PRODUCT DATASHEET

tbSOAR: Security Orchestration Automation Response

INTRODUCTION

Optimize your security Processes, Increase Team Efficiency, and Reduce Time to Respond with tbSOAR

tbSOAR Platform provides a central location to integrate not only your security tools but all of your security team's processes.
Document those processes increases efficiency with automation and orchestration. Continuously leverage high confidence threat intelligence stored within when making decisions related to both tactics and strategy. tbSOAR enables the automation and continuation of this feedback loop throughout your entire security team.

How tbSOAR Helps?

- **Resolves Alert Faster:** Average single alert resolution decreased from 30 minutes to 3 minutes, significantly reducing MTTR.
- **Automate Repetitive Tasks:** Repetitive analyst actions automated across 40 Playbooks to save 1000's of hours previously spent on tasks like manual look ups and notifications.
- **Prevent Employee Burn Out:** A reduced burden on analysts by 50% in the year - decreasing burnout and attrition
- **Save Time and Money:** Over $1.3 million per year saved in labour costs with 60 automated workflows.
- **High Confidence Intelligence Baked In:** Receive access to various pre-populated intelligence sources packaged in a digestible and easy-to-use format. Because it's baked in, there's no need for complicated data manipulation or time-intensive lookups: it's all converted to a predictable and easily understood format while still preserving the source's attribution information and reputation details.

Highlights:

- Visual Playbook Builder
- Threat Intel Management
- tbSOAR Mobile Application
- Incident Response Content Pack
- Role-Based Dashboards and Reporting
- Crisis Management with Incident War Room
- Role-Based, Streamlined Incident Management
- Ability to automatically identify observables that have been already seen in previous cases.

Key Features

- Useful for the: SOCs, CSIRTs,CERTs
- Provide the platformfor detail investigation for the Security incident
- Support MISP as threat intelligence platform

- Decrease Ambiguity to make more Confident Decisions: Capture, correlate, and make decisions based on high-fidelity intelligence relevant to your organization. Adjust decisions on the fly based on the changes seen in the intelligence that is influencing the process. Automatically incorporate the latest intelligence to inform decision-making consistently.
- Integrate Seamlessly with Existing Tools for More Efficient Processes: Integrations with the tools and technologies in users' existing ecosystems make security easy and effective. Whether pre- built templates or completely customizable workflows are preferred - tbSOAR supports the integrations required to power the use cases you need.
- Minimize the Time Analysts Spend Looking for Relevant Information: Automatically save relevant information as Artifacts for further usage and analysis. Leverage data to gain more insight from thousands of tbSOAR users around the globe into intel-related Artifacts such as IP addresses, emails, or URLs. Add those Artifacts back into intelligence repository to help during future investigations and across other team initiatives.
- Correlate Critical Intel to Events and Reduce the Risk of Overlooking Insights: tbSOAR tells you about potential and known associations across threat intelligence and cases to give you an immediate understanding of previous or open investigations related to a piece of threat intelligence you're investigating and vice versa. Get insight into these relationships and the associated details automatically, before you even need to ask.
- Flexible Deployment Options: Flexible deployments in Cloud or On-Premises get you up and running the way you want quickly. Multi Environment Orchestration allows for orchestration across cloud, multi-cloud or hybrid on-premises environments. Wherever your security controls reside, tbSOAR connects them seamlessly.

FEATURES:

