



Hyper DefeneX

**"AI and Blockchain Powered automated
SIEM and SOAR platform"**

A fully automated, blockchain-secured, explainable AI-driven cybersecurity and log defense platform that redefines threat detection, SOC automation, and forensic trust at scale.



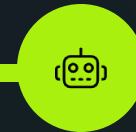
Project Summary

HyperDefeneX is a next-generation cybersecurity platform designed to protect digital systems using advanced log analysis, AI-based threat detection, immutable blockchain-backed evidence storage, and smart contract-driven response mechanisms. It is built to automate the work of a SOC analyst while enabling real-time threat detection, explainable decision-making, and trustworthy compliance reporting.



Advanced Log Analysis

Utilizes sophisticated algorithms to analyze log data for anomalies and potential threats.



AI-Based Threat Detection

Employs artificial intelligence to identify and predict cyber threats in real-time.



Blockchain-Backed Evidence

Ensures the immutability and trustworthiness of forensic evidence through blockchain technology.



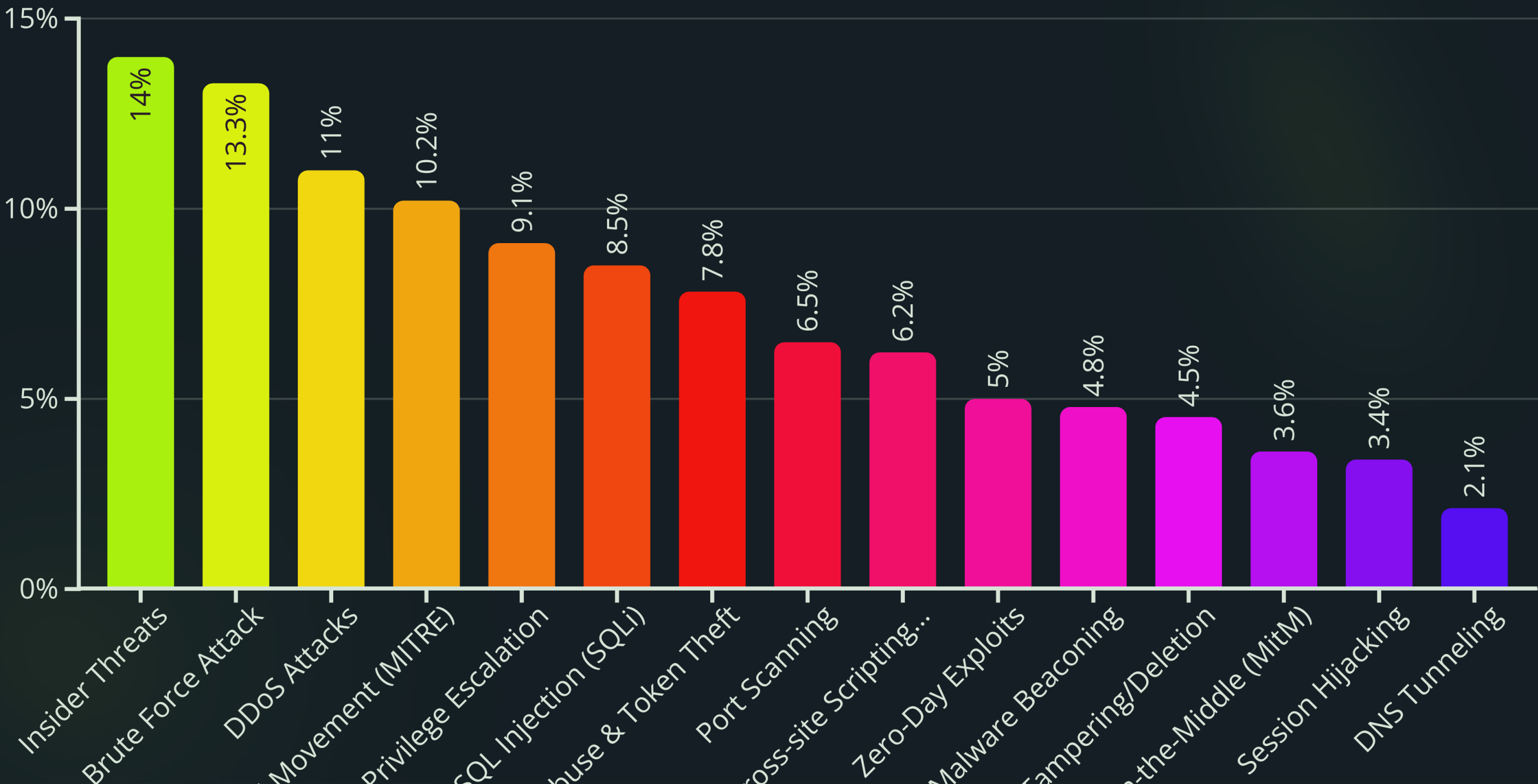
Smart Contract Response

Automates threat response mechanisms using secure and transparent smart contracts.

