Security Information & Event Management

Compliance through Security Information and Event Management, Log Management, and Behavioral Analysis of Network. Unified event correlation and risk management for modern networks.

The solution that provides real-time analysis of security alerts generated by applications and network hardware.

That’s where **tbSIEM** comes in.

Product Overview

tbSIEM security information and event management system, integrating a selection of tools designed to aid network administrators in computer security, intrusion detection and prevention. It can be used to effectively secure small to very large heterogeneous networks.

tbSIEM is a platform that helps large and small businesses monitor their networks for security-related events. Features provided by the platform include incident response, threat detection, health monitoring, and compliance verification. Helps identify vulnerabilities in advance and scan for expired SSL certificates.

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 assessment tools 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.

Highlights

- Logging Framework is compatible with SIEM framework
- Self-Monitoring Capability
- Supports HA
- Customized reporting option
- Security information management
- Security event management
- Asset management and discovery
- Log management
- Network management
- IDS (intrusion detection)
- HID (host intrusion detection)
- Vulnerability assessment
- Intelligent Threat detection
- Behavioral monitoring
- Reporting
- Powerful and user-friendly web interface
- Quick prioritization of incident by using correlation

Benefits

- NOC and SOC staff can focus on actionable information without having to struggle to interpret the millions of daily events generated by network security appliances, switches, routers, servers, and other applications.
- Use advanced monitoring and forensic analysis to provide situational awareness of both external and internal threats Includes improper content, IM, file transfers, unwanted local traffic, data theft, and malicious worm infections.
- Reduce time to value through out-of-the-box capabilities, rapid deployment, and increased employee efficiency while leveraging your existing investment in network and security infrastructure.
- Integrates with TechBridge's Intrusion Prevention System (IPS), Network Access Control (NAC), and NMS solutions to provide a unified view of threat situations in real time for effective detection, isolation, and protection which eliminate threats automatically.
- Integrate with a variety of third-party security and networking products such as firewalls and routers for the highest levels of visibility and protection.
- Meet the deployment needs of large enterprises with modular component options and easy-to-deploy high availability features.
- Manage and monitor the entire device and manufacturer
- Provides threat management, log management, compliance reporting, and operational efficiency improvements beyond traditional security information and event managers, and network behavior analysis products.
- Collect and combine network activity data, security events, logs, vulnerability data, and external threat intelligence into a powerful management dashboard for intelligent correlation, normalization, and prioritization. This significantly improves repair and response times and greatly improves the efficiency of IT staff.
- Baseline normal network behavior by capturing, analyzing, and aggregating network flows from different network and security applications. It then detects network traffic patterns that deviate from this criterion and flags potential attacks or vulnerabilities. Abnormal behavior is captured and reported for correlation and repair.
- Track extensive logging and trend information, Generates a wide range of reports on network security The purpose of network optimization and regulatory compliance.

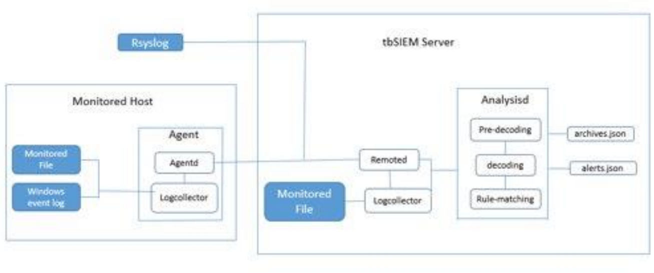
All tbSIEM appliances provide high availability (HA) capabilities This ensures that SIEM data is available in the event of a hardware or network failure. HA provides automatic failover and full disk replication between the primary and secondary hosts. The secondary host manages the same data as the primary host by replicating the data on the primary host or accessing the shared external storage. The secondary host periodically sends a heartbeat ping to the primary host to detect hardware or network errors. If the secondary host detects an error, the secondary host automatically takes over all responsibility for the primary host.

