



GCSA 安全研究与产品白皮书

HoneyTrace 白皮书

蜜罐与攻击情报平台

以高交互遥测、统一分析与安全隔离降低蜜罐落地门槛，让真实攻击行为更快转化为可执行情报。

版本 V1.1 · 2026 年 7 月

Global Cyber Security Association (GCSA)

01 执行摘要

从“部署一个蜜罐”走向“持续运营一套攻击观测能力”。

HoneyTrace 是 GCSA 构建的蜜罐与攻击情报平台，将诱捕节点、协议交互、遥测接入、行为分析和节点运维整合为一套持续运营能力。平台既可使用默认 Shell 快速模拟类 Unix 环境，也可通过 Proxy 接入高交互目标，或使用大语言模型生成上下文一致的 SSH、Telnet 与 HTTP 响应。

平台接收连接、认证、命令、会话、文件、HTTP 请求与探测事件，在统一数据模型中完成归一化、去重、检索与聚合。运营人员可以从风险总览进入攻击来源、攻击者画像、会话时间线、端口探测与样本证据，并在同一后台完成节点安装、配置下发、版本更新和删除。

3 Shell / Proxy / LLM 模式	3 SSH / Telnet / HTTP 入口	1 一键安装与远程运维
多形态蜜罐 默认 Shell、Proxy 与 LLM 三类运行模式覆盖低成本部署、真实系统交互和自适应对话场景。	统一运营后台 节点、配置、版本、会话、凭据、扫描、样本、通知与导出集中管理，减少工具链割裂。	云端与私有部署 云端通过 GCSA SSO 自动创建隔离工作区；私有化部署保留独立数据、网络 and 运维边界。

本版本边界：提供个人工作区，不提供组织成员邀请、跨用户共享、工作区转移与统一账单；这些能力列入后续演进。

02 问题与设计原则

互联网攻击观测需要长期在线、可追溯、可隔离，而不是一次性演示。

传统蜜罐项目常见的问题并不只在传感器本身：部署脚本、节点身份、数据接收、日志检索、样本管理和账号权限往往分散在不同系统中。随着用户数与节点数增长，全局共享令牌、全局事件表或公共仪表盘都会放大误操作与数据越界风险。

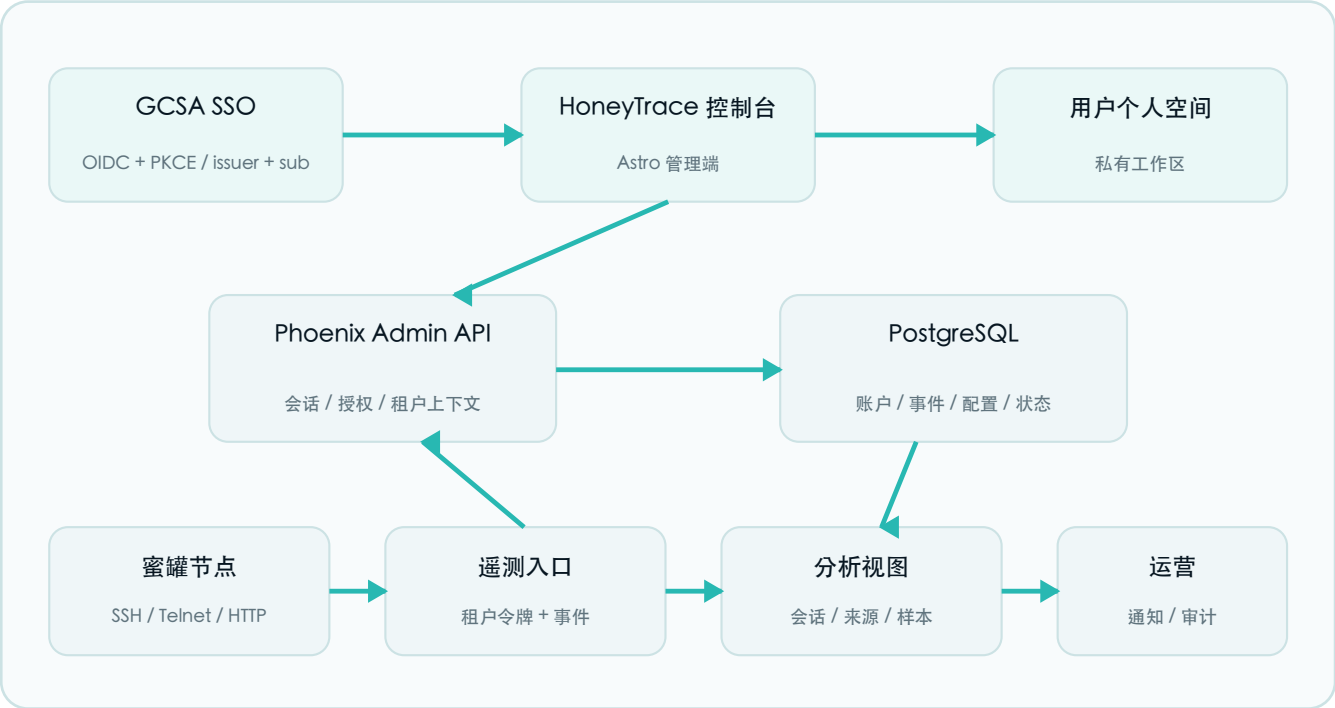
HoneyTrace 的首要目标，是在保持节点接入简单的同时，将身份、租户、数据和操作权限组合为同一条安全边界。

