BROCHURE

tbSIEM: Security, Information and Event Management

INTRODUCTION

Discover, Prioritize, and Prevent Real Threats in Real Time

tbSIEM is a cybersecurity analytics tool that has built-in threat intelligence and anomaly detection capabilities that analyses data streams from various endpoints in real time to discover non-compliant system activities, aberrant behavior's, security issues, and cyber threats. built for precise detection.

Features

- Advanced Real-Time Collection
- Threat Detection and Prevention
- Detection of anomalous situations:
  Within Networks
  Operating Systems
  Application layers
- Rapid Incident Response and Resolution

This technology provides an excellent foundation for a security operations centre (SOC). It operates quickly and independently, links to all systems and security measures, and performs as needed by stakeholders and employees. For large environments, tbSIEM is renowned for its wide-scale scalability and compliance monitoring capabilities.

Next Gen SIEM security solution offers the most value and also lower implementation and operation costs. This solution offers advanced functionalities as per revised Gartner SIEM model:

- UEBA – advanced analytics to determine behavioral anomalies and alert prioritisation (Alert Triage)
- SOAR – automation and orchestration of incident response
- Threat hunting interface – Empowering analysts to actively seek out threats using a point-and-click threat hunting interface
- Dashboards and visualizations
- Flexible searching, querying, and data exploration

TechBridge
Making the World Smarter

tbSIEM – How it works?

1. SECURITY MONITORING &COMPLIANCE

tbSIEM is the foundation of the highly recognised Security Platform. This comprehensive security and compliance solution offers:

- Integrated incident management capabilities for incident investigation, escalation, and resolution
- Role-based access controls, audit trails, and high levels of automation to streamline security operations
- Detection of unknown and unknowable threats
- Highly flexible architecture and support for high volume data throughput rates
- Comprehensive data display, dashboard, and investigation capabilities
- In-depth data gathering, threat detection, alert analysis, incident response, and reporting lifecycles are all supported
- It has an entirely integrated incident management module that highlights events to make sure that alarms can be recorded, examined using a set methodology, escalated, and quickly handled

2. FLEXIBLE DATA COLLECTION

To collect any data from any source, arrange it, and parse it through the analytics engines, tbSIEM offers a flexible, completely customizable interface
(Agent & Agentless)

- A fast, real-time, stream-based processing, correlation, and alerting engine that enables the quick detection of policy violations, security, loss, or fraud threats, and non- compliant activities.
- Complete flexibility in terms of collection, providing agent-based and agentless options for syslog, event logs, file-based, XML, database query, network traffic data, etc.
- The capacity to support third-party cloud-based services at the IaaS, PaaS, or SaaS layers, allowing total security visibility over on- and off- premise systems.
- A collection of original and normalized log files for forensic and evidentiary use.
- Supports unlimited off-line storage for archives, compliance, or historical analysis, scalable data model; many live/accessible repositories.

3. ADVANCED ANALYSIS

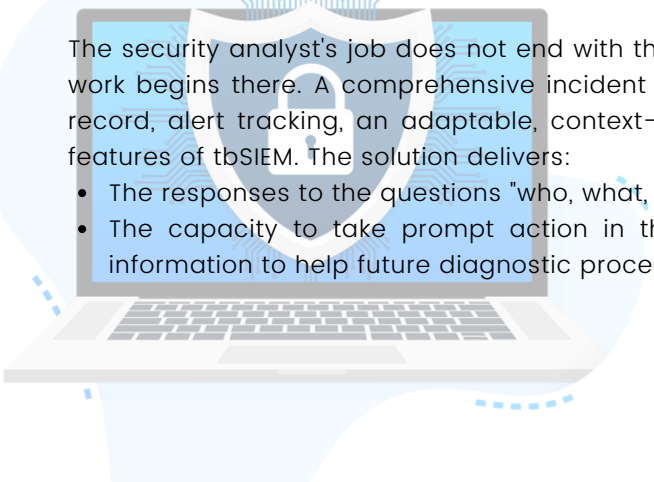
The analytical engine of tbSIEM performs real-time analysis using policy-based deterministic algorithms and correlation to identify problems that require the operators' immediate attention.

- Using machine learning to give behaviorally based profile and detection, real-time anomaly detection of behavior's
- Monitoring by security operators of several concurrent alarms from various sources
- Monitoring the integrity of files and directories to protect sensitive company data
- Risk and asset classification to identify threats, potential consequences on the firm, and significant business issues
- Sets information and alarms in order of priority manual or automated corrective action

4. EFFECTIVE RESPONSE

The security analyst's job does not end with the detection of potential cyber-security problems; rather, the hard work begins there. A comprehensive incident management solution that preserves case data in a single case record, alert tracking, an adaptable, context-based query interface, and automated workflow support are all features of tbSIEM. The solution delivers:

- The responses to the questions "who, what, where, when, and how" right after an occurrence.
- The capacity to take prompt action in the wake of an alarm to neutralize threats or collect any extra information to help future diagnostic procedures..



TechBridge
Making the World Smarter

- Comprehensive alert monitoring and issue management solution with workflow support, escalation, case data management, and closure reporting.
- Integration with third-party solutions for threat reduction, SNMP / network management, ticketing, and API access.

5.STATE-OF-THE-ART VISIBILITY & BUSINESS INTELLIGENCE

A key component of the product is access to data that (i) gives security analysts in-depth technical views to aid in incident resolution; and (ii) shows a one-page compliance summary and risk views for senior stakeholders, allowing for a quick understanding of the cyber-security and compliance posture of your business.

- Constant real-time risk and security dashboards for monitoring compliance status "as events happen."
- Business intelligence drill-down query interface with tabbed data views, interactive filtering, and ad hoc or saved context-based queries.
- A dynamic real-time view of all system activity, network connections, and user interactions.
- Scheduled and ad hoc reports that are pre- made or customized, with automatic storage and distribution to management and technical stakeholders.
- Vast library of pre-defined reports organized by source type, event type, and compliance criteria.
- A complete audit trail with trusted replay for all activity, a fully role-based and granular access control approach.

PRODUCT FEATURES

DATA COLLECTION & ANALYSIS

- Threat Intelligence
- Real-time Collection
- Unlimited/free Agents
- Continuous Monitoring
- Network flow monitoring
- Correlation and Alerting
- Original log file collection
- File/Directory integrity monitoring
- Behavioral Anomaly Detection/Machine Learning Engine
- References tables of platforms, hosts, users for analysis

REPORTING & VISIBILITY

- GRC Dashboards
- Query/Display Interface
- Operational Dashboards
- OOTB Compliance Packs
- Ad-hoc and Scheduled Reports
- Web-based “Business Intelligence” interface

WORKFLOW & AUTOMATION

- Incident Manager
- Alert Tracking and Workflow Support
- Scripted/Defined Response (Automatic or Manual)

MANAGEMENT

- Full Audit trial
- Asset manager Tool
- High Availability/Clustering
- Multiple on-line data repositories
- Role based and granular access control
- Automatic data backup, Aging and archive

SUPPORT

- Onsite
- Phone/Email

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:-

Contact Us:
Mail Id: marketing@tech-bridge.biz
LinkedIn: https://www.linkedin.com/company/techbridge_2/
Website: https://tech-bridge.biz

TechBridge
Making the World Smarter