ENERGY SOAR

bako tech®

SOAR FOR BEGINNERS

The high frequency of attacks, the complexity of IT networks, and the lack of qualified specialists expose many companies to data loss, financial losses, and reputational damage. In response to these challenges, many organizations are leveraging SOAR (Security Orchestration, Automation, and Response) solutions.

www.energysoar.com

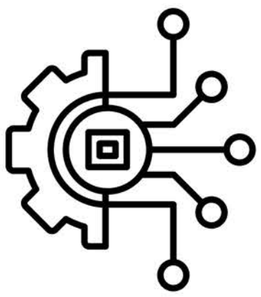
What is SOAR?

SOAR is a solution that enables the automation of security incident response processes. Energy SOAR is one of the latest and most innovative SOAR solutions available in the market. It is an integrated platform with the company's IT systems designed to enhance the speed and effectiveness of security incident response.

SOAR stands for Security Orchestration, Automation, and Response, and each component of this platform plays a specific role in the security incident response process.

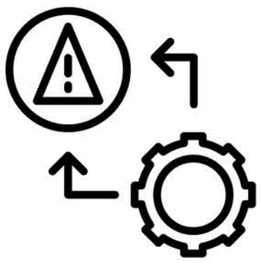
Orchestration

Orchestration in SOAR involves coordinating actions and integrating various tools, systems, and processes to effectively respond to security incidents. Orchestration enables the creation of automated incident response processes and improves collaboration among different teams involved in incident response.



Automation

Automation is a key element of SOAR as it allows for faster and more efficient response to attacks. Through automation, it is possible to automatically trigger appropriate response procedures, detect and isolate threats, and send incident notifications, among other actions.



Response

The response component in SOAR involves promptly and effectively taking actions to minimize the damages resulting from a security incident. This includes identifying and classifying incidents, isolating and neutralizing threats, as well as analyzing and documenting incidents.

Why implementing SOAR?

Lack of adequate resources

Many organizations struggle with a shortage of appropriately skilled personnel capable of effectively responding to security incidents. SOAR enables the automation of response processes, saving time and human resources while ensuring effective incident response.

Regulatory requirements

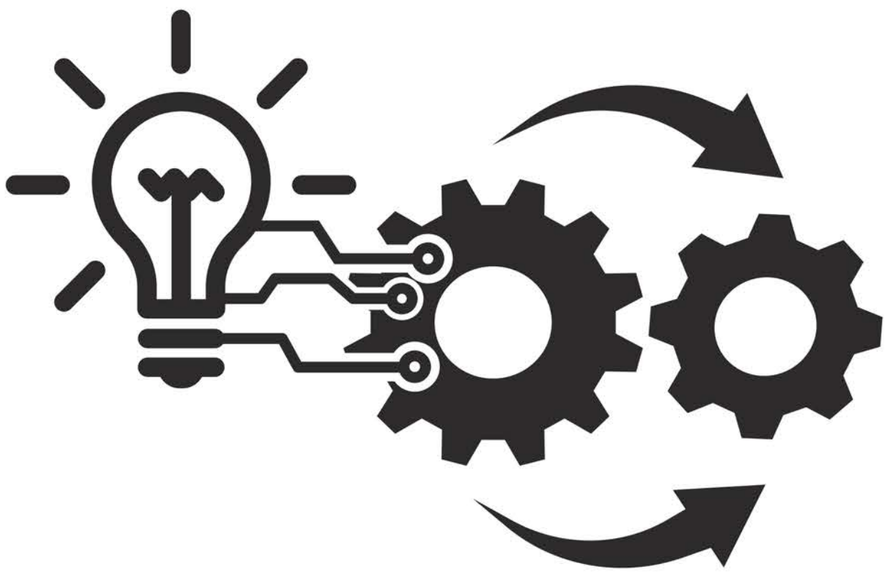
Many sectors of the economy are subject to stringent regulatory requirements regarding cybersecurity. SOAR enables organizations to meet these requirements by automating incident response processes and reporting results.

Need for swift response

In today's landscape, incident response needs to be swift and effective. SOAR allows for rapid detection and response to threats, minimizing the damages resulting from attacks.

