AGILEBLUE

Automation. Visibility. Confidence.

THE VALUE OF SOC-AS-A-SERVICE TO ORGANIZATIONS

Whitepaper

AgileBlue, 2021

Organizations are under constant cyberattack from a diverse group of assailants ranging from opportunist cyber criminals to highly motivated and resourced nation states. Attacks have increased in both frequency and sophistication and include ransomware, business email compromise, and theft of sensitive customer information. Organizations no longer have the luxury to investigate and respond to cyber anomalies and suspected attacks when resources become available; cyberattacks propagate quickly and can inflict significant brand damage. Organizations looking to augment cybersecurity capabilities with third-party services have a dizzying array of choices in the marketplace today. Further, Organizations across the world are increasingly hybrid and multi-cloud / multi-tenant environments as they look to numerous cloud providers to lift-and-shift or build cloud-native applications fast in efforts to meet different technical and business requirements. Whether you want to run on a reliable infrastructure for the best performance, use cloud services such as containers and analytics or avoid vendor lock-in, a multi-cloud approach should dominate your cloud strategy.

This whitepaper explains the various service options and provides examples of why an outsourced security operations center (SOC-as-a-Service) provides exceptional value to organizations. This report also provides a case study demonstrating the value of SOC-as-a-Service.

The primary benefits of SOC-as-a-Service are economics and cybersecurity coverage. Substituting an in-house security operations center for a SOC-as-a-Service provider can reduce annual spend by up to 80%. A capable and proven SOC-as-a-Service provider will be able to perform nearly all the required cybersecurity and regulatory support functions as well as allow the organization to focus on management oversight regarding the successful performance of the SOC provider.

A SOC-as-a-Service provider will bring advanced technologies to the engagement. These are normally well beyond the reach of midsize organizations to procure, implement, deploy, and maintain independently. Examples include enhanced detection, user behavior and entity behavior analytics, risk analysis weighting, and incorporation of threat intelligence data. Coupled with advanced automation and AI/machine learning, these technologies will benefit the organization and the service provider.

Outsourcing to a SOC-as-a-Service provider does not completely release the organization from cybersecurity requirements. The organization will still need to have a structure to define cybersecurity strategy and risk appetite, and the CIO or other designated executive will be responsible for informing and guiding key stakeholders of cyber-related risks. The CIO or designated representative will also remain responsible for cyber-related interactions with examiners, regulators, and auditors. However, a capable SOC-as-a-Service provider will successfully offload the day-to-day cybersecurity functions and be ready to jump into the action in the event of a cyber incident.

If properly planned, designed, and implemented, the SOC-as-a-Service will essentially be a logical extension to the organization's IT staff. The CIO or designee will need to ensure that the provider has access to required resources and information. This will allow the provider to customize runbooks, create incident response procedures, and keep current communications plans for both daily operations in the event of cyber incident.

The SOC-as-a-Service provider will, in most cases, provide the supported organization with relevant reports and data regarding cyber health and risk levels. Many SOC-as-a-Service providers currently do this via web-based dashboards.

Although a SOC-as-a-Service relationship allows an organization to offload key cybersecurity functions, to be successful, the partnership requires active interest and involvement by a responsible member of the supported organization's CIO or designated representative. Otherwise, it is unlikely that the provider will receive sufficient input and feedback to best serve the organization

SOC-AS-A-SERVICE DIFFERENTIATORS

Capabilities and service level quality can vary widely between SOC-as-a-Service providers. Potential buyers of cybersecurity services should look for SOC-as-a-Service providers that can offer the following:

