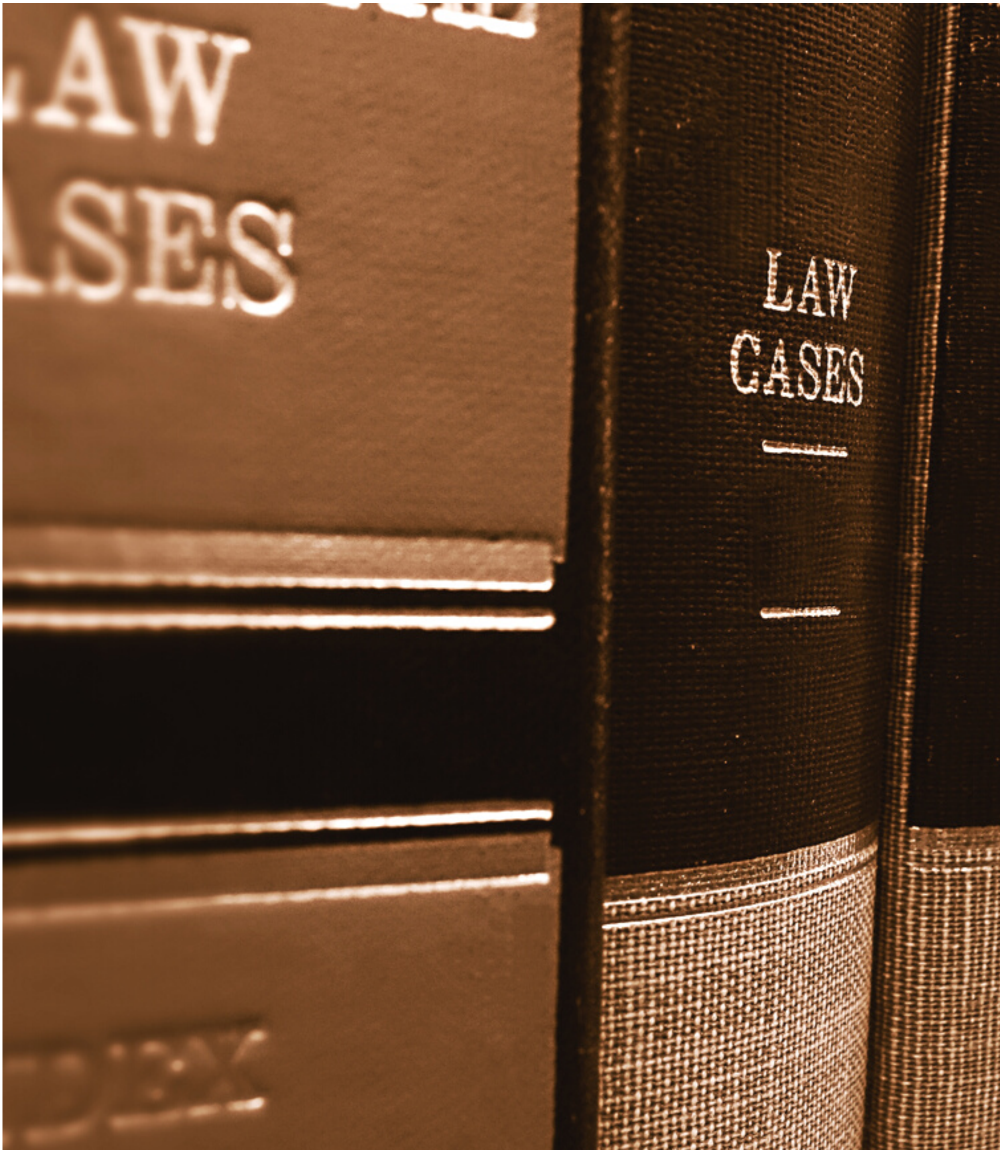
CYGILANT®

SOC-as-a-Service for Law Firms

How to Select a Security Operations Center as a Service Provider

HUNT. DETECT. RESPOND. COMPLY.