The tbSIEM HA feature is easy and inexpensive to deploy via appliances and wizards without the need for additional fault management solutions or storage options. The solution portfolio includes appliances that are quick and easy to set up.

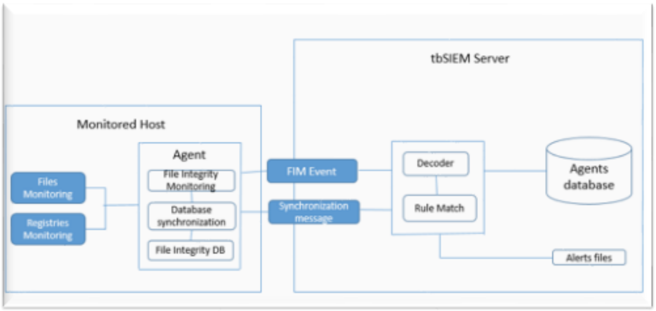
Components:-

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

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.

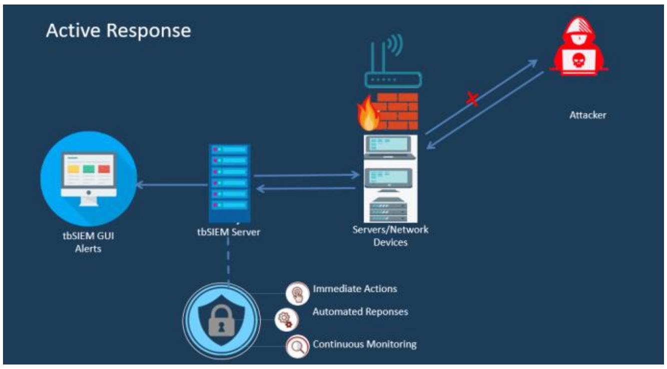


File Integrity Monitoring*:* In FIM, the system monitors selected directories and files in a directory and triggers an alert when a file is added, deleted, or modified in that particular directory. The component responsible for this task is called syscheck.

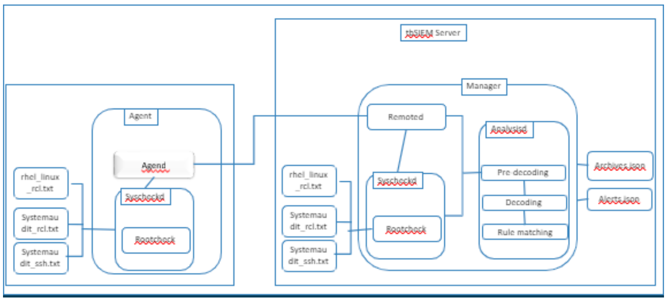


Rootkit Check*:* tbSIEM performs enhancement and configuration policy scans to detect applications that are known to be vulnerable, unpatched, or misconfigured.

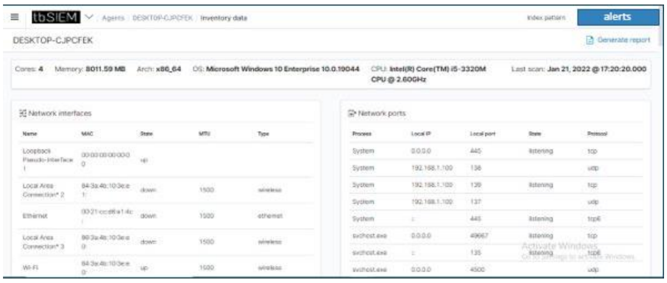
Active Response*:* The action taken when a threat is detected on a monitored node to protect the system is called an active response. In particular, the tbSIEM agent can block network connections, stop processes running, and delete malicious files.



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.