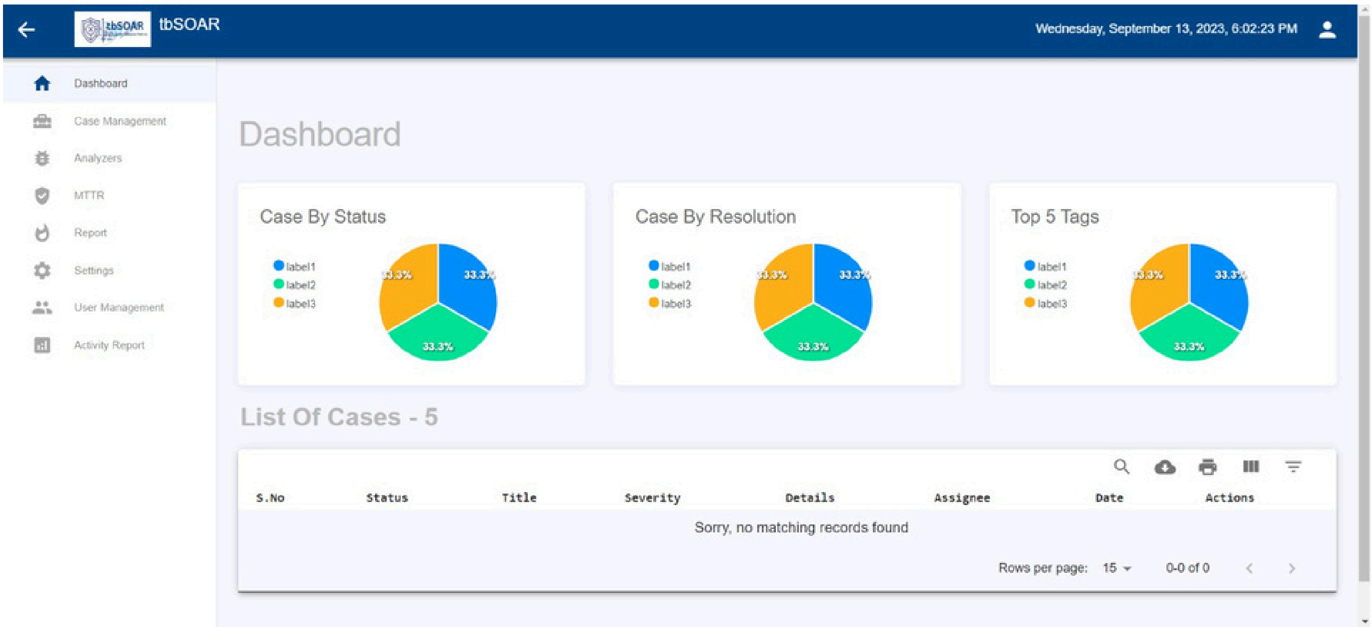
- Collaborate: Multiple analysts from one organizations can work together on the same case simultaneously. Multi-tenancy and fine grained user profiles let organizations and analysts work and collaborate on a same case across organizations.
- Elaborate: Every investigation corresponds to a case. Cases can be created from scratch or from MISP events, SIEM alerts, email reports and any other noteworthy source of security events.
- Analyze: You can add one or hundreds if not thousands of observables to each case you create. You can also create a case out of a MISP event. it is possible to send SIEM alerts, phishing and other suspicious emails and other security events.
- Multi-tenancy: Use a siloed multi-tenancy: many organizations can be defined without allowing them to share data; Use a collaborative multi-tenancy: a set of organizations can be allowedto collaborate on specific cases/tasks/observables, using custom defineduser profiles (RBAC).
- Case Management: tbSOAR enables you to manage and collaborate data to resolve case efficiently on a single pane of glass. The case management helps streamline investigations and expedite case resolution.
- Consolidation: You can aggregate alerts from different sources based on configured time-span or common conditions. This helps in gathering all the correlated information for the suspected threat and further helps in finding the optimized solution for case handling.
- Orchestration: The automated solutions provided by SOAR can seek information from the SOC or pass the control to the security operations center (SOC) for decision making and then take the control back to automation. Depending on the case scenario, tbSOAR can orchestrate the control flow from automation to human analyst.
- Enrichment: SOAR uses enrichment feature to gather additional information about the event contexts. These additional insights act as guides to carry on the detailed threat investigation.
- Automation: SOAR leverages both fully automatic and semi automatic solution for threat remediation and response. You can automate mundane repetitive tasks, prioritize events and streamlines security processes to deliver accelerated case response.
- Response: SOAR automation can execute protective actions, stored in playbooks, to prevent any threat impact to your organization. This capability offers unique solution to respond to events in a quick and effective manner.
- Reporting and Analytics: You can generate reports to view detailed information about cases. SOAR offers a pre-defined report template for data presentation or you can create your own template to specify which data you want to include. To analyze the data further, you can view

- **Pollen**: For granular interaction with, without needing to open the web browser allows analysts to send alerts to out of different sources. Those alerts can then be previewed and imported into cases using pre-defined templates.
- Provide previewed and transformed into new cases using pre-defined incident response templates or added into existing ones.
- The analyst can also easily mark observables as IOCs and isolate those using a search query then export them for searching in a SIEM or other data stores.
- Security analysts with a knack for scripting can easily add their own analyzers to Orchestration engine in order to automate actions that must be performed on observables or IOCs.
- All data statistics in the form of tables and charts in Dashboard.

- **Authentication:**
  local accounts
  Active Directory
  LDAP
  Basic Authenticate
  API keys
  AUTH2
  Multi Factor Authentication

- **Incident Creation through following ways:**
  Email
  SIEM
  MISP Events
  Other security tools through RestAPI

- High Confidence Intelligence Baked-In
- Leverage Insights from Other TechBridge Users
- Providing insights into your security operations
- Bi-Directional Integrations with 100's of Products
- Customizable Dashboards to Bubble Up What Matters Most
- Complete Investigations from a Single Interface
- Dedicated TechBridge Customer Success Team
- Deployment Support for Cloud and On- Premises
- Scale Incrementally Without Affecting Performance
- The platform is powerful for engineers and intuitive for analysts
- **Uniting context with a threat-centric approach:** tbSOAR automatically groups related alerts into a single threat-centric case, reducing caseload, improving efficiency, allowing for a single analyst to work the case and shrinking overall noise for the SOC.



