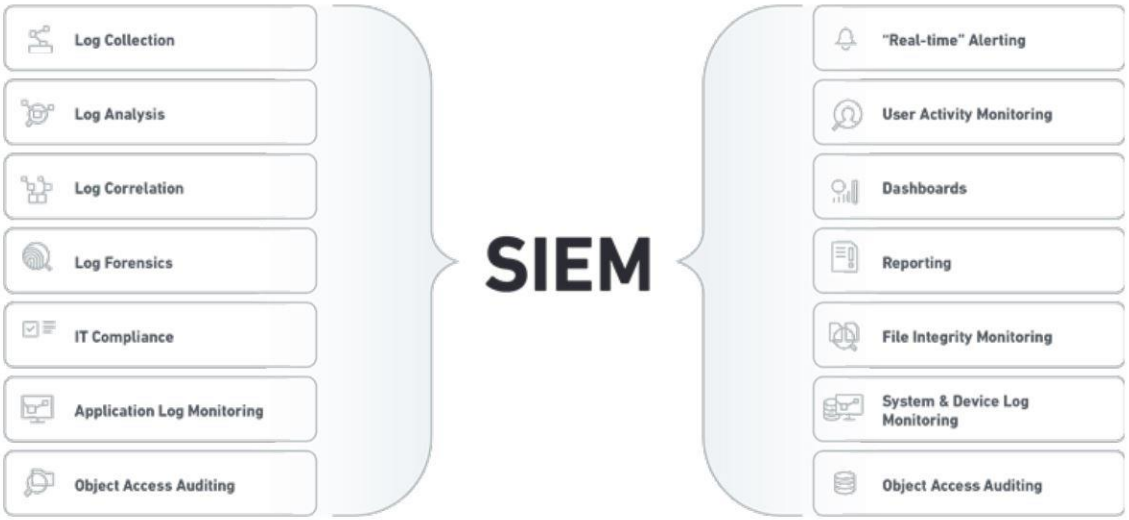
HPT INTELLIGENT SECURITY FOR MODERN WORKPLACE

HCapollo: Your Strategic Defense Partner

HCapollo, the pinnacle of intelligent security solutions, acts as the vital link between traditional security and advanced defense systems. Engineered to centralize data management, integrate advanced features, and ensure 24x7 operational excellence, HCapollo is designed to proactively detect threats, fortify compliance, and overcome security challenges faced by organizations.



Key Features and Benefits

1. Unified Security Management:

- Overcome incoherence between security systems.
- Enable comprehensive 24x7 monitoring for enhanced security.

2. Digital Transformation Support:

- Facilitate effective monitoring of applications.
- Seamless integration for organizations undergoing digital transformation.

3. Rapid Threat Detection and Response:

- Quick detection and alerting of security incidents.

- Swift response to complex and targeted attacks on the system.

4. Digital Forensics Capability:

- Enable digital forensics in the event of a security incident.
- Provide valuable insights for post-incident analysis.

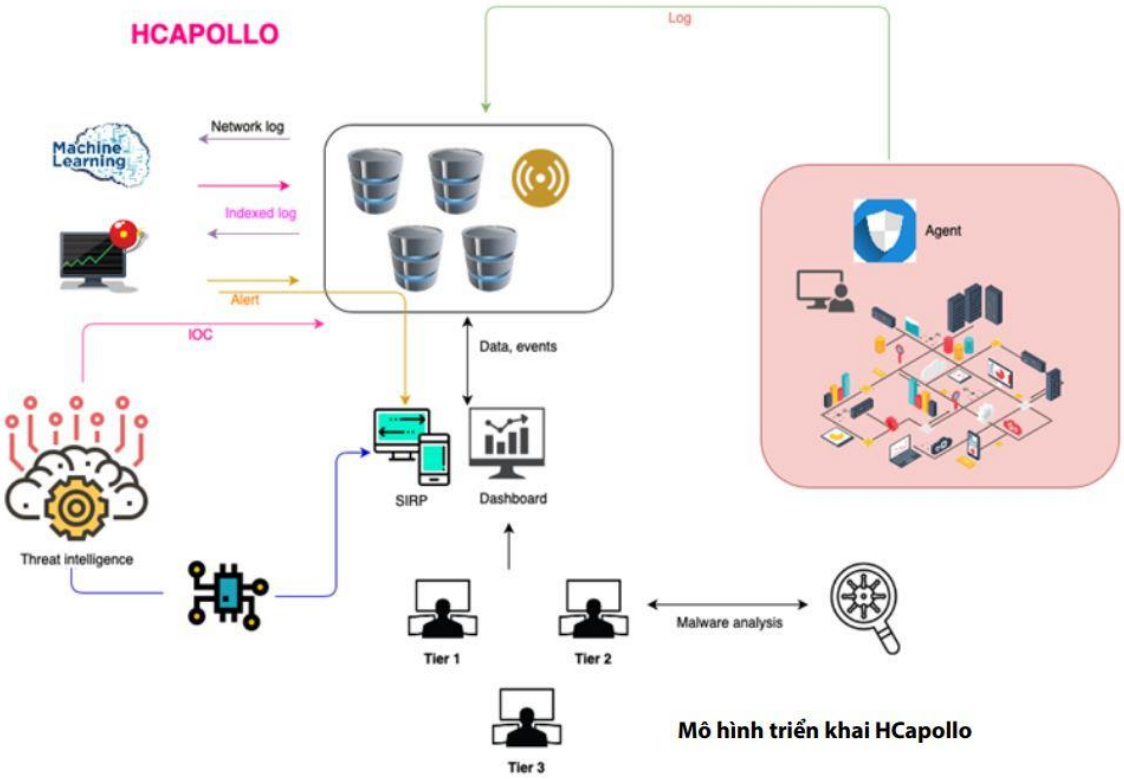
5. Scalability and Customization:

- Support integration for unlimited input and events per second (EPS).
- Meet compliance, log policy requirements, and adapt to organizational characteristics.