DESKTOP-CJPCFEK

Cores: **4** Memory: **8011.59 MB** Arch: **x86_64** OS: **Microsoft Windows 10 Enterprise 10.0.19044** CPU: **Intel(R) Core(TM) i5-3320M CPU @ 2.60GHz** Last scan: **Jan 21, 2022 @ 17:20:20.000**

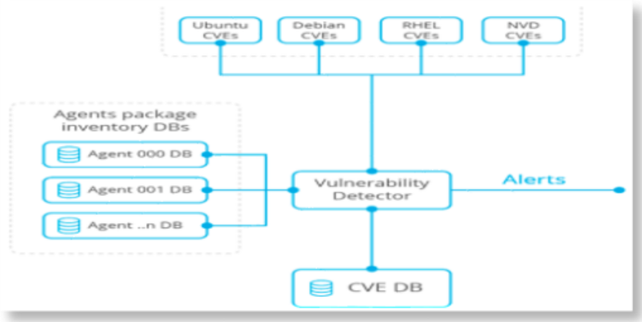
Network interfaces

Name	MAC	State	MTU	Type
Loopback Pseudo-Interface 1	00:00:00:00:00:00	up		
Local Area Connection* 2	84:3a:4b:10:3e:e1	down	1500	wireless
Ethernet	00:21:cc:d8:a1:4c	down	1500	ethernet
Local Area Connection* 3	86:3a:4b:10:3e:e0	down	1500	wireless
Wi-Fi	84:3a:4b:10:3e:e0	up	1500	wireless

Network ports

Process	Local IP	Local port	State	Protocol
System	0.0.0.0	445	listening	tcp
System	192.168.1.100	138		udp
System	192.168.1.100	139	listening	tcp
System	192.168.1.100	137		udp
System	::	445	listening	tcp6
svchost.exe	0.0.0.0	49667	listening	tcp
svchost.exe	::	135	listening	tcp6
svchost.exe	0.0.0.0	4500		udp

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.



Specifications:-

Analysis	Asset Management	Dashboard	Event Management	Compliance
Alarm Management	Asset Discovery	Event Dashboard	Event Normalization	Business Real Impact Risks
Security Event Management	Adding & Deleting Assets	Tickets Dashboard	Event Correlation	HIPAA
Raw Logs Management	Vulnerability Scanning	Security Event Dashboard	Event Cross Correlation	PCI-DSS 2.0
Tickets Management	Monitoring Asset	Network Activity Dashboard	Event management of Networks, application, user activities & system related events	PCI-DSS 3.0
Root Cause Analysis	Asset Configuration	Inventory Dashboard		Trends
Policy based Correlation	Asset Prioritization	Networks Flow Dashboard		GDPR
Fault Analysis	Physical & Logical Inventory	Vulnerability Dashboard		ISO:27001
Security Threats Detection	Assets Analysis			
Web application threats analysis				

