Symantec | CYBER SECURITY SERVICES

DATA SHEET

Incident Response

Retainer Subscription, Emergency Response, and Readiness Services

Why Do You Need Incident Response?

A Compromise Doesn't Have to Equal Disaster. It's well known that the threat landscape is populated with highly skilled, well-funded, and motivated adversaries whose only job is to overcome your security measures to steal, deliver malware, and generally disrupt your business activity. When compromised, you need to respond quickly to understand the scope and impact of the incident and know that it has been contained and eradicated.

Preparation is Key. When security incidents occur, response teams face immense pressure to outmaneuver and defeat skilled opponents while also juggling the needs of stakeholders. Manual disjointed efforts challenge and stretch the capabilities of your security team who may or may not be able to remediate the incident. Successful incident response requires consistent plan execution that's well orchestrated, measurable, repeatable, and optimized. The ability to respond is improved when everyone knows his or her role and the right process to follow. This minimizes business disruption, brand damage, and data loss while reducing the operational impact to respond. Symantec™ Cyber Security Services: Incident Response provides Readiness Services such as Incident Response Plan Assessments, Tabletop Exercises, and Advanced Threat Hunting to help our customers build and refine their incident response plans and turn them into proactive programs.

Act with Speed and Precision. The global Symantec Incident Response team is a proven and experienced team of experts and is backed by Symantec's Global Intelligence Network and rich Symantec Cyber Security Services: DeepSight™ threat and adversary intelligence. Symantec Emergency Response Services provides remote and/or on-site investigation support to help organizations without a Retainer to quickly mitigate the impact of an incident and quickly restore business as usual. Incident Response Retainer Services is an annual subscription that includes onsite readiness services, pre-negotiated terms, and SLAs all to enable customers to resolve incidents quickly, prevent reoccurrence, and keep executives informed.

> "The skills, professionalism and recommendations provided by Symantec's Incident Response team were instrumental in our ability to respond effectively and were the best we have ever experienced.
>
> — VP of Information Systems, Large Insurance Company

If you are currently experiencing an incident and need response assistance, contact: incidentresponse@symantec.com or call

United States – 855-378-0073
United Kingdom – 0800 917 2793
Singapore – 800-120-6718
Australia – 1-800-481-774
Japan – 0066-33-813303

Benefits

- Improve Response Times
- Lower Response Costs
- Improve Response Effectiveness
- Enable Continuous Improvement

Retainer Features

- Specialized service management from experienced service liaisons who are experts in your industry and will manage your incident from beginning to end.
- Emerging Threat Reports with expert analysis of the threat landscape and potential impacts to help you proactively prepare for or mitigate attacks.
- Insights from Symantec DeepSight™ Intelligence and the Symantec Global Intelligence Network to enhance response efforts.
- Performance SLAs to ensure critical resources are available when you need them.
- Documentation of response actions and recommended post-incident improvements.
- Post-incident technical and management briefings and lessons-learned sessions.

Available Services

- **Emergency Response** – Incident Response Services on an as-needed basis.
- **Incident Response Retainer** – Subscription service for proactive response readiness and investigation needs.
- **Incident Readiness Assessment** – Assessment of existing ability to respond, as well as recommendations on how to reduce the time between incident detection and resolution.
- **Incident Response Tabletop Exercises** – Onsite testing and refinement of your response plan and process.
- **Incident Response Plan Development** – Create a response plan to minimize the impact of security incidents and shorten the timeframe between incident identification and incident resolution.
- **Incident Response Plan Assessment** – In-depth assessment of Customer's information security incident response plan to determine current and future needs.
- **Advanced Threat Hunting** – Proactive search across your network to uncover and eradicate the presence of compromises and threat activity previously unidentified in your environment.
- **Executive and Management Preparation** – Executive engagement to achieve response objectives, facilitate PR activities, and communicate clearly during every step of the investigation.

Symantec's Emergency Response not only eliminated the threat from our environment, they provided our team with tools, recommendations, and best practices that have resulted in our ability to build a stronger response team.

— IT Systems Manager, Healthcare Organization

For customers who want a more proactive approach to incident response and want to have a response partner on retainer, we have four different offerings: Standard, Enterprise, Advanced Enterprise and Custom.

SYMANTEC INCIDENT RESPONSE – PROACTIVE RETAINER SERVICES

FEATURE	STANDARD	ENTERPRISE	ADV. ENTERPRISE	CUSTOM
Specialized Service Management	✔	✔	✔	✔
Emerging Threat Reports	✔	✔	✔	✔
Remote Assistance SLA	12 hours	12 hours	12 hours	12 hours
Call Back SLA	3 hours	3 hours	3 hours	3 hours
Fly to Site Investigation SLA	Priority Access	48 hours In Transit	24 hours In Transit	24 or 48 hours In Transit
Pre-paid Fly to Site Incident Investigation	10 days	30 days	60 days	5—500 days
Discounted Pricing for Additional Responders	✔	✔	✔	✔
Ability to use Pre-Paid Time for IR Plan Assessment, IR Plan Development, Tabletop Exercises, Advanced Threat Hunting	✔	✔	✔	✔

> The Symantec IR team fit into the culture of our company and adapted well to the limitations of our infrastructure, providing the services required to remediate our incident while delivering the right amount of information at the appropriate level to our executive management team and board.

— Chief Information Security Officer, Services Organization

Complementary Services

Consider the benefits of leveraging additional Cyber Security Services:

Symantec Cyber Security Services: DeepSight™ Intelligence: Provides a customizable view into the changing security landscape with timely detailed adversary, vulnerability and cyber threat analysis which enables your organization to take proactive defensive actions and more effectively respond to incidents. DeepSight™ leverages one of the industry's largest threat collection networks and advanced software algorithms along with formal intelligence analysis processes to deliver a comprehensive range of market leading cyber threat intelligence.

Symantec Cyber Security Services: Managed Security Services: Delivers 24x7 security monitoring services by expert security staff, providing broad visibility of activity and potential threats across your organization's infrastructure. The Managed Security Services team reduces the time it takes to detect and prioritize security incidents and can improve response times by providing detailed analysis of your log data to your incident responder including vertical-specific and customer-specific context and incident history.

Symantec Cyber Security Services: Cyber Security Exercise: Engages participants in hands-on challenges through live simulation of advanced attacks; drives curiosity, learning, and passion across IT and security teams by putting participants in virtual scenarios where they act as the attacker and work their way through multi-stage attack scenarios.

Symantec Cyber Security Services: Consulting Services: Provides the experience, expertise, and industry knowledge to help optimize your security program and mature your organization's security posture. Symantec consultants support your business goals via design, implementation and optimization services in these areas: security strategy; risk and compliance assessment, network, application, and code testing; security residencies; and implementation of Symantec solutions.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec™ 350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

SYMC_DS_CSS_IncidentResponse_EN_v2