Fact Sheet

Cogito Group

Discovery

The next generation of Record Automation - introducing Discovery

Bring certificates and keys under management quickly and effectively

Jellyfish discovery tool is used to discover existing certificates and keys within an environment to bring them under management quickly and effectively.

The Jellyfish Discovery Services Module includes certificate discovery tools to perform discovery of certificates in use within the targeted networks.

Networks are scanned to identify any devices operating on them, and the devices are then scanned to determine any certificates present. Details of discovered certificates and devices are stored within the Jellyfish data store, allowing reports to be generated on data relating to the discovery run.

Bring device information under management quickly and effectively

When Jellyfish discovery tool is used in conjunction with the Jellyfish Security Client or Mobile app, Jellyfish can also be used to populate data into our Configuration Management Database (CMDB), Internet Protocol Address Management (IPAM) capability or even into our service monitoring tools. This allows the service to become a one stop shop for managing assets from an equipment and functional point of view. The CMDB can provide information such as IP address, operating system, patch levels, CPU, RAM, Hard Driver capacity, Hard Drive usage, purchase and warranty information, etc.

How does Discovery work?

The discovery tool captures data by through a number of methods such as interrogating network ports, but also through the devices themselves. It can reach certificate information in stores such as the Windows Machine certificate stores and Java Keystores for what certificates and keys they are storing. Other computer information can be gathered through various methods depending on the platform.

This allows for keys, certificates and numerous other asset management information to be brought under more active management. It allows for a significant reduction in unknown certificates and assets.

It also allows for rouge or unapproved assets, IP allocations, PKIs and Key Generation tools to be identified, as well as giving information on

This process will poll servers, services, and applications to attempt to detect the use of certificates within the network. These will then be registered within the Jellyfish application. As the responsible

entity for these certificates may not be known, these certificates are reported to Jellyfish administrators to ensure that action can be taken to determine the person or group responsible for their management.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.