NEXOR

KEEPING SENSITIVE MILITARY INFORMATION SAFE

In a military force, the management of information and the security of data transfer are both of paramount importance. Networks have to be kept updated and safe from external threat. A variety of information has to pass between internal networks of differing security classifications.

To enable clients to carry out these operations securely, Nexor has replaced existing systems set up by other vendors, and provided multiple high assurance solutions to facilitate the secure passing of data between multiple security domains.

THE CLIENT

A military organisation.

THE CHALLENGE

In addition to the secure transfer of data, applications, systems and networks had to be kept right up to date. This was necessary to maximise functionality and performance, whilst protecting against vulnerabilities and a constantly evolving security threat.

The flow of network events and logs from separate sources all had to be brought to a single location, such as a Security Operations Centre (SOC) for better management of data, enabling visualisation, analysis and insight – without any **data leakage or loss** from within the secure network/high security domain.

The military organisation also had problems with the performance of the existing technologies it was using. In particular, it was experiencing higher than desired occurrences of **random data loss**, which was hindering the transfer of information and, on a larger scale, the smooth running of the organisation's operations.

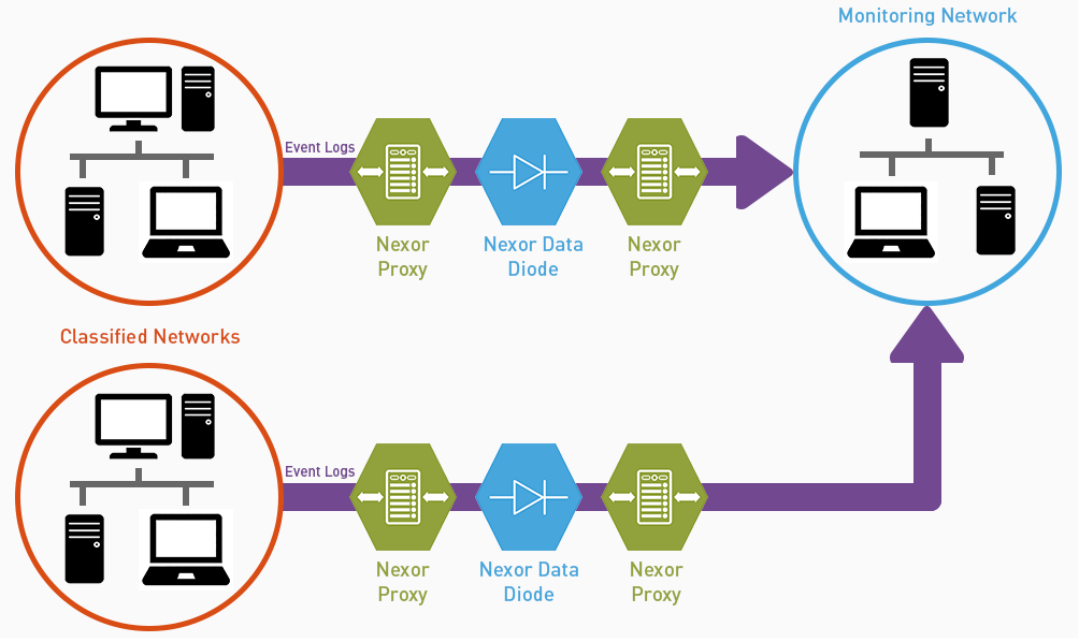
+44 (0)115 952 0500 info@nexor.com www.nexor.com

NEXOR

THE SOLUTION

Clearly, network monitoring and applying system updates are critical operations, but when an organisation has multiple networks of differing security classifications, they can become more difficult to achieve. We worked with our client to help it to adopt solutions that give it **central network monitoring and secure system updates in its high assurance environments**.

The **Nexor Data Diode** played a key role in this solution deployment. It enforces traffic flow entirely in one direction within a physically separate, hardware-only, data diode device. This is connected to proxy servers both upstream and downstream via fibre cables.



Different variants of the Nexor Data Diode are available including options for both Windows and Linux platforms. We have implemented solutions on both platforms for this military organisation.

These particular solutions were developed at our secure facility using our CyberShield Secure® methodology, which is based on years of experience of working in cutting edge technology security.

CyberShield Secure® is a **consultative process** which places the client's business requirements and security constraints at the heart of any engagement, and is based on industry best practice for secure engineering.

In short, it focuses on understanding the client's wider operational context and information needs, which can then drive the design of the most appropriate solution.

NEXOR

TRUSTING THE SOLUTION

Nexor has a great deal of experience in delivering commercial off-the-shelf and bespoke solutions to enable secure information exchange across management and security domains. We take a consultative approach throughout the product lifecycle, from understanding the user requirements to designing, deploying and supporting the system when in-service. This ensures that the most appropriate and cost-effective solution is delivered to the customer.

We devised and developed a bespoke solution for this client using our accredited professionals, SIXA® technology portfolio and CyberShield Secure® processes.

SIXA® technology is our industry-leading portfolio of trusted information exchange products which are based on our Secure Information eXchange Architecture (SIXA). The portfolio consists of configurable modular building blocks that follow **best practice from National Cyber Security Centre (NCSC)**, the UK National Technical Authority, for the import and export of data across security domain boundaries.

In addition, all of the proxy appliances used were **Common Criteria** certified to Common Criteria EAL 4+, while the Nexor Data Diodes are assured to Common Criteria EAL7+.

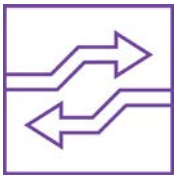
Software was developed using our CyberShield Secure® development process that conforms to Microsoft SDLC, CMMI and TickITplus standards. The entire system was delivered by our cyber security professionals who have industry-recognised accreditations, with penetration testing carried out by a third-party organisation to **independently verify** the solutions.

After completion and testing, the solution was accredited by an external accreditation authority, which allowed our client to deploy the solution in an operational environment.

THE IMPACT

The information management and security system devised by Nexor quickly realised a number of benefits for the client. There is now **no data loss**, and the robust reliability of the new technology has freed up staff to concentrate on managing other aspects of their network.

The solution has proved so successful that there have been **multiple procurements** over the last 18 months, including supplying two variants of the Nexor Data Diode for both Windows and Linux platforms. The solution has also been adopted for other cross-domain challenges within the same client's organisation.



NEXOR CAPABILITIES

Nexor provides solutions to get information into and out of secure networks. This enables organisations to perform more efficiently and effectively. The connection of secure networks is achieved by using people, process and technologies that align to best cyber security practice established by national authorities.

+44 (0)115 952 0500 info@nexor.com www.nexor.com