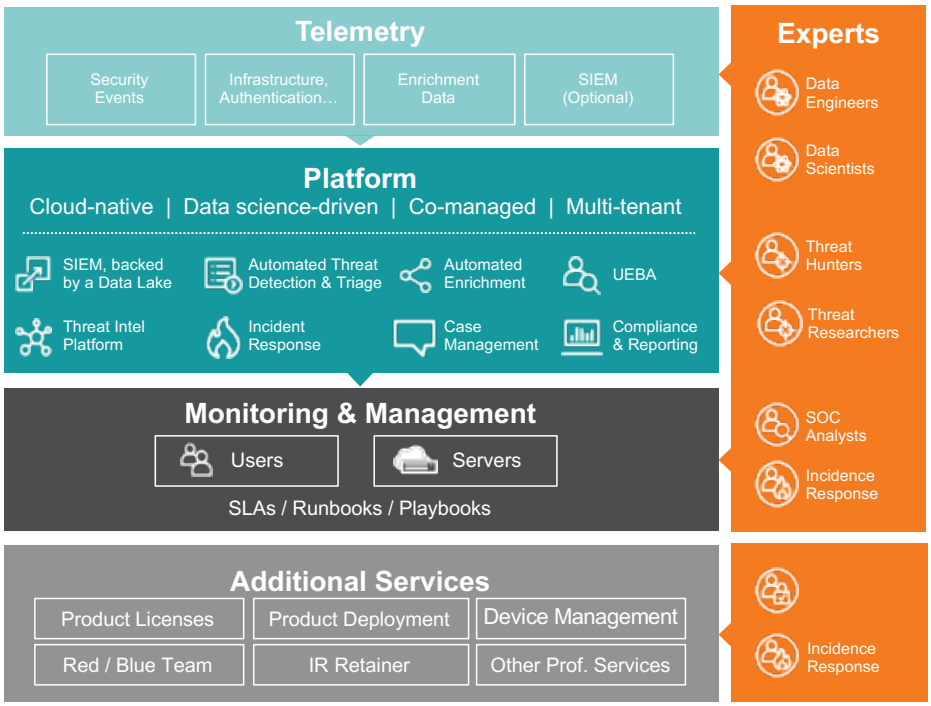
Data Sheet

Cysiv SOC-as-a Service

Cysiv Soc-As-a-Service

Cysiv SOC-as-a-Service delivers all of the benefits of having a dedicated 24/7 SOC, but without the high costs, complexity, burden and frustrations that come with building, staffing and operating one. You outsource the people, processes and technology needed for a SOC to Cysiv, and Cysiv provides it as a service, which is operated and managed offsite and delivered as a cloud-based service.

Soc-as-a-service:
Proactive threat defense, with a managed security product stack



Benefits

- Faster threat detection and remediation
- Lower cyber risk
- Cost reduction
- Better leveraging of existing security investments
- Enhanced business agility and scalability
- Greater visibility, reporting and compliance

"The faster a data breach can be identified and contained, the lower the costs. Breaches with a lifecycle less than 200 days were on average $1.22 million less costly than breaches with a lifecycle of more than 200 days."

-- Ponemon Institute, 2019

To learn more, please visit www.cysiv.com

Cysiv SOC-as-a-Service provides:

- A modern, cloud-native SaaS platform that accelerates, and improves the effectiveness of, threat detection, hunting, investigation, triaging, case management and remediation
- A team of experts that operate as an extension to your security operations team
- Comprehensive and timely threat intelligence and research
- Incidence response
- Security monitoring and management
- All supported by SLAs, runbooks and playbooks

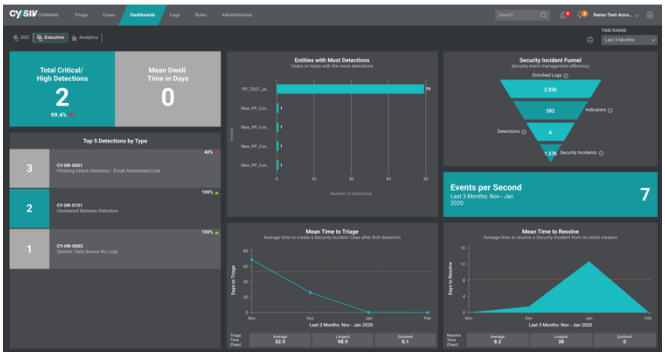
With complementary services such as deployment, an incident response retainer, penetration testing, and red team- blue team services.

SOC Augmentation & Virtual SOC

Cysiv SOC-as-a-Service augments enterprises' and MSPs' existing SOC or service offerings with complementary threat protection, comprehensive cyber expertise, or 24/7 coverage. Or, it can operate as a virtual SOC for organizations that lack the resources to build, staff and operate one.