设计原则	落地方式	预期结果
身份先于数据	SSO 身份验证成功后先完成账户与工作区配置，再建立会话。	每次读取和写入都能获得明确租户上下文。
默认私有	个人 SaaS 空间禁止开启匿名仪表盘；公开能力仅保留给明确管理的 system 空间。	开放 SSO 注册不等于开放用户数据。
最小权限	普通成员可管理自己的蜜罐；许可证等平台级操作仅允许受控角色。	产品权限与平台运维权限分离。
向后兼容	历史事件默认迁移到 system；旧节点令牌继续映射到 system。	降低升级风险并保留既有服务连续性。
可验证	双用户隔离、同 subject 稳定映射、跨租户操作拒绝纳入自动化测试。	隔离从设计要求变成持续回归条件。

安全边界不是单一 SQL 条件。它由身份映射、请求上下文、令牌声明、存储分区、查询过滤、文件路径和管理权限共同组成。

03 总体架构

控制面、数据面与身份面相互解耦，又通过租户上下文贯通。



层级	核心组件	职责
身份面	GCSA SSO / OpenID Connect	完成注册、登录、令牌签发与可选角色声明；HoneyTrace 不接触用户密码。
体验层	Astro 管理控制台	呈现风险总览、会话、蜜罐、节点、配置、通知和样本；根据能力集隐藏无效入口。
控制面	Phoenix Admin API	验证会话与节点身份，建立 tenant_id 上下文，执行授权、配置与查询。
数据层	PostgreSQL + 租户样本目录	持久化账户、事件和设置；事件复合唯一键与样本目录均包含租户维度。
传感层	HoneyTrace 蜜罐节点	采集连接、认证、命令、会话、文件和服务探测遥测，并通过租户令牌上报。

部署拓扑可以把官方网站、管理端和 API 置于同一域名下，并由反向代理统一 TLS 与路由；生产数据库和样本卷独立持久化。

04 核心蜜罐能力总览

用三种运行模式适配不同交互深度、风险边界与部署成本。

HoneyTrace 不把蜜罐限定为单一模拟器。每个节点可根据目标环境选择 Shell、Proxy 或 LLM 后端，并独立设置 SSH、Telnet、HTTP 等入口。不同模式产生的遥测进入同一分析链路，因此运营团队可以在不更换后台的情况下组合多层诱捕策略。

运行模式	交互方式	主要能力	适用场景
默认 Shell	中交互命令模拟	类 Unix 文件系统、常见命令、认证与文件传输记录。	快速铺设、批量节点、稳定可控的基线诱捕。
Proxy	高交互真实后端	转发 SSH / Telnet 到单一目标或目标池，并保留会话观测。	需要真实系统行为、复杂工具链或高拟真环境。
LLM	自适应上下文响应	结合会话历史、身份、目录和协议上下文生成命令或 HTTP 响应。	长尾命令、动态对话、未知 Web 路径与研究场景。