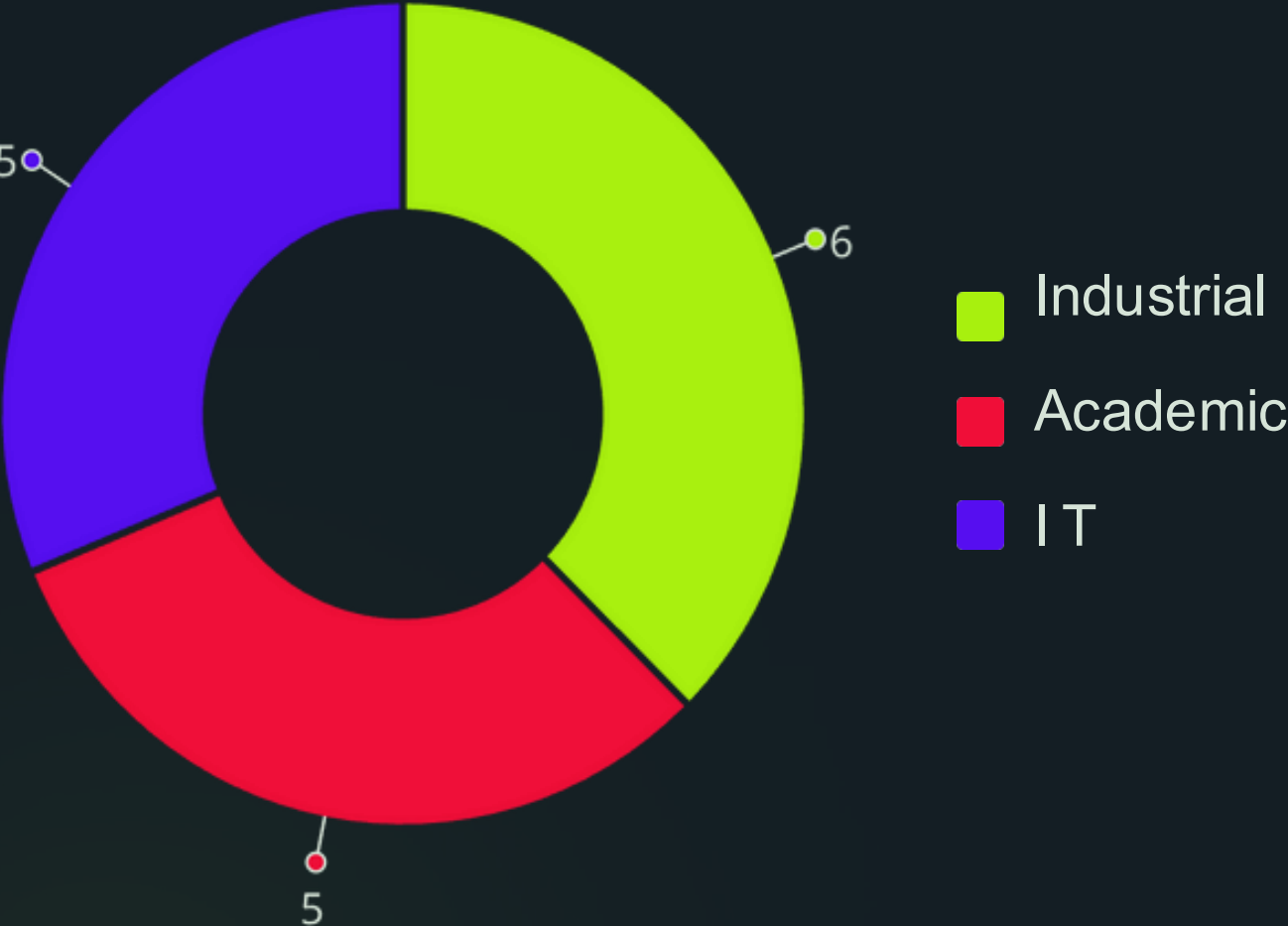
Need of this project

Reason for Development	Why Existing Solutions Fall Short
Full SOC Automation with Explainable AI	Most tools rely on manual analyst intervention or offer black-box ML decisions
Immutable Blockchain-Backed Logs	Traditional SIEMs store logs that can be altered or deleted post-incident
Smart Contract-Based Autonomous Response	Existing SOAR platforms require manual configuration and lack trusted execution
Self-Healing of Logs and Systems	No mainstream platform can auto-restore corrupted/missing logs in real-time
Federated Threat Intelligence without Data Sharing	Current platforms rely on centralized databases and compromise data privacy
Zero Trust Enforcement via Behavioral Log Analysis	Most Zero Trust tools don't dynamically adapt based on log intelligence
One-Click Compliance and Forensic Replay	Compliance is manual, slow, and lacks trustworthy log trails in current tools
Real-Time Explainability (XAI) for Analyst Confidence	Most EDR/AI tools provide no interpretability, reducing trust in automation
Integration of All Layers in One Unified Stack	Tools like SIEM, SOAR, XDR, and blockchain are separate, fragmented, and costly

