LogEase SOC Security Operation Center

COMPANY INTRODUCTION

Beijing Yottabyte Information Technology Co., Ltd. (LogEase), a big data company driven by in-house technology and solutions, was founded in 2014 and has R&D centers in Beijing, Tianjin,Wuhan, Guangzhou, and Shenzhen.

LogEase is committed to helping customers in various countries and industries to optimize the value of big data, tackle IT difficulties efficiently, improve their IT operation capabilities and guarantee user experience in real time . The number of customers grows rapidly and has already reached over 800, spanning in over 100 cities in China and overseas .

LogEase was certified as National Specialized and Sophisticated "Little Giants" that produces the New and Unique Products in 2021. The company has obtained nearly 200 million RMB of VC investment from ZhenFund, Sequoia China, Danhua Capital and CGP Investment.

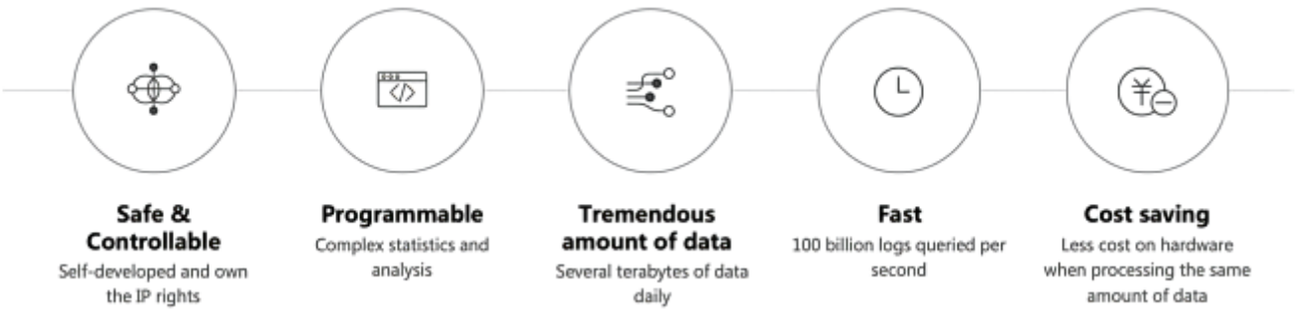
*"Little giants" are similar to "hidden champions", a term coined by German author Hermann Simon to describe the small, highly specialized world market leaders in Germany.

Gartner

LogEase is named sample vendor in two Gartner reports

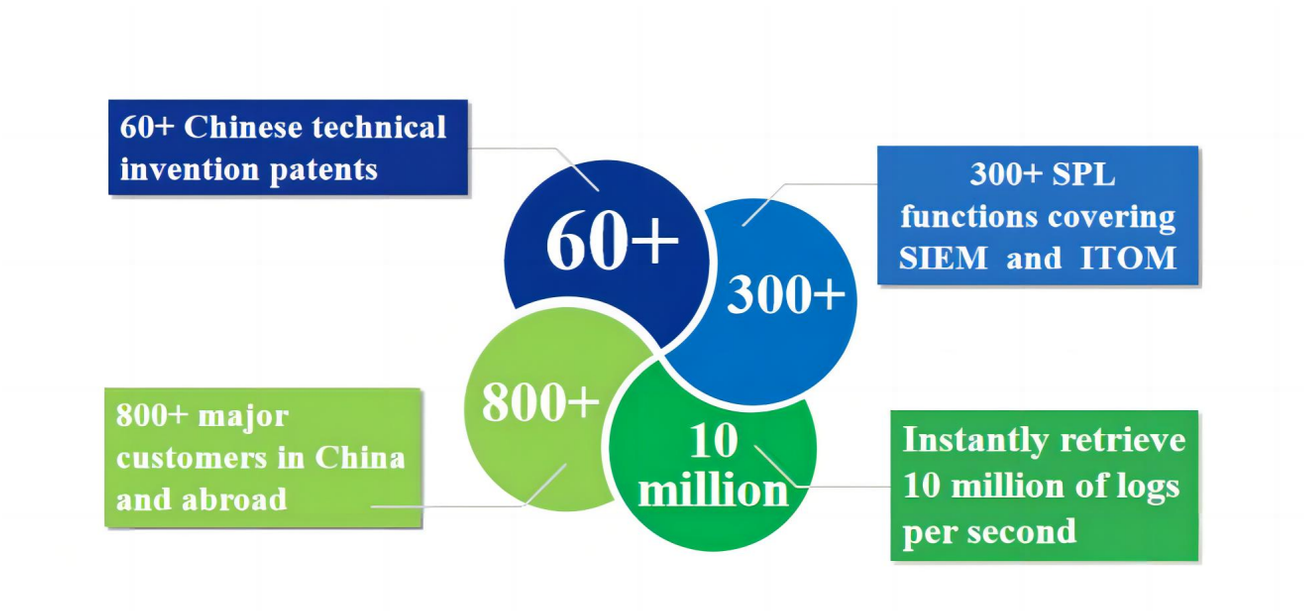
- **Hype Cycle™ for Security in China, 2024**
- **Market Guide for Managed Detection and Response Services, China**

