SYNNEX Stellr Microsoft Cybersecurity Assessment

How can you develop an action plan to improve your environment's IT security?

Developing an action plan to improve the security of the IT infrastructure is not simple. Where should you start? What are the top priorities? What vulnerabilities exist? Improvements can be made, but determining what needs to be improved can be complex. There must be a better way!

An Action Plan Based on Facts

An effective action plan to improve IT security must be based on the facts collected from the IT infrastructure. Though the technical infrastructure is important, you must also take user activity into account and decide which improvements to implement first based on the data you find. This can quickly become a difficult and time-consuming task.

SYNNEX Stellr Provides Insight Into Vulnerabilities

The SYNNEX Stellr Cyber Security Assessment offering helps organizations quickly develop a concrete and comprehensive plan to improve their security, based on facts collected from the IT infrastructure. The Cyber Security Assessment Tool (CSAT) uses state of the art algorithms to scan your IT infrastructure and report on potential vulnerabilities. This provides quick, accurate, and comprehensive insight into the current state of the system's security.

The CSAT collects relevant data by:

- Scanning the Windows endpoints
- Scanning the Active Directory, Azure AD and Intune
- Scanning content in Office 365 and SharePoint
- Evaluating policies and procedures
- Collecting relevant information through an automated survey

The Stellr team of expert level security specialists will identify and analyze vulnerabilities on your behalf. After your assessment, you'll be provided with an action plan so you can implement improvements quickly and efficiently. We'll even help you prioritize your most immediate needs based on the data.

If you are interested in receiving a Cybersecurity Assessment by the SYNNEX Stellr team, please contact Stellr.MSPServices@SYNNEX.com.