LeoTechnoSoft

Intelligence Driven SOC for Orbis Financial

Overcoming compliance burdens while maximizing 24/7 security

From investment management to custodial holdings,Orbis Financial is directly responsible for the safety of assets and securities worth hundreds of millions of dollars since 2005. They utilize and employ innovative technology and "zero-conflict" practices for a variety of India-based and foreign concerns wishing to grow and safeguard their investments in India. Orbis is a registered member of the Securities and Exchange Board of India (SEBI). Though their primary headquarters is located in Gurgaon, Haryana India, they also maintain a significant European presence in Switzerland. Orbis Financial earned multiple ISO certifications that cover business practices and technological standards. These include ISO 9001:2008, ISO 27001:2005, ISO/IEC 27001:2013 and ISO 22301:2012 . They are one of the few custodial financial management organizations recognized with these certifications.

The Challenge

The continuous pressure on financial organizations like Orbis Financial to **effectively secure its network extends** beyond preventing intrusion from outside attacks. There are as many internal threats, exponential ATPs, identity thefts, frauds and other complex means to compromise both corporate and client information and financial assets. To that end, organizations like Orbis are subject to rigorous oversight by regulatory agencies to ensure compliance with best security practices. In fact, Orbis is ***subject to more than 36 audits per year.*** Each of these audits are comprehensive which strains the bandwidth of the personnel responsible for maintaining the requirements. A considerable part of the issue was the disparate silos of security information required to be analyzed in advance of these audits.

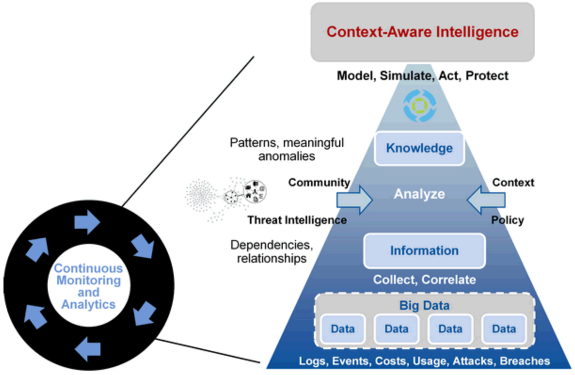
According to **Mani Kant Singh, Orbis' Head – IT & CISO**, "*We had to maintain so many logs, which get generated from many devices; store them, back them up and restore them for the audit requirement. It was not only cumbersome, but deflected focus away from our core business.*"

Additionally, in accordance with its fiduciary commitment to clients and shareholders, Orbis was committed to providing elite security and risk mitigation services. Towards that goal, Orbis also needed to minimize the CapEx impact and expenses of a lingering phased deployment that traditional security solutions often incur.

LTS Secure’s Intelligence Driven SOC

Intelligence Driven SOC with Integrated Security Solutions to move enterprise from "incident response" to "continuous response” for Advance Threat. Intelligence Driven SOC includes

- SIEM (Security Info & Event Mgmt)
- Log Management
- Identity Management
- Access Management
- Single Sign On
- Pattern Recognition and Behavioral
- Analytics
- Preveliage Identity Management
- Advance Threats Analytics


Context-Aware Intelligence
Model, Simulate, Act, Protect
Patterns, meaningful anomalies
Knowledge
Community
Analyze
Context
Threat Intelligence
Policy
Dependencies, relationships
Information
Collect, Correlate
Big Data
Data
Data
Data
Data
Logs, Events, Costs, Usage, Attacks, Breaches
Continuous Monitoring and Analytics

The Solution

After analyzing several alternatives, Orbis Financial chose LTS Secure's Intelligence Driven Security Operation Center SIEM i.e CloudAccess to serve as the cornerstone of its security management initiative. Apart from the enterprise-comparative feature set, Orbis was intrigued by LTS Secure's unique hybrid SOC approach that reduced their capital expenditures towards the project to virtually nil. The data remains safely behind existing secure firewalls and on-premise, and local sensors collect all the logs and send them encrypted (via VPN) to the powerful,cloud-based correlation engine. LTS Secure's Intelligence Driven SOC SIEM was able to analyze all the logs in real time and provide the necessary visibility to find usage anomalies and other potential alerts requiring actionable intelligence.

