SYGNIA

Witz Cybersecurity
Australia & New Zealand Partner

RECOGNIZED BY Gartner FORRESTER

INCIDENT RESPONSE

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.

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.

PROVEN BENEFITS

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

> 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 are able to out-think, out-maneuver and outpace attackers.

Technological Superiority

Our agile teams effectively respond to incidents in any environment, with any IT or security stack. Our experience includes cloud, application, CI/CD, OT, mobile, and IoT. Sygnia has also developed an advanced, proprietary crossplatform XDR that is used to augment the client's existing security tools when needed.

Combat-Proven Methodology and Rapid Response

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

SYGNIA's 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 is able to execute all of the workstreams in parallel, orchestrate among them, and manage the incident end-to-end.

Executive Crisis Management

Sygnia teams with executive leadership to lead through the crisis and provide accurate answers to stakeholders, employees, and the general public. In parallel with technical incident resolution streams, Sygnia supports executive crisis management including legal, regulatory, PR and internal management efforts.

Containment

It is critical to quickly ensure that areas of the environment that have not yet been impacted by the attack, will not be compromised. This can be achieved by segregating or quarantining them. 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. Sygnia rapidly and accurately identifies 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 identifies and closes security, and the attacker’s presence in the environment is eradicated.

Threat Monitoring

Attackers may attempt additional malicious actions at any time. To minimize this risk, Sygnia’s incident response team performs tailored 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

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.

Sygnia's IRR (tier 2 and above) includes an onboarding session with every new client. The session includes a high-level review of the client's network and IT architecture, critical systems, secure data sharing, and access processes. Response guidelines are defined and captured by Sygnia in a client-specific IRR activation handbook that enables an accelerated incident response.

RETAINER BENEFITS

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

SERVICE TIERS

Sygnia provides four different retainer service tiers so clients can choose the tier that best aligns with their business needs

	Tier 1	Tier 2	Tier 3	Tier 4
Signed agreement with terms and conditions	●	●	●	●
24/7 IR notification hotline	●	●	●	●
Deployment of Proprietary Technologies	●	●	●	●
IRR onboarding session	○	●	●	●
Remote response time SLA	Best effort	6 hours	4 hours	2 hours
En-route response time SLA	Best effort	48 hours	24 hours	24 hours
Prepaid IR support time	○	100 hours	200 hours	300 hours
Discounted rate for IR services	Standard rate	10% discount	15% discount	20% discount
Retainer Term	1 Year	1 Year	1 Year	1 Year

SYGNIA IRR ADVANTAGE

Multiple Tiers to enable alignment with organization's needs

Onboarding Process designed to ensure seamless response

Rapid Response SLA

100% Utilization of retainer hours: can be repurposed for any Sygnia service

Dedicated Account Manager

Complementary Services for IRR clients

FLEXIBLE UTILIZATION OF RETAINER HOURS

Unused IRR hours can be repurposed towards any other Sygnia services. Sygnia also offers a set of services designed specifically for IRR clients, that includes executive tabletop wargames, technical tabletop wargames, joint triage and escalation exercises, and adversarial simulations.

Australia & New Zealand Partner

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