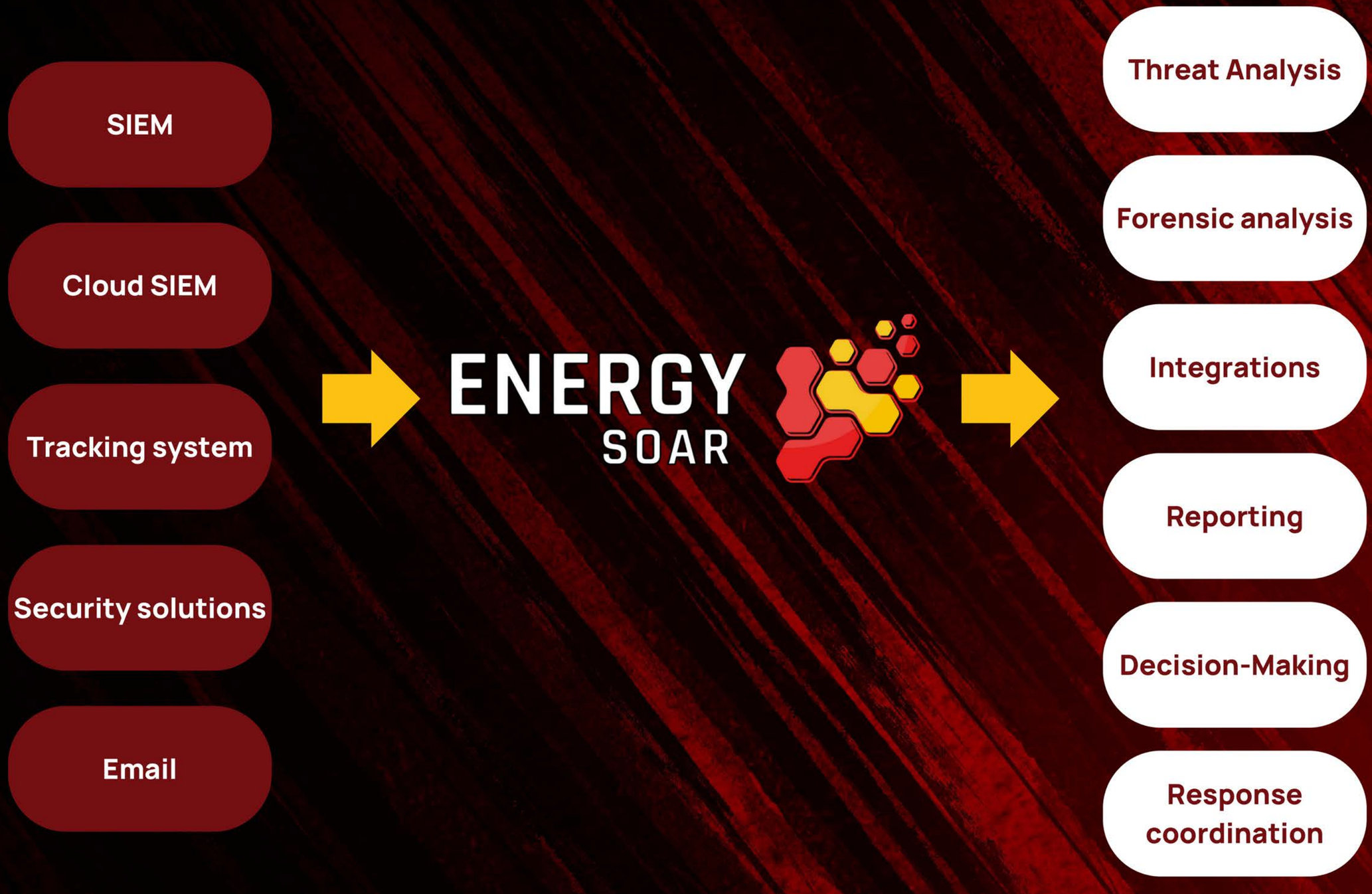
Need for continuous improvement

Modern organizations must constantly enhance their procedures and processes in the realm of cybersecurity to address growing threats. SOAR facilitates continuous improvement of incident response processes and enhances the operations of the IT security team.



