LTS Secure

ADAPTIVE SOC PLATFORM FOR CYBERSECURITY

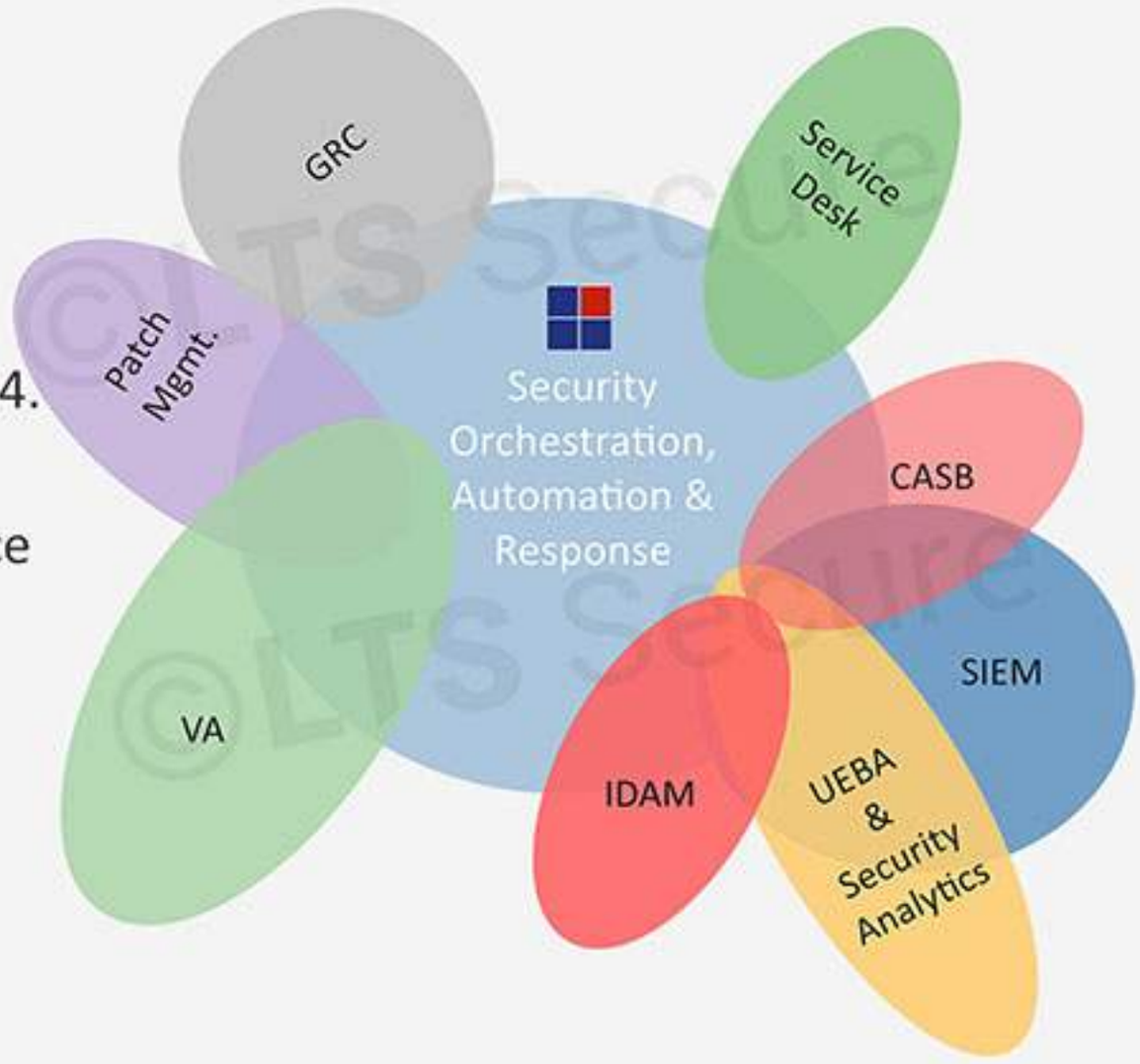
Rationalize, Prioritize, Automate Risk & Responses in Context

LTS Secure

Built for security orchestration and automation, that helps to create business orchestrate cyber environments that are truly integrated.

