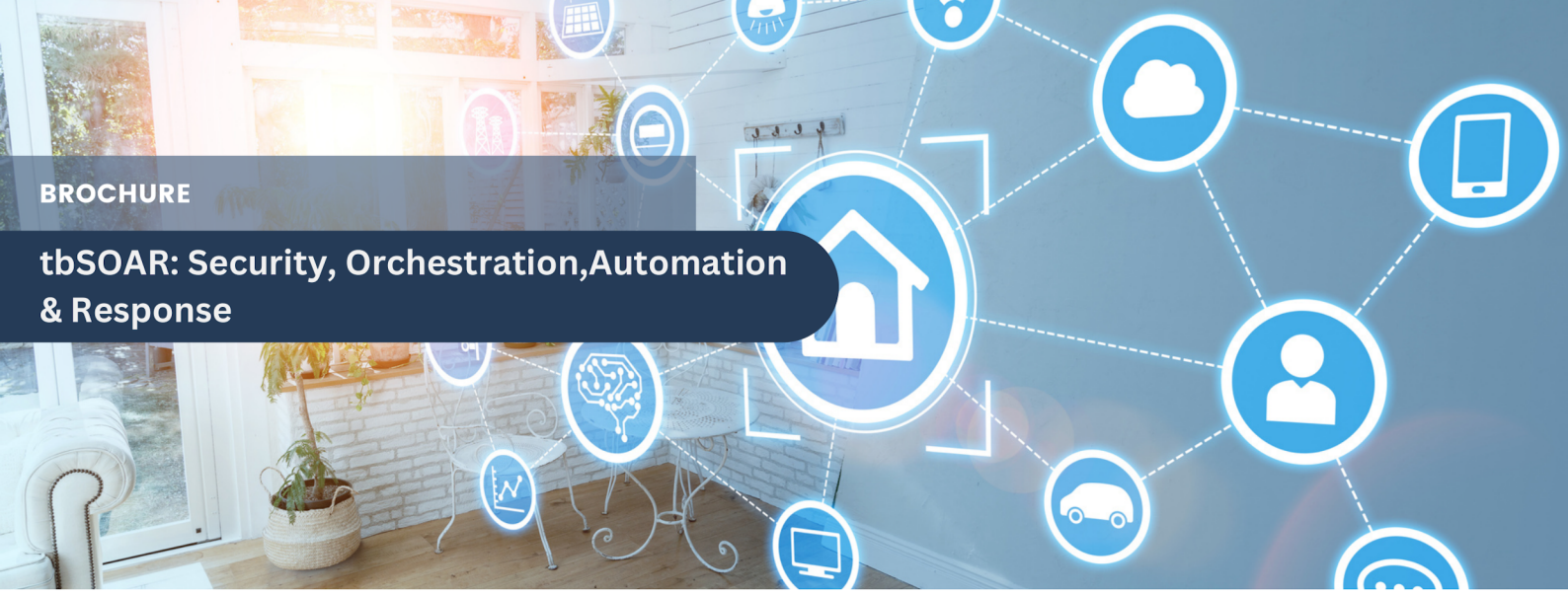

BROCHURE

tbSOAR: Security, Orchestration,Automation & Response

INTRODUCTION

SOAR connects teams and tools to accelerate security and IT processes.
It refers to a collection of software solutions and tools that allow organizations to streamline security operations in three key areas: threat and vulnerability management, incident response, and security operations automation.

Security automation is the automatic handling of security operations-related tasks. It is the process of executing these tasks—such as scanning for vulnerabilities, or searching for logs—without human intervention. Security orchestration refers to a method of connecting security tools and integrating disparate security systems. It is the connected layer that streamlines security processes and powers security automation.

HOW CAN SOAR HELP YOUR ORGANIZATION

Organizations today face many challenges when it comes to getting ahead of their security goals. For one, finding talent is time-consuming, and once you do find the right fit you want them to be able to focus on the most impactful work—not get bogged down in manual, recurring, time- intensive tasks. Additionally, chances are high that your organization uses technology that multiple teams need to touch and collaborate on, yet the various pieces don't always integrate.

While adding a 25th hour into the day will remain a pipe dream, it is possible to get some time back and achieve your security goals. That's where security orchestration and automation comes in. With an effective security orchestration, automation, and response (SOAR) solution, it's possible to achieve more, in less time, while still allowing for human decision-making when it's most critical. Move beyond relying on point-to-point integrations for your technology stack; instead, rely on a solution that empowers you to build out your various processes and connects you with the right people and technology to achieve your goals.

