Shield 24x7 UEBA Capabilities

AI-ML Powered User and Entity Behavior Analytics

UEBA Solutions in 2024

UEBA (user and entity behavior analytics) first used by Gartner Research in 2015 to describe the cybersecurity process of monitoring activity of devices, applications, servers and data with user activity. With the age of big data, cloud computing and high-speed networking, many legacy SIEM vendors and startups built solutions that enabled better threat detection and response. UEBA is an improvement over UBA and legacy SIEM systems because it overcomes the limitations of SIEM correlation rules. These rules can be problematic because they lack context, miss incidents that have never been seen before, and require too much maintenance. Improperly filtered rules can also slow down incident response execution. UEBA reduces false positives and alert fatigue, enabling AI/ML capabilities to detect potential threats and rank them on a risk scale to either alert analysts or automate a response.

How does Shield 24x7's UEBA capabilities work?

Shield 24x7 User Entity Behavior Analytics (UEBA) is one of the detection engines in our comprehensive AI/ML powered cybersecurity platform: aiSIEM and aiXDR. Here's how it works:

1.**Holistic Approach:** Shield 24x7 aiSIEM & aiXDR takes a holistic approach to cybersecurity gathering deep insights from networks, endpoints, servers, devices, applications, IoT, and OT. It combines user identity, threat intelligence feeds, and vulnerability assessment to establish threat profiles, generate threat indicators, alerts and, manual or automated responses via playbooks.

2.**Behavior Baselining:** It applies machine learning for users and entities based on host-centric insights (services, processes, file access, telemetry, etc.) and network flows.

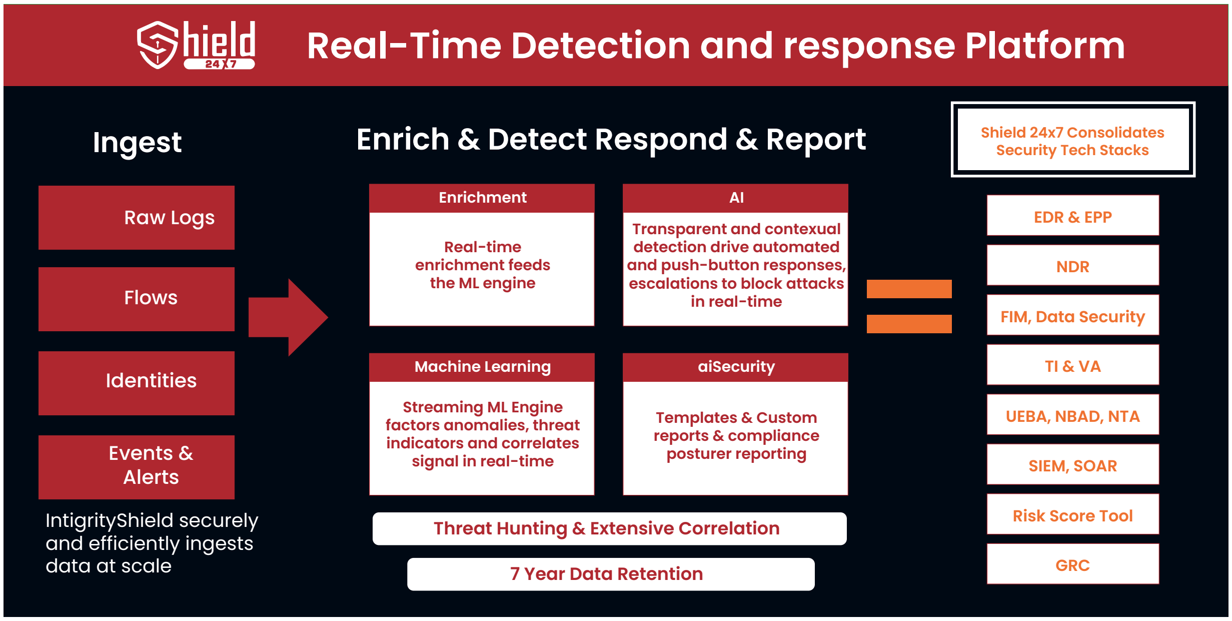
3.**Threat Detection with ML & AI:** Shield 24x7 uses automation through machine learning for anomaly detection, and artificial intelligence for Dynamic Threat Modeling (DTM) as accurate decisions are made around threat indicators and risks are mitigated before they turn into incidents.

4.**Insider Threat Detection:** Insider threat detection uses the UEBA capabilities & machine learning algorithms to identify various tactics & techniques used by the perpetrators. For example, a compromised credential is a clear indicator of an insider trying to gain access to information that they could potentially misuse.