TECHNOLOGICAL SUPERIORITY



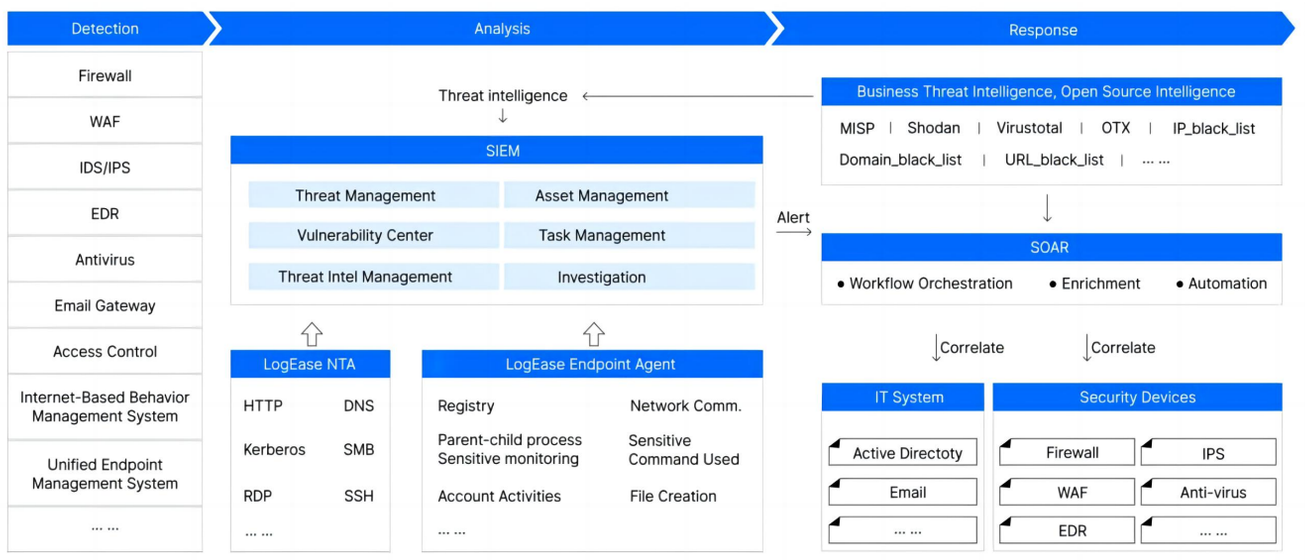
To achieve the independent innovation on the SIEM (Security Information and Event Management) and AIOps (Artificial Intelligence for IT Operations) , LogEase solved a series of key technologies and to self-develop the data search engine Beaver and LogEase SPL (Search Processing Language) that hold self-property right.

LogEase holds over 60 Chinese technical invention patents and over 40 Chinese appearance patents in LogEase SIEM (Security Information and Event Management)，SOAR (Security Orchestration, Automation and Response)， UEBA (User and Entity Behavior Analysis) ， AIOps (Artificial Intelligence for IT Operations)， IT Observability Monitoring Platform，Data Factory and Large Screen Display.



