Security Orchestration, Automation and Response (SOAR)

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 lookups 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.
- **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:
- Useful for the: SOCs, CSIRTs, CERTs
- Provide the platform for detail investigation for the Security incident
- Support MISP as threat intelligence platform
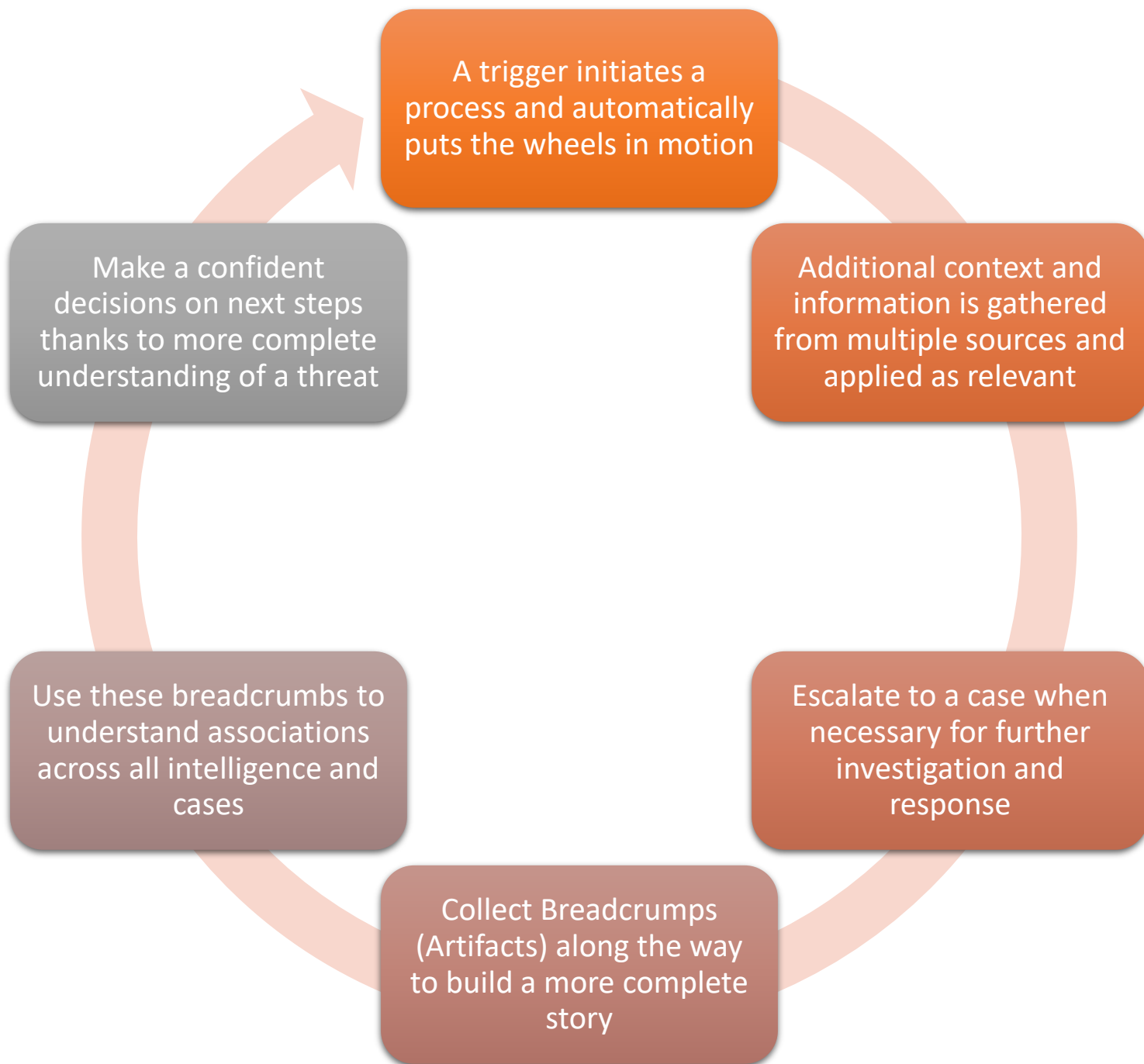
Key Features:
- **Collaborate:** Multiple analysts from one organizations can work together on the same case simultaneously. Multi-tenancy and fine grained user profiles let organizations and analysts work and collaborate on a same case across organizations.

- **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.

- Ability to automatically identify observables that have been already seen in previous cases.

- 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.

- **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 allowed to collaborate on specific cases/tasks/observables, using custom defined user profiles (RBAC).

- **Authentication:**
  - local accounts
  - Active Directory
  - LDAP
  - Basic Auth
  - API keys
  - OAUTH2
  - Multi Factor Authentication

- Incident Creation through following ways:
  1. Email
  2. SIEM
  3 MISP Events
  4. Other security tools through RestAPI

- Provide previewed and transformed into new cases using pre-defined incident response templates or added into existing ones.

- Following Integration supports:
  - Threat Hunting Platform
  - Meta Alert Feader
  - SIEM
  - MISP
  - User Behavior Analysis
  - Other Security Devices through rest API

- **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.

- Role-Based, Streamlined Incident Management

- Visual Playbook Builder

- Crisis Management with Incident War Room

- Role-Based Dashboards and Reporting

- Threat Intel Management

- tbSOAR Mobile Application

- Incident Response Content Pack

How tbSOAR is different?

- High Confidence Intelligence Baked-In
- Bi-Directional Integrations with 100's of Products
- Leverage Insights from Other TechBridge Users
- 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
- **Uniting context with a threat-centric approach:** Forget focusing on alerts and drowning in analysis. Our patented technology 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.
- **The platform is powerful for engineers and intuitive for analysts:** From our visual investigation to our code-free playbook builder, you don't need to be a python guru or memorize complex command lines.
- **Providing insights into your security operations:** We've intentionally built in the ability to easily see the scope of activities, generate insights that drive improvement, and measure improvement over time - so you can easily report progress to upper management, get a close-up view on what's being worked on, what's delayed and where the bottlenecks are occurring.

How tbSOAR works?

A trigger initiates a process and automatically puts the wheels in motion

Additional context and information is gathered from multiple sources and applied as relevant

Escalate to a case when necessary for further investigation and response

Collect Breadcrumps (Artifacts) along the way to build a more complete story

Use these breadcrumbs to understand associations across all intelligence and cases

Make a confident decisions on next steps thanks to more complete understanding of a threat

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	ISO 27001	ISO 20000	CMMi L3

ISO 15408-1	PinkVERIFY

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