How tbSIEM & tbIAM intersects the modern Cyber Security?

www.tech-bridge.biz

How tbSIEM and tbIAM intersects the modern Cyber Security?

Reference: tbSIEM & tbIAM

In today cybersecurity world what company/organization do to protect their employees' identities and databases during a still turbulent time? Why should company embed both identity management and SIEM in their security solution?

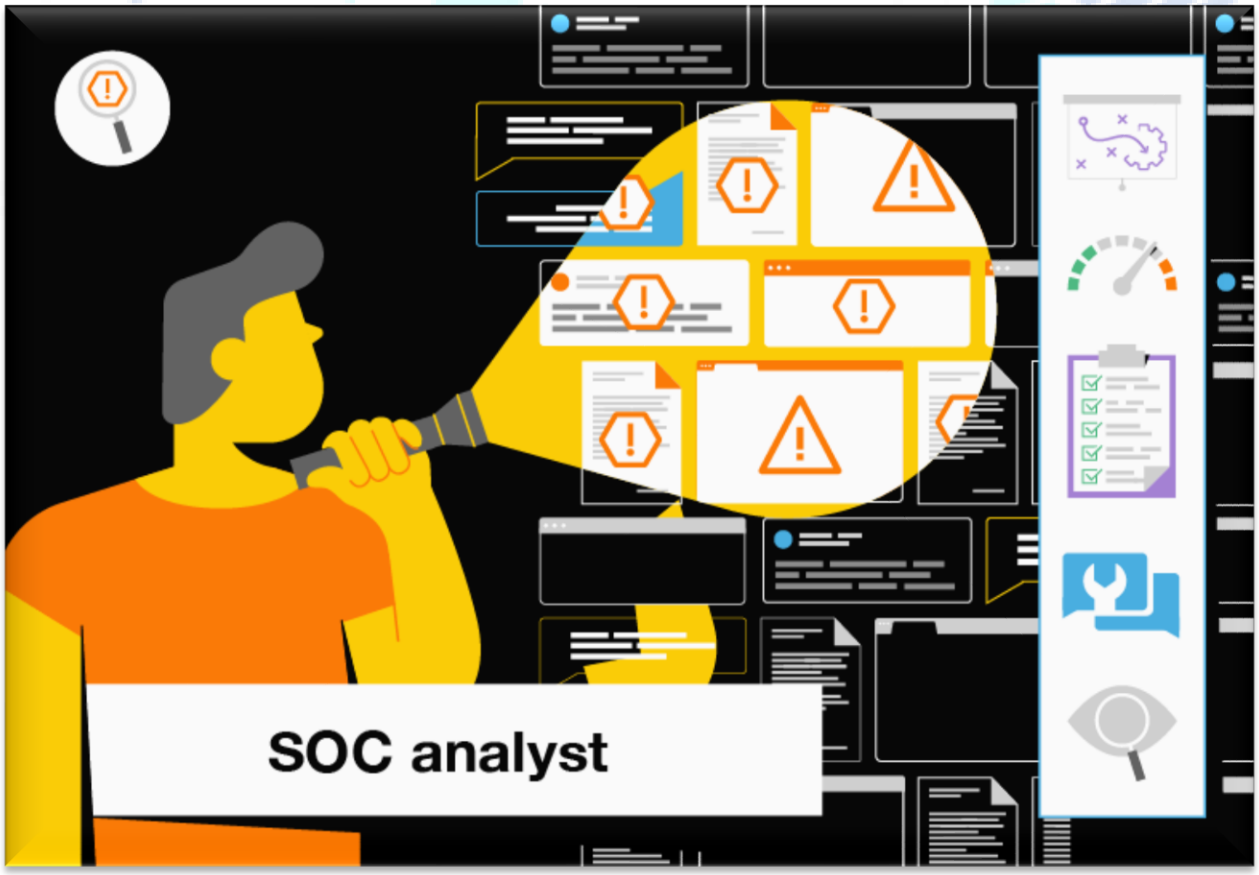
Now a days, organizations are integrating them bi-directionally. For security analysts, this brings better context to their events of interest. In their world, context is everything for effective triage.

How the tbIAM and tbSIEM utilize together and enhance the overall Cyber Security?

Remote Workforce Management	•Due to n number of problems, sudden need to shift to remote work. tbIAM provides multifactor authentication, an essential tool for ensuring employee identities remain safe; the more factors between requester and database, the more secure the account. However, tbSIEM provides user and entity behavior analysis (UEBA), which can help detect if a hacker has compromised an account.
Zero Trust Architecture	•According to Forrester Research, a ZT architecture "abolishes the idea of a trusted network inside a defined corporate perimeter. ZT mandates that enterprises create micro-perimeters of control around their sensitive data assets to gain visibility into how they use data across their ecosystem to win, serve, and retain customers."
Secure most Sensitive data	•Through identity management, enterprises can benefit from step-up authentication. This combines the strengths of both multifactor authentication and continuous authentication while cutting some of the perceived downsides.

Example: In an event of a newly created account, this might be a local operating system account, an app account, a software-as-a-service account or a domain account. If the SIEM system registers the event of a created account in a connected system, it won't be clear if this is a desired or malicious event.

But if your SIEM system is able to correlate this 'account add' with a related action from the IAM system, it's easy to distinguish between an approved or malicious account creation. Remember, new account creation is often part of the 'persistence' attack phase. Therefore, this enhances your SIEM capabilities.



FOR MORE INFORMATION

About TechBridge

TechBridge is the World's leading Product & Solutions Company. Data Center Applications, Collaboration and Real Time Communication. DC Management and Monitoring, Disaster Management, Security, Collaboration and Cloud. Its market-leading Network Modernization, Unified Communications, Mobility and Embedded Communications solutions enable customers to quickly capitalize on growing market segments and introduce differentiating products, applications and services. We are an expert and leader in Government Solutions, Smart City Solutions, Data Centers and Large Enterprises. We do custom applications also, as per the customer requirements.

Certificates: -

ISO 9001

ISO 27001

ISO 20000

CMMi L3

ISO 15408-1

PinkVERIFY

Mail us at: sales@tech-bridge.biz

Address: - TechBridge Consultancy Services LLP
326, Tower B3, Spaze iTech Park, Sector-49, Sohna Road, Gurgaon-122018, Haryana