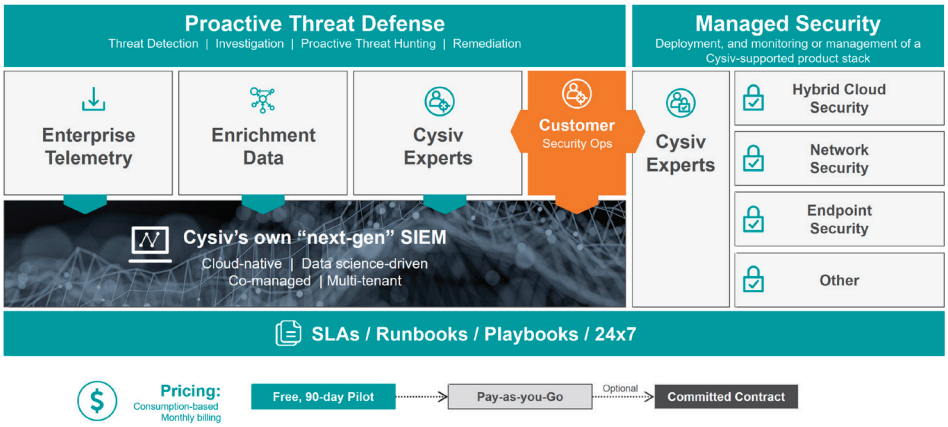
CYSIV SOC-AS-A-SERVICE

Cysiv combines all the elements of an advanced, proactive, threat hunting security operations center (SOC) with a managed security product stack and delivers them as a 24/7 service, with simple, consumption-based, monthly billing. Whether augmenting your existing SOC or being your virtual SOC, Cysiv operates as an extension to your cybersecurity operations team, elevating and extending its capabilities.

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

CYSIV SOC-AS-A-SERVICE PROVIDES:

- Around-the-clock (24/7) security event monitoring, detection, investigation and alert triaging
- Proactive threat hunting, and mapping to the kill chain and Mitre Att&ck framework
- Security incident response management, including malware analysis and forensic analysis
- Threat intelligence management (collection, fusion, and dissemination)
- Threat and vulnerability management
- Deployment and monitoring or management of an integrated, market-leading security product stack
- SLAs, runbooks, and playbooks

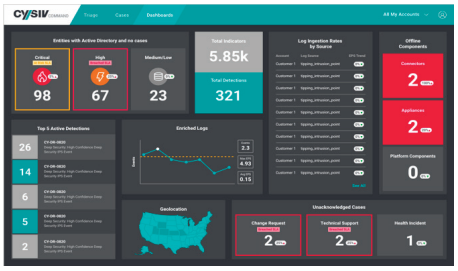
"The faster a data breach can be identified and contained, the lower the costs. Breaches with a lifecycle less than 200 days were on average $1.22 million less costly than breaches with a lifecycle of more than 200 days."

— **Ponemon Institute, 2019**

SOC AUGMENTATION AND 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. Virtual SOC is suited to enterprises that lack the resources to build, staff, and operate one.

PROACTIVE THREAT DEFENSE



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.

Next-Gen SIEM: Cysiv has developed its own advanced, next-gen SIEM. This unique and powerful cloud-native, co-managed, multi-tenant platform combines a number of essential technologies and functions, leveraging a broad range of advanced data science techniques to automate, accelerate, and improve the process of finding and prioritizing threats that truly warrant deeper human investigation. Plus, 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.

Enterprise 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.

Enrichment Data: The telemetry is further enriched with threat intel and other information—including that from vulnerability assessments, asset inventories, and Active Directory—to further improve correlations, reduce false positives, help highlight false negatives, and to better identify truly suspicious and malicious activity.

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.

MANAGED SECURITY

In addition, Cysiv will manage security controls from Trend Micro and other market-leading vendors, on your behalf, for hybrid cloud (datacenter, cloud workloads, containers, serverless), network and endpoint security, as well as for deception. This includes deploying and integrating the security controls, monitoring system activity, tuning rules and policies, deploying patches and updates, and performing regular health checks to ensure they've been optimized for your environment.

CONSUMPTION-BASED PRICING

Cysiv gets you up-and-running quickly, ensures you only pay for the services and licenses you consume each month, all while providing maximum flexibility and savings.

- Define service requirements
- Define SOC escalation process
- Data integration / ingestion
- Demonstrate value

- Monthly consumption billing
- Pay in arrears for services used, per unit
- No long-term, fixed contract
- No CapEx

- Monthly consumption billing
- Negotiated contract
- Minimum fixed term (1+ years)
- Discounted pricing based on term

BUSINESS ISSUES ADDRESSED

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

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

TO LEARN MORE, OR FOR A CONSULTATION AND DEMO, CONTACT US TODAY

Cysiv LLC. 225 E. John Carpenter Freeway, Suite 1500, Irving, Texas, USA, 75062

sales@cysiv.com www.cysiv.com

CYSIV