Architecture

The Energy SOAR system is a comprehensive solution for handling security incidents, consolidating information on identified threats. It seamlessly integrates with diverse organizational IT and security systems—including SIEM, email, cloud environments, ticketing systems, firewalls, and security systems. This integration enables the gathering of information from various sources for comprehensive incident management.



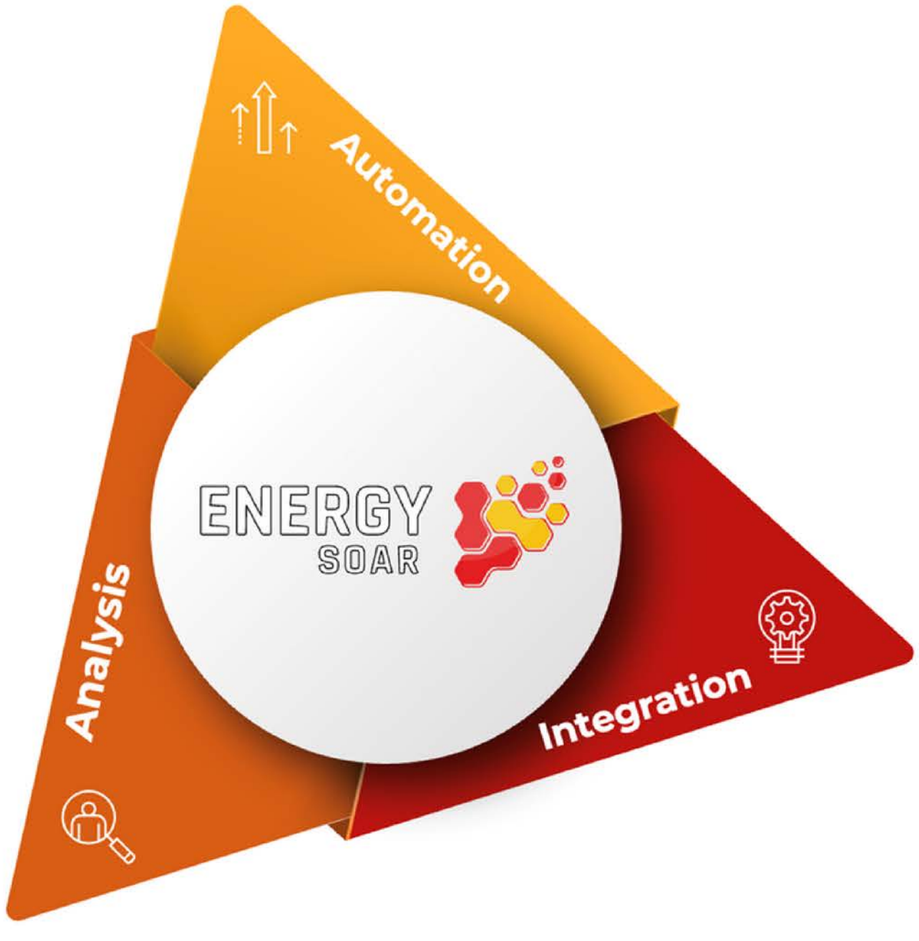
Integrations

The Energy SOAR system goes beyond data collection from source systems; it can initiate automated actions on integrated IT and security systems through API integration. When detecting a threat or incident, SOAR can trigger specific responses, such as quarantining a computer or blocking an IP address in the firewall. Additionally, it can send notifications to other systems or teams, prompting them to take action.

SOAR employs various mechanisms, including PowerShell or Python scripts, and integrates with network management tools, security analysis tools, and other IT functionalities through APIs. Importantly, administrators can configure SOAR to choose actions based on specific conditions, aligning with the organization's established security rules and policies.

Integration with CSIRT

The integration of a SOAR-class system with an external CSIRT (Computer Security Incident Response Team) involves facilitating collaboration and information exchange between the organization and the external CSIRT service provider.



