Datasheet

Cygilant SOC-as-a-Service

Experts in Cybersecurity. Experts in Service.

Cybersecurity is hard work. Resource constraints - not enough time or limited resources - and ever increasing threats coupled with compliance requirements is leaving your business at a disadvantage and causing team burnout. Cygilant SOC-as-a-Service exists to help you.

Extend your team with Cygilant SOC-as-a-Service.

True 24x7 SOC

We operate global Security Operation Centers (SOCs) with four tiers of humans from level 1s to 4s working around the clock.

Cybersecurity expertise

Experienced staff deliver industry leading security using bleeding edge techniques and tools.

Best-in-class service

Relieving you of the stress and burnout associated with cybersecurity is our main goal.

Militant about security. Militant about service.

When you select Cygilant for Managed Detection & Response, you build your own bundle of services. Included with every bundle is our SOC-as-a-Service. We pride ourselves on delivering white-glove service.

Continuous eyes on your systems	- 24x7 global coverage - Experts in cybersecurity - Monitor, triage, investigate, and provide tailored remediation advice
SIEM and log management	- Choose best-of-breed threat detection technology - Event correlation, network intrusion detection (IDS), and threat intelligence - Log management, with at least 12 months log retention - Incident response
White-gloved service	- Your cybersecurity partner, expect only the best service in the market - Security incident severity response from P1-P4

Single-pane of glass	- View security incidents, vulnerabilities, and reports in the Cygilant SOCVue platform - A clear dashboard to view your cybersecurity posture
Alert policies and incident response	- SOC will develop rules to trigger alerts for suspicious activity or security violations - Continuous fine-tuning and policy updates on an ongoing basis - Integrated SOCVue ticketing system guides you through the incident response process from detection to resolution
Compliance reporting	- Audit logs - Cloud access and activity logs - Compliance reports to meet your industry regulations FFIEC, PCI DSS, HIPAA

Your Partners in Cybersecurity

With 20 years of cybersecurity under our belt, Cygilant has strong credentials to partner as your SOC team.

- **Diverse education.** Many of our SOC team members hold masters degrees and PhD's in cybersecurity and come from Security Operation Centers, Network Operations Centers (NOCs), software engineering and IT backgrounds. This diversity and experience in real world environments allows us to deliver security value to all of our customers whether they use Linux in AWS, Windows in Azure, or a hybrid cloud mixture of network hardware and software in on- premises solutions.
- **Personal development.** We heavily invest in personal development, and continually deliver ongoing training. Entry level analysts complete full training in line with and exceeding industry standards.
- **Global analysts.** Our analysts are located globally in Boston, Belfast (UK), and Hyderabad, India. Our geo diversity allows us to take advantage of skill pools in multiple regions.
- **Certifications**. Our SOC team members all become certified via certifications such as Comptia Security Plus, CEH (Certified Ethical Hacker), GIAC, Cisco, and SANS.

How Cygilant SOC-as-a-Service Works

Choose your Cygilant Managed Detection and Response bundle to include security monitoring, vulnerability management and/or patch management. With each service, you gain access to a dedicated Cybersecurity Advisor and the Cygilant SOC team.

- Your Cygilant SOC team monitors your systems for threats, vulnerabilities and patches.
- If a threat or vulnerability is identified, our analysts will investigate and triage to determine the threat level. We'll only call you in the middle of the night if an urgent action is required!
- We provide detailed reviews of triggered events across your entire attack surface to identify suspicious activity, make security observations, highlight policy violations and suggest improvements. We advise on security threats with in-depth knowledge about your environment, instead of treating each alert in isolation as good or bad.

Partner with Cygilant and you'll have a SOC team that understands your objectives and future strategic vision to ensure our security partnership continually evolves to delivery security value and meet expectations as they grow.

Let's talk: 1-877-564-7787

CYGILANT®