

Automated UEBA

(User and Entity
Behaviour Analytics)

Detect malicious user activity early
in your on-premise or cloud infrastructure



Detect internal cyber threats that would be missed by anti-malware and firewalls.

With today's sophisticated hackers, a cyber breach has become a matter of when, not if. Hackers can get inside your IT infrastructure despite the best defenses. Most organisations do not know if they are breached, until months later when it is too late.

It becomes essential to monitor for malicious user activity inside the infrastructure, so that you can know as early as possible when a hacker had gotten in. Early detection allows you to take action early, to avoid the data loss and public relations disaster.

With its machine learning and advanced user behavior analytics, Automated UEBA provides early detection of hijacked accounts, insider threats, compromised servers and more.



Benefits



Stop Internal Threats

Discover insider threats and hijacked accounts that would be missed by anti-malware and firewalls



Automated

Detect automatically and save on manpower



Advanced Sensors

Provides visibility needed to catch APTs



Proven Solution

Deployed by large enterprises and government

Who are using it today?

Singapore Government

Leading Technology Companies

Listed Real Estate Investment Firms

Listed Large Logistics Firms

Insurance Companies

Healthcare Institutions

How is Automated UEBA different?

1 Advanced Cybersecurity Algorithms

Unlike other UEBA, which are still heavily reliant on rules, Automated UEBA works out-of-the-box with hundreds of smart cybersecurity algorithms. For example, Automated UEBA provides early detection of sophisticated supply-chain attacks such as the SolarWinds attackers (even before the attack is publicly known).

2 Manpower Saving

Built to automate threat detection. Unlike other UEBA, there is no need for a large cyber team to operate the solution 24/7. It frees up the team to focus on response and other higher value work. Our approach saves manpower, and more importantly, results in faster and earlier detection.

3 Advanced Cyber Sensors

Deploys advanced cyber sensors on servers, to get the high visibility needed to catch today's Advanced Persistent Attackers (APTs).

4 IMDA Accredited and Award-winning

The only solution accredited by the Singapore Government for UEBA.

Address key cyber risks inside your infrastructure

1

Hacker

Hijacked user accounts or machines

2

Insider Threat

Disgruntled employees who steal data

3

Compromised Servers

Hackers installed backdoors in servers (including supply-chain attacks like SolarWinds)



Figure 1: Detect the high risk accounts and servers automatically



Figure 2: Get visibility into your infrastructure's network and user activities

Success Cases in Customers



Compromised Privileged Account

Automated UEBA reported a suspicious privileged account. There were behavior anomalies in the account's activities, and the account is behaving similar to what an attacker would do. Early detection enabled the customer to investigate early and prevent any serious damage.



Data Theft by Insider Threat

Automated UEBA reported a suspicious data transfer between a file repository and an employee's machine. This is due to behavior anomalies in the file access, and unusual network traffic. The customer is able to investigate the employee before there is a large data loss.



Backdoor Traffic

Automated UEBA discovered suspicious network activity, which turned out to be a backdoor installed in a customer server. Instead of relying on IP blacklists that are easily outdated, Automated UEBA looks for suspicious patterns in the network traffic. The customer is able to contain the breach early and prevent any serious damage.

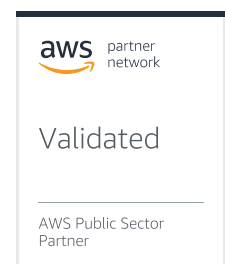
About InsiderSecurity

InsiderSecurity is an award-winning, Singaporean cybersecurity technology company. Its innovative cybersecurity products are used by government and large enterprises.

Awards and Featured in Media



Technology Partner



+65 6270 4029

hello@insidersecurity.co

<https://insidersecurity.co>

81 Ayer Rajah Crescent, #03-48,
Singapore 139967