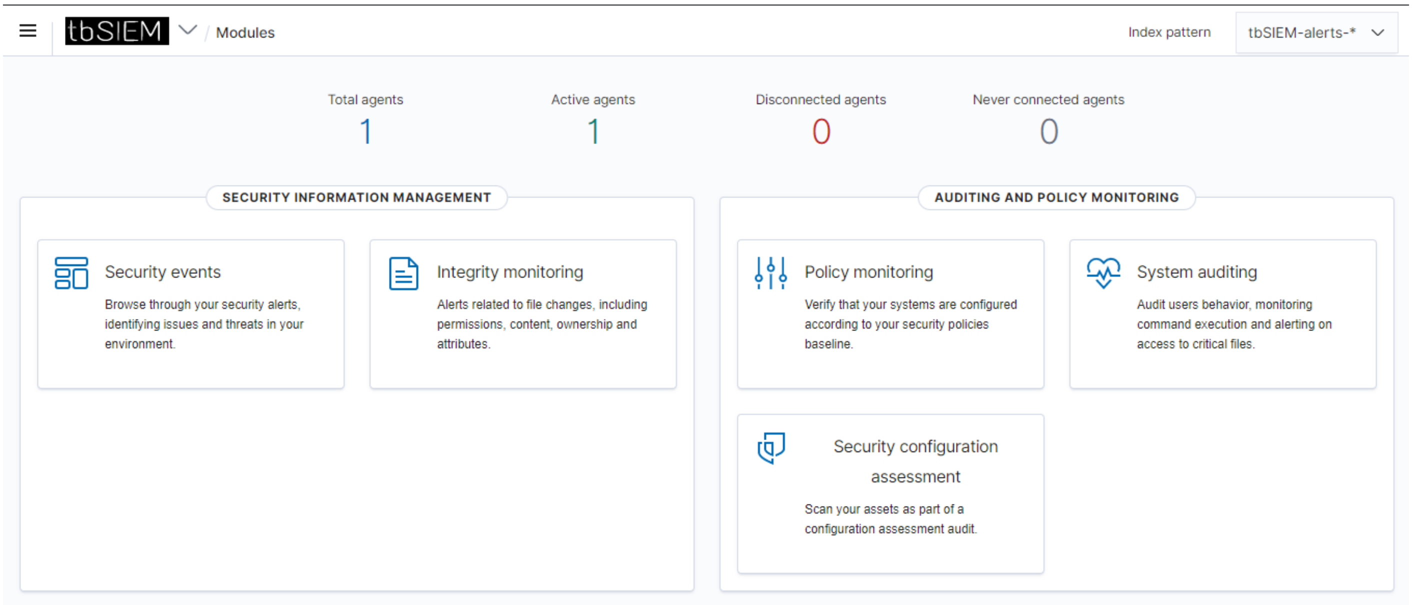
Deployment	Log Management	System Logs	User Management	Export Reports
Flexible Deployment	Collecting Data	All user Profile	Multiple account types	Pdf
HA Supported	Syslog	All current user's login	Role based Access Control	Email
DC-DR supported	Centralized Logging	User & Administration activity	Use Groups	Generate Report based on desired filter
	Normalized log into CEF format	Users successful & Unsuccessful login		
	Handles upto 20k – 50k EPS			

System Specifications

- 12 vCPU or 12 core CPU
- 16 GB RAM
- 250 GB Hard Disk
- Ubuntu 18.04 LTS or Centos 7.4 (physical or virtual)
- 2*1 Gbe Network
- 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.



Total agents	Active agents	Disconnected agents	Never connected agents
1	1	0	0

SECURITY INFORMATION MANAGEMENT

Security events

Browse through your security alerts, identifying issues and threats in your environment.

Integrity monitoring

Alerts related to file changes, including permissions, content, ownership and attributes.

