CYSIV | Google Cloud

CYSIV SECURITY OPERATIONS CENTER (SOC)-AS-A-SERVICE AND GOOGLE CLOUD PLATFORM

DETECTS, INVESTIGATES, HUNTS FOR ACTIONABLE THREATS, AND ENSURES THE SECURITY AND COMPLIANCE OF HYBRID CLOUD WORKLOADS.

PROTECT SENSITIVE DATA AND HYBRID CLOUD WORKLOADS FROM THREATS

Cloud security is a shared responsibility. And while Google Cloud Platform provides best-in-class secure infrastructure, organizations are responsible for complementing this with important measures that more fully protect sensitive data and workloads, and prevent damaging service disruptions caused by a breach or an attack that bypasses existing security controls.

In order to detect actionable threats, organizations must collect, continuously monitor, query and analyze a massive volume of security telemetry and other relevant data for indicators of compromise (IOCs), indicators of attacks (IOAs) and other threats. Doing this at scale, 24/7, across a hybrid cloud environment, cost-effectively, requires a cloud-native next-gen security information and event management (SIEM) system that fully leverages data science and automation, and a team of highly skilled data, security and threat experts that can manage the security operations process.

"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:

Cysiv SOC-as-a-Service combines everything required to detect, investigate, hunt for and remediate actionable threats, and ensure the security and compliance of hybrid cloud workloads:

24/7 Monitoring & Management:

Provides around-the-clock threat detection, investigation and incident management, including active response 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.

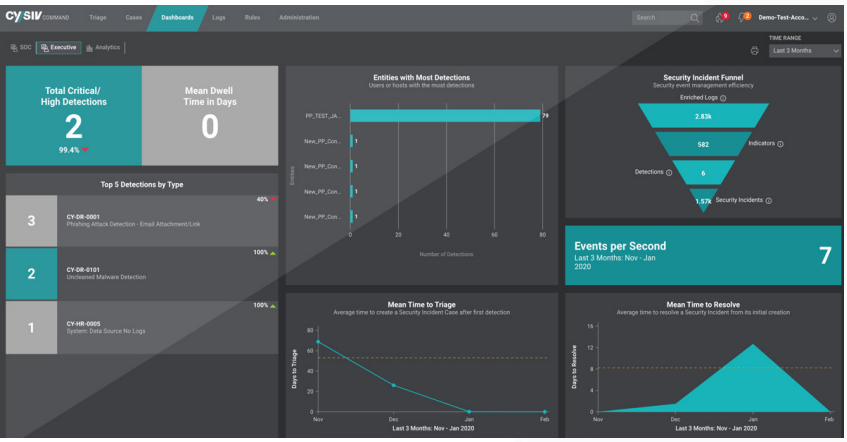
Data, Security and Threat Experts:

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.

- **Key technologies**: Built on Google Cloud Platform, it combines essential SOC technologies — including a SIEM/data lake, security orchestration automation and response (SOAR), a threat detection engine, user entity behavior analytics (UEBA), case management, and dashboards and compliance — in a single, integrated, modern SaaS platform.



- **Data science & automation:** The platform fully leverages data science to more efficiently and effectively convert raw 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.

- **Co-managed:** 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, Google Cloud and other cloud sources. This improves the breadth, speed and quality of threats detected and helps further accelerate the investigation and response process

Cysiv leverages a large and growing set of enterprise telemetry sources, including:

- **Cloud:** Google Cloud, AWS, Azure
- **Google Cloud Platform:** Security Command Center, Cloud Armor, StackDriver, Web Security Scanner, Cloud IAM, Cloud Audit, Cloud Firewall
- **3rd Party Security Products:** McAfee, Trend Micro, Symantec, CrowdStrike, Palo Alto Networks, and many other vendors
- **Applications:** G-Suite and 3rd party apps
- **Other:** SIEM, Vulnerability Management, Active Directory

