CYGILANT®
SECURITY AS A SERVICE

CASE STUDY

Midwestern Credit Union Chooses SOCVue to Gain Peace of Mind with Proactive Security Monitoring and Enhanced Security Event Data Analytics

60 State Street,
Boston, MA 02109
Tel: +1.617.337.4880
Fax: +1.617.337.4830

For more information or to request a demo, visit
www.cygilant.com

PLEASE NOTE:

This Cygilant Case Study is based on a real SOCVue customer. All names and personally identifiable information have been removed to maintain their safety and security.

Challenge

A Midwestern credit union with assets over 2 billion and a 190,000+ member base needed a robust IT security service that offered better ease of use, enhanced security data intelligence, and the ability to keep up with the company's growing cybersecurity needs, specifically when it came to its log management and SIEM analytics.

Solution

The Midwestern credit union chose Cygilant's hybrid security-as-a-service approach because it offered a one-stop shop that provided a better user interface that was intuitive for data analytics as well as enhanced security monitoring that helped to remove the noise of false positives.

Results

The Midwestern credit union now has enhanced network security monitoring that allows it to filter down thousands of events to a single snapshot view and analyze event data from across all of its critical IT assets so it can quickly determine what really needs attention.

> ***"Since the SOCVue Security Monitoring service is being managed by Cygilant's highly trained SOC team, it provides us with a great deal of comfort knowing we have extra eyes and ears on our day-to-day functions and enhanced alerting built into our network.***
>
> Will, IT Security Architect

Credit Unions Have Become Prime Targets of Cyber Attacks

For more information or to request a demo, visit **www.cygilant.com**

Credit unions face major challenges when protecting financial data in today's cyber threat landscape. In addition to protecting consumer data and financial records, IT security teams must also deal with strict compliance mandates for FFIEC, GLBA, PCI DSS, and a patchwork of federal, state, and other industry regulations. With so much to take into consideration, the task of securing an organization from breaches and vulnerabilities while meeting compliance requirements can seem overwhelming. Most credit unions tend to operate a smaller-scale IT team and are challenged to do more with less due to budget constraints, time availability, and limited resources. Cybercriminals have taken note of these disadvantages and over time, have begun a relentless barrage of cyber attacks, recognizing that the sensitive data in credit unions offers the potential for very significant financial gain.

"Your members' personally identifiable information is modern gold, and it's spread throughout your digital town, shuttled from safes to warehouses to storefronts when needed. The names, Social Security numbers, account numbers, and balances every credit union holds are valuable enough that complete profiles can be worth up to $400 when sold on the black market, according to an analysis by Quartz.com, although the median black market value is $20. And per capita cost to financial institutions of a data breach can top $200 in direct and indirect costs, according to the Ponemon Institute."

Ben Rogers, 3 Cybersecurity Threats Facing Credit Unions, Credit Union Times

> ***For professionals working in IT security, you need to utilize solutions that give you enhanced eyes and ears into the activity of internal users, external connections, and the various cyber attack attempts by cybercriminals.***
>
> Will, IT Security Architect

Midwestern Credit Union Needed to Improve Its Cybersecurity Posture

For more information or to request a demo, visit **www.cygilant.com**

Prior to partnering with Cygilant, the Midwestern credit union utilized the RSA envision™ SIEM solution. However, as the end-of-life of the product was nearing, the credit union decided it needed an IT security vendor that could provide more value to its cybersecurity investment. After researching various vendors in the market, the credit union came across Cygilant in an article about SIEM in SC Magazine. As the credit union learned more about Cygilant's SOCVue® hybrid security-as-a-service solution during a demo, it became clear that Cygilant's user interface was more developed, in that it was much more intuitive and required less effort to manage compared to its previous vendor product. Additionally, the credit union saw the value in Cygilant's managed approach, especially the supplementation of the Cygilant SOC team.

> ***The systems and solutions we have in place at our credit union are purchased only after an extremely thorough vetting process so we were very confident in our decision to purchase Cygilant's SOCVue Security Monitoring service.***
>
> Will, IT Security Architect

Midwestern Credit Union Refused to Become the Next Victim of a Cyber Attack

Given how attractive credit unions have become to cybercriminals, the credit union knew it had to continually adapt in order to stay ahead of cybercriminals. It seeks to always maintain a Defense-In-Depth (D-I-D) security program, which consists of performing continual analysis of security event data, executing penetration tests and internal audits, keeping up with security best practices, and following industry compliance requirements. By staying vigilant in these areas, the credit union's IT staff is able to assess gaps in the network infrastructure.

One of the main contributors to the D-I-D strategy is the credit union's IT Security Architect, whose role consists of looking at security from an endpoint perspective to the periphery, which involves developing strategies incorporating IT solutions that offer reliability, quality, and diversity. Will stated that every decision made in his department must support the ultimate goal of protecting his organization's network from those who seek to do it harm.

