LTS SECURE'S SOAR

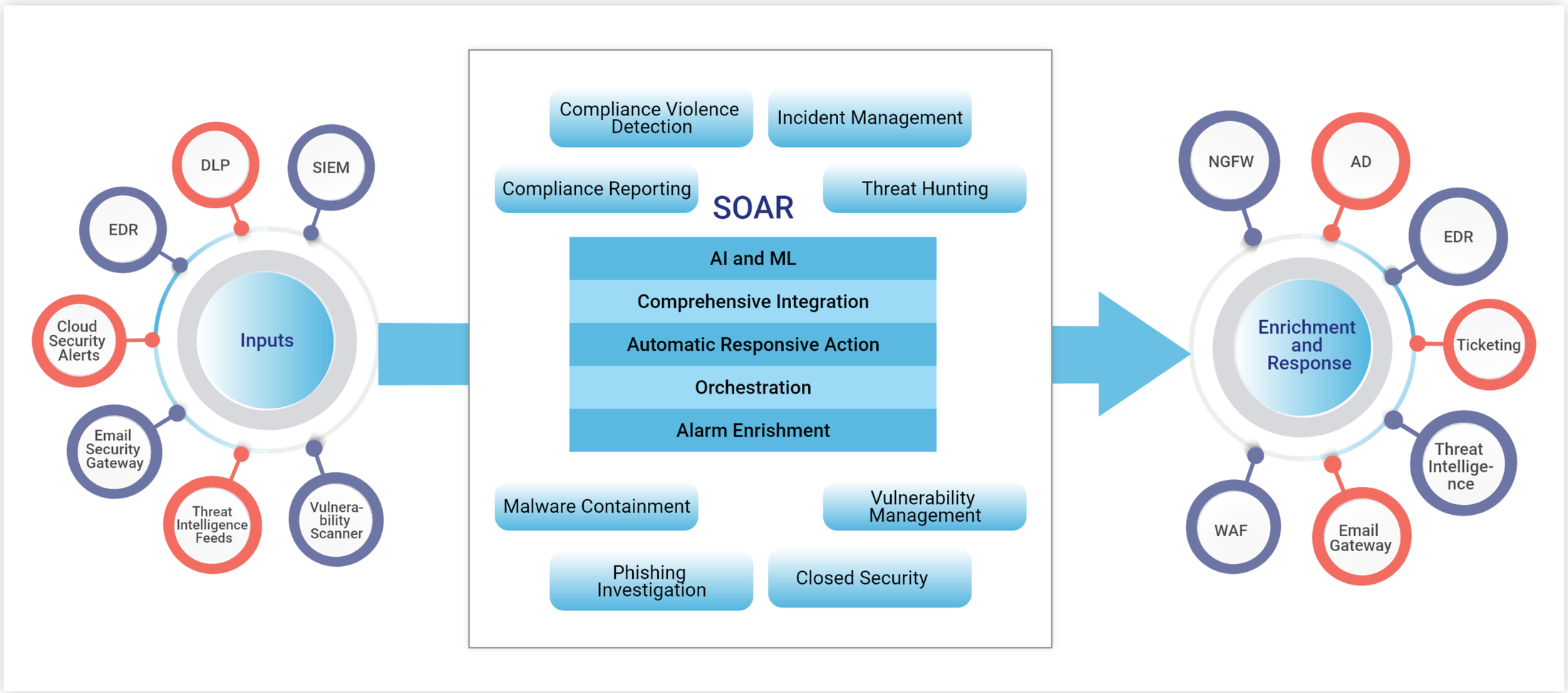
Effective Threat Detection and Remediation with **SOAR**

