SERVICE BRIEF

Digital Forensics & Incident Response

HERJAVEC GROUP

Experiencing an Immediate Security Incident?
Call 1-877-275-5549 or complete our web form at herjavecgroup.com/immediate-incident-support

Herjavec Group has practical experience addressing and managing the most complex security breaches. Through timely and strategic response to security incidents, Herjavec Group reduces recovery time, costs and damage.

HG Digital Forensics & Incident Response Services can be leveraged on an emergency basis, or as an integral part of your proactive cybersecurity program through our HG IR Retainers. Not only does an HG IR Retainer complement the resolver group initiation in our HG MSS offering, pending the remediation required, but it provides peace of mind and accelerated response times for expert level support when your enterprise needs it most.

Why Choose an HG Incident Response Retainer?

- Ultimate flexibility – retainer packages can be dedicated to additional HG services such as Table Top Exercises, Incident Response Planning and Advisory Services
- Budgeted line item with no surprises
- Shortened SLA's for Incident Response
- Seamless transition and collaboration between HG MDR, HG Threat and HG SOC experts supporting your HG Managed Security Service
- Coordinated program alignment in advance to save time and resource when you need it most

Why Trust HG To Lead Your Incident Response?

Herjavec Group's Incident Response Retainer Service is modeled after NIST SP800-61r2 and ISO 27035. Service differentiators include:

When an incident occurs, we respond with a customized response team.

We bolster your existing tools and processes with our state-of-the-art networking, discovery, and forensic tools. Our flexibility provides a faster, more effective response. We maintain a neutral perspective throughout our response delivery.

We are on-site offering a high-touch response.

While we can provide remote triage and expertise across multiple security domains, we believe that on-site presence is critical to managing an incident, interacting with management and ensuring the best outcome overall.

We do not abandon you once the incident is closed.

When a complex incident occurs, Herjavec Group follows through on recommendations and supports you through the entire cycle of remediation as required. This includes providing you with the consultation and technical expertise needed throughout the remediation process.

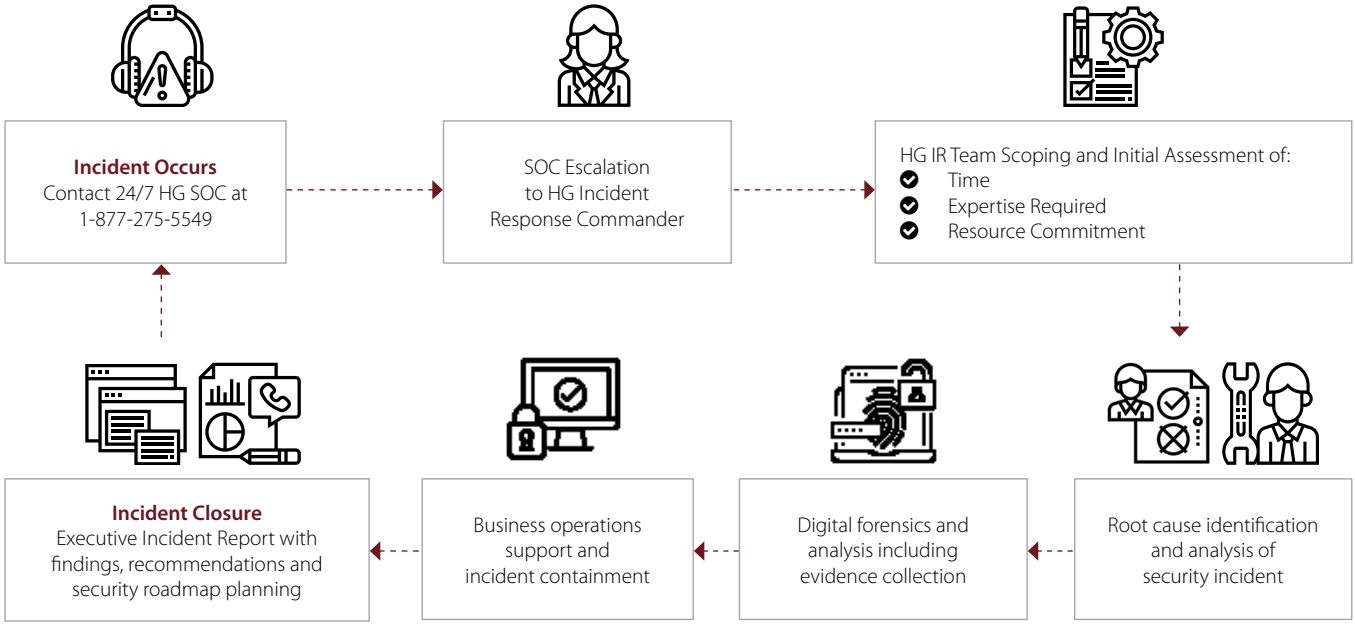
Our retainer hours are flexible and can be dedicated to additional cybersecurity services.