协议入口	观测内容	共享能力
SSH	连接、用户名/密码、公钥、命令、TTY、上传与下载。	会话关联、来源分析、凭据统计、文件 SHA-256 与导出。
Telnet	连接、认证尝试、交互命令、持续时间与会话结束。	统一事件模型、命令序列、攻击者画像与节点归属。
HTTP / HTTPS	方法、路径、查询、请求体、Host、User-Agent、Cookie、Header 与源地址。	规则路由、静态响应、LLM 兜底、请求证据和来源完整性保护。

模式可以按节点独立配置。生产环境应依据网络隔离、算力预算、可接受交互风险和研究目标选择组合，而不是一味追求最高交互。

05 LLM 驱动的 SSH、Telnet 与 HTTP 蜜罐

让响应适应攻击者上下文，同时保留可审计、可限制的运行边界。

LLM 模式通过 HoneyTrace Bridge 将蜜罐协议上下文转换为兼容模型服务的请求，可连接 OpenAI 兼容接口或 Ollama。SSH/Telnet 会话会携带客户端地址、用户名、主机名、当前目录、session id 与 exec 模式，并维护对话历史，使后续命令能够延续前序状态，而不是每次生成互不相关的输出。

SSH / Telnet 环节	实现能力	安全与运营价值
建立会话	记录协议、来源、用户名和会话标识。	模型响应与真实攻击源、用户身份和完整会话绑定。
上下文生成	传入 hostname、cwd、exec 模式及历史命令。	支持目录变化、连续探测和多轮命令的一致性。
长尾命令	无需为每条命令预先编写固定脚本。	覆盖未知工具、组合命令和研究人员未预设的输入。
文件与执行	识别 SCP 上传及 exec 请求并写入会话证据。	连接命令行为、文件活动和后续执行路径。
交互保护	对 vim、top、tail -f 等全屏或长运行命令做保护处理。	避免无效输出持续占用模型上下文与资源。

HTTP 蜜罐可先按路径或正则匹配确定性响应，再把未命中的请求交给 LLM 插件。系统记录方法、URI、有限大小的请求体、Host、User-Agent、Cookie、Header、源 IP/端口及 HTTPS SNI；可信代理规则用于避免攻击者伪造 X-Forwarded-For。

模型 API Key 只保存在节点或服务端配置中。运营方应设置调用限速、超时、输入/输出校验和成本上限，并把 LLM 响应视为诱捕内容而非可信执行结果。

06 默认 Shell 与 Proxy 高交互模式

在可预测模拟与真实系统交互之间提供清晰选择。

默认 Shell 以中交互方式模拟 Debian 风格类 Unix 系统。它不直接执行攻击者命令，而是通过虚拟文件系统和命令处理器返回可控结果；Proxy 则把连接转发到隔离的真实或仿真后端，适用于需要更高拟真度的研究。

默认 Shell 能力	具体表现	产生的证据
虚拟文件系统	使用可定制文件系统镜像和文本命令内容模拟目录、权限与系统文件。	访问路径、文件操作、攻击者关注点。
命令模拟	覆盖常见 shell 命令、SSH exec 与交互式 TTY。	逐条命令、时间顺序、退出状态与完整会话。
文件捕获	记录 wget/curl 下载，以及 SFTP、SCP 上传。	文件名、来源、方向、SHA-256 与关联会话。
可回放日志	生成结构化事件及兼容 UML 的 TTY 日志。	用于时间线分析、会话回放和离线研究。
可定制表象	可修改主机名、提示符、文件内容和命令输出。	针对行业、设备或资产画像构建诱饵。

Proxy 选项	工作方式	部署注意
Simple	SSH / Telnet 连接转发到固定目标主机与端口。	后端必须隔离，限制出站网络并准备快照或重置机制。
Pool	从 QEMU 等仿真目标池分配会话后端。	适合并发隔离和会话后恢复，需要额外计算与编排资源。
统一观测	代理会话继续进入 HoneyTrace 事件与会话链路。	高交互不等于无边界，应审计逃逸、横移和资源消耗。