Key Benefits

- Automates repetitive, menial tasks
- Responds quickly to complex attacks
- Orchestrate all aspects of the incident response process
- Enables fast decisions and quick actions by the incident response team
- Coordinate response process with privacy tasks and workflows
- Risk Assessment tools help evaluate notification requirements
- Speed up investigation with built-in real-time user and entity context

Modules

1. Track the following through customizable reports and dashboards:
- ROI
- MTTD
- MTTR

2. Reduce security incident discovery times from hours to seconds
3. A simplified, easy-to-use GUI that manages:
- Security Alerts
- Incident Indicators
- Assets and Tasks

SOAR HELPS BUILD WORKFLOWS, STREAMLINE OPERATIONS:

One way to be successful with the orchestration layer is to use a solution that comes with a library of plugins for the most-used technology and a set of pre-built workflows for common use cases, enabling you to easily connect your technology stack and automate across your security and IT processes. You will likely need to build additional orchestrations or workflows customized to your team, but having pre-built examples or easy-to-use building blocks to work from should help accelerate that process.

SOAR INCREASES FLEXIBILITY, EXTENSIBILITY, AND COLLABORATION:

A security orchestration, automation and response solution should provides you with flexibility and additional opportunities for collaboration. Whether it's adapting work flows for your organization, creating and managing integrations, or building entirely new processes, it's important to look for a vendor that is willing to partner with you.

A partnership built to last, with a community focus, will support you in achieving your security orchestration and automation goals to accelerate your security program. Your partner should set you up for success, working alongside you to achieve your goals. They should understand the use cases you're looking to optimize, and help you see solutions you may not have even thought of, all backed by easy-to-understand documentation and support.

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE:

It is a security orchestration, automation, and response solution that enables your team to accelerate and streamline time-intensive processes without writing a single line of code. With 200+ plugins to connect your tools and easily customizable connect-and-go workflows, you'll free up your team to tackle other challenges, while still leveraging human decision points when it's most critical. With significant time savings and productivity gains across overall security operations, you'll go from overwhelmed to operating at maximum efficiency in no time.

BENEFITS

- Improve operational efficiency when automation and orchestration is applied to prioritized, high-risk threats instead of low- value SIEM alerts
- Reduce mean time to resolution (MTTR) using robust automation capabilities with 275+ connectors and 3000+ playbook actions
- Extend advanced analytics to incident response using an artificial intelligence-driven recommendation engine that learns the actions analysts take in response to threats and uses what it learns to recommend or automate future response actions.
- Increase SOC team productivity by eliminating false positives and focusing only on the alerts that matter
- Automate within the Visual Playbook Designer with 350+ security platform integrations and 3000+ actions for automated workflows and connectors
- Minimize human error by employing clear, auditable playbooks and custom modules to handle ever-changing investigation requirements
- Scale your network security solution with a truly multitenant distributed architecture from a single, collaborative console
- Identify real threats with automated false positive filtering and predict similar threats and campaigns
- Eliminate repetitive tasks through automation, correlation of incidents, threat intelligence, and vulnerability data
- Take advantage of the in-built Incident War Room for streamlining crisis management and collaborative P1 incident investigations
- Leverage the mobile application for taking important decisions and staying informed while on the move
- Build and edit connectors easily within the product user interface using the Connector Builder Wizard n Flexible Deployment Options - VM, hosted or cloud.

KEY FEATURES:-

- Role-Based, Streamlined Incident Management

tbSOAR's Enterprise Role-Based Incident Management solution provides organizations with robust field level role based access control to manage sensitive data in accordance with SOC policies and guidelines. Easily manage alerts and incidents in a customizable filter grid view with automated filtering, to keep analysts focused on real threats. Execute dynamic actions and playbooks on alerts and incidents and analyze correlated threat data in an intuitive user interface. tbSOAR's ML-powered Recommendation Engine predicts various fields such as severity, asset, user, based on previously identified cases, aiding the SOC analyst in grouping and linking them together to identify duplicates and campaigns involving similar alerts, common threats, and entities. The tbSOAR mobile app adds a new dimension to the incident management and allows users to take actions like monitoring alert queue, triggering important playbooks, and providing critical approvals on the go.

- Truly Multi-Tenant

tbSOAR provides a truly distributed multi- tenant product offering with a scalable, resilient, secure, and distributed architecture, allowing MSSPs to offer MDR-like services, while supporting operations in regional and global SOC environments. With the ability to run automation workflows on specific tenants remotely, ability to manage tenant playbooks, modules, views remotely, handling unique customer environments and product diversity becomes streamlined. tbSOAR also involves tenants in case of approval requirements to control data flow to the master nodes. Other tenant features include creating tenant-specific alerts, incident views, reports and dashboards, and filter views. Service providers and customers can choose between a dedicated SOAR tenant node for complete isolation and management or a light-weight tbSOAR agent that can be used to leverage the customer's on- premise integrations. A hybrid model is also possible, providing a lot of flexibility in designing a right fit for various scenarios.

