingest pipeline.

Heavy forwarders per customer for parsing and filtering; universal forwarders on hosts; syslog receivers in pairs per data center [A]. Ingest metering per customer index so the 4 TB/day is attributable.

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
One indexer down	Cluster keeps RF2/SF2 with 29 members; searches complete; rebalance when the node returns	[A]
Search head member down	Two remaining members carry the SOC; ES continues	[A]
Ingest burst above 4 TB/day	Indexing queues fill first; forwarders buffer; license warning; no data dropped at the design margin of 3 spare indexers	[A]
Enterprise Agent host down	Cloud Agents still test the service from outside; alert raised on the agent itself	[A]
ThousandEyes webhook path down	Alerts remain in ThousandEyes; SOC dashboard shows the gap; polled on restore	[A]
Object storage for cold buckets unreachable	Searchable 90 days unaffected; archive writes queue	[A]

6 · Limits

- The 150 GB/day per indexer figure is an assumption, not a vendor figure; the first sizing test replaces it with a measured number.
- Cloud-only ES capabilities (the AI assistant, Attack Analyzer) are not in this on-premises design [S] editions page.
- ThousandEyes Path Visualization needs a minimum of three tests per agent [S]; single-test services do not get a path view.
- Detection coverage against ATT&CK is a mapping, not a measure of detection quality.
- Customer log onboarding beyond the standard source set is a per-customer task.

7 · Lessons learned

None yet — this is a design study; populated after the first build against it.

© 2026 Symbeeo. All rights reserved. · Public

8 · The author

WRITTEN BY

David Morgan

Principal Security Architect

CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP, Adopting Zero Trust (Forrester)

Signed off by Edwin Ozer, Founder.

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

SEC-004 · Version 1.3 · Oct 10, 2026