

01

SentraX

From Signal to Risk Decision

Threat Intelligence and Risk Decision Platform

Publication Note

This public white paper introduces the positioning, core capabilities, risk decision model, security governance, and deployment boundaries of SentraX.

It is intended for customer discussions and solution evaluation and focuses on user-visible product value rather than internal implementation details.

01	02	03	04	05	06
Intake	Identify	Analyze	Evidence	Decide	Operate

This white paper supports product introduction, solution discussions, and capability evaluation. Final response decisions should include organizational context and human review.

00

CONTENTS

Contents

01	Executive Summary	02	Product Positioning and Design Principles
03	Unified Analysis and Capability Architecture	04	IoC Threat Intelligence
05	Web3 Risk Analysis	06	Software Supply Chain Security
07	Console and Continuous Risk Operations	08	Evidence Chain and Risk Decisions
09	Identity, Security, and Deployment Boundaries	10	Roadmap and Conclusion
A	Key Terms		

01 Executive Summary

SentraX is a threat intelligence and risk decision platform for security teams, intelligence analysts, and risk operations teams. Starting with a domain, IP address, file hash, software package, wallet, or contract, the platform identifies the object type, correlates relevant context, and produces an explainable, traceable, and actionable risk decision.

Real attacks often span multiple object types. A suspicious domain may be connected to malicious infrastructure, poisoned packages, abnormal repository activity, or on-chain fund movements. Traditional tools separate these signals by object and data type, requiring analysts to switch between systems and assemble conclusions manually. SentraX brings these steps into one workflow so users can answer three questions faster: Is the object risky? What evidence supports that decision? What should happen next?

SentraX is organized around three core capabilities:

Capability	Primary objects	Core output
IoC threat intelligence	Domains, IPs, URLs, file hashes	Threat matches, severity, related entities, and actions
Web3 risk analysis	Wallets, contracts, tokens, dApps, transaction signals	Address and contract risk, approval exposure, interaction risk
Software supply chain security	Packages, dependencies, manifests, lockfiles	Malicious packages, vulnerabilities, abnormal behavior, remediation

SentraX does not replace SIEM, SOAR, EDR, vulnerability management, or full smart contract audit platforms. It operates at the investigation and decision layer, providing a unified entry point and evidence base for triage, response, and reporting.

02 Product Positioning and Design Principles

2.1 Product Positioning

SentraX is positioned as a threat intelligence and risk decision workspace for daily signal lookup, incident investigation, customer risk validation, and continuous intelligence operations. Users submit an object and receive a structured decision without first learning a complex toolchain.

Scenario	Input	Output
Suspicious object triage	Domain, IP, URL, file hash	Severity, matched evidence, related objects
On-chain risk review	Wallet, contract, token, dApp	Reputation, approval, and interaction risk
Dependency assurance	Package or dependency file	Component risk, affected versions, remediation
Continuous operations	Investigations and risk objects	Distribution, trends, priorities, and reports

2.2 Design Principles

- **Signal first:** users begin with an object rather than a complex tool selection.
- **Evidence first:** every risk decision should explain why it was made.
- **Consistent language:** different objects share the same severity, confidence, and action model.
- **Layered capability:** the unified entry supports fast decisions while specialist views support depth.
- **Minimum necessary data:** only information needed for analysis, authorization, and audit is processed.
- **Operational continuity:** results can move into history, reports, monitoring, and review workflows.

2.3 Capability Boundaries

SentraX does not actively scan a customer's internal network, directly perform destructive actions such as blocking or takedown, or treat a single intelligence match as a final legal or compliance conclusion. Its output is a risk decision input that should be evaluated with customer context and human review.

03 Unified Analysis and Capability Architecture

3.1 Unified Analysis Flow

SentraX organizes each analysis into six stages:

1. **Intake:** receive a domain, IP, URL, hash, package, wallet, contract, or other supported object.
2. **Identify:** determine the object type and select the appropriate analysis path.
3. **Analyze:** evaluate reputation, behavior, relationships, and history.
4. **Evidence:** extract matches, related entities, time context, and supporting facts.
5. **Decide:** assign severity and confidence and produce recommended actions.
6. **Operate:** save the investigation for reporting, review, and continued attention.

