PRODUCT DATASHEET

tbSIEM: Security Information & Event Management

INTRODUCTION

Our **Next-generation tbSIEM** refers to a more advanced and sophisticated approach to security management that goes beyond the capabilities of traditional SIEM systems.

KEY FEATURES

- **Real-time Monitoring and Analysis:** Our Next-gen tbSIEM focus on providing real-time analysis of security events and incidents. They leverage high-speed data processing and machine learning algorithms to detect and respond to threats as they happen, reducing the time gap between detection and response.
- **Advanced Analytics and Machine Learning:** tbSIEM go beyond simple rule-based correlations. They employ advanced analytics and machine learning techniques to detect anomalous behaviour, identify unknown threats, and improve overall threat detection accuracy.
- **User and Entity Behaviour Analytics (UEBA):** Our Next-gen tbSIEM analyse user and entity behaviour to establish a baseline of normal activities. When deviations from this baseline occur, the system can alert security teams to potential insider threats or compromised accounts.
- **Scalability and Flexibility:** tbSIEM are designed to scale efficiently to handle the massive volumes of data generated by modern enterprises. They provide flexible deployment options to accommodate varying organizational needs and resources.
- **Integrated SOAR (Security Orchestration, Automation, and Response):** Our tbSIEM solutions often integrate with SOAR platforms to automate incident response actions, streamline workflows, and reduce the manual effort required to handle security incidents.

Highlights:

- Logging Framework
- Supports HA
- Customized reporting option
- Security information management
- Security event management
- Asset management and discovery
- Log management
- Vulnerability assessment
- Intelligent Threat detection
- Behavioral monitoring
- Reporting
- Powerful and user-friendly web interface
- Quick prioritization of security event by using correlation
- Regular expression based search engine
- File Integrity Monitoring
- System configuration Assessment
- Agentless Monitoring

The Benefits

🛡️ Incident Response
🔍 Threat Detection & Prevention
🔒 Integrity Monitoring
✅ Compliance Verification
🔍 Proactive Vulnerability Identification
💡 Actionable Intelligence

TechBridge
Making the World Smarter

- **Threat Intelligence Integration:** Our tbSIEM incorporate threat intelligence feeds from various sources to enrich their analysis and provide context to security events.
- **Improved User Experience:** Next-gen SIEMs often focus on providing a more intuitive and user-friendly interface, making it easier for security analysts to interact with and derive insights from the data.

PRODUCT OVERVIEW

- tbSIEM is a powerful platform designed to monitor networks and safeguard both small and large enterprises from security threats. With cutting-edge capabilities like incident response, threat detection, integrity monitoring, and compliance verification, we proactively protect your network
- tbSIEM identifies vulnerabilities and expiring SSL certificates in advance. Our solution empowers you with context, intelligence, and situational awareness, ensuring you have full control over your network's security
- tbSIEM Enterprise Security Monitoring takes things to the next level, offering endpoint visibility and harnessing your organization's capabilities for fortified defence. While our platform provides contextual visibility for alerts and anomalous events, it thrives with the active involvement of our expert security analysts
- Other tasks such as incident response and network forensics are performed proactively by the solution. After an incident is detected. It provides the network with context, intelligence, and situational awareness. Enterprise Security Monitoring takes tbSIEM to the next level with endpoint visibility and other organizational capabilities
- Although tbSIEM provides network traffic and contextual visibility for alerts and anomalous events, it requires the active involvement of security analysts to see alerts and monitor network activity
- It combines best-in-class detection methods with information from behavioral analysis and third-party vulnerability database to provide the industry's most intelligent security management solution. tbSIEM provides actionable intelligence to effectively manage the security regimes of organizations of all sizes

BENEFITS

- Use advanced monitoring and forensic analysis to provide situational awareness of both external and internal threats
- integration with diverse third-party security and networking products ensures unparalleled visibility and protection
- Tailored for large enterprises, our solution offers modular components and hassle-free high availability features to meet deployment requirements
- Go beyond conventional security solutions: our offering encompasses threat management, log management, compliance reporting, and operational enhancements
- Unify network activity, security events, logs, vulnerability data, and threat intelligence into a robust dashboard for intelligent correlation, prioritization, and swift response, enhancing IT staff efficiency
- Establish a baseline of normal network behavior through analysis and aggregation of flows from diverse network and security apps, promptly detecting deviations and flagging potential vulnerabilities for swift correlation and remediation
- Track extensive logs and trends, generating diverse cybersecurity reports for network optimization and regulatory compliance

All tbSIEM solutions offer robust high availability (HA) features, guaranteeing uninterrupted access to SIEM data during hardware or network failures. HA ensures automatic failover and seamless data replication between primary and secondary hosts. The secondary host mirrors primary host data or accesses shared external storage, periodically sending heartbeat signals to identify issues. Upon detection, the secondary host seamlessly takes over all primary host functions for uninterrupted operations

