

# RektRadar

# RektRadar

Predictive crypto project incident risk scoring engine

# Story



GitHub Features

On-chain Architecture

Team/History

Social/Comms

commits/30d, unique committers/90d, bus factor (top-k authors share), PR latency, issue close rate, vectorized text features

GitHub Features

On-chain Architecture

Team/History

Social/Comms

verified?, proxy pattern?, upgradeability path, admin EOA vs multisig, signer count, timelock delay, pause/upgrade rights existence + last use time, privileged function call frequency (past 90d), deployer reputation

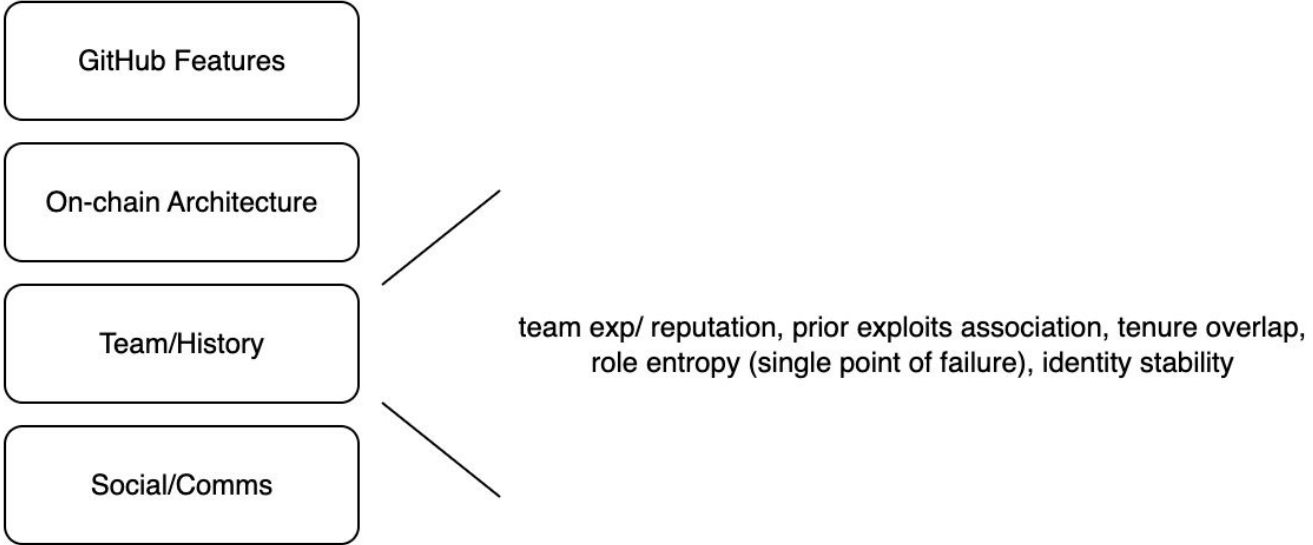
GitHub Features

On-chain Architecture

Team/History

Social/Comms

team exp/ reputation, prior exploits association, tenure overlap,  
role entropy (single point of failure), identity stability



GitHub Features

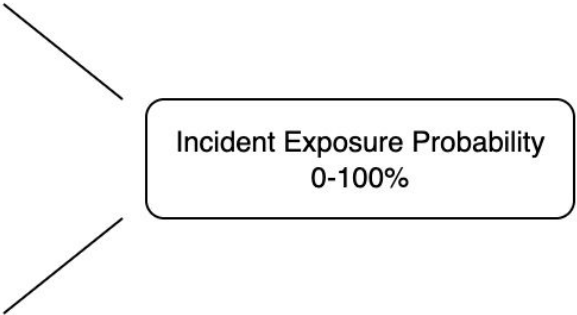
On-chain Architecture

Team/History

Social/Comms

follower/engagement ratio, spike residuals, telegram heuristics,  
issue-tracker vs social hype divergence (high hype + low  
engineering)