AUDITING AND POLICY MONITORING

Policy monitoring

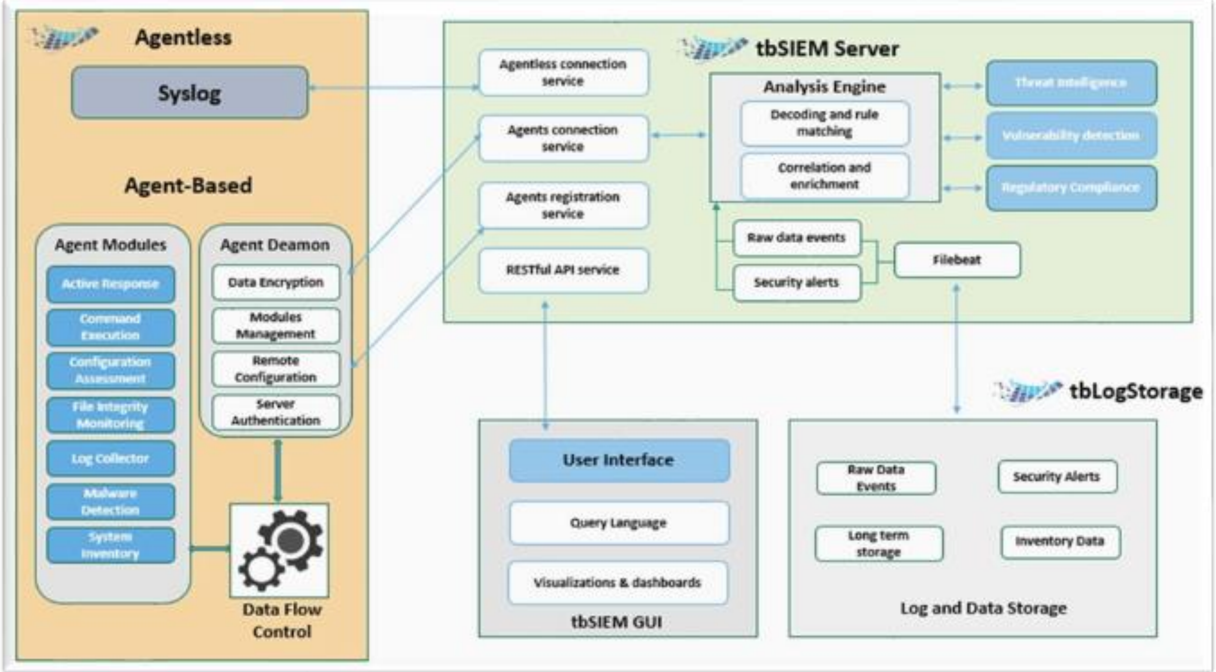
Verify that your systems are configured according to your security policies baseline.

System auditing

Audit users behavior, monitoring command execution and alerting on access to critical files.

Security configuration assessment

Scan your assets as part of a configuration assessment audit.



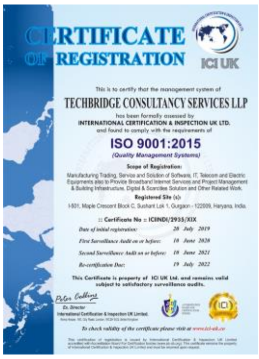
FOR MORE INFORMATION

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



CERTIFICATE OF REGISTRATION

ICI UK

This is to certify that the management system of

TECHBRIDGE CONSULTANCY SERVICES LLP

has been formally assesed by
INTERNATIONAL CERTIFICATION & INSPECTION UK LTD.
and found to comply with the requirements of

ISO 9001:2015
(Quality Management Systems)

Scope of Registration:
Manufacturing Trading, Service and Solution of Software, IT, Telecom and Electric Equipments also to Provide Broadband Internet Services and Project Management & Building Infrastructure, Digital & Scarcities Solution and Other Related Work.

Registered Site (s):
I-501, Maple Crescent Block C, Sushant Lok 1, Gurgaon - 122009, Haryana, India.

:: Certificate No :: ICIINDI/2935/XIX

Date of initial registration:	20 July 2019
First Surveillance Audit on or before:	10 June 2020
Second Surveillance Audit on or before:	10 June 2021
Re-certification Due:	19 July 2022

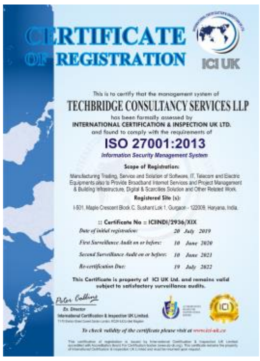
This Certificate is property of ICI UK Ltd. and remains valid subject to satisfactory surveillance audits.

Peter Collins
Ex. Director
International Certification & Inspection UK Limited.
[illegible]

To check validity of the certificate please visit at www.ici-uk.co

This certification of registration is issued by International Certification & Inspection UK Limited accredited with Accreditation Board For Certification bodies (www.ab-cb.org). This certificate remains the property of International Certification & Inspection UK Limited and must be returned upon request.

