CYGILANT™

SECURITY AS A SERVICE

A CYGILANT WHITEPAPER

Security Monitoring Buyer's Guide

60 State Street, Boston, MA 02109

Tel: +1.617.337.4880 | Fax: +1.617.337.4830

https://www.cygilant.com

CYGILANT™
SECURITY AS A SERVICE

Security Monitoring Buyer's Guide

An effective security program is a balance of people, process, and technology. When evaluating a security monitoring solution, it is important to consider each of these areas in the decision-making process. Your organization also needs to determine which areas should be handled internally and which should leverage a trusted partner.

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.

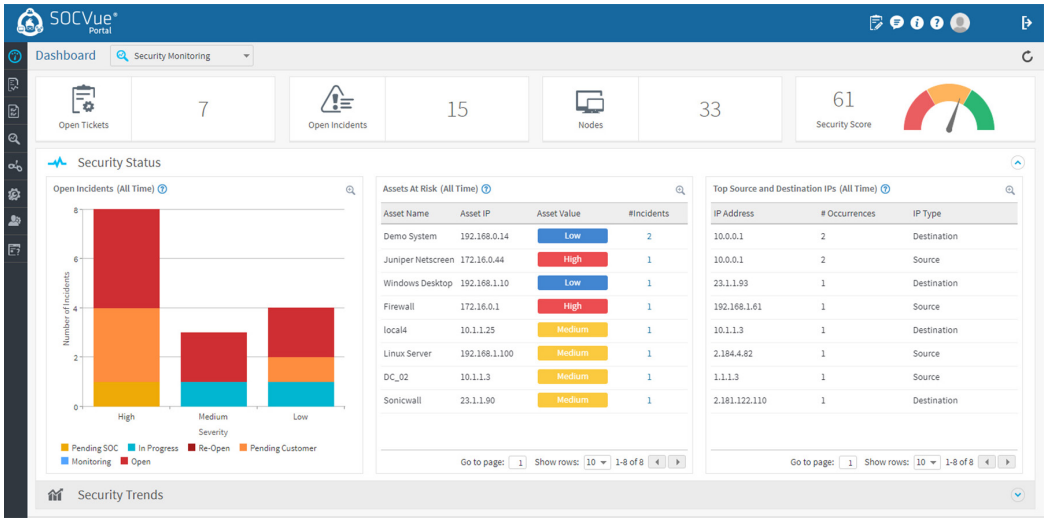
- [ ] **Defined Security Program**
  Identify a set of critical security controls with measurable objectives. Program proactively finds security gaps and potential vulnerabilities in order to reduce the risk of a security breach.
- [ ] **Aligned With Security Best Practices (SANS/CIS Critical Security 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

SOCVue® Security Monitoring provides 24/7/365 threat detection, compliance monitoring, and log management at a fraction of the cost of alternate solutions. The SOCVue Security Monitoring service is a subscription-based service that combines the perfect balance of people, process, and technology to deliver an effective information security monitoring program, including:

- **Managed SIEM & Log Management Software as a Service (SaaS)**
- **24/7/365 Security Monitoring by Cygilant SOC Analysts**
- **Incident Notification and Remediation Guidance**
- **Compliance Automation and Reporting**

SOCVue Portal



The SOCVue Portal is the central command center for your information security program. The Cygilant Security Operations Center filters thousands of events down to a snapshot of your current security posture, so you can quickly determine what needs your attention.

Security Incident Notification

SOCVue Security Monitoring includes 24/7/365 monitoring of your environment by Cygilant's trained security professionals. The Cygilant SOC team will analyze event data from across your IT assets and provide timely notification of any security incidents along with remediation guidance.

The SOCVue Portal gives you the ability to drill down on any security incident to find the incident details provided by the Cygilant SOC team. These incident details include Cause, Impact, and Remediation Guidance. With SOCVue Security Monitoring, 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.

5 Important Reasons to Consider

Cygilant's SOCVue Security Monitoring

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

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**