For more information or to request a demo, visit **www.cygilant.com**

After seeing all the benefit's Cygilant has to offer, such as the 24/7/365 security monitoring, supplementation of his IT team with Cygilant's SOC team, incident notification and remediation guidance, compliance reporting, and best practices for maintenance, monitoring, and analysis of audit logs, Will agreed that Cygilant's SOCVue Security Monitoring service was the most optimal addition to the D-I-D strategy. "The systems and solutions we have in place at our credit union are purchased only after an extremely thorough vetting process so we were very confident in our decision to purchase Cygilant's SOCVue Security Monitoring service," said Will.

Log Management & SIEM Still Matters

As most IT professionals can attest, a SIEM's traditional function is to serve as a security audit's checklist. After this, most SIEM technologies haven't proved to be significantly effective when it comes to analyzing log data, making improvements to security response times, or offering remediation guidance. However, Cygilant's SOCVue Security Monitoring service manages to stand out from all the rest due to its best-of-breed Log Management and SIEM technologies. Utilizing these advanced technologies from Cygilant, the credit union is able to receive 24/7/365 monitoring of its IT environment by Cygilant's highly trained and certified security experts. The Cygilant SOC team monitors and analyzes activity across all the IT assets, continually reducing false positives, and provides timely notifications of any security incident along with remediation guidance. "Since the SOCVue Security Monitoring service is being managed by Cygilant's highly trained SOC team, it provides us with a great deal of comfort knowing we have extra eyes and ears on our day-to-day functions and enhanced alerting built into our network," said Will.

> ***Raw logs remain the ultimate drill down into analyzing the effects of a possible security incident. Unfortunately, raw logs are simply an ugly thing to have to cycle through. However, Cygilant's SOCVue Security Monitoring service is one of the best I've seen at achieving the easy drill-down results that help IT security professionals do their jobs.***
>
> Will, IT Security Architect

Additionally, he noted that it's just as important to monitor the audit logs being created by all the network activity. "Raw logs remain the ultimate drill down into analyzing the effects of a possible security incident. Unfortunately, raw logs are simply an ugly thing to have to cycle through. However, Cygilant's SOCVue Security Monitoring service is one of the best I've seen at achieving the easy drill-down results that help IT security professionals do their jobs," added Will.

Improved IT Security and Peace of Mind

For more information or to request a demo, visit **www.cygilant.com**

Will and his IT team have been very pleased with the business benefits they've experienced while using the SOCVue Security Monitoring service. Some of these benefits include the ability to use the SOCVue Portal as a single dashboard to view all alerts gathered across the entire network, the ability to troubleshoot Windows logon events relating to Event IDs such as 4640 (A user account was locked out), 4671 (An application attempted to access a blocked ordinal through the TBS), and 4676 (The domain controller attempted to validate the credentials for an account), and the overall ease of use for needs such as security event data analytics and drill-down reporting.

> ***It's important to employ tools that help humans quickly assess and act on incidents as close to real-time as possible. A good SIEM can go a long way towards achieving this intended outcome and Cygilant's SOCVue Security Monitoring certainly helps to achieve this.***
>
> Will, IT Security Architect

Will stands firm in his belief that having the proper SIEM and log management solutions in place can greatly affect how strong a company's security and compliance posture can be. "For professionals working in IT security, you need to utilize solutions that give you enhanced eyes and ears into the activity of internal users, external connections, and the various cyber attack attempts by cybercriminals. It's important to employ tools that help humans quickly assess and act on incidents as close to real-time as possible. A good SIEM can go a long way towards achieving this intended outcome and Cygilant's SOCVue Security Monitoring certainly helps to achieve this," he concluded.

How Can Cygilant Help You?

For more information or to request a demo, visit **www.cygilant.com**

Cygilant's SOCVue hybrid security as a service provides the perfect balance of people, process, and technology for an effective security program. SOCVue provides the flexibility and cost savings of a SaaS offering, but unlike alternate solutions, Cygilant also provides the security team to manage the service and help implement security best practices. SOCVue enables your organization to:

- Reduce the cost of purchasing and maintaining security platforms
- Supplement existing IT staff with Cygilant's 24/7/365 Security Operations Center (SOC)
- Improve your security posture through proactive security and vulnerability assessment
- Help meet compliance requirements such as PCI DSS, FFIEC, GLBA, and more

SOCVue Security Monitoring provides a clear view into your network activity, which is one of the core foundations of a strong security posture. Monitoring the level of traffic that devices are experiencing, what actions are being performed, and by whom, are necessary components for discovering abnormalities in your IT environment. This service will give you enhanced visibility and control over your IT environment to strengthen your cyber defenses. You'll get best-of-breed Log Management and SIEM that is managed around-the-clock for real-time threat detection, analysis and notification, proactive remediation guidance, and compliance auditing.

About Cygilant

Cygilant, a pioneer in **hybrid security as a service**, is transforming how mid-market organizations build enterprise-class security programs. Acting as an extension of our customers' IT teams, Cygilant provides continuous security operations based on best-of-breed technology at a fraction of the cost of alternate solutions. Cygilant is a trusted advisor to organizations that need to improve their IT security and compliance posture and protect against cyber threats and vulnerabilities.

For more information or to request a demo, visit: **https://www.cygilant.com**