OVERVIEW

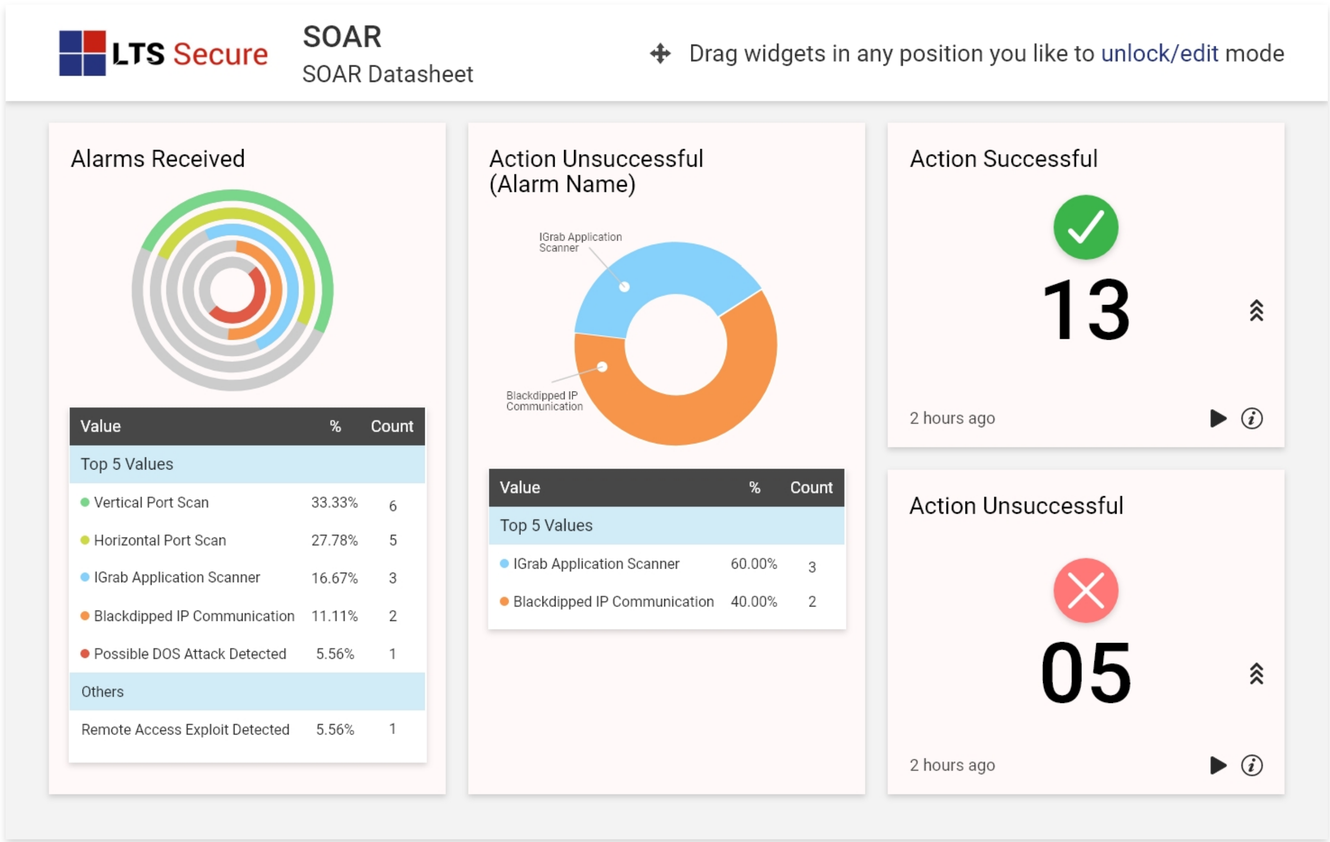
With threat actors constantly evolving their TTP's to outmanoeuvre the various security solutions being deployed by organizations, it has become more & more challenging for them to adopt to the growing number of advanced threats out there. This problem has caused them to turn to automated solutions like SOAR, to help them better identify & respond to advanced security threats.

LTS Secure SOAR solution is specifically designed to address this challenge faced by many organizations enabling them to collect threat data & alerts from multiple sources, identify & prioritize cybersecuirty risks and respond to low-level security threats automatically.

Our solution can help organization's SOC to integrate & augment their existing security solutions like SIEM, EDR, NGFW, etc., allowing them to deal with security threats more quickly & efficiently, while at the same time reducing their workload & making their Incident Response process more standardized.



