Data Sheet

NTT Security Critical Incident Response Services

Prove Preparedness and Minimize the Impact of Security Breaches

The NTT Security Critical Incident Response (CIR) Services provide incident response planning and testing, in addition to rapid response to minimize the impact of security incidents.

Limit the Impact of Attacks

An organization's ability to respond to a security incident is crucial to limiting the impact of the attack, minimizing response costs and recovering quickly. Planning and preparation are the keys to successful resolution of a cyberattack. Knowing what to do and who to call when time matters can help to reduce the duration and mitigate the impact of an attack quickly.

Planning and Testing in Advance

NTT Security CIR Services include prior planning, the integration of the NTT Security and client incident response teams and testing of the incident response plan. This will help ensure when an incident occurs, the response will be as efficient and effective as possible, with expert resources, proven processes and accessible log data. Testing activities include incident plus log data analysis to ensure necessary information is available.

NTT Security CIR Services clients have the peace of mind that comes from demonstrating to stakeholders—with third-party validation—that all necessary, reasonable steps have been taken in advance of an incident.

CIR Services are delivered by the NTT Security Professional Security Services (PSS) team. This team includes certified security professionals with expertise in incident response, forensics, malware analysis and countermeasures.

Prove Preparedness

Most security frameworks and regulatory requirements require organizations to have an IT security program and an incident response plan. Organizations that can prove the effectiveness of their incident response capability, including third-party validation, will not only meet requirements but will be seen by assessors and regulators as being truly serious about meeting their compliance commitments. NTT Security can provide clients with an Opinion Letter regarding the efficiency and effectiveness to identify and respond to a security incident.

Leverage the Power of ActiveGuard®

The patented, cloud-based ActiveGuard Service Platform collects and correlates log event data, which is essential for threat detection. The combination of ActiveGuard, 24/7 security operations centers (SOCs), certified experts and proven preparedness allows seamless, execution of the incident response process. During the design of an incident response plan, NTT Security determines if the client's current log monitoring is adequate, and whether additional security controls such as NTT Security Log Monitoring would be a better solution to ensure that propersecurity event logging is taking place.

Incident Response Plan Development

Whether starting from scratch or reviewing an existing plan, NTT Security consultants work jointly with an organization to create a sustainable incident response plan. By using industry best practices and following compliance regulations, incident response policies and procedures will be developed or modified.

The resulting incident response plan may include:

- Executive management support
- Incident response team structure
- Team roles, responsibilities and levels of authority
- Definition of an incident
- Incident classification matrix
- Organizational incident reporting procedures
- On-call information
- Response team communication
- External communications
- Evidence gathering, handling and storage
- Incident analysis resources
- Post-incident lessons learned
- Plan review and testing
- Performance measures

Additional documents can be created, depending on client requirements.

Features Include:

- Incident response testing
- 24/7 incident response
- Incident coordination and management
- Incident analysis and mitigation
- Data/image acquisition and forensic analysis
- Incident reporting and documentation
- Access to our security and threat research team

NTT Security Critical Incident Response Services

Retainer-Based Packages to Match Organizational Needs

NTT Security clients can choose from two retainer-based options to suit the needs of the organization. Clients can choose to test and validate incident response plans in advance or to be prepared with resources in the event of an incident. The Proactive CIR package provides an incident response plan gap analysis, plan validation and testing, a quantity of immediately available incident response hours based on client requirements and a set hourly rate for any additional incident response needs. The On-Demand CIR Retainer provides a quantity of immediately available incident response hours based on client requirements, and a set hourly rate for any additional incident response needs.

In both cases, clients benefit from having a contract in place before an incident occurs. This saves precious time during incident response. Both packages provide a two hour service level agreement (SLA) for NTT Security first response.

Package	Proactive CIR Plus Retainer	On-Demand CIR Retainer
Response SLA	2 hours (24/7)	4 hours (24/7)
Minimum Retainer Hours	60 hours	60 hours
Reporting	✓	✓
Incident Triage and Response Management	✓	✓
Forensic Analysis	✓	✓
Malware Analysis	✓	✓
Reverse Engineering of Malicious Code	✓	✓
Forensically Sound Image Acquisition*	✓	✓
On-site Support**	✓	✓
Incident Response Plan Gap Analysis	✓	N/A
IR Plan Validation and Testing	✓	N/A
IR Plan Integration	✓	N/A
Incident Response Preparedness Opinion Letter	✓	N/A
IR Plan Development and Maintenance	Optional Service (Additional Fees Apply)	Optional Service (Additional Fees Apply)

* Additional charges may apply.

** Does not include travel expenses.

A Partner You Can Trust

We don't believe that one size fits all. That's why we deliver a cybersecurity, risk management and compliance program that is as unique as your business. Our goal is to ensure that every organization develops the cyber resilience required to make the most of every business opportunity. We can provide the solution you need in the manner best suited to your specific situation and help you to avoid technical blind alleys, missed exits and roads that lead to nowhere.

The Full Security Life Cycle

NTT Security has created a Full Security Life Cycle model based on many years of providing efficient and effective security, risk and compliance services to organizations around the world. We provide the know-how and experience to plan for and optimize the architecture and deployment of services, ensure that they are managed and operated to deliver the key information needed, and are integrated into an overall response plan to make the results actionable. We deliver these services using local resources that leverage our global capabilities.

Get Started Today

See how NTT Security can help optimize security, improve efficiency and ease compliance. Contact NTT Security (US) today at us-info@nttsecurity.com or visit our website at www.nttsecurity.com.

About NTT Security

NTT Security seamlessly delivers cyber resilience by enabling organizations to build high-performing and effective security and risk management programs, with controls that enable the increasingly connected world and digital economy to overcome constantly changing security challenges. Through the Full Security Life Cycle, we ensure that scarce resources are used effectively by providing the right mix of integrated consulting, managed, cloud, and hybrid services – delivered by local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest information and communications technology (ICT) companies in the world. For more information, visit **www.nttsecurity.com.**