CYGILANT®
SECURITY AS A SERVICE

DATASHEET

SOCVue® Security Monitoring

SOCVue Security Monitoring provides 24/7/365 threat detection, compliance monitoring, and SIEM and Log Management at a fraction of the cost of alternate solutions.

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

SOCVue Security Monitoring is a subscription 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)**
- **24/7/365 Security Monitoring of on-premises and AWS cloud infrastructure**
- **Incident Notification and Remediation Guidance by Cygilant SOC Security Analysts**
- **Automated Compliance Reporting**
- **Best Practices for Maintenance, Monitoring, and Analysis of Audit Logs as recommended by the SANS/CIS Critical Security Controls**

CYGILANT®
SECURITY AS A SERVICE

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

Key Benefits:

GAIN PEACE OF MIND

Your security posture is being monitored around the clock by Cygilant's expertly trained SOC Security Analysts

EXTEND YOUR IT TEAM

Supplement your team with Cygilant's Security Operations Center staff

ACHIEVE COMPLIANCE

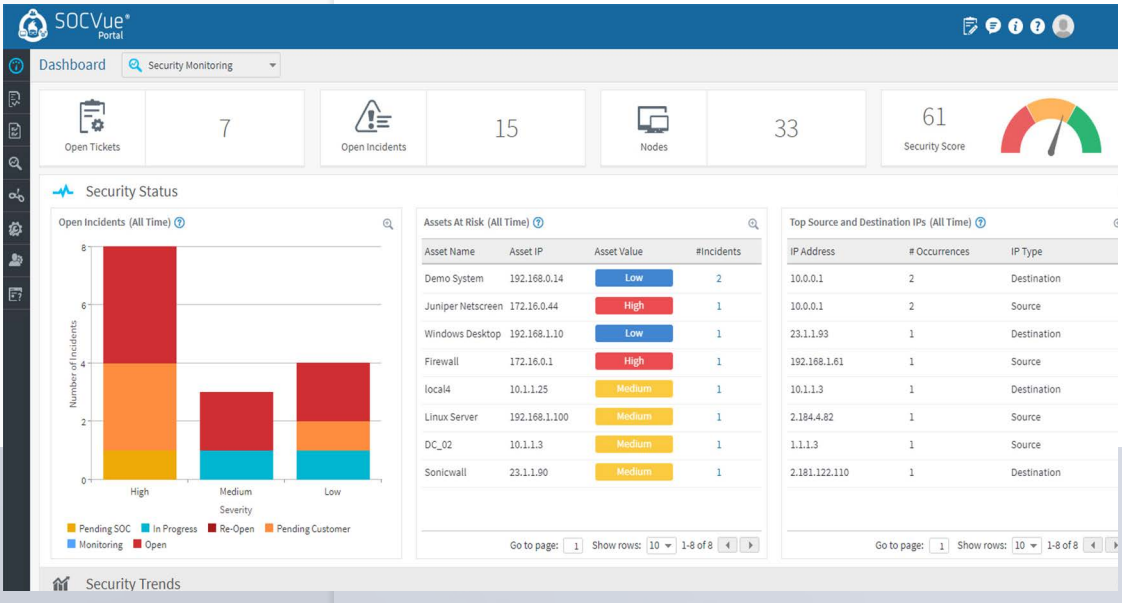
Meet compliance requirements through Cygilant's managed SIEM and Log Management

DEPLOY EASILY

Take advantage of flexible on-premise and cloud-based deployment options

SOCVue Portal

The SOCVue Portal is the central command center for your information security program. As part of the SOCVue Security Monitoring, the Cygilant SOC team will filter thousands of events down to a single snapshot of your current security and compliance posture, so you can quickly determine what needs your attention.



Access your security monitoring data anytime, anywhere, with the SOCVue Portal.

SOCVue Security Monitoring Delivers:

- **Deployment and management of SIEM and Log Management solution**
- **24/7/365 monitoring and incident notification by Cygilant's SOC team**
- **Daily security and compliance reports & monthly security summary and consultation**
- **Cloud-based deployment option**
- **Integrated threat feeds to quickly detect and respond to activity from known malicious IP addresses**
- **Audit log management as recommended by the SANS/CIS Critical Security Controls**

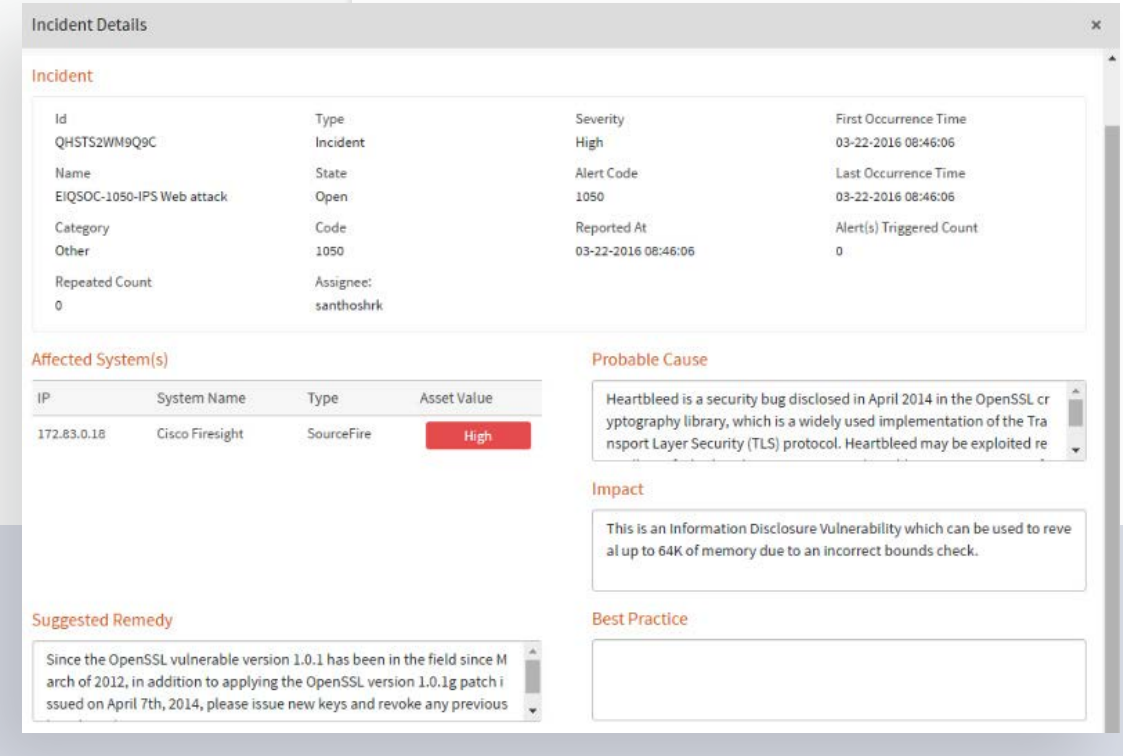
CYGILANT®
SECURITY AS A SERVICE

Security Incident Notification

SOCVue Security Monitoring includes 24/7/365 monitoring of your IT 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.

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



Use the SOCVue Portal to see what is happening in your IT environment, including cause, severity level, affected systems, impact, and remediation guidance.

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.

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

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