07 一键安装与蜜罐全生命周期管理

从生成安装命令到远程配置、更新和删除，都在同一控制面完成。

上线阶段	平台动作	节点结果
选择方式	后台选择 Docker 镜像或原生安装，并生成一键命令或完整脚本。	适配现有主机环境，无需手工拼接配置。
下载与安装	官方安装包按 amd64 / arm64 选择相应产物。	降低架构不匹配和人工选包错误。
安全注册	短时安装令牌只用于首次引导；节点生成 UUID 与 ECDSA 公钥。	后续请求改用节点身份签名，避免长期复用安装凭据。
自动上线	完成 enroll 后写入租户、sensor、端口和运行模式配置。	节点开始心跳并向所属工作区上报事件。
状态可见	后台展示在线状态、版本、架构、公共 IP 和最近心跳。	运营人员快速识别离线、版本漂移和部署异常。

远程操作	工作机制	可见反馈
实时改配置	保存期望配置后通过 SSE 推送节点；支持模式、端口、Proxy、LLM 与高级 JSON。	期望/已应用版本和逐步进度用于确认是否生效。
实时更新版本	后台比较当前与官方最新版本，通知节点拉取官方镜像并重启。	版本、更新时间及失败状态可追踪。
后台删除	删除请求校验租户归属，并通知节点清理对应运行实例。	资产列表、配置和节点状态同步收敛。
轮换节点凭据	为指定 sensor 重新生成令牌，不影响其他节点。	缩小泄露凭据影响面并支持周期轮换。

配置进度覆盖数据库保存、事件推送、版本检查、配置应用、重启开始和重启成功等阶段。运营人员应在变更前保留可回滚配置，并对 Proxy 与 LLM 变更安排额外验证。

08 身份与工作区生命周期

开放注册时，每个受 SSO 接纳的身份都能安全地开始使用。

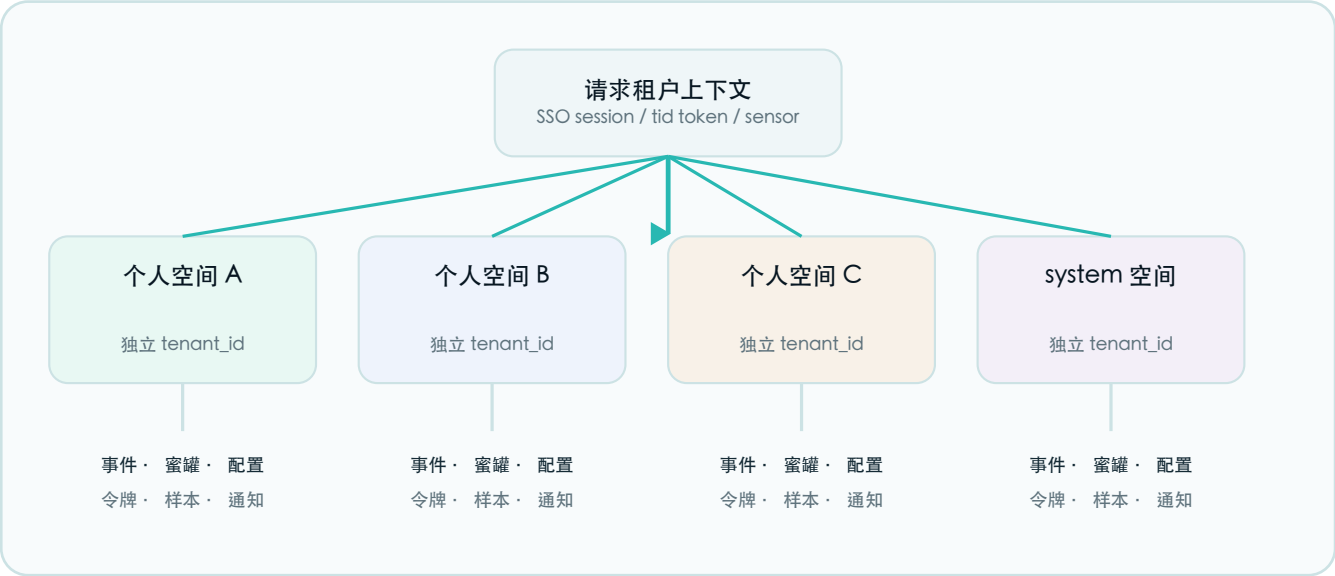
HoneyTrace 使用 OpenID Connect Authorization Code Flow + PKCE。客户端发起登录时生成 state、nonce 与 code_verifier；回调阶段校验上下文，交换授权码并验证 ID Token。身份通过应用授权规则后，后端以 issuer + sub 作为稳定主键创建或更新 SaaS 账户。电子邮箱和显示名称可以变化，但不会导致工作区漂移。

