

[Request Information](#)

[Permalink](#)

Host-Based Intrusion Detection Systems Powered By Large Language Models

Tech ID: 34610 / UC Case 2026-533-0

BRIEF DESCRIPTION

SHIELD leverages a customized large language model pipeline to detect and investigate sophisticated cyber threats with high accuracy and interpretability.

FULL DESCRIPTION

SHIELD is an innovative host-based intrusion detection system (HIDS) that integrates advanced large language model (LLM) techniques with semantic reasoning and behavioral profiling to analyze fine-grained system logs. It addresses common challenges in traditional HIDS such as high false-positive rates and inconsistent results by employing a tailored LLM pipeline featuring event-level Masked Autoencoders, deterministic data augmentation, and multi-purpose prompting. This results in precise detection and interpretable attack investigations across diverse computing environments.

SUGGESTED USES

- » Enterprise security operations centers (SOCs) for advanced threat detection
- » Research environments focusing on cybersecurity and intrusion detection
- » Organizations requiring protection across diverse platforms like Linux and Windows
- » Enhancement of existing HIDS deployments through AI-driven analysis
- » Security benchmarking and testing of host activity datasets

ADVANTAGES

- » High accuracy in detecting advanced persistent threats (APT) and insider threats
- » Robust across various operating systems and log datasets
- » Reduced false positives and enhanced interpretability for analysts
- » Integrates semantic analysis and behavioral profiling for comprehensive threat detection
- » Supports both real-time and retrospective intrusion detection
- » Automates generation of detailed attack narratives to aid security triage

CONTACT

Jane Park
jane.park@uci.edu
tel: .



OTHER INFORMATION

CATEGORIZED AS

- » **Computer**
 - » Software
- » **Security and Defense**
 - » Cyber security

RELATED CASES

2026-533-0

UCI Beall
Applied Innovation

5270 California Avenue / Irvine, CA
92697-7700 / Tel: 949.824.2683



© 2026, The Regents of the University of
California
[Terms of use](#)
[Privacy Notice](#)