- **Simplified setup and service initiation**: SOC-as-a-Service providers should have detailed and tested plans, procedures, and timelines for starting the service. This will include distribution and installation of agents, adapting runbooks to the specific customer environment, and granting access to reporting. This will also include briefing and training designated members of the supported organization.
- **Highly reliable anomaly detection and reduced false positiv**es: The SOC-as-a-Service provider should be able to demonstrate that the service can accurately and quickly detect cyber anomalies and cyberattacks. False positives can significantly impact the reliability, efficiency, and credibility of the service, and the SOC-as-aService provider should be able to demonstrate how false positives are minimized.
- **Highly intuitive dashboards**: Organizations should be able to measure their cyber risks against an established baseline or framework. Ideally, the dashboards should display an overall risk score to allow personnel without cybersecurity experience to quickly assess the overall state of cyber health.
- **Robust logging and analysis**: The service should include log collection, aggregation, and analysis to support regulatory compliance and review by examiners, assessors, and auditors.
- **Contract flexibility**: Committing to 2–3-year agreements instead of 5 years plus.
- **Highly responsive cybersecurity specialists**: This is the most important aspect of a SOC-as-a-Service provider. Buyers should look at the qualifications, training, tenure, and certifications of security analysts, threat intelligence specialists, and SIEM and EDR administrators. The provider should be able to offer references from other clients, particularly any that have needed to use the provider's remediation and incident response services.

COMPARISON OF CYBERSECURITY SERVICES

Buyers of cybersecurity services will be presented with a broad range of offerings that can often be difficult to quantify and compare. Service descriptions vary widely, while some basic categories of cybersecurity services do exist.

Many providers will indicate that they are integrating AI, machine learning, and/or automation into their service offerings, primarily to make the services more responsive and capable. Automation is already having a demonstrable impact on cyber defense, and improvements will continue in 2021 and beyond. Both the service provider and the supported organization benefit from automation. For the service provider, automation reduces the human requirements of the providers' services and enables or increases provider competitiveness and profitability. For the supported organization, automation results in more efficient and faster handling of cyber anomalies and reduction in remediation times.

The table below contains examples of generic cybersecurity services offered by MSPs and MSSPs.

Service Category	Considerations for small and midsize financial services organizations
Managed SIEM: The provider will offer a SIEM capability based on event data collection and analysis, usually as a cloud-based service. The provider will supply the core infrastructure, management, and administration of the SIEM on a subscription basis.	A SIEM capability, while an integral part of cybersecurity operations, is not sufficient by itself to provide highly targeted organizations with coverage against cyberattacks.
Endpoint detection and response (EDR): The provider will offer agent-based monitoring of activities on desktops, laptops, and servers as well as some basic response and mitigation services.	EDR is a partial solution as the supported organization would still have to act in response to anomalous activities or actual indications of a cyberattack.
Managed detection and response (MDR); The provider will offer advanced threat detection as well as incident management and remediation services for cyber events. This is the fastest growing segment of today's cybersecurity services market.	The MDR provider's capabilities are suitable for organizations that elect to outsource cybersecurity services. However, not all MDR providers provide a SIEM capability that would likely need to be provided to meet regulatory and compliance requirements for logging. This would require a separate SIEM provider and increase complexity.
Extended detection and response (XDR): This offering goes beyond MDR to encompass additional telemetry and cyber services based on cloud workloads. This is a relatively recent market category that is still evolving in the marketplace.	XDR from some providers may be more than most small and midsize organizations can successfully integrate into their cybersecurity strategies. Pricing and technical requirements may exceed the organizations' budgets and integration capabilities.
OC-as-a-Service: The provider offers the functionality of a security operations center based on a subscription model. The SOC is staffed by security analysts, threat intelligence specialists, and SIEM and EDR administrators. The SOC provides a 24/7 monitoring capability, operations and maintenance functions based on standardized runbooks, and a comprehensive cyber incident management capability.	SOC-as-a-Service will in most cases be the best fit for small and midsize organizations that move to outsource a broad range of cybersecurity functions and obtain a SIEM capability for regulatory requirements from a single provider.
Co-Managed SIEM and/or Co-Managed SOC – Some providers offer these options that require the supported organization to play an active role. in the functioning of the service.	The co-managed options may not be suitable for organizations that have limited cybersecurity staff. Also, delineation of responsibilities can be complex and may result in poor handling of cyber events.