5.**Alert:** Shield 24x7 can alert analysts and technicians multiple ways and provides the correlation & situational awareness of the where, when, how of the threat timeline.

6.**Respond:** Shield 24x7's platform has comprehensive response capabilities including manual & automated blocking, stopping and quarantine of attacks and breaches, and a drag-and-drop playbook designer.

In essence, Shield 24x7's UEBA is a key component of its aiSIEM & aiXDR platform, providing a comprehensive solution for threat detection and response.



Real-Time Detection and response Platform

Ingest

Raw Logs

Flows

Identities

Events & Alerts

IntigrityShield securely and efficiently ingests data at scale

Enrich & Detect Respond & Report

Enrichment

Real-time enrichment feeds the ML engine

AI

Transparent and contexual detection drive automated and push-button responses, escalations to block attacks in real-time

Machine Learning

Streaming ML Engine factors anomalies, threat indicators and correlates signal in real-time

aiSecurity

Templates & Custom reports & compliance posturer reporting

Threat Hunting & Extensive Correlation

7 Year Data Retention

Shield 24x7 Consolidates Security Tech Stacks

EDR & EPP

NDR

FIM, Data Security

TI & VA

UEBA, NBAD, NTA

SIEM, SOAR

Risk Score Tool

GRC

Shield 24x7 UEBA use cases:

Shield 24x7's User and Entity Behavior Analytics (UEBA) can be applied in various use cases:

1. **Malware Detection:** Shield 24x7's UEBA can detect malware tactics & techniques that have evolved to avoid detection by software tools & security controls. It relies primarily on machine learning & behavioral patterns across users & entities while questioning suspicious processes, file changes, connections, scans, etc.

2. **Zero-Day Threats & Ransomware Detection:** Shield 24x7's UEBA can catch zero-day threats, ransomware, & other malware variants with a high degree of confidence.

3. **Brute Force Attack Detection:** In a brute force attack, the adversary tries to guess the username-password combination repeatedly to gain access. Shield 24x7's UEBA can detect such attempts.

4. **Insider Threat Detection:** Shield 24x7 addresses insider threat detection through User Entity Behavior Analytics (UEBA) riding on machine learning algorithms to identify various tactics and techniques used by the perpetrators.

5. **Data Exfiltration (Breach) Detection:** Shield 24x7's UEBA can detect data breaches by analyzing network traffic patterns.

6. **MITRE ATT&CK Modeling:** Shield 24x7 leverages MITRE ATT&CK Tactics, Techniques, and Procedures to model actual intrusions and attacks.

7. **Policy Enforcement:** Shield 24x7's UEBA can activate instant response to governance policy violations through user-defined controls and initiate automated remediation to threats with high severity and confidence level, targeted at business-critical assets.

Benefits of Shield 24x7 UEBA in threat protection:

Shield 24x7's User & Entity Behavior Analytics (UEBA) is crucial for threat protection today due to the following reasons:

1. **Proactive Approach:** UEBA strengthens security by monitoring users and other entities, detecting anomalies in behavior patterns that could be indicative of a threat. It's a proactive approach to security and gains more visibility into user and entity behavior.
2. **Improved Detection:** UEBA represents an important improvement over traditional SIEM and standalone UEBA solutions for a number of reasons. It overcomes the limitations of traditional correlation rules and leverages both user behavior and entity behavior-based analytics, and models threats based on individual user behaviors.
3. **Reduced False Positives:** UEBA also reduces false positives, helping to eliminate alert fatigue. And by enabling teams to prioritize their alerts, UEBA makes it possible for your security experts to focus on the most credible, high-risk alerts.
4. Protection Against Insider Threats: UEBA can help weed out compromised accounts before a hacker can do any harm. It also detects when power users were created and monitors if they still have unnecessary permissions.
5. **Efficient Use of Resources:** UEBA can also help organizations save money by reducing the need for manual investigations of suspicious activity.

About Shield 24x7

Shield 24x7 reduces cyber threat risks and security stack complexity while significantly improving the ability to detect and block threats and breaches at scale. Shield 24x7's Open Threat Management (OTM) platform enhances and automates security with our AI and ML-powered aiSIEM and aiXDR solutions. The platform provides comprehensive coverage by collecting telemetry from logs, identity management systems, networks, endpoints, clouds, and applications. This data is enriched and analyzed in real-time using threat intelligence, AI and ML models based on behavioral analysis, and correlation engines to generate reliable and transparent detections and alerts. IntegrityShield supports over 8,000 clients by delivering high-margin, efficient security services with automated cyber threat remediation and continuous compliance.

Learn more about Shield 24x7 UEBA

Schedule a Demo