



Incident Response

Flexible Incident Coverage Options for Your Organization

Minimize the disruption to your operations and keep your security team focused on their current business critical responsibilities when you make Cysigma your partner for incident response. With our professional onboarding, guaranteed service-level agreements for event handling and years of experience helping organizations respond swiftly to incidents, we've got you covered

for any size attack with our Incident Response Retainer Program (IRR).

Your organization will stop breaches faster and recover more quickly from incidents — minimizing damage, cost and harm to the brand — with our experienced professionals applying a best practice framework to your incidents. And the Cysigma team will work side-by-side with your in-house resources throughout the incident, ensuring a seamless process for information sharing and incident resolution.

The Cysigma Advantage

- We offer flexible packages based on your preference for response type, with options for remote and onsite and the ability to repurpose unused hours for other incident readiness and threat services.
- The Cysigma Incident Management Framework was built from industry best practice standards (NIST, SANS, ISO, PCI)
- We provide regular updates through your incident manager through the lifecycle of the response and generate a detailed incident report, explaining all evidence collected, significant findings, chain of custody, etc.
- Cysigma team can interact with law enforcement or legal counsel to expedite those processes
- 24/7/365 call support is available through Cysigma-staffed SOCs
- The Cysigma team will be an extension of your in-house resources, working side-by-side with staff during the incident
- Smooth handoff to available resources for Restoration and Recovery

Proof Points

Tenured IR professionals with experience handling real-life incidents

35+IRR retainer clients

250,000 hours of Threat Services delivered to clients

How We Do It

Professional Onboarding

We'll document key contacts, review security environment/technologies, establish secure data transfer protocols and discuss evidence collection/handling procedures

Four-Hour Remote SLA

Many of incident handling services can be executed fully remotely, so this fast response will get you quickly on the road to containment and recovery

Onsite SLA

If you select the standard package and need onsite support, we'll arrive with experienced personnel ready to take immediate action

Incident Manager for Each Event

Your single point of contact for planning, updates and questions throughout your incident and the reporting process

Repurpose Unused Hours

At any point in time during the retainer, no later than 30 days prior to renewal, select from our menu of proactive threat/incident readiness options

Cyber Threat Intelligence Report (daily/weekly/ad hoc)

Our detailed intelligence reporting with clear threat rankings, which helps teams act quickly to prioritize and defend their organization using reliable and trusted threat information

Containment and Isolation

Our containment and isolation practices will help regain control of infrastructure, limit attackers' actions and minimize impact to operations

Media and Forensics

Cysigma's review and analysis of binary applications to determine malware capabilities

Day 0/1 Response Team

We provide a rapid tactical response through our Day 0/1 Response Team for clients on retainer, including assistance deploying technology to hunt for threats in your environment

Incident Response Retainers

Packages that include remote-only response:

Remote-only Response Package	• 100 retainer hours	• 4-hour remote SLA
1 Remote-only Response Package	• 150 retainer hours	• 4-hour remote SLA •
2 Remote-only Response P	• 200 retainer hours	4-hour remote SLA

Packages that include options for onsite or remote response:

Standard Package 1	• 100 retainer hours	• 4-hour remote SLA • 48-hour onsite SLA
Standard Package 2	• 150 retainer hours	• 4-hour remote SLA • 24-hour onsite SLA
Standard Package 3	• 200 retainer hours	• 4-hour remote SLA • 24-hour onsite SLA

No-Cost Retainer

Get the advantage of rapid IR engagement with the Cysigma team	• Includes business-related documentation needed to scope and engage rapidly • Rate is pre-determined, cost is provided after scoping • No SLA, no included retainer hours
--	--



CYSIGMA PVT LTD

Secure greatness®

Cysigma is a leading company in cybersecurity, helping businesses in different industries with strategic and technical guidance. We work closely with organizations to develop, implement, and manage effective cybersecurity programs. Our services include creating strategies, managing security, assessing risks, integrating solutions, and leveraging technology. By putting clients at the center of our approach, which includes people, products, partners, and programs, we drive business growth in a special way. At Cysigma, we handle and minimize cyber risks to unlock the full potential of your business. For more information, visit www.cysigma.com.