

Heimdall Intelligence Platform, developed by Zaden Technologies, is a state-of-the-art cybersecurity solution designed to protect critical systems against the ever-evolving landscape of cyber threats. By leveraging advanced artificial intelligence and machine learning, Heimdall offers unparalleled threat detection and automated incident response capabilities, ensuring the security and resilience of your organization's digital assets.

KEY FEATURES



AI-DRIVEN ANOMALY DETECTION

Real-Time Analysis:

Continuously monitors network traffic and system logs for real-time threat detection.

Advanced Algorithms:

Utilizes unsupervised learning techniques like clustering and autoencoders, and supervised methods such as SVMs and random forests.



USER & ENTITY BEHAVIOR ANALYTICS (UEBA)

Behavior Profiling:

Establishes baseline behavior profiles to detect deviations indicating insider threats or breaches.

Contextual Analysis:

Reduces false positives by using contextual information for more accurate threat detection.



AUTOMATED INCIDENT RESPONSE

Playbooks:

Features automated playbooks for rapid threat containment and system isolation.

SIEM Integration:

Seamlessly integrates with existing SIEM systems for centralized logging and analysis, enhancing incident response.



SCALABILITY & ADAPTABILITY

Containerization:

Built with containerization technologies like Docker and orchestration platforms like Kubernetes for easy deployment and management.

Data Integration:

Supports integration with various data sources, including Elasticsearch, Amazon S3, and PostgreSQL, for comprehensive data ingestion and analysis.



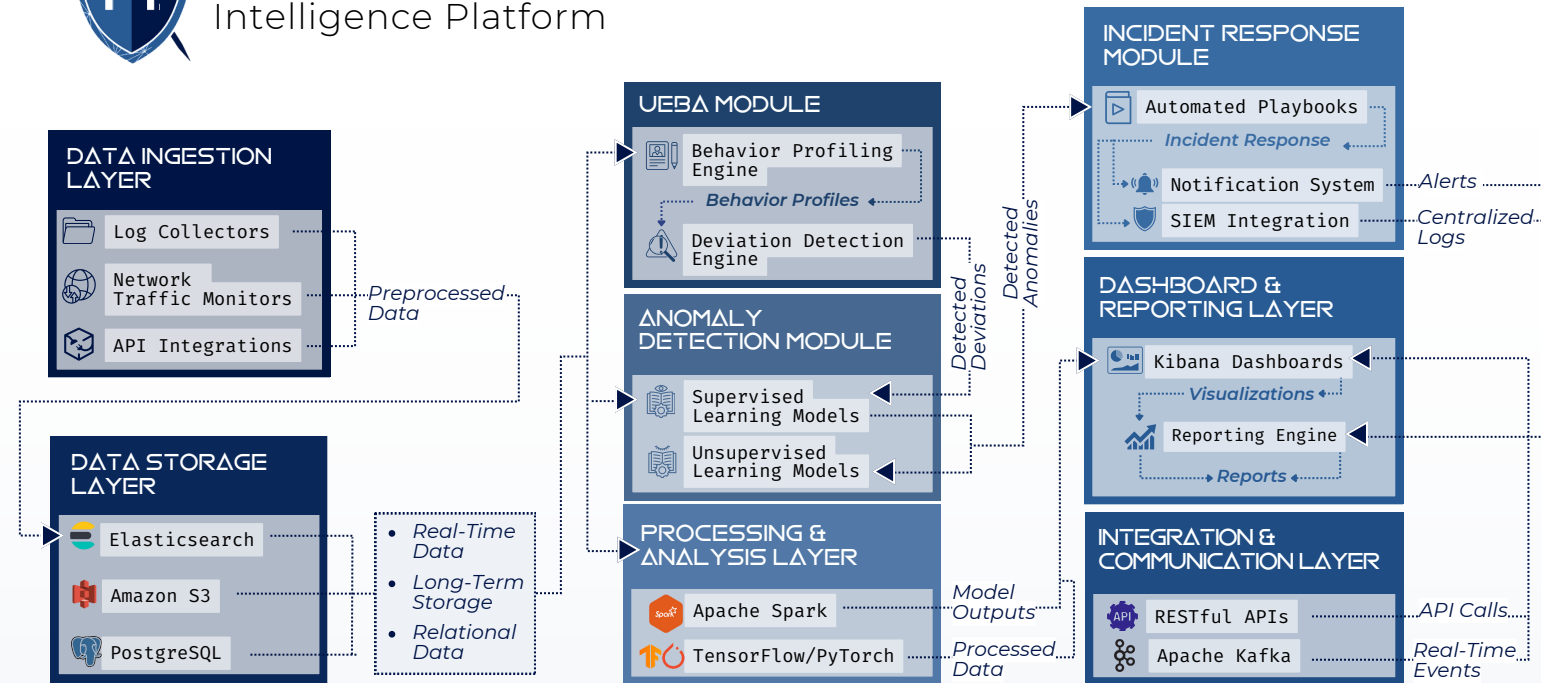
ZERO-TRUST SECURITY PRINCIPLES

Continuous Authentication:

Enforces continuous authentication and least-privilege access control to minimize attack surfaces.

Micro-Segmentation:

Implements micro-segmentation to contain breaches, ensuring robust network security effectively.



HEIMDALL INTELLIGENCE PLATFORM ARCHITECTURE

INTEGRATED SECURITY FRAMEWORK

ON-PREMISE SECURITY OPERATIONS CENTER

Web Application:

Provides a user-friendly interface for security analysts.



API Gateway:

Routes requests to appropriate services ensuring seamless communication and data flow.



CYBER HARDENED CLOUD INFRASTRUCTURE

Data Processing:

Processes data for advanced threat detection and analysis.



Long-term Storage:

Securely store raw and processed data for long-term analysis and retrieval.



HEIMDALL'S CONTINUOUS FEEDBACK WORKFLOW

Request a Demo &

Learn how **Heimdall** can enhance your organization's cybersecurity posture.

Google Form:

<https://forms.gle/S21AYLxJ37BykdHF6>