At a Glance

- LTS Secure incubated in 2012.
- First version launched the in early 2014.
- Over 20 years of cumulative experience in security operations.
- LTS has successfully established SOC platforms globally in USA, UK, Dubai, Saudi Arabia, and India.



LTS Secure is an Integrated Security Platform (SIEM + UEBA + CASB + IDM) that enables continuous monitoring & detection of Threats, Vulnerabilities and Risk of IT Network, Applications and by Users in a single pane based on Security Orchestration, Automation and Response.

LTS Secure platform was developed to deliver scalable, innovative & flexible security solution to the organization struggling with security monitoring, access governance and identity management. LTS offers a broad array of product and features aimed at helping organization to address both simple and complex activities. With our intelligence driven SOC, you can perform security operations, reporting analysis, and management capabilities to support operational security infrastructure.

By implementing LTS SOAR stack you can improve the efficiency of your security operations through a series of aligned capabilities and processes. It begins with broad and deep visibility across your IT environment and ends with rapid mitigation and recovery from a security incident.

Product Overview

SIEM

LTS SIEM technology is an extremely useful tool to safeguard all size of business and IT systems, Quickly detecting and identifying security events is just one of the many features that makes SIEM, an excellent tool for businesses and IT departments.

Key Features

- Assets Mgmt and Availability Monitoring
- Vulnerability Assessment
- Real Time Threat Analytics
- Advance Malware attacks detection
- HIDS/NIDS/FIM
- IT Risk Gap Analysis
- IT Compliance Reporting

LTS SIEM Technology Integrates

- Log management, threat analytics, & compliance reporting.
- Real-time monitoring and incident management for security-related events from networks security devices, systems, & applications.

Use Cases of LTS SIEM Technology

- Advanced threat detection
- Basic security monitoring
- Investigation and incident response

IDM

As the shifting of users, application, and management to the cloud, and acceleration of the IT innovation has changed IDM landscape, so does the Next-Gen protection. With LTS Secure advance authentication and authorization process will reduce runtime access risk and improve user logging experience.

LTS Identity Management Integrates

- Risk scoring, computation and analysis
- Identity correlation and profiling
- Behavioral and data analysis
- Data presentation and visualization

Use Cases of LTS IDM Technology

- Governance regulatory framework - compliance and review procedures.
- Management Level administration of identities, rights, and authorization tokens.
- Execution Level information review as well as synchronization at runtime.

UEBA

UEBA technologies are maturing becoming more robust and valuable, seeing broader adoption with forward leaning organization. LTS UEBA utilizes analytics to build the standard profile and behavior of the user and entities across time and peer group horizons.

Key Features

- O365 Threat and Risk Visibility
- Cloud Apps and Infra Threats and Risk Visibility
- User Risk Scoring
- User Behavior Security Risks & exploits detection
- Privilege Activities Monitoring
- Alarms Prioritization

LTS UEBA technology Integrates

- Behaviors from both users and other entities and focus on a multiple use cases.
- Ingest event data from user and entity activities.
- Detection of anomalies via advanced analytics capabilities.

Use Cases of LTS UEBA

- HIgh privileged access visibility & monitoring
- Anomalous behaviour detection
- Hybrid Infrastructure visibility.

Security Analytics

Our LTS Security Analytics team constantly monitoring and focusing on the report data to produce proactive security measures. No business can predict the future, especially where security threats are concerned, but by deploying security analytics tools that are able to analyze security events it is possible to detect a threat before it has a chance to impact your infrastructure and bottom line.

Key Features

- Log Management for Forensic Analysis
- Network Behavior Analytics
- Device Activities Baselining and Machine Learning
- Security Events Analytics
- Security Controls Monitoring