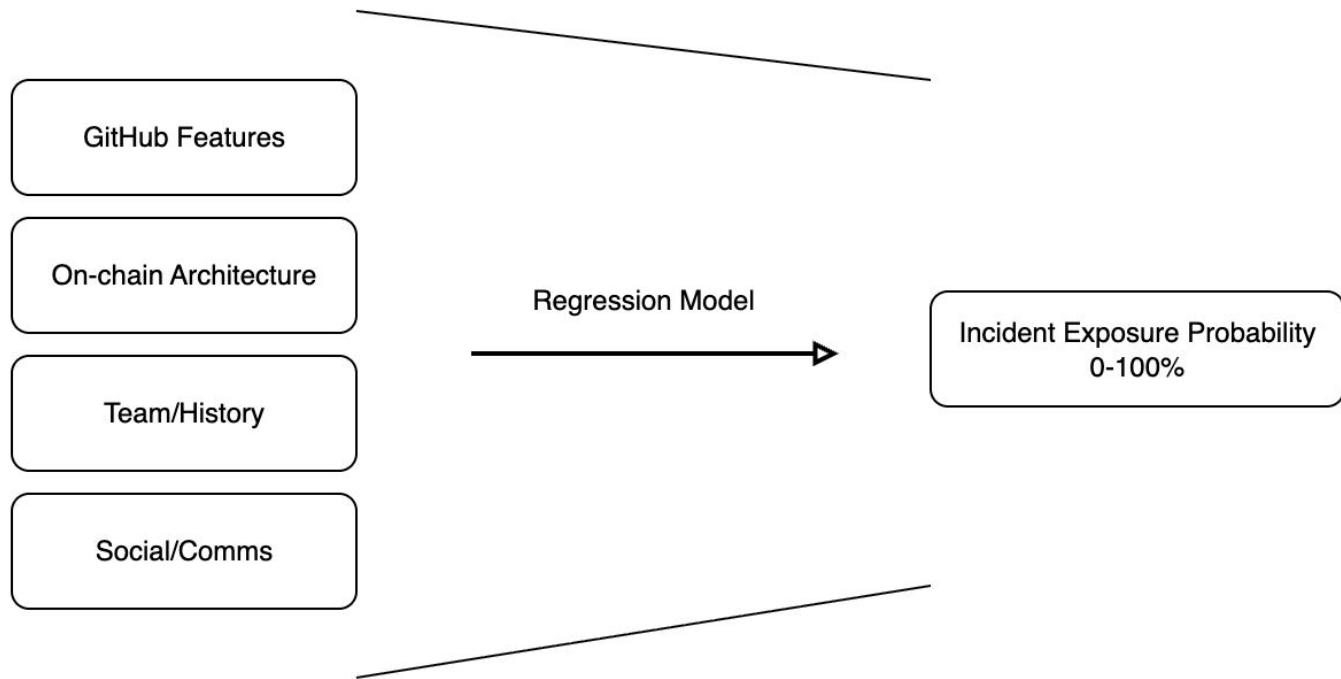
incidents related to project, attack complexity,  
attack relevance



Incident Exposure Probability  
0-100%

The diagram consists of a rectangular box on the right containing the text 'Incident Exposure Probability' and '0-100%'. Two diagonal lines extend from the left side of this box towards the left, pointing towards the text 'incidents related to project, attack complexity, attack relevance'.





# Current Solutions

Certik Skynet Score Methodology

$\text{Feature1} * w1 + \text{Feature2} * w2 + \dots = \text{Risk Score}$

# Current Solutions

Certik Skynet Score Methodology

$\text{Feature1} * w1 + \text{Feature2} * w2 + \dots = \text{Risk Score}$

- Unscalable (semi-manual scoring)

# Current Solutions

## Certik Skynet Score Methodology

$$\text{Feature1} * w1 + \text{Feature2} * w2 + \dots = \text{Risk Score}$$

- Unscalable (semi-manual scoring)
- Simplified, uncorrelated metric (features do not attend to itself)