What is a SOC and why is it important?

A Security Operations Center (SOC) is a team of cybersecurity professionals whose task it is to monitor networks for cyberattacks and suspicious behavior, as well as improve internal security controls and procedures. Some large enterprises will have their own SOC, but for many law firms that’s simply out of the question. At minimum, to gain the 24x7 security a SOC provides, law firms would need to employ five full time SOC professionals. In most cases, we find that law firms simply do not have the resources to do this and are better off seeking help from managed SOC services.

A SOC team provides several opportunities to monitor a law firms systems for threats, vulnerabilities and patches. They provide expertise and a repeatable SOC process for effective and scalable operations. Every workflow follows these rules and is documented and recorded for SOC2 compliance.

If a threat or vulnerability is identified, SOC analysts will investigate and triage to determine the threat level. In-house teams should only be called in the middle of the night if an urgent action is required.

A SOC should provide detailed reviews of triggered events across an entire attack surface to identify suspicious activity, make security observations, highlight policy violations and suggest improvements. They should also advise on security threats with in-depth knowledge about a law firm's environment, instead of treating each alert in isolation as good or bad.

Selecting a SOC-as-a-Service provider

When building an RFP or evaluating a SOC-as-a-Service company, here are some criteria to consider:

Look for a Provider Who's Operations are 24/7/365

One reason to consider moving SOC monitoring to a provider is to improve overall tracking.

An in-house team is likely too busy to be watching its systems constantly. They have other tasks to attend to, so they may not respond to threats until there's an alarm. Some security tasks may be forgotten or neglected, or, by the time an alarm sounds, it may be too late.

A SOC service provider should be able to respond to potential threats before there's a warning or alarm. They also should be available 24/7/365 for round-the-clock care.

Ask for Security Features to Protect the Investment in SOC-as-a-Service

The best SOC has built-in security features to help prevent compliance gaps. This protects both the law firm and the service provider from security incidents.

Take a look at the provider's contract and certifications and see if they include the following:

- Regular performance of, and reporting on, third-party cybersecurity audits
- Certification in at least one recognized cybersecurity standard
- The use of encryption to send and receive data and encrypted traffic visibility

These are some of the ways to assess any provider’s security efforts. Looking for them will help integrate services smoothly and improve security when the time comes to work with a SOC.

Look for a Provider Who Assigns a Dedicated Cybersecurity Advisor to the Law Firm

The best service will come from people familiar with how law firms work. More specifically, a firm's systems, processes, compliance requirements and security goals. Look for providers who will assign dedicated security experts to the law firm. They should become an extension of the IT team, and:

- Provide cybersecurity best practices, processes and workflows
- Proactively hunt for threats
- Research alerts and eliminate false positives
- Deliver recommendations, based on incident investigation and analysis
- Work to continuously reduce the attack surface
- Help to create audit artifacts that prove compliance with various regulations

In an evaluation of SOC-as-a-Service providers, don’t just look at technology dashboards – look for proof points around service delivery.

Think About Location(s)

Where is the service provider located? Geography can be important for a few reasons.

- Does the service provider operate more than one location? The provider should have two or more sites; this allows them to provide disaster recovery and backup services.
- Determine where the business’ service team is working. A virtual SOC means the team could be located anywhere in the world. Compliance may mean services must be delivered from a certain country.

Technology Supports SOC-as-a-Service

Take a look at the technology the service provider uses.

Unlike other areas of IT and security, technology takes a back seat when it comes to SOC services. That's because human touch is still the defining factor.

Nonetheless, the SOC should offer real-time monitoring and analytical tools to help analyze this data, as well as a dashboard, or a single pane of glass from which they can review the security posture of the organization at any time.

The SOC should also have staff trained and certified to use what they've adopted to ensure they're using these tools to the greatest effect.

The Provider Builds a Relationship

Keep in mind that this will be an ongoing partnership. A provider should take steps to build a relationship from first contact. If they're not concerned about great service or customizing plans now, don't expect more later.

