Cyber Ensō

Overview

At Nihon Cyber Defence (NCD), we have seen the impact that cyber-attacks and in particular ransomware attacks can have. Whilst there have been major ransomware attacks that have dominated the headlines, the reality is that an enormous range of organizations are being impacted.

This increase in the number and sophistication of attacks has been driven by Ransomware as a Service (RaaS), that has made sophisticated cyber tools available to a growing range of criminal groups.

The sole purpose of the NCD Advice Service is to help you recover from a cyber-attack.

Products and Services

Ransomware Assessment: NCD will help you assess the overall impact and severity of the ransomware. Organizations will be advised on the next steps after a complete assessment has been undertaken.

Ransomware Incident response: NCD will provide a detailed plan on how to manage the incident. A highly expert group of advisors will help you tackle the incident in the best possible way.

Extortion Negotiations: NCD provides extortion negotiations and the required communication with the threat actor as a service to organizations. NCD will take the responsibility of handling the complete incident by acquiring all necessary information from the threat actor.

Settlement and Decryption Support: NCD provides all the necessary support required for decrypting the files that have been encrypted in the ransomware attack. We also will provide settlement services based on communication with the threat actor.

Ransomware Crypto Forensics: The purpose of our Crypto Ransomware Forensics service is to give you a detailed insights into your crypto transactions, the addresses, and wallets they are transferred between, as well as the relationships between transactions, addresses, wallets, and those that are involved in the transactions.

Incident Response retainer: NCD provides retainer services which serves as an insurance policy to the organizations. The retainer service is a combined set of services that include proper incident response, detailed report analysis, complete support during the incident, cryptocurrency settlement and decryption support, extortion negotiations, detailed incident response and recovery report within given SLA's. Organizations will also be provided with complete access of alerting and research from NCD.

Additional services: These additional services come with all the services defined above and it includes:

- Development and deployment of the technical solutions pre and post in a cyber incident.
- boards awareness, incident planning and exercising.

Incident Types

We deal with the following incident types:

- Ransomware.
- Threat actors encrypting the data files.
- Threats of Data leakage.
- Account and data compromise.

Process

The way that this service works is:

- Companies that believe that they may have become the victim of a cyber-attack, contact NCD through our online portal (please do not use an email address that may have been compromised in the attack).

- A Non-Disclosure Agreement (NDA) is quickly put in place to ensure complete confidentiality.

- After an initial discussion with a native Japanese speaker, a secure video conferencing call will be set up between the company's management and world-class cyber security experts who have dealt with many hundreds of cyber security incidents. This call can be in English or with Japanese translation.

- During the call senior managers (CEOs, CIOs, CFOs, CISOs, or anyone else who finds themselves in a cyber incident management leadership role) will have the opportunity to ask questions of these experts. These can be general questions around best and poor practice or specific technical questions.