Proactive Threat Defense

By leveraging enterprise telemetry and its cloud-native platform, Cysiv experts monitor your environment for threats, investigate and triage them, and do proactive threat hunting. We then recommend the appropriate actions for you to take or we can remediate the threats directly.



Telemetry: Logs, data, and other telemetry from as many relevant sources as possible—security controls, infrastructure - including cloud (AWS®, Microsoft® Azure™, Google Cloud Platform™), applications and other contextual data sources—are first normalized to facilitate correlations, reduce false positives and help highlight false negatives. This improves the confidence in detections triaged for further investigation. Cysiv is vendor-agnostic and ingests telemetry from a large number of sources and vendors.

Platform: Cysiv has developed its own modern, cloud-native, co-managed, multi-tenant SOC platform that is the foundation for its service. It is massively scalable and combines a number of essential technologies – including SIEM, automated threat detection and triage, a threat intelligence platform, user and entity behavior analysis (UEBA), and incidence response – all tightly integrated into a single SaaS. And, it's backed by a massively scalable, purpose-built, indexed data lake with tiered data storage (hot, warm, and cold) to better manage costs and support compliance requirements.

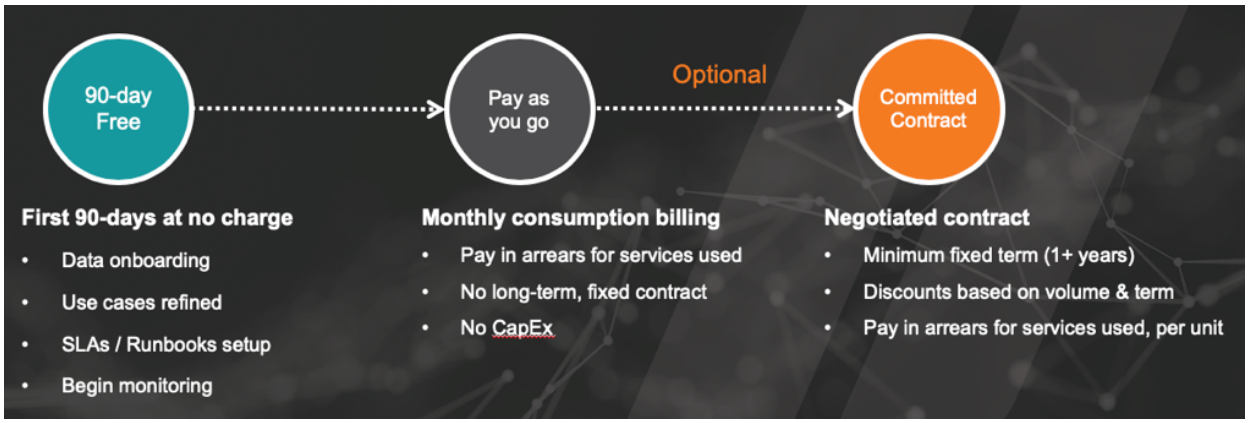
From within the platform, Cysiv then rigorously applies a comprehensive and blended set of data science techniques to automate and improve the time-consuming, complex but critical activities and processes for truly fast and effective threat detection, hunting, investigation and response. This includes cyber intel-, signature-, behavior-, statistics-, and algorithm-based detection techniques.

Monitoring and Management: By leveraging enterprise telemetry and the platform, Cysiv provides 24/7 threat monitoring, detection, triage, investigation and remediation. Cysiv can also configure, manage and optimize the availability, health and policies of selected security controls and devices.

Experts: Cysiv certified experts—including security analysts and engineers, threat hunters and researchers, data scientists and engineers, and incident response experts—are directly accessible to you. Cysiv experts operate as a virtual extension to your security team, collaborating as necessary to further ensure timely, superior detection and protection.

Consumption-Based Pricing

Cysiv gets you up-and-running quickly, and only invoices you for the services and licenses consumed each month, with no long-term contracts or CapEx, to provide maximum flexibility and savings.



Business Issues Addressed

Cysiv SOC-as-a-Service can help enterprises address these common frustrations:

- Timely threat detection and remediation
- Alert fatigue
- SIEM deployment, deficiencies and cost
- Security tools complexity
- Skills shortage
- Ensuring regulatory compliance
- Rising costs

To learn more, or for a consultation and demo, contact us today.
Cysiv Inc. 225 E. John Carpenter Freeway, Suite 1500, Irving, Texas, USA, 75062

sales@cysiv.com www.cysiv.com