The Threat Detection and Response Imperative

The ability to rapidly detect and respond to cyber threats that bypass existing security controls is critical to the growth, success, and resilience of every organization. But doing this well has become more challenging of late for a number of reasons:

- **Modernization of Applications:** The complexity of monitoring modern applications (cloud, containers, serverless and composable infrastructure), and the associated volume of data that needs to be processed and correlated to find the hidden threats, have grown exponentially.
- **Fluid Threat Environment:** The attack surface is very dynamic with cloud, mobile, IoT / IIoT, and work-from-anywhere environments, and it is increasingly difficult to defend against threat actors that are more numerous, more motivated and better armed with more sophisticated and effective weapons.
- **Increasing Security Complexity:** Fully leveraging the data generated from numerous and disparate security solutions that have already been deployed, and correlating and monitoring this data to find indicators of an attack requires specialized tools that are expensive and difficult to integrate and operate effectively.

Overcoming these challenges requires a range of specialized security skills that are difficult to find and expensive to hire, manage and retain. This has created the need for a modern, more effective approach to threat detection and response.

The Importance of Rapid Detection & Response:
The mean time to detect and contain a breach is 287 days, and the average total cost of a breach is $9 million, up 10% from the previous year.

Source: Cost of a Data Breach Report, 2021, IBM Security

Cysiv Delivers: Better Detection and Faster Response of True Threats*

Cysiv is an innovator in delivering SOC-as-a-service. We provide better detection and faster response of true threats across an enterprise's complete IT environment. We do this by combining a data-centric approach, with our modern SOC platform and a response-centric SOC operating model. All of this is delivered as a unified, subscription-based service, with simple, predictable, and flexible pricing, and can be operational in weeks.

> 85% of cases escalated to clients are true threats

< 5 minutes to respond to true threats

** "True threats" are confirmed malicious threats – such as malware, unauthorized access, malicious code, scans and probes, and improper usage – that IT/security teams need to be quickly made aware of and respond to. They are the "needles in the haystack", and are the opposite of the noisy false positives and low fidelity alerts that enterprises are buried in, today.*

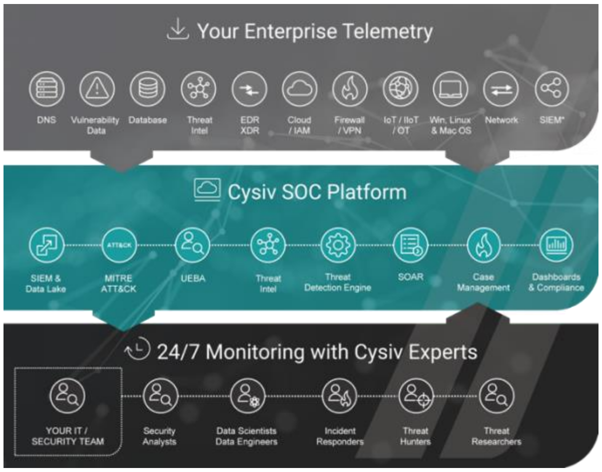
The Cysiv Advantage

Data-centric Approach

We leverage industry-standard frameworks like MITRE ATT&CK to prioritize the data sources that should be ingested for broad or specific TTP coverage, and to identify potential blind spots. We then ingest—at scale, and on day one of client operation—essential data and telemetry from the broadest range of relevant sources to get a more complete view of the threats across your entire IT environment. We automatically enforce a common information model (CIM) to normalize and enrich this data, which maximizes its security detection value, and facilitates faster correlations and threat hunting across multiple data sources.

