CASE STUDY

OAKWOOD BANK

OAKWOOD BANK
FINANCIAL SERVICES

CHALLENGES

- PHISHING SITES
- COMPLIANCE
- DARK WEB INVESTIGATIONS
- MERGER AND ACQUISITION (M&A) RISK

SOLUTION

DARK WEB MONITORING & INVESTIGATIONS

> Our first demonstration of Searchlight Cyber was jaw dropping, we were blown away by the robustness of the platform and its features, and could immediately see the value that dark web intelligence would add to our cybersecurity toolset.

EDWARD FRANCO
Chief Technology Officer, Oakwood Bank

PRIORITIZING PROACTIVE SECURITY

Oakwood Bank has put cybersecurity front and center throughout its journey of company growth. Operating since 1900, and once known as the smallest bank in America, Oakwood Bank has rapidly grown its customer base in recent years through a combination of organic growth and acquisition. Its infrastructure has had to keep pace and its technology department has put a heavy emphasis on cybersecurity throughout. The bank wanted a solution that would enable it to monitor the dark web for threats against its infrastructure and customers and the team were immediately impressed by the data and features of Searchlight Cyber.

Edward Franco, Chief Technology Officer at Oakwood Bank explained: "Our first demonstration of Searchlight Cyber was jaw dropping, we were blown away by the robustness of the platform and its features, and could immediately see the value that dark web intelligence would add to our cybersecurity toolset. Cybersecurity is always top of mind for us, it's part of our culture. We are really big on cybersecurity training of our staff and ensuring we have all the right tooling in place to protect our organization and the data we hold."

MONITORING AND INVESTIGATING THREATS ON THE DARK WEB

Oakwood Bank uses Searchlight to proactively monitor the dark web for data relating to both the organization and its customer base to identify security breaches as soon as possible. For example, the bank has used Searchlight to identify employee credentials on the dark web, which had been captured in the data breach of third party sites where employees had used their work email addresses. This information has informed security awareness training within the business.

Searchlight's dark web investigation capabilities also allowed the bank to investigate an incident where they believed the debit card details of a customer had been leaked, which they successfully identified based on the Bank Identification Number (BIN) found on a dark web site. Oakwood Bank has found Searchlight's Stealth Browser feature especially valuable for conducting these types of investigations, as this temporary virtual machine for investigating dark web sites allows the team to visit the dark web without putting its infrastructure at risk.

SEARCHLIGHT. CYBER

"Visiting the dark web is dangerous. Before we used Searchlight, conducting an investigation on the dark web was a complicated process that involved the use of an isolated computer off the network," **explained Franco**. "Searchlight's Stealth Browser allows us to immediately go into the dark web and find what we are looking for, while providing us with the assurance that our infrastructure is not at risk of being compromised by dark web threat actors."

Franco shared that the ability to get first-hand access to dark web data was one of the biggest advantages of the Searchlight platform, as it opens up new opportunities for threat research and improving organization security. These capabilities also impressed Oakwood Bank's auditors by demonstrating that it goes above and beyond in the protection of its customers.

"All organizations should have security tools that help them monitor internally but Searchlight provides us with visibility a lot of companies don't have," **said Franco**. "The ability to see what is happening globally on the dark web gives us additional knowledge that allows us to be more proactive in protecting our customers, which was recognised by our auditors. One of the key differentiators in using Searchlight is that we can access this data ourselves within the platform, without being reliant on external analysts to assess what they think is important."

AUTOMATED IDENTIFICATION OF PHISHING SITES

One of the main benefits Oakwood Bank has experienced from using Searchlight's dark web monitoring platform is the automated identification of phishing sites - fake websites set up by hackers to trick unsuspected customers into inputting their sensitive information. The company had previously been manually searching for malicious sites but this was a labor-intensive exercise and inevitably some sites fell through the cracks.

> "Searchlight has saved us a lot of time and resources - approximately **32-40 hours a month** that were previously spent on research and attempting to discover new potential phishing sites. Searchlight continuously scans for phishing sites, which helps us identify threats quicker and also allows our team to dedicate more time to remediation.

This capability became especially critical when Oakwood Bank acquired another financial institution, which meant that it had taken on responsibility for another domain that could potentially be abused.

"We were monitoring for phishing sites before but it was tough," **said Franco**. "Searchlight has automated what was an incredibly manual task, identifying more than 70 sites that we were either able to take immediate action against or can actively monitor for any indication that they are malicious. Searchlight's capabilities have allowed us to take down malicious sites before they can cause harm to our customers and helped us maintain our security through an acquisition.

"In the process, Searchlight has saved us a lot of time and resources - approximately 32-40 hours a month that were previously spent on research and attempting to discover new potential phishing sites. Searchlight continuously scans for phishing sites, which helps us identify threats quicker and also allows our team to dedicate more time to remediation."