Datasheet

Viettel Anomaly & Kill-chain Detection
(VCS - KIAN)

viettel security

Necessity of the Solution

In the 4.0 technology era, it is more and more complex to handle such dangerous actors like malware, internal threats, and targeted attacks from other hacker groups. Since the methods of exploiting and masking the behavior of these actors are increasingly sophisticated and difficult to detect, traditional solutions quickly become ineffective and unable to meet the needs of the Security Operation Center (SOC). To solve this problem, organizations need an advanced solution based on top innovations such as machine learning, behaviors analytics, and big data.

Viettel Kill-chain & Anomaly Solution

Viettel Kill-chain & Anomaly is a solution based on User and Entity Behavior Analytics. VCS-KIAN can automatically and constantly profile and chain the behavior of users and entities, combined with machine learning technology and real-time big data processing. This provides a powerful top-layer of analytics on the centralized Log management solutions like SIEM, allowing SOC experts to detect threats in early stage and promptly respond to them.

MAIN FEATURES

Integrate with SIEM and popular Security Solutions with Contents Mapping to MITRE ATT&CK

KIAN supports input data from many popular layers of Security solutions such as Firewall, VPN, Authentication, Email Security Gateway, EDR, etc. These data sources are integrated with SIEM (and ready to integrate with VCS-CyM, IBM QRadar, McAfee ESM). Immediately after integrating the input, KIAN perform behavioral analysis, and run use cases for each integrated data types. The use cases of KIAN are classified by APT problem groups, Insider Threat, Data Exfiltration, etc. and are referenced according to MITRE's ATT&CK matrix.

Model Behaviors of User and Entity

The Profiling Engine continuously analyzes and models the behavior of objects in the system, thereby building models to detect anomaly. Behavior classes are predefined by Security experts and cover all layers of monitoring solutions integrated in the system, such as the behaviors in Endpoint, behaviors related to Network, Email, Authentication, etc.

Provide Powerful Rule Engine

To solve the UEBA problem, KIAN improved the traditional rule-based approach and combined it with entity profiling and big data processing technology. Besides, focusing on the Content Developer/Detection Engineer user, KIAN provides an intuitive rule-writing interface and optimize the ability to transform knowledge from experts into system knowledge.

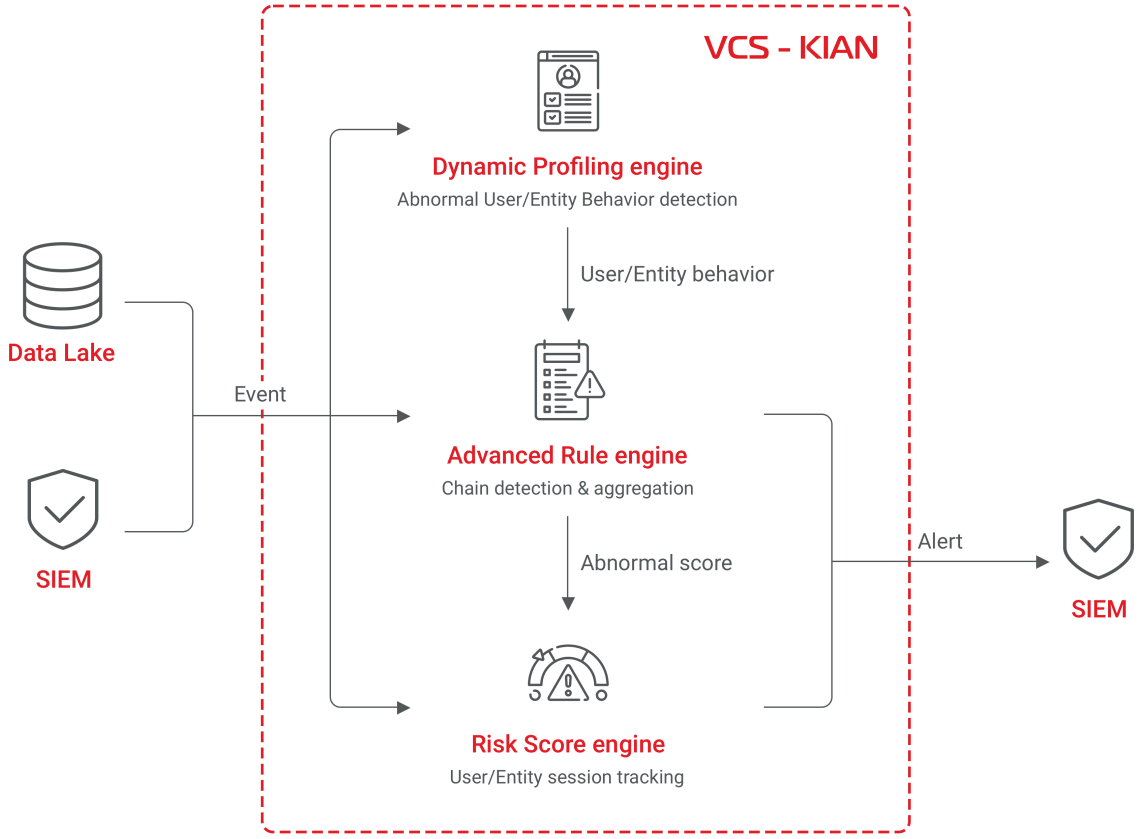
Provide Insight into Existing Threats in the Organization with Threat Management

With Threat Management, KIAN provides user with signs of threats on users and objects in the system. KIAN automatically assesses the threat level and the objects need operating by the analyst. Each object is reconstructed by the system with a timeline of anomalies, rule breaks, as well as information that the system has profiled. Thus, SOC experts can make quick decisions to assess the threat level of objects based on the popular Kill chain model.

Viettel Anomaly & Kill-chain Detection

(VCS - KIAN)

viettel security



OPERATION MODEL

Dynamic Profiling engine

Engine uses statistical modeling, machine learning to analyze Security data to create users' profiles users and entities in the monitored system. It is possible to identify abnormal events that may be from the attacker.

Advanced Rule engine

The engine processes the real-time rule, analyzes events and gives abnormal warnings when the event violates the predefined scenario by the Security expert. Unlike traditional rule engines, KIAN Advanced Rule engine supports advanced math operations such as Model Profile Logics, AI Logics, Aggregate/ Windows Function Logics, Chain Rules.

Risk Score engine

The Engine relies on anomalous behaviors that the system monitors to make an assessment of the risk level of each user and entity. Then, prioritize the entities that need to be operated and handled to prevent information security incidents early.