



CYGILANT[®]
SECURITY AS A SERVICE

A CYGILANT WHITEPAPER

Resellers: Expand Your Portfolio of Services with SOCVue Hybrid Security-as-a-Service Solutions from Cygilant

60 State Street, Boston, MA 02109

Tel: +1.617.337.4880 | Fax: +1.617.337.4830

<https://www.cygilant.com>

© 2017 Cygilant, Inc. All Rights Reserved.

Cygilant, the Cygilant logo, the SOCVue logo, SecureVue, ThreatVue, SOCVue, ComplianceVue, ForensicVue are trademarks or registered trademarks and Security as a Service is service mark of Cygilant in the US and/or other countries. All other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. All information presented here is subject to change and intended for general information.

An effective security program is a balance of people, process, and technology. When evaluating a security monitoring solution for your IT security portfolio, it is important to consider each of these areas in the decision-making process:



Technology

Security monitoring usually involves the deployment of a Log Management & SIEM solution. This technology has been incrementally improving for more than 10 years and has settled into a stable market with a handful of vendors advertising similar features. The critical question is how your organization will get value out of the technology. Consider your use cases and objectives when evaluating a feature list or data sheet. These use cases are most commonly related to threat detection, security operations, and compliance.



People

Unfortunately, some SIEM products have gained a reputation for being difficult to manage and slow to deliver valuable insights. It is important to consider the personnel skills and time required to manage and tune the collection policies, correlation rules, and reporting. Effective security and compliance also requires a commitment to 24x7 monitoring. Whether your organization chooses to use in-house resources, outsource to an MSSP, or use a continuous monitoring service such as Cygilant's SOCVue[®], be sure to evaluate the team that will be detecting and providing guidance in response to incidents and compliance violations.



Process

A final consideration is the set of processes that will be put in place as part of your security program. Installing a security product or hiring a service provider without having a well-thought-out plan is a sure way to squander resources. Security monitoring should be more than just a reactive firefighting exercise. Look for a solution that uses industry best practices to proactively improve your organization's security and compliance posture.

Solution Requirements Checklist

Does Your Vendor Offer...

Technology

There are a number of log management vendors competing on similar features, but not all of these vendors have mature technology for the uses cases that might be important to your organization. Be sure that your security monitoring service uses technology that is proven for these core requirements.

Log Collection and Storage

Reliably collect event and security logs from a wide range of devices, applications, servers, and databases. Meet long-term retention mandates.

Normalization, Categorization, Correlation

Translate log data into actionable security intelligence. More than just a log search engine.

Advanced Threat Detection

Continuously monitor for threats, policy violations, and other security incidents. Generate timely alerts that are easy-to-understand and provide actionable security intelligence.

Compliance Reporting

Deliver out-of-the-box reports for relevant audit regulations. Easy-to-understand data is linked to specific requirements in each regulation. Allows customization of reports.

Forensic Search

Find and retrieve log data with a fast, easy-to-use search tool. Provide ability to drill down on reports and alerts in order to investigate root causes.

People

The Security Operations Center (SOC) team is the key to getting value from a security monitoring deployment. The solution must be quickly tuned to start delivering actionable intelligence as soon as possible. Massive amounts of event data are then processed and analyzed. Your people need to be able to make sense of the data and identify the proper steps to respond to security incidents.

Continuous Monitoring

Security analysts are monitoring for incidents and threats 24/7/365. Notification is provided in a timely manner.

Trained Security Personnel

SOC staff has the expertise to tune SIEM correlation rules and system performance and to investigate security incidents.

Compliance

SOC staff has the resources and expertise required to collect and organize security data to meet the needs of compliance auditors.

Process

Security programs often falter when attention is given to technology and people, but not to the way these resources will be best utilized. An effective security monitoring program should include a set of processes that ensure consistent performance by your SOC team and monitoring technology.

Defined Security Program

Identify a set of critical security controls with measurable objectives. Program proactively finds security gaps and potential vulnerabilities in order to reduce the risk of a security breach.

Aligned With Security Best Practices (SANS/CIS Critical Security Controls)

Security program is based on recommended best practices such as the SANS/CIS Critical Security Controls for Effective Cyber Defense.

Continuous Monitoring and Improvement

Program controls and objectives are continuously measured to provide security awareness and a prioritized list of remediation actions.

Introducing SOCVue from Cygilant

Cygilant's SOCVue hybrid security-as-a-service offerings help overcome challenges such as limited budget or staffing by providing the right people, process, and technology in order to deliver increased security visibility and guidance. Cygilant provides continuous security intelligence and vulnerability assessment that helps organizations proactively address security and compliance challenges rather than using a reactive checklist approach. We utilize our own log management and SIEM technology that collects data from a broad range of sources and delivers the monitoring and reporting that forms the backbone of any compliance program. Cygilant can help your customers monitor and protect their networks from a costly data breach, as well as meet compliance monitoring and auditing requirements.

