GCSA
GLOBAL CYBERSECURITY ALLIANCE

GCSA 安全研究与产品白皮书

01

SentraX

从线索到风险判断

威胁情报与风险判断平台白皮书

PUBLIC WHITE PAPER
VERSION 1.0 / JULY 2026

发布机构
Global Cyber Security Association

版本日期
V1.0 · 2026 年 7 月

00 PUBLICATION NOTE

文档说明

本文为 SentraX 对外产品白皮书，介绍平台定位、核心能力、风险判断方法、安全治理和部署边界。

内容面向客户沟通与方案评估，聚焦用户可感知的产品价值，不涉及内部技术实现。

01	02	03	04	05	06
输入	**识别**	**分析**	**证据**	**判断**	**运营**

> 本白皮书用于产品介绍、方案交流与能力评估。平台输出应结合组织自身环境、业务上下文和人工复核形成最终处置决策。

00 CONTENTS

目录

01 执行摘要
02 产品定位与设计原则
03 统一分析与能力架构
04 IoC 威胁情报能力
05 Web3 风险分析能力
06 软件供应链安全能力
07 控制台与持续风险运营
08 证据链与风险判断
09 身份、安全与部署边界
10 路线图与结语
A 关键术语

01 执行摘要

SentraX 是面向安全团队、情报分析人员和风险运营团队的威胁情报与风险判断平台。平台从一个域名、IP、文件哈希、软件包、钱包或合约等线索开始，识别对象类型、关联上下文，并输出可解释、可追溯、可执行的风险判断。

真实攻击活动通常跨越多个对象。一个可疑域名可能同时关联恶意基础设施、软件包投毒、异常仓库活动或链上资金行为。传统工具按对象和数据类型拆分，分析人员需要在不同系统之间反复切换，再手动整理结论。SentraX 将这些步骤归一为统一工作流，帮助用户更快回答三个问题：对象是否危险、判断依据是什么、下一步应如何处置。

平台围绕三项核心能力构建：

能力方向	主要分析对象	核心输出
IoC 威胁情报	域名、IP、URL、文件哈希	威胁命中、风险等级、关联实体与建议
Web3 风险分析	钱包、合约、Token、dApp、交易线索	地址与合约风险、授权暴露、交互风险
软件供应链安全	软件包、依赖、manifest、lockfile	恶意包、漏洞、异常行为与修复建议

SentraX 不替代 SIEM、SOAR、EDR、漏洞管理平台或链上审计平台。它定位于安全运营的前置研判环节，为调查、处置和报告提供统一入口与证据依据。

02 产品定位与设计原则

2.1 产品定位

SentraX 定位为“威胁情报与风险判断工作台”，适用于日常线索查询、事件调查、客户风险验证和持续情报运营。用户无需先理解复杂工具链，只需提交待分析对象，即可获得结构化判断。

场景	输入	输出
可疑对象研判	域名、IP、URL、文件哈希	风险等级、命中证据、关联对象
链上风险排查	钱包、合约、Token、dApp	信誉、授权与交互风险

场景	输入	输出
依赖安全确认	软件包、依赖文件	组件风险、受影响版本、修复建议
持续风险运营	调查记录与风险对象	风险分布、趋势、重点对象与报告

2.2 设计原则

- **线索优先：** 用户从对象开始，而不是先选择复杂工具。
- **证据优先：** 每个风险结论都应说明判断依据。
- **语言统一：** 不同对象归一为一致的风险等级、置信度和建议动作。
- **能力分层：** 综合入口负责快速判断，专项页面负责深入分析。
- **最小必要：** 仅处理完成分析、授权和审计所需的信息。
- **可运营：** 调查结果能够进入历史、报告、监控和复核流程。

2.3 能力边界

SentraX 不主动扫描客户内网，不直接执行封禁或下线等破坏性操作，也不把单一情报命中视为最终法律或合规结论。平台输出是安全运营中的风险判断依据，应结合客户环境和人工复核形成最终决策。

