PHANTOM: Predictive Security Policy Orchestration for Detecting Multi-stage Stealthy Attacks

Authors : Yujeong Seo, Hyunwoo Lee | Number : 108

WISA 2025

1. Why PHANTOM?

1.1 Spread of intelligent attacks

Recent cyberattacks have evolved into intelligent, multi-step Advanced Persistent Threat (APT) attacks, evading detection at each stage.

Conventional security solutions (firewalls (FW), intrusion detection systems (IDS), endpoint detection and respons(EDR)) provide only partial visibility and fail to detect the full attack chain.

PHANTOM We develop a unified system to respond to such APT attacks.

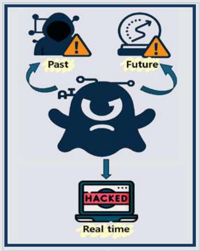
1.2 Limitations of existing systems

1) Inability to detect novel attack scenarios
2) A challenge of maintaining rules
3) Dependency on logs from individual device

1.3 Necessity and role of PHANTOM

PHANTOM overcomes existing security limitations with AI-driven predictive orchestration :

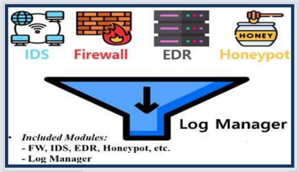
- Past
  Honeypot-based threat discovery that reveals past intrusions and hidden footholds
- Real time
  AI-powered log correlation that detects ongoing attacks by analyzing all security event data in real time
- Future
  Attack chain modeling that anticipates and blocks future threats before they unfold



2. How is PHANTOM structured?

2.1 Data collection & preprocessing

PHANTOM gathers security logs from diverse sources (e.g., FW or IDS) and standardizes them for analysis.

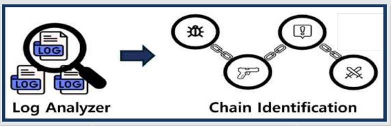


- *Included Modules:*
  - FW, IDS, EDR, Honeypot, etc.
  - Log Manager

- ***Log Manager***
  - Collects and unifies logs from diverse security devices.
  -Removes noise and normalizes data for consistent analysis.

2.2 Threat detection & scenario analysis

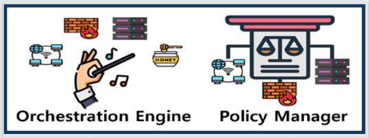
PHANTOM detects abnormal behaviors and reconstructs attack scenarios through event correlation.



- ***Log Analyzer***
  - Detects abnormal behaviors using AI and threat intelligence.
  - **Associates meaningful events** while filtering irrelevant events.
- ***Chain Identification***
  - **Reconstructs multi-step attack chain** by correlating related events.
  - Provides full-context understanding of threat progression.

2.3 Decision making & response orchestration

PHANTOM determines system-wide decisions and generates real-time response strategies based on analytical insights.



- ***Orchestration Engine***
  - Evaluates threats in context and selects suitable response strategies.
  - **Coordinates system-wide decisions** based on real-time analytics.
- ***Policy Manager***
  - Generates actionable policies from orchestration outcomes.
  - Supports automated, device-specific policy deployment.

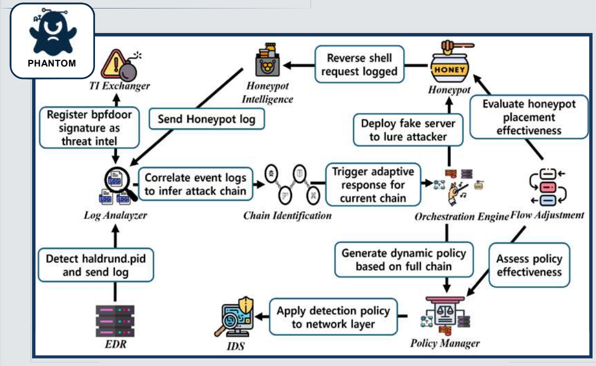
2.4 Execution & intelligence feedback

PHANTOM enforces defense actions and continuously enhances system intelligence through feedback and threat data integration.

- ***Flow Adjustment***
  - Evaluates the effectiveness of isolation and honeypot engagement
  - Dynamically adjusts policies or deception components to enhance response accuracy
- ***Honeypot Intelligence***
  - Analyzes attacker behavior in decoy environments.
  - **Reveals stealthy activity** and strengthens future detection.
- ***Threat Intelligence Exchanger***
  - Fuses internal detection with external TI sources.
  - Continuously updates system knowledge for improved accuracy.

3. What can PHANTOM do?

3.1 Respond to BPFDoor


PHANTOM
TI Exchanger
Honeypot Intelligence
Reverse shell request logged
HONEY
Honeypot
Register bpfdoor signature as threat intel
Send Honeypot log
Deploy fake server to lure attacker
Evaluate honeypot placement effectiveness
Correlate event logs to infer attack chain
Trigger adaptive response for current chain
Log Analayzer
Chain Identification
Orchestration Engine
Flow Adjustment
Detect haldrund.pid and send log
Generate dynamic policy based on full chain
Assess policy effectiveness
Apply detection policy to network layer
EDR
IDS
Policy Manager

This work was supported by the Technology Innovation Program (RS-2025-02653102, An Unbreachable Multilayer AI-based Security Mechanism that Continuously Adapts and Evolves in Dynamic Conditions) funded By the Ministry of Trade Industry & Energy (MOTIE, Korea)