Key Benefits of SOCVue

- **Security Visibility: Get continuous visibility into security events and compliance posture. SOCVue provides real-time incident notification to minimize the risk of compromised financial records and cardholder data.**
- **Security Controls: Don't wait for an incident to occur. Unlike traditional security monitoring, Cygilant will assist you with proactive security controls to reduce the risk of a data breach occurring in the first place.**
- **FFIEC, PCI DSS, GLBA, and SOX Compliance: Go beyond simple compliance checklists. Instead of a point-in-time assessment, SOCVue gives you around-the-clock coverage of your IT environment and consumer financial data.**
- **Managed SIEM & Log Analysis: Don't waste money on "shelfware." Cygilant provides the dedicated security analysts that make security monitoring pay off, allowing your customer's organization focus on their core mission.**

Cygilant offers two security services that can help IT teams of any size improve security and compliance outcomes at a lower cost than alternate solutions: SOCVue Security Monitoring and SOCVue Vulnerability Management.

Use Cygilant as a Trusted Technology Partner to Implement a Comprehensive Security Program

Throughout Cygilant's history, we have deployed security intelligence in a variety of environments at scale and understand the expense of a security implementation in budget, time, and resources. Using Cygilant as a trusted technology partner can combine log management, threat detection, and compliance automation to deliver a single solution at a fraction of the cost of an in-house security service.

Cygilant delivers industry-leading services that combine the expertise of our certified Cygilant security analysts along with proven processes based on industry best practices, and best-of-breed technologies to meet your customers' IT security and compliance objectives.

The Cygilant Alliance Program is designed to help you succeed. Our all-inclusive, transparent subscription-based pricing allows you to generate new, recurring revenue streams. We offer the expert assistance of our own sales organization to help position and present our services to your customers. In addition, you will gain access to our Partner Portal that features easy deal registration and co-branded materials, and other resources to assist in building your success.

Key Benefits of Partnering with Cygilant:






- Drive additional revenue and complement your existing security and compliance offerings with security monitoring and vulnerability management services
- Get started quickly with no investment or minimum upfront revenue commitment required
- Enjoy predictable recurring revenue through our affordable subscription-based licensing model
- Develop pipeline with sales enablement and co-branded marketing materials
- Benefit from deal registration and protection
- Meet your customer's specific needs and environment with customized deployment
- Gain visibility into clients' real-time security status through Cygilant's multi-tenant portal
- Deliver the best possible customer experience through co-management of service

About SOCVue Security Monitoring

SOCVue® Security Monitoring Service provides 24x7 threat detection, compliance monitoring, and log management at a fraction of the cost of alternate solutions. SOCVue Security Monitoring Service is a subscription-based service that combines people, process, and technology to deliver an effective information security monitoring program, including:

- Managed SIEM & Log Management Software-as-a-Service (SaaS)
- 24x7 Security Monitoring by Cygilant SOC Security Analysts
- Incident Notification and Remediation Guidance
- Compliance Automation and Reporting

5 Reasons to Consider SOCVue Security Monitoring

	 1) Save Time	 2) Save Money	 3) Improve Compliance	 4) Strengthen Security	 5) Lower Risk
People	Augment your existing staff with Cygilant security analysts dedicated to monitoring your network	Let Cygilant deploy, configure, and fine tune the solution, without the cost of professional services	One-on-one consultations to customize compliance reporting, and to drive continuous improvement	24/7/365 continuous monitoring by Cygilant's trained security staff	Timely notification of any suspicious activity, on-demand investigative analysis
Process	Implement best practices for prioritizing and responding to security events	Use repeatable processes to lower the operational costs of security monitoring	Apply best practices to meet audit log requirements for compliance	Maintenance, monitoring, and analysis of audit logs as recommended by the CIS Critical Security Controls	Program controls are designed to be effective against the most common advanced threats
Technology	Automatically filter thousands of events to identify important security incidents	Gain immediate and comprehensive visibility in a cloud-based portal	Automated compliance reports delivered monthly or compiled on-demand	Quickly drill down and investigate security events, and utilize the built-in remediation guidance from Cygilant	Real-time monitoring of all relevant security data to gain timely notification of high-risk security concerns

About SOCVue Vulnerability Management

The SOCVue Vulnerability Management service is a subscription-based service that delivers the proper people, process, and technology to implement an effective vulnerability management program.





Cygilant partners with the leading vulnerability scanning technologies to ensure that scans are comprehensive and that the vulnerability database is up-to-date with the latest zero-day threats. The results can be integrated with the SOCVue Security Monitoring service so that vulnerabilities are correlated with other security event data.

