DefenseStorm

DELIVERING CUSTOMER SUCCESS FOR LIVE OAK BANK

Streamlined data aggregation and smart analytics shift security response from reactive to proactive

CLIENT CHALLENGES

With multiple sites and staff traveling around the United States, Live Oak Bank has data centers hosting many systems, technologies and applications that support their small business lending and deposit platforms. Like many financial institutions, Live Oak was faced with a need to have visibility into all areas of the bank's network in order to support companywide security and operational activities. With multiple point solutions, Live Oak needed a way to consolidate the view into these point systems—while still allowing them to operate as intended. The DefenseStorm solution allowed Live Oak to aggregate all logs and event data together into one analysis engine that enabled advanced searching and incident management. The objective was to increase visibility of security threats and reduce reaction time to high-risk, high-threat activities, without large-scale increases in headcount.

SOLUTION SUMMARY

DefenseStorm's collaborative, comprehensive solution for Live Oak Bank crossed a variety of key service areas, including security, intelligence, incident response and compliance. In the area of security, DefenseStorm helped Live Oak to better leverage the benefits of the security systems the bank already had in place by creating a single, agnostic collector of all security event data that allowed IT personnel to consolidate both operations and response. By deepening the bank's ability to search and interpret large, disparate sets of event data, DefenseStorm enabled Live Oak to streamline their analysis of the total environment.

Live Oak Bank

NEIL UNDERWOOD
PRESIDENT, LIVE OAK BANK

"The value of the DefenseStorm solution to our operations is incalculable. Within a few months, the system transformed our security response from reactive to proactive, saving us tens of thousands in hard expenditures instantly—and averting fraud that could have had massive systemic and enterprise impact, with losses in the millions."

DefenseStorm

With regard to intelligence, DefenseStorm's solution for Live Oak helped the company to better utilize their IP reputation engines and reports across the entire organization, regardless of location—including the ability to proactively automate search and detect activities based on industry analysis and reports. Executive dashboards also made it easy to capture search logic and present it graphically for easier interpretation. With regard to compliance, the DefenseStorm solution made possible actionable tracking of company wide incident management for quick and efficient reporting to state and federal regulatory agencies.

THE OVERALL RESULT:

Live Oak Bank was able to shift their security response from reactive to proactive.

SPECIFIC RESULTS

Since the deployment of the DefenseStorm solution, Live Oak Bank's scalability and data collection has improved by 100%. The company's legacy SIEM solutions were not scalable, and security analysis degraded with increased event traffic. The DefenseStorm platform is a Big Data analytics engine that is built to work efficiently and effectively with large data sets; it accepts all types of data, scales quickly, and improves with increased traffic. The result is proactive threat detection that improves with larger data sets and solid intelligence. DefenseStorm's SaaS platform has also helped Live Oak Bank to optimize big data searching. Overall, the company has seen 50–60% improvement in their internal process workflow and incident discovery. This is a direct result of the increased performance, data analysis and research capabilities that this platform brings.

Live Oak Bank's security research has increased manyfold with advanced single-click features included in the DefenseStorm platform. With older tools, the average time spent working on any given event is 15–60 minutes. With DefenseStorm platform, staff members are able to determine the scope of an event in 1–5 minutes, and can make a determination as to converting the event into a formal incident for remediation.

Live Oak Bank

DATA SOURCES

INFRASTRUCTURE LOGS
Router, firewall, IPS

SERVER LOGS
VMware, Windows, Linux, AIX

APPLICATION LOGS
ERP, web, e-commerce and email

BUSINESS IMPACT

50–60%
improvement in incident discovery

Up to 60x
faster security event scoping

$30–$60k
initial IT annual cost savings

Up to 4x
faster proactive threat analysis

95% decrease
in incident response time

DefenseStorm

DefenseStorm has also enabled Live Oak Bank to segment security research, proactively examining event data to decide where threats may exist. This includes reviewing geographic sources to focus on high-risk locations, examining threat types by severity, category, or protocol, and narrowing location-based searching for certain groups of locations within the company. With older tools, this process would take 1–3 hours and the focus of a dedicated team. With DefenseStorm, it is a simple lateral or horizontal search string that only takes minutes.

When it came to search string intelligence, the company's older SIEM tools made custom searching quite costly, often requiring a secondary appliance to run a search string semi-offline. Searches were not always in real time, and cost of the secondary system can vary from $30–60K, according to solution. The DefenseStorm platform is optimized for searching in real time, as soon as data is received. Cloud infrastructure eliminates the need for secondary systems, as well as the cost of running searches on systems that can't handle high volumes.

In addition, Live Oak Bank's incident response speed has increased exponentially. Prior to deploying the DefenseStorm solution, the company did not have a tool to coordinate a formal incident response—all processes were manual and very time consuming. A typical action could be from 1–3 hours, if all data components were available. Today, the company has a collaboration tool that allows for streamlined queuing for analysis in a matter of minutes.

And finally, prior to implementing the DefenseStorm solution, reporting for Governance was a manual process. Monthly/Quarterly/Annual reporting on cyber-security was an arduous process. With the DefenseStorm solution, the reporting is automatic and can be generated on demand.

LIVE OAK BANK

ABOUT LIVE OAK BANK

Live Oak Bank was founded in 2008 with a singular goal: to provide business loans to independent businesspersons in niche industries. Today, Live Oak is one of the largest originators of small business loans, with one of the strongest loan portfolios in the country. The company has extensive experience lending to selected niche small businesses as a preferred Small Business Association (SBA) lender.

DefenseStorm is a Security Data Platform that watches everything on your network and matches it to your policies, providing cybersecurity management that is safe, compliant and cost effective. Built from the ground up in the cloud, DefenseStorm unifies detection, investigation, reporting, and compliance into a single place to manage cybersecurity data. Formed by bankers and technology experts, DefenseStorm aggregates event data across all cybersecurity tools and links policies to real-time alerts, so that financial institutions can prove to regulators they are both secure and compliant with evolving FFIEC cybersecurity requirements. For more information please visit www.DefenseStorm.com.