Rest assured knowing that your investment with HG can be leveraged for Incident Response support as needed or dedicated to additional services, such as tabletop exercises and Incident Response planning.

> "Within 12 hours we had Herjavec Group on site helping us troubleshoot, taking control of the situation, and helping us with an incident response management plan"
>
> - VP of Technology at Goldcorp Inc

> "We found the Herjavec Group's creativity, knowledge and professionalism to be a great asset in both identifying our network security weaknesses and also in educating our staff on identifying targeted attacks."
>
> - Scott Powers, Director of Information Technology at the Dallas Mavericks

HG IR PROCESS



Through Herjavec Group's years of experience in handling incidents, we have found that a typical incident lasts approximately 5 days and can be resolved with the support of an Incident Controller and two Incident Handlers from Herjavec Group.

The Incident Commander will determine the size of the Incident Response team during your initial call. The size of the team may change throughout the handling of the incident. For each incident, there will be a daily call between your organization's contact, the Incident Controller, and the Incident Commander to determine if the incident is resolved and the response services are no longer needed.

Communication during this emergency time is critical. Over the course of the incident response, you can expect to receive daily updates on:

- The status of the incident
- Completed, current and planned activities
- Hours accumulated on the project
- Recommendations on next steps, including staffing requirements

Following the incident closure, Herjavec Group will deliver a summary incident report that includes:

1. Incident timeline as discovered throughout the response
2. Activities executed during the incident
3. Recommendations to prevent the incident from happening again, to make the environment more secure and security roadmap planning for future consideration

Incident Commander

Your first point of contact to understand the scale and scope of the incident. In contact with you and incident controller daily to understand status and support the team daily.

Incident Controller

On-site resource responsible for tracking activities and providing daily reporting on the progress of the incident handling.

Incident Handler

The resources working on the incident itself. Specifically selected based on their skill and experience. The skills include incident detection/analysis, incident control/handling, containment, eradication/recovery, and forensic investigation/root cause analysis.

HG INCIDENT RESPONSE RETAINER PACKAGES

Herjavec Group four incident Response Retainer Packages with predetermined hourly rates and SLA requirements. The block of hours included with each package can be dedicated to any Incident Response Service.

Retainer Packages

Package	Hours Included	Remote SLA	On-Site SLA	Project Management	Expiration
Silver	135	24 hours	Best Effort	Included	12 months
Gold	235	4 hours	48 Hours	Included	12 months
Platinum	335	4 hours	24 Hours	Included	12 months
Custom	Adjustable	Adjustable	Adjustable	Included	12 months

Notes:

- Hours are available for any **HG Incident Response Service**
- Minimum 40 hours consumption at one time
- Travel and expenses not included
- SLAs as indicated are for Emergency Incident Response only

CUSTOMER SUCCESS STORY:

World-Class Developer and Operator of Luxury Resorts

A publicly traded, world-class developer and operator of luxury resorts fell victim to a cyber attack by a foreign government adversary. Over the course of a four day period, key computing networks were dismantled, resulting in millions of dollars in damages. The attack is an example of a frightening trend: governments hacking private, for-profit companies.

The firm turned to a number of security providers at this critical time and none were willing to come in, assess, remediate and provide executive consulting without exploiting the firm by selling brand new product.

Within 48 hours, Herjavec Group assembled a team on-site to scope, contain and remediate the threat and restore the firm to business operations. From there, a successful partnership in security was established.

Services Provided:

- **Incident Response**
- **Executive Consulting**
- **Network Security Assessment**

Industry:
Hospitality

Users:
51,000+

Operating Locations:
Worldwide

Annual Revenue:
$14B

HERJAVEC GROUP

Robert Herjavec founded Herjavec Group in 2003 to provide cybersecurity products and services to enterprise organizations. We have been recognized as one of the world's most innovative cybersecurity operations leaders, and excel in complex, multi-technology environments. We have expertise in comprehensive security services, including Advisory Services, Technology Architecture & Implementation, Identity & Access Management, Managed Security Services, Threat Hunting & Management, Digital Forensics and Incident Response. Herjavec Group has offices and Security Operations Centers across the United States, United Kingdom, Canada and India. For more information, visit HerjavecGroup.com or contact us at info@herjavecgroup.com.