Digital Forensics Incident Response Services (DFIR)

Cyberthreat continues to be among top five concerns of global CEOs However, only 15% can withstand the attacks and recover quickly

Cyber threat continues to be among the top concerns of CEOs

30% (2019)

CEO concern:
Cyberthreats, 2019

	North America	Middle East
Rank	#1	#2
	45%**	38%**

**% of respondents (n=1,378)

59%

of companies are not confident that they can resume business as usual 24 hours after a cybersecurity incident

(NTTS Twitter Survey 2019)

*Note: 2019 was the first year CEOs were asked about 'policy uncertainty' and 'trade conflicts'; Also, 'protectionism' entered the top 10 list | Source: PwC, 22nd Annual Global CEO Survey, 2019, Oct 2018

Increasing IT infrastructure complexity and talent gap are driving cyberattacks

Rising cyberattacks with new tools, tactics and better techniques

Increasing **complexity of IT infrastructure** is resulting into security issues

Gap in the security skills persists

Organizations are **not proactive for cyber security**

Regulatory and privacy challenges will continue to grow in conjunction with digital business' insatiable appetite for personal data

Source: Gartner, Top Security and Risk Management Trends, Jan 2019; Dimension Data Insight and Analytics

Cyberattacks Require Organizations to Have Robust Response Capabilities

Our client engagement model:

Management
- operations
- maintenance
- support

Consulting
- business requirements
- workshops and interviews
- risk analysis
- gap analysis
- technical analysis
- recommendations

Strategy
- business alignment
- vision and strategy
- roadmap

Architecture
- evaluation
- optimization
- design
- deploy

Controls
- platform
- automation
- configuration
- integration
- consumption
- threat intelligence

Incident response process

Identification

- What happened?
- How did it happen
- What was exposed?

Containment

- Contain the incident

Eradication

- Stop the incident
- Remove the threat

Restore operations

- Restore operations
- Prevention/Detection

Lessons learned

DFIR Retainer Service features

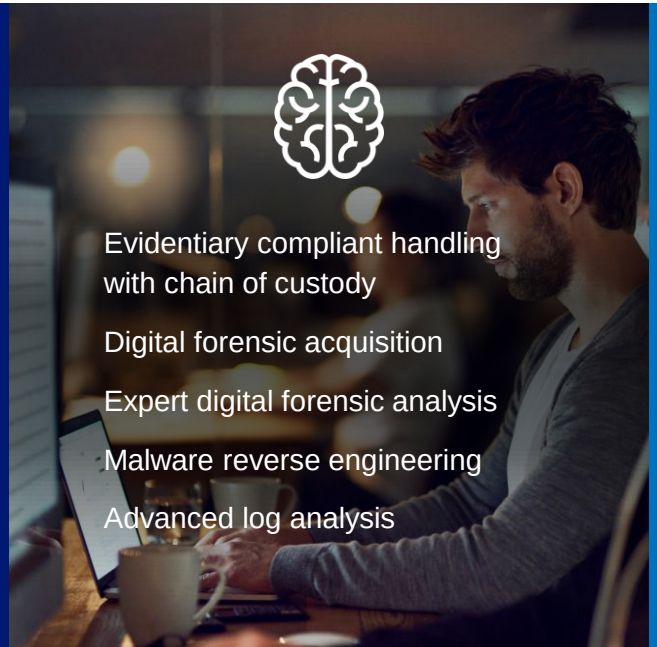
On-call 24/7 to Respond

Incident Management

Daily/weekly status updates

Rapid remote deployment of DFIR tools

On-site deployment as needed



Evidentiary compliant handling with chain of custody

Digital forensic acquisition

Expert digital forensic analysis

Malware reverse engineering

Advanced log analysis

Incident mitigation/containment

Integration with NTT Ltd.’s Global Threat Intelligence Center (GTIC)

Integration with NTT’s Managed Security Services

Incident reporting/documentation

DFIR Retainer Service Tiers

	Silver	Gold	Platinum
Retainer hours	80	120	240
Initial remote response	4	2	2
Onsite analysis SLA	Best effort	Best effort	Best effort
% of unused hours available for other DFIR Services	15%	25%	50%

DFIR Readiness Services

Incident response
plan development

Incident response
plan runbooks

Incident response
plan gap assessment

Compromise
assessments

Incident response
plan testing

DFIR Readiness Services

IR plan development	Develop a basic framework required by the organization to operate effectively in the event an incident occurs.
IR plan gap assessment	Review of organization's incident response documentation, provide an assessment report with gap analysis using best business practices, common standards.
IR plan testing	Develop test scenarios specific to organization's vertical market and facilitate exercises with client internal IR team to evaluate how well they respond to incidents.
Digital forensics and incident response training	Develop and execute in-depth training in forensics tailored to the client's needs. Ex: forensic acquisition, evidence collection, volatile memory, identify files for preservation, etc.
Compromise assessment	Evaluate the client's environment for the presence of breach activity and detection of persistent threats. Identify IOCs, malware artifacts or malicious network traffic activity.
IR runbook development	Detailed guide on how to respond to very specific attacks such as ransomware, malware, denial of service attacks, etc.

Network intrusion

The incident

NTT DFIR were engaged by the client, following detection of malicious activities across circa 50 servers. The client requested forensic analysis of all servers to identify any indicators of compromise. Furthermore, the client requested a review of log files associated to their active directory to identify any further risks. The client requested all analysis to be conducted within their own infrastructure, due to the sensitive nature of the detections.

The response

NTT DFIR setup several dedicated forensic investigation servers in the client's environment, in order to facilitate forensic analysis of memory and disk images from the 50 servers. Log files were also provided, which were also subject to analysis. NTT DFIR coordinated the forensic investigation and provided ongoing support to the client.

The conclusion

Following examination of the available material, NTT DFIR identified a successful network intrusion on multiple servers. The attacker exploited several JAVA vulnerabilities in a subsidiary's web applications, in order to gain access to the internal network. NTT DFIR identified several Cobalt Strike beacons used by the attacker in order to facilitate malicious actions. The attacker maintained persistence by modifying current scheduled tasks via VBScripts to execute the beacons. Following a review of the active directory, several suspicious accounts were found to have been created. Information was provided to the client for further investigation.

Why clients choose NTT Ltd.

Market leader

NTT is a Challenger: Gartner Magic Quadrant for Managed Security Services, Worldwide.

Toby Bussa, Kelly M. Kavanagh, Sid Deshpande, Pete Shoard, February 2018

Extensive experience

We have over **2,000 cybersecurity** specialists.

Global scale

More than 15,000 security engagements with clients spanning 57 countries across multiple industries.

Global insights

- 6.2 billion attacks analysed
- 10 Security Operations Centers
- seven R&D centers

Great partnerships

Working with our top five global security partners.

Global DFIR

FIRST membership

- Members of international incident response association where information is shared in a secure way about vulnerabilities, incidents, technical tools as global security incidents have no boarders.
- Members can communicate with peer teams, exchange ideas, share viewpoints and practices on handling certain types of security incidents that have not been seen in another part of the world. This allows for improvement of computer security incidents worldwide.

CREST accreditation

- Cybersecurity incident response services CREST member company.
- Crest provides a clear indication of the quality of an organization providing incident response services.
- All crest member companies have submitted policies, processes and procedures relating to the service provision to crest.
- Policies, processes and procedures have been assessed by crest and have been deemed fit for purpose.
- Resubmission is required every year and a full re-assessment is required every three years.


NTT
Together we do great things