LTS Secure's Intelligence Driven SOC SIEM provided Orbis enhanced capabilities to better manage event, application, vulnerability and machine data in order to identify and prevent compliance policy violations found on the network or host based systems. This meant a new, improved visibility and capability to deal with various threats, frauds and apply behavior analysis; all without adding any hardware or capital expenses. This also created a new policy flexibility which gave analysts complete visibility into the granular reporting necessary to satisfy all the compliance audits. In fact, since LTS Secure's Intelligence Driven SOC has been in service, Orbis has *not failed a single audit, nor incurred any compliance fines*
.
Orbis used LTS Secure's Intelligence Driven SOC SIEM centralized dashboard to "make the right decisions at the appropriate time" and augmented its staff with additional security-as-a-service analysts (maintained as a value add service from LTS Secure) to keep up with the 24/7/365 monitoring demand.

The Result

Orbis gives LTS Secure's Intelligence Driven SOC SIEM high marks across the board. Not only has Orbis been able to continuously meet the requirements of the multiple compliance agencies, but they have also noted definitive improvements in 5 mission critical areas:

Operational:
Increased visibility has obviously produced comprehensive ability to detect advanced threats, apply 24/7/365 monitoringacross the enterprise (including privileged accounts), and provide actionable intelligence, vulnerability scans and risk routing,but more specifically:

- Achieved faster log data analysis and forensic investigation when incidents arose
- Achieved unprecedented visibility into everything happening on the network, including insider activityand external cyber threats.
- Accelerated response to security threats from days to minutes
- Significantly reduced the number of false positives and redundant events.

Financial:

In terms of the "bottom line," Orbis was not required to spend any capital expenditure budget and was able to scale to the existing deployment in less than 90 days.

- Orbis reduced associated security costs by 35%.
- Orbis saved an additional $12,000 USD because no hardware or licenses were required.
- OPEX model allowed for strategic modular deployment which promoted budget-friendly right-sizing: paying only for the IT services it needs, *when* it needs it.

Productivity:

- In all, IT regained more than 30% of its time back which has been reassigned to core business concerns and revenue generating activities
- Gained ability to handle massive amount of security events with a small team
- Expanded virtual headcount through security-as-a-service analyst augmentation at no additional cost.
- Reduced auditing and compliance costs through continuous monitoring
- Reduced the time required to ensure compliance

Customer Service:

LTS Secure’s Intelligence Driven SOC facilitated maximum uptime of the enterprise including secure access to key applications. This translated into a **50% improvement** in customer service based on reduced service calls and end-user survey responses.

Improved market share:

- Since the deployment of LTS Secure’s Intelligence Driven SOC SIEM, Orbis' market share as a financial custodian increased by 15%. This is directly attributed to the smoother operation of applications services, the nimbleness to move quicker on customer issues (because IT is not otherwise occupied), and word of mouth that Orbis is a secure and trustworthy

ABOUT LTS SECURE’S Intelligence Driven SOC:

LTS Secure’s Intelligence Driven SOC is an integrated Stack of Security Solutions - Security Incident and Event Management (SIEM), Identity and Access Management (IDM), Privilege Identity Management (PIM) and Cloud Access Security Broker (CASB), which is built on Security Big Data. LTS Secure’s Intelligence Driven SOC is the only SOC, which can correlate Device Events, Identity, Access and Context together to predict advance risks and threats across all IT layers. LTS Secure’s Intelligence Driven SOC has inbuilt capability of Security Analytics, which collects events from all integrated security solutions to conduct analytics on User Behaviors, activities, security events & threats and Identities.