Predict | Protect | Prevent

User Behaviour Analytics

www.arconnet.com

Overview

Corporate insiders are now one of the most dominant threats to enterprises. Detection of the malicious activities they indulge upon is another challenge which these enterprise face frequently off late. It is mostly impossible to monitor thousands of end-users in a typical IT set-up. The root cause remains undetected.

There are few organizations who largely depend on firewalls, SIEM (Security Information and Event Management), DLP (Data Loss Prevention), and IDS (intrusion detection systems) to prevent security breaches. However, all these tools help in providing isolated alerts. However, most data breach or threat to systems stem from unmonitored end-user activities. The risk and security management often fails to determine the threat arising from an end-user activities and eventually 'reward' the malicious actors with necessary security gaps.

The science of user behaviour analytics has been with us since many years. It automatically scrutinizes the suspicious activities, provides details about each end-user. This enables the analysts to delve deep into such type of activities and overcome security vulnerabilities at the onset. With the help of UBA, IT security team can get to know about suspicious end-user activities, threats and vulnerabilities in real time. Hence, it enables them to mitigate security risks across the entire network infrastructure.

UBA can even gather data from various sources and analyze the action to detect anomalous events that normally points towards:

- System compromise
- Account compromise
- Data leak
- Insider threats

Information Security and Access Control are the two most essential components for a robust IT ecosystem. However, enterprises are dynamic and ever-evolving which has led to complexities. The general approach is to restrict as much as possible. They say, “Close as many doors as possible,” which has led to a restrictive practice and all the investments made in automation, technology and internet etc. to create efficiencies are now challenged. We believe ARCON | UBA will transform the way Information Security is approached in the next decade. It will essentially be “do what you want” but we will assess and monitor you as and when required. ARCON is a pioneer in self learning user behavioural analytics. Our UBA is a comprehensive tool that is capable to crunch huge amount of data, spot suspicious end-user behavioural profiles and trigger alerts.

Key Features

Behaviour Analytics

The tool enables to design an enterprise security framework. Machines are configured as per the policy and applied to all end-users. The centralized framework thus helps organizations to identify user behaviour by comparing against the configured baseline activities.

Data Loss Prevention

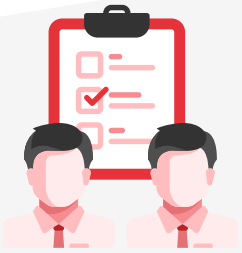
User Behaviour Analytics provides a continuous monitoring framework to mitigate insider threats and suspicious activities across the enterprise. The tool built upon technical and non-technical analytic methodologies automates the entire risk- assessment process by acting as a floodgate to block unusual and suspected activities.

Session Monitoring

Enables recording of all activities performed by an end-user on the desktop along with a screen capture through a web-based engine that stores and analyzes user behaviour profiles.

Productivity Enhancements

Centralized monitoring framework facilitates standard machine configuration policy that allows enterprise to guard against any anomalies in end –user behaviour profiles. This enables to boost overall productivity as it helps to generate performance reviews on non-technical observables such as security violations and fraudulent events caused by disgruntled end-user.



Meeting Compliance

ARCON User Behaviour Analytics empowers enterprise to meet various compliance requirements by offering real-time threat alerts such as misuse of trusted privileges or other Admin accounts whilst offering granular access control mechanism. A host of regulatory requirements PCI-S, SOX, NIST, GDPR are fulfilled.

Dynamic Report

The tool's programmatic approach to strengthen security and compliance framework through dynamic report allows management to keep a real-time track on technical observables such as unusual working hours, misuse of Privilege Access, anomalous network service usage, printing activity and so forth.

Live Dashboard

Investigating abnormal incidents and timely response to threats simplified as the all-encompassing reporting mechanism raises immediate alerts on Live Dashboards. This feature is beneficial to keep control over operations, governance and compliance requirements.

Privilege Elevation

Mitigates data breach risk by discarding large number of ADMIN (privileged) users. The tool offers flexibility to enterprises with on-demand and on-request admin rights that allows end-users to access certified applications only after a valid approval process.

Benefits

1. **Governance**
Helps IT security personnel to align IT security policies with operations ensuring compliance.

2. **Performance Matrix**
enables management to evaluate major reasons behind the gap between deliverables and the actual end-user output.

3. **Security**
offers an additional layer of risk and fraud detection layer thereby ensuring security framework is uncompromised.

4. **Change Management**
measures the effectiveness of end-user output as a result of any transformation from existing IT setup.

5. **Cyber Risks Analytics**
monitors security logs and network flows to identify malware infections.

6. **Identity an access control**
analyzes and monitors privileged user activities and blocks access to suspicious activities.

7. **Mitigate fraud risk**
isolates anomalies in real-time thereby stopping activities that could be fraudulent

Conclusion

Detection of malicious insiders remain the biggest challenge for organizations who:

- Fails to align IT security policies with IT operations
- Unable to evaluate the gap between deliverables and end-user output
- Not able to measure the effectiveness of end-user output
- Unable to detect and block suspicious activities
- Not able to isolate anomalies in real-time

ARCON | UBA is definitely the best remedy to get rid of current security threats and even combat the unprecedented ones related to privileged accounts. By analyzing user behaviour, ARCON | UBA notifies the administrators immediately if any deviation occurs. ARCON's people centric approach provides a different edge to the security level. It also accommodates the Information Security staff with the mechanism which allows identification of the end-user behaviour. Today, risk prediction is highly important for organizations under any circumstances. Thus, they need to seriously consider deploying ARCON | User Behaviour Analytics tool, which monitors, and assesses all end-user behaviour profiles and generates real-time alerts if there is any deviation from base-line activities.