NCIRT

CYBER INCIDENT RESPONSE TEAM

# Cyber Incident Response

Ready for the inevitable?

# 01 Nettitude Incident Response services

Nettitude provides a managed Incident Response (IR) retainer tailored to suit the needs and threats your organisation could be facing. Using leading industry technology and certified experts, the Nettitude cyber response team manages, contains, remediates, and reports on cyber incidents. Importantly, a manager IRR gives you assurance when you most need it.

The cost of an average data breach is $3.86 million. The average resolution time is 280 days. Proper incident response management helps reduce the impact of a cyber-breach by immediately sending triage to your organisation.

As cyber-threats evolve at pace around the world, the likes of ransomware, malware, and insider threats pose a serious risk to organisations. Especially when they go undetected for a while.

Once a breach is identified, time is of the essence and having experts on hand to control the damage is vital to getting your systems back on the road to recovery.



# 02 Incident Response Service Benefits

Cyber incidents are only a matter of time. Nettitude's experienced Cyber Incident Response Team (NCIRT) is committed to helping you at every stage of the incident response lifecycle. From preparation, eradication, and remediation, through to lessons learnt.

As part of our Managed Incident Response, we provide a full range of tactical and strategic solutions tailored to your environment and organisational needs ensuring a robust security posture when you need it the most.

- Certified expert team on hand 24/7 as part of your team to support your business response to a cyber attack
- Expert advice and guidance covering Technical remediation, Incident Management, Risk & Business continuity planning during an event
- Dramatically reduce the time, and therefore the costs, of resolving incidents maintain productivity whilst specialist staff resolve incidents
- Expeditious containment of the incidents will prevent spread, and thus cost, of a Cyber incident
- Early resolution of incidents prevents further losses of data from a compromised system
- Your organisation could qualify for lower cyber insurance premiums by having aligned experts in place
- Conform to industry best practice and emerging legal requirements


NCIRT
CYBER INCIDENT RESPONSE TEAM

Cyber Response Engagement Manager

Cyber Response Incident Manager

- Certified Incident Response Analysts & Consultants
- Cyber Response Engagement Manager
- Cyber Response Incident Manager
- 24/7 response SLA
- Cyber Risk Assessment & Guidance
- Assisted Onboarding & Preparation
- Incident Response Business Continuity Preparation
- Host, Network, Malware Analysis & Reverse Engineering

# 03 Service Features

We provide a full range of tactical and strategic solutions tailored to your environment and organisational needs ensuring a robust security posture when you need it the most. A managed IR is there to help you get back to normal operations quickly with confidence.

### Global Expertise

Nettitude has been at the forefront of cybersecurity since 2003. Our NCIRT team has the know how and expertise to quickly identify, investigate and remediate the breach

### Rapid Response

Nettitude's NCIRT team understand that a rapid response is critical to containing and limiting the impact of a cyber incident. Our experts can start work within hours backed by guaranteed response SLAs and rapidly analyse for signs of compromise or breach

### Hands-on Remediation

NCIRT can provide guided and assisted hands-on technical remediation support to help guide your teams to implement recommendations to contain and eradicate then reduce the risk of future compromise

### Command & Control

Nettitude have dedicated Cyber Incident & Engagement Managers with years of industry expertise in managing crisis situations to aid in the command, control & communications over all cyber incident response activity

### Technology & Threat Intelligence

Leading industry technologies and sophisticated Threat Intelligence is available to the NCIRT team to assist the rapid response capability when you need it most

### Reporting

Cyber response and incident level reporting covering impact, recovery, technical analysis & investigation and executive level summary encompassing all facets of a cyber incident management

### Research & Reverse Engineering

Nettitude can provide host, network and malware analysis and reverse engineering through our dedicated Research & Innovation centre.

### Service Flexibility

Our services provide flexibility for you and any unused IR hours can be used on alternative IR professional services to ensure you maximise value from your service

# 04 Service Options

Nettitude's NCIRT works with you regardless of your budget, environment, or organisation size. We ensure you get the right care and readiness you need ranging from a basic IR consultation triage service to the premium level services with guaranteed SLAs and flexible consumption models.

| Service Level | 24/7 Hotline | Guaranteed SLA | Pre Paid Hours | Transfer Unused Hours | Cyber Incident & Engagement Manager |
|---|---|---|---|---|---|
| Bronze | ✓ | 4 Hours | ✓ | ✓ | ✓ |
| Silver | ✓ | 4 Hours | ✓✓ | ✓ | ✓ |
| Gold | ✓ | 4 Hours | ✓✓✓ | ✓ | ✓ |

*Prepaid IR Consult hours can only be used for IR Triage hotline activity and not DFIR services

# 05 What is included?

- Nettitude Guided and assisted onboarding process for all Incident Response Services:
  - IR Policy and procedure review
  - IR Table top planning and readiness exercise
- 24 Hour IR Hotline
- NCIRT Guaranteed Response - 4 Hour SLA (IR consultant contact)
- Aligned Cyber Response Incident Manager
- Aligned Cyber Response Engagement Manager
- Access to Elite NCIRT expert technical team
- Bank of retained hours aligned and ready for an event

NCIRT
CYBER INCIDENT RESPONSE TEAM



# 06 Cyber Incident Response Consultancy

Nettitude's Incident Response service offerings can evaluate and significantly enhance an organisation's ability to respond to a cyber attack.

