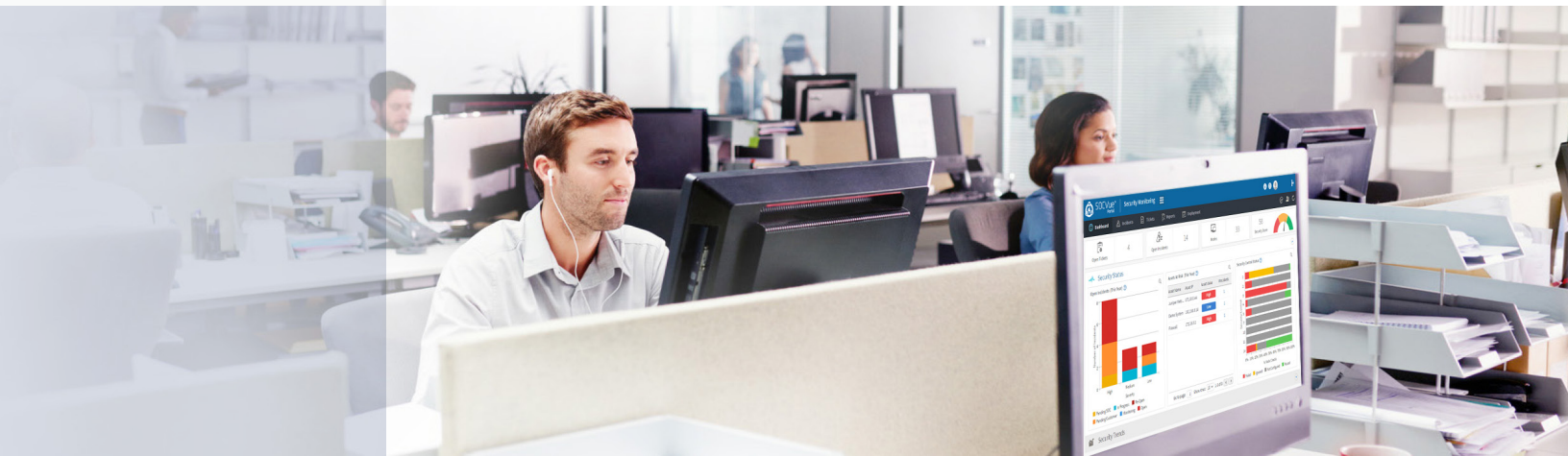


DATASHEET

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**





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



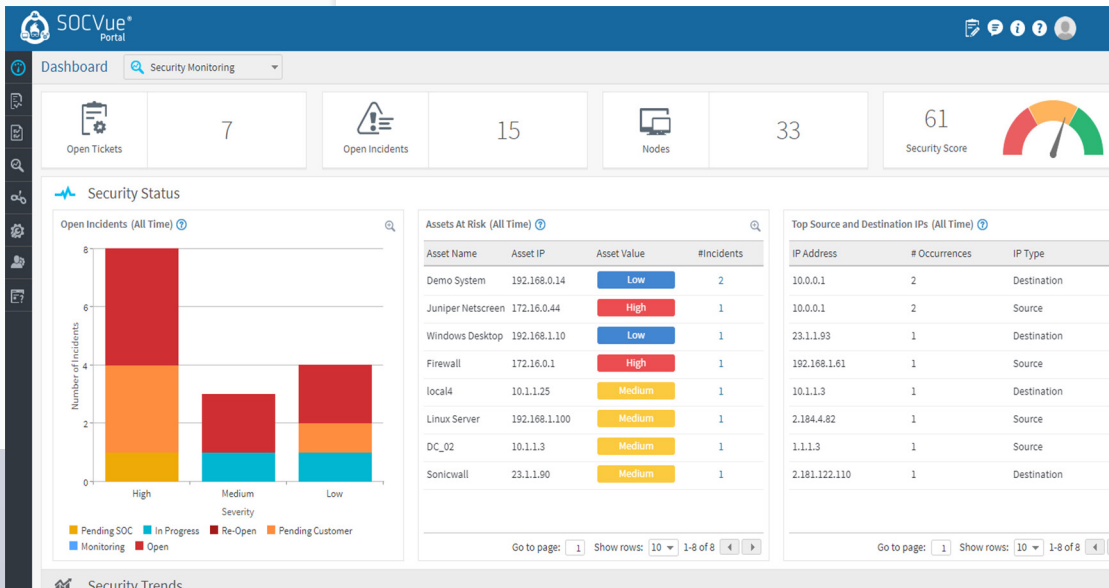
DEPLOY EASILY

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

For more information or to request a demo, visit www.binat.net.il

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



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.binat.net.il

Incident Details

Incident

| | | | |
|---|--------------------------------|---|---|
| Id QHSTS2WM9Q9C | Type Incident | Severity High | First Occurrence Time 03-22-2016 08:46:06 |
| Name EIQSOC-1050-IPS Web attack | State Open | Alert Code 1050 | Last Occurrence Time 03-22-2016 08:46:06 |
| Category Other | Code 1050 | Reported At 03-22-2016 08:46:06 | Alert(s) Triggered Count 0 |
| Repeated Count 0 | Assignee: santhoshrk | | |

Affected System(s)

| IP | System Name | Type | Asset Value |
|-------------|-----------------|------------|-------------|
| 172.83.0.18 | Cisco Firesight | SourceFire | High |

Probable Cause

Heartbleed is a security bug disclosed in April 2014 in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. Heartbleed may be exploited re

Impact

This is an Information Disclosure Vulnerability which can be used to reveal up to 64K of memory due to an incorrect bounds check.

Suggested Remedy

Since the OpenSSL vulnerable version 1.0.1 has been in the field since March of 2012, in addition to applying the OpenSSL version 1.0.1g patch issued on April 7th, 2014, please issue new keys and revoke any previous

Best Practice

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

About Internet Binat

Internet Binat provides communication and information security services to the business sector. Our services include internet access, information security, communication infrastructure administration, WAN networks and server hosting in Israel and abroad.

For more information or to request a demo, visit: <https://www.binat.net.il>