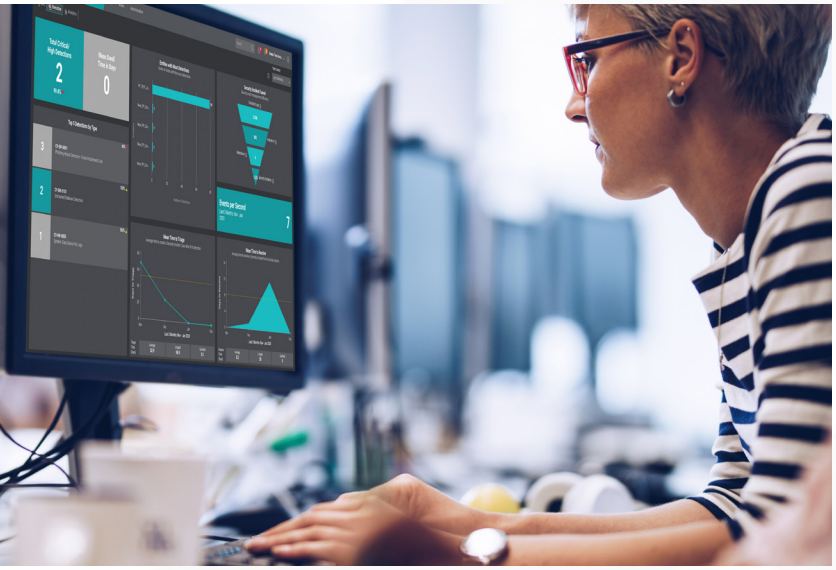
Cysiv SOC-as-a-Service is a single, comprehensive approach for organizations that lack the staff, expertise, time, technology or other resources to effectively detect and respond to actionable threats, 24/7, or to deploy and manage powerful hybrid cloud and other security.

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.



Hybrid Cloud Security SaaS:

Cysiv can optionally deploy and manage the market-leading hybrid cloud security SaaS to ensure that all of your workloads – regardless of whether they're in an on-premise, Google Cloud, other 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.