- Visual Playbook Builder

tbSOAR's Visual Playbook Designer allows SOC teams to design, develop, debug, control, and use playbooks in the most efficient manner. The intuitive design includes a drag and drop interface to string multiple steps together, using350+ OOB workflow integrations, 3000+ automated actions, a comprehensive expression library for easy development, playbook simulation and referencing, ability to execute code in workflows like python, versioning, privacy control, crash recovery, advanced step controls like looping, error handling, notifications, undo/redo, and more.

Advanced features such as playbook prioritization, public/private visibility, and simulation engine provide a greater degree of control in designing a well orchestrated solution.

tbSOAR's extensible platform provides the ability to define new modules with customization of fields, views, and permissions, and creation of smart automated workflows and playbooks on top of them, simplifying the analyst's ability to support solutions for vulnerability and threat management as well as regulation and compliance.

- Crisis Management with Incident War Room

tbSOAR offers a dedicated crisis management framework, the Incident War Room, which can be used for streamlining and collaborative PI incident investigations. Any critical incident can be a trigger to start a war room around it and quickly gather in team members across the board. It has built-in access control to ensure who gets to see what, task management for assigning, monitoring, and organizing the investigation, dedicated collaboration facility that can work in sync with external collaboration tools like MS teams, Slack, Zoom, and much more. Purpose-built for crisis management, it takes care of other important elements like Announcements board and a dedicated Reporting section also.

- Role-Based Dashboards and Reporting

Role-based dashboards and reporting empower SOC teams to measure, track, and analyze investigations and SOC performance granularly with quantifiable metrics. tbSOAR's ready-made library of industry standard, persona focused dashboard templates, intuitive drag and drop visual layout builders, ensures SOC teams have the best tools to optimize their time and resources. Comprehensive charts, listings, counters, and performance metrics help create rich views and informative data models. tbSOAR also provides industry-standard reports for Incident Closure, Incident Summary, Weekly Alert and Incident Progress, IOC Summary, and many others. It enables SOC teams to track metrics such as MTTR and MTTD over various NIST approved incident phases, analyst loads, escalation ratios, Automation ROIs, and other SOC performance metrics.

- **Threat Intel Management**

tbSOAR delivers Enhanced Threat Intelligence Management Support leveraging its deep integration with FortiGuard offering unrestricted lookup of indicator reputations, threat categories, and Threat Encyclopedia access. Ingestion of structured and unstructured feeds is supported with the ability to import indicators from CSV/STIX files and exporting indicators in STIX format.

Analysts can also manage indicators more easily with TLP (Traffic Light Protocol) for indicator sharing, indicator expiry, and exclusion lists. tbSOAR also includes multiple out-of-box playbooks for sharing indicators with standard SIEM and UEBA products.

- **tbSOAR Mobile Application**

tbSOAR mobile application is an extension of tbSOAR's Web interface, which facilitates important and urgent actions such as immediate approvals, notifications, and threat monitoring allowing SOC teams and executives to act swiftly and provide critical inputs on the go. Analysts can easily navigate tbSOAR through the application's rich user experience and execute actions like viewing and reassigning records, providing approvals, triggering important playbooks, and monitoring alert queues.

- **Connector and Widget Creation Studio**

With the built-in Connector Wizard, analysts can easily create custom connectors for sending and retrieving data from various third-party products as well as edit existing connectors.

The easy-to-use interface offers a built-in testing framework and facilitates building connectors directly in the product UI using a guided wizard framework. Analysts can select from multiple pre-made templates to help develop their connectors, ensuring best practices.

In a similar manner, the Widget Creation Wizard allows for building custom new widgets within the UI, ensuring that users are never limited in ways to represent their data as required.

- **Incident Response Content Pack**

The tbSOAR Incident Response Content Pack enables Analysts and Users to experience the power of tbSOAR's incident response. Built with a modular architecture, the Incident Response Content Pack is the implementation of best practices to configure and implement an efficient Security Orchestration, Automation, and Response solution in an optimal manner.

The content pack consists of various default modules, comprehensive collection of utility and use case Playbooks, industry-standard Dashboards and Roles, as well as many samples, simulations, and training data that enable SOC teams to experience the power of tbSOAR and get a quick head start.

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