LOGEASE SECURITY INFORMATION AND EVENT MANAGEMENT

Based on LogEase Platform, enhance your threat detection, analysis and closed-loop response capabilities

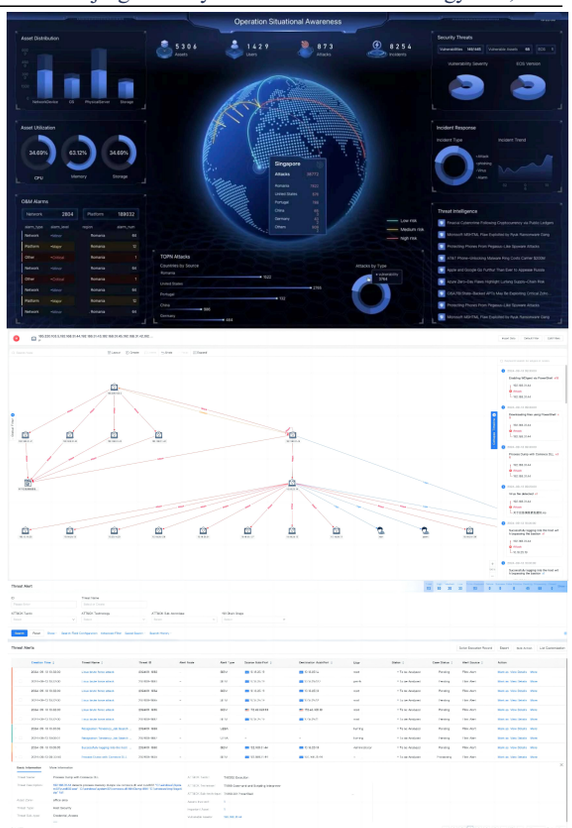


LogEase SIEM Platform Architecture

Relying on credible correlation and anomaly analysis capabilities, the LogEase SIEM platform can efficiently and flexibly detect, analyze, and respond to all-around threats. You can fully understand your data analysis, asset management, vulnerability management, threat management, an other information on the LogEase Large Screen, and easily adjust it through an intelligent, scalable, and customizable interface. After collecting, managing, retrieving, and analyzing all your data, the LogEase SIEM platform can conduct real-time and thorough investigations by analyzing abnormal threats, tracing the source of the kill chain according to the timeline, and detecting lateral movement through correlation analysis. LogEase is designed to facilitate your rapid, accurate, and automatic closed-loop response to threats, and deeply enhance your decision-making and proactive defense capabilities in daily security operations.

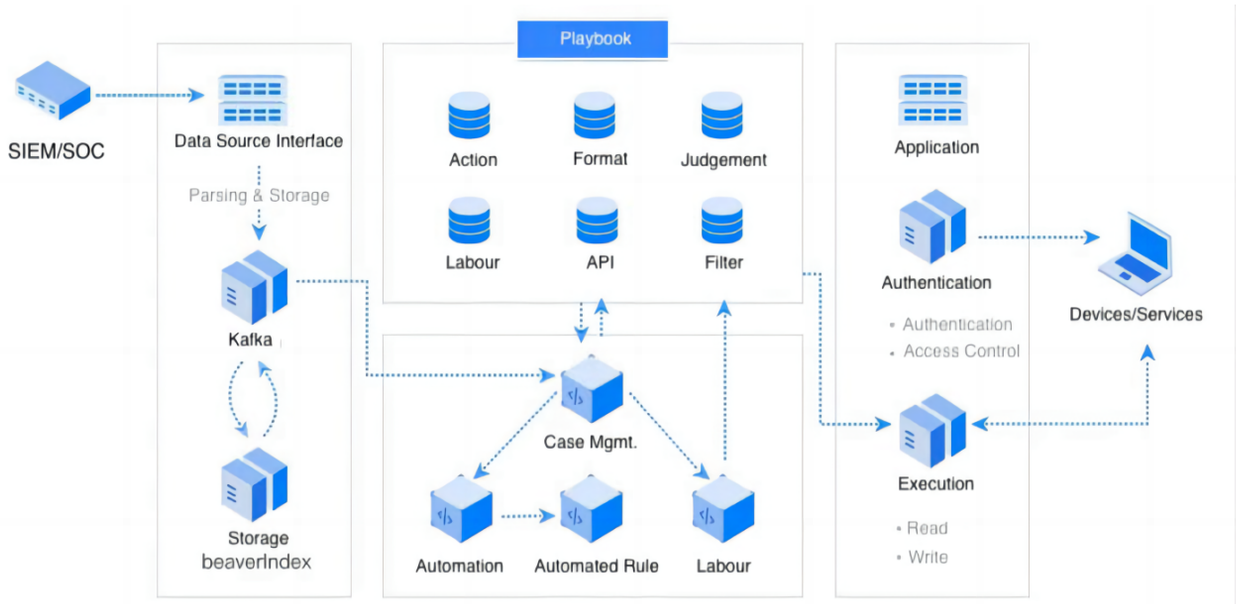
Threat Management Capability

A. Security posture and threat handling (correlating assets, vulnerabilities and threat intelligence, combining the exploitations of vulnerabilities and threats for correlation and matching to find high-risk threats)
B. Correlation analysis and alert noise reduction
C. Threat intelligence correlation
D. Threat investigation (endpoint investigation and network investigation)
E. Investigation (attack path analysis and timeline analysis)
F. Traceability analysis