Lifecycle of a SOAR System in an Organization

Energy SOAR lifecycle is a cyclical process designed for peak efficiency and alignment with organizational security needs, requiring methodical planning and active participation from staff at all stages.

Key to the success of implementing a SOAR system is proper planning and alignment with the organization's needs, as well as continuous development and adaptation to changing requirements.

1 PLANNING

This foundational stage involves setting clear objectives aligned with the organization's security goals. It includes identifying common incident types and their management strategies and assessing integration capabilities with existing security infrastructure.

2 IMPLEMENTATION

Following planning, the SOAR system is established within the organization. This entails configuring the system to organizational specifications, integrating with current security tools, designing automated workflows for efficiency, and training staff responsible for its operation.

3 OPERATION AND DEVELOPMENT

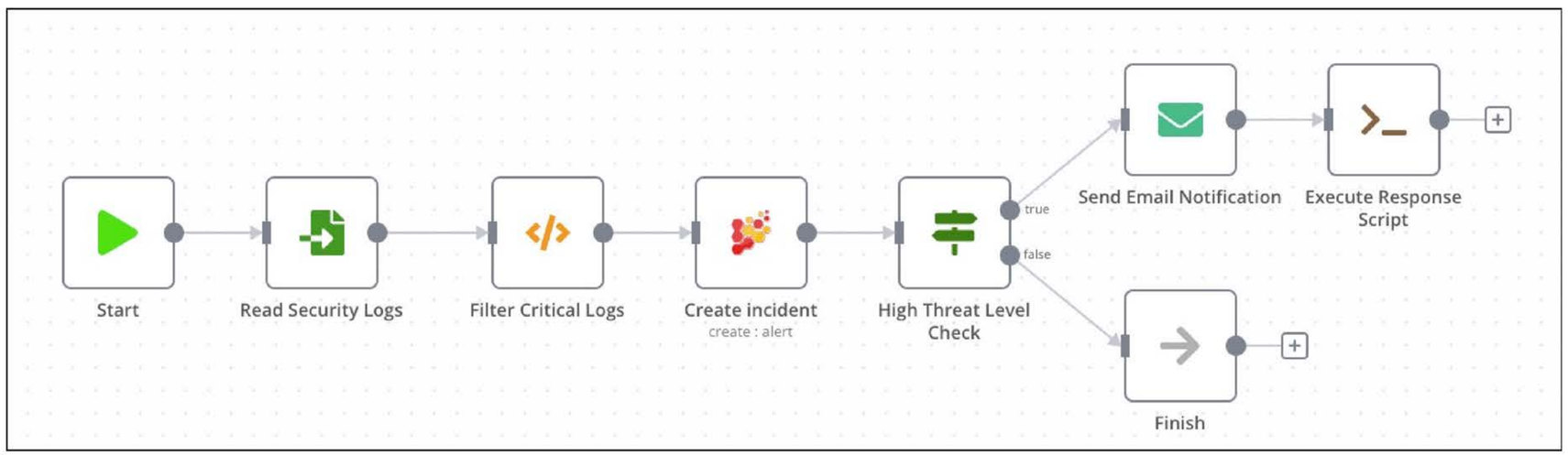
Post-implementation, the SOAR system requires constant monitoring and iterative development to stay relevant and effective. It is a dynamic framework, supporting the organization's growth by continuously automating new and more complex processes, ensuring that the security measures evolve in response to changing threats and organizational demands.

Creating Workflows

The Energy SOAR system's workflow process is designed using elements like business rules, actions, conditions, and system integrations. Users configure workflows in the system's editor, adding stages such as actions, decisions, and conditions. Workflows can be triggered manually, automatically by specific events, or at set times.

Each stage can interact with other systems (e.g., IT, security systems) to automate actions in response to threats. For instance, detecting a threat can activate workflows in systems like SIEM, IDS/IPS, and antivirus programs, enhancing process automation and efficiency during security incidents.

The system supports numerous pre-built integrations and allows for custom integrations using APIs. These capabilities streamline workflow creation, automate actions, and integrate systems effectively for security incident responses



SOAR System in Practice

Energy SOAR streamlines and expedites security incident management throughout its lifecycle within an organization.