COMPONENTS

- tbSIEM Agent
- tbSIEM Server
- tbSIEM Log Collector
- tbSIEM GUI

USE CASE

- Log Data Analysis: Logs can be the evidence of an attack, log management and analysis speed up threat detection. tbSIEM agent used to automatically aggregate and analyze log data.
- File Integrity Monitoring: In FIM, the system monitors selected directories and files in a directory and triggers an alert when a file is added, deleted, or modified in that particular directory. The component responsible for this task is called sys check
- Rootkit Check: tbSIEM performs enhancement and configuration policy scans to detect applications that are known to be vulnerable, unpatched, or misconfigured.
- Vulnerability Detection: tbSIEM can use the Vulnerability Detector Module to detect vulnerabilities in applications installed on agents. This software audit is performed by integrating the vulnerability feed
- Active Response: The action taken when a threat is detected on a monitored node to protect the system is called an active response. In particular, the tbSIEM agent can block network connections, stop processes running, and delete malicious files.
- System Auditing: The endpoint has the tbSIEM agent installed and installs the service. Because of the large number of events generated and the difficulty of distinguishing and classifying events according to the tbSIEM server, check rules use key arguments to facilitate the handling of endpoint-generated events. Any changes that violate the defined validation rules will be warned in the same way.
- System Inventory: This module collects the most relevant information from monitored systems (hardware, operating system, packages, etc.) and transfers the collected data to the tbSIEM server.

SPECIFICATIONS

Deployment	**Log Management**	**System Logs**	**User Management**	**Export Reports**
Flexible Deployment	**Collecting Data**	**All user Profile**	**Multiple account types**	**Pdf**
HA Supported	**Syslog**	**All current user's login**	**Role based Access Control**	**Email**
DC-DR supported	**Centralized Logging**	**User & Administration activity**	**Use Groups**	**Generate Report based on desired filter**
	Normalized log into CEF format	**Users successful & Unsuccessful login**		
	Handles up to 20,000 – 100,000 EPS.			

SPECIFICATIONS

Analysis	**Asset Management**	**Dashboard**	**Event Management**	**Compliance**
Security Incident Management	**Asset Discovery**	**Event Dashboard**	**Event Normalization**	**HIPPA**
Security Event Management	**Adding & Deleting Assets**	**Alert Level Evaluation**	**Event Correlation**	**GDPR**
Raw Logs Management	**Vulnerability Scanning**	**Security Event Dashboard**	**Event Cross-Correlation**	**PCI-DSS**
Active Response	**Monitoring Asset**	**Top MITRE ATT&CKS**	**Security-related Event Management**	**NIST 800-53**
Anomaly & Malware Analysis	**Asset Configuration**	**Top 5 Agents**		**SOC 2**
Normalization & Correlation	**Asset Prioritization**	**FIM Dashboard**		
Log Analysis	**Physical & Logical Inventory**	**Vulnerability Dashboard**		
Security Threats Detection	**Assets Analysis**			
Forensic Analysis		**Compliance Dashboard**		

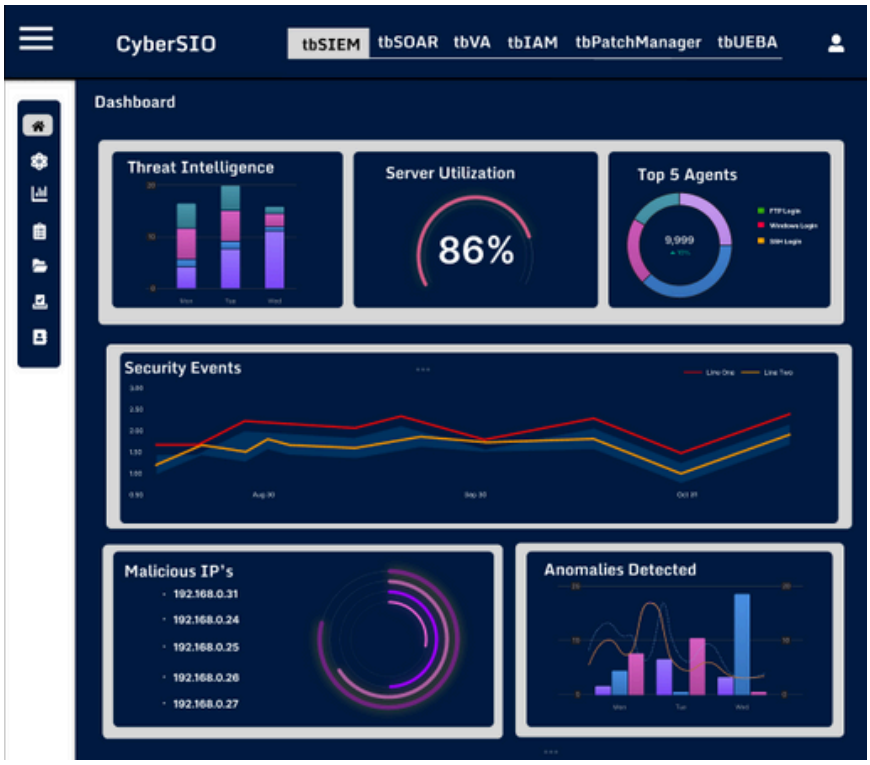
SYSTEM SPECIFICATIONS

- 12 vCPU or 12 core CPU
- 16 GB RAM
- 250 GB Hard Disk
- Ubuntu 20.04 LTS
- Storage – As per Data Retention period

SERVICE &SUPPORT

- TechBridge offers a comprehensive range of services, from professional services to customer network design, deployment, optimization, custom technical training, and personalized service and support.

TechBridge
Making the World Smarter



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