Modern SOC Platform:

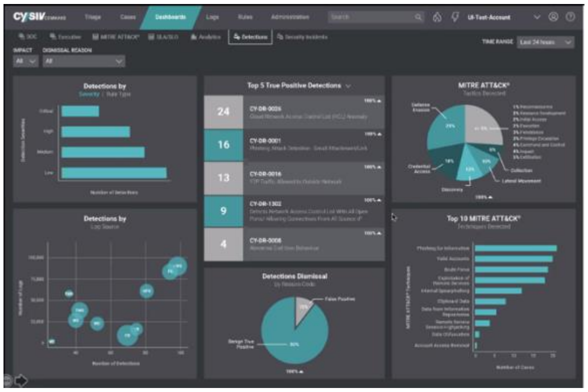
Our cloud-native, next-gen SIEM has been purpose-built to accelerate and improve the threat detection, investigation, hunting, and response process. It combines essential SOC technologies into a single unified platform, and is fully co-managed, ensuring you have complete visibility into these threats and the investigation process, to help further accelerate and improve the outcomes.



The platform uses our advanced two-tier detection engine that applies a blend of five discrete techniques to accelerate and automate the process of accurately identifying true threats that warrant deeper investigation, while weeding out false positives.

Response-centric SOC Model
Our team of experts – including data scientists, data engineers, threat researchers and hunters, security analysts and incident responders – collaborate directly with your team, to ensure the threat detection, investigation and response process meets your specific needs and is continuously improving. We tune the rules for you, constantly add new ones, and help create custom rules on your behalf, to ensure the best possible detection coverage for your organization based on our experience of supporting a global client base and handling complex threats in all kinds of environments.

We augment our machine-led threat detection engine with human-led threat hunting that further improves the threat detection process. And we continuously explore and support new data sources, create new rules, and tune the threat detection engine, while seamlessly delivering new platform features, to ensure the best possible security, risk, and business outcome for you.



Key Use Cases

Cysiv SOC-as-a-Service helps enterprises in each of these situations:

LAUNCH YOUR SOC

You've got the basic security measures in place, but have a small IT/security team, and are under pressure to do more, because of:

- Compliance requirements
- Customer, partner, or investor expectations
- A recent incident, or near miss
- Fear of a data breach or service disruption

PIVOT YOUR SOC

You've got a lot of the elements in place for 24/7 monitoring, but are frustrated with your current approach because of:

- Poor service quality and response
- High false positives / alert fatigue
- Data support / visibility issues
- Long-term, fixed contracts
- Low ROI / Slow time-to-value

ELEVATE YOUR SOC

You've got a 24/7 SOC, with lots of security technologies, but you need to modernize it, and take it to the next level with:

- Higher fidelity alerts, and fewer false pos.
- Automation & data science
- Human-led threat hunting
- Lower SIEM / storage-related costs
- Technology consolidation & savings
- Cloud / SaaS / IoT monitoring

Benefits

Security, Risk & Compliance

- Lower risk of a breach, data theft or service disruption
- Greater visibility of threats across your entire IT environment (multi-cloud, campus, remote, datacenter, IoT/IIoT/OT)
- Helps ensure compliance with key regulations, and enforce data sovereignty requirements

Operational Efficiency & Savings

- Ensures you better leverage your existing security investments
- Enables your IT/security team to focus more time on other high-value initiatives or priorities
- Consolidates and reduces cost to license, configure, integrate, learn, manage, and operate multiple SOC tools

Business Continuity & Growth

- Helps make your business more resilient to cyber-attacks and other unpredictable and expensive disruptions
- Allows you to quickly and cost-effectively scale your security operations to support growth, without disruption
- Enables you to confidently focus more resources on your organization's core business

Company Profile

Security Categories
SOC-as-a-service (SOCaaS)
Managed Detection and Response
Advanced Managed Security Services
Next-Gen SIEM / SIEM-as-a-service

Leadership
Partha Panda – CEO & Co-founder
Justin Foster – CTO & Co-founder

Investors
ForgePoint Capital
Trend Forward Capital

Headquarters
Irving, Texas

Current SOC Locations
USA, India, Egypt

Certifications
SOC 2 Type II, ISO 27001