CYSIV SECURITY OPERATIONS CENTER (SOC)-AS-A-SERVICE

DETECTS, INVESTIGATES, HUNTS FOR AND RESPONDS TO ACTIONABLE THREATS.

The impact of a successful cyber-attack can be devastating, which is why detecting and responding to cyber threats, quickly and confidently, has never been more important, or challenging:

- Your attack surface is rapidly expanding (remote workforce, cloud, iot)
- Adversaries are increasingly well-armed and motivated, and the frequency of attacks is alarmingly high
- Big data is a big problem: the volume of security events and other essential data that has to be correlated and investigated has grown exponentially in recent years
- Analysts have to rely on multiple security tools that are outdated, complex, and lack integration or automation
- Overwhelmed with alerts and false positives, security teams often miss critical signals of an impending breach
- And with the global cyber skills shortage, it's all but impossible to hire and retain the breadth of talent required to tackle this challenge

Cysiv SOC-as-a-Service combines everything required to detect, investigate, hunt for and respond to actionable threats.

"Building, implementing, running and sustaining a fully staffed 24/7 SOC is cost-prohibitive for most organizations."

- Gartner, "Selecting the Right SOC Model for Your Organization", Gorka Sadowski, Mitchell Schneider, John Collins, 24 February, 2020

KEY FEATURES:

24/7 Monitoring & Management:

Provides around-the-clock threat detection, investigation and incident management, including containment and remediation that integrates with your workflows, backed by service level agreements, runbooks and playbooks. A recommended set of security products for endpoints, workloads and networks can also optionally be deployed and managed on your behalf.

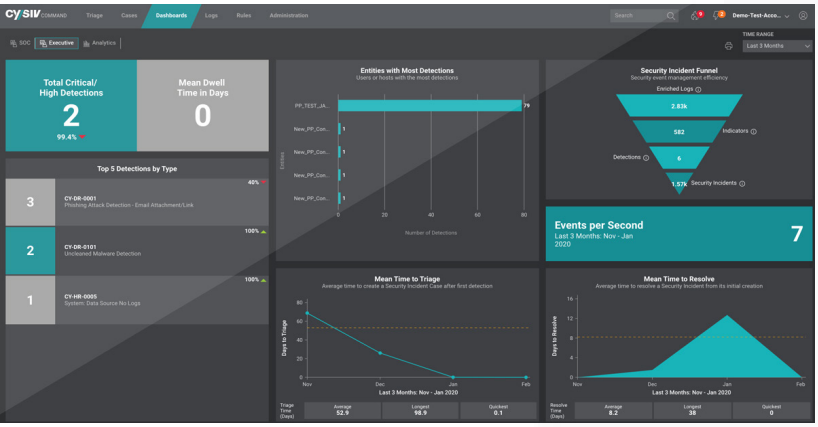
Data, Security and Threat Experts:

Cysiv's team of data scientists and engineers, security analysts and engineers, threat researchers and hunters, and incident response professionals operate as a virtual extension to your team and collaborate to defend your organization, and help further elevate its overall security posture.

Next-gen SIEM Platform:

Our proprietary cloud-native, next-gen SIEM is at the heart of Cysiv SOC-as-a-Service.

- It combines essential SOC technologies — including a SIEM/data lake, security orchestration automation and response, a threat detection engine, user entity behavior analytics, case management, and dashboards and compliance — in a single, integrated, modern SaaS platform.



- The platform fully leverages data science to more efficiently and effectively convert raw logs and data from a broad range of sources into actionable, high-quality, high-confidence detections and security incidents that truly warrant deeper human investigation. Cysiv uniquely relies on a blend of detection techniques, including cyber intel, behavior, statistics, and algorithms/ML, based on the use case. Cysiv data scientists and threat hunters continuously update the threat detection engine with new rules and use cases to ensure the best possible proactive protection from new threats. Customer-defined use cases and rules are also supported.

  By fully leveraging data science and automation, the platform accelerates and improves the process of detecting, investigating, hunting for and remediating threats.

- The multi-tenant platform can be co-managed, allowing you to log-in and directly participate in the full threat detection and response process to the extent you'd like to, alongside Cysiv experts, and to monitor SLAs, access threat intelligence, and dynamically generate persona-based dashboards and reports.