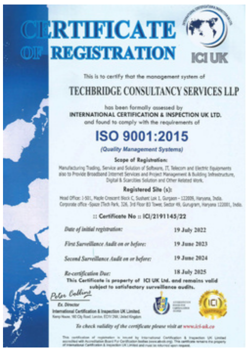
S.No	Status	Title	Severity	Details	Assignee	Date	Actions

Sorry, no matching records found

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:-



CERTIFICATE OF REGISTRATION

ICI UK

This is to certify that the management system of

TECHBRIDGE CONSULTANCY SERVICES LLP

has been formally assessed 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):

Head Office: I-501, Maple Crescent Block C, Sushant Lok 1, Gurgaon - 122009, Haryana, India.
Corporate office -Space ITech Park, 326, 3rd Floor B3 Tower, Sector 49, Gurugram, Haryana 122001, India.

:: Certificate No :: ICI/2191145/22

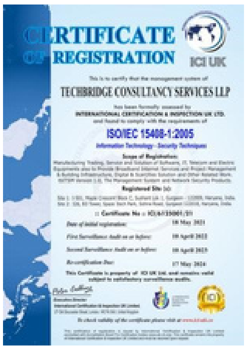
Date of initial registration: 19 July 2022
First Surveillance Audit on or before: 19 June 2023
Second Surveillance Audit on or before: 19 June 2024
Re-certification Due: 18 July 2025

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.
Kemp House, 160 City Road, London, EC1V 2NX, 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.abcb.org). This certificate remains the property of International Certification & Inspection UK Limited and must be returned upon request.



CERTIFICATE OF REGISTRATION

ICI UK

This is to certify that the management system of

TECHBRIDGE CONSULTANCY SERVICES LLP

has been formally assessed 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. ISITSM 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 :: [illegible]

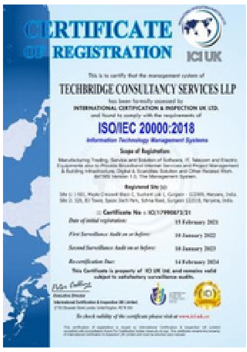
Date of initial registration: 18 May 2021
First Surveillance Audit on or before: 09 April 2022
Second Surveillance Audit on or before: 09 April 2023
Re-certification Due: 17 May 2024

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

Executive Director
International Certification & Inspection UK Limited
[illegible]

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

[illegible]



CERTIFICATE OF REGISTRATION

ICI UK

This is to certify that the management system of

TECHBRIDGE CONSULTANCY SERVICES LLP

has been formally assessed 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. ISITSM 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

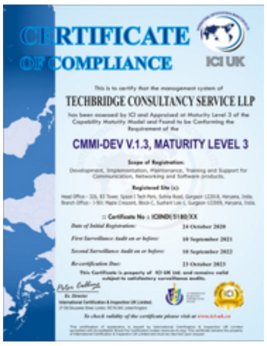
Date of initial registration: 15 February 2021
First Surveillance Audit on or before: 10 January 2022
Second Surveillance Audit on or before: 10 January 2023
Re-certification Due: 14 February 2024

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

Executive Director
International Certification & Inspection UK Limited
[illegible]

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

[illegible]



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

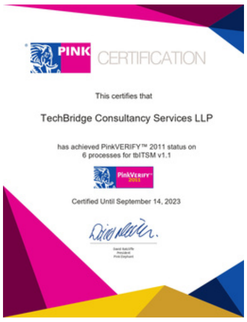
Date of Initial Registration: 24 October 2020
First Surveillance Audit on or before: 10 September 2021
Second Surveillance Audit on or before: 10 September 2022
Re-certification Due: 23 October 2023

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.
[illegible]

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

[illegible]



PINK CERTIFICATION

This certifies that

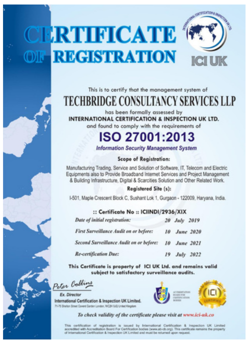
TechBridge Consultancy Services LLP

has achieved PinkVERIFY™ 2011 status on
6 processes for tbITSM v1.1

PinkVERIFY™ 2011

Certified Until September 14, 2023

David Ratcliffe
President
Pink Elephant



CERTIFICATE OF REGISTRATION

ICI UK

This is to certify that the management system of

TECHBRIDGE CONSULTANCY SERVICES LLP

has been formally assessed 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.
71-75 Shelton Street Covent Garden London, WC2H 9JQ United Kingdom

ACCREDITATION BOARD FOR CERTIFICATION BODIES

ICI CERTIFIED

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.

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