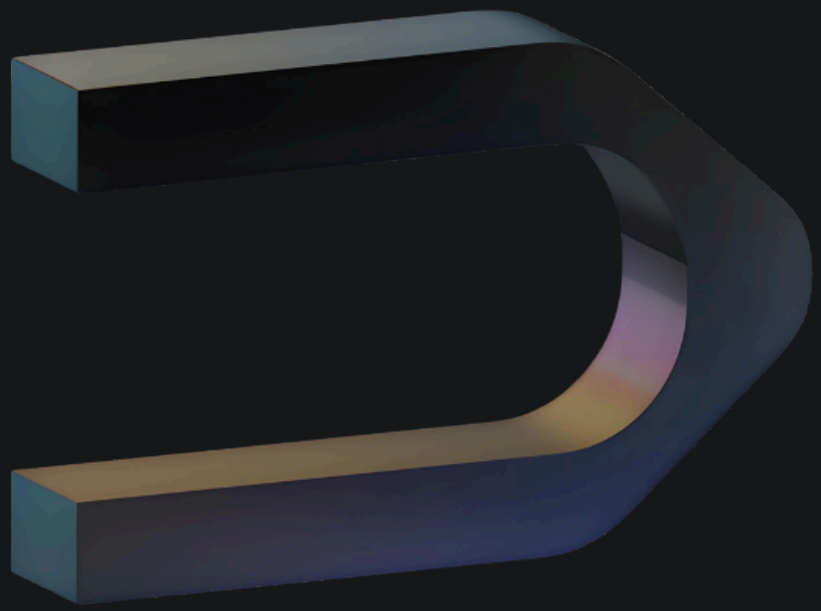
DEDAUB

Is Your Project Safe From Hackers?

We build guardrails for onchain businesses.

$70B	300+	29M
Assets Protected	Security Audits	Smart Contracts Decompiled



SERVICES

Senior-led audits. Every line reviewed. No shortcuts.

300+ audits · 160+ public reports · $70B in assets protected

A dedicated team of senior researchers reviews 100% of your code and then challenges each other to break it—backed by the Dedaub Security Suite, which leverages 100+ static analysis techniques, fuzzing, and LLMs.

300+	160+	80+	30+
Total Audits	Public Reports	Clients	Chains

METHODOLOGY

How We Audit

At least two senior researchers per engagement. Each independently examines 100% of the codebase, with rotating support from the broader team.

Two-Phase Review

Phase A: map functionality. Phase B: adopt an attacker mindset. Two passes ensure broad coverage and deep adversarial analysis.

Constant Challenging

Auditors cross-examine each other's understanding — adversarial peer review surfaces edge cases solo review would miss.

Multi-Level Analysis

Beyond single-contract review: complex combinations of protocol parts reveal unexpected cross-component behavior.

Advanced Tooling

100+ static analysis algorithms, AI-driven testing, automated fuzzing, and machine-generated leads via the Security Suite.

Zero Hacks Record

No audited protocol has been exploited through a vulnerability in code reviewed by Dedaub. Thoroughness over speed.

Gas & Integration

Gas inefficiencies, cost optimizations, and external integration audits — AMMs, oracles, and cross-protocol dependencies.

FOCUSED EXPERTISE

Our Web3 Consultancy Services

Perpetual Protocols · Zero-Knowledge Systems · Consensus-Driven Middleware

We partner with Web3 teams to review system architecture, identify economic and security risks, and strengthen system design before launch.

1. ## Architectural Review

   Assess architecture for robustness across perpetuals, ZK systems, and consensus infrastructure. Prevent structural vulnerabilities early.

2. ## Risk Mitigation

   Identify MEV exposure, oracle dependencies, and economic attack vectors. Ensure resilience against sophisticated threats.

3. ## Security Practice Audit

   Evaluate internal security practices, development processes, and documentation against the highest Web3 standards.

4. ## Gas Fees Optimization

   Review complex execution paths for gas inefficiencies. Keep cryptography-heavy contracts both secure and cost-efficient.

5. ## Protocol Design Advisory

   Tailored design guidance for economic models and scalable architectures that remain robust from day one.

CLIENTS

Trusted by Leading Protocols

From Layer 1 foundations to DeFi protocols, Dedaub secures the infrastructure that manages billions in onchain assets.

ethereum foundation	coinbase	Chainlink	LEDGER	EigenLayer
Immunefi	LIDO	DeFi Saver	PENDLE	0x
OASIS	LayerZero.	Liquity	SONIC LABS	Maverick
Maple				

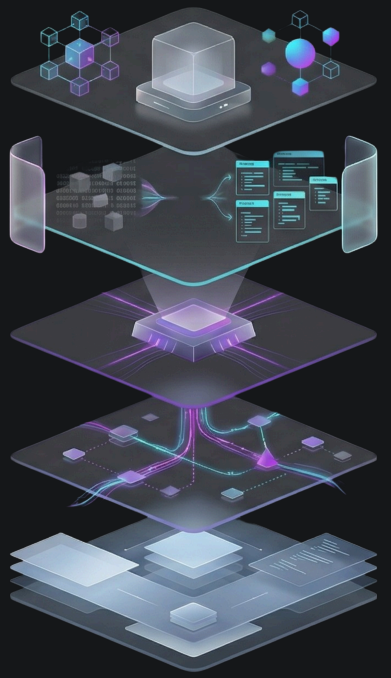
TECHNOLOGY

Security Suite | Onchain Technology Stack

Dedaub's Security Suite is a multichain security infrastructure layer that transforms large-scale onchain data into a unified, indexed, and queryable intelligence platform.

