

# New Ransomware Incident Response Service Bundle

A cost-effective and complete solution to ransomware incidents

Kivu has created a new incident response packaged service for ransomware incidents to provide partners and clients with greater transparency, cost control and more efficient service delivery.

## Cost-effective investigations that follow best practice

In the current market, a lower rate is often seen as a measure of cost savings to the client or insured. However, as scope creep sets in, or important services are omitted, clients are often faced with unexpected extra costs, ineffective incident response (IR), or results that do not comply with the necessary regulations.

At Kivu our services have always been structured to deliver comprehensive and complete incident response. Our fixed price model offers professionalism in service and certainty in rate.

## A new delivery model

Kivu is taking the guesswork out of IR pricing and commits to complete transparency in our service delivery. We have implemented a fixed price structure for ransomware incidents while still maintaining billing flexibility for clients who prefer a by-the-hour model.

Our ransomware IR service is bundled into packages tiered by the size of the affected environment. No need for multiple vendors, no need for price-adjustments – a complete solution that provides our quality services at a defined price point and clarifies the scope of service delivery from the outset.

No surprises, no broad budget figures, no scope creep

Clarity on service inclusions and cost drivers

Kivu bears the risk of cost overrun



Kivu is a Money Services Business (MSB) registered with the U.S. Treasury. If a ransom payment is needed, Kivu's status as a MSB ensures the highest degree of OFAC due diligence and regulatory compliance.

## How we deliver

All Kivu investigations are structured to deliver consistent and high quality investigations to clients of all sizes. Engagements are tiered into four categories, based on the size of the network and number of sources of compromise in the incident.

Investigations consist of the following deliverables:

- 1 RESPONSE TO ATTACKER'S DEMAND**
  - Determining whether attack can be remediated and data recovered without paying the ransom. Insight and due diligence on the attacker.
  - If required, facilitation of ransom payment (up to USD\$10M).
- 2 REMOTE DECRYPTION**
  - Remotely assisting the client and their in-house IT team with the decryption and recovery of data, and system remediation.
- 3 THREAT MONITORING AND DETECTION DURING THE INCIDENT**
  - Deployment of endpoint monitoring solution to block further malicious activity during the investigation. *Optional for Tier 1*
- 4 FORENSIC INVESTIGATION**
  - Remote collection and analysis of relevant log data, forensic images and artifacts. Identification of attack source and vector.
  - Assessment of whether data was accessed or stolen.
- 5 REPORTING**
  - Provision of regular updates throughout, with written reports upon request.

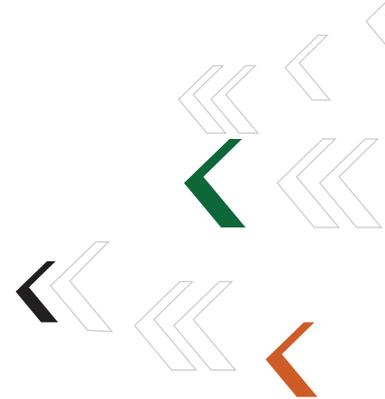
## What makes Kivu's investigations best practice

At Kivu, we combine insight gathered from over 700 ransomware cases, commitment to legal compliance, in-house threat intelligence, patented evidence collection tools and a fixed price package offering best-in-class professional service.

Engaging Kivu for incident response means:

- Access to global capacity, with response teams in the US, Canada and Europe.
- Best practice investigations, with end-to-end case management and consistent service delivery.
- Secure and swift preservation of crucial evidence and restoration of digital operations.

Our fixed price model also works in step with our premier Post Breach Remediation services to reduce business interruption and restore client operations.



## About Kivu

Kivu is a leading global cyber security firm that offers a full suite of pre- and post-breach services, specializing in the forensic response to cyber-attacks and ransomware incidents. We deliver cutting edge cyber security solutions to organizations in need and are a trusted cyber incident partner to insurance carriers and law firms worldwide.

[KIVUCONSULTING.COM](https://www.kivuconsulting.com)  

**CONTACT US**

Our purpose is to restore freedom of operation and to minimize business interruption, getting organizations back online quickly and securely. Contact us to learn more at [info@kivuconsulting.com](mailto:info@kivuconsulting.com).