SOAR (Security Orchestration, Automation and Response)

LogEase SOAR solution mainly realizes automated response through playbook defined for different types of security incidentsIt can obtain alerts from LogEase SIEM and realize automated security operations by interfacing with third-party systems, or other SIEM functional modules. LogEase SOAR built-in 80+ playbooks containing 50+ components for mainstream security devices (Firewall, WAF,EDR, etc.) and system (Email, Ticketing System), which can be linked to automatically respond to security incidents in seconds.



UEBA (User and Entity Behavior Analytics)

High-frequency Behavior Analysis

Through behavioral baseline analysis, certain types of user behaviors or multiple types of behaviors are found and compared with their historical baseline, and behaviors with large deviation degree (mainly positive deviation) are found. For example, if the AD login data shows that user A's login counts are different from the normal login counts on a certain day. an exception may exist.

Rare Behavior Analysis

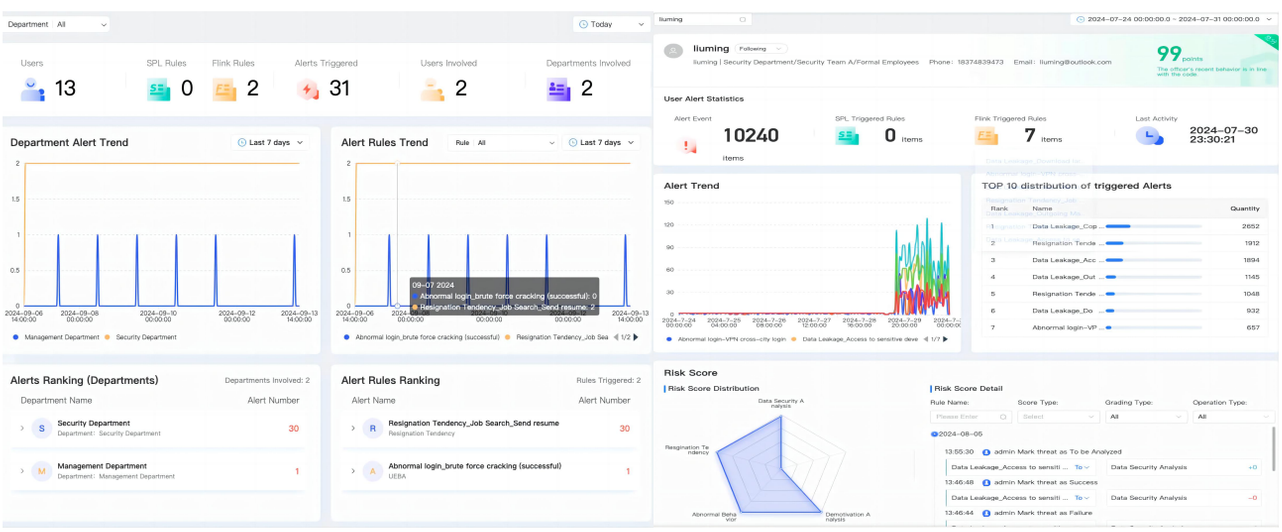
Normal users' office behaviors are often repetitive (generally related to the work content). If some rare behaviors occur, there may be abnormalities. For example, rare commands (such as rm -rf) are executed on the server and emails are sent to uncommon recipients. Sufficient historical data is required to support such analysis.

Individual/Group Behavior Comparison

People in the same department tend to behave in the same way, and abnormal behaviors can be found by comparing individual behaviors with group behaviors (mainly behavior baseline). For example, document copy baseline of the department, frequency of access to peripherals, etc.

Automated Behavior Discovery

Regular behavior is sometimes abnormal. Discover scheduled execution/operation behaviors, such as sending emails in batches by script. Discover possible leaks.



Features of LogEase SIEM

- High-performance log query and analysis engine
- A large number of log analysis models are built-in
- Correlated rule models
- Security orchestration, automation and response
- Graph analysis capability
- Security data streaming analytic capability

400-085-0159
contact@yottabyte.cn
https://www.logease.cn/