阶段	系统动作	安全要点
1. 发起登录	跳转 GCSA SSO 授权端点，携带 openid profile email。	state / nonce 防止登录上下文混淆；PKCE 限制授权码被截获后的滥用。
2. 完成认证	后端交换 code，读取并验证 claims。	客户端密钥仅存在于 API 运行环境，不下发浏览器。
3. 应用授权	按 required role、subject 或 email 白名单（若配置）判定。	不配置约束时，任意被 SSO 接纳的身份可使用 SaaS。
4. 配置工作区	按 issuer + sub upsert 账户，生成 UUID tenant_id。	同一身份重复登录稳定复用空间；不同 subject 必然分离。
5. 建立会话	会话保存用户与 workspace 信息，后续请求恢复租户上下文。	写请求要求同源 Origin；会话过期后重新认证。
6. 退出登录	清理本地会话并进入 SSO end-session 流程。	统一退出降低共享终端上的残留会话风险。

平台运维角色与产品成员身份分离。普通 SaaS 成员不会获得机器码、许可证激活或清除权限；平台角色仅用于受控的服务运维。

09 多租户隔离模型

一次身份判定，贯穿数据库、配置、令牌和对象存储路径。

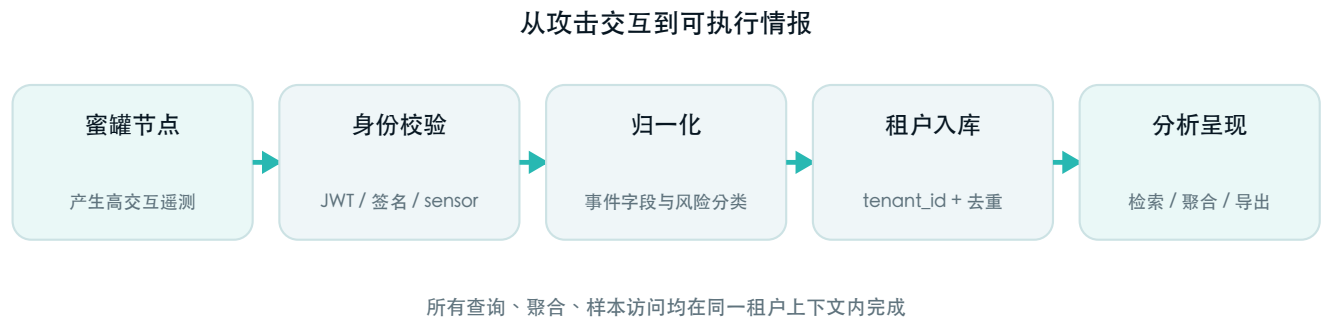


数据域	隔离键 / 机制	跨租户行为
账户与工作区	saas_accounts.id (UUID)	issuer + sub 唯一；用户属性更新不改变工作区。
事件	ingest_events.tenant_id	所有计数、分页、会话、端口和样本关联查询自动限定当前 tenant_id。
蜜罐注册	registry entry.tenantId + 租户令牌 tid	列表、更新、心跳、删除和令牌轮换只对所属租户可见。
设置与配置	tenant:{uuid}:setting_key	控制令牌、仪表盘设置、节点配置与同步状态独立持久化。
样本	base_dir/{tenant_id}/{sha256}	下载或预览同时校验事件可见性与租户目录。
通知状态	租户命名空间 setting key	已读状态不会影响其他用户。
既有私有部署	保留字 system	历史事件与旧令牌继续归属 system，支持平滑升级。

个人空间默认且强制关闭匿名访问。即使 SSO 侧开放自助注册，新用户也只会看到刚创建的空工作区。

10 遥测接入与数据链路

让每条事件在进入系统之前就携带可验证的归属。



新建蜜罐时，平台签发带有 tid 的 HoneyTrace JWT；节点上报时，API 根据已验证令牌或已登记 sensor 建立租户上下文，再验证事件中的 sensor 是否属于同一租户。非 system 空间不接受未登记传感器名称，避免通过伪造字段把事件注入其他空间。