ISO 27001



CERTIFICATE OF REGISTRATION

ICI UK

This is to certify that the management system of

TECHBRIDGE CONSULTANCY SERVICES LLP

has been formally assesed by
INTERNATIONAL CERTIFICATION & INSPECTION UK LTD.
and found to comply with the requirements of

ISO 27001:2013
Information Security Management System

Scope of Registration:
Manufacturing Trading, Service and Solution of Software, IT, Telecom and Electric Equipments also to Provide Broadband Internet Services and Project Management & Building Infrastructure, Digital & Scarcities Solution and Other Related Work.

Registered Site (s):
I-501, Maple Crescent Block C, Sushant Lok 1, Gurgaon - 122009, Haryana, India.

:: Certificate No :: ICIINDI/2936/XIX

Date of initial registration:	20 July 2019
First Surveillance Audit on or before:	10 June 2020
Second Surveillance Audit on or before:	10 June 2021
Re-certification Due:	19 July 2022

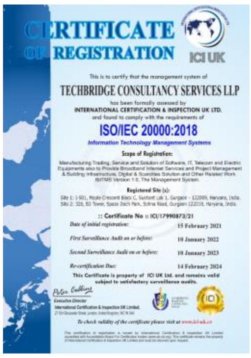
This Certificate is property of ICI UK Ltd. and remains valid subject to satisfactory surveillance audits.

Peter Collins
Ex. Director
International Certification & Inspection UK Limited.
[illegible]

To check validity of the certificate please visit at www.ici-uk.co

This certification of registration is issued by International Certification & Inspection UK Limited accredited with Accreditation Board For Certification bodies (www.ab-cb.org). This certificate remains the property of International Certification & Inspection UK Limited and must be returned upon request.

ISO 20000



CERTIFICATE OF REGISTRATION

ICI UK

This is to certify that the management system of

TECHBRIDGE CONSULTANCY SERVICES LLP

has been formally assesed by
INTERNATIONAL CERTIFICATION & INSPECTION UK LTD.
and found to comply with the requirements of

ISO/IEC 20000:2018
Information Technology Management Systems

Scope of Registration:
Manufacturing Trading, Service and Solution of Software, IT, Telecom and Electric Equipments also to Provide Broadband Internet Services and Project Management & Building Infrastructure, Digital & Scarcities Solution and Other Related Work. tbITMS Version 1.0, The Management System.

Registered Site (s):
Site 1: I-501, Maple Crescent Block C, Sushant Lok 1, Gurgaon - 122009, Haryana, India.
Site 2: 326, B3 Tower, Spaze Itech Park, Sohna Road, Gurgaon 122018, Haryana, India.

:: Certificate No :: ICI/17990873/21

Date of initial registration:	15 February 2021
First Surveillance Audit on or before:	10 January 2022
Second Surveillance Audit on or before:	10 January 2023
Re-certification Due:	14 February 2024

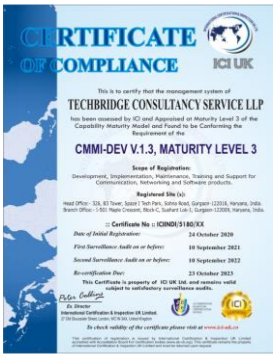
This Certificate is property of ICI UK Ltd. and remains valid subject to satisfactory surveillance audits.

Peter Collins
Executive Director
International Certification & Inspection UK Limited.
27 Old Gloucester Street, London, United Kingdom, WC1N 3AX

To check validity of the certificate please visit at www.ici-uk.co

This certification of registration is issued by International Certification & Inspection UK Limited accredited with Accreditation Board For Certification bodies (www.ab-cb.org). This certificate remains the property of International Certification & Inspection UK Limited and must be returned upon request.

CMMi L3



CERTIFICATE OF COMPLIANCE

ICI UK

This is to certify that the management system of

TECHBRIDGE CONSULTANCY SERVICE LLP

has been assessed by ICI and Appraised at Maturity Level 3 of the Capability Maturity Model and Found to be Conforming the Requirement of the

CMMI-DEV V.1.3, MATURITY LEVEL 3

Scope of Registration:
Development, Implementation, Maintenance, Training and Support for Communication, Networking and Software products.

