LTS Secure SOAR

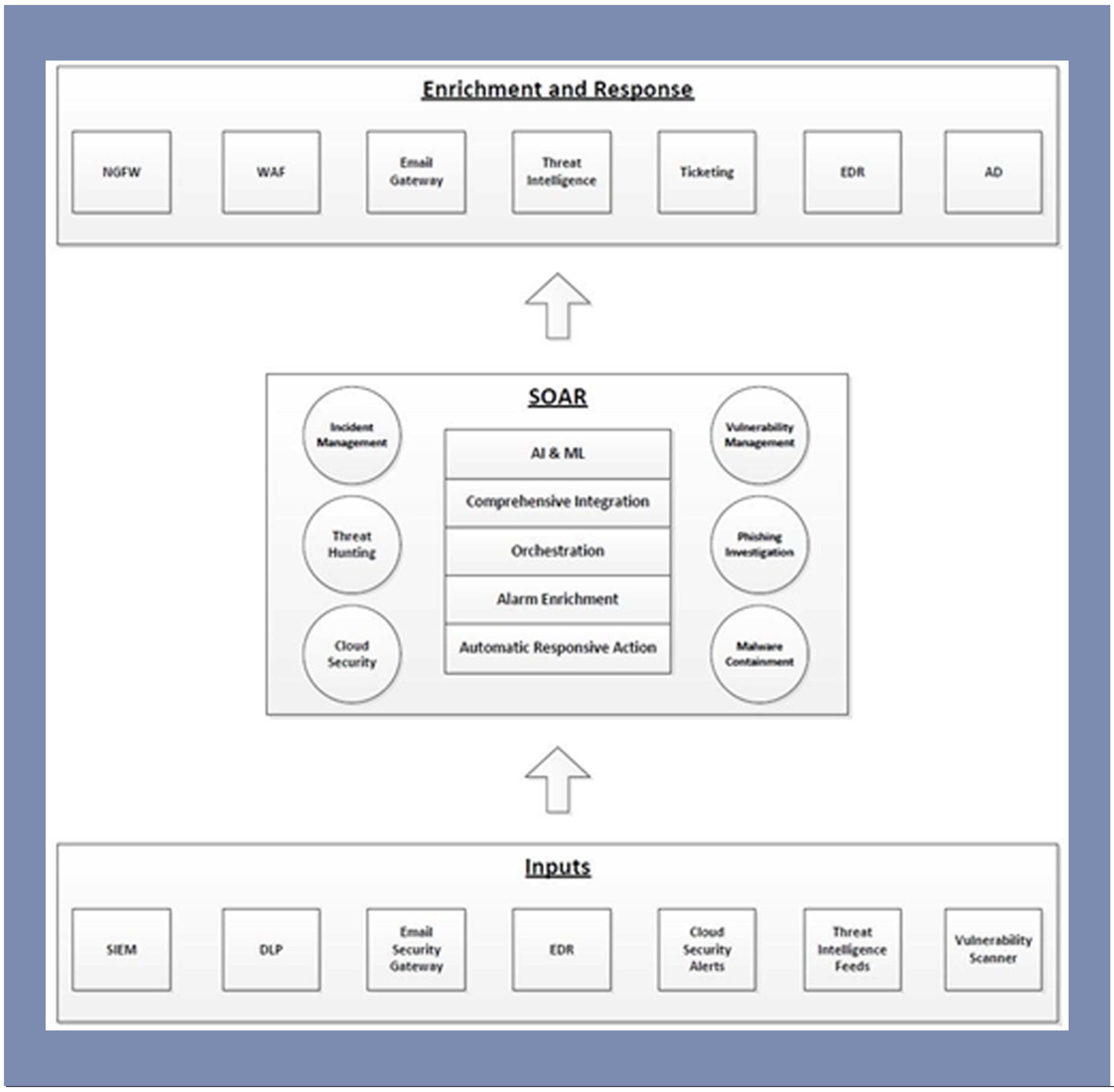
LTS Secure SOAR

With threat actors constantly evolving their TTP's to outmaneuver 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.

LTS Secure SOAR solution also helps organization 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.

LTS Secure SOAR Architecture



HIGHLIGHTS

- Ingest alerts for various security solutions and trigger automated triage, context enrichment & automatic response through playbooks.
- Manage assets, alerts, indicators & tasks from a single, easy-to-use console.
- Shorten security incident discovery time from hours to just a matter for seconds.
- End-to-End incident response helps overcome alert fatigue by automatically detecting & responding to known security threats with automated workflows.
- SOAR engine ensures that your analyst only focus on real threats by filtering out all false positive alerts.
- Automation, vulnerability feeds, correlation of incidents & threat intelligence ensure that repetitive tasks are eliminated.
- Automation templates help SOC teams save their valuable time & resources, thus improving the efficiency & effectiveness of their defined processes.

LTS Secure

Feature	Benefits
Security Orchestration	● Allows SOC teams to see the big picture by correlating alerts from various security solutions like SIEM, EDR, NGFW, etc.
Alarm Enrichment	● Provides key essential information to make well informed decision to remediate security incidents.
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.
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.
Case Management	● Helps centralize evidence gathering & incident management.
Case Metrics	● Get Complete audit trails & key incident response milestones for reporting.
Dashboards & Reports	● Allows SOC teams, CISO's & auditors to properly visualize & analyse relevant data, measure success & access potential business risks.