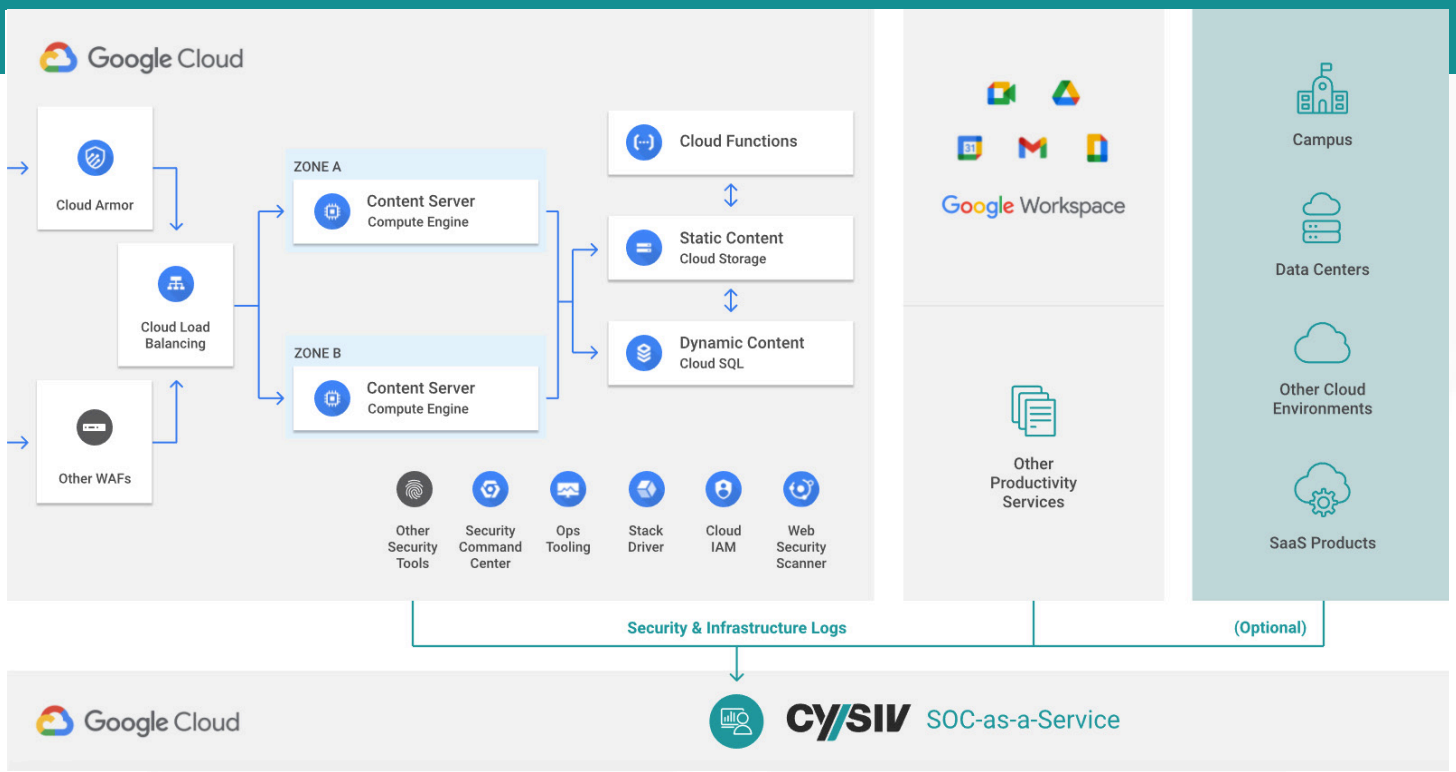
SECURITY SERVICES FOR YOUR MODERN ARCHITECTURE

Cysiv SOC-as-a-Service is designed to support modern enterprise architectures, and hybrid IT environments. The Cysiv platform can readily ingest security and infrastructure logs from:

Different zones, across the Google Cloud Platform, including data from Cloud Armor and other web application firewalls, Web Security Scanner, and other security tools that run on GCP.

G-Suite and other cloud-based productivity tools and applications.

Other cloud environments, including AWS and Azure, as well as from on-premise campus and data center sources.



BENEFITS:

Security & Compliance

- Accelerates the success of workload migration and application development initiatives by addressing important security, operations and compliance issues.
- Comprehensive protection from ransomware, advanced malware, insider threats, business email compromise and other threats
- 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).

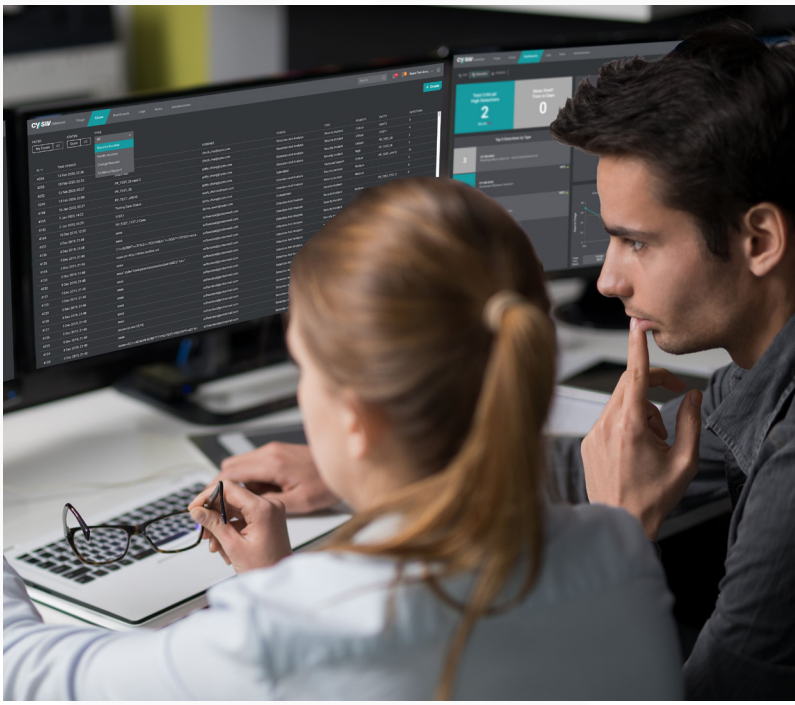
Cost-Optimization

- 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.

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.

Accelerate the success of your workload migration and application development initiatives, and avoid damaging service disruptions and breaches, with Cysiv SOC-as-a-Service and Google Cloud Platform.



CONTACT US

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

www.cysiv.com/google-cloud
google@cysiv.com