ManageEngine
Log360

User and entity behavior analytics (UEBA)

Learn how to identify and thwart malicious insiders and external threat actors.

manageengine.com/log-management

What is UEBA?

- ✓ Known as the anomaly detection capability of SIEM solutions, UEBA uses machine learning (ML) algorithms to detect anomalies in the behavior of users, hosts, and entities within a network.
- ✓ UEBA monitors log data to create behavioral profiles for every user and entity.

How UEBA detects anomalies

- ✓ UEBA leverages ML and statistical models to establish the baseline of expected activity.
- ✓ Anomalies are flagged when behavior deviates from the established baseline, and a suitable risk score is assigned.
- ✓ Example: A user who typically logs in at 10 AM is flagged if they log in at 5 AM.

Types of anomalies identified by UEBA

Time anomaly

Deviation in timing (e.g., logging in at unusual hours).

Count anomaly

Unusual frequency of actions (e.g., accessing the database 50 times in an hour).

Pattern anomaly

Irregular sequence of events (e.g., successful logins after multiple failures).

Types of anomalies identified by UEBA

Use cases

Insider threats, account compromise, data exfiltration, zero-day attacks.

Data sources

SIEM solutions, data lake, and data warehouse.

Analytics

Machine learning, statistical models, threat signatures, and rules to detect anomalies.

Components of UEBA

Data analytics

Collects and analyzes data to create behavioral baselines.

Data integration

Integrates data from various sources with existing security systems.

Data presentation

Visualizations, charts, and reports to help analysts interpret findings.

How UEBA works

Robust principal component analysis (RPCA)

Collects and analyzes data to create behavioral baselines.

Markov chains

Detects pattern anomalies by analyzing the probability of events occurring in sequence.

Anomaly detection techniques

Supervised ML

System learns from a set of predefined behaviors (good/bad).

Unsupervised ML

System independently learns normal behavior and detects deviations.

UEBA in convergence with SIEM

Integration

UEBA is integrated into SIEM solutions for enhanced threat detection.

Benefits

Proactive defense mechanism against insider threats and cyberattacks.

UEBA use cases

Insider threats

Unusual system access, file modifications, excessive login failures.

Account compromise

Multiple software installations, failed logins, unauthorized logons.

Data exfiltration

Unusual file downloads, excessive data transfers.

Logon anomalies

Multiple login failures, logins from unusual locations.

Benefits of UEBA

Better threat detection

Identifies zero-day exploits and reduces false positives.

Holistic security view

Tracks long-term malicious lateral movements.

Improved incident response

Risk scoring helps focus on the most credible threats.

UEBA in different industries

Healthcare

Detects ransomware, safeguards patient data, ensures compliance.

Banking, financial services, insurance

Detects financial crimes, monitors insider threats, ensures regulatory compliance.

Education

Protects student records, monitors campus systems for cyberthreats.

Key features to look for in UEBA solutions

Real-time alerts

Get notified instantly when anomalies are detected.

Customizable anomaly models

Tailor detection models to your organization's needs.

Accurate risk scoring

Assign risk scores to users based on the severity of anomalies.

Peer grouping analysis

Compare users' behaviors to similar peers for enhanced detection.

Key takeaways

- ✓ Proactive threat detection through machine learning and behavioral analytics.
- ✓ Reduced false positives for a more focused security response.
- ✓ Better risk assessment through custom anomaly models and risk scoring.

ManageEngine
Log360

Thank you

manageengine.com/log-management