3.2 Capability Architecture

Layer	Purpose	User-visible result
Intake	Accept multiple signal types	Unified search and specialist views
Identification	Determine object type and path	Automatic detection or manual selection
Analysis	Evaluate risk across dimensions	Severity, confidence, and context
Evidence	Organize matches and relationships	Reasons, entities, and time context
Response	Produce recommended actions	Block, monitor, review, remediate, or report
Operations	Retain history and metrics	Dashboard, records, and authorization status

3.3 Consistent Output

Across object types, SentraX aims to provide severity, confidence, object type, match status, evidence chain, related entities, and recommended actions. If no clear match exists, the platform states that no explicit risk evidence was found or that further review is required. An absence of data is never presented as proof of safety.

04 IoC Threat Intelligence

The IoC capability supports the investigation of domains, IP addresses, URLs, and file hashes.

Object	Analysis focus
Domain	Reputation, threat matches, resolution relationships, infrastructure
IP address	Malicious activity, attack origin, historical matches, related domains
URL	Phishing, malicious redirects, impersonated login, delivery paths
File hash	Sample reputation, malicious labels, family context, detections

IoC results go beyond a matched or unmatched label. They describe the risk type, severity, confidence, and related objects and recommend blocking, monitoring, or human review. Analysts can begin with one suspicious signal and continue the investigation through connected entities.

Common use cases include phishing domain validation, attack source verification, malicious file triage, and customer-supplied signal review. A consistent output model reduces field interpretation and makes findings easier to communicate.

05 Web3 Risk Analysis

Web3 risk analysis evaluates whether an on-chain address, contract, or interaction may create asset or security risk.

Object	Analysis focus
Wallet address	Reputation, abnormal activity, risky interactions, approval exposure

Object	Analysis focus
Token contract	Contract privileges, trading restrictions, holder and behavior risk
dApp URL	Phishing, impersonation, and malicious interaction entry points
Calldata or transaction signal	Call intent, approvals, and potential asset impact

The result is organized as a risk profile that explains suspicious activity, high-risk relationships, dangerous approvals, and possible interaction impact. For high-risk objects, SentraX recommends pausing the interaction, adding the object to monitoring, and performing human review. Approval findings should trigger verification of the target and scope.

Web3 analysis is not investment advice and does not replace a full contract audit. Its role is pre-transaction risk awareness, suspicious object triage, and on-chain context during incident investigation.

06 Software Supply Chain Security

The software supply chain capability focuses on malicious packages, vulnerabilities, abnormal behavior, and dependency exposure across development and delivery workflows.

Object	Analysis focus
Package and version	Reputation, malicious behavior, vulnerabilities, maintenance
PURL	Standard component coordinates and ecosystem identification
Manifest	Declared dependencies, direct dependencies, ecosystem type
Lockfile	Installed versions, transitive dependencies, dependency graph
Repository signal	Suspicious release, name confusion, and poisoning path

SentraX groups findings into malicious packages, suspicious versions, vulnerabilities, name confusion, install-script risk, and maintenance risk. Dependency-file analysis should show dependency counts, risk counts, important nodes, and remediation rather than only file-processing status.

Recommended actions include upgrading to a safe version, removing a high-risk dependency, reviewing install scripts, restricting component use, or monitoring future changes.

07 Console and Continuous Risk Operations

The SentraX console provides a unified workspace for general analysis, IoC intelligence, Web3 risk analysis, software supply chain security, dashboards, reports, and settings.