Source: Aite Group

CASE STUDY

The following details outline a recent case study with with the chief information security officer (CISO) and senior infrastructure engineer at Legal Aid Society of America (LAS), a research, education, and support nonprofit based in the United States. The organization supports communities and citizens who cannot afford legal representation. LAS had engaged a well-known MSSP with less than favorable results. The CISO noted that a combination of the lack of transparency regarding alerts, poor provider performance, and high monthly fees drove a decision to suspend the contract and bring cybersecurity services back in-house. During the tool selection phase for the in-house build, LAS was introduced to AgileBlue, a U.S.-based SOC-as-a-Service provider.

After a brief review of AgileBlue's services, the CISO said he realized that SOC-as-a-Service would be ideal for LAS' business and alleviate the need to invest in infrastructure and personnel while protecting the company from sophisticated cyberattacks. The CISO also noted that AgileBlue's service offering would help them demonstrate capabilities to help their clients meet U.S. non-profit compliance requirements. AgileBlue initiated services at the end of January 2021.

The CISO and senior infrastructure engineer expressed satisfaction with the ease of implementation. Specifically, they noted the "one click" deployment of agents, strong controls around how the agents securely communicate with AgileBlue, and elimination of the need to reboot endpoints after agent installation. The experienced senior infrastructure engineer also mentioned that implementation of AgileBlue was the smoothest agent deployment he had encountered. The CISO was particularly pleased with a comprehensive project plan provided by AgileBlue to facilitate the deployment and the team's ability to work with AgileBlue's dedicated support team. The CISO and senior infrastructure engineer accessed AgileBlue's web-based portal to review monitoring activities and cyber health, and they reported that this portal provides them all they need to manage cybersecurity operations and respond to queries.

AgileBlue's benefits include a much smoother auditing process and what the CISO is positioning as a competitive advantage for LAS during discussions with stakeholders. In essence, the CISO reported that LAS is now receiving a complete range of cybersecurity services at roughly 10% of the monthly cost of the previous MSSP. When comparing SOC-as-a-Service provides, AgileBlue focuses on their three main differentiators. First, they provide their clients with enhanced visibility regarding cyber risk via the AgileBlue analytics reporting dashboard. Next is the AgileBlue proprietary risk scoring algorithm, including industry comparisons and risk analysis trends. And finally, AgileBlue's proprietary Silencer technology significantly reduces false positives, with a 95% confidence score on incident alerts based on its proprietary machine learning and user behavior analytics.

CONCLUSION

- Non-profit organizations are receiving the same sophisticated threats and attacks as major organizations; however, most do not have the resources to defend against them. The use of outsourced cybersecurity services can help close that gap.

- The landscape of cybersecurity services includes hundreds of providers offering a broad array of capabilities ranging from basic blocking and tackling, all the way to sophisticated remediation and incident response offerings. The MSP, MSSP, and related technology solution provider markets are experiencing frequent M&A deals, making supplier commercial profile analysis an important of service provider selection criteria.

- The use of AI, machine learning, and automation help cybersecurity service providers more quickly identify cyber anomalies, respond to incidents, and perform remediation actions.

- SOC-as-a-Service offers a broad range of cyber capabilities that can be used as a logical extension of an organization's IT staff. Small and midsize financial services should consider SOC-as-a-Service when contemplating outsourcing of cyber functions.

ABOUT AGILEBLUE

AgileBlue is a SOC-as-a-Service platform that's proven to detect cyber threats faster and more accurately across your entire digital infrastructure and cloud. We provide 24/7 monitoring, detection and response to identify cyber threats before a breach occurs.

Our tech is intelligent and automated, but we take a custom approach for every client we work with, analyzing and detecting exactly what you need it to. Our products are 100% cloud-based including advanced machine learning and user behavior analytics backed by our team of cyber experts who are always just a call away.

Ready to protect your company? Contact Us.