Digital Forensic Laboratory

NEC’s Digital Forensic Laboratory allows us to conduct forensic investigations on computer hardware and storage media to ascertain if an organisation has been compromised and to assess the level of penetration and damage.

Through our collaboration with Interpol, our laboratory will be developing internationally recognised forensics procedures and standards in the area of evidence preservation and processing (e.g. clean room), using tried and tested tools and techniques that Interpol itself recommends.

Professional Services

Security is a challenging and diverse field and NEC stands at the forefront with our extensive and unmatched experience and expertise. Our experienced, highly trained team is able to provide a host of services. These include:

- **Security Advisory**
  - Policy, Standards, Guidelines and Procedures Development & Review
  - Development of Security Governance, Enterprise Security Architecture and Implementation Road-map / Blue-prints

- **Assurance Reviews**
  - Technical Security Architecture Design Review
  - Consultancy / Post-mortem Reviews on current/past cybersecurity incidents
  - Reviews on Project Development Life-cycle and IT Operations

- **Security Testing**
  - Penetration Testing & Vulnerability Assessments.

- **IT Security Standards Audits**
  - IT security management and governance framework
  - IT Systems and Services

NEC’s three decades of global security expertise makes us the perfect partner to audit your IT security systems and processes.

About NEC Global Safety Division

NEC Global Safety Division, a business division within NEC Corporation, spearheads the company’s public safety business globally. The Division is headquartered in Singapore and offers solutions in the following domains: Citizen Services & Immigration Control, Law Enforcement, Critical Infrastructure Management, Public Administration Services, Information Management, Emergency & Disaster Management, Inter-Agency Collaboration. Leveraging on its innovative solutions, the Division aims to help government and business make cities safer.

NEC Global Safety Division
Global headquarters: No.1 Maritime Square #12-10, HarbourFront Centre, Singapore 099253
For enquiries, please contact safety@gsl.jp.nec.com
Thanks to three decades of experience in providing security-related systems integration for demanding national-level projects in Asia and around the world, NEC has the ability to deliver turnkey solutions to clients regardless of complexity.

That is why Interpol selected NEC when the global police body needed a systems integrator for their Digital Crime Centre that they are setting up in Singapore*. NEC is now in the process of setting up the Digital Forensic Laboratory and the Cyber-Fusion Centre for Interpol.

At NEC, we utilise a layered, integrated threat mitigation strategy to protect data at all levels and in all circumstances. The solutions that we can integrate include:

- Security for data in transit/secure file transfers
- Protection of data at rest and in offline storage media
- Anti-malware and anti-spam
- Database encryption
- Virtual Private Networks (VPN)
- Mitigation against Advanced Persistent Threats (APTs)
- Security Information and Event Management (SIEM)
- Next-Generation firewalls
- Web application firewalls with auto-defacement detection and restoration
- Mitigation against Distributed Denial-of-Service (DDoS)
- Two-factor authentication via one-time password (using token or SMS) or smart cards
- Privileged user identity management
- Anti-malware and anti-spam
- Data Loss Prevention (DLP)
- Enterprise-wide management of encryption keys and public key infrastructure
- Web application firewalls with auto-defacement detection and restoration
- Mitigation against Distributed Denial-of-Service (DDoS)

As every customer has different requirements, we are able to tailor our suite of solutions to the needs of the individual customer, working either with legacy solutions or in a greenfield situation.

Integrated Layered Defence Cyber Security Solution Provider

As a systems integrator specialising in IT security, we adopt a layered defence methodology in our proposed cyber security solutions to mitigate different threat categories. Our tested and proven delivery model includes:

Requirements Gathering
Our security consultants will conduct the requirements and security analysis, which includes threat and risk assessments to identify the IT security threats to the protected system. A payment gateway system, for example, will have different IT security needs from a patient medical records system.

Design
Our architects will design comprehensive solutions that meet the customer’s needs, incorporating tightly integrated, cost-effective third party products/systems. We will also ensure that the final IT system will meet the business, operational and security objectives of the customer’s enterprise. Proof-of-concepts may also be carried out upon customer request.

Integration and Configuration
Our system and security engineers will integrate, interface, configure and fine-tune all the components, ensuring that these work seamlessly as a single system for the customer.

Installation
Our technical support team will perform on-site installations, from security appliances to system switches and servers, including patch panel connections.

Testing
Our project management team will conduct (via internal quality controls) and also facilitate customer validations/assurance procedures that the solution delivered is performing according to functional and security specifications. This typically includes the conduct of a User Acceptance Test with the client as a witness.

Our consultants will also engage and work with independent parties for penetration tests and security reviews, aimed at uncovering vulnerabilities due to dynamic changes in the cyber security threat landscape.

Commissioning
Our change management and handover process will ensure a smooth transition from the development to the production environment. Training and briefing sessions will be held for customers. Close monitoring of the system performance will also be carried out.

The Cyber Security Training and Simulation Platform

Companies that are looking for better training to upgrade their IT security staff can now tap into NEC’s expertise and skills with NEC’s Cyber Security Training and Simulation Platform. Our Simulation Platform can also be used for testing and validating large-scale IT security solutions in a virtual environment, including validating SCADA (supervisory control and data acquisition) systems. Training-wise, the platform offers opportunities to master:

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

As a simulation platform, NEC’s Cyber Security Simulator enables companies to test and validate large-scale IT security solutions. The realistic virtual environment even allows for the testing of large-scale, multi-site industrial control systems such as SCADA. The strength of the platform is that it offers real-life virtualisation and real-time simulation of networks and systems.

As a simulation platform, NEC’s Cyber Security Simulator enables companies to test and validate large-scale IT security solutions. The realistic virtual environment even allows for the testing of large-scale, multi-site industrial control systems such as SCADA. The strength of the platform is that it offers real-life virtualisation and real-time simulation of networks and systems.

When your security staff graduate from our training, they’ll have the skills and experience to react swiftly and expertly in a real security crisis thanks to our realistic simulation environment.