The Challenge
In recent years, law enforcement has faced increasingly challenging digital landscapes where criminals take advantage of advancements in technology and fast-evolving threats. It is crucial that we stay vigilant round-the-clock to cater to perpetual threats that will lead to adversity of the technology world. In today’s world, the digital age has opened up immense new opportunities to the law enforcement, providing fast, secure communications channels and instant access to criminal data. With that comes greater opportunities for crime as well.

The Solution
NEC’s vision is that of a world where each and every individual can securely communicate, share, and access information wherever and whenever they need to, with no fear of unauthorized access. To that end, NEC is delighted to announce a three-pronged strategy to manage the cyber threats that we face on a daily basis.

1. Cyber Fusion Platform
2. Digital Forensic Platform
3. Training and Simulation Platform

Solution Benefits:
- To enhance the current capabilities of criminal investigation.
- To safeguard from being the target of cyber attack.
- To provide the essential tools/platform made accessible and intuitive for investigation.
- To provide comprehensive packages to cater to the needs of individuals.

### Function List

<table>
<thead>
<tr>
<th>Basic</th>
<th>Standard</th>
<th>Premium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Fusion Platform</td>
<td>N/A</td>
<td>On-premise Cyber Information Sharing portal (essential)</td>
</tr>
<tr>
<td>Digital Forensic Platform</td>
<td>Data extraction capability</td>
<td>Data extraction and malware analysis (essential)</td>
</tr>
<tr>
<td>Training</td>
<td>Web-based training</td>
<td>Onsite training (standard scenario)</td>
</tr>
<tr>
<td>Operation Support</td>
<td>Remote support</td>
<td>Onsite support (1 person x 1 year)</td>
</tr>
</tbody>
</table>

As a strategic partner of INTERPOL, NEC Corporation works together with INTERPOL to combat cyber crime. NEC provides technical and human resources to establish Digital Forensic Lab and Cyber Fusion Centre within INTERPOL Digital Crime Centre (IDCC).

| CYBER SECURITY FACTORY FOR LAW ENFORCEMENT |

As an orchestrating a brighter world partner of INTERPOL, NEC Corporation works together with INTERPOL to combat cyber crime. NEC provides technical and human resources to establish Digital Forensic Lab and Cyber Fusion Centre within INTERPOL Digital Crime Centre (IDCC).
It is essential for law enforcement to enhance their capability on cyber criminal investigation. In the training platform, it offers opportunities to master:

- Early detection of cyber attacks
- Cyber incident response and investigation protocols
- Real-time cyber security defense strategies

NEC offers educational programs for cyber investigation.

Example of training course:

**Web Application Hacking**

In this course, you will learn hands-on, of how web application vulnerability can be used in an attack, and what kind of information an attacker can extract from web applications. This course will be conducted in a role-play environment, where you become the attacker, trying to abstract information to clear the missions given by the instructor. By completing all the missions, you will be able to experience the beginning to advanced level of web application attack methods.

**Malware Analysis**

This training course offers knowledge and skills to analyse an incident that may be caused by malware infection. You can obtain knowledge required to collect and initiate multilateral to multidimensional analyses of malware specimens.

**Network Hacking**

In this course, you will learn hands-on, of how to use hacking tools and to see the damage by actual experiencing of various attacking methods, moving from researching attack points against networks, Hitler, analyzing powerpoints, and then hacking man in the middle attacks. The mission of this course is to take over the target network/host using various tool commands used for hacking.

**Smartphone Application**

This course is designed to train forensic analysts who can respond to security incidents and cyber crimes. This course offers knowledge when a terminal installed with a smart-device OS, such as iOS or Android, is your analysis target.

**Basic Incident Handling**

This training course is designed to help improve your capability of detecting cyber incidents and to improve your initial response capability. It provides an opportunity to learn about the current cyber threats and the incident handling procedures, as well as to improve your skills in handling cyber incidents.

**Digital Forensic Platform**

In order for law enforcement to better coordinate and conduct cyber crime investigation proactively, it is necessary to extract data from computer devices, recover deleted information so that it can serve as digital evidence in court.

Digital Forensic Platform focuses on practical technology and provides investigators with the necessary tools to conduct forensic investigations and prosecute criminals.

The activities of the lab can be broken down into 3 core elements:

- **Disk Forensic**: Extracts forensic information from hard disk images.
- **Mobile Forensic**: Recovers digital evidence or data from a mobile device following best forensic practices.
- **Malware Forensic**: Examines a system to determine the profile and sophistication level of the malware attack.