03 统一分析与能力架构

3.1 统一分析流程

SentraX 将一次分析组织为六个阶段：

1. **输入：** 接收域名、IP、URL、哈希、软件包、钱包或合约等对象。
2. **识别：** 判断对象类型并选择对应分析路径。
3. **分析：** 从信誉、行为、关系和历史等维度评估风险。
4. **证据：** 提取命中原因、关联实体、时间和上下文。
5. **判断：** 形成风险等级、置信度与建议动作。
6. **运营：** 保存调查记录，用于报告、复核和持续关注。

3.2 能力架构

层级	作用	用户可感知结果
入口层	接收多类型线索	统一搜索与专项分析页
识别层	判断对象类型与分析路径	自动识别或手动选择
分析层	进行多维风险分析	风险等级、置信度、上下文
证据层	组织命中与关联关系	命中原因、实体、时间线索
处置层	形成建议动作	阻断、监控、复核、修复或报告
运营层	沉淀历史和统计	数据面板、记录与授权状态

3.3 统一输出结构

无论对象属于哪一类，平台均尽量提供风险等级、置信度、对象类型、命中情况、证据链、关联实体和推荐动作。对于暂无明确命中的对象，平台会明确提示“暂无明确风险证据”或“需要进一步复核”，避免将无结果解释为安全结论。

04 IoC 威胁情报能力

IoC 威胁情报能力用于研判域名、IP、URL 和文件哈希等传统安全对象。

对象	分析重点
域名	域名信誉、威胁命中、解析关系、关联基础设施
IP 地址	恶意活动、攻击来源、历史命中、关联域名
URL	钓鱼页面、恶意跳转、伪装登录与投递路径
文件哈希	样本信誉、恶意标签、家族线索与历史检出

IoC 结果不仅呈现“命中”或“未命中”，还会说明风险类型、严重程度、判断置信度和相关对象，并给出阻断、监控或人工复核建议。用户可以从一条可疑线索进入调查，再沿关联实体继续分析。

典型场景包括钓鱼域名确认、攻击来源核验、恶意文件研判和客户线索验证。平台通过统一结果结构减少字段解释成本，帮助安全人员更快形成可交付结论。

05 Web3 风险分析能力

Web3 风险分析能力用于判断链上地址、合约和交互行为是否可能带来资产或安全风险。

对象	分析重点
钱包地址	地址信誉、异常活动、风险交互与授权暴露
Token 合约	合约权限、交易限制、持有人与行为风险
dApp URL	钓鱼、仿冒和恶意交互入口
calldata / 交易线索	调用意图、授权行为和潜在资产风险

结果页以风险画像为核心，说明对象是否存在可疑活动、是否关联高风险对象、是否包含危险授权，以及当前交互可能产生的影响。对于高风险对象，平台建议暂停交互、加入关注并进行人工复核；对于授权风险，则提示检查授权目标和范围。

Web3 结果不构成投资建议，也不替代完整合约审计。它主要用于交易前风险提示、可疑对象排查和事件调查中的链上上下文补充。

06 软件供应链安全能力

软件供应链安全能力关注开发与交付链路中的恶意包、漏洞、异常行为和依赖暴露。

对象	分析重点
软件包与版本	包信誉、恶意行为、漏洞与维护状态
PURL	标准化组件坐标与生态识别

对象	分析重点
manifest	项目声明依赖、直接依赖与生态类型
lockfile	实际安装版本、间接依赖与依赖树
仓库相关线索	可疑发布、名称混淆和投毒路径

平台将供应链风险归纳为恶意包、可疑版本、漏洞风险、名称混淆、安装脚本风险和维护风险。对依赖文件进行分析时，结果应展示依赖数量、风险数量、关键风险节点和修复建议，而不只是文件处理状态。

推荐动作包括升级到安全版本、移除高风险依赖、复核安装脚本、限制组件使用或持续关注后续变化。

07 控制台与持续风险运营

SentraX 控制台为安全团队提供统一工作区，主要包括综合分析、IoC 情报、Web3 风险分析、供应链安全、数据面板、报告和设置。

7.1 一致的分析状态

状态	用户体验
初始	说明可分析对象，不展示虚构结果
分析中	展示当前对象和分析进度
成功	展示结论、证据、关联实体和建议
部分结果	明确已完成与待补充的部分
无命中	提示暂无明确风险证据
错误	说明可理解的原因并提供重试入口

