SYGNIA

ARMIS®
THE Cyber Exposure Management & Security Company

Inc. POWER PARTNER 2022

RECOGNIZED BY
Gartner FORRESTER®

INCIDENT RESPONSE AND RETAINER SERVICES

When confronted with a breach, you need the best team at your side.

Sygnia's global incident response teams have a proven track record of swiftly containing and defeating cyber attacks, minimizing business disruption, and guiding organizations through the crisis.

PROVEN BENEFITS

- **Swiftly contain and defeat cyber attacks**
- **Minimize business disruption and damage**
- **Effectively manage the crisis**
- **Emerge from the crisis stronger**

Whether the threat-actor is a criminal group, a state-sponsored actor or an insider threat, Sygnia helps clients swiftly investigate, contain and eradicate the attacker. Sygnia deploys top talent with digital combat experience from elite military units and a deep understanding of threat-actor tactics.

> “Often described as a cyber security Delta Force…(Sygnia) has developed a reputation for speed and decisiveness in responding to attacks and helping Fortune 100 companies build their cyber resilience.”
>
> **Forbes**

THE SYGNIA ADVANTAGE

Attacker Perspective

We employ only highly experienced A teams with extensive nation-state level cyber warfare backgrounds, offensive and defensive capabilities, and decades of incident response experience. Our teams outthink, outmaneuver, and outpace attackers.

Technological Superiority

Our agile teams effectively respond to incidents in any environment, across all IT or security stacks, and have experience in cloud, application, CI/CD, OT, mobile, and IoT. Sygnia also developed a proprietary crossplatform MDR that is used to augment a client’s existing security tools when needed.

Combat-Proven Methodology and Rapid Response

Sygnia’s modus operandi is the product of extensive cyber combat experience. Our incident response methodology encompasses parallel execution of the wide variety of activities needed to handle an attack: investigation and forensics, containment, tactical negotiation, remediation and recovery, executive crisis management, litigation support, and post-breach threat monitoring.

Advanced Threat Research Team

Threat research and continuous monitoring of the global threat landscape is incorporated into Sygnia’s incident response efforts, ensuring effective forensic investigations and revealing novel threat actors to the global security community.

RAPID, MULTIPRONGED RESPONSE

When an organization is under attack, every minute counts. Sygnia commences activities in multiple workstreams to accelerate incident resolution. To enable a highly robust and agile response, Sygnia executes all workstreams in parallel, orchestrates among them, and manages the incident end-to-end.

Executive Crisis Management

Sygnia collaborates with executive leadership to manage the crisis and provide evidence-based answers to stakeholders, employees, and the general public. In parallel with technical resolution streams, Sygnia supports executive crisis management including legal, regulatory, PR, and internal management efforts.

Containment

A critical step is to quickly ensure areas of the environment that have not yet been impacted by the attack will not be compromised. Investigative findings are leveraged to rapidly contain the threat and prevent further damage to the business.

Investigation

Sygnia performs triage and investigation to identify the initial entry point, the scope of compromise, how the attack propagated through the environment, the tools used by the attacker, and the current threat level. Our responders rapidly and effectively identify attack vectors, timelines, and attacker capabilities that must be remediated.

Tactical Negotiation

Sygnia leverages expert negotiators to gain critical time and feed valuable information from the attacker back to the technical investigative team. This approach serves not only to significantly lower ransom demands, but also to substantially improve the speed of technical investigation and recovery efforts.

Remediation and Recovery

Recovery efforts are initiated immediately, in parallel with the initial investigation. By leveraging a “secure island” environment in which key services are re-created before the compromised method has been cleared, the organization can return to full business operations much faster. The remediation effort closes security gaps and eradicates the attacker’s presence in the environment.

Threat Monitoring

Attackers may attempt additional malicious actions at any time. To minimize this risk, Sygnia’s incident response team performs tailored threat monitoring throughout and after an incident, to ensure additional malicious activities and re-entry attempts are detected and blocked immediately.

SYGNIA'S INCIDENT RESPONSE RETAINER

PREPARE SMART. ACT FAST.

Sygnia's Incident Response Retainer (IRR) provides predetermined critical engagement parameters that decrease the resolution time of a cyber incident. They enable Sygnia's team to hit the ground running and immediately initiate response efforts when an incident occurs.

RETAINER BENEFITS

- **Ensure peace of mind**
- **Shorten response time**
- **Lower response costs**
- **Improve response effectiveness**
- **Enable continuous improvement**

SYGNIA IRR ADVANTAGE

Onboarding and Discovery | **Rapid Response SLAs** | **Tailored Activation Playbook**

Service Tier Options – 3 Months Retainer Term	Essential
IR-ready relationship with pre-established Ts & Cs	●
24/7 IR notification hotline	●
Onboarding and discovery	●
IRR activation playbook	●
Remote response time SLA	4 hours
En-route response time SLA	48 hours
Prepaid IR support time	20 hours**
Discounted rate for IR services	5% discount off regional standard

**20 hours included in the event of a first major incident that requires over 100 hours.

SYGNIA

ARMIS
THE Cyber Exposure Management & Security Company

Sygnia is the foremost global cyber readiness and response team, applying creative approaches and battle-tested solutions to help organizations beat attackers and stay secure. Sygnia is a trusted advisor and service provider of technology and security teams, executives and boards of leading organizations worldwide. Learn more at Sygnia.co.

A TEMASEK COMPANY AND MEMBER OF THE ISTARI COLLECTIVE

TEMASEK ISTARI

24/7

INCIDENT RESPONSE COVERAGE

Suspicious of an incident? Call +1-877-686-8680 now. Learn more at www.sygnia.co