事件归一化将不同协议的原始字段转化为统一结构，并保留 raw 文档以支持后续分析。入库时同时写入 tenant_id 与 import_hash；复合唯一索引 (tenant_id, import_hash) 在避免同一空间重复导入的同时，允许不同用户拥有内容相同的独立事件。

遥测类别	典型字段	运营价值
连接与探测	src_ip、dst_ip、protocol、sensor、timestamp	发现暴露端口扫描、来源分布与节点健康变化。
身份尝试	username、password、success、session	观察凭据字典、成功链路与同源关联行为。
命令与会话	input、ttylog、duration、session	还原攻击者意图、工具链和交互顺序。
文件与样本	shasum、filename、url、direction	建立会话到样本的可追溯关系，并支持受控预览与下载。
节点状态	heartbeat、version、arch、publicip	判断在线状态、版本分布和远程配置进度。

11 分析与运营能力

围绕攻击路径组织数据，而不是只展示孤立日志。

风险总览 聚合事件、会话、来源、协议与节点状态，提供 12H / 24H / 7D 等时间范围观察。	攻击来源 按 IP、地理与时间分布查看热点来源，并把来源与会话、端口和行为关联。	攻击者画像 汇总凭据尝试、命令序列、交互深度与样本活动，形成行为侧写。
会话与威胁日志 以 session 为主线恢复连接、认证、命令、文件和关闭事件，支持分页与上下文查看。	蜜罐与节点运营 创建、接入、心跳、更新、删除、令牌轮换与配置版本状态集中管理。	样本与导出 样本按 SHA-256 管理；预览、下载和表格导出受当前工作区能力约束。

HoneyTrace 的分析模型强调“来源 - 会话 - 行为 - 样本 - 节点”之间的可追溯关系。通过统一事件时间线，运营人员可以从宏观趋势进入单次交互，再回到同源或同样本的横向关联。

使用场景	推荐视图	处置输出
新暴露服务遭扫描	端口探测日志 + 攻击来源	确认来源、目标端口与扫描节奏，调整暴露面和阻断策略。
疑似弱口令成功	凭据 + 会话时间线	核对成功认证后的命令与文件行为，提取检测线索。
出现未知文件	会话 + 样本视图	定位下载来源、SHA-256、关联会话和同源后续活动。
节点离线或配置不一致	蜜罐管理 + 配置进度	检查心跳、期望版本与应用状态，触发更新或重启。

平台展示的是攻击观测与运营辅助信息，不替代组织自身的事件响应流程、取证保全或风险决策。

12 管理后台能力详解

把发现、调查、节点运维和证据输出汇聚到统一工作界面。

风险总览 按 12H / 24H / 7D 汇总事件、会话、攻击源、协议、趋势和节点状态，快速建立全局态势。	攻击来源分析 结合来源 IP、地理位置、时间分布、目标端口和关联会话，识别热点与重复活动。	攻击者画像 聚合凭据字典、命令序列、交互深度、文件活动和会话行为，形成可复用的行为侧写。
实时大屏 持续展示最新攻击事件、趋势与来源信息，适用于值守、态势展示和快速异常发现。	会话时间线 按 session 恢复连接、认证、命令、文件、持续时间和关闭事件，支持上下文调查。	威胁与扫描日志 分别查看入侵事件、端口扫描、Ping 探测与凭据尝试，并按条件检索和分页。

后台模块	提供能力	典型用途
样本中心	按 SHA-256 归档，提供受控预览、下载与会话关联。	提取 IOC、核对下载链路并交给后续沙箱分析。
蜜罐与节点	清单、心跳、版本、架构、IP、配置进度、更新、删除和凭据轮换。	统一完成资产盘点、健康检查与远程运维。
通知中心	记录关键状态变化并在租户范围内维护已读状态。	减少节点离线、配置失败或新事件被遗漏。
检索与导出	对事件、会话、来源、凭据与样本进行筛选、分页和表格导出。	支撑调查留档、离线统计与外部系统对接。
体验与访问	多语言、亮暗主题、响应式界面、SSO 会话和受控公开仪表盘。	适配桌面/移动值守，并明确个人空间与公开视图边界。