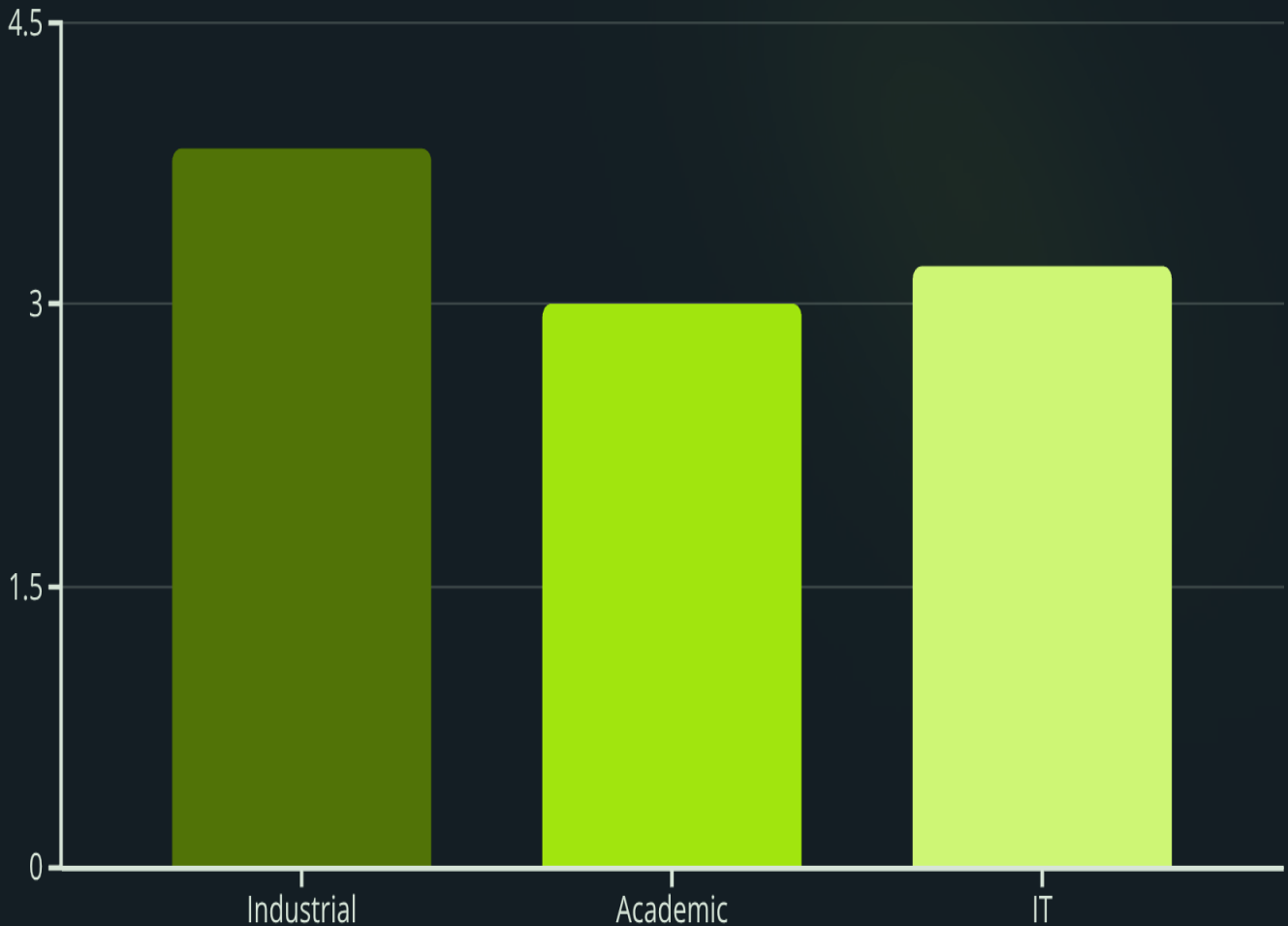
Current Threats in Industries



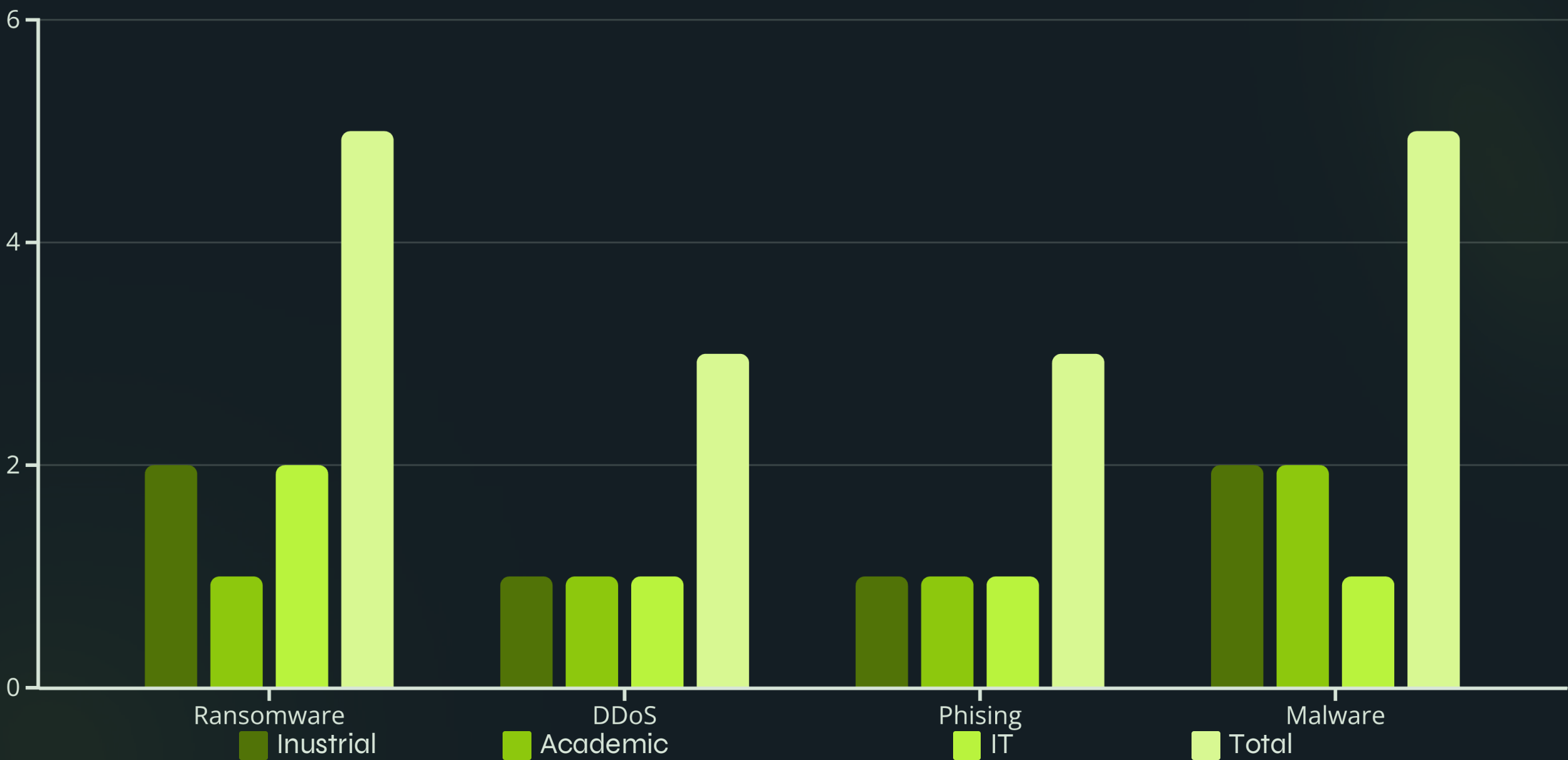
Attack Frequency by Sector











Average Severity by Sector (Scale: 1 = Low, 5 = Critical)



Attack Type Breakdown (Example placeholder)