SOCVue Vulnerability Management helps reduce your attack surface, while saving time and reducing your operational costs. The service includes:

- **Regular scanning of critical IT systems for known vulnerabilities**
- **Prioritization of vulnerabilities based on your unique business and security needs**
- **Summary data to stakeholders with easy-to-read executive reports**
- **Help meeting compliance requirements for vulnerability management**
- **Targeted scans for new or modified systems upon request**
- **Regular consultation with Cygilant Security Analysts to discuss risk assessment and vulnerability trends**
- **Correlation of vulnerability results with active attacks by combining this service with SOCVue Security Monitoring**

SOCVue Vulnerability Management Service includes access to the SOCVue Portal, the web-based command center for your information security program. Working with the Cygilant Security Operations Center (SOC), you'll determine the business value of each IT asset, and decide how frequently to scan for vulnerabilities.

4 Advantages of Using Cygilant's SOCVue Vulnerability Management Service

 1) Improve Your Security	 2) Improve Your Compliance	 3) Save You Time	 4) Save You Money
Provide visibility into security posture	Deliver PCI ASV scans	Manage deployments and scans	No upfront software cost
Remove easily exploited vulnerabilities	Scan frequency set to meet requirements	Analyze and prioritize	Better value than one-time assessments
Implement structured remediation process	Measurable results to track progress	Provide actionable guidance	Reduce personnel costs
		Verify remediation	Lower the risk of data breach or compliance failure

About SOCVue Patch Management

SOCVue Patch Management reduces your exposure to known vulnerabilities by proactively deploying recommended security patches. The SOCVue Patch Management service combines the low cost and flexibility of a SaaS solution with the support and expertise of a 24/7/365 Security Operations Center. Cygilant's SOC team will install and maintain the platform, and assist with the ticketing and audit reports to meet industry best practices. There is no hidden server maintenance cost or effort for your in-house team.

- **Decrease the time and complexity associated with patching servers, desktops and laptops on or off your network.**
- **Meet compliance requirements for remediating vulnerabilities as required by PCI DSS, HIPAA, FFIEC, and other security framework.**

Core Components of the SOCVue Service

Log Management & SIEM

A core component of any compliance program is log management. Cygilant allows an organization to collect, normalize, archive, correlate, and analyze event logs from assets in the IT infrastructure. These assets could include network and security devices, hosts, applications, and databases. The solution assists with asset discovery and management, and it meets the log collection and storage mandates included in most compliance directives.

Security Monitoring & Threat Detection

Privacy regulations and compliance programs are intended to help protect sensitive information. Therefore, it is critical to detect internal and external threats to information security. While traditional event search and correlation programs leave intelligence gaps, Cygilant's advanced correlation that can detect threat patterns across traditionally disparate systems. Cygilant helps organizations improve detection of more advanced threats including insider theft, brute force attacks, worms, and botnets. Threat patterns are correlated over long time frames, improving an organization's ability to detect the presence of advanced persistent threats. Our technology's real-time alerting engine and drill-down dashboards enable our SOC analysts to quickly deliver detailed information and guidance about any identified problems quickly. Our SOC analysts will work with your customer's team to create customized threat detection policies that are tailored to your organization.

Compliance Reporting

Cygilant's Log Management and SIEM technology combines all data (logs, vulnerability and network flow data) into a comprehensive compliance report, thus eliminating the need to manually collate data from multiple point products. These reports can be automated for regular intervals or can be run ad-hoc.

Cygilant includes comprehensive, pre-packaged, compliance reports targeted at specific regulatory mandates and best

practices. This compliance content helps organizations meet specific compliance reporting requirements and reduce compliance costs. Cygilant maps all compliance data, including data based on events, system configurations, network traffic and performance into detailed compliance reports that map directly into specific sections of the standard. Our SOCVue security analysts will work with your customer's team to identify reports that meet their compliance objectives.

Vulnerability Management

SOCVue Vulnerability Management Service provides cutting-edge vulnerability assessment technology, along with an extended security team, to effectively analyze vulnerabilities and track the remediation process. The service can save an IT team hundreds of hours every year, while providing the vulnerability management necessary to meet compliance mandates and reduce information security risk.

Patch Management

SOCVue Patch Management reduces your exposure to known vulnerabilities by proactively deploying recommended security patches. The service automatically scans Windows and Linux endpoints for missing patches for the OS, browser and 3rd-party applications like Java and Adobe. Through Cygilant's SOCVue Portal, you can review, approve and remediate patches with the proper change control processes and reporting.

SOCVue Portal

The SOCVue Portal is the central command center for your customers' information security programs. The Cygilant Security Operations Center filters thousands of events down to a snapshot of their current security posture, so you can quickly determine what needs attention. The SOCVue Portal gives your customers the ability to drill down on any security incident to find the incident details provided by the Cygilant SOC personnel. These incident details include Cause, Impact, and Remediation Guidance. With SOCVue, you no longer need to dig through thousands of events or analyze raw log files to determine what is happening in your network and what to do about it.

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>



© 2017 Cygilant, Inc. All Rights Reserved.

Cygilant, the Cygilant logo, the SOCVue logo, SecureVue, ThreatVue, SOCVue, ComplianceVue, ForensicVue are trademarks or registered trademarks and Security as a Service is service mark of Cygilant in the US and/or other countries. All other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. All information presented here is subject to change and intended for general information.