7.1 Consistent Analysis States

State	User experience
Initial	Explain supported objects without fabricated results
Analyzing	Show the current object and analysis progress
Complete	Present decision, evidence, related entities, and actions
Partial	Distinguish completed and unavailable portions clearly
No match	State that no explicit risk evidence was found
Error	Explain the issue and provide a retry path

7.2 Dashboard

The dashboard aggregates the platform's own investigations and decisions. It answers what was analyzed recently, where risk is concentrated, and which objects need attention. Key areas include analysis volume, high-risk count, risk distribution, recent investigations, priority objects, and remaining authorization.

Users can move from the dashboard to an investigation, from a result to a report, or from one entity to another related analysis. This creates an operational loop from signal intake to investigation review.

08 Evidence Chain and Risk Decisions

The core value of SentraX is not a standalone score. It is a risk decision with traceable supporting evidence.

8.1 Decision Components

Component	Meaning
Severity	The assessed seriousness of the object's risk
Confidence	The strength of evidence supporting the decision
Match status	Specific threat, behavior, or relationship findings
Related entities	Connected domains, IPs, packages, repositories, wallets, or contracts
Time context	First seen, most recent match, and analysis time
Recommended action	Block, monitor, review, remediate, or report

8.2 Decision Path

For a suspicious domain, SentraX identifies the object, checks threat matches and related infrastructure, and incorporates relevant software supply chain or on-chain activity into the evidence chain. A high-risk decision requires sufficient support. Where evidence is weak, the platform should return unknown or review required rather than force a definitive conclusion.

Severity	Recommended action
High	Block, monitor, report, and notify relevant teams
Medium	Perform human review, add context, and observe
Low	Record the result and monitor when appropriate
Unknown	Add samples, related signals, or business context

09 Identity, Security, and Deployment Boundaries

9.1 Identity and Authorization

SentraX exposes console capabilities to authorized users. The platform supports sign-in and sign-out, session status, workspace membership, authorization usage, and personal preferences. Unauthenticated users are directed to sign in before entering a protected workspace.

Authorization usage controls customer trials and contracted use. Users can review total, used, and remaining units together with the necessary usage history.

9.2 Security and Privacy

SentraX follows data minimization principles and processes only the information required for analysis, audit, and authorization. Investigation records remain within workspace boundaries, unauthorized users cannot access the console, and sensitive operations require a valid session.

Risk results are intelligence-driven decision inputs. High-impact actions still require customer context and human review.

9.3 Deployment Models

Model	Suitable scenario	Responsibility boundary
Managed	Fast adoption, daily analysis, customer validation	GCSA operates, upgrades, and maintains the platform
Private deployment	Strong data boundaries, internal integration, high confidentiality	Identity, access, and data policies are configured for the customer environment

Deployment should be selected according to data sensitivity, network environment, identity architecture, and operational process, with explicit access, retention, and operating responsibilities.

10 Roadmap and Conclusion

SentraX will continue to improve decision quality across object types, strengthen evidence chains and reporting, and expand organization-level access, monitoring, and notification workflows.

Near-term work focuses on dashboard clarity, better result explanation, stronger dependency-file analysis, and clearer Web3 interaction risk. Medium-term priorities include team permissions, subscriptions and notifications, more detailed evidence visualization, and standardized intelligence output.

The value of a threat intelligence platform is not the number of fields it displays. It is the speed and confidence with which a security team can reach a defensible decision. SentraX brings signals, risk, evidence, and actions into one workflow so users can begin with an object and reach an explainable, traceable, and actionable conclusion.

A Key Terms

Term	Meaning
IoC	An indicator associated with intrusion or threat activity, such as a domain, IP, URL, or file hash.
Risk decision	A conclusion about an object's risk based on multiple pieces of evidence.
Evidence chain	Facts, matches, and relationships that support a risk decision.
Confidence	The assessed strength of support for the current decision.
Related entity	A connected domain, IP, repository, package, wallet, or contract.
Web3 risk	Risk arising from an address, contract, token, dApp, or transaction interaction.
Supply chain risk	Malicious, vulnerable, or abnormal behavior in packages, dependencies, build, or distribution.
Workspace	A controlled area where users analyze objects, review records, and manage authorization.