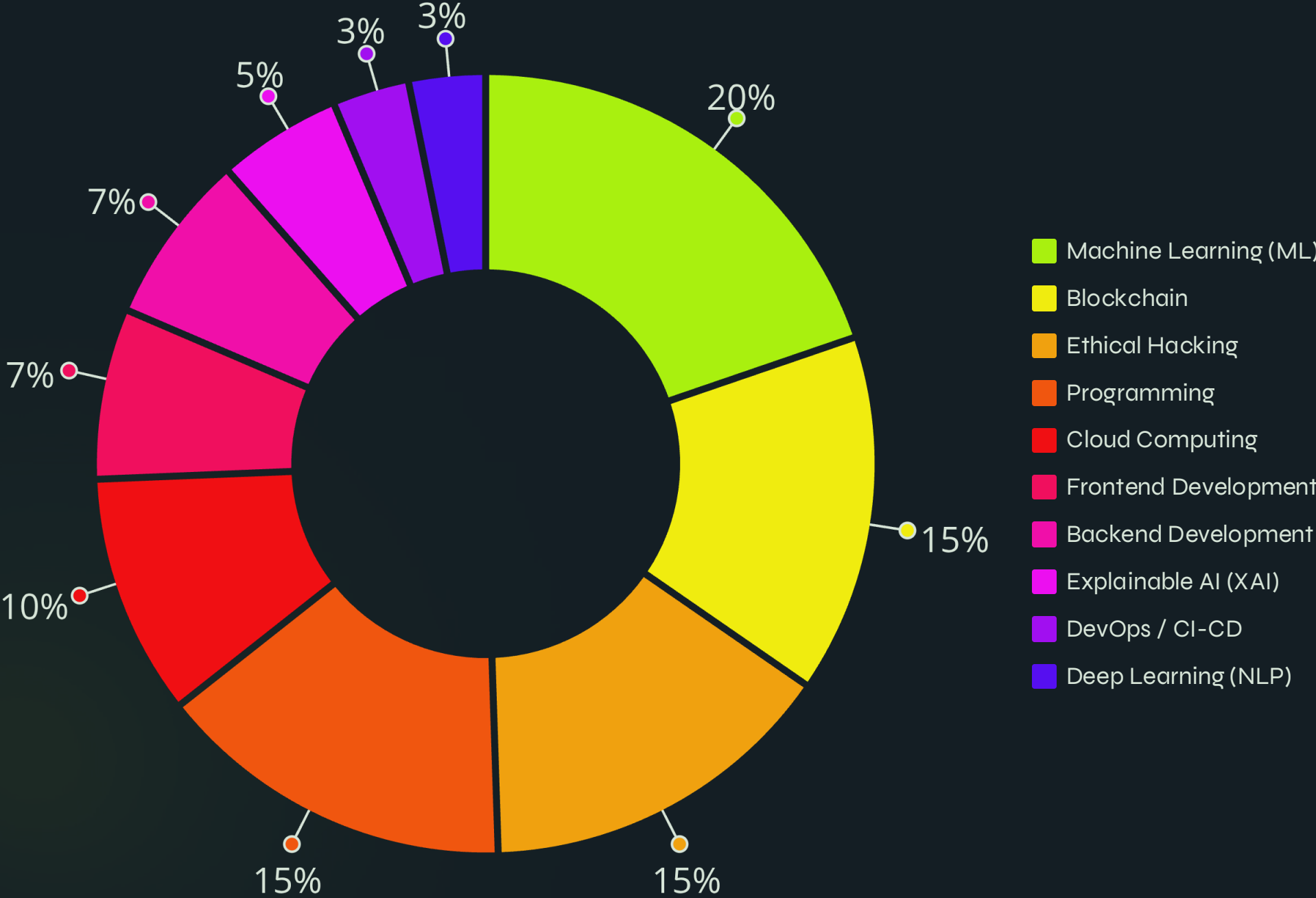
UNIQUE SELLING POINTS

USP Component	Description
 Explainable AI (XAI)	Transparent decisions using SHAP, LIME, and attention models for every detected threat
 Immutable Blockchain Logging	Logs are tamper-proof and cryptographically verifiable using Ethereum + IPFS
 Smart Contract SOAR Automation	Autonomous threat response and compliance enforcement via on-chain smart contracts
 Self-Healing Infrastructure	Automatically detects, repairs, and replaces corrupted or deleted logs
 Federated Threat Intelligence	Learns from global threat patterns without sharing private data (privacy-preserving learning)
 Zero Trust Architecture	Dynamic risk-based access control powered by continuous log behavior analysis
 One-Click Compliance Reporting	Instantly generate SOC2, NIST, ISO27001-compliant reports with forensic log replay
 Unified Full-Stack Platform	Combines SIEM, SOAR, XDR, Blockchain, and XAI into a single deployable system

TECHS TO BE USED

Category	Description	Best Tech Stack / Language
Machine Learning (ML)	For log classification, anomaly detection, and threat prediction	Python (scikit-learn, PyTorch)
Blockchain	Immutable log storage + smart contract-driven responses	Solidity + Python (web3.py)
Ethical Hacking	Simulate attacks for ML training/testing (e.g., SQLi, brute force)	Kali Linux tools (Nmap, Burp Suite)
Programming	Core logic, orchestration, integrations across all modules	Python
Cloud Computing	Hosting services, backend deployment, data security	AWS (EC2, S3, CloudWatch)
Frontend Development	SOC dashboard, real-time alerts, visualizations, explainable AI	JavaScript (React.js)
Backend Development	APIs, microservices, ingestion engine, smart contract interactions	Python (FastAPI)