Registered Site (s):
Head Office:- 326, B3 Tower, Spaze I Tech Park, Sohna Road, Gurgaon-122018, Haryana, India.
Branch Office:- I-501 Maple Crescent, Block-C, Sushant Lok-1, Gurgaon-122009, Haryana, India.

:: Certificate No :: ICIINDI/5180/XX

Date of Initial Registration:	24 October 2020
First Surveillance Audit on or before:	10 September 2021
Second Surveillance Audit on or before:	10 September 2022
Re-certification Due:	23 October 2023

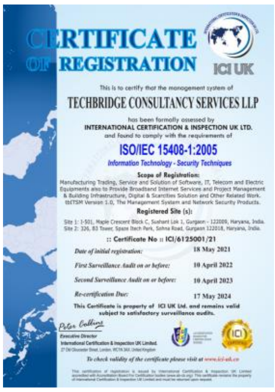
This Certificate is property of ICI UK Ltd. and remains valid subject to satisfactory surveillance audits.

Peter Collins
Ex. Director
International Certification & Inspection UK Limited.
27 Old Gloucester Street, London, WC1N 3AX, United Kingdom

To check validity of the certificate please visit at www.ici-uk.co

This certification of registration is issued by International Certification & Inspection UK Limited accredited with Accreditation Board For Certification bodies (www.ab-cb.org). This certificate remains the property of International Certification & Inspection UK Limited and must be returned upon request.

ISO 15408-1



CERTIFICATE OF REGISTRATION

ICI UK

This is to certify that the management system of

TECHBRIDGE CONSULTANCY SERVICES LLP

has been formally assesed by
INTERNATIONAL CERTIFICATION & INSPECTION UK LTD.
and found to comply with the requirements of

ISO/IEC 15408-1:2005
Information Technology - Security Techniques

Scope of Registration:
Manufacturing Trading, Service and Solution of Software, IT, Telecom and Electric Equipments also to Provide Broadband Internet Services and Project Management & Building Infrastructure, Digital & Scarcities Solution and Other Related Work. tbITSM Version 1.0, The Management System and Network Security Products.

Registered Site (s):
Site 1: I-501, Maple Crescent Block C, Sushant Lok 1, Gurgaon - 122009, Haryana, India.
Site 2: 326, B3 Tower, Spaze Itech Park, Sohna Road, Gurgaon 122018, Haryana, India.

:: Certificate No :: ICI/6125001/21

Date of initial registration:	18 May 2021
First Surveillance Audit on or before:	10 April 2022
Second Surveillance Audit on or before:	10 April 2023
Re-certification Due:	17 May 2024

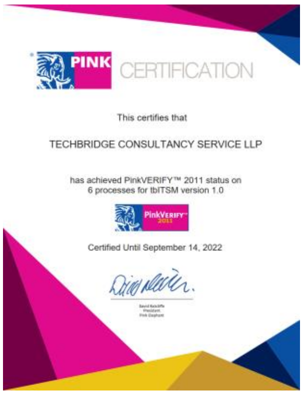
This Certificate is property of ICI UK Ltd. and remains valid subject to satisfactory surveillance audits.

Peter Collins
Executive Director
International Certification & Inspection UK Limited.
27 Old Gloucester Street, London, WC1N 3AX, United Kingdom

To check validity of the certificate please visit at www.ici-uk.co

This certification of registration is issued by International Certification & Inspection UK Limited accredited with Accreditation Board For Certification bodies (www.ab-cb.org). This certificate remains the property of International Certification & Inspection UK Limited and must be returned upon request.

PinkVERIFY



PINK CERTIFICATION

This certifies that

TECHBRIDGE CONSULTANCY SERVICE LLP

has achieved PinkVERIFY™ 2011 status on
6 processes for tbITSM version 1.0

PinkVERIFY™ 2011

Certified Until September 14, 2022

David Ratcliffe
President
Pink Elephant

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