所有后台查询、下载、导出和操作都继承当前工作区上下文。页面上的“可见”不只是展示逻辑，后端仍需对每次资源读取和变更执行租户归属校验。

13 安全控制与隐私

将“开放使用”与“开放数据”彻底分离。

控制域	当前实现	运营建议
认证	OIDC Authorization Code + PKCE；验证 state、nonce、issuer、签名与时效。	在 SSO 侧启用 MFA、异常登录检测与账号生命周期管理。
会话	服务端加密 Cookie 会话；退出时清理本地会话并联动 SSO。	保持 HTTPS、合理会话时长并限制共享终端使用。
写操作	SSO 会话写请求要求同源 Origin；节点请求使用 Bearer 或签名验证。	反向代理应保留 Host 与 Origin，并拒绝异常跨域请求。
租户隔离	请求级 tenant_id，数据库查询、设置键、令牌 tid 和样本目录联动。	上线前持续执行双用户隔离与越权回归测试。
密钥	client_secret、管理令牌和签名密钥仅保存在服务端环境。	使用密钥管理系统注入，定期轮换，不写入仓库或日志。
数据最小化	前端只接收显示所需字段；敏感内容在公开视图中受限。	制定原始事件与样本保留周期，避免超期存储。
平台权限	许可证管理只允许 Bearer 管理令牌或配置的平台角色。	平台角色与普通成员角色分离并定期复核。

隐私责任取决于实际部署地域、日志内容与使用方式。运营方应明确告知范围、保留周期和访问主体，并根据适用法律与组织制度完成评估。HoneyTrace 不应被用于未经授权的监控。

开放 SSO 的推荐前提：完成数据库迁移；确认个人空间强制私有；配置生产 TLS；轮换所有演示令牌；验证 SSO issuer/JWKS；执行跨租户自动化测试；建立备份、监控与删除流程。

14 可用性、运维与升级

SaaS 不是一次部署，而是一套可持续运行的服务纪律。

领域	运行机制	建议指标
数据库	PostgreSQL 持久化账户、事件与设置；迁移在版本升级时执行。	连接池、查询延迟、磁盘增长、迁移成功率、备份恢复演练。
样本存储	独立持久卷，非 system 空间按 tenant_id 分目录。	容量、文件数量、写入失败、恶意样本访问审计与清理任务。
API	Phoenix 提供健康检查、认证、接入与查询端点。	请求量、P95/P99 延迟、4xx/5xx、OIDC 回调失败、令牌拒绝。
节点	心跳、版本、架构、公共地址和配置进度可见。	在线率、心跳延迟、版本落后、更新失败与重启失败。
前端	静态 Astro 产物由站点服务提供，通过同域 API 工作。	构建完整性、静态资源命中率、关键页面可用性与 SSO 跳转。
发布	容器镜像、Compose、持久卷与反向代理协同升级。	镜像摘要、回滚时长、迁移窗口、部署后冒烟检查。

推荐发布顺序：备份数据库与关键配置 → 构建并校验镜像 → 运行向后兼容迁移 → 启动 API 与站点 → 检查健康端点 → 验证 SSO 登录 → 创建测试蜜罐并上报事件 → 验证双用户互不可见 → 再扩大访问范围。

当前多租户迁移是增量式的：为事件表加入 tenant_id，并将已有记录默认标记为 system；原有 import_hash 唯一约束升级为 tenant_id + import_hash；新增 saas_accounts 表保存稳定身份映射。

15 部署模式与适用边界

同一产品核心支持云端个人空间与受控私有部署。

维度	HoneyTrace SaaS	HoneyTrace 私有化
身份入口	GCSA SSO；可开放任意受 SSO 接纳的用户。	可接 GCSA SSO；必要时保留受控 break-glass 本地登录。
数据空间	每个 issuer + sub 对应独立个人 tenant_id。	既有数据位于 system；可按组织需求控制部署边界。
匿名访问	个人空间强制关闭。	system 可由管理员明确配置公开仪表盘。
许可证	SaaS 能力由服务提供，普通用户不管理机器码。	支持机器码、签名许可证、传感器限制与维护期限。
基础设施	由平台运营方管理 API、数据库、样本卷、TLS 与升级。	由客户管理容器、PostgreSQL、卷、反向代理与备份。
适用场景	快速试用、个人研究、分散节点、无需自建控制面的团队成员。	数据驻留、内网部署、定制集成、专属运维和合规要求。