Providing great security requires an in-depth understanding of an organization's business. A great SOC services provider knows that. It's why they should be taking steps to understand the business and its needs from the beginning of the relationship.

Alignment with Security Needs and Plans

Think about how any provider's offerings fit with the law firm. Each firm will already have its own security protocols and processes. Some of these may be required to maintain compliance.

The main elements of cybersecurity a SOC-as-a-Service provider should offer includes:

- Security Monitoring – To collect security events across IT infrastructure, network, and applications, triage and investigate potential security incidents to give rapid, actionable recommendations. Combine log management and SIEM technology with machine learning to save time digging through the noise of thousands of events or eliminate analyzing raw log files to determine what is happening in the network.
    - Endpoint Security, a subset of security monitoring, provides next-generation malware detection for workstations and servers. The technology provides increased visibility into suspicious activity and potential threats.
- Vulnerability Management – Quickly detect vulnerabilities from software flaws or misconfigurations with scanning technology. Look for a provider that offers a centralized platform where all scanning results integrate directly with prioritized vulnerabilities and determine remediation steps.
- Patch Management – Work with a SOC-as-a-Service provider that offers automated patch scanning and installation, as well as patch rollbacks, to ensure best practices are followed and compliance can easily be proved to an auditor.

Any service provider should be able to integrate with what is already in use. Be sure to align deliverables against security objectives; specifically, what should the service provider do to help a law firm achieve its goals? Make sure to define metrics and reporting. This will help manage expectations from the onset.

Consider Pricing Factors

When it comes to cybersecurity operations, cost is often a concern. It may be one reason an in-house team isn't as large as it needs to be. It might also be the reason to consider SOC-as-a-Service in the first place.

Pricing is often the first concern for the partners, but it shouldn't be the only thing considered when looking for a provider.

There are many pricing models, and they can be confusing: volume-based pricing, user-based pricing, node-based pricing, etc. Some vendors make it very simple to predict what the pricing for their service will be. That said, predictable costs don't mean lower costs.

Keep in mind that providers at either end of the pricing spectrum may not be the best options. Those who are priced too high will end up costing too much. Those with lower prices may look like a safe bet, but they might also be unable to deliver the service needed.

Think about value. The right provider may not offer the lowest price, but they will offer the services needed and what you want in a long-term relationship.

Cygilant SOC-as-a-Service

With 20 years of cybersecurity under our belt, Cygilant has strong SOC credentials.

Diverse Education

Our SOC team holds Masters and PhDs in cybersecurity and come from SOC, NOCs, software engineering and IT backgrounds. Our diversity allows us to deliver value across hybrid environments.

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 in Boston and Belfast, UK. Our geo-diversity allows us to take advantage of skill pools in multiple regions.

Certifications

Our SOC team members hold certifications such as Comptia Security Plus, CEH (Certified Ethical Hacker), GIAC, Cisco, and SANS.

How Cygilant SOC-as-a-Service Works

Choose a Cygilant bundle including either security monitoring, vulnerability management and/or patch management. With each service, you'll gain access to a dedicated Cybersecurity Advisor and the Cygilant SOC team.

1. The Cygilant SOC team monitors systems for threats, vulnerabilities, and patches.
2. If a threat or vulnerability is identified, Cygilant analysts will investigate and triage to determine the threat level. We'll only call in the middle of the night if an urgent action is required.
3. We provide detailed reviews of triggered events across the 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 the environment, instead of treating each alert in isolation as good or bad.

About Cygilant

Cygilant protects mid-sized organizations from the latest cybersecurity threats through a combination of automated tools and personalized advice. The company provides dedicated Cybersecurity Advisors (CSAs), who work directly with customers as an extension of their team; global 24×7 Security Operation Centers (SOCs), which constantly monitor customers' networks using the latest threat hunting, detection, patch management and incident response technologies; and its SOCVue Platform, which consolidates multiple streams of security data to help detect and respond to threats faster.

Hunt. Detect. Respond. Comply.