Explainable AI (XAI)	Visualizing ML decisions with SHAP/LIME for analyst trust	Python (SHAP, LIME)
DevOps / CI-CD	Pipeline automation, containerization, version control integration	GitHub Actions + Docker
Deep Learning (NLP)	NLP-based threat detection from unstructured logs	Python (Hugging Face, Transformers)

Tech Stacks



SOLUTIONS

Problem in Cybersecurity	Solution Provided by SentinelOneX HyperDefender
Log overload and slow detection	AI/ML log classification and real-time threat detection
Insider threats and privilege abuse	Behavioral monitoring with Explainable AI
Log tampering and lack of evidence	Blockchain-based immutable logging
SOC analyst burnout and inefficiency	90%+ automated SOC operations via AI + smart contracts
Insecure threat sharing	Federated model updates without raw data sharing
Lack of visibility and context	Interactive dashboards + replayable incident timelines
Regulatory burden and manual audits	One-click compliance reports (SOC2, NIST, ISO27001)
Static trust models	Zero Trust access enforcement based on real-time logs

Key Inputs

- Web server logs (Apache, Nginx)
- Application and API logs
- Authentication & access logs (login, session events)
- Firewall/IDS logs (e.g., Snort, Suricata)
- System logs (process execution, script activity)
- Cloud infrastructure logs (AWS/GCP audit events)
- DNS and network logs (for tunneling/exfiltration detection)

Key Outputs

- Real-time threat alerts (dashboard, email, webhooks)
- SOC dashboard (live heatmaps, AI verdicts, filters)
- Immutable log storage (via Ethereum + IPFS)
- Smart contract-triggered responses (e.g., block IP)
- Explainable AI reports (SHAP, LIME visualizations)
- Compliance reports (SOC2, NIST, ISO27001)
- Forensic timeline & session replay
- Auto-generated threat summaries



Developmet timeline