两种模式可以共享事件模型、节点接入和分析体验，但责任边界不同。选择 SaaS 时应关注数据保留与平台条款；选择私有化时应确保数据库、密钥、网络与升级能力达到生产要求。

当前 SaaS 个人空间模型不应被解释为企业组织模型。若同一团队需要共享蜜罐、成员权限、统一账单或审计，应等待组织工作区能力或采用独立私有部署。

16 路线图与结语

先把诱捕、隔离与可用性做扎实，再扩展协作和生态。

阶段	重点能力	状态说明
当前版本	SSO 自动配置个人空间；事件/蜜罐/配置/令牌/样本隔离；SaaS 能力集；双用户回归测试。	已纳入 V1.1 技术基线。
近期	注册开放策略、配额与限流、数据保留策略、租户级运营指标、账号停用与删除流程。	面向规模化开放的运营完善。
中期	组织工作区、成员邀请、RBAC、共享蜜罐、工作区转移、团队审计。	从个人使用扩展到团队协作。
后续	威胁情报交换、检测规则生态、Webhook/API 集成、分层存储与高级报表。	强化跨系统联动和长期研究价值。

HoneyTrace 把默认 Shell、Proxy 和 LLM 蜜罐放在同一控制与分析平面中：节点负责观察真实攻击交互，统一事件模型保存调查上下文，后台把来源、会话、命令、凭据、扫描和样本连接为可追溯路径，一键安装与远程生命周期管理则让这些能力可以持续铺设和演进。

云端开放注册必须以可验证的租户隔离为前提。统一身份解决“你是谁”，个人工作区解决“哪些数据属于你”，租户令牌解决“节点为谁上报”，而端到端查询与文件隔离解决“你最终能看到什么”。这套基线也为组织协作、配额、审计与威胁情报生态保留清晰的演进路径。

了解更多

honeytrace.gcsa.org · [联系 GCSA 专家](#) · gcsa.org

本文档描述 V1.1 技术设计与产品边界，不构成法律、合规或商业承诺。实际能力以部署版本、服务条款和运行配置为准。

附录 关键配置与接口

用于技术评估和上线核对的最小参考。

OpenID Connect 配置

变量	示例 / 说明
GCSA_SSO_ISSUER	https://sso.gcsa.org/oidc
GCSA_SSO_CLIENT_ID	由 GCSA SSO 分配的应用 ID。
GCSA_SSO_CLIENT_SECRET	仅注入后端运行环境，禁止出现在浏览器和仓库。
GCSA_SSO_REDIRECT_URI	https://honeytrace.gcsa.org/admin/auth/callback
GCSA_SSO_POST_LOGOUT_REDIRECT_URI	https://honeytrace.gcsa.org/admin/
GCSA_SSO_SCOPES	openid profile email；若依赖角色声明，再加入相应 scope。
GCSA_SSO_REQUIRED_ROLE / ALLOWED_*	可选应用授权约束；均为空时接受所有已通过 SSO 的身份。
GCSA_SSO_PLATFORM_ADMIN_ROLES	默认 honeytrace_admin,gcsa_admin；仅授予服务运营者。

关键端点

端点	用途
GET /api/auth/sso/login	创建 OIDC 登录上下文并跳转授权端点。
POST /api/auth/sso/callback	交换 code、验证身份、配置工作区并建立会话。
GET /api/session	返回当前用户、workspace 与管理会话状态。
POST /api/honeypots	在当前工作区创建蜜罐并签发 tenant-aware 节点令牌。
POST /api/honeypots/install	生成 Docker 或原生一键安装命令与短时安装凭据。
PATCH /api/sensor-config	保存期望配置并通过实时事件通道通知节点应用。
POST /api/honeypots/:sensor/update	请求节点拉取官方最新版本并重启。
DELETE /api/honeypots/:sensor	校验租户归属后删除蜜罐并请求节点清理实例。
POST /api/ingest	验证节点归属后接收并写入租户事件。
GET /api/dashboard	在当前 tenant_id 下执行聚合、分页与能力判定。
GET /api/health	部署后健康检查入口。

上线核对：迁移成功 · TLS 生效 · SSO 元数据可达 · client_secret 已轮换 · system 历史数据可见 · 新用户空间为空 · A/B 用户互不可见 · 节点上报归属正确 · 备份与恢复已验证。