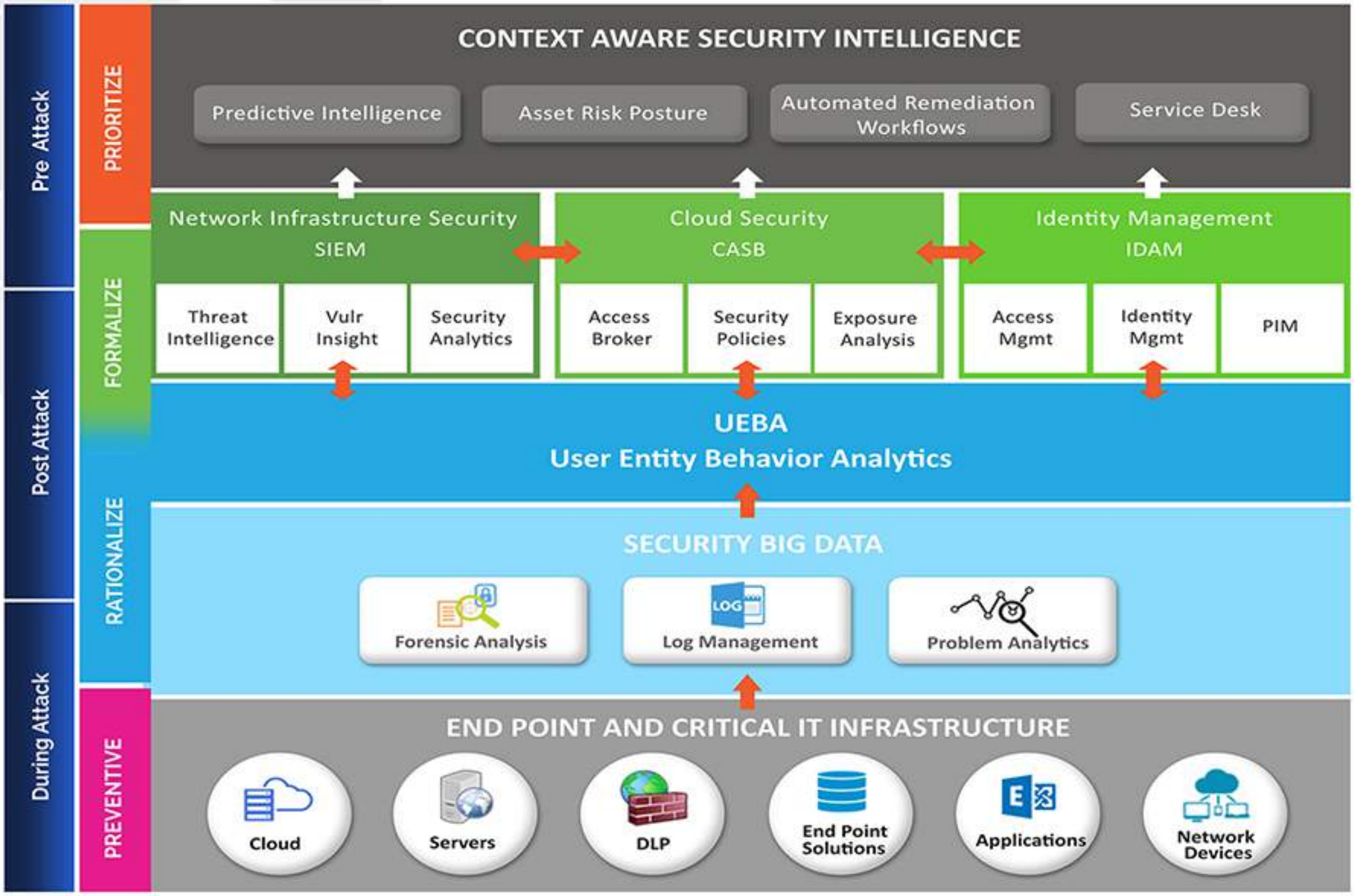
LTS Security Analytics Model

With a single, agentless solution, you get scalable security that grows with your digital business. Instead of deploying hundreds of sensors throughout your network, the network infrastructure itself becomes the sensor, and this leaves threat actors with nowhere to hide. Three core approaches for catching threats at the earliest point.

Behavioral Modeling | Multilayer Machine Learning | Global Threat Intelligence

SOAR Stack & Integrated Modules

LTS Secure automates and orchestrates the incident response, collecting alert and event data from virtually any security platform with minimal effort. It automatically centralizes and responds to alerts using automated workflows to reduce mean time to detect and respond.



SOAR STACK Benefits

- Comprehensive Security visibility of network, users and application from single dashboard.
- Rationalize cross-vendor security controls in asset and business contexts.
- Address the full security operations management (SOM) life cycle.
- Prioritize security operations activities.
- Automate and enforce remediation and response workflow