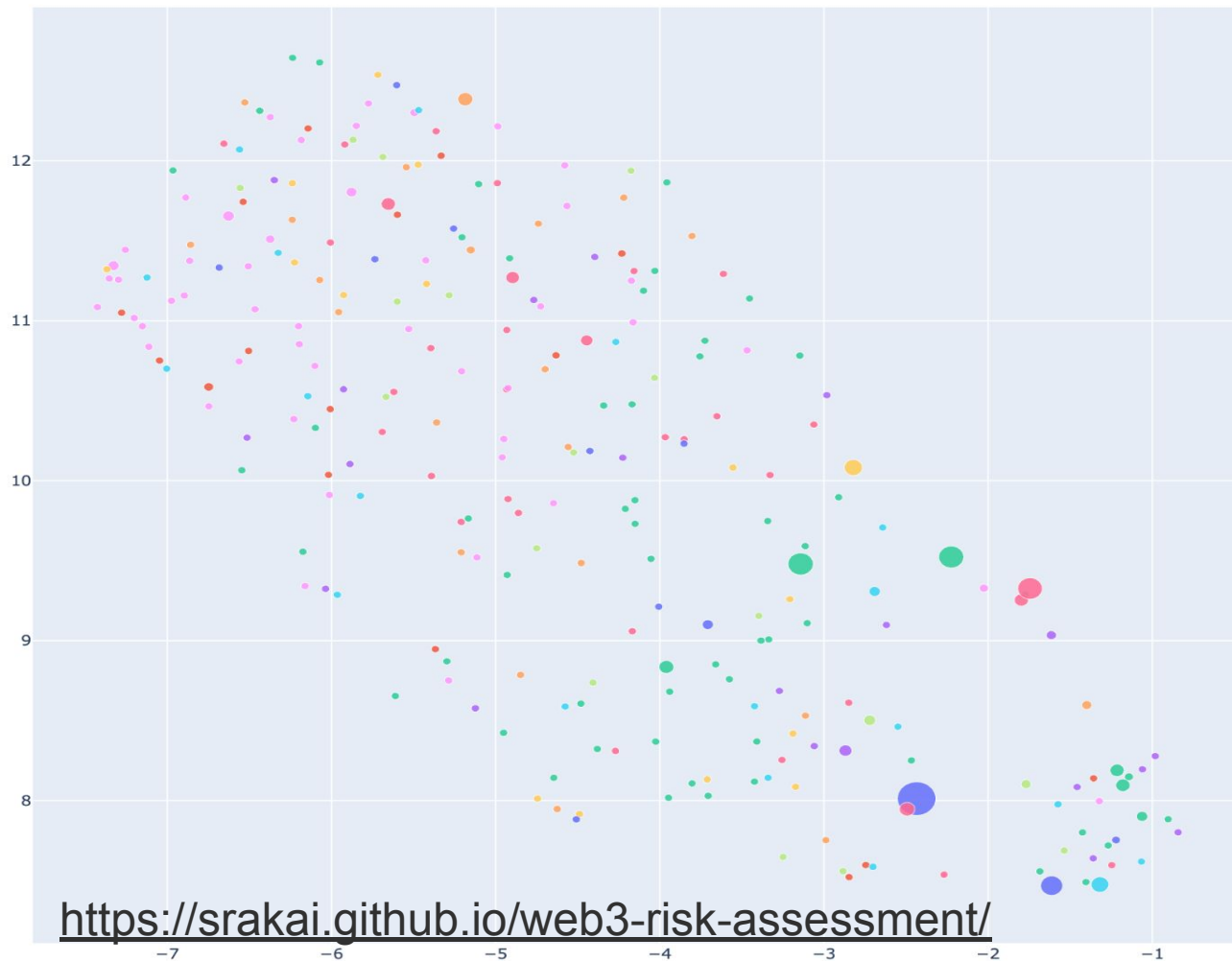
# Current Solutions

## Certik Skynet Score Methodology

$$\text{Feature1} * w1 + \text{Feature2} * w2 + \dots = \text{Risk Score}$$

- Unscalable (semi-manual scoring)
- Simplified, uncorrelated metric (features do not attend to itself)
- Predefined weights induce human bias (risk for oracles)

## Global Hacking Landscape – App Embedding Projection (UMAP)



### Attack Vector

- Improper access control
- Integer Underflow
- Compromised Keys
- Access Control Vulnerability
- liquidity drain
- Rounding Error
- Logic Error
- Misconfiguration
- Re-entrancy
- Compromised Private Key
- Logic Error/Insider Trading
- Hot Wallet Compromise
- Access Control
- Private Key Compromise
- honeypot
- Reentrancy via IBC hooks
- Governance Takeover
- Supply Chain Attack
- Fake Token Attack
- flash-loan-attack
- Front-end attack
- Price Manipulation
- liquidity pull
- Telegram Message Oracle Manipulation
- Flash Loan Attack
- hot wallet compromise
- Forged Proofs/Bridge Exploit
- Infinite Mint
- Price Oracle Manipulation
- admin-key-compromise
- Front-end Spoofing, Blind Signing, Smart Contract Vulnerability
- phishing-attack
- Infinite Mint / Incomplete Collateral Validation
- Bug Bounty Abuse
- Precision/Rounding Error
- Proxy contract exploit
- Read-only Reentrancy & Sandwich Attack
- Improper Input Validation
- infinite-mint-vulnerability
- Governance Manipulation

<https://srakai.github.io/web3-risk-assessment/>