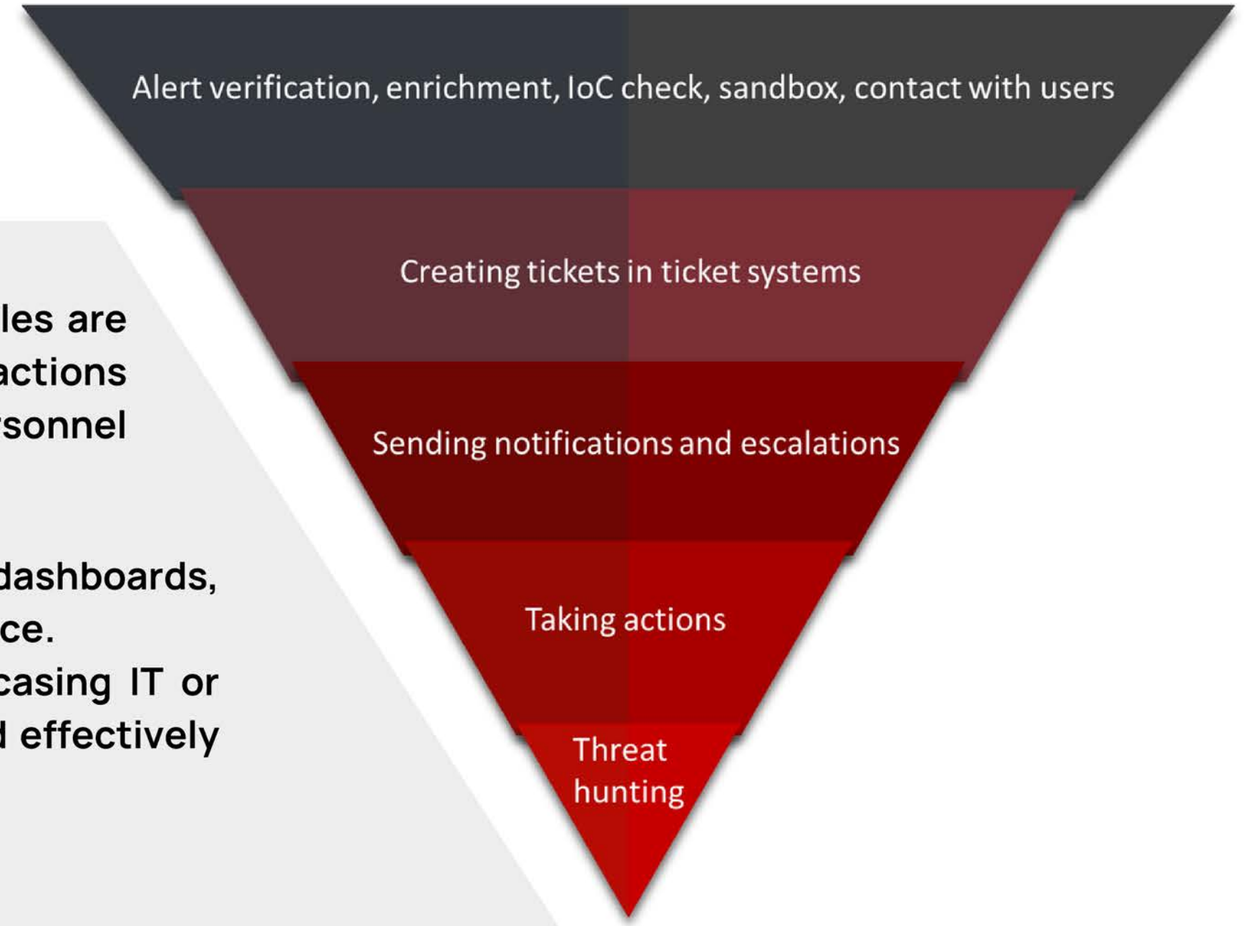
Let's explore the process from detection to resolution in detail.

