Thrive Secure IR
Incident Response & Remediation

Challenge

Thrive Incident Response & Remediation provides on-demand security response services to contain and remove threats, along with engineering assistance to rebuild and restore critical systems. The service provides faster recovery time from a cybersecurity incident so that the costs associated with business disruption are minimized.

Thrive Incident Response & Remediation requires an Incident Response Retainer that ensures Thrive and the Client are prepared prior to an incident. The retainer entitles the Client to a dedicated Incident Responder from the Thrive Security Operations Center (SOC) in the event of a security incident. Thrive will collaborate with the Client on pre-incident planning, will pre-deploy the Thrive incident response agent on Client systems, and proactively run an automated compromise assessment that will hunt for threats currently in the environment.

In the event of an incident, the Thrive SOC team will assess the incident's scope and provide an estimated scope of work for any response and remediation tasks that exceed the standard scope of the Client's services with Thrive. These threat containment and remediation services are an additional cost not included in the retainer.

Discounted or Free Retainer

Thrive will automatically apply a discount to the monthly retainer price for clients that use our managed security and advisory services. Subscribe to a service from all three categories and receive the IR Retainer for no additional monthly cost.

Discount Type	Required Thrive Services	Retainer Discount
Information Security Program Discount	Virtual CISO (minimum 8hr monthly)	25%
Attack Surface Reduction Discount	Vulnerability Management *and/or* Autonomous Penetration Testing	25%
Detection & Response Discount	Endpoint Security & Response *and/or* Managed Detection & Response	50%
	Total Discount Available	**100%**

Discounts only apply to the retainer and do not apply to incident response and remediation project cost quoted at the time of an incident. The discount is applied to the client's monthly invoice for any month in which the service conditions are met. Specific SKU requirements are subject to change. Please contact your Thrive representative for a complete list.

(continued)

Thrive's Incident Response & Remediation services include:

- **Pre-Incident Planning**
  Thrive security experts engage with subscribed clients to ensure that they have an approved incident response plan, an asset inventory prioritized based on business impact and a backup strategy for critical systems

- **Incident Response Tools**
  Upon working together, an incident response agent is installed on systems prior to an incident. These advanced tools ensure potential threats are contained faster and provide high value forensic artifacts

- **Compromise Assessment**
  Thrive conducts an automated compromise assessment during onboarding to identify current threats that may impact systems

- **Prioritized Incident Management**
  Users can report an incident with a 15-minute response time guaranteed from the Thrive SOC to begin threat assessment and scoping

Comprehensive P1 technical post incident report, including cyber malware analysis

Cybersecurity Insurance

Cybersecurity insurance will typically cover the costs associated with incident response, but insurance companies usually call in their own IR partners to take the lead. This is good for the insurance company, because they have pre-negotiated rates and can control the process. The downside for companies utilizing these services is a) an outside firm is coming in without knowledge of the infrastructure or the business and will take time to get up to speed b) these firms are security specialists and will consider their work complete when the initial threat is contained and removed, leaving the client to restore their business operations.

Thrive can supplement the work of the insurance company's forensics provider and bridge gaps in service by

- providing immediate response actions before the 3rd-party is engaged
- working with the client to restore services after the 3rd-party has moved on.

About Thrive

Thrive delivers global technology outsourcing for cybersecurity, Cloud, networking, and other complex IT requirements. Thrive's NextGen platform enables customers to increase business efficiencies through standardization, scalability, and automation, delivering oversized technology returns on investment (ROI). They accomplish this with advisory services, vCISO, vCIO, consulting, project implementation, solution architects, and a best-in-class subscription-based technology platform. Thrive delivers exceptional high-touch service through its POD approach of subject matter experts and global 24x7x365 SOC, NOC, and centralized services teams. Learn more at **www.thrivenextgen.com** or follow us on **LinkedIn**.