Enterprise Telemetry:

The threat detection process begins with data. Cysiv SOC-as-a-Service is vendor-agnostic, and leverages security and other essential infrastructure and contextual data from a broad range of on-premise, and cloud sources. This improves the breadth, speed and quality of threats detected and helps further accelerate the investigation and response process. Cysiv is vendor-agnostic and leverages a large and growing set of enterprise telemetry sources, including:

- **Security Controls:** Firewalls, IDS/IPS, endpoint security, server, workload and container security, email security, web proxy
- **Infrastructure, Monitoring, and Authentication:** SIEM, cloud (AWS, Azure, Google Cloud), Windows, AD, IAM/SSO, DNS, DHCP, NAT/VPN/Proxy, network metadata
- **Enrichment Sources:** AD object properties / LDAP, asset inventory, configuration and patch management, IoCs, Vulnerability scan results
- **Applications:** Productivity suites (G-Suite, Office 365), database, ERP, CRM, APIs

Cysiv SOC-as-a-Service is a single, comprehensive approach for organizations that lack the staff, expertise, time, technology or other resources to effectively detect and respond to actionable threats, 24/7, or to deploy and manage powerful hybrid cloud and other security.

Threat Intelligence:

A constantly updated and searchable database of actionable threat intelligence, including known bad domains, URLs, and IPv4 and IPv6 addresses is integrated into, and managed from within, the Cysiv next-gen SIEM platform. This threat intelligence, which is curated from over a dozen of the most respected IOC sources worldwide and augmented with IOCs from Cysiv threat research and customer- or community-supplied threat intel, is leveraged throughout the threat-monitoring, hunting and investigation process. It is also leveraged by managed security controls to more quickly and reliably identify known and unknown threats, advanced malware attacks, malicious attacks and other IOCs, before they impact your organization.

Managed Product Stack:

Cysiv can optionally deploy and manage the market-leading solutions for hybrid cloud security SaaS to ensure that all of your workloads – regardless of whether they're in an on-premise, cloud, container or serverless environment – are automatically detected, and instantly provisioned with the appropriate security, without impacting performance. It enables you to build and run applications your way, with security controls that work across your existing infrastructure or modern code streams, development toolchains, and multi-platform requirements:

- **Workload Security:** Runtime protection for workloads (virtual, physical, cloud, and containers)
- **Container Security:** Image scanning in your build pipeline
- **File Storage Security:** Security for cloud file and object storage services
- **Application Security:** Security for serverless functions, APIs, and applications
- **Network Security:** Cloud network layer IPS security
- **Conformity:** Cloud security and compliance posture management

Consumption-based Monthly Billing:

You're invoiced monthly for the services and licenses consumed in the previous month, with no long-term contracts or CapEx, to provide maximum flexibility and savings.

BENEFITS:

Security & Compliance

- Faster, higher fidelity detections result in more timely containment and remediation
- Comprehensive protection from ransomware, advanced malware, insider threats, business email compromise and other threats
- Accelerates the success of workload migration and application development initiatives by addressing important security, operations and compliance issues.
- Improves the maturity of your security operations with capabilities that are essential to a modern, proactive, automated SOC.
- Helps enable cost-effective compliance with a growing set of regulatory requirements (HIPAA/HITECH, PCI DSS, GDPR, CCPA, NIST800-53).

Cost-Optimization

- Provides all of the benefits of having your own highly effective 24/7 SOC, but without the high costs, complexity and challenges that come with building, staffing and operating one.
- Reduces or eliminates the need for a number of security products, threat intelligence feeds, and additional staff.
- Improves the efficiency and effectiveness of your IT / security operations team, enabling them to focus on other priorities, and new or strategic initiatives.

Cysiv SOC-as-a-Service Use Cases:

- Managed Detection & Response (MDR)
- 24/7 security monitoring
- Co-managed, cloud-native SOC / SIEM
- SOC augmentation
- MSSP alternative / augmentation

Continuity and Growth

- Helps make your business more resilient to cyber-attacks and other unpredictable and expensive disruptions.
- Enables you to better respond to new opportunities, grow your business, and leverage the merits of a multi-cloud, container or serverless strategy, without worrying whether cyber security might limit you.

Avoid damaging service disruptions and breaches, and accelerate the success of your workload migration and application development initiatives, with Cysiv SOC-as-a-Service.

To learn more, **visit www.cysiv.com**.

CONTACT US

225 E. John Carpenter Freeway, Suite 450
Dallas, Texas 75062, United States

www.cysiv.com