REBASOFT

Customer use case: Charity

Organisation Profile

A £250 million charity operating in more than 30 countries worldwide, focusing on Africa and Asia. The charity has more than 500 staff, most of whom work remotely. The IT team is based in Surrey, UK.

IT profile

The charity uses Microsoft based systems. End-users connect via a dial-in VPN's or from remote office networks. These are managed through several, non-integrated systems. A third-party manages firewalls and the data centre under an outsourcing contract.

Project Drivers

With some 440 cyber security breaches reported by charities in 2019/20, a security project was sponsored by the senior leadership team. The Information Security Manager (ISM) was tasked with improving security and implementing Cyber Essentials Plus. Such frameworks have been shown to reduce cyber-attacks by 86%. Cyber Essentials Plus (CEP) requires an "auditable record of conformance", something which the charity was "then unable to deliver".

Evaluation and Proof of Concept (PoC)

The ISM prepared a list of CEP framework control requirements to help choose a solution. Rebasoft was chosen for a PoC based on technical features, cost, and ease of deployment. The charity also wanted to deliver quick results to meet project timeframes. The areas for evaluation were:

See any configuration changes to firewalls made by outsourcing staff. There had been past cases where changes had been made without IT security being aware

- Discover all assets, including hardware, OS, installed applications and enabled features
- Check systems against security policy:
    - Is anti-malware installed?
    - Is disk encryption enabled?
    - Are secure settings enabled to prevent users installing software or Autorun programs from running?
- Report & integrate with existing ticketing and executive reporting systems

Challenges

The ISM had little to no visibility of the network and infrastructure. Firewall and server management was outsourced. Network and Wi-Fi was cloud managed - Cisco Meraki. End-user PCs were managed via either Domain, SCCM or Intune. This made it hard assess security from information in the existing management systems.

The Covid19 pandemic meant the PoC needed to be run without the need for anyone to go physically to site.

Rebasoft Approach

Rebasoft overcame the challenges

- Quick results: Rebasoft was installed on an available Hyper-V server in about an hour
- Network data was collected from the existing Cisco Meraki cloud
- Configurations were collected directly from the firewalls
- End point data was collected with PowerShell to allow security compliance reporting

Little involvement was needed from the IT operations team, other than providing credentials and network access (firewall rules). Rebasoft did not need to install software agents on PC's.

Rebasoft Benefits

The PoC delivered against the Charity's stated needs:

- Automated discovery found all connected devices and built a reliable, accurate asset baseline
- Direct collection of data, including OS version, installed applications, enabled features was performed without the need for software agents
- Firewall configurations were collected and changes "diffed" so they could be tracked
- Security compliance: endpoints missing malware, checking BitLocker was enabled and AutoPlay/Admin rights settings were simply reported, allowing easy identification of systems for remediation
- The inbuilt vulnerability scans automatically run against discovered systems. This was an additional value that Rebasoft delivered

Outcome

"Having such a distributed network always caused problems seeing the network all the way to the outlying edges. With Rebasoft I can now see all my network attached devices in one system and validate them for compliance and audit purposes." – Charity ISM

See for yourself how Rebasoft can improve any Charity's cyber-resilience