### Incident Response Plan and Policy Writing
Nettitude will work with your organisation to create an Incident Response policy and plan that is tailored to your organisational needs and aligned to industry best practice. The plan will outline the tools and procedures that your security team will use to identify, eliminate, and recover from cybersecurity threats. By having a well-planned and documented policy and response plan you can ensure an expedient response when it is needed most.

### Table Top Exercises – Cyber Response
Regular practice of your organisation's response to a cyber incident means teams are likely to respond more effectively when under the pressure of a real cyber Incident. This engagement has been designed to test your organisation's incident response plan Nettitude carefully crafts bespoke scenarios based on the biggest threats to the organisation. During the course of the engagement, multiple scenario injects are used to test your team's thought process and decision-making skills. At the end of the engagement, a report is provided that identifies any areas that may require improvement or present risk.

### Cybersecurity First Responder Training
This one-day training course is designed to prepare your cybersecurity team to act effectively and efficiently against a cyber attack. Ensuring that your team have the correct knowledge to be able to react to a cyber incident can help minimise and ensure an expedient response.

### Ransomware Resilience Assessment
The threat from ransomware has increased significantly over the past years with different techniques being adopted by threat actors and ransomware as a service operators. Nettitude have designed this service to assess an organisation's current preparation, security technologies and backup strategy to ensure that it can recover from a ransomware attack. This also assesses an organisation's security posture to prevent and detect attackers who are intent on widely distributing ransomware across the organisation's endpoints. A successful ransomware attack can cause an organisation critical impacts and lengthy recoveries across their business services and operations.

### Incident Response Maturity Assessment
Nettitude's Incident Response Maturity Assessment will provide valuable insight into your incident response capability covering, people, processes and technology. Part of the assessment includes the benchmarking of your current capability against a robust incident response capability framework. Analysis of the results will provide a set of recommendations that can be used as a roadmap toward improvement. The assessment will also include a review of your existing logging capability and make recommendations on how to enhance them in order to maximise the capability of any SIEM or SOC solutions that you have in place.

### Playbook Review
Response to Cyber incidents requires a well-planned and repeatable process. Through the use of playbooks we make sure that your security team know what to do in a particular event. This engagement has been designed to support maturing security teams by reviewing in-use playbooks and providing guidance on best practice as well as how to optimise processes to reduce incident volumes.

### Threat Hunting
This is a proactive service and compliments a penetration test to provide the organisation with the confidence that they have not been compromised. A penetration test is used to identify weaknesses in the organisation's infrastructure. A threat hunt can use the findings of this report to complete targeted 'hunting' to see if any of these weaknesses have been exploited and if an attacker is hiding in the infrastructure.

### Compromise Assessment
This is a reactive engagement when an organisation suspects that its infrastructure could have been compromised. This service can be called upon to provide confidence that a zero-day or critical vulnerability has not been exploited. This assessment has been designed to discover unknown security breaches, malware, and signs of unauthorised access.

CREST | VA | PEN TEST | STAR Intelligence-led PT | STAR Threat intelligence | CSIR | SOC

PCI Security Standards Council — QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council — APPROVED SCANNING VENDOR

CYBER ESSENTIALS

CHECK — IT Health Check Service

Computing Security Awards — ★ FINALIST ★

winner Cyber Security Awards

CYBERSECURITY BREAKTHROUGH AWARD 2020 — THREAT INTELLIGENCE COMPANY OF THE YEAR

bsi. ISO/IEC 27001 Information Security Management

INVESTORS IN PEOPLE

NETTITUDE
AN LRQA COMPANY


**UK Head Office**
Jephson Court, Tancred Close, Leamington Spa, CV31 3RZ

**Americas**
50 Broad Street, Suite 403, New York, NY 10004

**Asia Pacific**
18 Cross Street, #02-101, Suite S2039, Singapore 048423

**Europe**
Leof. Siggrou 348
Kallithea, Athens, 176 74
+30 210 300 4935

**Follow Us**

solutions@nettitude.com
www.nettitude.com