# Abyssal Watcher v1.0.6 - STUXNET-Resistant Edition

\*\*Abyssal Watcher\*\* is an advanced threat detection and defense framework designed with extreme resilience and security in mind. The v1.0.6 STUXNET-Resistant upgrade is engineered for high-assurance environments where zero-tolerance for breach or covert operations is critical.

## Key Features

### 1. Advanced Threat Detection Engine

* - Behavioral analysis of processes and binaries
* - Signatureless anomaly detection
* - Real-time threat mapping and alert generation

### 2. Modular Architecture

* - `core/`: Core detection logic and policies
* - `analyzer/`: Static and dynamic binary analysis modules
* - `defense/`: Automated response mechanisms (e.g., process kill, system lockdown)
* - `engine/`: Orchestrator for scan, detect, and respond routines

### 3. Hardened STUXNET-Grade Resistance

* - Binary-level obfuscation resistance
* - Anti-debugging, anti-emulation, and anti-reversing capabilities
* - Memory access audit and executable verification layers

### 4. Integration & Extensibility

* - Exports logs in standard syslog and JSON formats
* - SIEM integration ready (Elastic, Splunk, Graylog)
* - Clean RESTful API for data access and orchestration

## Web Dashboard

\*\*Tech Stack:\*\* React + TailwindCSS frontend, Rust API backend

### Features:

* - Real-time threat visualizations
* - Component health status
* - Authentication via JWT
* - Frontend (port `3000`), Backend (port `8080`)

## DevOps & Deployment

### Docker

* - Pre-built `Dockerfile` for Rust backend
* - `docker-compose.yml` to launch full stack (frontend + backend + logs)

### GitHub Actions

* - `.github/workflows/test.yml`: Runs unit tests on push/PR

### Unit Testing

* - Structured test suite for `core`, `engine`, and `defense` modules using Rust’s built-in test framework

## Documentation

### Whitepaper

* - Includes threat model, architecture overview, and unique innovations
* - Located in `docs/whitepaper.pdf`

### Installation Guide

```

git clone https://github.com/DDW-X/abyssal-watcher-site.git

cd abyssal-watcher-site

docker-compose up --build

```

## License

\*\*Apache License 2.0\*\*

* - Open for use, modification, and distribution
* - Requires attribution to original author

## Author

* - GitHub: [DDW-X](https://github.com/DDW-X)
* - Project Lead, Security Researcher, Systems Engineer

## Contributing

Pull requests, issue reports, and forks are highly welcome. Please see `CONTRIBUTING.md` for guidelines.

## Disclaimer

This software is provided "as is" without any warranties. Designed for educational, research, and enterprise-grade defense use. Ensure compliance with your local laws before deployment.