7.2 数据面板

数据面板聚合平台自身的调查与风险结果，用于回答近期分析了什么、风险集中在哪里、哪些对象需要继续关注。主要内容包括分析次数、高风险数量、风险分布、最近调查、重点对象和授权余量。

用户可以从数据面板进入调查详情，从结果页生成报告或继续分析关联实体，形成从线索输入到调查复盘的运营闭环。

08 证据链与风险判断

SentraX 的核心价值不是单独显示一个风险分数，而是让判断有证据可追。

8.1 判断组成

组成	说明
风险等级	对象风险的严重程度
置信度	当前证据对结论的支撑强度
命中情况	威胁、行为或关联风险的具体命中
关联实体	相关域名、IP、包、仓库、钱包或合约
时间线索	首次发现、最近命中和分析时间
推荐动作	阻断、监控、复核、修复或报告

8.2 判断路径

以可疑域名为例，平台会先识别对象类型，再检查威胁命中和关联基础设施，并结合相关软件供应链或链上活动形成证据链。高风险结论需要有足够证据支撑；证据不足时，应输出未知或需复核，而不是强行给出确定结论。

风险等级	建议动作
高风险	阻断对象、加入关注、生成报告并通知相关团队
中风险	人工复核、补充上下文并持续观察
低风险	记录结果，按需继续关注
未知	补充样本、其他线索或业务上下文

09 身份、安全与部署边界

9.1 身份与授权

SentraX 面向授权用户开放控制台。平台支持登录与退出、会话状态、工作区归属、授权次数和个人偏好。未登录用户访问控制台时进入身份验证流程，已登录用户进入所属工作区。

授权次数用于管理客户试用与正式使用范围。用户能够查看总次数、已使用次数、剩余次数和必要的使用记录。

9.2 安全与隐私

平台遵循数据最小化原则，仅处理完成分析、审计和授权所需的信息。调查记录遵循工作区边界，未授权用户不能访问控制台，敏感操作需要有效会话。

风险结论应被理解为情报驱动的判断依据。涉及高风险处置时，仍需结合客户业务环境和人工复核。

9.3 部署模式

模式	适用场景	责任边界
托管模式	快速试用、日常研判和客户验证	GCSA 负责平台运行、升级和维护
私有化模式	强数据边界、内部联动和高保密场景	按客户环境配置身份、访问和数据策略

部署方案应根据数据敏感性、网络环境、身份体系和运营流程确定，并明确访问控制、数据保留与运行责任。

10 路线图与结语

SentraX 将持续围绕三个方向演进：提高多类型对象的判断质量，增强证据链和报告能力，完善组织级权限、监控与通知流程。

近期重点包括优化数据面板、增强结果解释、完善依赖文件分析和 Web3 交互风险展示；中期将增加团队权限、订阅通知、细粒度证据可视化和标准化情报输出。

威胁情报平台的价值不在于展示更多字段，而在于帮助安全团队更快形成可信判断。SentraX 将分散的线索、风险、证据和建议组织成清晰工作流，让用户从一个对象开始，得到可解释、可追溯、可执行的结论。

A 关键术语

术语	说明
IoC	与入侵或威胁活动相关的指标，例如域名、IP、URL 和文件哈希。
风险判断	平台基于多维证据对对象风险程度形成的结论。
证据链	支撑风险判断的一组事实、命中结果和关联关系。
置信度	平台对当前判断可信程度的表达。
关联实体	与输入对象存在关系的域名、IP、仓库、包、钱包或合约。
Web3 风险	链上地址、合约、Token、dApp 或交易交互可能带来的风险。
供应链风险	软件包、依赖、构建和分发过程中出现的恶意、漏洞或异常风险。
工作区	用户进行分析、查看记录和管理授权的受控空间。