It powers contract inspection, vulnerability discovery, transaction structuring, and downstream Monitoring applications across major EVM networks.

DECOMPILE → VULNERABILITY DETECTION → TRANSACTION ANALYSIS



~28.9M	~15.6M	2,200+	340
Smart Contracts Decompiled	Threats Found	Datapoints Per Chain	Indexed Tables Per Chain

ARCHITECTURE

Architecture of the Stack

Security Suite is not a set of isolated tools. Each layer feeds into the next — from raw bytecode to structured intelligence — powering contract inspection, vulnerability discovery, and transaction analysis across major EVM networks.

01 — DECOMPILATION

Bytecode → analyzable program structure

Bytecode is lifted into Solidity-like representations. Function boundaries, storage layouts, control-flow graphs, and inferred ABIs are reconstructed — even without verified source.

02 — VULNERABILITY DETECTION

Continuously updated risk profiles

100+ proprietary algorithms analyze control flow and cryptographic misuse. Flagged contracts are fuzzed, while LLM-similarity and Hack-Related Proximity Scoring detect malicious linkages.

03 — TRANSACTION ANALYSIS

Execution traces → relational data

Transactions decoded against extracted ABIs. Internal calls, fund flows, events, and state changes materialized into structured records linking contracts, risks, and history.

SECURITY APPLICATION

tok{In}

Detect Malicious Tokens. Before Users Get Burned.

30+ detection flags · Multi-chain · API & MCP ready

Dedaub tok{In} delivers precise, real-time token safety insights — across all major EVM-compatible chains. Built for wallets, exchanges, and AI trading agents.

30+ DETECTION FLAGS | MULTI-CHAIN | API & MCP READY

Bytecode-Based Analysis

Decompiles bytecode to recover logic of 99.98% of tokens — full analysis even without source code.

Multi-Dimensional Detection

Combines static analysis, runtime behavior, and onchain signals like liquidity levels and holder distribution.

Cross-Pool Token Analysis

Analyzes token behavior independently across Uniswap V2, V3, V4 and forks to catch hidden per-pool risks.

SECURITY APPLICATION

Monitor

Your Protocol's Logic. Our Security Experts Watching It.

Custom agents · Multi-chain · Protocol-level granularity

Dedaub engineers write and maintain custom Monitoring queries built around your contracts — proactive threat detection, across every EVM chain you operate on.

CUSTOM AGENTS | MULTI-CHAIN | PROTOCOL-LEVEL GRANULARITY

Proactive Threat Detection

Identify pre-attack signals — abnormal state changes, suspicious deployments, and exploit sequences — before threats reach your protocol.

Expert-Written Rules

Dedaub engineers build and maintain Monitoring queries tailored to your protocol's contracts, risk model, and operational logic.

Full-Spectrum Oversight

Track governance proposals, transaction integrity, contract state changes, and known attack vectors in a single Monitoring layer.

SECURITY APPLICATION

Immunefi Firewall

powered by Dedaub

Transaction-Level Enforcement for High-Value Protocols

Transaction-level protection driven by contract and behavioral analysis. Firewall evaluates interactions before execution to help prevent exploit patterns, malicious calls, and abnormal contract behavior. Built to provide an enforcement layer for high-value protocols.

ENFORCEMENT LAYER | POLICY ENGINE | LIGHTWEIGHT PROTECTION

Pre-Execution Screening

Evaluates every transaction before execution, blocking exploit patterns and malicious calls at the contract level.

Behavioral Analysis

Uses contract structure and historical behavior patterns to detect abnormal interactions that static rules miss.

Zero-Overhead Integration

Lightweight onchain enforcement layer that integrates without modifying your protocol's core contract logic.

WHY US

Why Dedaub?

World-leading security research, academic rigor, and real-world hacker expertise — enabling deep smart contract audits and advanced security tooling, such as the Dedaub Security Suite and its industry-leading EVM decompiler.

$3M	$Billions	300+
BUG BOUNTIES	TVL SECURED	SECURITY AUDITS
across 11 critical claims	via white-hat hacking	for leading protocols

Trusted

Trusted by security teams at leading DeFi protocols and Web3 companies globally for reliable risk assessment.

Expertise

Years of smart contract security expertise and cutting-edge static analysis technology behind every engagement.

Knowledge

Comprehensive threat intelligence and security insights from industry-leading blockchain security researchers.

Chainlink Build Program
Partnership

Arbitrum DAO
Security Advisor

Oasis Protocol
Sapphire's Security Partner

SEAL 911
Founding Collaborator

Uniswap Foundation
Security Provider

zkSync
Security Council Member

DEDAUB

Let's Secure Your Protocol

From pre-deployment reviews to post-deployment Monitoring — we help your business launch successfully and stay secure.

contact@dedaub.com

dedaub.com