Initially, SOAR integrates with various security platforms like SIEM, IDS, IPS, EDR, and email systems, extracting incident data. The workflow engine then automates a sequence of actions, typically manual, enhancing efficiency.

System analyzes the event attributes (observables) such as IP addresses, hostnames, usernames, or URLs.
It augments incidents with additional data, adding them to the case roster, where each is auto-tagged with severity and relevant labels. Operators, assigned either manually or automatically, receive specific tasks. Users have a clear task list, with all actions recorded in the history log.

For certain cases, where conditions like specific correlation rules are met, SOAR autonomously manages the response, performing actions such as IP blocking or network isolation, without IT personnel intervention.

**SOAR's intuitive graphical interface, equipped with preset dashboards, offers insights into task status, team workload, and SLA adherence.
It facilitates the generation of comprehensive reports, showcasing IT or SOC activities. This tool empowers organizations to swiftly and effectively tackle security threats, safeguarding data integrity and privacy.**



Use cases

Email analysis

During the security workflow, when a suspicious email is received, it's directed to the integrated SOAR system by an employee who flags it.

The SOAR system conducts an in-depth analysis of the email's content and structure through syntactic and semantic scrutiny to detect signs of phishing, such as dubious links or attachments. It references threat intelligence databases to compare the email against known threat patterns.

Upon detecting a potential threat, the SOAR system categorizes the incident as a possible phishing attempt. It can then automatically initiate protective measures such as blocking the sender or their IP address, and escalating the issue to a specialized security response team for further analysis.

Additionally, the SOAR system is equipped to notify relevant internal security teams or CSIRT promptly, enabling swift action against the threat. These teams can perform an extensive review of the incident to identify and neutralize any additional risks.

A critical advantage of the SOAR system is its capacity to locate and neutralize parallel phishing threats within the organization. Leveraging the data from the initial incident, it can search for and mitigate similar threats across the organization's email system, automatically relegating them to spam or deleting them, thus bolstering the organization's defenses.

Use cases

Automatic host or IP blocking is a crucial use case in the Energy SOAR system, especially for defending against malware attacks and network breaches. Here's a simplified overview of how the system handles this scenario:

Analysis and Confirmation

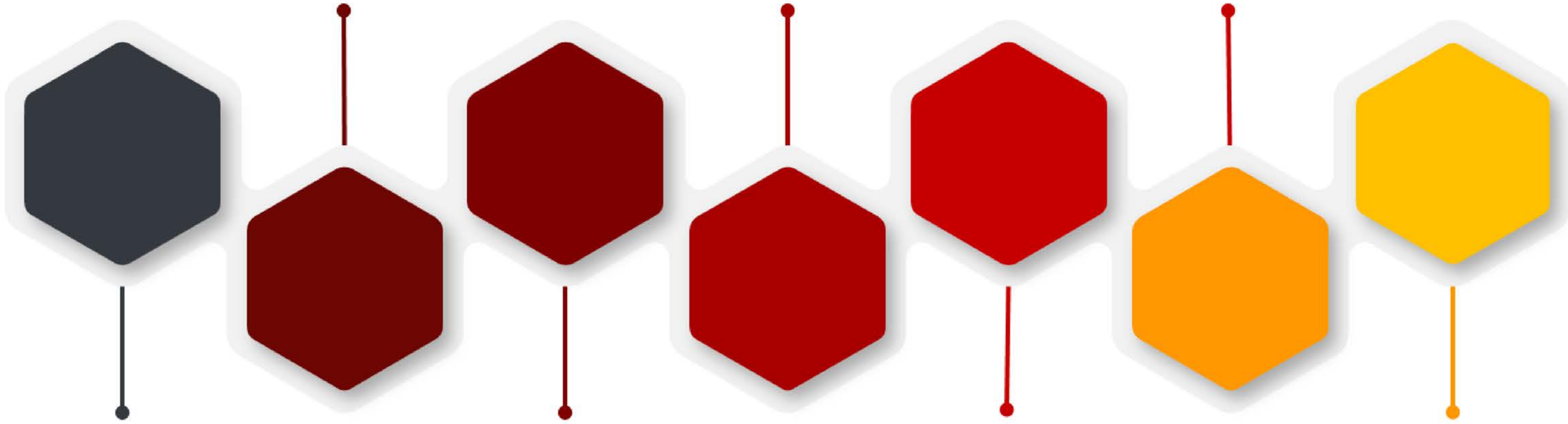
SOAR employs behavioral and trend analysis, along with external threat intelligence, to confirm whether the detected activity is a genuine threat.

