WHAT WE DO…

We offer a comprehensive range of risk assessment/ management services, cyber audits, and policies & procedures drafting and review. Our expertise includes employee, customer, and vendor training, as well as online, space, and physical security. We specialize in database management, intrusion monitoring/detection, incident responses, and forensic management. With system testing/hardening, HMI development, and SCADA security, we ensure robust protection. Additional services include off-site back-up & recovery, robotic surveillance, GSaaS (Ground Support as a Service), and more. Rely on our tried, true, state-of-the-art tools and techniques to safeguard your investments effectively.

Houdini Security Global

"Once you've called the rest, call the best"

Data Center – So. California

Tech Center (labs) – No. Ohio

website: www.hsglobal.org

e-mail: info.hsglobal@proton.me

Houdini Security Global

"Once you've called the rest, call the best"

Data Center – So. California

Tech Center (labs) – No. Ohio

website: www.hsglobal.org

e-mail: info.hsglobal@proton.me

#7-
Incident Response

Our incident response services are crucial for safeguarding your organization's digital assets. In the event of a security breach or cyberattack, our dedicated team promptly analyzes and addresses the situation, minimizing potential damage. By employing a systematic approach, we ensure that the incident is contained, investigated, and resolved effectively. Our incident response services offer you peace of mind by providing expert support and continuous protection against emerging threats, keeping your operations secure and resilient.

Houdini Security Global

"Once you've called the rest, call the best"

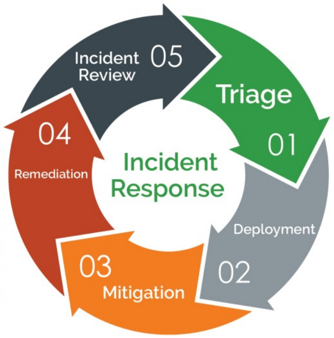
Data Center – So. California

Tech Center (labs) – No. Ohio

website: www.hsglobal.org

e-mail: info.hsglobal@proton.me

Offering Cyber/IT/SCADA/ IoT/Satellite/Mobile Phone/ Physical security products & services



Incident Response at a glance…

In today's increasingly connected digital landscape, the risk of cyber threats is ever-present. The potential damage from a security incident can be catastrophic, affecting not just the IT infrastructure but also your brand reputation, customer trust, and bottom line. Recognizing this need, we offer a comprehensive Incident Response as a Service (IRaaS) tailored to protect, detect, respond, and recover from any cyber incidents, ensuring that your business remains secure and resilient.

THERE'S MORE…

1. Prevention and Preparation

a. Threat Intelligence and Risk Assessment

- Continuous monitoring and analysis of the global threat landscape.
- Identification of vulnerabilities specific to your organization's systems.
- Development of proactive strategies to mitigate potential risks.

b. Incident Response Planning

- Creation of a customized incident response plan (IRP) detailing roles, responsibilities, communication protocols, and procedures.
- Regular review and updates to ensure the IRP is aligned with the evolving threat landscape.

c. Training and Awareness

- Training your staff in recognizing and reporting potential threats.

Conducting regular drills and simulations to ensure readiness in the event of an incident.

2. Detection and Analysis

a. 24/7 Monitoring

- Real-time monitoring of your systems, networks, and applications for signs of suspicious activity.
- Utilization of cutting-edge detection technologies and methodologies to identify potential incidents quickly.

b. Incident Analysis

- In-depth investigation of detected anomalies to confirm and classify the incident.
- Gathering evidence and determining the scope and potential impact of the threat.

AND FINALLY…

3. Containment, Eradication, and Recovery

a. Immediate Response

- Rapid containment of the incident to prevent further damage or spread.
- Coordination with key stakeholders to ensure transparent communication and effective action.

b. Eradication

- Identification and removal of malware, compromised accounts, and other threat actors.
- Comprehensive analysis to ensure complete elimination of the threat from the environment.

c. Recovery

- Restoration of affected systems, data, and services to their pre-incident state.
- Ongoing monitoring to ensure no remnants of the threat remain.

d. Post-Incident Support

- Continuous support and guidance to ensure long-term resilience against future incidents.

Recommendations and implementation of enhanced security controls and practices.

4. Post-Incident Analysis and Reporting

a. Forensic Analysis

- Detailed forensic examination of affected systems to understand the incident's nature, origin, and evolution.
- Preservation of evidence for potential legal or regulatory requirements.

b. Lessons Learned and Continuous Improvement

- Comprehensive review of the incident response to identify strengths and areas for improvement.
- Integration of lessons learned into the existing IRP and security practices.

c. Compliance and Reporting

- Creation of detailed incident reports, including actions taken, outcomes, and recommendations.

Ensuring compliance with regulatory requirements such as GDPR, HIPAA, and others by following prescribed reporting procedures.

5. Partnership and Consultation

a. Dedicated Team of Experts

- Access to a dedicated team of cybersecurity professionals with diverse expertise and experience.
- Collaboration and guidance at every step, from preparation to recovery.

b. Strategic Consultation

- Ongoing consultation to align your security posture with your business goals and industry best practices.
- Providing insights and recommendations based on emerging trends and threats.