Implement automation, process standardization and integration alongside. Existing security tools to accelerate incident response.
LTS Secure SOAR stack with inbuilt Artificial Intelligence ‘AI’ technology including Threat and Vulnerability Management, Incident Response and Security Operations Automation and Orchestration allows detection and prevention of frauds, data leaks and advanced internal and external attacks.



SECURITY ORCHESTRATION

Allows SOC teams to see the big picture by correlating alerts from various security solutions like SIEM, EDR, NGFW, etc. Allow Security operations to build a communicable network of coordinated complex workflows, technologies and methodologies with numerous integrations and APIs supported by SOAR

ALARM ENRICHMENT

Provides key essential information to make well informed decision to remediate security incidents. Identify predictable, repeatable business processes with less or no human interference, and automate workflows to create efficient, fast and high performance processes with reduced human error.

SECURITY AUTOMATION

Out-of-the-box playbooks help automate response to certain threat types without the need for human intervention.

AUTOMATIC RESPONSE

Taking automatic action’s on repetitive tasks, helps prioritize critical security threats & streamlines the security processes, allowing significant reduction in response time.

LTS SECURE'S SOAR DEPLOYMENT REQUIREMENTS (INCLUDING HARDWARE AS WELL AS SOFTWARE)

LTS Secure's SOAR has the following Hardware requirements for deployment:

LTS SIEM Requirements		
Recommended Hardware/Software		**Server Quantity**
Operating System	CentOS 7.5 minimal	1
Platform	VMware ESXi 5.5 and above/ Hyper-V	
Processor	4 Core VCPU	
Memory	12 GB	
Ethernet	1 GB X 2	
Hard Disk	300 GB Note: Assuming – 20 to 25 Alarms for 24 hrs and will store alarms for 6 months	
Installation Media	CD/DVD/USB	

- Require DNS Server to resolve other host names in the network
- Require host names to get access to server
- Static IP address to deploy SIEM Server
- Require a Netmask
- Require Gateway to route to other network

LTS Secure's SOAR has the following Software requirements:

- Python3.6 or higher
- Python3-pip
- Python code dependent packages

SUPPORTED ENVIRONMENTS

- Operating System
- VM's
- Database
- Networking Devices
- Security Solutions (NGFW, WAF, EPP, EDR, etc)
- Cloud

BENEFITS AFTER DEPLOYMENTS

- **Comprehensive Integration**

  Supporting multiple integrations and APIs, SOAR allows multiple security products to communicate and work synchronously, increasing flexibility of organizational infrastructure using languages like Python, APIs and Perl.

- **Faster Response Time**

  ML Engine of SOAR enables it to identify false positives & take appropriate response to low-risk security alerts without the need for any human intervention.

- **Reduce Damage From Attacks**

  Minimize the number of steps that actually require any sort of human intervention and help SOC teams investigate & respond quickly so they can begin the mitigation process sooner.

- **Operational Costs Being Reduced**

  With SOAR taking automated actions against tedious & time-consuming tasks, like responding to low-level alerts and dealing with false positives, operational costs are significantly reduced.

- **Dashboards & Reports**

  Allows SOC teams, CISO's & auditors to properly visualize & analyse relevant data, measure success & access potential business risks.

TO REQUEST A LIVE DEMO OR FOR MORE INFORMATION ON LTS SECURE SOAR, PLEASE GET IN TOUCH WITH US:

enquiry@ltssecure.com

www.ltssecure.com

About LTS Secure

LTS Secure is a global provider of Cyber security services with client spanning across industries. Offering security Suite to rationalize, prioritize & automate response to risks in your environment. LTS Secure provides comprehensive Cyber Security solutions with continuous monitoring at all layers of the IT stack including network packets, flows, OS activities, content, user behaviors and application transactions. Detect and Prevent Fraud, Data Leaks and Advanced Internal as well as External Attacks with advanced Security Orchestration, Automation and Response solutions.

LTS Secure