SECDO | CASE STUDY

VALLEY NATIONAL BANK AUTOMATICALLY INVESTIGATES ALERTS WITH SECDO

BACKGROUND

Founded in 1927, Valley National Bancorp (NYSE:VLY) is a regional bank-holding company headquartered in Wayne, New Jersey with over $23 billion in assets. Its principal subsidiary, Valley National Bank (VNB), operates more than 200 branch locations serving 30 counties throughout northern and central New Jersey, Manhattan, Brooklyn, Queens, Long Island and Florida.

Cyber criminals regard banks as lucrative targets. Banks process vast volumes of personal identifying information — addresses, phone numbers, email addresses, social security numbers — all of which can command hefty prices from scammers who steal or encrypt data for ransom and other nefarious purposes.

Naturally, much banking information is financial and confidential. In its digital form, vital information can be removed from compromised bank accounts and sent in milliseconds to offshore accounts. The Financial Services Information Sharing and Analysis Center, a non-profit threat intelligence-sharing group for the financial sector, estimates that banks deal with 400 serious threats each and every day.

Michael Livni, CISO

Valley National Bank

FOUNDED *1927*

EMPLOYEES *3500*

INDUSTRY *Banking*

BRANCHES *200+*
in New Jersey, New York and Florida

RESULT WITH SECDO
Significant boost to endpoint security. Processing of all alerts in real-time. Quick and effective response without business interruption.

CHALLENGES

VNB was facing several daunting challenges to its cyber security regime:

> *“We face the same challenges as everybody else: time to market, movement to the cloud and many different ways of consuming data. With mobility in the picture and with borderless perimeters, we now need to trust our endpoints.”*

1. ***It was difficult to view what was happening on the endpoints.*** Time-to-detect was measured in days, weeks or months – far too long for effective response, leaving gaping security holes.
2. ***The daily volume of correlated endpoint events exceeded 1500 and was tying up resources.*** To investigate each potentially serious incident, the security team had to sift through many disparate logs from intrusion prevention/detection systems, firewalls and other security systems. The process for a single incident could engage a senior analyst for days.
3. ***Applying remediation on endpoints would often take end users and key systems out of commission***, interrupting productivity and hampering customer service.

SOLUTION

At the cutting edge of cyber security, Livni was searching for an automatic incident response solution that would handle events automatically and accurately. After conducting an exhausting search for a solution to its challenges, Livni decided to try out Secdo.

Livni challenged Secdo to perform a quick proof of concept. The results looked promising. After three weeks of testing with legacy systems, VNB was able to deploy Secdo in only one day to 2500 endpoints. Right away, Secdo agents began collecting activity from the endpoints and correlating them on the Secdo server hosted on VNB's premises.

With a bit of training on the browser-based management console, VNB's security team was able to use the Secdo product effectively.

> *“Automation is always preferable over hiring more staff. Repeatable automated processes are always more accurate. Secdo's Preemptive Incident Response concept looked like it might be the breakthrough we were seeking.”*

RESULTS

Secdo continuously collects all activities, events and behaviors from each endpoint and stores them on a secure server in anticipation of events. Providing unmatched endpoint visibility, Secdo enables security teams and IT personnel to observe the entire gamut of endpoint activity in context from now well into the past.

“Suddenly, we were able to find errors on the part of administrators that would never have been found with any other system,” Livni declared.

Secdo brings time-to-detect close to real time, helping VNB correlate real events as they occur.

“With reliance on a security incident event manager (SIEM) alone, we would get 1500 correlated events a day,” explained Livni. *“To deal with them meant endless sifting through logs from Intrusion Prevention Systems, firewalls, and other systems. With Secdo we were able to bring the volume down to 60 a day with only two actual incidents, entirely manageable by our staff.”*

Remediation on endpoints is another strongpoint of Secdo. Instead of having to take infected endpoints off-line for treatment – frequently involving wiping and re-imaging – Secdo's advanced suite of remediation tools enables security and IT people to remotely identify and freeze individual process in endpoint memory without disturbing the work of the end-user or application.

“Secdo gives us the ability to freeze any process we want – whether on a workstation, server or IoT device – in real time. This helps us remediate any issues immediately,” Livni noted. *“This benefits us by not taking a key person out of commission for a day or two or a key system out of commission while we remediate.”*

> *“With Secdo, we are the masters of our own destiny. The team still does a fair amount of investigation and incident response, but now that Secdo has streamlined that process, we're able to get more involved in business initiatives and innovation where we weren't able to before without growing the team by two-fold.”*