AutomaticBlocking

SOAR automatically takes action to block the malicious IP address or host. This involves configuring firewalls or implementing network-level blocks.

Analysis and Response

Security team receives notification, conducts further analysis, take additional measures to address incident, such as tracking attack source or strengthening security measures.



Threat Detection

SOAR system, integrated with security tools like IDS/IPS and malware protection, identifies suspicious IP addresses or unusual network traffic

IncidentClassification

If the activity is deemed malicious, the incident is classified as a threat, and relevant information is stored for further analysis.

Notification

Notifications areautomaticallysent to the relevantindividualsorteams, providingdetailedinformationabout the incident and the actions taken..

Resolution and Reporting

Afterresolvingincident, informationisstored in SOAR for reporting and improvement. This data supports trend analysis and identifies security gaps

Use cases

Utilizing Threat Intelligence Trends

Energy SOAR system not only manages security incidents effectively but also examines Indicators of Compromise (IoC) from threat intelligence lists, leveraging current attack trends within the organization.

Example 1:

When detecting a malware campaign using a specific domain for HTTP communication, SOAR users can perform DNS log analysis to verify communication with that domain. If an endpoint is found to have established such communication, actions within the SOAR system, such as quarantining or isolating the host, can minimize the risk of further threat propagation.

Example 2:

In phishing campaigns using domains resembling popular companies (e.g., "mlcrosoft.com" instead of "microsoft.com"), the SOAR system analyzes logs for connections to suspicious domains. If connections are found, swift measures, such as blocking access or warning users, can be implemented to secure the organization against phishing threats.

Leveraging SOAR's capabilities in integrating with threat intelligence lists and analyzing attack trends, the Energy SOAR system enables organizations to promptly respond to potential threats. Serving as a centralized security management hub, it consolidates information on security incidents and events, facilitating effective monitoring and response to emerging threats.

Detecting Unauthorized Administrator Logins After Hours with SMS Verification

We present a case study of organization XYZ, which had a need to secure their system against unauthorized administrator logins outside of working hours. The goal was to implement a login verification mechanism through the use of an SMS message with a unique link that the administrator had to confirm within a specified timeframe; otherwise, the administrator account would be automatically locked.

Implementation process:

1 Detection of unauthorized login attempts:

The Energy SOAR system was configured to monitor system logs and events related to login activities. If an unauthorized login attempt by an administrator outside of working hours is detected, the system initiates the verification procedure.

2 Generation of SMS message:

The SOAR system automatically generates an SMS message containing a unique login confirmation link. Each login attempt is assigned a specific link with a defined validity period (e.g., 30 minutes).

3 Sending the SMS message:

The SOAR system sends the generated SMS message with the login confirmation link to the registered mobile device associated with the administrator's account.

4 Login confirmation:

The administrator receives the SMS message with the login confirmation link on their mobile device. To confirm the login, the administrator needs to click on the provided link.

5 Account lockdown in case of non-confirmation:

If the administrator fails to confirm the login within the defined timeframe, the SOAR system automatically locks the administrator account, minimizing the risk of unauthorized access and activities within the system

6 Actions after login confirmation:

Upon clicking the login confirmation link, the SOAR system receives confirmation from the administrator's end. If the confirmation is received within the specified timeframe (e.g., 30 minutes), the login is considered authorized.

ENERGY SOAR

Energy SOAR is a tool that does not force you to compromise or reduce requirements. On the contrary, it expands your capabilities and adds control in the most incredible areas.

To obtain a demo version of Energy SOAR, contact us:

logserver@bakotech.pl

www.bakotech.pl/vendors/energy-logserver

www.energysoar.com

bako tech®