High Performance and Deployment Models

High Availability and Redundancy:

- Designed with redundancy for maximum fault tolerance.
- Two platform architectures: Single for small organizations, Cluster for large-scale enterprises.
- Supports on-premises, on-cloud, or hybrid deployment models.



Mô hình triển khai HCapollo

Data Collection, Identification, Normalization, and Enrichment

Enhanced Visibility for Effective Analysis:

- Collects and processes data from unlimited sources.

- Normalizes, filters, classifies, and enriches data for comprehensive analysis.
- Enrichment includes external sources for expanded context.

Collectable and Unlimited Event Sources:

- Security events, network events, network activity, cloud events, user and asset context, endpoint events, application events, and threat intelligence.

Threat Core Analytics, Detection, and Alert

Real-Time Attack Analysis and Correlation:

- Utilizes advanced correlation, signature recognition, blacklisting, whitelisting, statistical analysis, and machine learning.
- Leverages MITRE ATT&CK for understanding attack scenarios and early alerting.

Knowledge-Powered Alerting:

- Harnesses MITRE ATT&CK knowledge base and Threat Intelligence for accurate threat identification.
- Offers a flexible rule set system for customization.

Security Alert and Incident Lifecycle Management

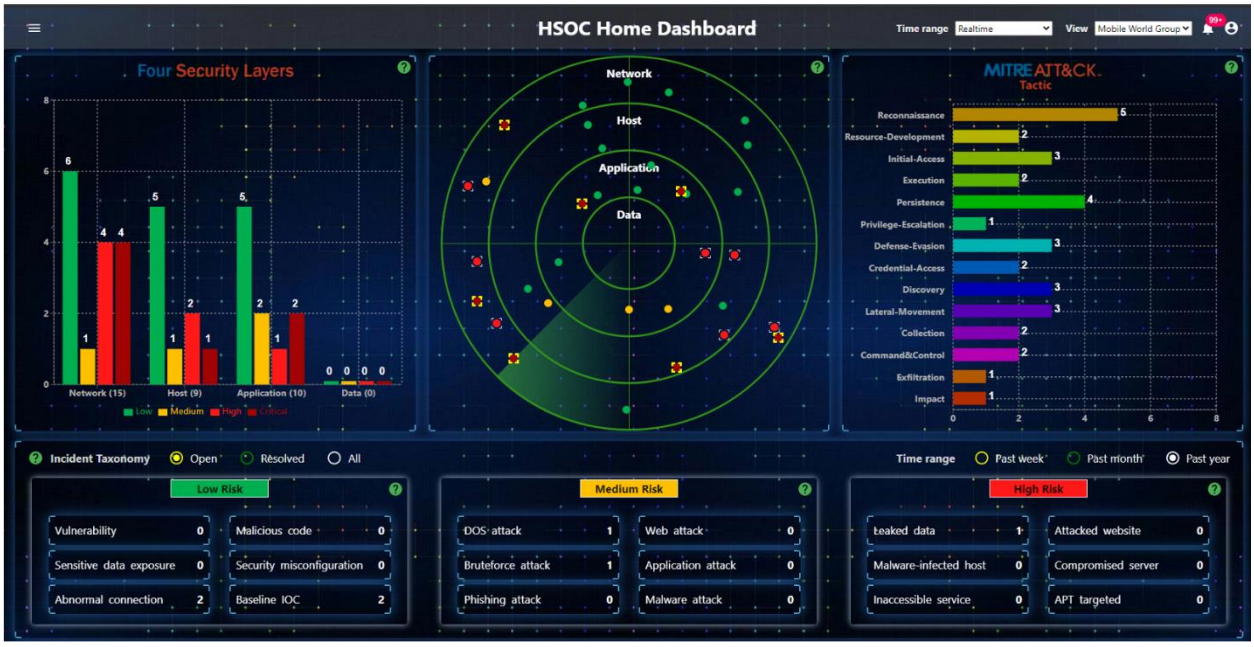
Efficient Incident Response:

- Manages security alert and incident lifecycle according to defined workflows.
- Customizable workflows built on organizational experience, policies, and knowledge.
- Provides a unified console for different user roles.

Security Monitoring Interface

Comprehensive Monitoring Dashboard:

- Intuitive and diverse main monitoring dashboard.
- Built according to HPT SOC's best practice.
- Visual representation of assets, EPS, processed data, and common security incident use cases.



Automation Workflow

Maximizing SOC Efficiency:

- Provides automation workflows for information security incident handling.
- Customizable templates ensure efficiency and maintainability.
- Augments monitoring teams, reducing investigation time and maximizing processing capacity.

Empower Your Security Strategy with HCapollo – Your Shield in the Cyber Battleground